UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN: MENCIÓN SEGURIDAD INFORMÁTICA

ESTUDIO COMPARATIVO DE METODOLOGÍAS DE PENTESTING PARA LA DETECCIÓN DE VULNERABILIDADES DE LA INFRAESTRUCTURA INFORMÁTICA DE UNA COOPERATIVA DE AHORRO Y CRÉDITO SEGMENTO TRES.

Trabajo de Titulación previo a la obtención del Título de Magíster en seguridad informática

AUTOR: Romario David Echeverría Bedón
DIRECTOR: MSc. Luis Alberto Pazmiño Gómez

IBARRA - ECUADOR

2024

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

1. 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:	172373369-5		
APELLIDOS Y NOMBRES:	Echeverría Bedón Romario David		
DIRECCIÓN:	Jacinto Egas y Tobías Mena		
EMAIL:	rdecheverriab@utn.edu.ec		
TELÉFONO FIJO:	No dispone	**TELÉFONO MÓVIL:**	0983203004

DATOS DE LA OBRA	
TÍTULO:	Estudio comparativo de metodologías de pentesting para la detección de vulnerabilidades de la infraestructura informática de una cooperativa de ahorro y crédito segmento tres.
AUTOR (ES):	Echeverría Bedón Romario David
FECHA: DD/MM/AAAA	19/06/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **GRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA:	Magister en computación con mención en seguridad informática
ASESOR /DIRECTOR:	MSc. Luis Alberto Pazmiño Gómez, MSc. Cristina Fernanda Vaca Orellana

2. CONSTANCIAS

El autor (es) manifiesta (n) 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 (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 19 días del mes de junio de 2024

EL AUTOR:

Firmado electrónicamente por:
ROMARIO DAVID
ECHEVERRIA BEDON

Nombre: Echeverría Bedón Romario David
CI.: 1723733695

APROBACIÓN DEL TUTOR

Yo MSc. Luis Alberto Pazmiño Gómez, en calidad de director de la tesis titulada: "ESTUDIO COMPARATIVO DE METODOLOGÍAS DE PENTESTING PARA LA DETECCIÓN DE VULNERABILIDADES DE LA INFRAESTRUCTURA INFORMÁTICA DE UNA COOPERATIVA DE AHORRO Y CRÉDITO SEGMENTO TRES." de autoría del Echeverría Bedón Romario David, para optar por el grado de Magister en Computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 19 días del mes de junio de 2024

Lo certifico

MSc. Luis Alberto Pazmiño Gómez
CI.: 0603784570
DIRECTOR DE TESIS

Dedicatoria

A Isabel Herrera, mi compañera incansable en cada paso de este camino, agradezco profundamente tu apoyo incondicional, tu amor y tu paciencia. Eres mi fuente constante de inspiración.

A mi hermano Cristian Echeverría, quien siempre ha estado a mi lado brindándome su apoyo incondicional y quien fue mi principal impulso para embarcarme en esta maestría.

A mi hermana Ana Echeverría, ejemplo de madurez y valentía, quien nunca se rinde ante las adversidades, inspirándome a seguir adelante.

A mi padre José Echeverría, agradezco su constante respaldo en cada etapa de mi vida.

Y de manera muy especial, a mi madre Susana Bedón, mi mayor motivación. Ella me ha enseñado que, aunque los obstáculos parezcan insuperables, siempre se pueden superar con una sonrisa en el rostro y una mente enfocada en los objetivos. Gracias por ser mi luz en los momentos oscuros.

Por último, pero no menos importante, agradezco a mi familia, amigos y a todas las personas que han formado parte de este viaje llamado vida, su presencia y apoyo incondicional han sido fundamentales en mi camino hacia el éxito.

PER ASPERA AD ASTRA.

Agradecimientos

A la Universidad Técnica del Norte, agradezco sinceramente por brindarme la oportunidad de formar parte de su programa de maestría. Esta experiencia ha sido invaluable para mi desarrollo profesional, llenándome de experiencias enriquecedoras que sin duda marcarán mi trayectoria.

Quiero expresar mi profundo agradecimiento a los distinguidos docentes de esta institución, cuyo compromiso y dedicación han sido fundamentales en mi formación académica durante el programa de posgrado. En particular, deseo reconocer y agradecer al MSc. Luis Pazmiño, mi tutor de proyecto de investigación, por su generosidad al compartir su tiempo, conocimiento y brindarme un apoyo constante a lo largo de este trabajo.

A Isabel Herrera, mi compañera y sostén incondicional durante este trayecto, quiero expresar mi más sincero agradecimiento. Su apoyo constante y su guía han sido indispensables para mantenerme en el camino del bien y alcanzar esta meta con éxito.

A mi amada familia, les estoy eternamente agradecido por su inquebrantable apoyo y preocupación constante. Su respaldo ha sido fundamental para culminar este importante capítulo de mi vida. En especial, deseo reconocer el papel fundamental de mi tía Samia Bedón, cuya ayuda y aliento fueron imprescindibles para hacer realidad este sueño.

Índice de contenidos

RESUMEN ..... **X**

ABSTRACT ..... **XII**

CAPITULO I **1**

EL PROBLEMA **1**

PROBLEMA DE INVESTIGACIÓN 1
INTERROGANTES DE LA INVESTIGACIÓN 3
OBJETIVOS DE LA INVESTIGACIÓN 3
Objetivo general *3*
Objetivos específicos *3*

JUSTIFICACIÓN **4**

JUSTIFICACIÓN 4

CAPITULO II **7**

MARCO REFERENCIAL 7
Antecedentes *7*
MARCO TEÓRICO 8
Conceptos sobre Pentesting y ciberseguridad *8*
Características de la información *9*
Integridad 9
Confidencialidad 9
Disponibilidad 9
Autenticación 10
No repudio 10
Seguridad de la información *10*
Vulnerabilidad 11
Amenaza 11
Riesgo 11
Fases del Pentesting *12*
Reconocimiento 12
Escaneo 12
Obtener acceso 12
Mantener acceso 12
Esconder rastro 12
Seguridad en profundidad *13*
Seguridad física 13
Perímetro 13
Redes 15
Datos 15
Host 15
Seguridad de la información en entidades financieras *16*
Importancia de la seguridad en las entidades financieras. 16
Riesgos y amenazas específicos para el sector financiero. 17
Infraestructura informática de la entidad financiera. 18
Hallazgos significativos sobre la seguridad digital en las entidades financieras en América Latina y el Caribe: 19
Tipos de vulnerabilidades comunes en infraestructuras financieras. *22*
METODOLOGÍAS PENTESTING 23
Osstmm 3 ..... *23*
Pasos para definir un test de seguridad: 23
Tipos de test de seguridad: *24*
Alcance (scope): *26*
Contratos o reglas de acuerdos: *28*

Resultados de los test: ... *28*
Fase regulatoria ... 29
Fase de definición ... 29
Fase de información ... 29
Fase interactiva de prueba de controles ... 30
ISSAF ... 30
Planificación y preparación ... *31*
Evaluación ... *31*
Information Gathering (Obtención de información) ... 31
Network Mapping (Análisis de la red de datos) ... 32
Vulnerability Identification (Identificación de vulnerabilidades) ... 32
Penetration (Pentesting o entrada) ... 33
Gaining Access and privilege escalation (Obtener acceso y escalado de privilegios) ... 33
Enumerating further (Lista de objetivos) ... 33
Compromise remote users/sites (Sitios y usuarios remotos comprometidos) ... 34
Maintaining Access (Mantenimiento de los privilegios y accesos obtenidos) ... 34
Covering Tracks (Borrado de huellas) ... 34
Informe ... *35*
Verbal ... 36
Informe final ... 36
PTES TECHNICAL GUIDELINES ... 37
Pre-engagement Interactions (Interacciones previas al compromiso) ... 37
Intelligence Gathering (Recolección de información) ... 38
Threat Modeling (Modelado de amenazas) ... *39*
Vulnerability analysis (Análisis de vulnerabilidad) ... *39*
Exploitation (Explotación) ... *40*
Post exploitation (Después de la explotación) ... *40*
Reporting (Informes) ... *41*
MARCO LEGAL ... 42

CAPITULO III ... 43

MARCO METODOLÓGICO ... 43
Descripción del área de estudio / descripción del grupo de estudio ... *43*
ENFOQUE Y TIPO DE INVESTIGACIÓN ... 43
Tipo de investigación ... *43*
Diseño de la investigación ... *43*
Población ... *44*
Técnicas e instrumentos de recolección de datos, validez y seguridad ... *45*
TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS ... 46
Procedimiento de análisis de datos. ... *46*

CAPITULO IV ... 47

ANÁLISIS DE VULNERABILIDADES ... 47
Resultados en tablas y figuras. ... *47*
Discusión y resultados ... *49*
Estudio teórico de las metodologías de pentesting para su implementación ... *53*
Análisis comparativo de las metodologías analizadas ... 53
Resultados de la evaluación de las metodologías ... *58*

CAPÍTULO V ... 59

DESARROLLO DE PENTESTING EN UNA COOPERATIVA DE SEGMENTO TRES ... 59
Propósitos específicos de la investigación ... *59*
FUNDAMENTACIÓN DE LA SELECCIÓN DE ISSAF ... 59
Establecer un escenario donde se van a hacer las pruebas de pentesting ... *59*
Ámbito del test ... *60*
Fundamentación de pruebas a puertos abiertos ... *60*
Herramienta por utilizar: Nmap ... *61*

Pruebas a servidores *62*
Herramienta por utilizar: OpenVAS *63*
Fundamentación del uso de Nessus *63*
Ataque de fuerza bruta *64*
Ataques de diccionario *64*
Herramienta por utilizar para generar diccionario: CUPP *65*
Herramienta por utilizar para ataque de fuerza bruta con un diccionario: Burp Suite *65*
Fase i. Planificación y preparación: *66*
Fase ii. Evaluación: *67*
Puertos abiertos *67*
Vulnerabilidades *68*
Fase iii. Reportes, limpieza y destrucción de artefactos: *73*

CONCLUSIONES Y RECOMENDACIONES 75

CONCLUSIONES. 75
RECOMENDACIONES. 76

REFERENCIAS 78

Índice de Tablas

Tabla 1 *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe* 19
Tabla 2 *Canales y secciones de OSSTMM* 27
Tabla 3 *Escala de valoración para evaluación de las metodologías ISSAF, PTES Y OSSTMM* 47
Tabla 4 *Lista de cotejo con las principales vulnerabilidades de instituciones financieras* 48
Tabla 5 *Herramientas de pentesting sugeridas por las metodologías ISSAF, PTES Y OSSTMM* 52
Tabla 6 *Análisis de indicadores de metodologías de pentesting ISSAF, PTES Y OSSTMM* 53
Tabla 7 *Comparación de metodologías de pentesting ISSAF, PTES Y OSSTMM* 55
Tabla 8 *Cantidad de puertos abiertos con Nmap, OpenVAS Y Nessus* 67
Tabla 9 *Cantidad de vulnerabilidades encontradas con las herramientas OpenVAS y Nessus* .. 69

Índice de Figuras

Figura 1 *Esquema del Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM)* 27
Figura 2 *Fases de evaluación ISSAF* 35
Figura 3 *Interacciones pre-compromiso* 38
Figura 4 *Threat modelling* 39
Figura 5 *Esquema de la investigación realizada.* 43
Figura 6 *Fases del Pentesting para la detección de vulnerabilidades.* 45
Figura 7 *Resultados de evaluación a la lista de cotejo con la escala de evaluación de las principales vulnerabilidades de las instituciones financieras* 49
Figura 8 *Prueba de puertos abiertos con Nmap* 61
Figura 9 *Escaneo de vulnerabilidades con Nessus* 64
Figura 10 *Contrato de auditoria técnica de seguridad* 66
Figura 11 *Plan de trabajo Gantt para desarrollo de pentesting.* 67
Figura 12 *Cantidad de puertos abiertos* 67
Figura 13 *Cantidad de vulnerabilidades encontradas* 69
Figura 14 *Identificación de puertos abiertos del servidor principal.* 70
Figura 15 *Prueba al servidor NAS de vulnerabilidad Samba remote code execution vulnerability (CVE-2017-7494)* 70
Figura 16 *Escaneo a una cooperativa de ahorro y crédito segmento tres con OpenVAS* 71
Figura 17 *Login de biométrico en la intranet de una cooperativa de ahorro y crédito segmento tres* 71
Figura 18 *Diccionario de datos* 72
Figura 19 *Ataque de Fuerza Bruta con burp suite.* 72
Figura 21 *Detalle de vulnerabilidades del servidor NAS* 73
Figura 22 *Informe Final generado con la herramienta Nessus de las vulnerabilidades de la cooperativa.* 73
Figura 23 *Informe generado por OpenVAS.* 74

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN: MENCIÓN SEGURIDAD INFORMÁTICA

ESTUDIO COMPARATIVO DE METODOLOGÍAS DE PENTESTING PARA LA DETECCIÓN DE VULNERABILIDADES DE LA INFRAESTRUCTURA INFORMÁTICA DE UNA COOPERATIVA DE AHORRO Y CRÉDITO SEGMENTO TRES.

Autor: Romario David Echeverría Bedón

Tutor: MSc. Luis Pazmiño

Año: 2024

RESUMEN

El presente estudio se enfoca en comparar metodologías de pentesting, detectar las vulnerabilidades en la seguridad de la infraestructura informática de una cooperativa de ahorro y crédito segmento tres en la provincia de Imbabura. Según Raytheon (2015) las instituciones financieras son el objetivo principal para los ciberdelincuentes, el motivo de vulnerar las seguridades son: el lucro financiero, geopolítica o una combinación, en este sentido la Superintendencia de Economía Popular y Solidaria (SEPS) mediante su Oficio Nro. SEPS-SGD-IGT-2021-21112-OFC indica que la ciberseguridad es un campo en continuo cambio y evolución que requieren un control constante, por consiguiente las instituciones financieras deben realizar actualizaciones, pruebas, parches, realizar cambios acordes a los avances tecnológicos y al desarrollo del negocio a fin de mantener la seguridad informática en las organizaciones. El objetivo de esta investigación es evaluar la eficacia de estas metodologías en dicho contexto, para determinar la metodología de pentesting a utilizar en una entidad financiera del segmento tres, además se identificarán vulnerabilidades mediante la ejecución de herramientas de pentesting

extraídas de las metodologías evaluadas y comparar la aplicabilidad en la identificación y explotación de vulnerabilidades, el procedimiento para el análisis de datos fueron mediante un escala evaluativa del 0 a 3 en donde se establece si las metodologías: aluden, mencionan o realizan pruebas de seguridad a las principales vulnerabilidades del sector financiero, mismas que fueron extraídas en base al estudio realizado por Organización de los Estados Americanos (2018), en la cual se obtuvo que ISSAF con una puntuación de 18 supero a OSSTMM Y PTES que obtuvieron 11 puntos, por lo cual se determinó que ISSAF es la metodología más óptima para realizar el pentesting en la cooperativa de ahorro y crédito segmento tres, llevando a cabo diferentes pruebas de seguridad en dicha institución financiera.

Palabras claves: pentesting, evaluación, metodologías, vulnerabilidades, instituciones financieras

ABSTRACT

The present study aims to compare pen testing methodologies and detect vulnerabilities in the cybersecurity infrastructure of a third-tier savings and credit cooperative in the province of Imbabura. According to Raytheon (2015), financial institutions are the primary targets for cybercriminals, driven by motives such as financial gain, geopolitics, or a combination thereof. In this regard, the Superintendence of Popular and Solidarity Economy, through its Office No. SEPS-SGD-IGT-2021-21112-OFC indicates that cybersecurity is a continuous change and evolution field requiring constant monitoring. Consequently, financial institutions must undertake updates, tests, and patches, and make changes following technological advancements and business development to maintain cybersecurity within organizations. This research aims to evaluate the effectiveness of these methodologies in this context and determine the pen testing methodology to be used in segment three financial institutions. Furthermore, vulnerabilities will be identified through the execution of pen testing tools extracted from the evaluated methodologies and compared for applicability in identifying and exploiting vulnerabilities. The data analysis procedure employed an evaluative scale ranging from 0 to 3, establishing whether the methodologies allude to, mention, or conduct security tests on the main vulnerabilities of the financial sector. These vulnerabilities were extracted based on the study conducted by the Organization of American States (2018), which found that ISSAF, scoring 18 points, surpassed OSSTMM and PTES, which scored 11 points. Therefore, it was determined that ISSAF is the most optimal methodology for conducting pen testing in the third-tier savings and credit cooperative, carrying out different security tests in said financial institution.

Keywords: pentesting, assessment, methodologies, vulnerabilities, financial institutions

CAPITULO I

EL PROBLEMA

PROBLEMA DE INVESTIGACIÓN

El constate avance tecnológico ha traído beneficios en la forma de acceder a la información, estas soluciones actualmente son aplicadas en ámbitos educativos, políticos, sociales, económicos, entre otros. Las soluciones tecnológicas son cada vez más variadas y fáciles de usar y se encuentran cada vez más cerca, tanto que actualmente podemos acceder desde nuestro móvil a muchas facilidades tecnológicas.

Raytheon (2015) menciona que el ámbito financiero tiene muchos avances tecnológicos en los últimos años, como: el cajero automático, banca virtual, sistemas de cobros, entre otros, el acceso a la información es práctica e inmediata, sin embargo, este avance conlleva a que la información tenga facilidad de acceso para los hackers, quienes aprovechan el amplio número de posibilidades de acceder a estos datos y usarlos para sus beneficios propios.

Las instituciones financieras actualmente tienen el reto de combatir a estas personas mal intencionadas, evitar pérdida de ingresos y confianza del consumidor, rentabilidad reducida, daño a la reputación, mayores niveles de deuda y devaluaciones de divisas, entre otros riesgos.

Según Raytheon (2015) el sector financiero es el principal objetivo para los ciberdelincuentes, puesto que en estas instituciones es donde se encuentra el dinero. La motivación de vulnerar las seguridades es la ganancia financiera, geopolítica o una combinación, los hackers tienen una amplia gama de herramientas y patrocinadores de estas.

Estos factores han conllevado a ciberataques sofisticados contra el sector financiero, prevenir el robo de datos en este sector es de suma importancia para conservar la integridad de los

sistemas; si bien supone que estos servicios están a la vanguardia de la implementación de ciberseguridad, sin embargo, el constate avance y la alta demanda de ataques conllevan a que sea necesario probar a través de un pentesting estas seguridades, para encontrar vulnerabilidades.

En esta medida la Superintendencia de Economía Popular y Solidaria (SEPS) mediante su Oficio Nro. SEPS-SGD-IGT-2021-21112-OFC menciona que, la seguridad cibernética es un campo en constante cambio y evolución que requiere una supervisión continua. Es necesario realizar actualizaciones, pruebas, parches y realizar cambios acordes a los avances tecnológicos y al desarrollo del negocio. La SEPS considera que implementar controles es fundamental para la seguridad en la infraestructura tecnológica de las instituciones financieras. No abordar estos procesos es una de las principales razones por las cuales se producen brechas de seguridad. En este contexto, recomendamos implementar al menos los siguientes controles, sin descartar la aplicación de medidas adicionales o complementarias. (Chimbo, 2021)

Desde este punto de vista la SEPS propone en el Oficio Nro. SEPS-SGD-IGT-2021-21112-OFC

“Las entidades deberán al menos una vez al año revisar la seguridad de sus activos mediante ejercicios prácticos y controlados, que simulen varios tipos de amenazas posibles, tales como Hacking Ético, pentesting, entre otros; exponiendo a la infraestructura que soporta los servicios de la entidad a diferentes escenarios de nivel básico a avanzando en medida de lo posible.”

La Superintendencia de Economía Popular y Solidaria (SEPS) busca que las entidades financieras fortalezcan su seguridad informática, sin embargó en ninguna normativa propone la utilización de una metodología de pentesting para la detección de vulnerabilidades, en la cual las

instituciones se puedan ayudar para realizar los respectivos procesos de verificación, por tales razones se plantean las siguientes preguntas.

INTERROGANTES DE LA INVESTIGACIÓN

¿Cuáles son las metodologías de pentesting más utilizadas en el sector financiero?

¿Qué metodologías de pentesting son más efectivas para la detección temprana de vulnerabilidades en una cooperativa de ahorro y crédito de segmento tres?

¿Cuáles son las principales vulnerabilidades en una entidad financiera de segmento tres, y qué herramientas de pentesting se pueden utilizar para identificar estos hallazgos?

¿Cómo se comparan las metodologías de pentesting en términos de su capacidad para identificar y explotar vulnerabilidades?

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo general

Comparar metodologías de pentesting, para la detección temprana de vulnerabilidades de la seguridad en la infraestructura informática de una cooperativa de ahorro y crédito segmento tres en la provincia de Imbabura.

Objetivos específicos

Determinar las metodologías de pentesting aplicables en una infraestructura de una entidad financiera segmento tres.

Identificar vulnerabilidades por medio de la ejecución de herramientas de pentesting en una entidad financiera de segmento tres.

Comparar la aplicabilidad de las metodologías de pentesting en la identificación y explotación de vulnerabilidades de seguridad en la infraestructura de una entidad financiera de segmento tres.

JUSTIFICACIÓN

JUSTIFICACIÓN

Raytheon (2015) afirma que uno de los activos más importantes de las organizaciones es la información digital y a medida que se incrementa es fundamental contar con métodos, estrategias y tecnologías para salvaguardar la misma, de forma que se garantice y preserve la integridad, confidencialidad y disponibilidad como ejes principales.

Rivera (2016) menciona que el Pentesting como metodología de detección de vulnerabilidades es indispensable dentro de las instituciones financieras para mantener la seguridad en los sistemas informáticos y evitar la pérdida de datos, es por esta razón que las instituciones tienen como gran desafío prevenir los ataques de hackers malintencionados.

En búsquedas bibliográficas sobre las metodologías de Pentesting aplicadas en instituciones financieras Villares Saltos (2017) menciona:

“En el desarrollo del Pentesting para monitorear los niveles de seguridad en la intranet de la cooperativa de ahorro y crédito segmento tres de la ciudad de Ventanas, se utilizó la metodología del PTES Technical Guidelines que consta de las siguientes fases: 1.- Reconocimiento 2.- Escaneo 3.- Obtener Acceso 4.- Escribir Informe 5.- Presentar el Informe” (pág. 43)

Para Mora Ortega (2017) en su estudio sugiere:

“PTES Technical Guidelines Esta metodología está orientada 100% en la práctica y la obtención de la información de una forma paulatina vulnerando cada vez más cada nivel de seguridad, en la obtención de la información crítica para el negocio, las fases son:

Reconocimiento, Descubrimiento, Obtención de Acceso, Mantener el acceso y Limpiar el rastro." (pág. 92)

"OSSTMM es una metodología muy enfocada que pretende no solo evaluar las seguridades que debe tener una organización, sino que se administra también la ejecución de la prueba en cada una de sus etapas, para que se lo lleve de una manera correcta" (p. 42)

Por otra parte, Garcia Vega et al. (2022) en su investigación indican que:

"ISSAF (Information Systems Security Framework): El objetivo de esta metodología es proporcionar elementos de manera minuciosa para el análisis de comprobación en base a la información de los sistemas de gestión en una situación. Las redes de datos cumplen el rol de conectar computadoras entre puntos de conexión, lo cual demanda requerimientos a cumplir de manera óptima, estos son 24 sistemas formados por múltiples equipos que se enlazan por medio de comunicaciones, estas pueden ser conexiones de cable LAN, señal de radio y fibra óptica"

Tomando en cuenta estas investigaciones y la necesidad que tienen las entidades financieras, con respecto a la alta demanda de intentos de vulneración de seguridad en los sistemas de información, para ello se analizará las vulnerabilidades en la infraestructura de una cooperativa de ahorro y crédito segmento tres, realizando pruebas de pentesting con las metodologías antes mencionas, esta investigación va comparar la efectividad en la detección temprana de vulnerabilidades de seguridad en la infraestructura utilizado las metodologías PTES e ISSAF, el pentesting estará adaptado a las necesidades y preocupaciones específicas de la institución. Cada prueba de intrusión será única y su éxito dependerá de los métodos empleados.

Según Las Naciones Unidas (2018) en el Eje Institucional y en el "Objetivo 16: Promover sociedades, justas, pacíficas e inclusivas, en el punto 16.10 Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y

los acuerdos internacionales", este objetivo va encaminado con la disponibilidad e integridad de la información que debe bridar cada institución a servicio de sus clientes y usuarios, en este sentido es fundamental para las instituciones cumplir con los estándares de seguridad de su información, con un análisis a profundidad de sus riesgos y vulnerabilidades a fin de solventar y evitar que la información de la institución se vea adulterada o borrada por hackers.

Las Naciones Unidas (2018) en el Eje Económico, en su "Objetivo 2: Impulsar un sistema económico con reglas claras que fomente el comercio exterior, turismo, atracción de inversiones y modernización del sistema financiero nacional. Este se liga al ("Eje Económico – Plan Nacional 2021 – 2025") Y el Objetivo 4: Garantizar la gestión de las finanzas públicas de manera sostenible y transparente.", hacen mención a que es indispensable modernizar la infraestructura de los sistemas financieros, pero a su vez garantizar una gestión de su información de forma sostenible y trasparente, a fin de que los usuarios tengan la confianza de que sus datos entregados están seguros y no serán adulterados, para ello es necesario contar con el personal, infraestructura y software que garantice el correcto funcionamiento del mismo y para ello es necesario realizar un análisis actual de los niveles de seguridad mediante un Pentesting a la infraestructura y a partir de esto tomar las medidas correspondientes en las instituciones.

Este proyecto de investigación se relaciona con la línea de investigación Nro. 10 vigente y aprobada por el Honorable Consejo Universitario de la UTN: Desarrollo, aplicación de software y cyber security (seguridad cibernética) (UTN, 2023).

CAPITULO II

MARCO REFERENCIAL

Antecedentes

Desde sus inicios, los sistemas informáticos han enfrentado el desafío de proteger la información con la que trabajan y, a medida que avanza la tecnología, las técnicas de seguridad informática han evolucionado considerablemente para hacer frente a la sofisticación de los ataques y dado que los atacantes también están desarrollando métodos cada vez más sofisticados para violar dicha seguridad, es necesario anticipar tales eventos mediante la simulación de pruebas de pentesting.

Una prueba de pentesting conlleva etapas y fases para su desarrollo, esta se compone de la planificación, reconocimiento, descubrimiento, evaluación, intrusión, análisis y reporte. Teniendo en claro las fases es necesario definir las herramientas necesarias para cumplir con un pentesting, Salas (2012) menciona que existen diversas herramientas para realizar las pruebas que varían en su grado de complejidad y requieren que el atacante o Pentester tenga una gran habilidad y astucia para manejarlas. estas herramientas abarcan desde simples scanners de puertos hasta algoritmos complejos para descifrar claves, sistemas de intrusión por fuerza bruta, herramientas de sniffing de redes y penetración de firewalls, entre otras. La diversidad y sofisticación de estas herramientas reflejan la continua evolución del campo de la seguridad informática.

Para Burbano (2019) Se pueden emplear diversas herramientas especializadas en las pruebas de pentesting para agilizar y mejorar la detección de vulnerabilidades. Realizar una prueba de pentesting es una tarea compleja porque exige un sólido conocimiento de las tecnologías presentes en los sistemas, aplicaciones y servicios involucrados, así como una amplia perspectiva y experiencia en el comportamiento de diferentes sistemas operativos.

Según León et al. (2021) el Pentesting financiero brinda hoy la capacidad de revisar y verificar los agujeros de seguridad para proteger la información de los clientes, la misión de un hacker ético hoy es implementar tecnología y seguir protocolos de seguridad para determinar y diagnosticar los servicios los cuales pueden ser afectados o vulnerados por personas malintencionadas y crear un riesgo de posible pérdida de información y dinero, las metodologías de pentesting representa una fotografía al estado de la ciberseguridad de una organización en un determinado tiempo.

La finalidad del proyecto es llegar a descubrir qué tipo de metodología de pentesting se acopla mejor a una entidad financiera de segmento tres, las cuales están regidas por normativas, que piden que se cumpla con la integridad, disponibilidad y confidencialidad de la información, para ello es necesario realizar pruebas de pentesting con el fin de solventar los agujeros de seguridad de la institución, es por esto que se analizará qué tipo de metodología es la más adecuada para encontrar los vulnerabilidades y qué tipo de herramientas se utilizará para detectar las misas.

MARCO TEÓRICO

Conceptos sobre Pentesting y ciberseguridad

Rivera (2016) sostiene que **e**l Pentesting está ganando terreno en las instituciones financieras. A medida que los servicios tecnológicos avanzan; las transacciones en línea, las compras y los servicios bancarios, se vuelven más comunes, es importante tener en cuenta que los usuarios utilizan cada vez más estos servicios ofrecidos por los bancos para agilizar los procesos tecnológicos. Sin embargo, esto conlleva un aumento en la vulnerabilidad de la seguridad informática, ya que los ataques de phishing contra instituciones financieras están en aumento. Como respuesta, se están implementando nuevas tecnologías de seguridad en las plataformas virtuales, así como también se están desarrollando y mejorando constantemente las herramientas

utilizadas para atacar con mayor precisión y calidad. El objetivo siempre es comprometer la seguridad informática, poniendo en riesgo los pilares fundamentales de confidencialidad, integridad y disponibilidad de la información.

Características de la información

Integridad

El mantenimiento de la integridad de la información se refiere no solo a la información que se encuentra almacenada en los equipos informáticos, sino también a aquella que se encuentra en los respaldos, documentos, reportes y cualquier otro medio que se utilice para su registro y almacenamiento. Cornejo Velázquez et al. (2015) describe que la integridad de la información tiene como objetivo evitar que esta sea modificada, alterada o corrompida por personas no autorizadas, asegurando así su precisión y fiabilidad.

Confidencialidad

Según Velázquez et al. (2015) La confidencialidad de la información se refiere a garantizar que solamente las personas autorizadas tengan acceso a ella, evitando su divulgación, comunicación, robo o sabotaje por parte de personas o sistemas no autorizados.

Disponibilidad

Velázquez et al. (2015) se refiere a que la información debe estar disponible para quienes tienen autorización para acceder a ella, ya sea a través de personas, procesos o aplicaciones. El acceso a la información debe ser controlado y limitado a las personas autorizadas y solo en el momento en que lo necesiten.

Autenticación

La autenticación es un proceso que permite verificar la identidad del emisor de la información. Al recibir un mensaje, es fundamental que el sistema se asegure de que el remitente es realmente quien dice ser y no un tercero que se hace pasar por él, lo que se conoce como suplantación de identidad. En los sistemas informáticos, la autenticación se realiza a través de una combinación de cuenta de usuario y contraseña de acceso, que permite verificar la identidad del usuario que intenta acceder al sistema (Velázquez et al. 2015).

No repudio

El servicio de seguridad de *No repudio* garantiza que tanto el emisor como el receptor de un mensaje no pueden negar haber enviado o recibido la transmisión. Esto significa que, aunque el emisor pueda verificar que el mensaje fue enviado, no puede negar haberlo hecho después, asegurando así la integridad del mensaje y su origen (ISO, 2013).

La seguridad de No repudio impide que tanto el emisor como el receptor de un mensaje nieguen haber enviado o recibido la transmisión. Esto significa que, al enviar un mensaje, el receptor puede verificar que el emisor lo envió y, al recibir un mensaje, el emisor puede verificar que el receptor lo recibió. De esta manera, se garantiza la autenticidad y la integridad del mensaje (Velázquez et al. 2015).

Seguridad de la información

La seguridad de la información se apoya en la tecnología y su objetivo es garantizar la confidencialidad de los datos. La información es un activo valioso y se encuentra centralizada, lo que la hace vulnerable a la divulgación, el uso indebido, el robo, el borrado o el sabotaje, lo que afectaría su integridad, disponibilidad y confidencialidad (Laudon et al. 2016).

Vulnerabilidad

Según Laudon et al. (2016) Una vulnerabilidad se refiere a una debilidad o falla en un sistema informático, software o infraestructura que podría ser explotada por atacantes para comprometer la seguridad y causar daño, perturbación o acceso no autorizado a la información.

Amenaza

Ambit Bst (2020) considera que una amenaza hace referencia a cualquier suceso o acción que tiene la capacidad de ocasionar perjuicio o poner en riesgo la seguridad de los sistemas, datos o infraestructuras tecnológicas. Estas amenazas pueden originarse de múltiples fuentes, como hackers, malware, virus, ataques de phishing, intrusos internos, desastres naturales, errores humanos, entre otros.

Estas amenazas pueden tener una variedad de propósitos, como la sustracción de información confidencial, la interrupción de servicios, el perjuicio a la reputación de una organización, la extorsión, el sabotaje o el espionaje. Valiéndose de vulnerabilidades en sistemas y redes, se aprovechan de debilidades en las políticas de seguridad, o engañan a los usuarios para obtener acceso no autorizado.

Riesgo

Se considera amenaza informática a cualquier factor que pueda ocasionar perjuicio a los sistemas informáticos, resultando en una consecuencia negativa que interrumpe las operaciones de una organización o empresa (Velázquez et al. 2015).

Fases del Pentesting

Reconocimiento

Ortega (2017) menciona que esta etapa implica que un atacante busca recopilar información crucial sobre el objetivo antes de llevar a cabo el ataque. También puede ser considerada como un posible punto de retorno en alguna de las fases, ya que se pueden descubrir más detalles que requieren ser identificados.

Escaneo

Ortega (2017) señala que el proceso de escaneo tiene como objetivo detectar vulnerabilidades y puntos débiles en un sistema o red, con el fin de determinar cómo podrían ser aprovechados.

Obtener acceso

León et al. (2021) afirma que la obtención de acceso se refiere al momento en el que se lleva a cabo el ataque real, como utilizar un exploit o fallo de seguridad para obtener una contraseña.

Mantener acceso

León et al. (2021) describe que una vez que un atacante ha logrado obtener acceso a un sistema o red, su objetivo es avanzar y obtener mayores niveles de control y autoridad.

Esconder rastro

Según Castro (2017) eliminar cualquier rastro que pueda revelar su presencia. Un hacker ético, con el objetivo de prevenir ataques responde a las siguientes preguntas: ¿Qué información puede un intruso obtener sobre el objetivo? ¿Qué acciones puede llevar a cabo un intruso con esa información? ¿Es posible detectar un intento de ataque?

Seguridad en profundidad

Según Ortega (2017) es crucial considerar que la seguridad no depende únicamente de los dispositivos de seguridad como firewall, routers, IPS, IDS y antivirus, sino que debe ser abordada de manera integral. Esto implica que, para proteger la información proporcionada por los sistemas de información, se debe fomentar una cultura de seguridad en la que todos estén involucrados. Esto incluye desde la definición de políticas relacionadas con la cultura de seguridad de las personas, hasta los mecanismos de seguridad física, los dispositivos electrónicos de seguridad, los controles de acceso a la información, el cifrado, entre otros aspectos.

Seguridad física

Según Urbina (2016) la seguridad física son las medidas y controles implementados para proteger los recursos y activos físicos relacionados con los sistemas informáticos. Esto incluye la protección de los componentes físicos como: servidores, equipos de red, dispositivos de almacenamiento, centros de datos y otros elementos críticos de infraestructura. La seguridad física en informática aborda los riesgos y amenazas que pueden surgir debido a accesos no autorizados, robos, daños físicos, vandalismo, desastres naturales y otros incidentes. Su objetivo es salvaguardar la integridad, confidencialidad y disponibilidad de los activos informáticos y garantizar la continuidad de las operaciones.

Perímetro

Según Urbina (2016) el perímetro se refiere al límite de una red o sistema informático. Es el punto de conexión entre la red interna de una organización y redes externas, como Internet. Se establecen controles de seguridad en el perímetro para proteger los activos y datos de la organización de amenazas externas. Esto se logra mediante el uso de firewalls, sistemas de detección de intrusiones y otros mecanismos de seguridad. Sin embargo, con los avances

tecnológicos, el concepto de perímetro ha evolucionado, ya que las organizaciones adoptan enfoques más flexibles y basados en la identidad para la seguridad, teniendo en cuenta la movilidad y la nube.

Redes

Para Buendía (2013) las redes se refieren a la interconexión de dispositivos y sistemas informáticos que permiten el intercambio de datos y recursos. Una red informática es un conjunto de equipos, como computadoras, servidores, enrutadores y conmutadores, que se conectan entre sí a través de cables o conexiones inalámbricas. Estas redes facilitan la comunicación y colaboración, permitiendo compartir archivos, impresoras, aplicaciones y acceso a Internet. Además, las redes informáticas pueden ser locales (LAN) o extensas (WAN), dependiendo del alcance geográfico. También existen redes privadas virtuales (VPN) que permiten conexiones seguras a través de redes públicas como Internet.

Datos

Según Urbina (2016) los datos se refieren a la información cruda y sin procesar que se almacena y se manipula en sistemas informáticos. Los datos pueden tomar diversas formas, como: números, texto, imágenes, videos o cualquier otro tipo de contenido digital. Estos datos pueden ser ingresados, almacenados, organizados y procesados por computadoras y otros dispositivos electrónicos. La información derivada de los datos puede utilizarse para tomar decisiones, realizar análisis, generar informes y llevar a cabo diversas tareas. La gestión adecuada de los datos es fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información en un entorno informático.

Host

Para Buendía (2013) host se refiere a un dispositivo o sistema que proporciona servicios, recursos o información en una red. Un host puede ser una computadora, servidor, dispositivo de red o cualquier otro equipo conectado a una red. Actúa como un punto final en la comunicación de red y puede tener una dirección IP única que lo identifica en la red. Los hosts pueden ofrecer

servicios como alojamiento de sitios web, correo electrónico, almacenamiento de datos, impresión, entre otros. Además, los hosts pueden funcionar como clientes al solicitar y acceder a servicios o recursos proporcionados por otros hosts en la red.

Seguridad de la información en entidades financieras

Importancia de la seguridad en las entidades financieras.

Según Wirton (2021) la seguridad en las entidades financieras es de vital importancia debido a la gran cantidad de información confidencial y sensible que manejan, como datos bancarios, transacciones financieras y datos personales de sus clientes. La falta de seguridad en estas instituciones puede llevar a consecuencias graves, tanto para los clientes como para la propia entidad. Algunas de estas consecuencias pueden incluir:

Robo de información: para Wirton (2021) Los ciberdelincuentes pueden acceder a los sistemas de la entidad y robar información financiera, lo que puede resultar en pérdidas económicas para los clientes y daños a la reputación de la entidad.

Fraude financiero: Wirton (2021) menciona que, si los sistemas de seguridad de una entidad financiera son vulnerables, los delincuentes pueden realizar transacciones fraudulentas, tanto en nombre de la entidad como en nombre de los clientes.

Violación de la privacidad: Wirton (2021) señala que la falta de seguridad puede llevar a la exposición de datos personales de los clientes, lo que puede resultar en problemas de privacidad y posibles violaciones legales.

Daños a la reputación: para Wirton (2021) un incidente de seguridad en una entidad financiera puede dañar seriamente su reputación y la confianza de los clientes. Esto puede afectar negativamente a la entidad a largo plazo, ya que los clientes pueden optar por no hacer negocios con una entidad que no garantice la seguridad de su información.

Por todas estas razones, es fundamental que las entidades financieras implementen medidas de seguridad sólidas, como el uso de metodologías de pentesting, para detectar vulnerabilidades y proteger la información de sus clientes. Esto ayudará a garantizar la integridad, disponibilidad y confidencialidad de la información, y a mantener la confianza de los clientes en la entidad.

Riesgos y amenazas específicos para el sector financiero.

El sector financiero se enfrenta a una serie de riesgos y amenazas específicos en relación con la seguridad informática. Algunos de ellos incluyen:

Riesgo de fraude financiero: según Commission Federal Trade (2016) Los ciberdelincuentes pueden intentar obtener acceso a las cuentas bancarias de los clientes, realizar transferencias no autorizadas de fondos o utilizar información confidencial para cometer fraudes financieros.

Riesgo de robo de datos personales: la Commission Federal Trade (2016) menciona que la información personal y financiera de los clientes, como números de tarjetas de crédito, contraseñas y números de seguridad social, puede ser robada y utilizada para cometer fraudes o robo de identidad.

Riesgo de ciberataques: para la Wirton (2021) los ciberdelincuentes pueden utilizar diferentes técnicas, como ataques de phishing, malware o ransomware, para infiltrarse en los sistemas informáticos de las entidades financieras y obtener acceso no autorizado a la información confidencial.

Riesgo de interrupción del servicio: la Commission Federal Trade (2016) indica que los ciberataques pueden causar interrupciones en los sistemas informáticos de las entidades financieras, lo que puede afectar la disponibilidad de los servicios bancarios y causar pérdidas económicas tanto para los clientes como para la propia entidad.

Riesgo de incumplimiento de regulaciones: Las entidades financieras están sujetas a regulaciones y normativas estrictas en relación con la seguridad de la información y la protección de datos personales. El incumplimiento de estas regulaciones puede resultar en sanciones legales y pérdida de confianza por parte de los clientes.

Es importante que las entidades financieras implementen medidas de seguridad robustas, como firewalls, sistemas de detección y prevención de intrusiones, encriptación de datos y capacitación en seguridad informática para el personal, a fin de mitigar estos riesgos y proteger la información confidencial de sus clientes.

Infraestructura informática de la entidad financiera.

Según Wirton (2021) la infraestructura informática juega un papel fundamental en la operación de las entidades financieras. Hoy en día, la mayoría de las transacciones bancarias se realizan de forma electrónica, lo que implica que la infraestructura informática debe estar disponible, segura y confiable en todo momento.

La infraestructura informática de una entidad financiera incluye tanto hardware como software. En cuanto al hardware, se requieren servidores, equipos de almacenamiento, redes de comunicación y dispositivos de seguridad, como firewalls y sistemas de detección de intrusiones. Estos componentes son necesarios para garantizar que los sistemas estén en funcionamiento y puedan manejar un gran volumen de transacciones de manera eficiente.

En cuanto al software, Villares Saltos (2017) menciona que se requieren sistemas operativos, bases de datos, aplicaciones de banca en línea y sistemas de seguridad. Estos sistemas permiten a las entidades financieras realizar operaciones bancarias, gestionar cuentas y proteger la información confidencial de los clientes.

Por otra parte, Chimbo (2021) menciona que la infraestructura informática también debe tener mecanismos de respaldo y recuperación de datos, para garantizar la disponibilidad y la integridad de la información en caso de un desastre o un fallo en el sistema.

En resumen, la infraestructura informática es esencial para que las entidades financieras puedan ofrecer servicios bancarios de manera eficiente y segura. Por lo tanto, es fundamental que estas entidades inviertan en tecnología y en medidas de seguridad para proteger su infraestructura informática y la información confidencial de sus clientes.

Hallazgos significativos sobre la seguridad digital en las entidades financieras en América Latina y el Caribe:

En la Tabla 1 se muestran los hallazgos significativos de un análisis realizado por Organización de los Estados Americanos (2018)

Tabla 1

Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe

Bancos Grandes	Bancos Medianos	Bancos Pequeños
En el 67% existe una única área responsable de la seguridad digital	En el 74% existe una única área responsable de la seguridad digital	En el 79% existe una única área responsable de la seguridad digital
En el 61% existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital	En el 38% existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital	En el 46% existe un (1) nivel jerárquico entre el CEO y el máximo responsable de la seguridad digital
Los Bancos grandes (27%) cuenta con un equipo conformado por 16- 30 miembros	Los Bancos medianos (48%) cuenta con un equipo conformado por 1-5 miembros	Los Bancos pequeños (94%) cuenta con un equipo conformado por 1-5 miembros

El 26% no están implementando herramientas, controles o procesos usando tecnologías digitales emergentes	El 44% no están implementando herramientas, controles o procesos usando tecnologías digitales emergentes	El 67% no están implementando herramientas, controles o procesos usando tecnologías digitales emergentes
Fueron objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de casi todos por la mayoría en la región	Fueron objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de algunos por la mayoría en la región	Fueron objeto de ataques de algunos tipos de eventos de seguridad digital, resaltando identificación de pocos por la mayoría en la región
El 40% identificaron ocurrencia de eventos de malware diariamente	El 28% identificaron ocurrencia de eventos de malware diariamente	El 9% identificaron ocurrencia de eventos de malware diariamente
La mayoría (41%) detecta entre un 61% y un 80% de eventos con sistemas propios	La mayoría (28%) detecta entre un 61% y un 80% de eventos con sistemas propios	La mayoría (40%) detecta entre un 0% y un 20% de eventos con sistemas propios
El 65% manifiestan que sí fueron víctimas de ataques exitosos	El 43% manifiestan que sí fueron víctimas de ataques exitosos	El 19% manifiestan que sí fueron víctimas de ataques exitosos
El 73% realizó una evaluación de madurez y está adelantando actualmente las acciones correspondientes	El 47% realizó una evaluación de madurez y está adelantando actualmente las acciones correspondientes	El 21% realizó una evaluación de madurez y está adelantando actualmente las acciones correspondientes
El 85% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos	El 72% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos	El 56% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos
El 77% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su	El 65% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando	El 56% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando

información personal se haya visto comprometida	su información personal se haya visto comprometida	su información personal se haya visto comprometida
El 81% reportan los incidentes sufridos ante autoridad de aplicación de la ley	El 65% reportan los incidentes sufridos ante autoridad de aplicación de la ley	El 46% reportan los incidentes sufridos ante autoridad de aplicación de la ley
El 57% manifestaron que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 59% manifestaron que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 67% manifestaron que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal
El presupuesto destinado a la seguridad digital equivale aprox. al 1,86% del EBITDA del año inmediatamente anterior	El presupuesto destinado a la seguridad digital equivale aprox. al 2,14% del EBITDA del año inmediatamente anterior	El presupuesto destinado a la seguridad digital equivale aprox. al 2,27% del EBITDA del año inmediatamente anterior
En el 65%, el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediatamente anterior	En el 47%, el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediatamente anterior	En el 25%, el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediatamente anterior
El presupuesto asignado en 2017 a un miembro promedio del equipo de seguridad digital fue de US $22.713	El presupuesto asignado en 2017 a un miembro promedio del equipo de seguridad digital fue de US $21.766	El presupuesto asignado en 2017 a un miembro promedio del equipo de seguridad digital fue de US $13.927
El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 24,1%	El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 23,85%	El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 23,33%
El 53% manifestaron que el costo total de respuesta y de recuperación ante incidentes equivale en promedio a	El 81% manifestaron que el costo total de respuesta y de recuperación ante incidentes equivale en promedio a	El 83% manifestaron que el costo total de respuesta y de recuperación ante

menos del 1% del EBITDA del anterior año fiscal El costo total de respuesta y de recuperación ante incidentes de seguridad digital en 2017 equivale aprox. al 1,86% del EBITDA del año inmediatamente anterior (US $5.253.000 en 2017 aprox.)	menos del 1% del EBITDA del anterior año fiscal El costo total de respuesta y de recuperación ante incidentes de seguridad digital en 2017 equivale aprox. al 1,38% del EBITDA del año inmediatamente anterior (US $605.000 en 2017 aprox.)	incidentes equivale en promedio a menos del 1% del EBITDA del anterior año fiscal El costo total de respuesta y de recuperación ante incidentes de seguridad digital en 2017 equivale aprox. al 1,36% del EBITDA del año inmediatamente anterior (US $161.000 en 2017 aprox.)

Nota. Fuente: Organización de los Estados Americanos (2018)

Tipos de vulnerabilidades comunes en infraestructuras financieras.

Existen varios tipos de vulnerabilidades comunes en las infraestructuras financieras, entre las cuales se destacan:

Vulnerabilidades de software: para Wirton (2021) estas vulnerabilidades se producen cuando hay errores o fallas en el código de los programas o aplicaciones utilizados en la infraestructura financiera. Estas vulnerabilidades pueden permitir a los atacantes explotar las debilidades del software y acceder a información sensible o realizar acciones no autorizadas.

Vulnerabilidades de red: según Wirton (2021) Estas vulnerabilidades se refieren a las debilidades en la configuración de la red utilizada en la infraestructura financiera. Esto incluye problemas como puertos abiertos innecesarios, configuraciones incorrectas de firewall o routers, entre otros. Estas vulnerabilidades pueden permitir a los atacantes acceder a la red y comprometer la seguridad de los sistemas y datos.

Vulnerabilidades de acceso: Chimbo (2021) menciona que estas vulnerabilidades se producen cuando hay debilidades en los mecanismos de autenticación y control de acceso

utilizados en la infraestructura financiera. Esto incluye contraseñas débiles, falta de autenticación de dos factores, privilegios de usuario mal configurados, entre otros. Estas vulnerabilidades pueden permitir a los atacantes obtener acceso no autorizado a los sistemas y datos sensibles.

Vulnerabilidades físicas: según Chimbo (2021) estas vulnerabilidades se refieren a las debilidades en las medidas de seguridad física utilizadas en la infraestructura financiera. Esto incluye problemas como cámaras de seguridad mal configuradas, falta de controles de acceso físico, falta de medidas de protección contra incendios, entre otros. Estas vulnerabilidades pueden permitir a los atacantes acceder físicamente a los sistemas y equipos, comprometiendo la seguridad de la infraestructura.

La identificación y corrección de vulnerabilidades es crucial para salvaguardar la información financiera y asegurar la confianza en los servicios proporcionados por las instituciones. Para lograr esto, se deben implementar medidas de seguridad adecuadas, tales como: auditorías de seguridad, pruebas de pentesting y actualizaciones regulares de software y hardware.

METODOLOGÍAS PENTESTING

Osstmm 3

Según ISECOM (2010) OSSTMM (Open Source Security Testing Methodology Manual) es un marco de trabajo para evaluar la seguridad de sistemas informáticos y redes. La OSSTMM proporciona un enfoque sistemático y estructurado para evaluar la seguridad de un sistema, utilizando métodos y técnicas basadas en la experiencia de profesionales de la seguridad.

Pasos para definir un test de seguridad:

- Establecer los mecanismos de control que se utilizarán para evaluar la seguridad de los activos que se desean proteger.
- Es esencial identificar la *"zona de acuerdos"* en esta metodología, ya que es donde

se encuentran los procesos, mecanismos y servicios que protegen los activos.

- Establecer los límites de la zona externa es fundamental para proteger las operaciones de los activos, lo que implica delimitar el alcance de la prueba.
- Determinar el alcance de la prueba, ya sea interna o externa a la empresa, es esencial. Los vectores indican las direcciones de interacción, que pueden ser de dentro hacia fuera o viceversa, de dentro a dentro o de fuera a fuera. Cada vector debe ser probado individualmente y durante un período de tiempo limitado.
- La toma de decisiones sobre qué equipo se requiere para cada prueba se fundamenta en la interacción entre vectores que puede ocurrir en varios niveles. Estos niveles se han dividido en 5 canales por función, y cada canal debe ser probado de forma separada para cada vector.
- Se desarrolla un plan para identificar la información deseada en cada prueba y para planificar las pruebas a realizar.
- Es crucial garantizar que las pruebas a realizar cumplan con las disposiciones y acuerdos previos, evitando así malentendidos o expectativas engañosas.

Tipos de test de seguridad:

Según la ISECOM (2010) elegir el tipo de test de seguridad no implica necesariamente que este deba estar orientado únicamente a una metodología específica. En la práctica, es posible individualizar las pruebas y adaptarlas según las necesidades y características de cada proyecto. Es decir, la elección del tipo de test se realizará en función de la metodología aplicada y de las técnicas utilizadas.

Blind (a ciegas): Cuando nos referimos a la fase de "blind testing" dentro del ámbito de la ciberseguridad, nos encontramos frente a un escenario en el cual el pentester o auditor se enfrenta

al objetivo sin poseer conocimiento alguno sobre las defensas, canales de acceso o activos disponibles. Este tipo de prueba representa un desafío para el propio auditor, ya que su nivel de preparación y habilidades determinarán su capacidad para superar este desafío. (ISECOM, 2010)

Double blind o técnica de la caja negra, es ampliamente utilizada en diversos campos de investigación y experimentación. Este enfoque se caracteriza por el desconocimiento total del objetivo de estudio, donde ni los evaluadores ni los sujetos implicados son conscientes de la información o variables que están siendo evaluadas. (ISECOM, 2010)

Gray box: El test de caja gris es una modalidad de prueba en la cual el atacante tiene un conocimiento detallado de los canales de acceso de un sistema. A diferencia de otros tipos de pruebas, en el test de caja gris es posible determinar de antemano el alcance de la evaluación. La eficacia de este tipo de test radica en la calidad de la información aportada por el auditor, incluso antes de finalizar las pruebas. (ISECOM, 2010)

Double gray box: o caja doble gris, también conocida como caja blanca, implica que el auditor tiene un conocimiento limitado de las defensas y activos, pero posee un conocimiento completo de los canales. Esta metodología difiere del test previo en que no solo depende de la calidad de la información recibida, sino también del grado de comprensión del objetivo. (ISECOM, 2010)

Tándem: El auditor forma parte del equipo de seguridad y control de procesos, y tanto el cliente como el auditor tienen conocimiento de los términos de la auditoría. Se realizarán pruebas a los controles aplicados y se protegerá el objetivo mediante pruebas reales. El éxito de la auditoría depende de la meticulosidad en la preparación de las pruebas, para obtener una visión general de los resultados obtenidos. (ISECOM, 2010)

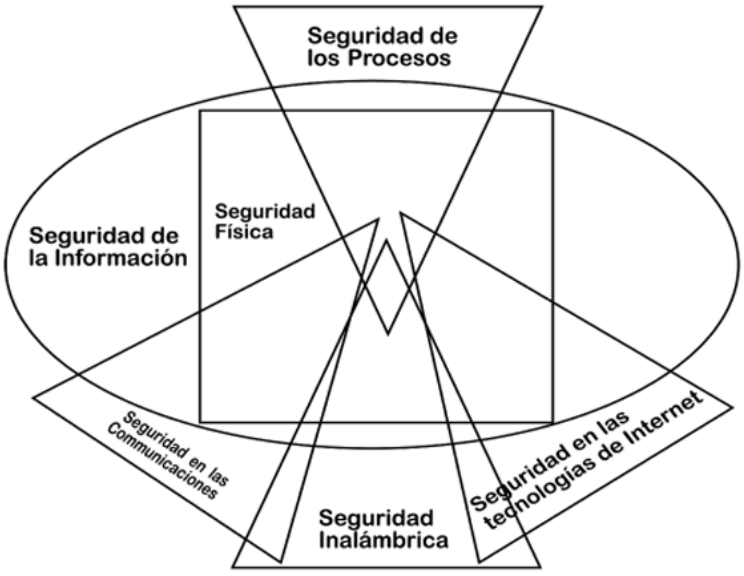
Reversal o reversible: En este test, el proceso de hackeo depende del nivel de creatividad y conocimientos del hacker. Además, el hacker tiene un conocimiento completo de todas las operaciones de la empresa. Es importante destacar que el cliente no tiene conocimiento del momento, la forma y la metodología específica de las auditorías. (ISECOM, 2010)

Alcance (scope):

Según Parandini et al. (2010) el alcance se compone de tres vías de acceso o canales: seguridades de comunicaciones (COMSEC), seguridades físicas (PHYSSEC) y seguridades espectro (SPECSEC). Para llevar a cabo una auditoría meticulosa, es esencial profundizar en estos tres canales, lo cual dependerá de la experiencia del auditor, así como de su equipamiento y recursos disponibles. La metodología aborda estos tres canales en cinco secciones lógicas como se muestra en la Figura 1 y la Tabla 2.

Figura 1

Esquema del Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM)



Nota. Adaptado de *Towards a practical and effective security testing methodology* (p.323), por Prandini, M., & Ramilli, M. (2010).. The IEEE symposium on Computers and Communications

A continuación, se detalla a mayor nivel los canales y las secciones referidas:

Tabla 2

Canales y secciones de OSSTMM

CANAL	SECCIÓN	DESCRIPCIÓN
Seguridad física	Humano	Comprende el elemento humano de la comunicación donde la interacción es física o psicológica.
	Físico	Pruebas de seguridad física donde el canal es de naturaleza tanto física como no electrónica. Comprende el elemento tangible de seguridad donde la interacción requiere

		esfuerzo físico o un transmisor de energía para manipular.
Seguridad del espectro	Comunicaciones inalámbricas	Comprende todas las comunicaciones, señales y emanaciones electrónicas que tienen lugar en el espectro EM conocido. Esto incluye ELSEC como comunicaciones electrónicas, SIGSEC como señales y EMSEC que son emanaciones no unidas por cables.
Comunicaciones Seguridad (COMSEC)	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción se realiza a través de líneas de redes cableadas y cableadas establecidas.
	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, digitales o analógicas, donde la interacción se realiza a través de líneas telefónicas establecidas o de redes similares.

Nota. Fuente: ISECOM (2010)

Contratos o reglas de acuerdos:

En esta sección, la metodología es meticulosa y ética en cada detalle. Según la ISECOM (2010) los requerimientos en el contrato se limitan únicamente a lo necesario tanto para el cliente como para el auditor. Es crucial definir con precisión el alcance del trabajo antes de llevar a cabo la auditoría. Además, se debe realizar una planificación detallada para cada prueba, tanto para los miembros del equipo de trabajo como para el auditor responsable.

Resultados de los test:

Para ISECOM (2010) Para elegir el test más adecuado para cada empresa, es fundamental comprender la estructura y diseño de los módulos con los que se trabaja. La planificación y

distribución de los detalles de la auditoría en diversas etapas estarán condicionadas por la naturaleza del negocio de la organización, el tiempo disponible y los requisitos particulares de la auditoría. Una vez que se hayan tenido en cuenta estos factores, el auditor estará en posición de estructurar y organizar el proceso de auditoría de manera adecuada.

La metodología tiene 4 fases de ejecución:

Fase regulatoria

Según ISECOM (2010) esta consiste en la toma de decisiones sobre qué tipo de pruebas se llevarán a cabo en la auditoría. Estas decisiones se basan en diversos factores, como los límites establecidos por la normativa, los requerimientos específicos del cliente, las restricciones existentes y los objetivos que se desean alcanzar. Durante esta fase, se evalúa cuidadosamente cada uno de estos aspectos para garantizar que las pruebas seleccionadas sean adecuadas y proporcionen la información necesaria para cumplir con los objetivos de la auditoría.

Fase de definición

En esta fase se busca establecer de manera precisa y clara el alcance que tendrá dicha auditoría. Cruz et al. (2017) mencionan que se debe determinar qué aspectos específicos serán evaluados y qué objetivos se pretenden alcanzar con la realización de la auditoría. Esta etapa es fundamental, ya que garantiza que el proceso de auditoría se enfoque en los aspectos relevantes y esenciales para la organización o entidad que está siendo evaluada.

Fase de información

Cruz et al. (2017) plantea que, durante la fase de información de una auditoría, se examina detalladamente la información existente para determinar si hay activos que no han sido correctamente ubicados, desatendidos o gestionados de manera inadecuada. Esta fase es

fundamental para identificar posibles áreas de mejora y corregir cualquier deficiencia en el manejo de la información.

Fase interactiva de prueba de controles

En esta fase, según ISECOM (2010) se verifica el efecto de las perturbaciones o ataques, así como el impacto de la información extraída. Es importante destacar que esta información no puede ser revelada hasta que se haya completado la ejecución de todas las fases previas. Asimismo, se realiza la verificación de la veracidad de las conclusiones obtenidas.

ISSAF

OISSG (2005) Afirma que el Marco de Evaluación de la Seguridad del Sistema de Información (ISSAF) es un marco estructurado revisado por pares que clasifica y evalúa la seguridad de los sistemas de información en diferentes dominios. Su objetivo principal es brindar una visión realista de la evaluación de la seguridad, reflejando escenarios prácticos. ISSAF se utiliza principalmente para cumplir con los requisitos de evaluación de seguridad de las organizaciones, pero también puede ser utilizado como referencia para satisfacer otras necesidades en términos de seguridad de la información. Además, ISSAF incluye la evaluación y el fortalecimiento de los procesos de seguridad, para obtener una visión completa de las vulnerabilidades que puedan existir.

De acuerdo con PYMESEC (2015), esta metodología es ampliamente adoptada por empresas debido a que cumple con los requisitos de evaluación y sirve como una referencia para implementaciones relacionadas con la seguridad de la información. Sus criterios de evaluación han sido revisados por expertos globales en la materia. La metodología se basa en un enfoque estructurado que consta de tres fases y nueve pasos de análisis. Estas etapas son:

1. Planificación y preparación.

2. Evaluación.

3. Informe.

Planificación y preparación

De acuerdo con PYMESEC (2015), este proceso permite la preparación del entorno de trabajo y es fundamental antes de iniciar la planificación. Antes de comenzar, se debe formalizar un contrato profesional con el cliente en el que se establezcan claramente las responsabilidades y funciones de ambas partes. Este contrato también sirve como un acuerdo legal de protección mutua, en el que ambas partes se comprometen entre sí. Además, se llevan a cabo reuniones de trabajo para definir el alcance del test, su enfoque y las metodologías a utilizar. También se establecen las pruebas a realizar y se definen rutas de escalado para resolver posibles problemas que puedan surgir durante el proceso.

Evaluación

En esta fase se lleva a cabo el test de pentesting o intrusión previamente definida. Este test se concentra en diferentes etapas, cada una de las cuales profundiza en los activos con un nivel de detalle mayor. Dichas capas pueden ser definidas como:

Information Gathering (Obtención de información)

Según PYMESEC (2015), en esta capa de análisis se exploran las posibilidades de ataques tanto internos como externos a la red. Se considera cualquier tipo de documento o información que pueda comprometer los sistemas, como correos electrónicos, números de teléfono, datos personales, información de empleados y socios comerciales, así como la implementación de tecnologías. También se contempla el bloqueo de propiedad intelectual, de manera que los datos precisos sobre los propietarios de dominios sean desconocidos.

En esta capa, ISSAF se asemeja a PTES, ya que detalla las diferentes capas y sugiere ejemplos de herramientas que podrían ser utilizadas en los ataques. Estas herramientas son recomendadas por expertos en la materia y pueden incluir (dig, nslookup, Nmap, entre otras.)

Network Mapping (Análisis de la red de datos)

Castro (2019) señala que el mapeo de red constituye una capa altamente técnica dentro de las mencionadas. Implica el análisis de diversas variables, como la topología de la red, la configuración de los routers y dispositivos de red, los firewalls, los nombres de los hosts, los servidores y los puertos activos en los ordenadores. También se consideran aspectos como el uso de NetBIOS, los sistemas operativos utilizados, las cuentas y privilegios asociados a ellos, entre otros factores.

Vulnerability Identification (Identificación de vulnerabilidades)

Según PYMESEC (2015) en primer lugar, hay que seleccionar los puntos a probar. Se desarrollarán actividades como:

- Se identifica servicios vulnerables que muestran banners.
- Se lleva a cabo un análisis de vulnerabilidades con el objetivo de identificar aquellas que son conocidas. Para obtener información sobre vulnerabilidades conocidas, se puede recurrir a los anuncios de seguridad de los proveedores o consultar bases de datos públicas como SecurityFocus, CVE o CERT.
- Para verificar falsos positivos y falsos negativos, se puede emplear un método como la correlación de las vulnerabilidades entre sí y con la información obtenida previamente.
- Las vulnerabilidades descubiertas deben ser enumeradas.

- Para estimar el impacto probable, es necesario clasificar las vulnerabilidades encontradas.
- Se busca identificar las rutas de ataque y los escenarios en los que se pueden aprovechar.

Penetration (Pentesting o entrada)

Según PYMESEC (2015), en esta fase los auditores buscan lograr acceso no autorizado, evadiendo las medidas de seguridad establecidas. Esta fase se puede dividir en varios pasos:

- Encontrar herramientas o código para probar el concepto.
- Desarrollar herramientas o scripts necesarios.
- Utilizar herramientas de prueba o código para prueba de concepto.
- Emplear el código de prueba de concepto en el objetivo.
- Verificar o descartar la existencia de una vulnerabilidad.
- Documentar los hallazgos obtenidos.

Gaining Access and privilege escalation (Obtener acceso y escalado de privilegios)

Según Castro (2019) Los privilegios de usuario se escalan desde el más básico hasta el usuario administrador, de esta manera pueden controlar y manipular los archivos y el sistema. Por lo tanto, se examina a todos los usuarios potenciales.

Enumerating further (Lista de objetivos)

Para PYMESEC (2015) en esta fase, los atacantes buscan acceder a las contraseñas mediante la captura de paquetes de tráfico en red. También analizan este tráfico utilizando cookies o historial de navegación, y pueden apuntar a direcciones de correo electrónico, enrutadores y

redes. Básicamente, esta fase implica varias tácticas para obtener acceso no autorizado y recopilar información confidencial.

Compromise remote users/sites (Sitios y usuarios remotos comprometidos)

Castro (2019) plantea que en este proceso, el auditor intentará manipular todos los sistemas adquiriendo tantas contraseñas como sea posible, ya sea dentro o fuera de la red objetivo. Durante esta fase, se utilizarán firewalls de escritorio remoto para evitar el acceso sin restricciones a cualquier parte de la red. El propósito de este enfoque es mejorar las medidas de seguridad y limitar las posibles vulnerabilidades que podrían ser explotadas por partes no autorizadas. Al tomar tales precauciones, el auditor puede garantizar que la red esté protegida contra posibles amenazas y que la información confidencial permanezca segura.

Maintaining Access (Mantenimiento de los privilegios y accesos obtenidos)

Según PYMESEC (2015), en esta etapa el objetivo es lograr un control efectivo de los sistemas comprometidos, manteniendo un perfil discreto frente a otros usuarios y administradores. Para lograrlo, se utilizan canales de comunicación disimulados o secretos, como túneles SSL, proxies o SSH, entre otros. La forma más común de ejercer un control oculto en múltiples máquinas es mediante el uso de troyanos, backdoors y rootkits.

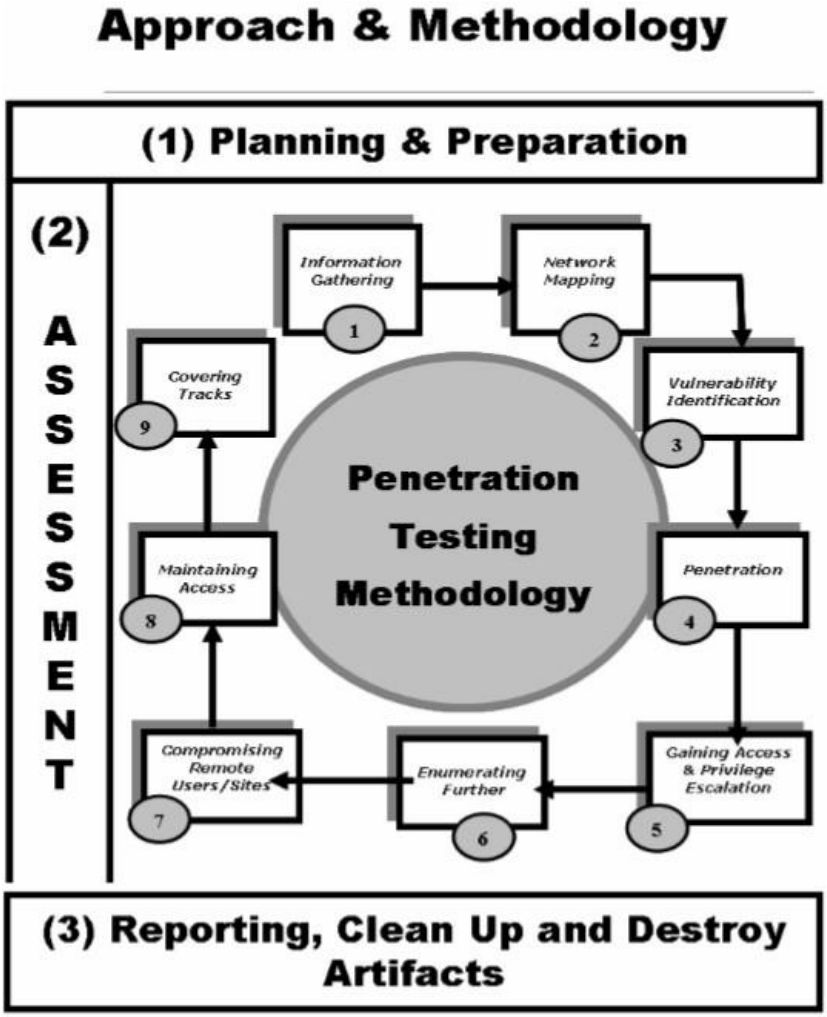
Covering Tracks (Borrado de huellas)

Según PYMESEC (2015), en esta etapa se busca eliminar todas las pistas utilizando herramientas de ocultación de pruebas, keyloggers, exploits, archivos, etc. Se ocultan carpetas en los sistemas operativos Windows y GNU/Linux, se limpian los registros de actividad si no están replicados, o se manipulan de alguna manera. Es importante recordar que, a pesar de estos

esfuerzos, un crimen nunca está exento de dejar rastros. La Figura 2, muestra las diferentes fases a tomar en cuenta en el proceso de evaluación. estas son cíclicas e iterativas.

Figura 2

Fases de evaluación ISSAF



Nota. Adaptada de *Fases de evaluación* ISSAF OISSG, 2005 (www.pymesec.org). CC BY 2.0

Informe

La fase final de la metodología consiste en la elaboración de dos informes, verbal y escrito.

Verbal

Castro (2019) menciona que este informe se utiliza únicamente para comunicar la existencia de vulnerabilidades graves que afecten significativamente la línea de negocio de la organización.

Informe final

PYMESEC (2015) El informe final es un documento detallado que incluye los siguientes apartados:

Resumen del trabajo llevado a cabo: Se presenta una breve descripción de las actividades realizadas durante el proyecto.

Alcance global del proyecto: Se explica en qué consistió el proyecto y qué objetivos se lograron alcanzar.

Herramientas utilizadas: Se mencionan las herramientas y tecnologías empleadas para llevar a cabo el proyecto.

Fechas de los tests a los sistemas incluyendo las horas: Se proporciona un registro de las fechas y horas en las que se realizaron las pruebas de los sistemas.

Conclusiones respecto a los tests diseñados: Se presentan las conclusiones obtenidas a partir de los tests realizados, incluyendo tanto los resultados positivos como los aspectos que requieren mejoras.

Informe específico de las vulnerabilidades encontradas: Se detallan las vulnerabilidades identificadas durante el análisis de seguridad del sistema.

Medidas preventivas relacionadas con las vulnerabilidades mencionadas: Se sugieren soluciones y medidas de seguridad para prevenir y mitigar las vulnerabilidades identificadas.

Listado de los puntos de intervención: Se enumeran los aspectos que requieren intervención, tanto para realizar mejoras inmediatas como para proponer soluciones futuras.

Este informe final brinda una visión completa de los trabajos realizados, las vulnerabilidades encontradas y las medidas sugeridas para garantizar la seguridad y estabilidad del sistema.

PTES TECHNICAL GUIDELINES

El Estándar de Ejecución de Pruebas de Pentesting (PTES) es un estándar que fue creado en 2009 por un grupo de profesionales de seguridad de la información. El propósito de este estándar era abordar la falta de calidad y orientación en la industria de las pruebas de seguridad cibernética. Su objetivo principal era proporcionar a las empresas y proveedores de seguridad un framework y un alcance común para llevar a cabo pruebas de pentesting, estableciendo así una línea de base para definir los límites de dichas pruebas. En otras palabras, Hout (2019) menciona que PTES busca especificar el conjunto mínimo de pruebas, procesos y resultados que deben llevarse a cabo antes de que una prueba de pentesting pueda ser considerada profesional y completa.

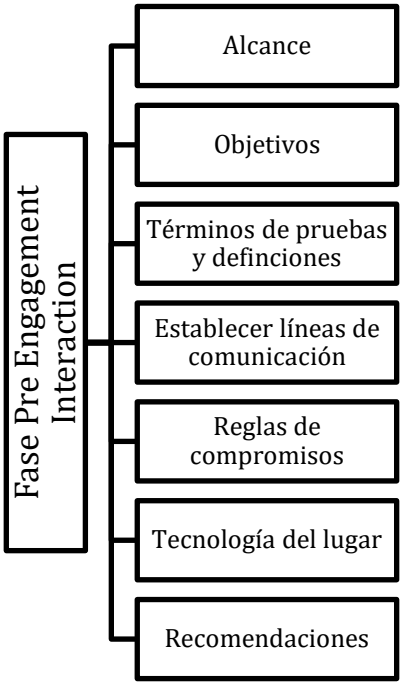
Nickerson et al. (2012) señala que el estándar abarca diversas etapas, que incluyen interacciones previas al compromiso, recopilación de inteligencia, modelado de amenazas, análisis de vulnerabilidad, explotación, post-explotación e informes. Además, PTES proporciona una lista exhaustiva de herramientas y técnicas utilizadas en cada una de las siete secciones, acompañadas de una descripción detallada de cada fase. El test de intrusión se realiza en 7 fases que se detallan a continuación.

Pre-engagement Interactions (Interacciones previas al compromiso)

Nickerson et al. (2012) establece el alcance del pentesting, incluyendo un acuerdo con el cliente sobre la profundidad y el impacto de las pruebas, así como: un test de caja negra, gris o blanca, entre otros aspectos relevantes a destacar. Como se lo muestra en la Figura 3.

Figura 3

Interacciones pre-compromiso



Intelligence Gathering (Recolección de información)

Nickerson et al. (2012) menciona que se recopilará información de inteligencia competitiva publicada en motores de búsqueda para obtener conocimiento sobre los temas de estudio y los recursos de la empresa. Además, se incluirá información sobre el sistema y la planificación de la organización. Se analizará e identificará interna y externamente los servicios, el mapeo, la VoIP y los protocolos disponibles. También se investigarán los perfiles de usuario, la ubicación física de

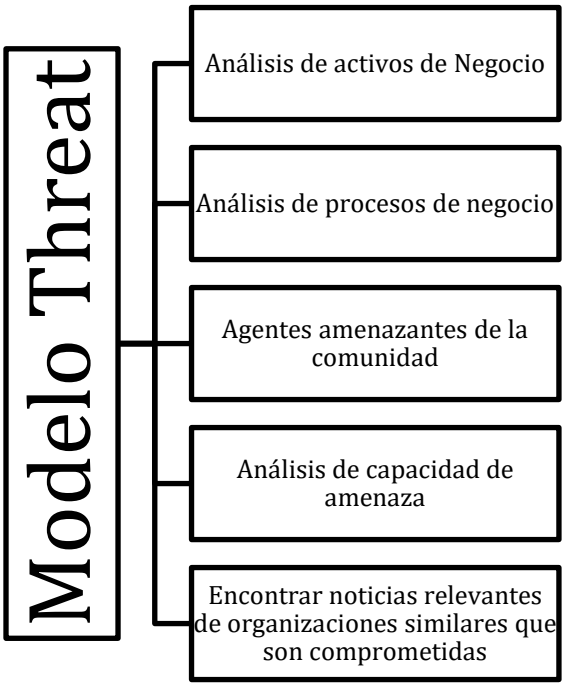
los empleados y el uso de redes sociales. Se considerarán aspectos competitivos como los planes de marketing o la visión de productos.

Threat Modeling (Modelado de amenazas)

Nickerson et al. (2012) indica que después de recopilar la información relevante en las fases anteriores, se procede a identificar las áreas de negocio existentes y evaluar la importancia de los activos de tecnología de la información que se han identificado en el estudio. Esto es necesario para determinar los posibles vectores de ataque en etapas posteriores, como se muestra en la Figura 4.

Figura 4

Threat modelling



Vulnerability analysis (Análisis de vulnerabilidad)

Esta fase se denomina "Análisis de vulnerabilidades". Según Nickerson et al. (2012), consiste en examinar activamente el objetivo, manipulándolo para identificar los puertos o

servicios presentes en la organización y buscar las vulnerabilidades existentes. Esta fase se divide en pruebas activas y pasivas, validación e investigación. Se recopila información sobre servicios, redes, escáneres web y VoIP, entre otros. Una vez identificados los puertos, se analizan posibles ataques y se validan las opciones reales de ataque, teniendo en cuenta los riesgos asociados. También se lleva a cabo una sub-fase de investigación en la que se revisa toda la información disponible en internet sobre brechas de seguridad y vulnerabilidades. Un consejo profesional importante es replicar el entorno de pruebas o simular pruebas en un ambiente real antes de realizar cualquier acción en la infraestructura, para garantizar la viabilidad y el alcance real de la auditoría y asegurarse de que se han tomado todas las medidas preventivas necesarias.

Exploitation (Explotación)

Según Nickerson et al. (2012) En esta etapa se incluye eludir los sistemas de detección de intrusos en el host (HIDS) y en la red (NIDS), que son programas diseñados para detectar accesos no autorizados al equipo y a la red, respectivamente, así como también los antivirus y otras contramedidas de seguridad existentes a nivel de red o en el dispositivo final. Se realizarán revisiones exhaustivas, que abarcarán desde el acceso físico mediante el uso de dispositivos USB, hasta las redes inalámbricas. Se asegurarán contramedidas para evadir la detección, teniendo en cuenta los servicios activos que la empresa utiliza.

Post exploitation (Después de la explotación)

Según Nickerson et al. (2012), el objetivo de esta fase es recopilar y almacenar pruebas, así como evaluar la intrusión y el alcance de la manipulación en el sistema comprometido. Se examina la eliminación de rastros y se lleva a cabo un ataque persistente, como la instalación de puertas traseras, rootkits o conexión inversa. Los riesgos de tener una red vulnerable son numerosos, por lo que es importante preguntarse qué información pueden llevarse de nuestra

organización. Tanto el departamento de auditoría de sistemas como la gerencia deben trabajar juntos para fortalecer la infraestructura de red, asegurando elementos para restringir la salida de datos (voz, video, cintas, discos, USB, entre otros), realizando copias de seguridad periódicas de la documentación, entre otras medidas. Es necesario prestar mayor atención a los ataques dirigidos directamente al negocio, como la lista de clientes, copias de seguridad eliminadas o discos dañados. Es fundamental ser conscientes y no escatimar recursos en la protección de elementos críticos mencionados anteriormente. Además, la auditoría realizada con esta metodología debe ser limpia, es decir, sin dejar rastro y garantizar la recuperabilidad de todos los sistemas.

Reporting (Informes)

En esta etapa, según Nickerson et al. (2012), se generan informes ejecutivos y técnicos que se entregan al finalizar el estudio de la organización. El informe debe resaltar las razones por las cuales la organización solicitó la prueba, así como los riesgos clasificados por orden de prioridad. Además, se incluyen métricas utilizadas y contramedidas propuestas para las inseguridades evaluadas. A continuación, se detalla la información obtenida o comprometida durante el estudio, se evalúan las vulnerabilidades encontradas y se confirma la explotación de dichas fallas, junto con las contramedidas propuestas y probadas, incluyendo otras contramedidas derivadas. También se analiza el grado de exposición de los activos de la empresa, es decir, si están accesibles para terceros y se calcula en función de su magnitud, frecuencia y riesgos asociados. Por último, se incluye un informe técnico que aborda los puntos mencionados anteriormente, así como un informe ejecutivo dirigido al gerente o CEO de la organización o empresa.

MARCO LEGAL

ISO/IEC 27001 (2022) provee los requisitos necesarios para implementar la gestión de la seguridad de la información en una organización ya sea con o sin fines de lucro, privada o pública, pequeña o grande.

ISO/IEC 27002 (2022) Es una guía que ofrece recomendaciones para mejorar la seguridad de la información en diversos contextos. Su enfoque abarca aspectos como la protección de datos personales y la responsabilidad social.

La norma ISO 31000 (2018) para la gestión de riesgos se estructura en tres elementos claves:

- Principios de la gestión de riesgos
- Marco de trabajo para la gestión de riesgos
- Proceso de gestión de riesgos

Según la normativa SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI (2022) emitida por la Superintendencia de Economía Popular y Solidaria (SEPS) menciona en las disposiciones generales, segunda cápsula; las entidades, empresas y CONAFIPS deberán solicitar al menos una vez al año a los prestadores de servicio sean estos personas naturales o jurídicas la documentación que demuestre que el servicio hoy prestado cuente con las revisiones(auditorías, exámenes especiales, certificaciones, entre otras) y controles necesarios para la adecuada administración de la seguridad de la información.

CAPITULO III

MARCO METODOLÓGICO

Descripción del área de estudio / descripción del grupo de estudio

El área de estudio se centraliza en la infraestructura informática de una cooperativa de ahorro y crédito segmento tres, en la cual se realizaron pruebas de pentesting para detectar las vulnerabilidades mediante diferentes tipos de ataques.

ENFOQUE Y TIPO DE INVESTIGACIÓN

Tipo de investigación

La evaluación propuesta se clasificó como una evaluación aplicada, ya que se utilizaron metodologías de pentesting, junto con herramientas y técnicas, para detectar vulnerabilidades y ataques en una cooperativa de ahorro y crédito segmento tres.

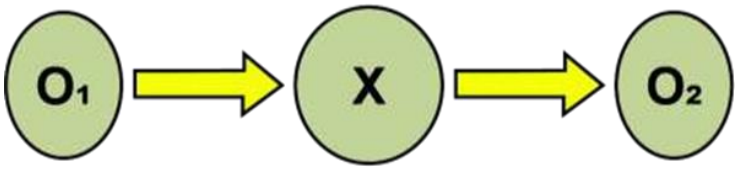
Diseño de la investigación

Esta investigación es de tipo cuasiexperimental, según (Rojas, 2015) este tipo de experimento se utiliza cuando la persona dedicada a realizar la indagación no es capaz de mostrar el nivel de la variable independiente a voluntad, y tampoco puede crear un grupo experimental de forma aleatoria.

En este estudio cuasiexperimental, solo hay un grupo, por lo que no se pueden hacer comparaciones entre varios conjuntos. El diseño se estructura como se muestra en la Figura 5:

Figura 5

Esquema de la investigación realizada.



Nota. Adaptada de Metodología de la investigación sexta edición (p. 85) por Fernández. (2016)

Donde:

O_1 = Nivel de seguridad informática de la cooperativa de ahorro y crédito segmento tres, antes de evaluar metodologías.

X = Implementación de una metodología de pentesting.

O_2 = Nivel de seguridad informática de la cooperativa de ahorro y crédito segmento tres, después de evaluar metodologías.

Población

Según, Hérnandez et al. (2014) señalan que la población se refiere a la totalidad de elementos que se investigarán, incluyendo sus características y componentes, así como cualquier otro elemento relevante para la presente investigación.

La población seleccionada para este estudio de investigación consiste en tres metodologías identificadas en la revisión sistemática, las cuales se centran en las técnicas más comúnmente utilizadas en la actualidad para la detección de vulnerabilidades. Estas metodologías se detallan a continuación:

OSSTMM (Open-Source Security Testing Methodology Manual): El objetivo principal es proporcionar un enfoque científico que contribuya a evaluar la seguridad de la empresa mediante pruebas exhaustivas desde el exterior hacia el interior. Además, busca brindar orientación a los profesionales de sistemas, para asegurar que la empresa cumpla con las normas establecidas por el ISECOM. Este documento describe detalladamente las diferentes fases involucradas en el proceso de pruebas de seguridad operativa, abarcando diversos aspectos como: el factor humano, las redes

inalámbricas, las instalaciones físicas, las telecomunicaciones y las redes de datos, entre otros. Todo esto se basa en una métrica efectiva. (ISECOM, 2010)

ISSAF (Information Systems Security Assessment Framework): El texto propuesto se refiere a la metodología de OISSG, que organiza la verificación de seguridad en distintos aspectos utilizando diferentes tipos de pruebas. ISSAF es una herramienta importante que ayuda a evaluar la seguridad informática para identificar vulnerabilidades. También se menciona que se utilizará una matriz de riesgos para analizar la eficacia de los controles implementados. (PYMESEC, 2015)

PTES (Penetration testing execution standard): Esta metodología se basa en el enfoque de OSSTMM, que combina los esfuerzos de analistas y expertos en seguridad para establecer un estándar que abarque todos los procesos comunes de una auditoría. (Nickerson et al. 2012)

Técnicas e instrumentos de recolección de datos, validez y seguridad

Análisis: Se examinan de forma minuciosa la información relacionada con la investigación. (Pedraza Melo et al. 2015)

Inductivo – deductivo: Según (Hérnandez et al. 2014) es el estudio de los conceptos y herramientas para la detección y explotación de vulnerabilidades que permitieron analizar el entorno de seguridad en la infraestructura de una cooperativa de ahorro y crédito segmento tres para identificar vulnerabilidades que se conviertan en posibles ataques informáticos.

Técnicas: Se utilizaron las etapas del pentesting para identificar y localizar vulnerabilidades en la seguridad informática. Estas etapas incluyen:

Figura 6

Fases del Pentesting para la detección de vulnerabilidades.

Nota. Adoptada de Método de inclusión de Pentesting en el proceso de Testing de software (p. 67) por Ariel & Rodríguez (2018)

TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

En este estudio, se emplean técnicas de observación directa, participativa y sistemática en la realidad actual de la cooperativa de ahorro y crédito segmento tres debido a la naturaleza de la investigación y los datos que se van a recopilar. Según Hernández et al. (2014), la observación implica un registro sistemático, efectivo y confiable del comportamiento. Por lo tanto, en esta investigación se observaron las principales vulnerabilidades de una institución financiera y se determinó una escala valorativa para la observación estructurada. Según Rojas (2015), se utiliza una guía diseñada previamente en la que se especifican los elementos que serán observados.

Procedimiento de análisis de datos.

Después de utilizar el instrumento y obtener los resultados correspondientes, es posible analizarlos mediante métodos estadísticos descriptivos con el propósito de presentar de manera objetiva la realidad. Los datos recolectados serán organizados, tabulados y representados gráficamente para una mejor comprensión de los resultados. Posteriormente, los resultados serán analizados e interpretados. Para facilitar el estudio y la utilidad de los resultados obtenidos, se emplearán histogramas cuando sea necesario, ya que esta es la forma más conveniente de representar los datos.

CAPITULO IV

ANÁLISIS DE VULNERABILIDADES

Durante el estudio de las principales metodologías de pentesting, se llevó a cabo un análisis cualitativo sobre las debilidades informáticas de una cooperativa de ahorro y crédito segmento tres. Para aplicar este análisis, se diseñó una escala valorativa planteada en la Tabla 3 que tiene como puntuación del 0 al 3, para determinar cuan eficiente son las metodologías de pentesting en comparativa con las principales vulnerabilidades de las instituciones financieras de acuerdo con el estudio del estado de la ciberseguridad en el sector bancario en América Latina y el Caribe realizado por Organización de los Estados Americanos (2018) cómo se detallan en la Tabla 4.

Resultados en tablas y figuras.

Tabla 3

Escala de valoración para evaluación de las metodologías ISSAF, PTES Y OSSTMM

Valor	Descripción
0	La descripción no hace referencia a la vulnerabilidad ni a pruebas de seguridad o comprobaciones relacionadas con ella.
1	se menciona la vulnerabilidad, pero no se proporciona información sobre cómo realizar pruebas de seguridad para detectarla.
2	Se proporciona una descripción sobre cómo llevar a cabo la prueba de seguridad, sin embargo, el contenido presentado no es lo bastante detallado o completo como para ejecutar una prueba de seguridad real.
3	Se proporciona una descripción detallada sobre cómo realizar la prueba de seguridad, la cual contiene suficientes detalles para ser aplicada directamente en una prueba de seguridad real.

Tabla 4

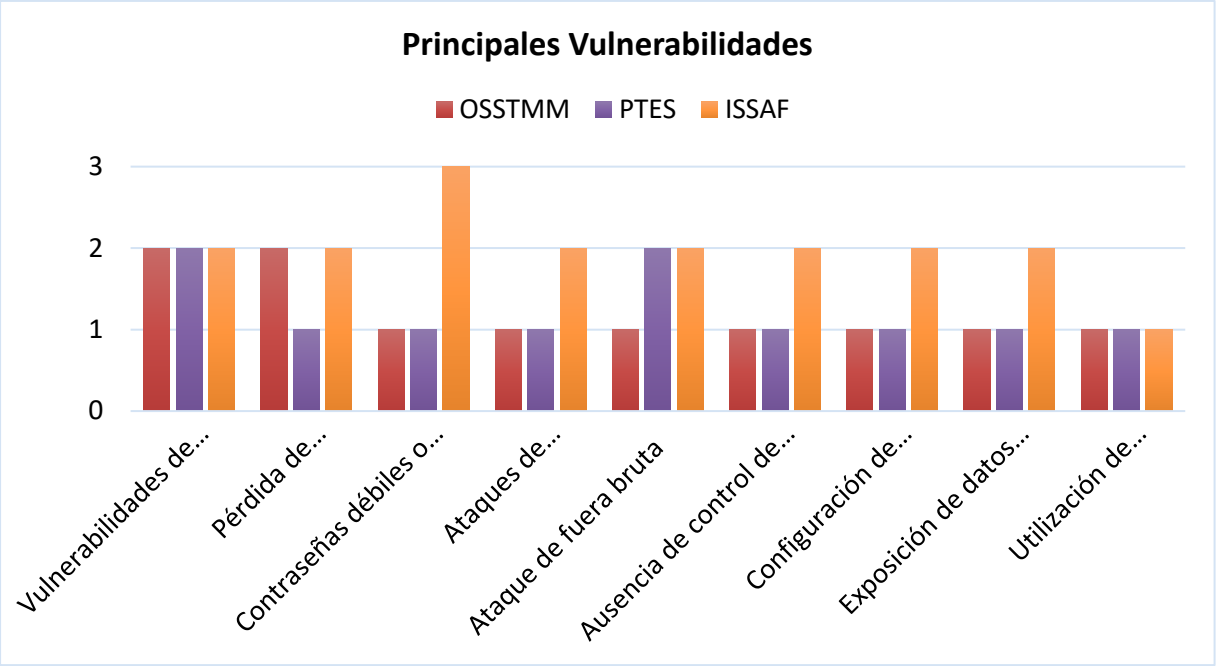
Lista de cotejo con las principales vulnerabilidades de instituciones financieras

Principales Vulnerabilidades	**OSSTMM**	**PTES**	**ISSAF**
Vulnerabilidades de software y sistemas operativos	2	2	2
Pérdida de autenticación y gestión de sesiones.	2	1	2
Contraseñas débiles o predeterminadas	1	1	3
Ataques de denegación de servicio	1	1	2
Ataque de fuera bruta	1	2	2
Ausencia de control de acceso a funciones	1	1	2
Configuración de seguridad incorrecta.	1	1	2
Exposición de datos sensibles.	1	1	2
Utilización de componentes con vulnerabilidades conocidas.	1	1	1
Totales	**11**	**11**	**18**

Los resultados de forma gráfica de las principales vulnerabilidades para cada metodología se lo muestran en la Figura 7.

Figura 7

Resultados de evaluación a la lista de cotejo con la escala de evaluación de las principales vulnerabilidades de las instituciones financieras



Las metodologías analizadas proporcionan una guía para detectar y abordar diversas vulnerabilidades y riesgos de seguridad en sistemas informáticos. Sin embargo, es importante analizar críticamente su eficacia y aplicabilidad en entornos específicos, como en el caso de una cooperativa de ahorro y crédito segmento tres. A continuación, se presenta la revisión del análisis de las metodologías PTES, OSSTMM e ISSAF, con sustento bibliográfico

Discusión y resultados

1. Vulnerabilidades de software y sistemas operativos:

Las tres metodologías proporcionan una guía para identificar vulnerabilidades en software y sistemas operativos. Sin embargo, se recomienda que las descripciones de las pruebas en PTES e ISSAF sean más detalladas para alinearlas con las pruebas de seguridad en un entorno real. Según

Lampson (2004), un análisis exhaustivo de las vulnerabilidades requiere también comprender cómo explotarlas y mitigarlas efectivamente.

2. Pérdida de autenticación y gestión de sesiones:

OSSTMM e ISSAF ofrecen información adecuada para realizar pruebas de seguridad en este aspecto, mientras que PTES podría mejorar. En concordancia, Howard et al. (2005) destacan la importancia de abordar las debilidades en la gestión de sesiones para prevenir ataques de suplantación de identidad.

3. Contraseñas débiles o predeterminadas:

ISSAF proporciona detalles específicos para aplicar en pruebas de seguridad real, por lo cual se destaca en este aspecto. Esta afirmación encuentra apoyo en la literatura de Wang et al. (2012), quienes enfatizan la necesidad de políticas de contraseñas sólidas para mitigar riesgos de seguridad.

4. Ataques de denegación de servicio:

Las tres metodologías ofrecen orientación suficiente para realizar pruebas de seguridad en este aspecto. Este hallazgo está en línea con la investigación de Zargar et al. (2013), que destaca la importancia de abordar las vulnerabilidades que podrían ser explotadas en ataques de denegación de servicio.

5. Ataque de fuerza bruta:

PTES e ISSAF ofrecen detalles suficientes para llevar a cabo pruebas de seguridad, mientras que OSSTMM podría mejorar. Investigaciones como las de Narasimhaiah & Manvi (2011) subrayan la necesidad de proteger contra ataques de fuerza bruta mediante medidas adecuadas de autenticación y control de acceso.

6. Ausencia de control de acceso a funciones:

Todas las metodologías ofrecen suficiente orientación para abordar este aspecto, lo que concuerda con los principios de seguridad de acceso descritos por Barkley & Kebert (2009)

7. Configuración de seguridad incorrecta:

La guía proporcionada por las tres metodologías es adecuada para abordar este aspecto, lo que está respaldado por investigaciones como las de Scarfone & Mell (2009) sobre mejores prácticas en la configuración de seguridad.

8. Exposición de datos sensibles:

Las metodologías ofrecen suficiente orientación para manejar este riesgo, lo que coincide con la importancia de la protección de datos sensibles enfatizada por la Ley Orgánica de Protección de Datos Personales (LOPD) (Asamblea Nacional del Ecuador, 2021).

9. Utilización de componentes con vulnerabilidades conocidas:

ISSAF destaca al ofrecer detalles específicos para pruebas de seguridad reales en este aspecto, lo que refleja la importancia de abordar vulnerabilidades conocidas en sistemas, según lo señalado por (Olson et al. 2012)

Para las principales vulnerabilidades de instituciones financieras detalladas en la Tabla 5 se sugieren las siguientes herramientas de pentesting.

Tabla 5

Herramientas de pentesting sugeridas por las metodologías ISSAF, PTES Y OSSTMM

Vulnerabilidad	**Herramienta 1**	**Herramienta 2**	**Herramienta 3**
Vulnerabilidades de software y sistemas operativos	Nessus	OpenVAS	Nexposed
Pérdida de autenticación y gestión de sesiones	Burp Suite	OWASP ZAP	Fiddler
Contraseñas débiles o predeterminadas	Hydra	John the Ripper	Cain & Abel
Ataques de denegación de servicio	LOIC	HOIC	Slowloris
Ataque de fuerza bruta	Aircrack-ng	RainbowCrack	Medusa
Ausencia de control de acceso a funciones	Metasploit	BeEF	SQLmap
Configuración de seguridad incorrecta	Nmap	Wireshark	Nikto
Exposición de datos sensibles	Acunetix	SQLmap	OWASP ZAP
Utilización de componentes con vulnerabilidades conocidas	Retire.js	Dependency-Check	FindSecBugs
Registro y monitoreo insuficiente	Splunk	ELK Stack	Nagios

En conclusión, aunque todas las metodologías son útiles para realizar pruebas de seguridad en una cooperativa de ahorro y crédito del segmento tres, ISSAF destaca por proporcionar detalles específicos para aplicar directamente en pruebas de seguridad reales, en comparación con OSSTMM y PTES en varios aspectos. Por lo tanto, considerar una combinación de estas metodologías para obtener una cobertura completa de las pruebas de seguridad podría ser beneficioso, esta información está respaldada por investigaciones como las de Vieira et al. (2017) sobre la efectividad de enfoques combinados en seguridad de la información.

Estudio teórico de las metodologías de pentesting para su implementación

Análisis comparativo de las metodologías analizadas

Una vez que se ha realizado un análisis exhaustivo de las diversas metodologías disponibles, se vuelve crucial realizar una comparación entre ellas, para tener una comprensión más clara de lo que cada una ofrece, incluyendo sus ventajas, desventajas, enfoque en determinadas organizaciones, facilidad de uso y otros puntos relevantes que se detallarán a continuación en la Tabla 6 y 7.

Tabla 6

Análisis de indicadores de metodologías de pentesting ISSAF, PTES Y OSSTMM

CARACTERISTICAS	OSSTMM	ISSAF	PTES
Define los requisitos previos necesarios para la evaluación.	X	✓	X
Permite realizar prácticas y evaluaciones de seguridad en cualquier tipo de base de datos.	✓	✓	✓
Incluye plantillas para la realización de las pruebas.	✓	✓	✓
Delimita las áreas de alcance.	X	✓	X
Incluye ejemplos de pruebas y sus resultados.	X	✓	X
Describe en detalle las técnicas para cada prueba.	X	✓	X
Define los procedimientos para la evaluación de peligros.	✓	✓	✓
Recomienda herramientas para cada prueba.	X	✓	X
Enumera y clasifica las vulnerabilidades identificadas.	X	✓	X
Establece las dimensiones de seguridad a evaluar.	✓	X	✓
Define las dimensiones de seguridad como un estándar.	✓	X	X

Genera informes.	✓	✓	✓
Presenta medidas beneficiosas que pueden ser útiles.	**X**	✓	✓
Incluye referencias a documentos y enlaces relevantes.	**X**	✓	**X**
Proporciona un acuerdo de confidencialidad.	✓	✓	**X**
Mantiene las actualizaciones al día.	✓	**X**	**X**

Tabla 7

Comparación de metodologías de pentesting ISSAF, PTES Y OSSTMM

Patrones (Ítems)	ISSAF	PTES	OSSTMM
Niveles de detalle	Carece de información de cloud. Computing y protección de datos. Aunque es detallado, también es bastante simple.	La documentación de sus procesos está completa y precisa, pero no se han registrado cambios desde la última actualización.	La propuesta de investigación no es tan exhaustiva como las anteriores, ya que se centra en la capacitación previa del auditor antes de llevar a cabo los requisitos.
Rigor de la metodología	Desactualizada, última versión 2006. Alto rigor	Desactualizada, última versión 2008. Alto rigor	Actualizada constantemente, alto rigor.
Facilidad de uso	Puede ser utilizado con conocimientos intermedios y es fácil de utilizar.	Es muy sencillo de utilizar, aunque se recomienda recibir instrucción antes de utilizarlo.	La facilidad de uso de esta metodología es moderada. Se necesita que el auditor cuente con capacitación y certificaciones, ya que es muy técnica.
Entornos de aplicabilidad	Se aplica principalmente a servidores de IBM, pero también es válido para otros sistemas.	Sería óptimo combinarlo con la metodología OWASP	Se puede aplicar esta metodología todo tipo de servidores, debido a su naturaleza dinámica.
Ámbitos de aplicación	Aplicada a PYMES	Organizaciones financieras complejas y PYMES orientadas a finanzas.	En general para organizaciones grandes y PYMES

Uso por los hackers éticos	Es fácil de aprender y abarca las etapas clave de una auditoría utilizando pruebas de intrusión, mientras se adhiere a los modelos de NIST.	En su mayoría, los profesionales no utilizan esta metodología de forma independiente, sino que la combinan con otras metodologías.	La metodología más comúnmente utilizada, sin embargo, es frecuentemente personalizada por profesionales para adaptarla a sus necesidades, simplificándola en el proceso. Por lo general, su implementación requiere un amplio conocimiento y experiencia en el campo.
Ventajas	La etapa de evaluación es bien reconocida debido a su capacidad para generar informes basados en los pasos seguidos y los datos obtenidos. Además, proporciona recomendaciones de herramientas para llevar a cabo la evaluación de manera efectiva.	El parecido entre ambas metodologías, ISSAF y OSSTMM, hace que se las relacione frecuentemente. Ambas metodologías tienen controles muy bien definidos para llevar a cabo las pruebas de intrusión.	La herramienta cuenta con una amplia documentación y el respaldo de una comunidad global. También proporciona guías detalladas de uso y se enfoca en los estándares de seguridad de la información. Además, se destaca por su alta calidad en los resultados obtenidos.
Desventajas	No hay restricciones en el uso de las pruebas, lo que resulta en acuerdos de uso deficientes con el cliente. Debido a la falta de estabilidad en las instrucciones de las pruebas, el nivel de desarrollo de la práctica es inmaduro y no está actualizado.	Aunque se puede usar como una guía de referencia, esta metodología carece de un proyecto sólido y completo, por lo que no ofrece muchos beneficios adicionales.	Esta metodología no es compatible con otras metodologías y depende en gran medida de la experiencia del hacker, ya que no especifica el tipo de objetivo de cada prueba.
Ámbito y enfoque	El enfoque se centra en satisfacer los requerimientos de evaluación de seguridad de una entidad.	Puede ser utilizado en diversos contextos.	El enfoque operativo es relevante para cualquier organización que

			desee evaluar la seguridad de su información.
Alcance	Se propone evaluar la red, los sistemas y la aplicación de controles utilizando las normas ISO 27001, COBIT, SAS70 y COSO.	El contenido se dirige a profesionales con conocimientos técnicos especializados.	El estudio abarca equipos y sistemas que están relacionados con la red.
Profundidad	El documento brinda pautas exhaustivas para la realización de pruebas en sistemas de información.	Esta metodología se basa en OSSTMM y se complementa con OWASP.	Análisis en detalle
Opinión Personal	La metodología es de fácil uso y puede ser utilizada por usuarios con o sin experiencia, pero no está actualizada. Es una metodología agresiva y altamente intrusiva.	Tiene una alta precisión en la detección de vulnerabilidades, que se incrementa cuando se combina con otra metodología. Es extremadamente detallada y, al igual que la metodología OWASP, es altamente efectiva para el proceso de aprendizaje.	A diferencia de la metodología ISSAF, la metodología OSSTMM establece límites en su aplicación según los acuerdos con los clientes. Esta metodología es considerada más agresiva e intrusiva en comparación. Además, no proporciona una lista de herramientas sugeridas.

Resultados de la evaluación de las metodologías

Después del análisis de las metodologías mediante una lista de cotejo en la cual recaba las vulnerabilidades más frecuentes en una institución financiera según la Organización de los Estados Americanos (2018) con una escala evaluativa que va desde el 0 al 3 se puede determinar que la metodología ISSAF es la más escrutada con relación a OSSTMM Y PTES, el nivel de detalle de ISSAF es más específica, esta misma metodología es aplicable en diferentes entornos debido a su dinamización.

ISSAF es reconocida en su etapa de evaluación por la factibilidad de uso y sus recomendaciones de herramientas para llevar acabo la evaluación de manera efectiva, por otra parte OSSTMM no recomienda herramientas para la evaluación pero si contiene una amplia documentación y sus guías detallan su uso y se enfocan en estándares de seguridad de la información, por último, tenemos a PTES que siguiere muchas herramientas aplicables en diferentes aspectos, sin embargo no cuenta con documentación a detalle.

Para complementar el análisis de las metodologías en necesario realizar las pruebas de vulnerabilidades con diferentes herramientas para comprender desde varias perspectivas conocimientos básicos para la aplicación de técnicas de pentesting.

CAPÍTULO V

DESARROLLO DE PENTESTING EN UNA COOPERATIVA DE SEGMENTO TRES

Propósitos específicos de la investigación

- Investigar y comparar teóricamente diversas metodologías de pentesting para determinar cuál sería más apropiada para aplicar en una cooperativa de ahorro y crédito de nivel tres.
- Configurar un entorno adecuado que sirva como escenario para llevar a cabo las pruebas de pentesting.
- Poner en práctica la metodología de pentesting seleccionada en el entorno establecido.
- Recopilar y analizar los resultados obtenidos durante las pruebas de pentesting para evaluar la efectividad de las medidas de seguridad y detectar posibles vulnerabilidades.

FUNDAMENTACIÓN DE LA SELECCIÓN DE ISSAF

El uso de la metodología ISSAF en una institución financiera se basa en su enfoque práctico y táctico, que proporciona detalles específicos y directrices claras para abordar una amplia gama de problemas de seguridad. ISSAF se destaca por su capacidad para ofrecer una orientación detallada y exhaustiva para garantizar que las pruebas de pentesting sean efectivas en la identificación y mitigación de vulnerabilidades, protegiendo así los activos financieros, dada la naturaleza crítica de la seguridad en el entorno financiero.

Establecer un escenario donde se van a hacer las pruebas de pentesting

Considerando las peculiaridades de las cooperativas de segmento tres, cuya gestión de información depende en gran medida de la disposición de la empresa para invertir, crecer y utilizar

tecnologías de la información y comunicación (TIC), se sugiere aplicar el pentesting siguiendo los siguientes pasos.

Ámbito del test

Durante la fase de análisis, se llevarán a cabo pruebas en la cooperativa que abarcarán:

- Evaluación de puertos abiertos para identificar posibles puntos de acceso vulnerables.
- Escrutinio de servidores para detectar posibles debilidades en la configuración o en el software utilizado.
- Ejecución de ataques de fuerza bruta para verificar la resistencia de las credenciales y contraseñas.
- Implementación de ataques de diccionario para intentar descifrar contraseñas mediante el uso de listas de palabras comunes o predefinidas.

Fundamentación de pruebas a puertos abiertos

Durante la exploración de puertos, se recopila información sobre los puertos abiertos en los equipos informáticos vinculados a la infraestructura de red de la cooperativa. Este procedimiento es comúnmente utilizado como parte del proceso de reconocimiento por parte de los hackers. Los puertos se dividen en tres categorías:

- Los puertos del rango de 0 a 1023 son considerados como puertos conocidos.
- Los puertos del rango de 1024 a 49151 son registrados.
- Los puertos del rango de 49152 a 65535 son privados o dinámicos.

Aunque es posible escanear los 65535 puertos disponibles, los atacantes suelen enfocarse en los "puertos conocidos" debido a su mayor potencial de vulnerabilidad.

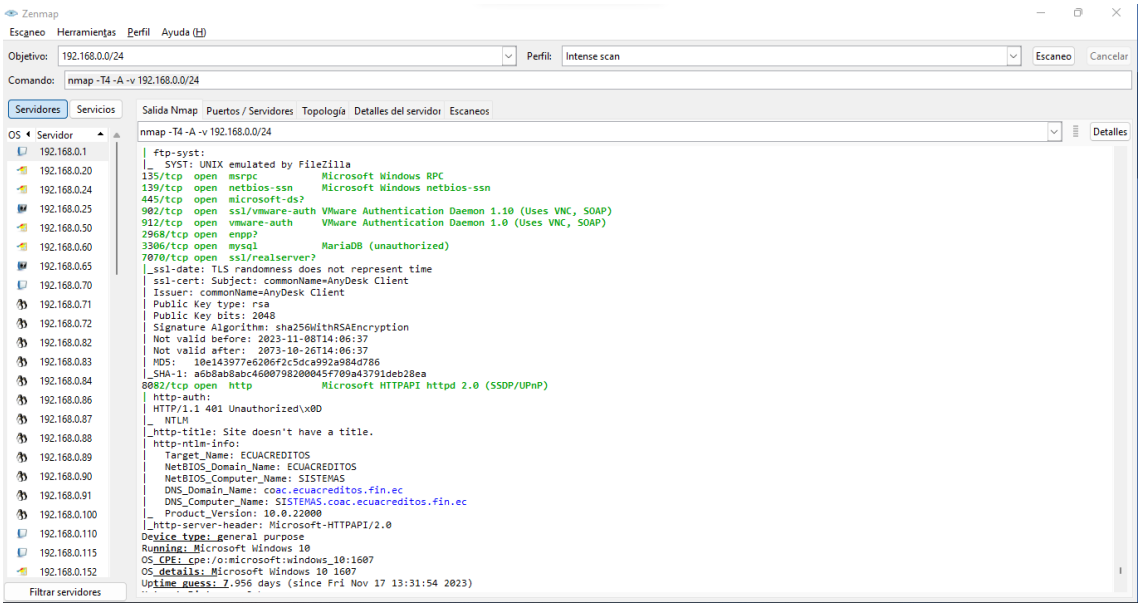
Las cooperativas de ahorro y crédito son susceptibles de convertirse en blanco de hackers, ya sea de manera aleatoria o mediante una identificación previa del objetivo. Una vez seleccionado el objetivo, el hacker procede a obtener la dirección IP de la máquina objetivo y a recopilar información adicional, como la topología de la red, el sistema operativo y otros datos relevantes de la organización. Para ello, se utilizan herramientas especializadas que exploran los puertos abiertos y los servicios activos en la máquina objetivo. Esta información proporciona al hacker datos cruciales sobre la configuración de la red, los sistemas operativos de los servidores, la presencia de firewall, los servicios de internet disponibles y otros detalles sobre la organización y sus usuarios. Con esta información en su poder, el hacker emplea sus habilidades analíticas para identificar posibles vulnerabilidades, puntos de acceso y rutas de escape en el sistema objetivo.

Herramienta por utilizar: Nmap

Según Calderon (2021) *Nmap* es una herramienta de auditoría de seguridad y descubrimiento de redes de código abierto y gratuita, muchos administradores de sistemas y redes la encuentran útil para realizar tareas complejas, como supervisar el tiempo de actividad de hosts o servicios, gestionar programas de actualización de servicios e inventariar redes. Herramienta utilizada para buscar puertos abiertos en la cooperativa de ahorro y crédito segmento tres como se muestra en la Figura 8.

Figura 8

Prueba de puertos abiertos con Nmap



Pruebas a servidores

El valor de la información contenida en los sistemas informáticos aumenta significativamente según el uso que se le pueda dar, ya sea para propósitos beneficiosos o perjudiciales. Por esta razón, existen individuos u organizaciones que buscan comprometer la seguridad informática de empresas e instituciones con el fin de robar información de los servidores para llevar a cabo actividades delictivas, lo que puede resultar en pérdidas significativas, algunas de las cuales pueden ser incalculables para estas instituciones. El objetivo principal de las pruebas de pentesting es proporcionar ayuda a la cooperativa para que pueda tomar medidas preventivas contra estas acciones maliciosas. Estas medidas de prevención se basan en pruebas de intrusión, que examinan la seguridad técnica de los sistemas de datos, redes, servidores, aplicaciones, entre otros. Estas pruebas simulan ataques controlados a las diferentes áreas de la infraestructura de la cooperativa.

Herramienta por utilizar: OpenVAS

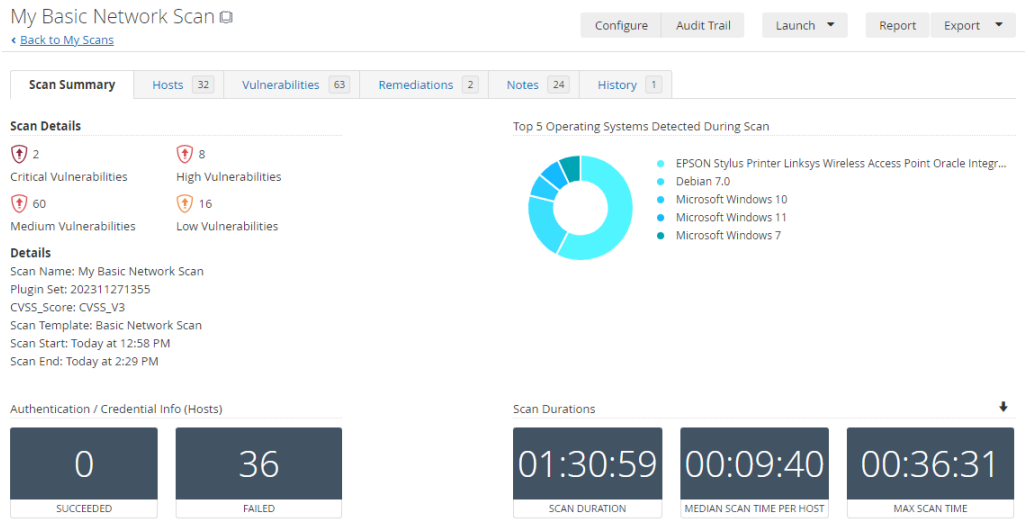
Según Nickerson et al. (2012) OpenVAS es un escáner de vulnerabilidades completo que posee diversas funcionalidades. Entre sus capacidades se encuentran las pruebas autenticadas y no autenticadas, la compatibilidad con protocolos industriales e Internet de alto y bajo nivel, la capacidad de ajuste de rendimiento para escaneos a gran escala y un lenguaje de programación interno potente que permite implementar cualquier tipo de prueba de vulnerabilidad

Fundamentación del uso de Nessus

Según Chicaiza (2019) la elección de este software se basa en su potencia y facilidad de uso como analizador de seguridad de redes. Cuenta con una extensa base de datos que nos permite realizar pruebas y determinar si nuestra red o equipo presenta vulnerabilidades de seguridad. Además de informarnos sobre las vulnerabilidades y su nivel de riesgo (alto, medio, bajo), también nos proporciona soluciones para mitigarlas. Herramienta utilizada para el escaneo de vulnerabilidades en la cooperativa de ahorro y crédito segmento tres como se muestra en la Figura 9.

Figura 9

Escaneo de vulnerabilidades con Nessus



Ataque de fuerza bruta

El propósito de la prueba es evaluar la resistencia ante ataques como consultas maliciosas en la base de datos y accesos no autorizados al sistema. En el caso de que no se detecten cuentas de usuario durante el ataque mencionado anteriormente, se recomienda reforzar la seguridad mediante intentos de fuerza bruta, como el uso de cuentas falsas para intentar colapsar el servidor a través de la autenticación. Es importante tener en cuenta que los hackers pueden dedicar desde minutos hasta años para descifrar una contraseña, dependiendo de su complejidad y longitud. Por lo tanto, se sugiere crear contraseñas con más de 8 caracteres, que incluyan caracteres especiales, letras mayúsculas, letras minúsculas y números.

Ataques de diccionario

Es importante realizar un diagnóstico de los ataques de diccionario. La estrategia consiste en probar todas las palabras de un diccionario. Aunque puede requerir mucho trabajo, esta técnica

suele ser más efectiva que el ataque de fuerza bruta, ya que los usuarios suelen utilizar palabras que les resulten fáciles de recordar. Esto es especialmente común en cooperativas.

Herramienta por utilizar para generar diccionario: CUPP

El uso de herramientas especializadas para la creación de diccionarios personalizados es crucial en el ámbito de la seguridad informática, particularmente en el desarrollo de pruebas de penetración. Una de estas herramientas es CUPP (Common User Passwords Profiler), la cual se destaca por su capacidad para generar diccionarios basados en la información personal del objetivo, como nombres, fechas de nacimiento y otras características específicas que aumentan la efectividad de los ataques de fuerza bruta. Según Ferrarini et al. (2020), CUPP permite crear perfiles de usuarios detallados y generar listas de contraseñas potenciales, lo que facilita la identificación de posibles vulnerabilidades en sistemas de autenticación.

Herramienta por utilizar para ataque de fuerza bruta con un diccionario: Burp Suite

Burp Suite es una herramienta integral ampliamente utilizada en pruebas de seguridad web, particularmente efectiva en la ejecución de ataques de fuerza bruta utilizando diccionarios. Esta herramienta permite a los profesionales de seguridad automatizar y personalizar los ataques, facilitando la identificación de contraseñas débiles y vulnerabilidades en los sistemas de autenticación. Según PortSwigger (2021), Burp Suite proporciona funcionalidades avanzadas para realizar estos ataques de manera eficiente, integrando módulos como el "Intruder", que permite realizar ataques de fuerza bruta y pruebas de fuzzing, optimizando así la evaluación de la seguridad de las aplicaciones web.

Fase i. Planificación y preparación:

Este proceso permite preparar el lugar de trabajo y es fundamental antes de comenzar la planificación. Antes de iniciar, se debe firmar un contrato profesional con el cliente donde se establecen claramente las responsabilidades y funciones de ambas partes como se muestra en la Figura 10 y 11.

Figura 10

Contrato de auditoria técnica de seguridad

CONTRATO DE AUDITORÍA TÉCNICA DE SEGURIDAD

En Otavalo, a XX de XXX de 202X

De una parte, **XXXXXXXXXXXXXXXX**, (en lo sucesivo "**AUDITOR**") con domicilio social en XXXXXXXXXXXX y C.I.F. XXXXXXXXX y de otra parte **XXXXXXXXXX** con domicilio social en XXXXXXXXXXXXX, y C.I.F. XXXXXXX (en lo sucesivo **CLIENTE**).

Ambas partes se reconocen mutuamente la capacidad legal suficiente para el otorgamiento del presente contrato y

EXPONEN

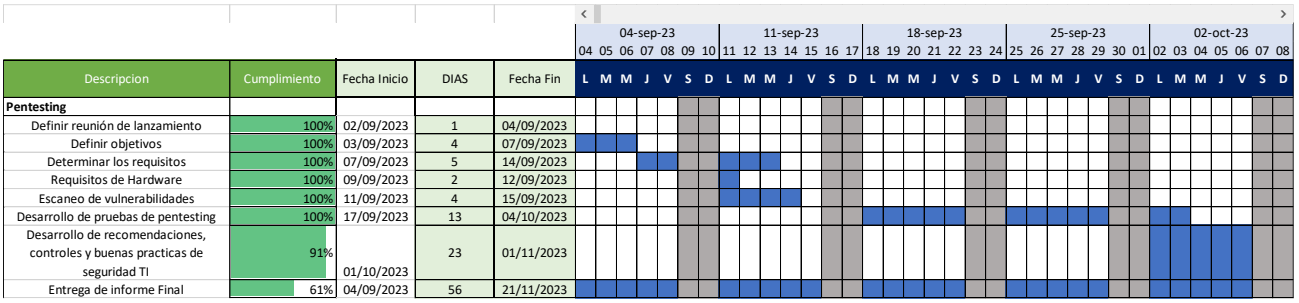
I.- Que **AUDITOR** es una empresa / un profesional del sector de XXXXXXXXXX y que se dedica, entre otras actividades, a proporcionar servicios de ciberseguridad.

II.- Que el **CLIENTE** está interesado en que **AUDITOR** le preste un Servicio de Auditoría Técnica de Seguridad con las características que se describen en el presente contrato.

III.- Que ambas partes están de acuerdo en llevar a cabo el presente contrato en base a las siguientes

Figura 11

Plan de trabajo Gantt para desarrollo de pentesting.



Descripcion	Cumplimiento	Fecha Inicio	DIAS	Fecha Fin
Pentesting				
Definir reunión de lanzamiento	100%	02/09/2023	1	04/09/2023
Definir objetivos	100%	03/09/2023	4	07/09/2023
Determinar los requisitos	100%	07/09/2023	5	14/09/2023
Requisitos de Hardware	100%	09/09/2023	2	12/09/2023
Escaneo de vulnerabilidades	100%	11/09/2023	4	15/09/2023
Desarrollo de pruebas de pentesting	100%	17/09/2023	13	04/10/2023
Desarrollo de recomendaciones, controles y buenas practicas de seguridad TI	91%	01/10/2023	23	01/11/2023
Entrega de informe Final	61%	04/09/2023	56	21/11/2023

Fase ii. Evaluación:

En la fase de evaluación se realizaron las diferentes pruebas de pentesting como se muestran en las siguientes Figuras:

Puertos abiertos

Se realizó una prueba de puertos abiertos con diferentes herramientas recomendadas por las diferentes metodologías como se lo muestra en la Tabla 8 y Figura 12.

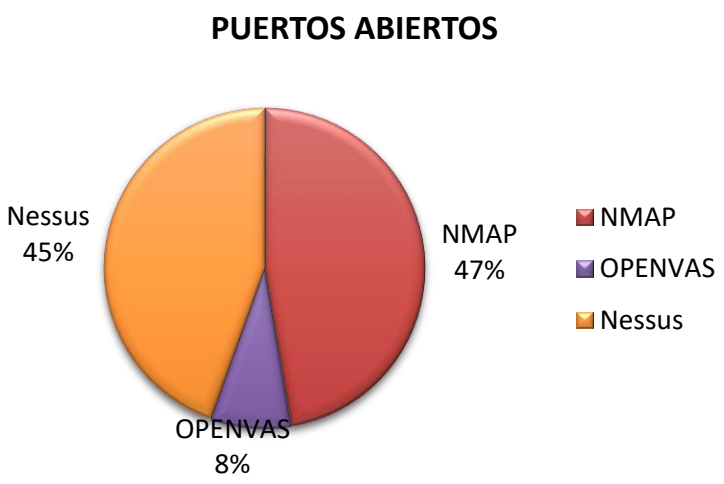
Tabla 8

Cantidad de puertos abiertos con Nmap, OpenVAS Y Nessus

	Nmap	OpenVAS	Nessus
PUERTOS ABIERTOS	204	35	192

Figura 12

Cantidad de puertos abiertos



Interpretación

En la Tabla 8 y en la Figura 12 se muestran los resultados en cuanto al indicador de la cantidad de puertos abiertos detectados en las pruebas realizadas hacia la infraestructura, con el fin de comparar la eficacia de diferentes herramientas. Según los datos recopilados, Nmap logró detectar 204 puertos abiertos, lo que representa un 47% del total. Por otro lado, Nessus identificó 192 puertos abiertos, equivalente al 45%, mientras que OpenVAS detectó solamente 35 puertos abiertos, representando un 8% del total.

Estos resultados indican que Nmap es la herramienta más eficiente para detectar puertos abiertos en los dispositivos escaneados, seguido por Nessus, mientras que OpenVAS mostró la menor eficacia en este aspecto.

Vulnerabilidades

Se realizaron pruebas de detección de vulnerabilidades con dos diferentes herramientas recomendadas por las diferentes metodologías como se lo muestra en la Tabla 9 Figura 13.

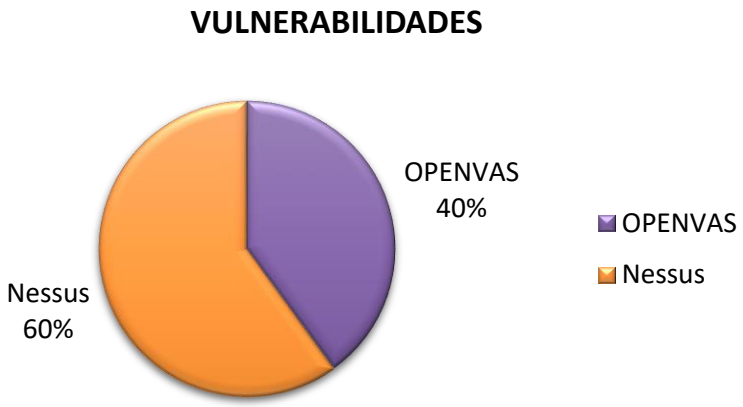
Tabla 9

Cantidad de vulnerabilidades encontradas con las herramientas OpenVAS y Nessus

	OpenVAS	Nessus
VULNERABILIDADES	42	63

Figura 13

Cantidad de vulnerabilidades encontradas



Interpretación

En la Tabla 9 y la Figura 13 se presentan los resultados relativos al número de vulnerabilidades detectadas durante las pruebas realizadas hacia la infraestructura, con el objetivo de comparar la eficacia de diferentes herramientas. Según los datos obtenidos, Nessus detectó 63 vulnerabilidades, equivalente al 60%, mientras que OpenVAS encontró 42 vulnerabilidades, lo que corresponde al 40%.

Estos resultados sugieren que Nessus es la herramienta más eficaz para detectar vulnerabilidades en la infraestructura evaluada, seguida por OpenVAS que mostró la menor eficacia en este aspecto.

Figura 14

Identificación de puertos abiertos del servidor principal.

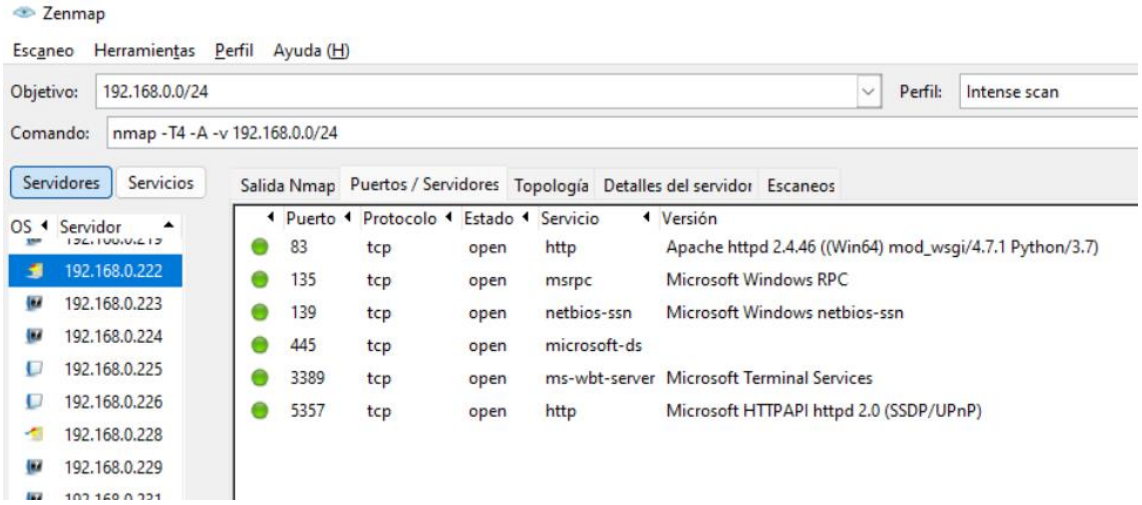


Figura 15

Prueba al servidor NAS de vulnerabilidad Samba remote code execution vulnerability (CVE-2017-7494)

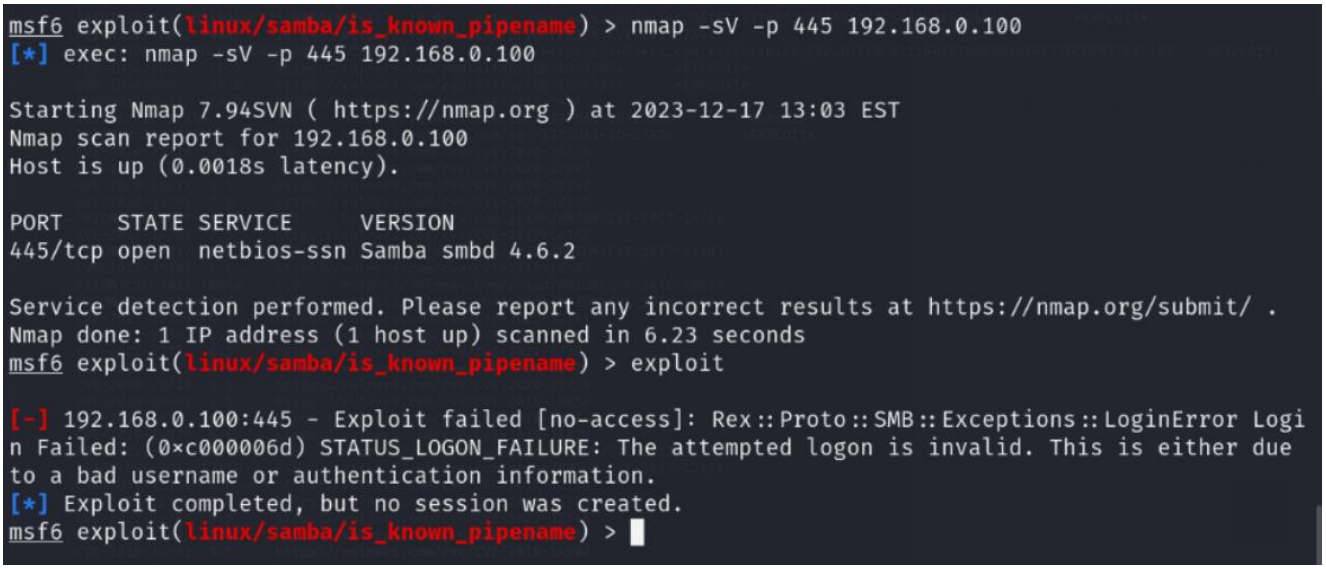


Figura 16

Escaneo a una cooperativa de ahorro y crédito segmento tres con OpenVAS

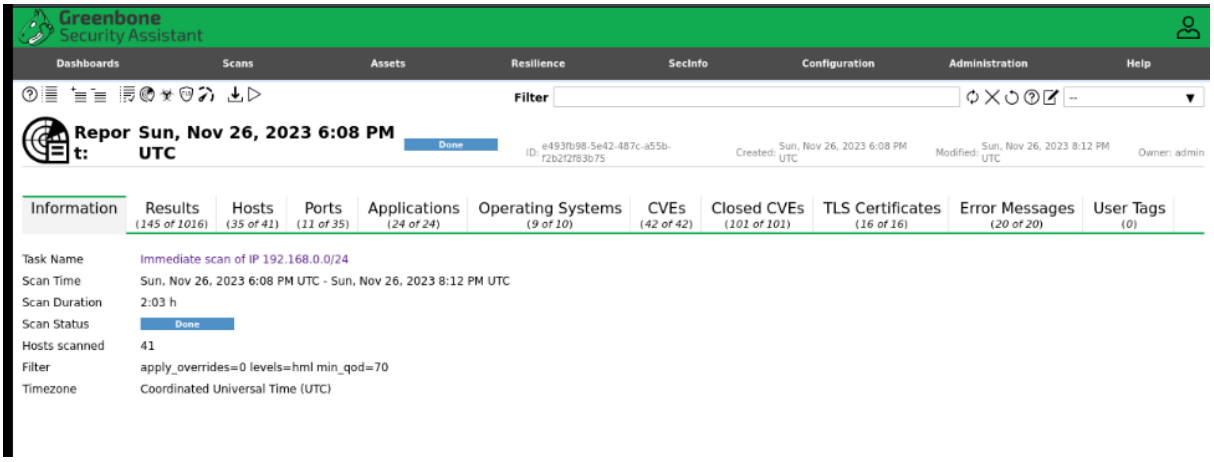


Figura 17

Login de biométrico en la intranet de una cooperativa de ahorro y crédito segmento tres

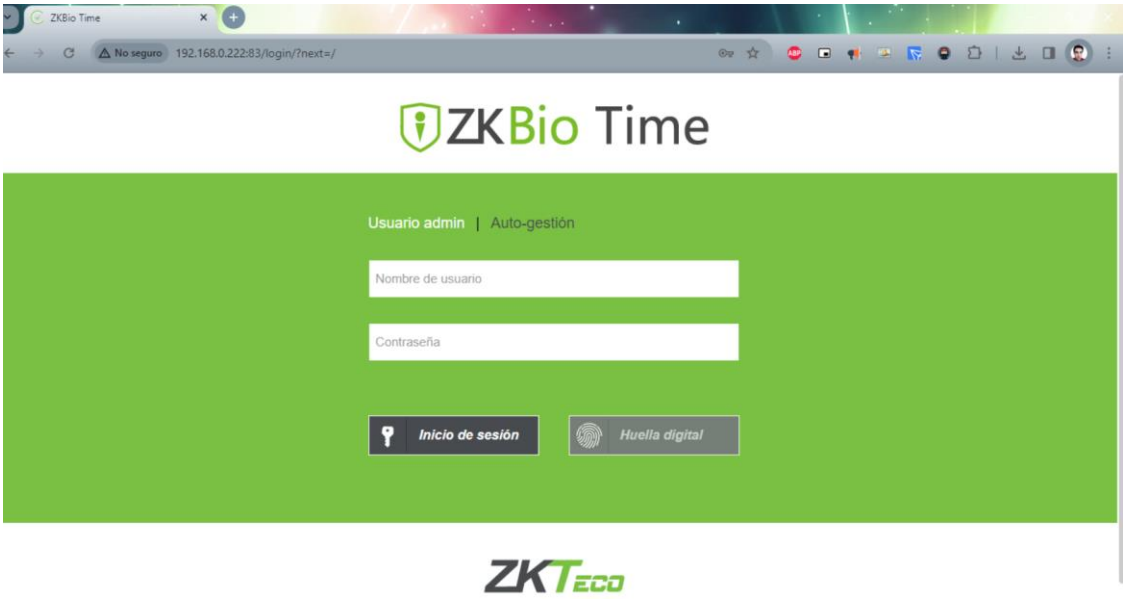


Figura 18

Diccionario de datos

Figura 19

Ataque de Fuerza Bruta con burp suite.

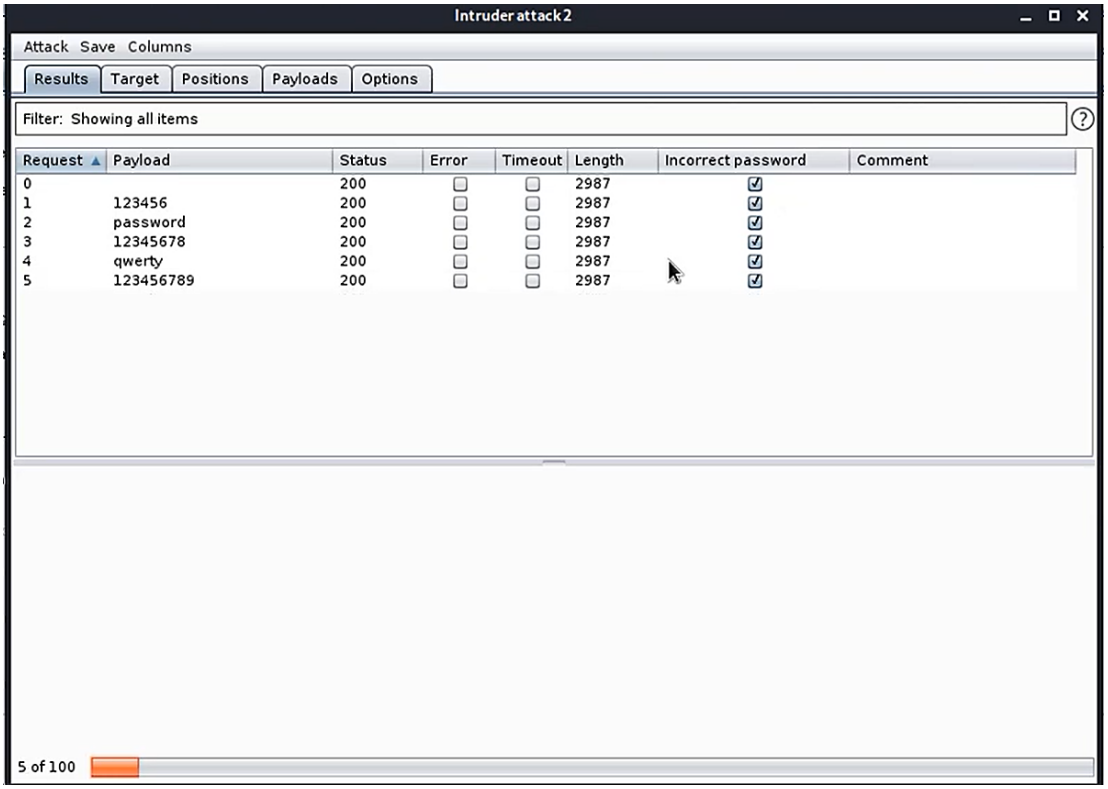
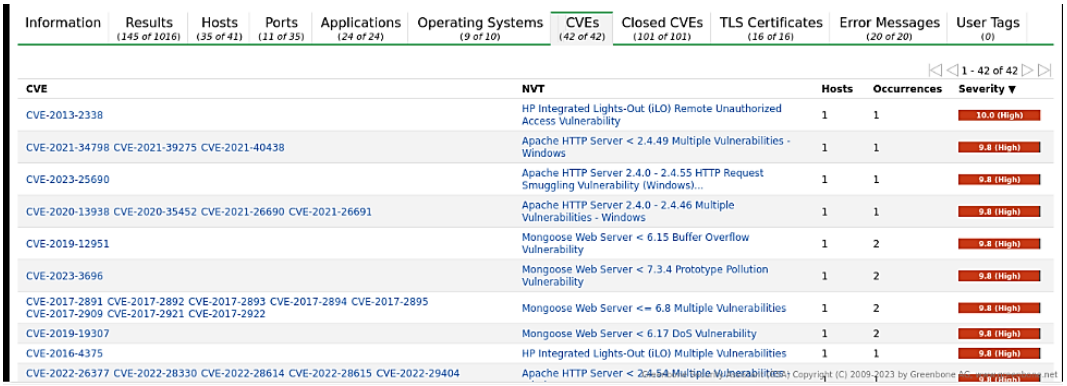


Figura 20

Detalle de vulnerabilidades del servidor NAS



Information | Results (145 of 1016) | Hosts (35 of 41) | Ports (11 of 35) | Applications (24 of 24) | Operating Systems (9 of 10) | CVEs (42 of 42) | Closed CVEs (101 of 101) | TLS Certificates (16 of 16) | Error Messages (20 of 20) | User Tags (0)

1 - 42 of 42

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2013-2338	HP Integrated Lights-Out (iLO) Remote Unauthorized Access Vulnerability	1	1	10.0 (High)
CVE-2021-34798 CVE-2021-39275 CVE-2021-40438	Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2023-25690	Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability (Windows)...	1	1	9.8 (High)
CVE-2020-13938 CVE-2020-35452 CVE-2021-26690 CVE-2021-26691	Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2019-12951	Mongoose Web Server < 6.15 Buffer Overflow Vulnerability	1	2	9.8 (High)
CVE-2023-3696	Mongoose Web Server < 7.3.4 Prototype Pollution Vulnerability	1	2	9.8 (High)
CVE-2017-2891 CVE-2017-2892 CVE-2017-2893 CVE-2017-2894 CVE-2017-2895 CVE-2017-2909 CVE-2017-2921 CVE-2017-2922	Mongoose Web Server <= 6.8 Multiple Vulnerabilities	1	2	9.8 (High)
CVE-2019-19307	Mongoose Web Server < 6.17 DoS Vulnerability	1	2	9.8 (High)
CVE-2016-4375	HP Integrated Lights-Out (iLO) Multiple Vulnerabilities	1	1	9.8 (High)
CVE-2022-26377 CVE-2022-28330 CVE-2022-28614 CVE-2022-28615 CVE-2022-29404	Apache HTTP Server < 2.4.54 Multiple Vulnerabilities	1	1	9.8 (High)

Fase iii. Reportes, limpieza y destrucción de artefactos:

En este contexto, la información se almacena y se guarda en los sistemas de las pruebas de protección, y posteriormente se eliminan sin dejar rastro como se muestra en las Figuras 22 y 23

Figura 21

Informe Final generado con la herramienta Nessus de las vulnerabilidades de la cooperativa.

Top 10 High Vulnerabilities: (CVSS v3.0)

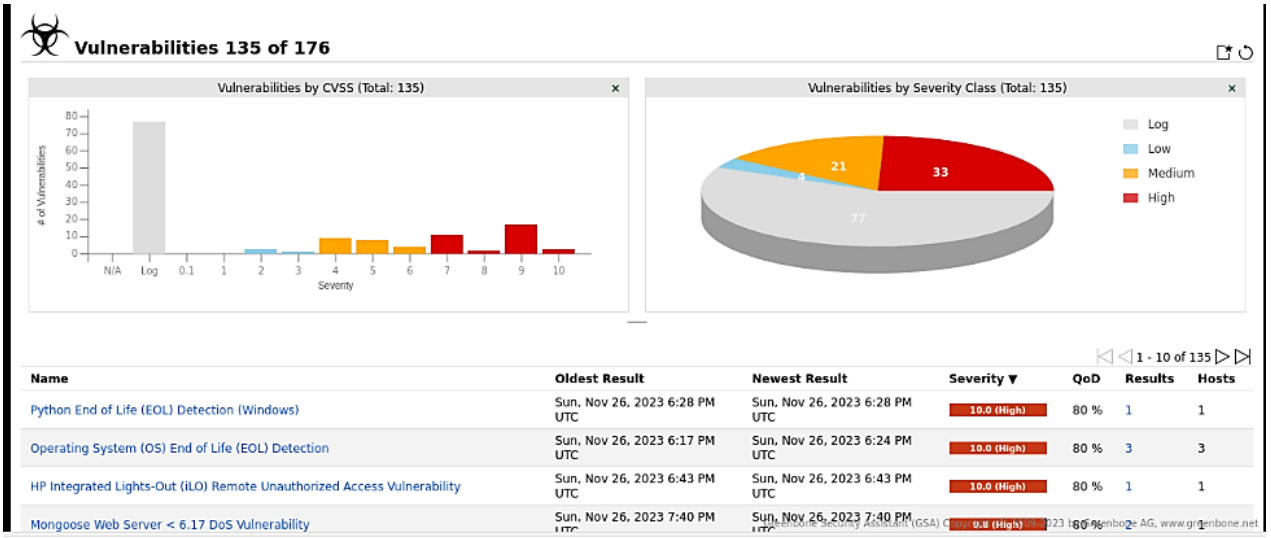
Top 10 most prevalent high vulnerabilities

Plugin ID	Plugin Name	Plugin Family	CVSS v3.0	Known Exploit?	Publication Date	Count
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	7.5	-	2016/08/24	3
35291	SSL Certificate Signed Using Weak Hashing Algorithm	General	7.5	Yes	2004/08/18	2
97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	Windows	8.1	Yes	2017/03/14	1
100464	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	8.1	-	2017/05/09	1
69552	Oracle TNS Listener Remote Poisoning	Databases	7.3	Yes	2012/04/30	1

* indicates the v3.0 score was not available; the v2.0 score is shown

Figura 22

Informe generado por OpenVAS.



Considerando las aplicaciones, podemos decir que existen pruebas de protección y herramientas autorizadas, pero estas no permiten estudiar todas las características requeridas en la actualidad.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES.

Se llevó a cabo una investigación teórica sobre las metodologías de pentesting para su aplicación en una cooperativa de ahorro y crédito segmento tres. Se compararon diferentes metodologías con el fin de entender mejor lo que cada una ofrece, evaluando sus ventajas, desventajas, enfoque y facilidad de implementación. Se decidió utilizar ISSAF debido a que proporciona tácticas adecuadas para una prueba exhaustiva de seguridad.

Se determino un escenario de 45 equipos informáticos conectados a la red de una cooperativa, donde se realizó el pentesting, de puertos abiertos y vulnerabilidades existentes en cada equipo, aplicando herramientas de pentesting sugeridas en la metodología establecida.

Después de un análisis exhaustivo utilizando una lista de cotejo y evaluación cualitativa de las tres metodologías establecidas, así como la ejecución de la metodología con diversas herramientas en el proceso de pentesting, se llegó a la conclusión de que la metodología ISSAF es la más eficaz para identificar vulnerabilidades de seguridad informática en una cooperativa de ahorro y crédito segmento tres. Esta determinación se basa en el análisis de las principales vulnerabilidades identificadas en una institución financiera según la lista de cotejo establecida en el estudio realizado por la Organización de los Estados Americanos (2018). La metodología ISSAF se destaca por su aplicabilidad en instituciones financieras y su disponibilidad de plantillas específicas para llevar a cabo pruebas de pentesting, lo que simplifica la gestión del proceso de diagnóstico.

El objetivo de realizar pruebas no anunciadas es simular una situación real en la que un analista intentará encontrar y comprometer la seguridad de la empresa. Estas pruebas tienen un

valor mayor que las anunciadas, ya que permiten analizar todos fallos de seguridad en los componentes de forma habitual.

De acuerdo con las pruebas realizadas en la cooperativa de ahorro y crédito segmento tres con las herramientas OpenVAS y Nessus en la cual se encontraron con Nessus que detecto 63 y OpenVAS 42, concluyendo que Nessus tiende a encontrar más vulnerabilidades.

El pentesting, como método preventivo y eficaz, se basa en la realización de pruebas que simulan casos reales con el fin de detectar vulnerabilidades en las redes de datos o sistemas de cualquier empresa, que puedan ser aprovechadas por ciberdelincuentes, de las pruebas de ataque por diccionario no se obtuvieron accesos éxito por la complejidad de las contraseñas utilizadas en la cooperativa de ahorro y crédito segmento tres, por otra parte de las vulnerabilidades encontradas se realizaron ataques con metasploit sin tener éxito puesto que cuentan con los parámetros necesarios para evitar el acceso.

RECOMENDACIONES.

La metodología ISSAF engloba todos los aspectos del análisis a un sistema informático, sin embargo, no en todos los casos se sugiere herramientas de pentesting a utilizar en las diferentes fases de ejecución, por lo cual es recomendable utilizar las sugerencias de herramientas proporcionadas por metodologías como PTES, misma que establece muchas herramientas documentadas para este proceso y de esta forma complementar el análisis.

Es fundamental documentar los procedimientos llevados a cabo durante el pentesting, de modo que se pueda proporcionar la información necesaria al personal y permitir que otros especialistas continúen con la ejecución de futuras pruebas de pentesting.

Es esencial que las cooperativas de cualquier segmento incluyan en su planificación anuales pruebas de pentesting, tal como lo establece la disposición de la SEPS. Esto permitirá detectar intrusos y proteger la información de posibles pérdidas de recursos. Por lo tanto, es importante evaluar esta práctica en el cronograma de la empresa y evitar cualquier descuido por parte del área administrativa en este asunto.

Es importante que los administradores de sistemas estén conscientes y actúen con precaución al utilizar las herramientas descritas en este documento, ya que la ética es un aspecto muy sensible. Además, es fundamental que realicen sus tareas dentro del marco legal establecido.

Es fundamental que a pesar de que no se obtuvieron ataques exitosos por las medidas de seguridad optadas por la cooperativa de ahorro y crédito de segmento tres, es necesario corregir las diferentes vulnerabilidades encontradas, con bloqueos de puertos o actualizaciones del sistema

REFERENCIAS

ISO/IEC 27002. (2022). *Information technology - Security techniques - Code of practice for information security controls.*

Ambit Bst . (2020, Noviembre 10). *Ambit Bst* . https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-informáticas

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales (LOPD).* Registro Oficial No. 431.

Barkley, J., & Kebert, A. (2009). *Information security principles: A practitioner's perspective. In 2009 IEEE International Conference on Electro/Information Technology.*

Buendía, J. F. (2013). *Seguridad informática.* España: McGraw-Hill. https://d1wqtxts1xzle7.cloudfront.net/34758985/Seguridad_Informatica_McGraw-Hill_2013_-_www.FreeLibros.me_-_copia.pdf?1410924373=&response-content-disposition=inline%3B+filename%3DSeguridad_Informatica_Mc_Graw_Hill_2013.pdf&Expires=1716311184&Signature=L8

Burbano, A. A. (2019). *PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE.* ESMERALDAS.

Calderon, P. (2021). *Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips.* Packt Publishing Ltd. .

Castro Cubillos, S. M. (2017). White hat: Hacking ético. *Universidad Piloto de Colombia*, 2-3.

Castro, C. (2019). *Pruebas de Penetración e Intrusión.* http://repository.unipiloto.edu.co/handle/20.500.12277/6273

Chicaiza, V. (2019). Metodología abierta de testeo en SeguridadNESSUS. *Nexos Científicos*, 35-41. https://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/25/25

Chimbo, C. P. (2021). *Recomendaciones para el manejo de información y administración de ciberseguridad en el Sector Financiero Popular y Solidario.* https://www.seps.gob.ec/wp-content/uploads/SEPS-SGD-IGT-2021-21112-OFC.pdf.pdf

Commission Federal Trade. (2016). *Cómo Proteger la Información Personal: Una Guía para Negocios.* https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf

Cruz Gavilanes, Y., & Martínez Santander, C. (2017). Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final. *Dominio de las Ciencias*, 505-516. https://dialnet.unirioja.es/descarga/articulo/6128529.pdf

Díaz, J., Cárdenas, A., & Manadhata, P. (2016). *A survey of cybersecurity management methods. ACM Computing Surveys* .

Férnandez, C. C. (2016). *Metódologia de la investigación sexta edición.*

Ferrarini, A., Fuchs, C., De Sanctis, E., & Petrioli, C. (2020). *Security and Privacy in the Era of Intelligent Devices and Communication.*

Frutos, A. M. (2015, Octubre 31). *ComputerHoy*. ComputerHoy: https://computerhoy.com/noticias/software/que-es-hacker-que-tipos-hacker-existen-36027

Fuentes Maestro, A. (2014). *Elaboración de una metodología de test para intrusión dentro de la auditoria de seguridad.* https://reunir.unir.net/bitstream/handle/123456789/2331/AntonioFuertesMaestroTFM.pdf?sequence=3&isAllowed=y

Gallardo Echenique, E. E. (2017). *Metodología de la Investigación.* Huancayo. https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

Garcia Vega, A. R., & Morales Baren, D. J. (2022). *Seguridad informática mediante hacking ético en la aplicación de pentesting para el análisis de vulnerabilidades en las redes de datos de la cooperativa sierra centro sucursal la maná, provincia de Cotopaxi.* La Maná. http://repositorio.utc.edu.ec/bitstream/27000/8458/1/UTC-PIM-000410.pdf

Hérnandez, ,. S., Férnandez, ,. C., & Baptista, L. P. (2014). *Metodólogia de la Investigación 6ta Edición.*

Hout, N. J. (2019). *Standardised penetration testing? Examining the usefulness of current penetration testing methodologies.* https://www.researchgate.net/publication/335652869_Standardised_Penetration_Testing_Examining_the_Usefulness_of_Current_Penetration_Testing_Methodologies

Howard, M., LeBlanc, D., & Viega, J. . (2005). *24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. McGraw-Hill Osborne Media.*

International Organization for Standardization. (2013). *Information technology - Security techniques - Code of practice for information security controls.*

ISECOM. (2010). *The Open Source Security Testing Methodology Manual.* https://www.isecom.org/OSSTMM.3.pdf

ISO. (2013, Marzo 28). *Management Standards - ISO 9000*. http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm

ISO 31000. (2018). *Risk management - Guidelines.*

ISO/IEC 27001. (2022). *nformation technology – Security techniques – Information security management systems – Requirements.*

Lampson, B. (2004). *Computer security in the real world.*

Laudon, J. P., & Laudon, K. C. (2016). *Sistemas de información gerencial.* México: Prentice Hall.

León, M., & León, P. (2021). Hacking ético en el sector financiero. 83-89. https://revistas.unl.edu.ec/index.php/suracademia/article/view/927/903

Llerena, A. E. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592020000100116&lang=es#aff1

M. Cornejo Velázquez, M. G. (2015). Principios de Seguridad Informática en Sistemas de Información. *Publicación semestral XIKUA No. 6 BOLETÍN CIENTÍFICO*.

Mora Ortega , A. S. (2017). *Metodología de Hacking Ético para Instituciones Financieras, aplicación de un caso práctico.* Cuenca. http://dspace.ucuenca.edu.ec/bitstream/123456789/28552/1/Trabajo%20de%20titulación.pdf

Muñoz, A. (2015, octubre 31). *Computerhoy*. Computerhoy: https://computerhoy.com/noticias/software/que-es-hacker-que-tipos-hacker-existen-36027

Naciones Unidas. (2018). *La Agenda 2030 y los Objetivos de Desarrollo Sostenible Una oportunidad para América Latina y el Caribe.* Santiago. https://repositorio.cepal.org/bitstream/handle/11362/40155/24/S1801141_es.pdf

Narasimhaiah, M., & Manvi, S. . (2011). *Comparative study of defense mechanisms against brute force attack. International Journal of Computer Science & Communication Networks.*

Nickerson, C., Kennedy, D., Riley, C. J., Smith, E., Amit, I. I., Rabie, A., Friedli, S., Searle, J., Knight, B., Gates, C., McCray, J., Perez, C., Strand, J., Tornio, S., Percoco, N., Shackelford, D., Smith, V., Wood, R., & Remes, W. (2012). *Penetration Testing Execution Standard*. Penetration Testing Execution Standard: http://www.penteststandard.org/index.php/PTES_Technical_Guidelines

OISSG. (2005). *Information Systems Security Assessment Framework(ISSAF) draft 0.2.*

Olson, B., Grance, T., & Scarfone, K. (2012). *Technical guide to information security testing and assessment. National Institute of Standards and Technology Special Publication.*

Organización de los Estados Americanos. (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.*

Ortega, A. S. (2017). Metodología de Hacking Ético para Instituciones Financieras.

Parandini, M., & Ramilli, M. (2010). *Towards a practical and effective security testing methodology (Proceeding).*

Pedraza Melo, N., Bernal Gonzalez, I., Lavín Verástegui, J., & Lavín Rodríguez, J. (2015). La calidad del servicio: Caso UMF. *Conciencia Tecnológica*, 29,39–45.

Penagos Muñoz, C. C. (2019). *ANALISIS DE METODOLOGÍAS DE ETICAL HACKING PARA LA DETECCIÓN DE VULNERABILIDADES EN LAS PYMES.*

PortSwigger. (2021). *PortSwigger*. https://portswigger.net/burp

PYMESEC. (2015). *PYMESEC*. PYMESEC: https://pymesec.org/issaf/

Raytheon, W. (2015). 2015 industry drill-down report financial services. *Websense® Security Labs*, 11. https://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf

Rivera, D. A. (2016, 05 10). LA IMPORTANCIA DEL HACKING ÉTICO EN EL SECTOR FINANCIERO. *Universidad Piloto de Colombia*, 6. http://repository.unipiloto.edu.co/handle/20.500.12277/2735

Rojas, C. M. (2015). *Tipos de Investigación científica: Una simplificación de la complicada incoherente nomenclatura y clasificación.*

Salas, M. G. (2012). *PROCEDIMIENTO FORMAL DE ETHICAL HACKING PARA LA INFRAESTRUCTURA TECNOLOGICA DE LOS SERVICIOS POR INTERNET DE LA BANCA ECUATORIANA.* https://bibdigital.epn.edu.ec/bitstream/15000/5736/1/CD-4677.pdf

Scarfone, K., & Mell, P. . (2009). *Guide to enterprise password management. National Institute of Standards and Technology Special Publication.*

SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI. (2022). *Norma de control respecto a la seguridad de la información en las entidades del Sector Financiero Popular y Solidario bajo control de la Superintendencia de Economía Popular y Solidaria.* https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

Tamayo Veintimilla, O. A. (2016). *Desarrollo de una guia técnica estándar para aplicar herramientas de ethical hacking en redes de datos, dirigido de PYMES.*

The Organization of American States. (2019). *DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA.* https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Urbina, G. B. (2016). *Introducción a la seguridad informática.* Grupo editorial PATRIA. https://books.google.es/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=SEGURIDAD+F%C3%8DSICA+informatica+&ots=0XSy9FxfFm&sig=CIHY28Q7JN40geOL-YgXiDwuPuE#v=onepage&q&f=false

Vieira, A., Madeira, H., & Figueiredo, M. (2017). *Assessing the effectiveness of combined approaches to information security risk management in organizations. Information Systems Frontiers.*

Villares Saltos, C. A. (2017). *Estrategia de hacking ético y los niveles de seguridad en la intranet de la cooperativa de ahorro y crédito 13 de abril ltda de la ciudad de "ventanas".* Babahoyo. https://dspace.uniandes.edu.ec/bitstream/123456789/8426/1/TUBMIE008-2017.pdf

Wang, Y., Ren, Y., & Lou, W. (2012). *Towards secure and practical password-based authentication systems on mobile devices. Wireless Networks,.*

Wirton, C. G. (2021). *Ciberseguridad en el Sector Financiero.* Madrid. https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/46570/TFG-Garcia%20Wirton%2C%20Carlota.pdf?sequence=2

Zargar, S., Joshi, J., & Tipper, D. (2013). *A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials.*