UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CARRERA: MAESTRIA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA.

INFORME FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR, MODALIDAD PROYECTO DE INVESITGACIÓN

TEMA:

"DESARROLLO DE UN ENTORNO SEGURO CAPTURE THE FLAG (CTF) CON INTEGRACIÓN DE ESCENARIOS DE CIBERATAQUES BASADOS EN MITRE ATT&CK COMO ESTRATEGIA DE PREVENCIÓN DE CIBERATAQUES. CASO DE ESTUDIO: UNIVERSIDAD TÉCNICA DEL NORTE"

Trabajo de Titulación previo a la obtención del Título de Magister en Computación con mención en Seguridad Informática.

Línea de investigación: Desarrollo, aplicación de software y cybersecurity (seguridad cibernética)

AUTOR:

FUENTES HERNÁNDEZ EDISON ALEXANDER

DIRECTOR:

MSC. FABIÁN GEOVANNY CUZME RODRÍGUEZ

Ibarra, junio 2025

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE TITULACIÓN CURRICULAR

Ibarra, 05 de junio de 2025

MSc. Fabián Cuzme Rodríguez

CERTIFICA:

Haber revisado el presente informe final de trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

Es todo en cuanto puedo certificar a la verdad.

Atentamente,

Fabián Cuzme Rodríguez

DIRECTOR DE TRABAJO DE GRADO

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

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

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:	0401533005		
APELLIDOS Y NOMBRES:	Fuentes Hernández Edison Alexander		
DIRECCIÓN:	Shyris 5-33 y Avenida Atahualpa		
EMAIL:	eafuentesh@utn.edu.ec		
TELÉFONO FIJO:	N/A	**TELÉFONO MÓVIL:**	0999584904

DATOS DE LA OBRA	
TÍTULO:	DESARROLLO DE UN ENTORNO SEGURO CAPTURE THE FLAF (CTF) CON INTEGRACIÓN DE ESCENARIOS DE CIBERATAQUES BASADOS EN MITRE ATT&CK COMO ESTRATEGIA DE PREVENCIÓN DE CIBERATAQUES. CASO DE ESTUDIO: UNIVERSIDAD TÉCNICA DEL NORTE
AUTOR (ES):	EDISON ALEXANDER FUENTES HERNÁNDEZ
FECHA:	05/06/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA:	Magister en Computación con mención en Seguridad Informática
ASESOR /DIRECTOR:	MSC. FABIÁN GEOVANNY CUZME RODRÍGUEZ

2. CONSTANCIAS

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

Ibarra, a los 05 días del mes de junio de 2025

EL AUTOR:

.....

Nombre: Edison Alexander Fuentes Hernández

Dedicatoria

Este trabajo quiero dedicárselo a mi amada esposa Yady, por ser mi apoyo incondicional en cada paso de este camino. Gracias por tu paciencia, comprensión y amor, por motivarme en los momentos difíciles y celebrar conmigo cada logro. Sin ti, este sueño no sería posible. A mis hijos, Iann y Santiago, la mayor inspiración en mi vida. Que este esfuerzo sea un ejemplo de perseverancia y dedicación para ustedes. Cada página de este trabajo lleva impreso el amor que les tengo y el deseo de brindarles un futuro mejor. A mi madre, la mujer más importante en mi vida gracias por enseñarme tantas cosas buenas y sobre todo por tu amor en cada momento, tu ejemplo de esfuerzo y nobleza han forjado lo que ahora yo intento ser como persona y padre. A mis abuelos, que, a pesar de estar lejos, siempre me demuestran su amor, los amo.

Finalmente dedico una sincera gratitud a todo el proceso recorrido en esta maestría, ha sido un viaje excepcional, con grandes docentes, quienes, con su guía, conocimientos y dedicación han contribuido significativamente a mi formación académica y profesional. Sus enseñanzas han sido un pilar fundamental en la construcción de este trabajo y sobre todo en mi crecimiento como profesional en ciberseguridad.

ÍNDICE GENERAL

1 CAPÍTULO 1 - EL PROBLEMA DE INVESTIGACIÓN 1

1.1 Problema de investigación 1

1.2 Interrogantes de la Investigación 3

1.3 Objetivos de la investigación 4

1.3.1 Objetivo General 4

1.3.2 Objetivos Específicos 4

1.4 Hipótesis de trabajo 5

1.5 Hipótesis alternativa 5

1.6 Categorización de Variables 5

1.7 Justificación 6

2 CAPÍTULO II – MARCO REFERENCIAL 9

2.1 Marco teórico 9

2.1.1 Seguridad informática 9

2.1.2 Ataques informáticos 10

2.1.3 Amenazas y vulnerabilidades 12

2.1.4 Aprendizaje de Ciberseguridad 15

2.1.5 Entrenamiento Cibernético 17

2.1.6 MITRE ATT&CK Framework 24

2.2 Marco legal 27
2.2.1 Legislación Nacional Aplicable 27
3 CAPÍTULO III - MARCO METODOLÓGICO 29
3.1 Descripción del área de estudio / Descripción del grupo de estudio 29
3.2 Enfoque y tipo de investigación 29
3.3 Procedimiento de investigación 30
3.3.1 Fase 1: Revisión bibliográfica. 30
3.3.2 Fase 2: Diseño e implementación de la infraestructura CTF 31
3.3.3 Fase 3: Desarrollo e integración de escenarios de ciberataques basados en MITRE ATT&CK 33
3.3.4 Fase 4: Evaluación de la Plataforma 34
3.4 Consideraciones bioéticas 36
4 CAPÍTULO IV – RESULTADOS Y DISCUSIÓN 37
4.1 Resultados según objetivos 37
4.1.1 Objetivo 1: 37
4.1.2 Objetivo 2: 38
4.1.3 Objetivo 3 39
4.1.4 Objetivo 4: Evaluar la efectividad y utilidad del entorno 40
5 CONCLUSIONES 48
6 RECOMENDACIONES 50

7 BIBLIOGRAFÍA 51

8 ANEXOS 1

8.1 Anexos Técnicos del Entorno Cyber Range UTN 2

Anexo A. Matriz de análisis documental 2

Anexo B. Manual técnico de implementación de la plataforma Cyber Range UTN 5

Anexo C. Matriz de escenarios basados en MITRE ATT&CK 16

Anexo D. Guía de creación de escenarios CTF. 18

8.2 Anexos de Evaluación del Entorno Cyber Range UTN 28

Anexo E. Encuesta previa al entrenamiento 28

Anexo F. Tabulación de resultados de la encuesta previa 31

Anexo G. Encuesta posterior al entrenamiento 36

Anexo H. Tabulación de resultados de la encuesta posterior 38

Anexo I. Informe de participantes en el entrenamiento 42

Anexo J. Manuales de resolución de los retos 1 y 2 47

Anexo K. Registro fotográfico del Entrenamiento 56

ÍNDICE DE TABLAS

Tabla 1 Tipos de ataques informáticos 10

Tabla 2 Niveles de severidad de una vulnerabilidad 13

Tabla 3 Métodos convencionales de enseñanza de ciberseguridad 16

Tabla 4 Objetivo del entrenamiento cibernético (intención de desempeño) 17

Tabla 5 Objetivo del entrenamiento cibernético (Efectos y resultados esperados) . 18

Tabla 6 Escenarios MITRE ATT&CK implementados 39

Tabla 7 Resultados entrenamiento cibernético 40

Tabla 8 *Métricas de rendimiento - Servidor Proxmox CITEL* 41

Tabla 9 Nivel de conocimientos y experiencia previa antes y después del entrenamiento 42

Tabla 10 Expectativas de aprendizaje antes del entrenamiento y resultados obtenidos después 43

Tabla 11 Facilidad de uso de la plataforma CTFd 45

Tabla 12 Conciencia sobre amenazas cibernéticas antes y después del entrenamiento. 45

Tabla 13 Percepción general del entrenamiento y recomendaciones 46

Tabla 14 Matriz de análisis documental 2

Tabla 15 Máquinas creadas 6

Tabla 16 Escenarios basados en MITRE ATT&CK 16

Tabla 17 Tabulación pregunta 4 - Encuesta previa a entrenamiento 32

Tabla 18 Tabulación pregunta 6 - Encuesta previa a entrenamiento 33

Tabla 19 Tabulación pregunta 9 - Encuesta previa a entrenamiento 35

Tabla 20 Tabulación pregunta 4 - Encuesta posterior al entrenamiento 39

Tabla 21 Tabulación pregunta 6 - Encuesta posterior al entrenamiento 40

ÍNDICE DE FIGURAS

Figura 1 Fases de un ciberataque..... 11

Figura 2 Taxonomía Cyber Range..... 20

Figura 3 Infraestructura guía de un Cyber Range 21

Figura 4 Proceso de investigación por fases..... 30

Figura 5 Arquitectura de Cyber Range UTN 32

Figura 6 Características servidor Proxmox Local 6

Figura 7 Creación máquina vulnerable 1..... 8

Figura 8 Asignación de imagen ISO a máquina vulnerable 1 8

Figura 9 Asignación de almacenamiento en máquina vulnerable 1 9

Figura 10 Asignación de CPU a máquina vulnerable 1 9

Figura 11 Asignación de RAM a máquina Reto 1..... 10

Figura 12 Sistema operativo para máquina Kali Linux..... 10

Figura 13 Asignación de almacenamiento para máquina Kali Linux 11

Figura 14 Vista general del entorno Proxmox CITEL..... 11

Figura 15 Página de configuración de CTFd..... 12

Figura 16 Nombre y descripción del Entrenamiento..... 13

Figura 17 Inicio-Fin Cyber Range UTN 13

Figura 18 Página de edición de logo 14

Figura 19 Página de inicio para participantes..... 14

Figura 20 Configuración de equipos 15

Figura 21 Arquitectura Escenario 1..... 19

Figura 22 Creación de usuario Santiago - Reto1..... 19

Figura 23 Creación usuario Jairo..... 20

Figura 24 Permisos a usuario para acceder por ssh 20

Figura 25 Instalación de servidor Apache 21

Figura 26 Código HTML de página web 21

Figura 27 Configuración de mysql 22

Figura 28 Base de datos creada 22

Figura 29 Reglas de firewall implementadas 23

Figura 30 Arquitectura Escenario 2 24

Figura 31 Configuración de servidor FTP 24

Figura 32 Reglas de Firewall Escenario 2 25

Figura 33 Pantalla de administración con retos CTF creados 26

Figura 34 Vista del reto desde perspectiva de participante 26

Figura 35 Gráfica pregunta 1 – Encuesta previa a entrenamiento 31

Figura 36 Gráfica pregunta 2 - Encuesta previa a entrenamiento 31

Figura 37 Gráfica pregunta 3 - Encuesta previa a entrenamiento 32

Figura 38 Gráfica pregunta 5 - Encuesta previa a entrenamiento 33

Figura 39 Gráfica pregunta 7 - Encuesta previa a entrenamiento 34

Figura 40 Gráfica pregunta 8 - Encuesta previa a entrenamiento 34

Figura 41 Gráfica pregunta 10 - Encuesta previa a entrenamiento 35

Figura 42 Gráfica pregunta 1 - Encuesta posterior al entrenamiento 38

Figura 43 Gráfica pregunta 2 - Encuesta posterior al entrenamiento 38

Figura 44 Gráfica pregunta 3 - Encuesta posterior al entrenamiento 39

Figura 45 Gráfica pregunta 5 - Encuesta posterior al entrenamiento 40

Figura 46 Gráfica pregunta 7 - Encuesta posterior al entrenamiento 41

Figura 47 Desafíos de Reto 1 48

Figura 48 Primer desafío (Reconociendo al enemigo) 48

Figura 49 Reconocimiento IP de máquina vulnerable 49

Figura 50 Servicios activos en máquina vulnerable 1 49

Figura 51 Segundo desafío (La caja secreta) 50

Figura 52 Página web de la máquina vulnerable 1 50

Figura 53 Código fuente de la página web 51

Figura 54 Tercer desafío "Raíces ocultas" 51

Figura 55 Desafío Reto 2 54

Figura 56 Acceso a servicio ftp 55

Figura 57 Flag reto 2 55

Figura 58 Exposición Cyber Range - CTF UTN 56

Figura 59 Equipo 1 – archlovers 56

Figura 60 Equipo 2 - error 404 57

Figura 61 Equipo 3 – CrushesUTN 57

Figura 62 Equipo 4 – secNet 58

Figura 63 Estudiantes usando la plataforma CTFd 58

Figura 64 Estudiantes realizando desafíos de seguridad informática 59

Figura 65 Grupo de participantes en Cyber Range UTN 59

RESUMEN

El desarrollo de la seguridad informática en los últimos años ha generado una creciente necesidad de profesionales capacitados para responder a los diversos tipos de ataques cibernéticos. En este contexto, los entornos de entrenamiento cibernético han surgido como herramientas fundamentales para la formación práctica de la ciberseguridad, permitiendo a los participantes enfrentar escenarios realistas en un ambiente controlado. Una de las metodologías más efectivas dentro de estos escenarios es el Capture The Flag (CTF), que combina el aprendizaje teórico con la resolución de retos prácticos, fomentado el desarrollo de habilidades técnicas, pensamiento crítico y toma de decisiones.

El presente trabajo de investigación se enfoca en el diseño e implementación de un entorno de entrenamiento cibernético basado en la metodología CTF, dirigido a estudiantes de la carrera de Telecomunicaciones de la Universidad Técnica del Norte. Este entorno permite a los estudiantes practicar técnicas de ataque, utilizando escenarios alineados con el marco MITRE ATT&CK, que simulan amenazas reales.

Este entorno busca generar alternativas que contribuyan a la protección de las organizaciones frente a amenazas cibernéticas, fomentando la aplicación de los conocimientos teóricos llevados al mundo práctico. Los resultados del entrenamiento demostraron una mejora significativa en las habilidades de los estudiantes, confirmando la efectividad de esta metodología para el aprendizaje de seguridad informática.

Palabras clave: Seguridad informática, Capture The Flag (CTF), MITRE ATT&CK, ataques cibernéticos.

ABSTRACT

The development of cybersecurity in recent years has created a growing need for trained professionals capable of responding to various types of cyberattacks. In this context, cyber training environments have emerged as essential tools for practical training in cybersecurity, allowing participants to face realistic scenarios in a controlled environment. One of the most effective methodologies within these environments is Capture The Flag (CTF), which combines theoretical learning with practical challenges, fostering the development of technical skills and critical thinking.

This research focuses on the design and implementation of a cyber training environment based on the CTF methodology, aimed at students in the Telecommunications program at the Universidad Técnica del Norte. This environment allows participants to practice attack techniques using scenarios aligned with the MITRE ATT&CK framework, which simulates real-world cyber threats.

This training environment seeks to generate alternatives that contribute to protecting organizations against cyber threats, encouraging the application of acquired knowledge in real-world scenarios. The training results demonstrated a significant improvement in students' skills, confirming the effectiveness of this methodology for cybersecurity learning.

Keywords: Cybersecurity, Capture The Flag (CTF), MITRE ATT&CK, Cyberattacks

CAPÍTULO 1 - EL PROBLEMA DE INVESTIGACIÓN

1.1 Problema de investigación

Los avances actuales en Tecnologías de la Información y Comunicación (TIC) están transformando nuestra vida diaria, ofreciendo una amplia gama de aplicaciones que mejoran las actividades cotidianas. No obstante, este progreso también conlleva el riesgo de un aumento en los delitos cibernéticos (Wara et al., 2017).

Un ejemplo de evidencia contundente se encuentra en el reciente estudio llevado a cabo por Kaspersky, titulado "Panorama de Amenazas para América Latina", el cual analizó datos desde junio de 2022 hasta julio de 2023. Este estudio revela un preocupante aumento en la actividad delictiva en la región en relación con los ataques de malware dirigidos a ordenadores y dispositivos móviles, con un incremento del 617%. Asimismo, se observó un aumento del 50% en los intentos de ataques de phishing y troyanos bancarios. Los sectores gubernamentales y financieros emergen como los más afectados, junto con los usuarios de Internet en general. En un lapso de 12 meses, Kaspersky registró un total de 286 millones de bloqueos por intentos de phishing, lo que representa un aumento del 617% en comparación con el periodo anterior, con un promedio de 544 ataques por minuto (Kaspersky, 2023).

Por este aumento considerable de amenazas cibernéticas, la seguridad informática ha adquirido una relevancia crucial en el contexto de la vida cotidiana de las personas. Sin embargo, el afán constante de conectividad y el consumo desmedido de recursos en línea han propiciado una situación en la que la seguridad informática es relegada a un segundo plano. Esta tendencia, caracterizada por la falta de conciencia y el escaso interés en las medidas de protección cibernética, otorga a los ciberdelincuentes la oportunidad de explotar las vulnerabilidades existentes en los sistemas digitales (Rodríguez, 2023).

La relevancia de la seguridad informática reside en la formación de profesionales capaces de enfrentar los desafíos de los ataques cibernéticos, salvaguardando así la información crítica de organizaciones y personas. En este sentido, la enseñanza en este campo debe ser óptima; sin embargo, tradicionalmente se ha centrado en un enfoque predominantemente teórico. Este método educativo, basado en textos y conferencias, puede resultar pasivo para los estudiantes, limitando su comprensión y aplicación práctica de los conocimientos. Es fundamental encontrar un equilibrio entre la teoría y la práctica para asegurar una comprensión profunda de los conceptos y mejorar la calidad del aprendizaje. La integración de prácticas desempeña un papel crucial al permitir la validación de los conocimientos teóricos adquiridos y al potenciar la profesionalidad de los estudiantes en escenarios del mundo real (Wara et al., 2017).

En el contexto de la investigación, durante una entrevista con el MSc. Fabián Cuzme, profesor de Seguridad Informática en la carrera de Telecomunicaciones (CITEL) de la Universidad Técnica del Norte, se destacó el uso de diversos recursos para la enseñanza de esta disciplina. Entre estos recursos se encuentran entornos de simulación como GNS3, VMWare, VirtualBox, así como herramientas como Kali Linux, Metasploit y una variedad de sistemas operativos tanto de código abierto como propietarios. Estos recursos permiten a los estudiantes llevar a cabo las tareas y prácticas asignadas en la materia. Sin embargo, se identifica una carencia actual en la disponibilidad de una plataforma centralizada que facilite el acceso a los laboratorios virtuales.

En una propuesta presentada por (Heredia, 2019), se planteó el desarrollo de una infraestructura basada en Honeypots de alta interacción con el objetivo de enseñar seguridad informática dentro del marco de la carrera de Ingeniería en Telecomunicaciones (CITEL).

Sin embargo, debido a los cambios frecuentes en los servidores de la facultad, esta herramienta dejó de estar disponible para su uso.

Ante esta situación, se hace evidente la necesidad de adoptar enfoques de enseñanza dinámicos e interactivos que fomenten una comprensión significativa de los principios de seguridad informática. En esta investigación, se propone el uso del entorno conocido como Capture The Flag (CTF), el cual constituye un tipo de juego que involucra la seguridad de redes e información, siendo utilizado tanto como material de enseñanza y aprendizaje, así como una herramienta de evaluación en competiciones de seguridad informática. El CTF desafía a los participantes a pensar de manera creativa y a resolver una serie de problemas de complejidad variable. Estos problemas se presentan en forma de niveles, donde la resolución exitosa de cada desafío lleva a los participantes más cerca de completar el juego en su totalidad (Rodríguez, 2023).

1.2 Interrogantes de la Investigación

¿Cuáles son los principios y directrices más relevantes utilizados en la implementación actual de entornos seguros de Capture The Flag (CTF), según la literatura revisada?

¿Cuáles son las mejores prácticas y estándares de seguridad cibernética que deben ser considerados para implementar una infraestructura robusta y segura para el despliegue de la plataforma CTF?

¿Cómo pueden ser integrados de manera efectiva los escenarios de ciberataques basados en MITRE ATT&CK en la plataforma CTF, abarcando una variedad de tácticas y técnicas utilizadas por los adversarios en entornos reales?

¿Qué impacto tiene la plataforma CTF en la mejora de la conciencia y las habilidades en seguridad cibernética, tanto en términos cuantitativos como cualitativos, según los resultados de los estudios de caso y el análisis de métricas de rendimiento?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

Desarrollar un entorno seguro de Capture The Flag (CTF) con la integración de escenarios de ciberataques basados en MITRE ATT&CK, con el propósito de establecer una estrategia efectiva de prevención de ciberataques y proporcionar una plataforma robusta para la capacitación y evaluación de habilidades en seguridad cibernética en la Universidad Técnica del Norte.

1.3.2 Objetivos Específicos

Realizar una revisión bibliográfica sobre la implementación actual de entornos seguros de Capture The Flag (CTF), centrándose en los principios y directrices utilizados para garantizar su protección.

Implementar una infraestructura robusta y segura para el despliegue de la plataforma CTF, siguiendo mejores prácticas y estándares de seguridad cibernética.

Integrar escenarios de ciberataques basados en MITRE ATT&CK en la plataforma CTF, que abarquen diferentes tácticas y técnicas utilizadas por los adversarios en entornos reales.

Evaluar la efectividad y la utilidad de la plataforma CTF en la mejora de la conciencia y las habilidades en seguridad cibernética mediante la realización de estudios de caso y análisis de métricas de rendimiento, tanto cuantitativas como cualitativas.

1.4 Hipótesis de trabajo

Desarrollar un entorno seguro de Capture The Flag (CTF) con la integración de escenarios de ciberataques basados en MITRE ATT&CK, permitirá establecer una estrategia efectiva de prevención de ciberataques y proporcionar una plataforma robusta para la capacitación y evaluación de habilidades en seguridad cibernética en la Universidad Técnica del Norte.

1.5 Hipótesis alternativa

Desarrollar un entorno seguro de Capture The Flag (CTF) con la integración de escenarios de ciberataques basados en MITRE ATT&CK, no permitirá establecer una estrategia efectiva de prevención de ciberataques y proporcionar una plataforma robusta para la capacitación y evaluación de habilidades en seguridad cibernética en la Universidad Técnica del Norte.

1.6 Categorización de Variables

Variable independiente: Entorno seguro de Capture The Flag (CTF) con la integración de escenarios de ciberataques basados en MITRE ATT&CK.

Variable dependiente: Estrategia efectiva de prevención de ciberataques y plataforma robusta para la capacitación y evaluación de habilidades en seguridad cibernética en la Universidad Técnica del Norte.

1.7 Justificación

En un mundo cada vez más interconectado, el desarrollo de profesionales altamente capacitados en seguridad informática es fundamental. La protección de los sistemas informáticos contra amenazas cibernéticas se ha convertido en una prioridad tanto para individuos como para organizaciones. La presencia omnipresente de la tecnología digital en todos los aspectos de la vida moderna ha aumentado la vulnerabilidad a ataques y brechas de seguridad, lo que subraya la necesidad crítica de contar con expertos bien formados en esta área para salvaguardar la información y mantener la integridad de los sistemas.

Sin embargo, el aprendizaje efectivo de seguridad informática requiere no solo de la adquisición de conocimientos teóricos, sino también de la práctica activa y la resolución de problemas prácticos en entornos simulados. Los Capture The Flag (CTF) ofrecen precisamente esta oportunidad al proporcionar escenarios de juego que simulan situaciones reales de seguridad informática, donde los participantes pueden poner en práctica sus habilidades y conocimientos en un entorno controlado y seguro.

De esta manera, se tiene la intención de desarrollar e implementar el entorno Capture The Flag (CTF) como parte integral del programa académico para los estudiantes de la carrera de Ingeniería en Telecomunicaciones (CITEL) de la Universidad Técnica del Norte. Este enfoque proporcionará un ambiente educativo propicio para mejorar la comprensión y las habilidades en seguridad informática entre los estudiantes. El CTF permitirá a los participantes aplicar de manera práctica los conocimientos adquiridos, promoviendo así un aprendizaje activo y significativo en esta área crucial.

La introducción de un entorno de Capture The Flag (CTF) personalizado representa una herramienta invaluable para enriquecer la formación académica de los estudiantes de CITEL. Según lo expresado por el MSc. Jaime Michilena, Coordinador de dicha carrera, en una entrevista, esta iniciativa ofrece una oportunidad excelente para que los estudiantes exploren la seguridad informática de una manera innovadora. La metodología CTF resulta especialmente atractiva ya que permite a los estudiantes enfrentarse a desafíos prácticos relacionados con la seguridad informática.

Este proyecto proporcionará a los estudiantes la posibilidad de desarrollar habilidades prácticas y obtener experiencia directa en el ámbito de la ciberseguridad, preparándolos de manera más efectiva para afrontar los desafíos del mercado laboral actual. Además, la personalización del Entorno CTF permitirá adaptar los desafíos y escenarios de juego a las necesidades específicas y los intereses de los estudiantes de la carrera de CITEL, maximizando así su relevancia y efectividad como herramienta de aprendizaje.

El desarrollo de un entorno de Capture The Flag (CTF) contribuye directamente al objetivo 4 del Plan Nacional del Buen Vivir 2013-2017, que subraya la importancia de fortalecer las capacidades y habilidades de la ciudadanía. Al implementar un entorno CTF, se potenciarán los conocimientos en seguridad informática de los estudiantes, lo que se alinea estrechamente con la línea de investigación de la Universidad Técnica del Norte, centrada en el desarrollo, aplicación de software y seguridad cibernética. Este enfoque no solo enriquece la formación académica de los estudiantes, sino que también contribuye al fortalecimiento de la ciudadanía y al avance de la sociedad en su conjunto hacia un futuro más seguro y resiliente en el ámbito digital.

En resumen, el desarrollo de un Entorno CTF personalizado para los estudiantes de la Carrera de Ingeniería en Telecomunicaciones de la Universidad Técnica del Norte se justifica por su potencial para mejorar la calidad de la enseñanza en seguridad informática, proporcionando a los estudiantes una experiencia práctica y significativa que complementa su formación académica y los prepara para enfrentar los desafíos del mundo laboral en el campo de la seguridad informática.

CAPÍTULO II – MARCO REFERENCIAL

En este capítulo, se presentan los fundamentos teóricos relacionados con el diseño e implementación de un entorno seguro de entrenamiento cibernético con la modalidad de CTF. Además del marco legal, que muestra las normativas y regulaciones aplicables al desarrollo de este entorno, con base a la matriz MITRE ATT&CK.

2.1 Marco teórico

2.1.1 Seguridad informática

La ciencia que se encarga de establecer mecanismos para la protección o defensa de sistemas informáticos, redes de telecomunicaciones e información de posibles ataques maliciosos por parte de ciberdelincuentes (Urcuqui & Navarro Cadavid, 2022). Se podrían establecer tres principios de la seguridad informática que son fundamentales para hacer frente antes las amenazas cibernéticas, las cuales son cada vez más frecuentes. Dichos principios son:

Confidencialidad: Se basa a la protección de la información contra el acceso no autorizado. Un ejemplo de este principio sería la encriptación de datos sensibles para evitar que sean leídos por personas no autorizadas (Mata, 2024).

Integridad: Consiste en la protección de la información contra la modificación no autorizada. El uso de firmas digitales se podría identificar como un ejemplo de este principio, ya que permiten garantizar que los datos no hayan sido modificados desde su creación (Mata, 2024).

Disponibilidad: Establece la garantía de que la información esté disponible en cada momento para los usuarios autorizados. Por ejemplo, el uso de sistemas redundantes permite que los usuarios puedan acceder a su información incluso si el sistema principal se ve comprometido (Mata, 2024).

2.1.2 Ataques informáticos

(Urcuqui & Navarro Cadavid, 2022) Un ataque informático es un intento de acceder o dañar a un sistema informático mediante la implementación de métodos sobre una o más vulnerabilidades; dependiendo del contexto, un atacante puede usar varios tipos de ataques informáticos, como los mostrados en la Tabla 1 (Urcuqui & Navarro Cadavid, 2022).

Tabla 1

Tipos de ataques informáticos

Tipo	Características
Pasivo	El atacante no interactúa directamente con el objetivo, por ejemplo, el monitoreo del tráfico de red y flujos de datos que se transmiten en una red de computadoras.
Activo	Acciones que conllevan a la interrupción de la comunicación o servicios de un sistema.
Cercano	El atacante tiene una aproximación física al objetivo, por ejemplo, ataques de ingeniería social.
Explotación de privilegios	Personas con privilegios dentro de una organización forman parte del conjunto de atacantes; muy peligrosos debido a su capacidad de acceso al perímetro del objetivo.
Distribuido	El atacante altera hardware o software antes de su instalación o adquisición del usuario.

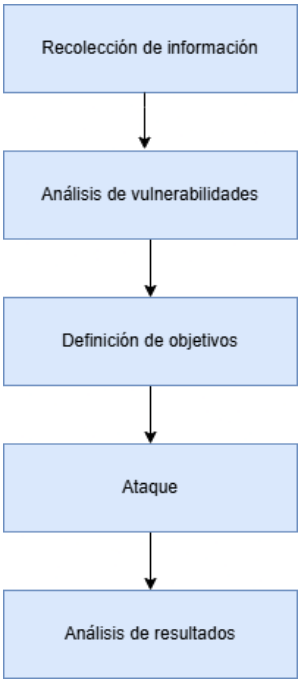
Nota. Adaptada de Tipos de ataques informáticos, (Urcuqui & Navarro Cadavid, 2022).

Fases de un ataque informático

Los ataques informáticos son cada vez más sofisticados, y los ciberdelincuentes utilizan una variedad de técnicas para explotar vulnerabilidades en los sistemas. Según Cuzme Rodríguez et al. (2018), una metodología de hacking ético bien estructurada puede ayudar a identificar y mitigar estas vulnerabilidades antes de que sean explotadas por ciberdelincuentes. La metodología propuesta por Cuzme Rodríguez et al. (2018) incluye fases como el reconocimiento, el escaneo, la explotación y la post-explotación, las cuales son fundamentales para entender como los atacantes operan en el mundo real (ver Figura 1).

Figura 1

Fases de un ciberataque



Nota. Adaptada de Fases de la metodología de Seguridad Ofensiva, (Cuzme-Rodríguez Fabiánand León-Gudiño, 2019)

2.1.3 Amenazas y vulnerabilidades

Una amenaza es un agente que pueda ocasionar daño. Existen amenazas que son naturales propias del ambiente como inundaciones, incendios, etc. Mientras que otras son de carácter humano siendo estas intencionadas o no intencionadas. Este tipo de amenazas pueden ser Estados, organizaciones criminales, empleados descontentos, usuarios descuidados o poco capacitados (Herrero Perez, 2022).

La detección de amenazas se las puede realizar mediante la implementación de sistemas de intrusiones. Según (Domínguez-Limaico Hernán and Nicolalde Quilca, 2023), los sistemas de detección de intrusos basados en redes neuronales artificiales (ANN) pueden mejorar significativamente la capacidad de identificar y responder a ataques en redes definidas por software (SDN). Este contexto es útil en entornos de ciberseguridad donde la velocidad y la precisión en la detección de amenazas son esenciales.

Una vulnerabilidad por otra parte se considera una falla o debilidad que puede ser usada para generar daño de manera voluntaria o involuntaria. Estas vulnerabilidades pueden estar en el desarrollo de software o en el diseño de Hardware, malas configuraciones de red o un mal diseño de la arquitectura de sistemas (Herrero Perez, 2022).

El riesgo dentro de seguridad informática se refiere al grado de probabilidad que tiene una amenaza de explotar o atacar a una vulnerabilidad. Un ataque es el medio por el cual la amenaza materializa su riesgo. Para ello usará un vector de ataque, que es el camino para lograr sus objetivos (Herrero Perez, 2022).

Tipos de vulnerabilidades. Es complejo determinar una clasificación de vulnerabilidades, sin embargo, se establecen los siguientes criterios de clasificación:

Vulnerabilidades según su severidad. Mediante el estándar *Common Vulnerability Scoring System (CVSS)* se puede llevar una medida para establecer el grado de severidad de una vulnerabilidad. Los aspectos que toma en cuenta este estándar son: el vector de acceso, la complejidad de la explotación, el nivel de autenticación que debe tener el atacante en el sistema, el impacto sobre la confidencialidad, integridad y la disponibilidad. Una vez evaluados dichos parámetros se establece una puntuación de 0 a 10 puntos (Herrero Perez, 2022). Los grados de severidad en base a la puntuación obtenida se pueden observar en la Tabla 2:

Tabla 2

Niveles de severidad de una vulnerabilidad

Nivel de severidad	Puntuación
Nula	0
Baja	0,1 - 3,9
Media	4 - 6,9
Alta	7,0 – 8,9
Crítica	9 - 10

Nota. Adaptado de (Herrero Perez, 2022).

Vulnerabilidades según antigüedad. En esta clasificación se toma en cuenta el tiempo desde que las vulnerabilidades han sido descubiertas, entre ellas se tiene:

- **De día cero (zero-day):** En este tipo no existen parches de seguridad que las puedan solucionar. Corresponden un tipo de vulnerabilidad potencialmente muy dañina, debido a que en muchas ocasiones el fabricante o desarrollador desconoce dicha brecha de seguridad, con lo cual el atacante puede ocasionar daños considerables (Herrero Perez, 2022).
- **De día uno (one-day):** En este caso el desarrollador o fabricante reconoce la vulnerabilidad y crea los parches de seguridad correspondientes, sin embargo, estos parches en determinados ambientes no se aplican de manera inmediata, sobre todo por temas de procesos relacionados con las políticas de organizaciones. Esta ventana de tiempo es usada por los atacantes, quienes conocen la vulnerabilidad (Herrero Perez, 2022).
- **Antiguas:** Este tipo se caracteriza por que ya cuentan con los parches de seguridad necesarios para impedir cualquier tipo de daño, e incluso existen *exploits* públicos para aprovechar estas vulnerabilidades, sin embargo, existen organizaciones que usan software desactualizado, lo que permite a los atacantes usar dichos *exploits* para realizar ataques (Herrero Perez, 2022).

Tipos de amenazas. Para esta clasificación, se puede dejar de lado a las amenazas de tipo natural, ya que lo más recomendable para mitigar su impacto serían establecer sistemas de redundancia. Dicho esto, la clasificación que se propone es la siguiente:

Poco estructuradas. La explotación se basa en vulnerabilidades que están documentadas, este tipo de amenazas es efectuada por una persona o en medida puede por un grupo pequeño que no pertenecen a ninguna organización ni cuentan con financiamiento externo. Sus propósitos pueden ser por curiosidad, probar sus habilidades y algunos casos por algún beneficio económico (Herrero Perez, 2022).

Estructuradas. En este caso son grupos de personas que están organizados, cuenta con tiempo y planificación para efectuar sus ataques, de igual forma pueden tener algún de financiamiento. Generalmente los ataques se realizan contra objetivos específicos y previamente establecidos. Emplean tiempo para obtener toda la información posible sobre el objetivo y usan vulnerabilidades no documentadas para realizar la explotación (Herrero Perez, 2022).

Muy estructuradas. Cuando los objetivos de ataque son mucho más grandes e importantes como, organizaciones gubernamentales, empresas estratégicas, quienes realizan estos ataques son entidades profesionales, que cuenta con financiación, recursos, materiales, herramientas, tiempo para llevar a cabo sus ataques (Herrero Perez, 2022).

2.1.4 Aprendizaje de Ciberseguridad

En base a los diferentes tipos de amenazas y vulnerabilidades que existen en el campo del medio digital o tecnológico, es crucial un correcto aprendizaje sobre la seguridad informática, con ello se busca formar habilidades en este campo para poder hacer frente no solo a hackers individuales o inexpertos sino también contra equipos coordinados de hackers que pueden o no tener apoyo de Estados (Shin et al., 2024). Los métodos habituales para enseñar habilidades en ciberseguridad se observan en la Tabla 3:

Tabla 3

Métodos convencionales de enseñanza de ciberseguridad

Métodos	Características
Conferencias o clases teóricas	Se explican conceptos, técnicas y fundamentos de seguridad.
Tareas o asignaciones	Ejercicios prácticos que permiten a los estudiantes aplicar lo aprendido en ambientes controlados.
Seminarios	Presentaciones en dónde se discuten tópicos específicos de seguridad informática.
Laboratorios prácticos	Entornos controlados donde los estudiantes aplican sus conocimientos en ambientes reales.

Nota. Adaptada de, (Shin et al., 2024).

Dentro de los métodos prácticos, se incluyen:

- **Competiciones:** Eventos donde quienes participan intentan resolver desafíos de ciberseguridad, por lo regular al capturar una bandera (Capture the Flag, CTF)
- **Desafíos:** Problemas específicos para poner a prueba las habilidades y conocimientos en la resolución de problemas.
- **Ejercicios:** Escenarios que representan situaciones reales de ciberseguridad, por ejemplo:
    - **Ejercicios de Red Team vs Blue Team:** Un equipo simula ataques (Red Team) y el otro (Blue Team) genera mecanismos de defensa contra esos ataques.

- **Simulaciones de incidentes:** Prácticas que imitan respuestas a brechas de seguridad.
- **Entrenamientos en cyber ranges:** Son entornos virtualizados que permiten practicar infraestructuras similares a las reales.

La capacidad de respuesta de un profesional ante situaciones de amenazas cibernéticas se ve mejorada gracias a la implementación de estos métodos en su formación, preparándolo para enfrentar desafíos tanto en al ámbito individual como en equipos coordinados (Shin et al., 2024).

2.1.5 Entrenamiento Cibernético

El entrenamiento cibernético básicamente consiste en aprender conocimientos y habilidades por medio de la educación y la práctica. Si se juntan estos dos principios el estudiante puede perfeccionar sus habilidades y conocimientos. El entrenamiento se puede llevar a cabo con diferentes propósitos, en este caso con dos perspectivas: la intención de desempeño y el efecto o resultado esperando. Sobre la intención de desempeño, se pueden identificar cinco tipos, explicados en la Tabla 4.

Tabla 4

Objetivo del entrenamiento cibernético (intención de desempeño)

Aspecto	Objetivo	Descripción
Intención de desempeño	Identificación	Identificar vulnerabilidades, fallas en procedimientos y procesos de intercambio de información.
	Prueba de mecanismos y/o procedimientos	Evaluación de herramientas, prácticas, procedimientos para asegurar que los sistemas existen sean los adecuados para su propósito, o que los nuevos

	sistemas que se desarrollen funcionen como se espera.
Ejercitación de mecanismos y/o procedimientos	Ejercicios usando mecanismos y procedimientos establecidos para asegurar la preparación en caso de un incidente real.
Incremento de la comunicación y cooperación.	Identifica canales de comunicación entre actores con diferentes prioridades en la práctica, como organizaciones del sector público y privado o marcos nacionales de ciberseguridad.
Desarrollo de políticas y procedimientos	A través del entrenamiento se busca identificar fallas en las políticas de seguridad informática y luego desarrollar políticas adecuadas.

Nota. Tomada de (Shin et al., 2024).

Con respecto al otro propósito del entrenamiento cibernético, el cual es efectos y resultados esperados puede categorizarse como se muestra en la Tabla 5. Estas categorías incluyen:

Tabla 5

Objetivo del entrenamiento cibernético (Efectos y resultados esperados)

Aspecto	Objetivo	Descripción
Efectos y resultados esperados	Concienciación	Introducir la ciberseguridad a individuos generales (participantes) para crear conciencia.
	Habilidades técnicas	Proveer habilidades técnicas a quienes necesiten realizar procedimientos específicos relacionados con el manejo de incidentes cibernéticos.

Habilidades no técnicas	Adquirir habilidades no técnicas como cooperación, comunicación y toma de decisiones formando una capacidad integral de gestión de ciber incidentes.
Resiliencia	Asegurar un alto nivel de resiliencia y capacidad de recuperación por medio de la evaluación de la capacidad de la organización para adaptarse a situaciones impredecibles.

Nota. Tomada de (Shin et al., 2024).

Componentes del entrenamiento cibernético

El entrenamiento cibernético requiere un cyber range (centro de entrenamiento cibernético) para llevarse a cabo. Un cyber range simula un entorno de red y proporciona escenarios de ataque o defensa en los recursos de dicha infraestructura (ya sea en el ciberespacio real o un ambiente virtual), dotando de las condiciones necesarias para que los participantes realicen el entrenamiento cibernético(Shin et al., 2024).

Estos entornos están diseñados para ser realistas, permitiendo a los usuarios interactuar con sistemas y redes que replican un entorno empresarial o gubernamental real. Los componentes de un entrenamiento cibernético pueden ser categorizados en dos fases, Preparación y ejecución. La fase de preparación consiste en el Entorno y el Escenario, mientras que la fase de ejecución se refiere a la Operación, que es el entrenamiento cibernético propiamente dicho (Shin et al., 2024).

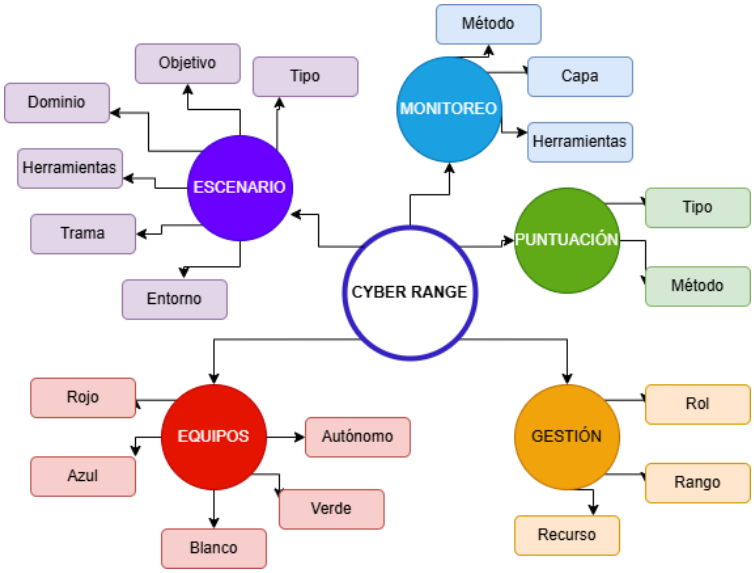
Entorno de Entrenamiento Cibernético. Un cyber range es una plataforma interactiva y simulada que replica redes, sistemas, herramientas y aplicaciones. Ofrece un entorno seguro y legal para adquirir habilidades prácticas en ciberseguridad. En los últimos

tiempos debido a problemas relacionados con espacio físico o costos, los entornos de entrenamiento cibernético se han implementado mediante la tecnología de virtualización (Shin et al., 2024).

Yamin et al., (2020) propone una taxonomía para clasificar a los elementos que un cyber range debería tener, tal como se muestra en la Figura 2.

Figura 2

Taxonomía Cyber Range



Nota. Adaptada de Taxonomía Cyber Range de, (Yamin et al., 2020)

Los cyber ranges pueden dividirse en las siguientes áreas:

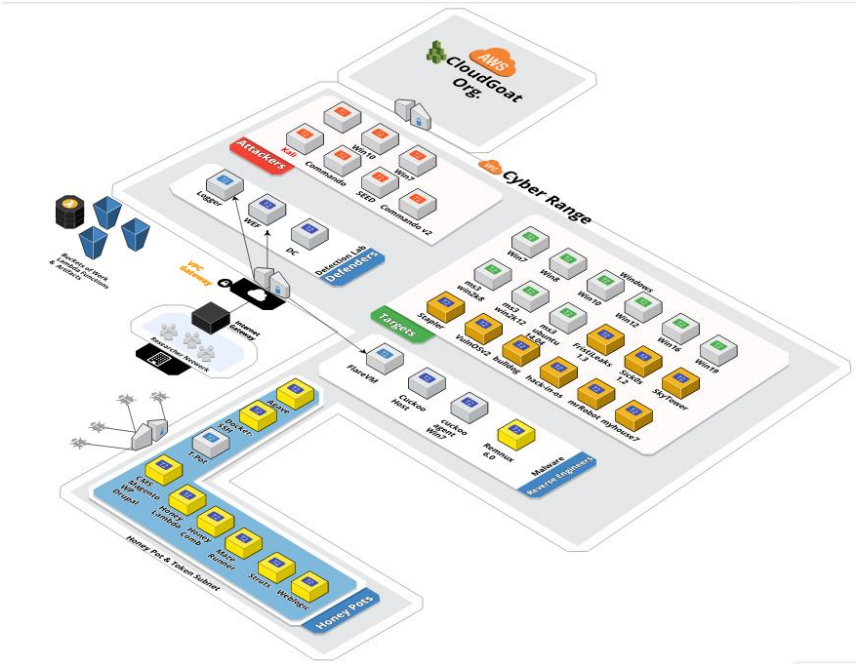
- **Área de Gestión:** Responsable de gestionar los sistemas para operar el cyber range, los participantes, el acceso a la interfaz web, los escenarios de entrenamiento, etc. Incluye sistemas de gestión, base de datos, monitoreo en tiempo real, seguridad preventiva, puntuación (Shin et al., 2024).

- **Área Blanca:** Simulas sitios web y usuarios en la red de entrenamiento, es decir, genera tráfico normal hacia el área de defensa para brindar un entorno de análisis para eventos cibernéticos reales (Shin et al., 2024).
- **Área de Ataque:** Simula el entorno de ataque donde los usuarios realizan sus técnicas ofensivas.
- **Área de Defensa:** Representa el área que los participantes deben proteger.

La Figura 3, muestra un ejemplo de un entorno o infraestructura de un cyber range.

Figura 3

Infraestructura guía de un Cyber Range



Nota. Tomada de (Long, 2020)

Escenario de Entrenamiento Cibernético. Es el contenido que permite realizar un ataque o una defensa dentro del entorno de un cyber range. Los escenarios se construyen usando sistemas vulnerables, y además se pueden considerar como un conjunto de tareas que los usuarios deben realizar, ya sea en formato de resolución de problemas o como ejercicios prácticos (Shin et al., 2024).

La creación de escenarios realistas y adaptados al entorno objetivo es fundamental para desarrollar en los participantes habilidades prácticas y con ello puedan afrontar amenazas cibernéticas reales. Existen dos tipos principales de escenarios de ejercicios:

- **Capture the Flag (CTF):** Se enfoca en identificar vulnerabilidades en los sistemas, realizar ataques y proporcionar una bandera como respuesta.
- **Live-Fire:** Este método se enfoca en la realización de ciberataques y defensa en tiempo real, esta metodología permite integrar escenarios altamente realistas.

Ambos métodos son cruciales para el entrenamiento cibernético, el estilo Jeopardy CTF brinda la capacidad de resolución de problemas y pensamiento crítico, mientras que el estilo Live-Fire proporciona una experiencia práctica en entornos reales, generando en los participantes, habilidades para responder de manera efectiva ante ciberataques en el mundo real (Shin et al., 2024).

Operación de Entrenamiento Cibernético. Para operar un entorno de entrenamiento cibernético, se necesita un espacio físico de tamaño y estabilidad adecuados, así como de equipamiento técnico como servidores, switches, routers y redes. Por otra parte, también se necesita software para operar el cyber range, junto con la configuración de red, servidores y

seguridad de los sistemas, reforzada para soportar la simulación de diversos escenarios de hacking y ciberataques (Shin et al., 2024).

Para el mantenimiento y operaciones es necesario contar entrenadores especiales (hackers de sombrero blanco) quienes pueden proveer tips o conocimientos cuando son requeridos. Un sistema de entrenamiento debe ser establecido para organizar el currículo educativo dependiendo de la situación y el nivel de complejidad, proporcionando varios programas de entrenamiento y escenarios que permiten a los participantes ganar experiencia ante situaciones reales de ciberataque. Es esencial contar con un sistema de seguimiento y evaluación del progreso de los usuarios para medir su desempeño y generar informes que permitan la mejora del entorno (Shin et al., 2024).

Los participantes suelen ser categorizados dentro de equipos como el rojo, azul, verde y blanco, cada uno de estos equipos tiene su respectivo rol asignado:

- **Equipo rojo:** Encargados de realizar los ciberataques.
- **Equipo azul:** Defiende al sistema de los ataques del equipo rojo.
- **Equipo verde:** Su función es dar mantenimiento a la infraestructura del cyber range.
- **Equito blanco:** Actúa como moderador o juez, supervisando el ejercicio y asegurando que se respeten las reglas.

Capture the Flag (CTF)

El concepto proviene o está relacionado con el ámbito militar, en dónde diferentes equipos competían por acceder a la bandera de su adversario concluyendo así el evento. En el campo de seguridad de informática el primer registro que se tiene sobre un CTF fue en la convención de hacking DEF CON, llevada a cabo en Estados Unidos en 1993. Este evento

marcó un punto de inicio en la aplicación de herramientas educativas en el campo de ciberseguridad (Tejeda Alcalde, 2025).

Desde ese momento los CTF tomaron un protagonismo en las instituciones educativas, ya que permitía poner a prueba las habilidades tanto de estudiantes como especialistas. En la actualidad se consideran una herramienta de formación de seguridad informática, ofreciendo la oportunidad de practicar habilidades como el reconocimiento de redes, análisis de vulnerabilidades, phishing o escalada de privilegios. Esto permite que sus usuarios desarrollen competencias que los prepara para afrontar desafíos de ciberataques reales (Tejeda Alcalde, 2025).

Tipos de CTF. Se pueden identificar tres tipos, El más común se denomina Jeopardy, en dónde los desafíos se clasifican en diferentes áreas como criptografía, explotación web, análisis forense, explotación binaria, ingeniería inversa, etc. Los participantes reciben puntos al resolver los retos propuestos mediante la obtención de una bandera. Otro tipo de CTF es el ataque-defensa, en este participan dos equipos, cada uno de ellos intenta atacar los sistemas del otro y al mismo tiempo intentan proteger sus propios recursos. Finalmente, se puede mencionar al CTF mixto en los cuales se combinan las funcionalidades tanto del Jeopardy como del ataque-defensa (Tejeda Alcalde, 2025).

2.1.6 MITRE ATT&CK Framework

MITRE ATT&CK es un marco de conocimiento mundialmente accesible que describe las técnicas, tácticas y procedimientos (TTP) utilizados por adversarios en ciberataques. Este marco desarrollado por la corporación MITRE, se basa en observaciones del mundo real y se usa como base para la creación de modelos de amenazas, metodologías de defensa y herramientas de ciberseguridad (MITRE, 2025).

ATT&CK se organiza en matrices que cubren diferentes entornos, como Enterprise, Mobile, ICS (Industrial Control Systems), lo que lo convierte en una herramienta importante para la prevención, detección y respuesta a ciberataques (Strom et al., 2018).

Componentes

El marco ATT&CK se compone de tres elementos principales:

- ***Tácticas:*** Representan el "Porqué" de una técnica. Es el objetivo del adversario, el motivo de realizar una acción. Por ejemplo, un ciber atacante puede querer obtener acceso a credenciales (MITRE, 2025).
- ***Técnicas:*** Describen los métodos específicos que los adversarios usan para lograr sus objetivos tácticos. Por ejemplo, el uso de phishing para obtener acceso inicial o el uso de PowerShell para ejecutar comandos maliciosos (Strom et al., 2018).
- ***Procedimientos:*** Son ejemplos concretos de cómo los adversarios implementan técnicas en ataques reales. Estos procedimientos se derivan de informes de inteligencia de amenazas y análisis de incidentes (Strom et al., 2018).

Relevancia en Ciberseguridad

MITRE ATT&CK se ha convertido en un estándar en el campo de la seguridad informática debido a su enfoque práctico y basado en observaciones reales. Algunas de sus aplicaciones más relevantes incluyen:

- ***Detección y análisis.*** ATT&CK permite que los grupos de seguridad puedan desarrollar reglas de detección y análisis en función de técnicas conocidas, lo

que fortalece su capacidad para reconocer actividades maliciosas (Strom et al., 2018).

- ***Emulación de adversarios.*** El marco se emplea para replicar las técnicas de adversarios identificados, permitiendo que las organizaciones evalúen y optimicen sus estrategias de defensa (MITRE, 2025).
- ***Inteligencia de amenazas.*** ATT&CK ofrece un marco unificado para comunicar y difundir información sobre amenazas, promoviendo la colaboración entre diferentes organizaciones (Strom et al., 2018).

Integración en entornos CTF

Los entornos Capture the Flag (CTF) son competencias de seguridad informática en dónde se simulan escenarios de ataques y defensa. La integración de MITRE ATT&CK en estos entornos permite:

- ***Crear Escenarios Reales.*** Al basar los desafíos en técnicas y tácticas de ATT&CK, los participantes enfrentan situaciones que reflejan amenazas del mundo real (MITRE, 2025).
- ***Mejorar Habilidades Prácticas.*** Los participantes pueden aprender a detectar, responder y mitigar ataques usando herramientas y metodologías alineadas al marco de ATT&CK (Strom et al., 2018).
- ***Fomentar la Prevención.*** Al entender como proceden los adversarios al momento de realizar ataques, los equipos pueden implementar medidas de protección a sus sistemas para prevenir o mitigar ataques informáticos (Strom et al., 2018).

2.2 Marco legal

El presente marco legal establece las normativas y regulaciones aplicables al desarrollo de un entorno seguro Capture The Flag (CTF), con base en la matriz MITRE ATT&CK, como estrategia para la enseñanza de ciberseguridad en la Universidad Técnica del Norte. Este estudio considera aspectos relacionados con la ciberseguridad, protección de datos y el uso de tecnologías en la educación, asegurando el cumplimiento de las disposiciones nacionales pertinentes.

2.2.1 Legislación Nacional Aplicable

El Estado Ecuatoriano cuenta con leyes que regulan la seguridad informática y la protección de datos personales. En ese sentido, las siguientes leyes son relevantes para el desarrollo de esta investigación.

Código Orgánico Integral Penal (COIP)

El COIP establece sanciones para delitos informáticos, garantizando la integridad de los sistemas tecnológicos en Ecuador. En concreto, el Artículo 232 menciona que:

"La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años, según el Artículo 232 del Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014)"

En este contexto, se garantiza que el entorno CTF será usando netamente exclusivamente con fines académicos y dentro de un laboratorio seguro, evitando cualquier uso indebido que pueda interpretarse como acceso no autorizado a sistemas informáticos externos.

Ley Orgánica de Protección de Datos Personales (LOPDP)

Esta ley regula el tratamiento de los datos personales en Ecuador y enmarca principios como la licitud, transparencia, confidencialidad y seguridad. El Artículo 8 establece que "Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo, Ley Orgánica de Protección de Datos Personales, (Asamblea Nacional, 2021)"

Debido a que el entorno CTF podría recopilar información sobre el desempeño de los participantes, se garantizará el anonimato de los datos y el cumplimiento de la LOPDP, protegiendo la identidad de los estudiantes.

Ley Orgánica de Educación Intercultural (LOEI)

La LOEI regula la educación en Ecuador y establece el uso de nuevas tecnologías como parte del aprendizaje. Según el Artículo 6 de la Ley Orgánica de Educación Intercultural (Asamblea Nacional del Ecuador, 2011).

"El Estado promoverá el acceso y uso de tecnologías digitales como herramienta de apoyo en la enseñanza y aprendizaje en todos los niveles educativos".

El desarrollo del entorno CTF se alinea con este principio, ya que busca el aprendizaje de ciberseguridad mediante una metodología interactiva y práctica, fortaleciendo las competencias en seguridad informática de los estudiantes.

CAPÍTULO III - MARCO METODOLÓGICO

En este capítulo se describe el enfoque metodológico adoptado para el desarrollo de esta investigación. Se detallan el tipo y nivel de investigación, el enfoque utilizado, los métodos aplicados para cada objetivo específico, así como las técnicas e instrumentos empleados para la recolección y análisis de datos. La metodología ha sido seleccionada con el fin de garantizar un desarrollo riguroso y coherente del entorno seguro Capture The Flag (CTF), integrando escenarios basados en la matriz MITRE ATT&CK y evaluando su efectividad en el fortalecimiento de habilidades de ciberseguridad.

3.1 Descripción del área de estudio / Descripción del grupo de estudio

El estudio se realizó en la Universidad Técnica del Norte, específicamente en el laboratorio de Fibra Óptica de la carrera de Ingeniería en Telecomunicaciones (CITEL) de la Facultad de Ingeniería en Ciencias Aplicadas (FICA). Los participantes fueron nueve estudiantes de CITEL, seleccionados mediante muestreo no probabilístico por conveniencia. Estos estudiantes cursaban asignaturas relacionadas con redes, seguridad informática y tecnologías de la información, lo que garantizó una base mínima de conocimientos para interactuar con el entorno propuesto.

3.2 Enfoque y tipo de investigación

La investigación se basó en un enfoque mixto, al combinar tanto métodos cuantitativos como cualitativos para obtener una compresión adecuada e integral del impacto del entorno CTF. En el componente cualitativo, se realizaron encuestas a grupos focales de estudiantes para identificar sus percepciones sobre el entorno CTF. En el componente cuantitativo, se recopilaron datos y métricas en la plataforma CTFd, incluyendo el número de participantes que lograron con éxito un desafío y el tiempo de resolución. Asimismo, se

registraron métricas de rendimiento del servidor que aloja el entorno. Además, el enfoque exploratorio permitió identificar las necesidades de los estudiantes en cuanto a formación en prácticas en ciberseguridad.

3.3 Procedimiento de investigación

El proceso de investigación se organizó en cuatro fases, alineadas con los cuatro objetivos específicos establecidos, como se puede observar en la Figura 4.

Figura 4

Proceso de investigación por fases

Nota. Figura elaborada por el autor

3.3.1 Fase 1: Revisión bibliográfica.

Se realizó una búsqueda sistemática de literatura en bases de datos académicas como IEEE Xplore, Scopus y otras fuentes especializadas, con el objetivo de identificar estudios relacionados con entornos Capture The Flag (CTF), laboratorios de ciberseguridad (Cyber ranges) y metodologías de formación práctica en seguridad informática. Para el análisis de los documentos seleccionados, se aplicó una matriz de análisis documental que permitió sintetizar los principios, enfoques pedagógicos y directrices comunes en implementaciones similares (ver Anexo A). Esta fase sentó las bases teóricas para el diseño del entorno propuesto.

3.3.2 Fase 2: Diseño e implementación de la infraestructura CTF

Durante esta fase se llevó a cabo el diseño y la implementación del entorno virtualizado necesario para ejecutar el Cyber Range UTN. Esta infraestructura fue diseñada considerando las limitaciones de hardware del servidor institucional (Dell EMC PowerEdge R750xs), debido a que en él se usan otras infraestructuras virtualizadas.

La solución se basó en una arquitectura distribuida y segmentada, compuesta por dos servidores independientes que interactúan mediante la red institucional EDUROAM UTN:

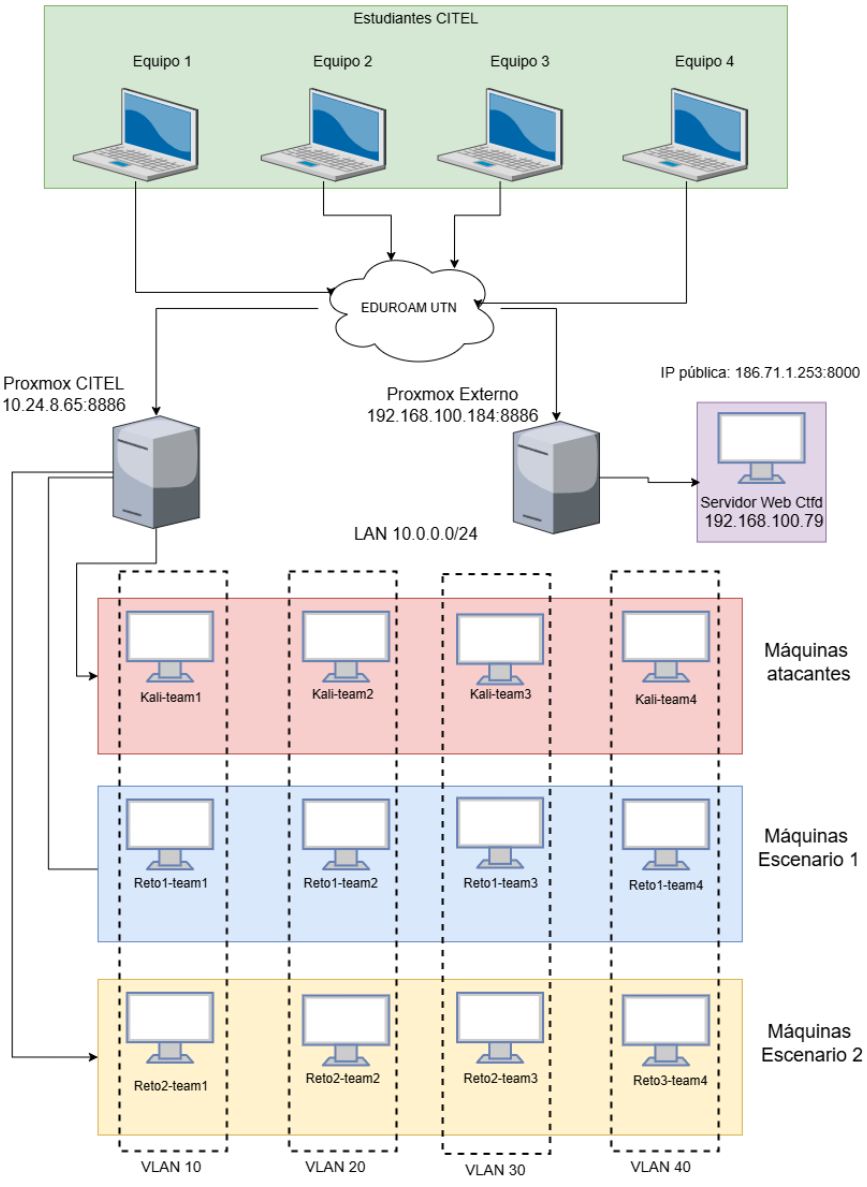
- **Servidor Proxmox CITEL:** Aloja las máquinas virtuales utilizadas en los retos prácticos, incluyendo tanto máquinas atacantes (Kali Linux) como máquinas vulnerables. La red interna está segmentada mediante VLANs para aislar el entorno de cada equipo de estudiantes, garantizando así que los grupos trabajen de manera independiente y segura.
- **Servidor Proxmox Local (externo):** Hospeda la plataforma CTFd, utilizada para la gestión de usuarios, retos y puntuaciones. Se decidió aislar esta plataforma del entorno de prácticas para proteger su integridad y asegurar su accesibilidad a través de una dirección IP pública (http://186.71.1.253:8000).

Esta configuración permitió distribuir eficientemente la carga de procesamiento y mantener una separación lógica entre la administración del entorno y la ejecución de los retos. Además, se asignaron recursos mínimos a las máquinas virtuales con el objetivo de no afectar el rendimiento del servidor institucional, el cual se utiliza simultáneamente en otras actividades académicas.

La Figura 5 presenta una vista general de la arquitectura del entorno, detallando la ubicación de los servidores, la segmentación de máquinas virtuales por equipos, y la conexión de los estudiantes desde sus estaciones a través de la red institucional.

Figura 5

Arquitectura de Cyber Range UTN



Nota. Figura elaborada por el autor

Para complementar el desarrollo de esta fase 2, se incluye en el Anexo A el Manual de implementación del entorno Cyber Range UTN, el cual se detalla de manera técnica y estructurada los pasos seguidos para la configuración de la infraestructura. Este manual sirve como guía práctica para replicar el entrono en otras instituciones o entornos académicos similares, asegurando la reproducibilidad y escalabilidad del proyecto.

3.3.3 Fase 3: Desarrollo e integración de escenarios de ciberataques basados en MITRE ATT&CK

En esta fase se desarrollaron e integraron los escenarios prácticos que conforman el entorno de entrenamiento tipo Capture The Flag (CTF), tomando como referencia la matriz MITRE ATT&CK como base para la simulación de técnicas reales utilizadas por atacantes. Los escenarios se implementaron en máquinas virtuales configuradas en el entorno Proxmox (Servidor CITEL) y se gestionaron mediante la plataforma CTFd (Servidor local del investigador), permitiendo a los participantes interactuar con los retos de forma segura y controlada.

Se desarrollaron dos escenarios iniciales, cada uno con características específicas que permiten a los participantes identificar vulnerabilidades, ejecutar ataques y capturar las banderas (flags) correspondientes. El primer escenario simula un compromiso multietapa, donde se deben explotar servicios como MySQL y SSH, y realizar escalada de privilegios. El segundo escenario plantea la explotación de un servidor FTP mal configurado con acceso anónimo, fomentando la identificación de servicios expuestos y vulnerabilidades relacionadas con configuraciones inseguras.

La selección de las técnicas a simular se realizó con base en las tácticas de acceso inicial, ejecución, escalada de privilegios y descubrimiento, conforme a la matriz MITRE ATT&CK. La relación entre los escenarios implementados y las técnicas empleadas se detalla en el Anexo C. Por su parte, el proceso de construcción de los escenarios, desde la instalación de servicios hasta la configuración de vulnerabilidades y banderas, se encuentra documentado en el Anexo D.

3.3.4 Fase 4: Evaluación de la Plataforma.

El propósito de esta fase fue evaluar la efectividad y utilidad pedagógica del entorno Cyber Range UTN desarrollado, con el fin de medir su impacto en la conciencia y habilidades en seguridad cibernética de los participantes. Esta evaluación se realizó mediante una combinación de métodos cuantitativos y cualitativos, enfocados en tres dimensiones clave:

- Percepción de los estudiantes antes y después del uso de la plataforma.
- Análisis de desempeño durante los retos CTF.
- Retroalimentación reflexiva y observación del proceso de aprendizaje.

Evaluación cuantitativa: Se aplicaron encuestas estructuradas antes y después de la participación en el entorno, con escalas de valoración de tipo Likert, a un grupo de estudiantes de la carrera de Telecomunicaciones. Las encuestas midieron aspectos como:

- Nivel de familiaridad con herramientas de ciberseguridad.
- Conocimiento sobre ciberataques y vulnerabilidades.
- Nivel de conciencia sobre amenazas reales.
- Percepción del aprendizaje basado en retos.

Los resultados fueron tabulados y analizados estadísticamente, comparando los valores previos y posteriores para identificar mejoras en la percepción y conocimiento. Las encuestas y sus resultados se encuentran detallados en los Anexos E, F, G y H.

Además, se recopilaron métricas de desempeño directamente desde la plataforma CTFd, como:

- Tiempo promedio de resolución de retos.
- Número de flags capturadas por equipo.
- Porcentaje de éxito por escenario.

Estas métricas permitieron identificar patrones de participación y efectividad del diseño de los escenarios.

Evaluación cualitativa: De manera complementaria, se aplicaron instrumentos cualitativos para obtener una comprensión más profunda de la experiencia de los participantes, entre ellos:

- Informes reflexivos por equipo (ver Anexo I), donde los participantes describieron las técnicas utilizadas, los restos enfrentados y las habilidades desarrolladas.
- Observación directa durante las sesiones de práctica, documentada mediante un registro fotográfico (ver Anexo K).
- Análisis de interacciones en la plataforma, incluyendo estrategias colaborativas, errores frecuentes y caminos alternativos de resolución.

Estos insumos permitieron analizar la utilidad formativa del entorno desde una perspectiva pedagógica, destacando su rol en la motivación, resolución de problemas y aplicación de conocimiento teóricos en escenarios reales.

3.4 Consideraciones bioéticas

Se aplicaron los principios éticos de beneficencia, precaución, responsabilidad y autonomía. Todos los participantes dieron su consentimiento para formar parte del entorno CTF garantizando su derecho de retirarse en cualquier momento. Asimismo, se implementó medidas para proteger la privacidad y confidencialidad de los datos, el anonimato tanto en encuestas como en el registro de actividad en la plataforma CTFd.

CAPÍTULO IV – RESULTADOS Y DISCUSIÓN

Este capítulo presenta los resultados obtenidos durante el proceso de investigación de este proyecto. Los hallazgos se organizan en función de los cuatro objetivos específicos planteados en la investigación, abordando aspectos técnicos y formativos. Para ello, se incluyen resultados cuantitativos y cualitativos, complementados con informes, gráficas, tabulaciones y métricas de rendimiento.

4.1 Resultados según objetivos

4.1.1 Objetivo 1:

La revisión bibliográfica realizada en la Fase 1 permitió identificar tendencias clave en la implementación de entornos de entrenamiento CTF, así como enfoques metodológicos efectivos para la formación práctica en ciberseguridad. El análisis incluyó fuentes académicas, informes técnicos, libros especializados y artículos científicos, sistematizados mediante una matriz de análisis documental (ver Anexo A).

Entre los principales hallazgos destacan:

- El uso frecuente de plataformas como CTFd por su accesibilidad, personalización y capacidad para gestionar desafíos y puntajes.
- La adopción del marco MITRE ATT&CK como referencia estándar para construir escenarios realistas alineados con tácticas y técnicas utilizadas por atacantes reales.
- La efectividad de metodologías activas como el aprendizaje basado en retos, la gamificación y el trabajo colaborativo en el desarrollo de habilidades prácticas.

- La implementación de entornos virtuales mediante Proxmox o Docker, que ofrecen flexibilidad y aislamiento para las prácticas.

Estos hallazgos sirvieron de base para definir los componentes técnicos del entorno Cyber Range UTN, así como para estructurar los escenarios de ataque implementados en las fases posteriores. Además, reforzaron la necesidad de vincular teoría y práctica mediante entornos accesibles, seguros y adaptables a diferentes niveles de conocimiento.

4.1.2 Objetivo 2:

Durante la Fase 2 se concretó el diseño técnico e implementación del entorno Cyber Range UTN, compuesto por dos servidores Proxmox:

- Servidor Proxmox en CITEL: Alojó las máquinas virtuales vulnerables y atacantes (Kali Linux), organizadas por VLANs para cada equipo.
- Servidor Proxmox local: Alojó la plataforma CTFd, accesible desde la IP pública http://186.71.1.253:8000

El entorno final implementado incluyó lo siguiente:

- 4 máquinas atacantes (Kali Linux)
- 8 máquinas vulnerables (Ubuntu 18.04)
- Segmentación por VLAN
- Plataforma CTFd para la gestión de retos y usuarios.

Los participantes accedieron al entorno desde sus estaciones de trabajo a través de la red EDUROAM UTN. La arquitectura general se presenta en la Figura 5 y el detalle técnico de implementación se encuentra en el Anexo A.

Antes de iniciar las sesiones de entrenamiento con los participantes, se realizó una validación técnica previa del entorno. Estas pruebas incluyeron:

- Verificación de conectividad entre los servidores y las estaciones de trabajo.
- Acceso simultáneo a la plataforma CTFd.
- Revisión del funcionamiento de los retos y del registro de puntuaciones.
- Monitoreo preliminar de CPU, RAM y disco de los servidores Proxmox.

Los resultados confirmaron que el entorno estaba operativo y listo para ser usado por los participantes.

4.1.3 Objetivo 3

Se diseñaron dos escenarios de entrenamiento alineados con técnicas del marco MITRE ATT&CK (Ver Tabla 6)

Tabla 6

Escenarios MITRE ATT&CK implementados

Escenario	Técnicas ATT&CK aplicadas	Objetivo principal
1	TA0043 (Reconocimiento), TA0001 (Acceso inicial), TA0002 (Ejecución)	Acceder a 3 banderas
2	T1078 (Cuentas válidas), TA0043 (Escaneo de servicios)	Extraer una bandera desde un FTP

Nota: Tabla desarrollada por el autor

Los cuatro equipos participantes lograron capturar al menos tres de las cuatro banderas disponibles. Los resultados se detallan en la Tabla 7:

Tabla 7

Resultados entrenamiento cibernético

Equipo	Puntuación (puntos)	Tiempo de resolución
CrushesUTN	450	1 hora 15 minutos
archlovers	450	1 hora 20 minutos
error404	400	1 hora 30 minutos
secNet	400	1 hora 30 minutos

Nota. Tabla desarrollada por el autor

El informe técnico del equipo archlovers (ver Anexo I) evidenció el uso de herramientas como Nmap, Hydra, análisis de código HTML, acceso FTP anónimo y escalamiento de privilegios. Además, en este informe se muestra de forma detallada toda la actividad realizada por el equipo, que técnicas utilizaron y su punto de vista sobre la plataforma implementada.

4.1.4 Objetivo 4: Evaluar la efectividad y utilidad del entorno

Evaluación técnica del entorno: Previo al entrenamiento con los participantes, se ejecutaron pruebas de funcionamiento para validar la estabilidad de la plataforma. Estas pruebas permitieron confirmar que:

- Las máquinas virtuales podían ser accedidas sin errores desde las estaciones de trabajo.
- La plataforma CTFd respondía correctamente ante múltiples conexiones simultáneas.

- Los retos estaban activos, registraban puntuaciones y validaban banderas correctamente.

Durante el entrenamiento, se recopilaron métricas del servidor Proxmox CITEL, resumidas en la Tabla 8.

Tabla 8

Métricas de rendimiento - Servidor Proxmox CITEL

Métrica	Valor	Interpretación
Uso de CPU	6.52 %	Bajo uso de CPU, indicando que el servidor no estuvo sobrecargado.
Uso de RAM	77.73% (23.94 GB de 30.81 GB)	Uso moderado de RAM, cercano al límite.
Uso de almacenamiento	89.87% (75.96 GB de 93.33 GB)	Alto uso de almacenamiento, se necesitaría aumentar espacio en disco.
Carga promedio	2.40, 2.15, 2.26	Valores bajos, indicando un buen rendimiento del servidor.
Uptime	2 días, 2 horas, 31 minutos	Estabilidad del entorno durante el entrenamiento.

Nota. Tabla desarrollada por el autor

Se puede observar en la Tabla 8, que el servidor demostró un buen rendimiento durante el entrenamiento, con su bajo uso de CPU y una carga promedio aceptable. Sin embargo, el alto uso de almacenamiento (89.97%) es un detalle que se debería tomar en consideración, para poder desplegar más laboratorios, por ese aspecto se implementaron dos escenarios.

Evaluación pedagógica de los participantes: Se aplicaron encuestas previas y posteriores al entrenamiento. Cuyos resultados indican mejoras significativas en conocimientos, habilidades y percepción de amenazas cibernéticas.

Nivel de conocimiento y experiencia previa: En la Figura 35 (Anexo E) se observa que la mayoría de los estudiantes (89%) se identificaron como principiantes en seguridad cibernética, mientras que solo un 11% se consideró en nivel intermedio (ver Tabla 9). Además, el 100% de los participantes no había participado en competencias CTF o entornos de entrenamiento similares, y el 100% no había usado herramientas de hacking ético como Kali Linux, Metasploit oWireshark. Estos resultados indican que los estudiantes tenían un conocimiento básico en el área, lo que sugiere que el entorno de entrenamiento debía ser accesible para principiantes.

Tabla 9

Nivel de conocimientos y experiencia previa antes y después del entrenamiento

Aspecto	Antes del entrenamiento	Después del entrenamiento
Nivel de conocimiento	89% principiantes, 11% intermedio.	78 %Mejora significativa en habilidades. 22% un poco de mejora en habilidades.

Experiencia en CTF	100% sin experiencia previa	100% practicó explotación de vulnerabilidades.
Uso de herramientas	100% no había usado Kali Linux, Metasploit, etc.	Uso de herramientas durante el entrenamiento.
Conocimiento de MITRE ATT&CK	67% no conocía la matriz	1 hora 30 minutos

Nota. Tabla elaborada por el autor

Después del entrenamiento, el 100% de los estudiantes practicaron explotación de vulnerabilidades, lo que indica que esta fue el área principal de enfoque. Además, el 78% consideró que el entrenamiento mejoró significativamente sus habilidades en seguridad informática, mientras que el 22% sintió que mejoró un poco (Ver Tabla 9). Estos resultados muestran que el entrenamiento fue efectivo para mejorar las habilidades prácticas de los estudiantes, especialmente en el área de explotación de vulnerabilidades.

Expectativas vs. Resultados: Antes del entrenamiento, los estudiantes expresaron expectativas claras sobre lo que esperaban aprender. El 67% indicó específicamente el interés en mejorar sus habilidades en ciberseguridad, mientras que otros destacaron áreas como criptografía, análisis de malware y explotación de vulnerabilidades (ver Tabla 10).

Tabla 10

Expectativas de aprendizaje antes del entrenamiento y resultados obtenidos después

Aspecto	Antes del entrenamiento	Después del entrenamiento

Expectativas de aprendizaje	67% esperaba mejorar en ciberseguridad; interés en criptografía, análisis de malware, etc.	78 % mejoró significativamente; áreas destacadas: seguridad de puertos, comandos, vulnerabilidades.
Áreas de interés	Criptografía (80%), análisis de malware (40%), explotación de vulnerabilidades (50%).	100% practicó explotación de vulnerabilidades.

Nota. Tabla elaborada por el autor

Después del entrenamiento, los participantes indicaron haber mejorado en áreas como la seguridad de puertos, el uso de comandos y la identificación de vulnerabilidades (ver Tabla 10). Estos resultados indican que el entrenamiento cumplió con las expectativas de los estudiantes, permitiéndoles aplicar conocimientos teóricos en el campo práctico.

Facilidad de uso de plataforma CTF: Luego del entrenamiento, el 78% de los estudiantes calificó la plataforma CTF como fácil o muy fácil de usar, mientras que el 11% la consideró difícil y otro 11% se mantuvo neutral (ver Tabla 11). Algunos participantes sugirieron mejoras, como incluir una descripción breve de los ataques o proporcionar más guías para los principiantes.

Tabla 11

Facilidad de uso de la plataforma CTFd

Aspecto	Después del entrenamiento
Facilidad de uso	78% la consideró fácil o muy fácil; 11% difícil; 11% neutral.
Sugerencias de mejora	Incluir descripciones de ataques, más guías para principiantes.

Nota. Tabla elaborada por el autor

Conciencia sobre amenazas cibernéticas: Antes del entrenamiento, el 40% de los estudiantes tenía una muy baja confianza para resolver desafíos de seguridad informática, mientras que el 50% se mantenía neutral (ver Tabla 12). Después del entrenamiento, el 56% calificó su nivel de conciencia sobre amenazas cibernéticas como neutral, mientras que el 22% la consideró alta o muy alta. Solo el 22% mantuvo una percepción baja o muy baja.

Tabla 12

Conciencia sobre amenazas cibernéticas antes y después del entrenamiento.

Aspecto	Antes del entrenamiento	Después del entrenamiento
Confianza para resolver desafíos	40% muy baja, 50% neutral	56% neutral, 22% alta o muy alta%.
Conciencia sobre amenazas	No aplica	56% neutral, 22% alta o muy alta.

Nota. Tabla elaborada por el autor

Después del entrenamiento, el 100% de los estudiantes recomendaría la plataforma a otros compañeros, lo que refleja una percepción positiva del entrenamiento (ver Tabla 13). Así mismo, el 78% consideró que sus habilidades en seguridad informática habían mejorado significativamente.

Tabla 13

Percepción general del entrenamiento y recomendaciones

Aspecto	Después del entrenamiento
Recomendación	100% recomendaría la plataforma a otros estudiantes.
Impacto en habilidades	78% mejoró significativamente; 22% mejoró un poco.

Nota. Tabla elaborada por el autor

Los resultados de las encuestas previa y posterior del Cyber Range UTN muestran un cambio significativo en las habilidades y percepciones de los estudiantes. Antes del entrenamiento la mayoría eran principiantes con poca o ninguna experiencia en competencias con modalidad CTF. Sin embargo, después del entrenamiento, el 78% consideró que sus habilidades en seguridad informática habían mejorado, especialmente en temas de explotación de vulnerabilidades.

La plataforma CTF fue calificada como fácil de usar por la mayoría de los participantes, aunque algunos sugirieron mejoras, como la inclusión de descripciones más detalladas de los ataques. Además, el entrenamiento incrementó la conciencia sobre amenazas cibernéticas en gran parte de los estudiantes que participaron en el entrenamiento.

El uso del framework de MITRE ATT%CK permitió a los estudiantes contextualizar los desafíos dentro de un marco teórico ampliamente reconocido, lo que contribuyó a una comprensión más profunda de las técnicas de ataque y defensa. Las fotografías del entrenamiento (ver Anexo K) reflejan el compromiso y la dedicación de los estudiantes durante la resolución de los retos. Estas imágenes complementan los resultados cualitativos obtenidos en las encuestas.

CONCLUSIONES

Se logró implementar un entorno de entrenamiento cibernético funcional y alineado con la matriz MITR ATT&CK. El entorno permitió a los estudiantes practicar técnicas de ataque en un contexto controlado y realista.

Los resultados de las encuestas post-uso mostraron que el 78% de los estudiantes consideró que sus habilidades en ciberseguridad mejoraron significativamente, especialmente en áreas como la explotación de vulnerabilidades y la identificación de vulnerabilidades. Esto confirma que el entrenamiento fue efectivo para reforzar los conocimientos teóricos adquiridos en la materia de Seguridad en Redes.

El 78% de los estudiantes calificó la plataforma CTFd como fácil o muy fácil de usar, lo que indica que la interfaz fue intuitiva y accesible para usuarios con poca experiencia en entornos CTF.

El entrenamiento aumentó la conciencia sobre amenazas cibernéticas en la mayoría de los estudiantes. Esto sugiere que el entorno fue útil para familiarizar a los estudiantes con técnicas de ataque y defensa, pero podría requerir ajustes para profundizar en la comprensión de amenazas.

La alineación de los escenarios con la matriz MITRE ATT&CK permitió a los estudiantes contextualizar los desafíos dentro de un marco teórico ampliamente reconocido en la industria. Esto contribuyó a una comprensión más profunda de las técnicas de ataque y defensa.

Las capacidades del servidor (CPU, RAM, almacenamiento) limitaron la implementación de más escenarios y la participación de un mayor número de estudiantes. Sin embargo, el entorno demostró ser estable y funcional para los objetivos planteados.

A partir de los resultados obtenidos, se puede afirmar que la hipótesis planteada en esta investigación fue confirmada. El desarrollo del entorno seguro de Capture The Flag (CTF), con la integración de escenarios alineados con MITRE ATT&CK, permitió establecer una estrategia efectiva de formación y concienciación en ciberseguridad. La plataforma resultó ser una herramienta robusta tanto para la capacitación práctica como para la evaluación de habilidades técnicas en estudiantes de la Universidad Técnica del Norte. Esta experiencia evidencia que los entornos CTF bien diseñados pueden contribuir significativamente a la prevención de ciberataques al fortalecer el aprendizaje activo y contextualizado de técnicas ofensivas y defensivas.

RECOMENDACIONES

Expandir la capacidad de almacenamiento y memoria RAM del servidos para permitir la implementación de más escenarios y la participación de un mayor número de estudiantes. Monitorear el uso de recursos en tiempo real para garantizar un rendimiento óptimo durante el entrenamiento.

Incluir más escenarios que aborde otras áreas de seguridad informática, como criptografía, análisis de malware y forense digital, para proporcionar una formación más integral. Diseñar escenarios progresivos que comiencen con niveles de dificultad baja y aumenta gradualmente, permitiendo a los participantes ganar confianza a medida que avanzan.

Incluir más escenarios alineados con la matriz MITRE ATT&CK y proporcionar una introducción detallada a este framework para familiarizar a los estudiantes con su uso. Integrar técnicas avanzadas de ataque y defensa basadas en actualizaciones recientes del framework.

Establecer alianzas con empresas y organizaciones del sector de ciberseguridad para enriquecer los escenarios con casos reales y actualizados. Invitar a expertos en ciberseguridad para impartir talleres o charlas que complementen el entrenamiento.

BIBLIOGRAFÍA

Asamblea Nacional. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. www.lexis.com.ec

Cuzme-Rodríguez Fabián and León-Gudiño, M. and S.-Z. L. and D.-L. M. (2019). Offensive Security: Ethical Hacking Methodology on the Web. In L. and G.-H. J. and V.-C. P. and S. G. O. and U.-F. M. I. Botto-Tobar Miguel and Barba-Maggi (Ed.), *Information and Communication Technologies of Ecuador (TIC.EC)* (pp. 127–140). Springer International Publishing.

Delgado Olivera, L. de la C., & Díaz Alonso, L. M. (2021). Modelos de desarrollo de software. *Revista Cubana de Ciencias Informáticas*, *15*(1), 37–51.

Domínguez-Limaico Hernán and Nicolalde Quilca, W. and Z. M. and C.-R. F. and M.-O. E. (2023). Intruder Detection System Based Artificial Neural Network for Software Defined Network. In M. and D. C. A. and Z. V. A. Zambrano Vizuete Marcelo and Botto-Tobar (Ed.), *I+D for Smart Cities and Industry* (pp. 315–328). Springer International Publishing.

Herrero Perez, L. (2022). *Hacking etico*. RA-MA Editorial. https://elibro.net/es/lc/utnorte/titulos/222693

Mata, A. E. (2024). *Ciberseguridad: curso practico*. RA-MA Editorial. https://elibro.net/es/lc/utnorte/titulos/273939

MITRE. (2025). *ATT&CK Matrix for Enterprise*. Https://Attack.Mitre.Org/.

Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats. *Electronics*, *13*(19). https://doi.org/10.3390/electronics13193867

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. In *Technical report*. The MITRE Corporation.

Tejeda Alcalde, A. (2025). *Diseño, implementación y resolución de un CTF guiado con enfoque narrativo*. http://hdl.handle.net/10609/152107

Urcuqui , C. C., & Navarro Cadavid, A. (2022). *Ciberseguridad: los datos tienen la respuesta*. Editorial Universidad Icesi. https://elibro.net/es/lc/utnorte/titulos/225844

Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, *88*, 101636. https://doi.org/https://doi.org/10.1016/j.cose.2019.101636

ANEXOS

En esta sección se presentan los materiales complementarios que respaldan y amplían la información presentada en el trabajo de investigación. Su propósito es documentar de forma detallada los aspectos técnicos, metodológicos y empíricos que respaldan el desarrollo, implementación y evaluación del entorno Cyber Range UTN.

En la primera sección se incluyen documentos técnicos relacionados con la infraestructura desplegada, la metodología de diseño basada en MITRE ATT&CK, y las herramientas utilizadas para garantizar la seguridad del entorno. En la segunda sección, se presentan los instrumentos de recolección de datos aplicados a los participantes, junto con sus respectivos análisis, así como evidencia del uso práctico del entorno por parte de los estudiantes.

Esta documentación adicional permite validar la rigurosidad técnica del proyecto, así como la relevancia pedagógica del entorno Cyber Range UTN como herramienta para la formación práctica en ciberseguridad.

Anexos Técnicos del Entorno Cyber Range UTN

Anexo A. Matriz de análisis documental

En este anexo se presenta una matriz de análisis documental con base a las fuentes consultadas durante la Fase 1 del proceso de investigación. Esta revisión bibliográfica permitió identificar tendencias, herramientas, enfoques pedagógicos y marcos de referencia que fundamentaron el diseño del entorno Cyber Range UTN. La matriz resume los principales aportes de cada fuente analizada (Ver Tabla 14).

Tabla 14

Matriz de análisis documental

N°	Fuente	Tipo de publicación	Enfoque pedagógico o técnico	Uso de ATT&CK	Aporte clave
1	Shin et al. (2024)	Artículo científico	Diseño de cyber range para entrenamiento efectivo	Sí	Propone arquitectura modular basada en amenazas reales.
2	Strom et al. (2018)	Informe técnico	Base teórica de ATT&CK	Sí	Explica filosofía y uso práctico de ATT&CK
3	Yamin et al. (2020)	Revista académica	Modelos de cyber ranges y testbeds	Parcial	Clasificación de funciones,

					herramientas y escenarios.
4	Tejeda Alcalde (2025)	Trabajo académico	CTF guiado con narrativa	Sí	Enfoque didáctico basado en historia y resolución guiada.
5	Mata (2024)	Libro técnico	Curso práctico	No	Enseña herramientas ofensivas como Kali y Metasploit.
6	Herrero Pérez (2022)	Libro técnico	Hacking ético paso a paso	Parcial	Enfoque pedagógico y práctico de explotación de vulnerabilidades.
7	Urcuqui & Navarro (2022)	Libro académico	Perspectiva legal y técnica de la ciberseguridad	No	Relación entre protección de datos y seguridad informática.

8	MITRE (2025)	Sitio web oficial	Marco ATT&CK actualizado	Sí	Referencia oficial para técnicas y tácticas.
9	Cuzme Rodríguez et al. (2019)	Artículo científico	Metodología de hacking web	Parcial	Ejemplifica paso a paso herramientas ofensivas.

Nota. Tabla elaborada por el autor.

Anexo B. Manual técnico de implementación de la plataforma Cyber Range UTN

El presente manual describe el proceso técnico realizado para la implementación de la plataforma de entrenamiento cibernético denominada "Cyber Range UTN". Esta implementación incluyó el despliegue de máquinas virtuales vulnerables, atacantes y la plataforma CTFd para la gestión de los retos, estos entornos se desplegaron en ambientes separados uno usando el servicio de Proxmox de CITEL y otro usando un Proxmox local de propiedad del investigador.

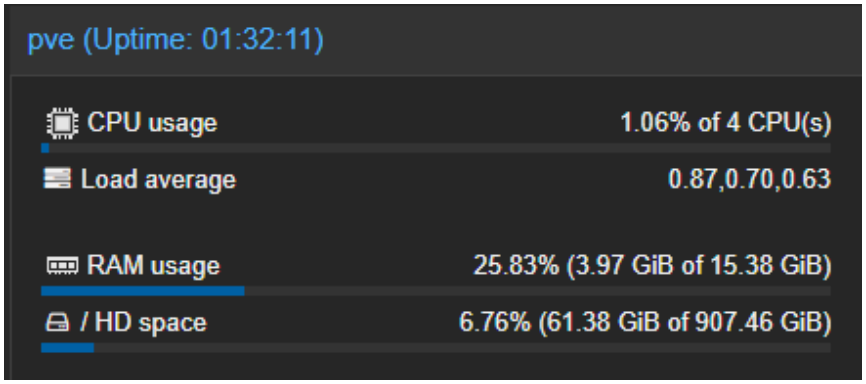
Arquitectura del Cyber Range: Se definió una arquitectura distriubida considerando las de hardware del servidor Dell EMC PowerEdge R750xs, dividiendo los servicios en dos entornos:

- **Servidor Proxmox CITEL:** Hospeda las máquinas virtuales para prácticas de ciberseguridad, incluyendo los equipos vulnerables y atacantes. Este servidor se configuró con:
    - Red de máquinas vulnerables segmentadas por VLAN
    - Red de máquinas atacantes (Kali Linux)
- **Servidor Proxmox Local:** Se utilizó para alojar la plataforma CTFd encargada de la creación y gestión de desafíos CTF. Con el objetivo de no sobrecargar el servidor Proxmox de CITEL, además de proporcionar seguridad al entorno, pues se aísla el sistema de puntuación tanto de la red de máquinas vulnerables como de la red de atacantes. Este servidor se configuró con:
    - Dirección IP pública: http://186.71.1.253:8000/
    - 4 CPU, 16 GB de RAM y 500 GB de almacenamiento

- Sistema operativo Ubuntu Server y CTFd instalado.

Figura 6

Características servidor Proxmox Local



Nota. Esta gráfica muestra las características en cuanto a CPU, RAM y Almacenamiento del servidor Proxmox Local.

Diseño de Máquinas Virtuales: En el servidor Proxmox de CITEL, se diseñaron tres máquinas virtuales base que sirvieron como plantillas para la creación de las demás (ver Tabla 15):

Tabla 15

Máquinas creadas

Máquina	ID Máquina	Sistema Operativo	CPU	RAM (GB)	Almacenamiento (GB)
Reto1	127	Ubuntu 18.04	1	2	10
Reto2	128	Ubuntu 18.04	1	2	10

Kali-Linux	129	Kali Linux 2024	2	2	20

Nota. Tabla elaborada por el autor

Se priorizó el uso eficiente de recursos para no afectar el resto de operaciones del servidor de CITEL. Se crean 2 máquinas vulnerables y una máquina atacante como guías, luego al terminar de realizar todas sus configuraciones se crean plantillas a partir de ellas. Las máquinas se configuraron con los siguientes pasos generales:

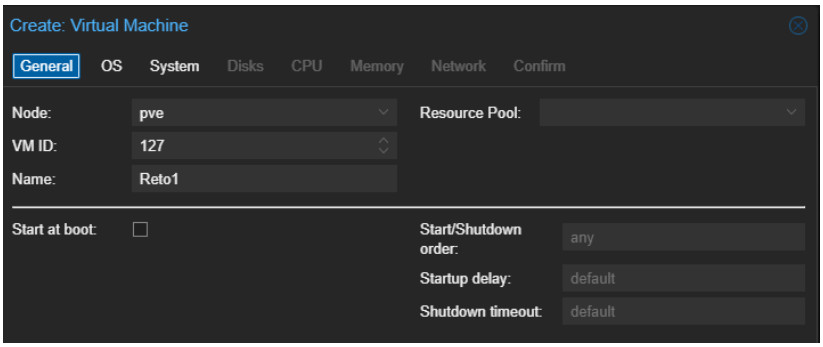
- **Creación de VM:** Usando “Create VM” en Proxmox.
- **Asignación de recursos:** CPU, RAM, almacenamiento
- **Carga de imagen ISO:** Ubuntu 18.04 (máquinas vulnerables), Kali Linux (máquinas atacantes.)
- **Segmentación de red:** Cada pareja de atacante-vulnerable fue ubicda en una VLAN diferente.

Máquina Vulnerable 1: Para la creación de la primera máquina vulnerable virtual, en el Proxmox de CITEL, se selecciona la opción “Create VM”, para luego asignar los recursos de dicha máquina.

- **Asignación de nombre e ID.** Nombre Reto 1, ID 127 ver Figura 7.

Figura 7

Creación máquina vulnerable 1

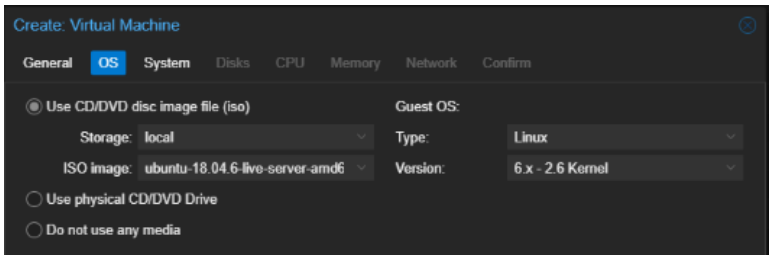


Nota. En la imagen se muestran los detalles del ID y nombre de la máquina del Reto 1.

- **Sistema Operativo de la Máquina:** Previamente se carga la imagen .iso correspondiente, en este caso un Ubuntu 18.04, se selecciona la opción de ISO image como se observa en la Figura 8.

Figura 8

Asignación de imagen ISO a máquina vulnerable 1

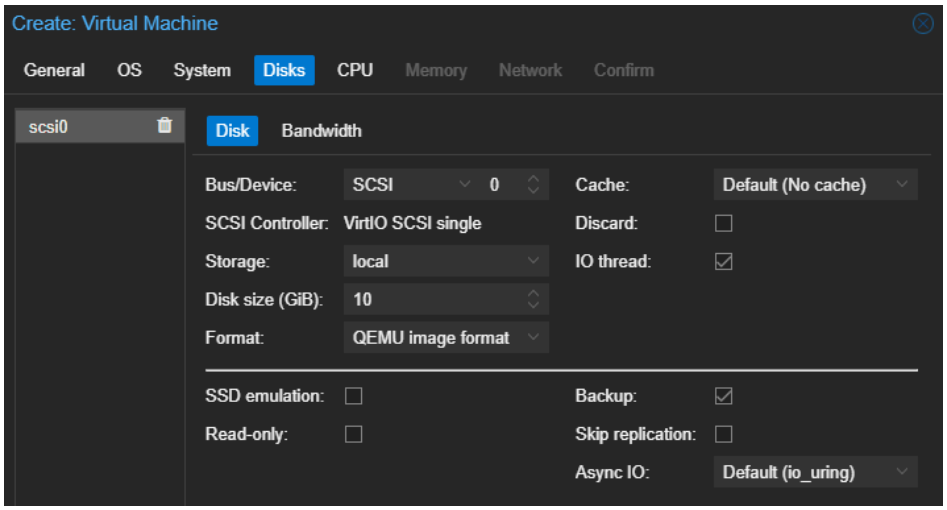


Nota: En la imagen se muestra la selección de la imagen .ISO de la máquina virtual.

- **Almacenamiento en Disco:** La Figura 9 muestra que el espacio asignado en cuanto a almacenamiento de la máquina es de 10 GB.

Figura 9

Asignación de almacenamiento en máquina vulnerable 1

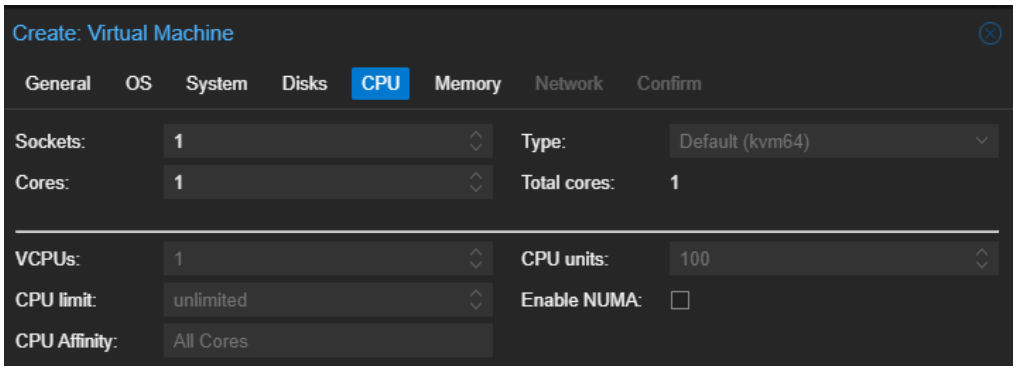


Nota: En la imagen se muestra la selección del tamaño del disco de almacenamiento de la máquina.

- **Núcleos de la máquina:** Se asigna un solo núcleo a la máquina, como se muestra en la Figura 10.

Figura 10

Asignación de CPU a máquina vulnerable 1

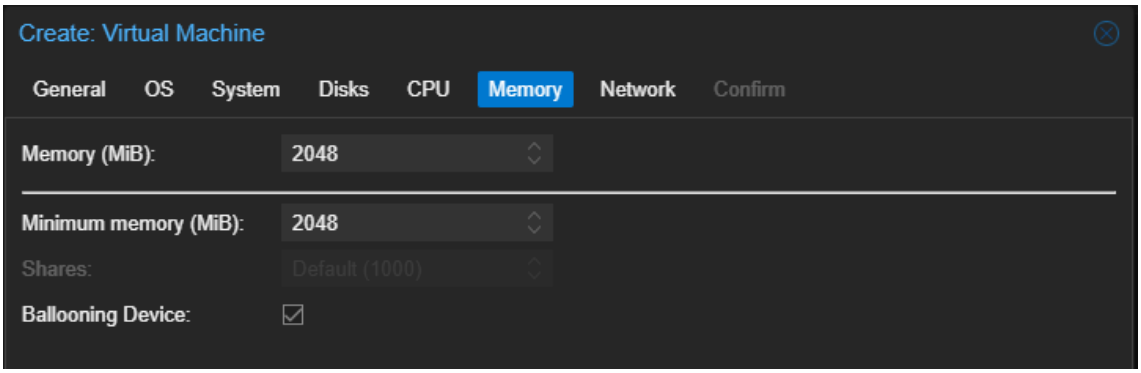


Nota: En la imagen se muestra la selección del número de núcleos a la máquina vulnerable 1.

- **Memoria RAM:** Se asigna 2 GB de memoria RAM a la máquina, esto se puede observar en la Figura 11.

Figura 11

Asignación de RAM a máquina Reto 1



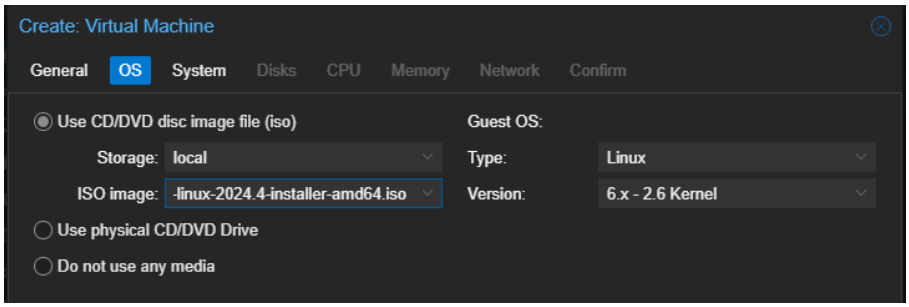
Nota: En el gráfico se muestra la selección del número de RAM a la máquina vulnerable 1.

El proceso de creación de la máquina vulnerable 2, es prácticamente similar al realizado en la máquina vulnerable 1. La diferencia radica en las configuraciones realizadas en cada máquina, generando diferentes tipos de vulnerabilidades, esas configuraciones se muestran en el Anexo D (Guía de creación de escenarios CTF).

Máquina atacante (Kali Linux): Proceso similar a la creación de la máquina vulnerable 1, la diferencia radica en el sistema operativo asignado y el almacenamiento en disco de 20 GB, esto se muestra en las Figuras 12 y 13 respectivamente.

Figura 12

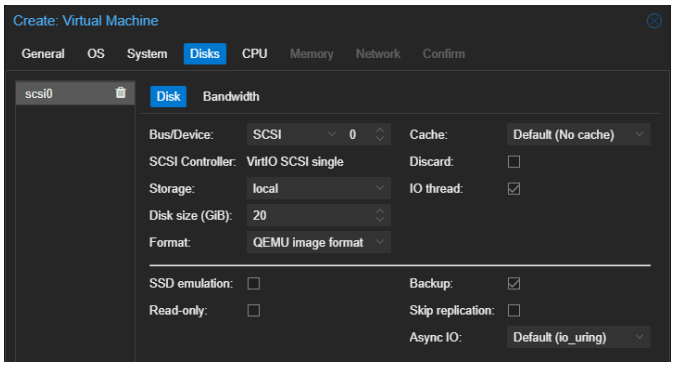
Sistema operativo para máquina Kali Linux



Nota: En el gráfico se muestra la selección del sistema operativo para la máquina Kali-Linux.

Figura 13

Asignación de almacenamiento para máquina Kali Linux

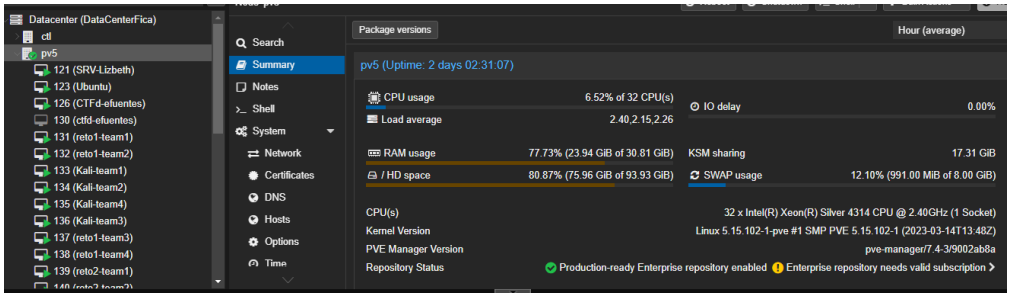


Nota: En el gráfico se muestra la selección del almacenamiento para la máquina Kali Linux.

Estas configuraciones se seleccionaron para minimizar el uso de recursos en el servidor Proxmox de CITEL, dado que este se encuentra en uso para otras actividades. Además, se priorizó la creación de un número limitado de máquinas virtuales (4 máquinas atacantes y 8 máquinas vulnerables) para no sobrecargar el servidor. En la Figura 14 se presenta una vista del entorno Proxmox del servidor CITEL, donde se observan las máquinas virtuales desplegadas, su estado y uso de recursos.

Figura 14

Vista general del entorno Proxmox CITEL



Nota. Captura de pantalla del panel principal de Proxmox del servidor CITEL con las máquinas activas del Cyber Range UTN.

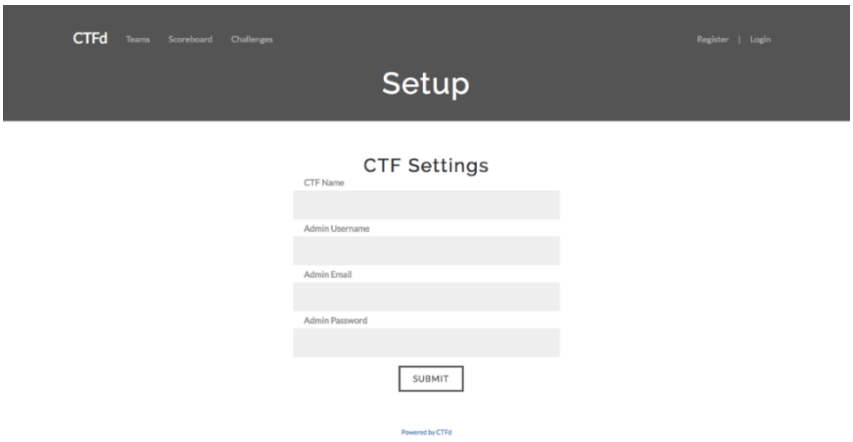
Instalación de plataforma CTFd en servidor local: Se desplegó una instancia de Ubuntu Server en el Proxmox local y se instaló la plataforma CTFd con los siguientes pasos:

- Requerimientos mínimos del sistema: 1 CPU de doble número con al menos 1 GB de RAM.
- Instalar Docker
- Instalar Docker Compose
- Clonar el repositorio CTFd con "*git clone https://github.com/CTFd/CTFd.git*"
- Modificar el archivo "Docker-compose.yml", ubicar un valor aleatorio de 9 dígitos en el campo "SECRET_KEY"
- Levantar Docker con "docker-compose up"
- Acceder a la plataforma CTFd mediante http://ip-del-servidor:8000

La Figura 15 muestra por defecto una página de configuración en donde se escoge el nombre del entorno CTF y las credenciales para el administrador de la plataforma.

Figura 15

Página de configuración de CTFd

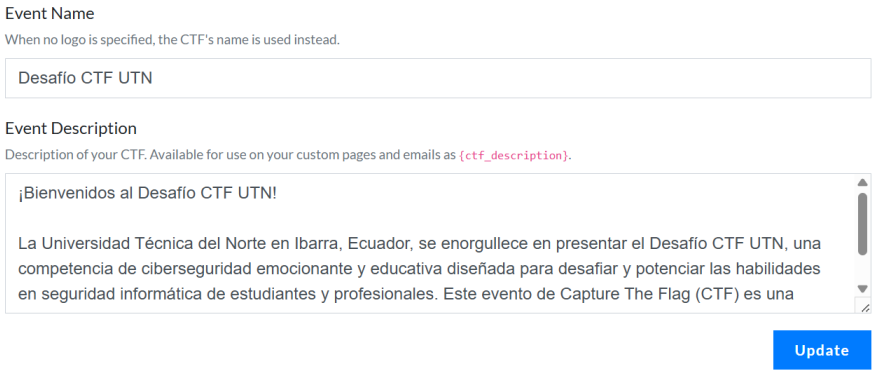


Nota. En esta sección se coloca las credenciales del administrador del entorno y el nombre de CTF.

Nombre: Desafío CTF UTN, se crea el evento del entrenamiento esto se hace en la sección de Configuración, se añade un nombre y descripción del evento (ver Figura 16)

Figura 16

Nombre y descripción del Entrenamiento

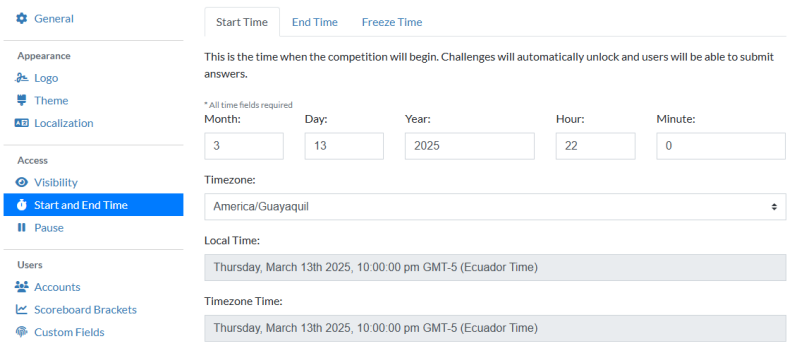


Nota. Figura elaborada por el autor

Fecha de inicio y fin del evento: Se configuraron las fechas correspondientes en las que se realizó el entrenamiento (ver Figura 17). La fecha de inicio definió el momento en que los retos se hicieron visibles para los estudiantes, mientras que la fecha fin cerró automáticamente el acceso a la resolución de estos.

Figura 17

Inicio-Fin Cyber Range UTN

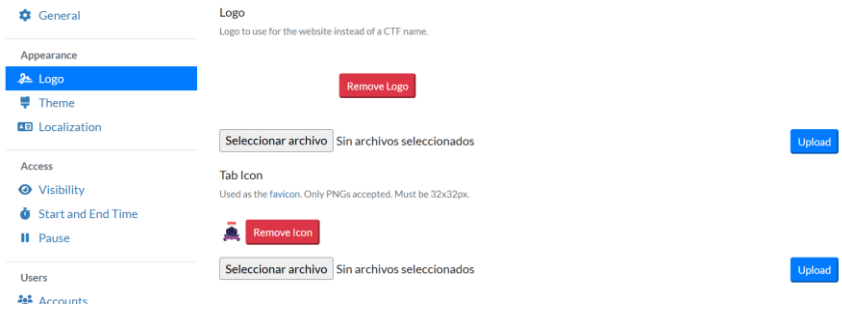


Nota. Figura desarrollada por el autor

Logo institucional y personalización de colores: Se cargó el logotipo oficial de la Universidad Técnica del Norte como parte de la personalización visual del evento en la plataforma CTFd, lo cual se realizó desde el panel de administración en la sección de configuración general. Además, se aplicó una paleta de colores acorde a la identidad institucional, personalizando el encabezado, fondo y botones de la interfaz. En la Figura 18 se muestra la pantalla de configuración del logo, y en la Figura 19 se puede observar la interfaz personalizada visible para los participantes.

Figura 18

Página de edición de logo



Nota. El logo diseñado se puede cargar en esta sección

Figura 19

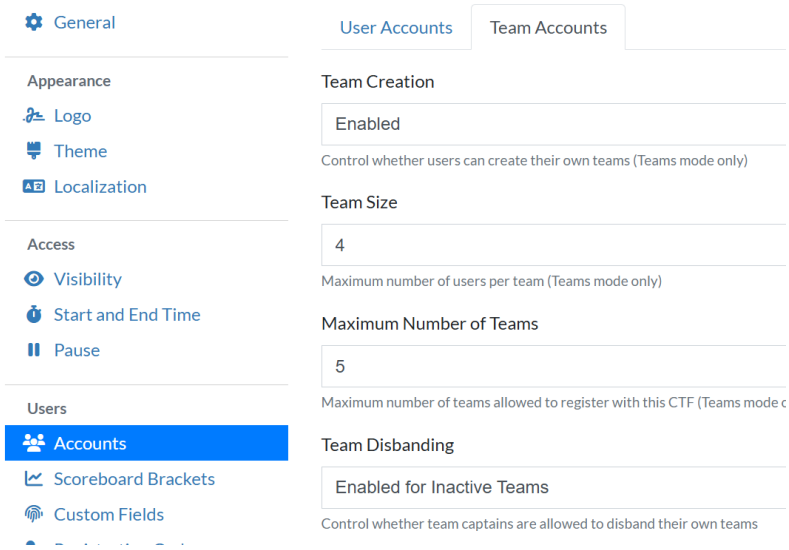
Página de inicio para participantes

Nota. Al ingresar a la plataforma CTFd los participantes pueden observar la personalización del entorno.

Creación de equipos: Se configuró el entorno de tal manera que exista un número máximo de 5 equipos y 4 miembros por equipos (ver Figura 20), posterior a ello cada líder de grupo tiene la posibilidad de crear su grupo, y los participantes pueden enrolarse a al equipo que se les asigne.

Figura 20

Configuración de equipos



Nota. Se pueden crear el número de equipos que sean necesarios.

Creación de usuarios: Se habilitó el registro automático para los participantes.

Pruebas de acceso: Se verificó el acceso desde la red interna y vía internet.

La implementación técnica del Cyber Range UTN permitió construir un entorno seguro, aislado y funcional para desarrollar competencias en ciberseguridad mediante retos prácticos. Este anexo documenta las decisiones técnicas y operativas que sustentan la infraestructura de la plataforma.

Anexo C. Matriz de escenarios basados en MITRE ATT&CK

En este anexo se presenta una matriz que relaciona los escenarios CTF implementados con las tácticas y técnicas de matriz MITRE ATT&CK. Esta matriz permite identificar de manera clara qué vectores de ataque fueron simulados en cada escenario, facilitando la comprensión y trazabilidad del proceso de diseño de los retos. Su propósito es evidenciar cómo se alinean los escenarios del entorno con un marco reconocido internacionalmente para el análisis de amenazas cibernéticas (ver Tabla 16)

Tabla 16

Escenarios basados en MITRE ATT&CK

Escenario	Táctica MITRE ATT&CK	Técnica	ID Técnica	Descripción breve
Reto 1	Acceso inicial	Exploitation for Public-Facing Application	T1190	Explotación de servicio MySQL vulnerable expuesto.
Reto 1	Ejecución	Remote Services (SSH)	T1021.004	Acceso remoto mediante SSH
Reto 1	Escalada de privilegios	Sudo and Sudo Caching	T1548.003	Uso indebido de privilegios mediante sudo.

Reto 1	Descubrimiento	System information Discovery	T1082	Obtención de información del sistema comprometido
Reto 2	Acceso inicial	Explotation of Remote Services	T1210	Acceso mediante servicio FTP con login anónimo.
Reto 2	Exfiltración	Exfiltration Over Unencrypted	T1048.003	Descarga de archivos sin cifrado desde FTP.

Nota. La codificación de técnicas y tácticas corresponde al framework MITRE ATT&CK para entornos Linux.

Anexo D. Guía de creación de escenarios CTF.

Este anexo describe el proceso seguido para diseñar e implementar los escenarios de entrenamiento CTF utilizados en el entorno Cyber Range UTN. Los escenarios se alinean con técnicas del marco MITRE ATT&CK y fueron integrados en las máquinas vulnerables y en la plataforma CTFd. Se documentan tanto las configuraciones internas de las máquinas como los pasos seguidos en la creación de los retos dentro de la plataforma CTFd.

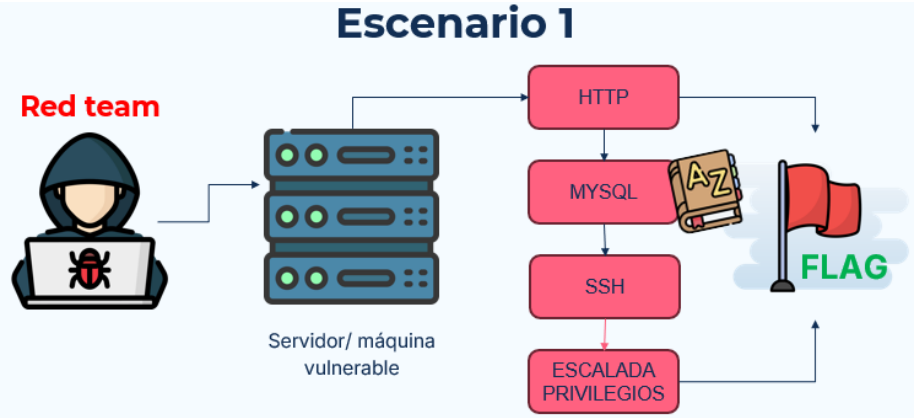
Escenario 1: Explotación de múltiples servicios y escalada de privilegios.

- Objetivo: Simular un entorno donde el atacante deba comprometer una base de datos MySQL, obtener credenciales, acceder vía SSH y escalar privilegios en el sistema.
- Técnicas ATT&CK utilizadas: Reconocimiento (TA0043), Acceso inicial (TA0001), Ejecución (TA0002)
- Servicios activados:
    - SSH, MySQL, Apache
- Flag 1: Ubicada en la versión del servidor web
- Flag 2: Ubicada en /var/www/html/index.html
- Flag 3: Requiere escalamiento de privilegios usando sudo.

Para este escenario se plantea generar una máquina que tenga diferentes servicios vulnerables, y el atacante deba comprometer primero el servicio de mysql, luego ssh para acceder a la máquina y luego ejecutar comandos para escalar privilegios, la arquitectura de este primer escenario se muestra en la Figura 21.

Figura 21

Arquitectura Escenario 1



Nota. En el gráfico se observan los servicios expuestos y cómo seguir la línea de acción para comprometer la máquina.

Creación de usuario 1: En la máquina Reto 1, se crea el primer usuario "santiago" cuya contraseña debe estar en el diccionario "rockyou.txt". Este proceso de creación se muestra en la Figura 22.

Figura 22

Creación de usuario Santiago - Reto1

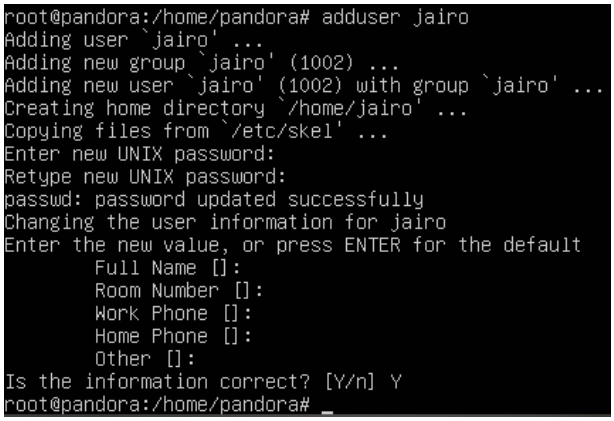
```
root@pandora:/home/pandora# adduser santiago
Adding user `santiago' ...
Adding new group `santiago' (1001) ...
Adding new user `santiago' (1001) with group `santiago' ...
Creating home directory `/home/santiago' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for santiago
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
root@pandora:/home/pandora# _
```

Nota. En la figura se observa la creación del primer usuario llamado Santiago

Creación de usuario 2: Creación de un nuevo usuario, cuya contraseña no se encuentre dentro del diccionario “rockyou.txt”, ver Figura 23.

Figura 23

Creación usuario Jairo

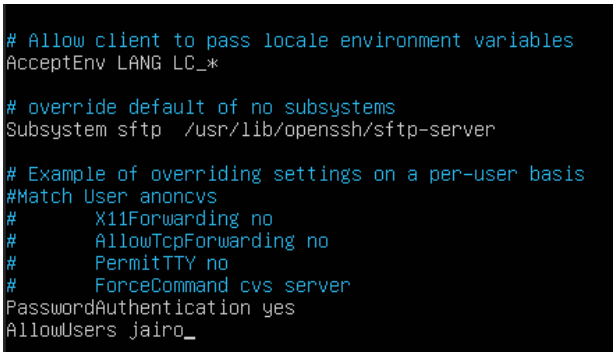


Nota. En la figura se observa la creación del usuario Jairo.

Habilitar SSH solo a usuario Jairo: Para permitir que solo el usuario “Jairo” pueda ingresar por ssh a la máquina, se configura el archivo “nano /etc/ssh/sshd_config”, y se agrega al final del archivo la línea de comando “AllowUsers jairo” como se muestra en la Figura 24. Luego reiniciar el servicio ssh.

Figura 24

Permisos a usuario para acceder por ssh

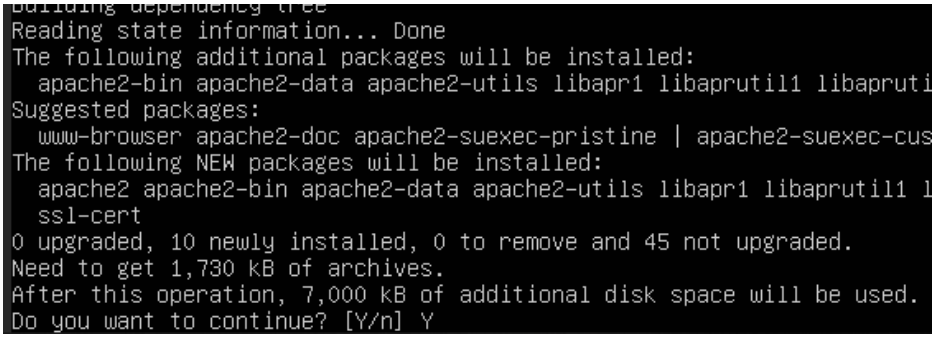


Nota. En la figura se observa como habilitar acceso ssh al usuario Jairo.

Servidor Web: Instalar un servidor web, esto se muestra en la Figura 25.

Figura 25

Instalación de servidor Apache

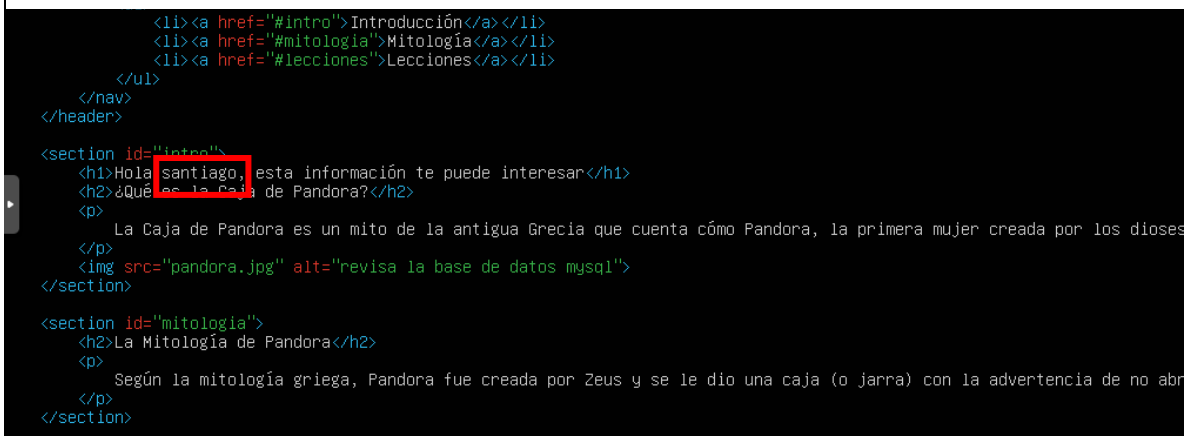


Nota. En la figura se observa la instalación de un servidor web.

Creación de página web: Para hacer el reto más atractivo se crea una página web sencilla donde se colocan pistas para resolver la máquina, la primera pista es introducir el nombre de “Santiago” en la página como se muestra en la Figura 26.

Figura 26

Código HTML de página web

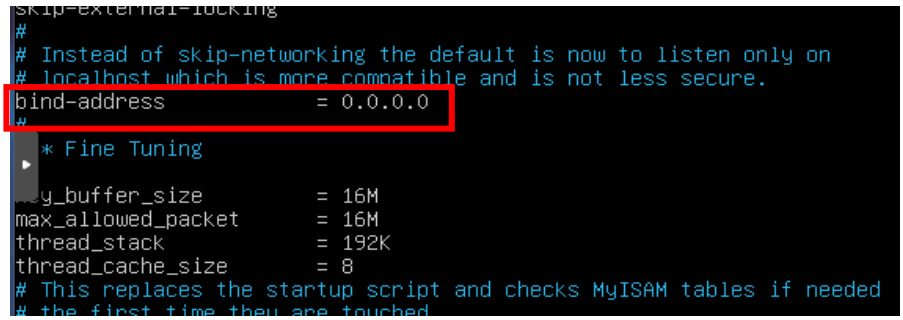


Nota. En la figura se observa parte del código html de la página creada donde se coloca un título “Hola Santiago, esta información te puede interesar”.

Instalación de mysql: Se instala mysql con el comando “apt install mysql-server”, luego de ello es necesario editar el archivo de configuración de mysql, este se encuentra en la ruta “/etc/mysql/mysql.conf.d/mysql.cnf”. Se cambia la configuración como lo muestra la Figura 27.

Figura 27

Configuración de mysql

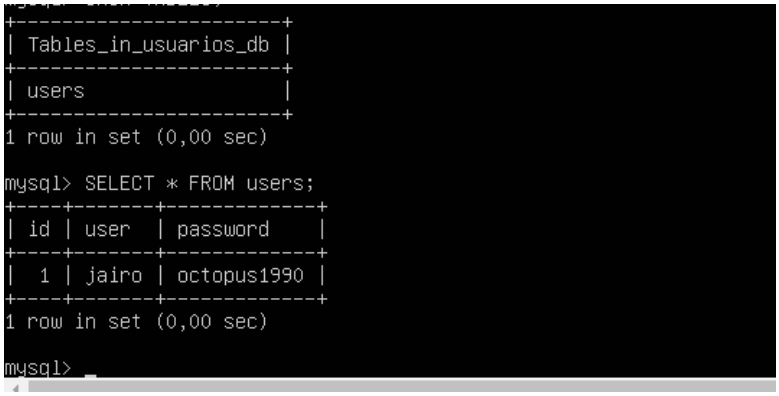


Nota. En la figura se observa que se debe editar el apartado bind-address y cambiarlo por 0.0.0.0, para permitir conexiones desde cualquier IP.

Crear base de datos en mysql: Ahora es necesario crear una base de datos, en donde se albergue información con las credenciales del usuario Jairo creado previamente. La base de datos se muestra en la Figura 28.

Figura 28

Base de datos creada

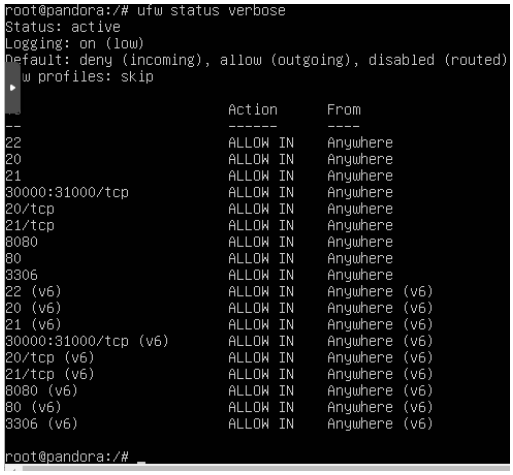


Nota. En la figura se observa la base de datos creada con la tabla usuarios.

Reglas de firewall: Habilitar los puertos de los tres servicios, Ssh, Http y Mysql, se lo realiza con el comando “ufw enable número_puerto”, la Figura 29 muestra el resumen de las reglas de Firewall implementadas en esta máquina.

Figura 29

Reglas de firewall implementadas



Nota. En el gráfico se observa los puertos permitidos, como 22 (ssh), 80(http) y 3306(mysql).

Escenario 2: FTP vulnerable

- Objetivo: Explotar un servicio FTP con acceso anónimo para obtener un archivo que contiene la flag.
- Técnicas ATT&CK utilizadas: Descubrimiento (TA0007), Persistencia (TA0009), Exfiltración (TA0010).
- Configuración:
    - Servicio ftp activado con acceso anónimo.
    - Flag 1: Archivo dentro de la carpeta ftp del servidor (flag.txt).
    - Firewall configurado con puertos específicos abiertos.

Para este escenario 2 se plantea generar una máquina que tenga un servicio vulnerable, el atacante debe identificar dicho servicio y atacarlo, la arquitectura de este escenario se muestra en la Figura 30.

Figura 30

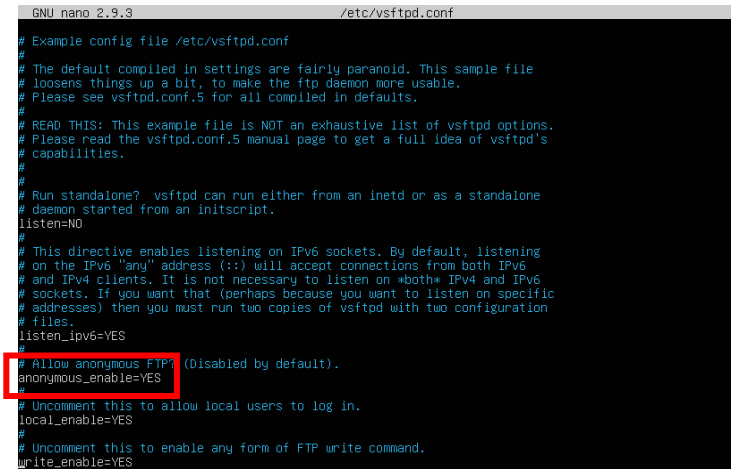
Arquitectura Escenario 2

Nota. En la figura se observa los servicios expuestos, pero solo uno de ellos permite el ataque para encontrar la Flag.

Instalar servicio FTP: Para instalar un servidor FTP, se usa el comando "apt install vsftp" y se habilita el login con usuario anónimo, esto se muestra en la Figura 31.

Figura 31

Configuración de servidor FTP

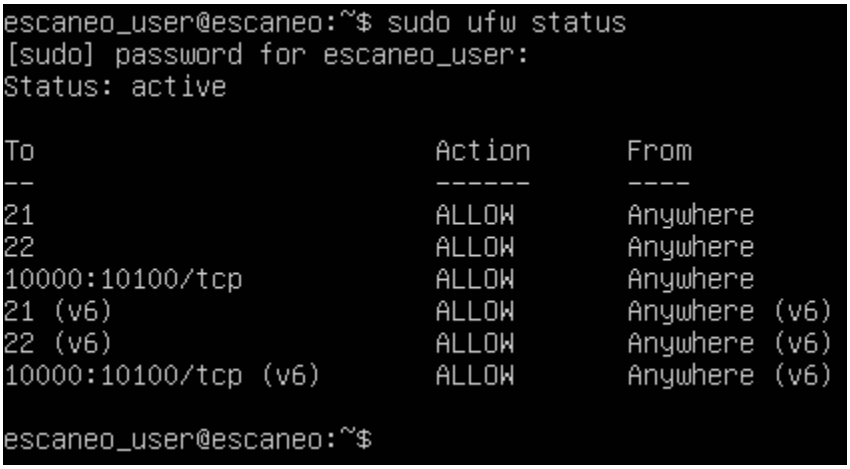


Nota. En la figura se observa cómo se habilita el login por usuario anónimo.

Habilitar reglas de Firewall: La Figura 32 muestra el resumen de las reglas de Firewall implementadas en esta máquina.

Figura 32

Reglas de Firewall Escenario 2



Nota. En la gráfica se observa que el puerto 21 (ftp) se encuentra abierto.

Implementación en la plataforma CTFd: Los escenarios fueron implementados en la plataforma CTFd para su evaluación por parte de los estudiantes. Para ello se realizó:

- Creación de retos: Se accede al panel de administración y se selecciona la sección “Challenges”. Luego se procede a agregar un nuevo reto haciendo clic en “Create Challenge”.

En el formulario de creación de retos se completa la siguiente información:

- **Nombre del reto:** Un título descriptivo para el participante.
- **Categoría:** Se escribe la categoría correspondiente (por ejemplo, Reto 1 o Reto 2)
- **Valor (puntaje):** Se asigna una puntuación según el nivel de dificultad (por ejemplo, 50 puntos).

- **Flag:** Se define la respuesta correcta que los participantes deben encontrar (por ejemplo, FLAG{Apache/2.4.18})

Una vez completado este proceso, el reto queda disponible en la plataforma para los participantes, respetando las fechas configuradas del evento. La Figura 33 presenta el panel de administración, donde se visualizan los retos creados en la plataforma. Por su parte, la Figura 34 muestra la interfaz desde la perspectiva de los participantes, evidenciando cómo se despliegan los retos al momento de ingresar.

Figura 33

Pantalla de administración con retos CTF creados

	ID	Name	Category	Value	Type	State
☐	2	Reconociendo al enemigo	Reto 1	50	standard	visible
☐	3	Pandora: La caja secreta	Reto 1	50	standard	visible
☐	8	Raíces ocultas	Reto 1	300	standard	visible
☐	11	AnonAccess	Reto 2	50	standard	visible

Powered by CTFd
Version 3.7.5

Nota. Configuración interna del panel para Reto 1 y Reto 2

Figura 34

Vista del reto desde perspectiva de participante

Nota. La imagen muestra la interfaz que visualizan los participantes al ingresar a la plataforma CTFd, donde pueden seleccionar y acceder a los distintos retos disponibles dentro del entorno de entrenamiento.

Recomendaciones de diseño

- Verificar que las flags sean accesibles solo después de realizar correctamente las acciones previstas.
- Validar los servicios vulnerables tras reinicio de las máquinas.
- Documentar cada reto con detalle para facilitar futuras actualizaciones o replicación.

La implementación de estos escenarios CTF dentro del entorno Cyber Range UTN permitió a los estudiantes enfrentarse a situaciones simuladas que representan amenazas reales en entornos controlados. Esta experiencia fortaleció el aprendizaje práctico de técnicas de ciberseguridad, aplicando conceptos del marco MITRE ATT&CK y utilizando herramientas profesionales en un ambiente educativo. La estructura modular y el registro automatizado a través de CTFd facilitaron la gestión del evento y el seguimiento del progreso de los equipos conformados.

Anexos de Evaluación del Entorno Cyber Range UTN

Anexo E. Encuesta previa al entrenamiento

En este anexo se incluye la encuesta realizada antes del entrenamiento. Esta encuesta permitió evaluar el nivel de conocimiento inicial de los participantes, sus expectativas y el impacto del entrenamiento en sus habilidades prácticas.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

Carrera de ingeniería en Telecomunicaciones

Proyecto: Desarrollo de un entorno seguro Capture The Flag (CTF) con integración de escenarios de ciberataques basados en mitre att&ck como estrategia de prevención de ciberataques. Caso de estudio: universidad técnica del norte

Objetivo: El objetivo de esta encuesta es evaluar la efectividad y utilidad de la plataforma CTF (Capture The Flag) en la mejora de la conciencia y habilidades en seguridad cibernética. Tus respuestas ayudarán a comprender cómo el entrenamiento en esta plataforma impacta en tu aprendizaje y preparación para enfrentar desafíos de ciberseguridad.

Indicaciones generales

- Responde con sinceridad y detenimiento.
- No hay respuestas correctas o incorrectas; tu opinión es valiosa.
- Las encuestas son anónimas.
- Completa la encuesta antes y después de utilizar la plataforma CTF.

1. ¿Cuál es tu nivel de conocimiento en seguridad cibernética?
    - Principiante
    - Intermedio
    - Avanzado

2. ¿Has participado anteriormente en competencias CTF o entornos de entrenamiento similares?
    - Sí
    - No
3. ¿Qué áreas de seguridad cibernética conoces o has practicado? (Marca todas las que apliquen)
    - Criptografía
    - Análisis de malware
    - Explotación de vulnerabilidades
    - Forense digital
    - Otros: _____
4. ¿Qué esperas aprender o mejorar con el uso de la plataforma CTF?

---

5. ¿Cómo calificarías tu confianza actual para resolver desafíos de seguridad cibernética?
    - Muy baja
    - Baja
    - Neutral
    - Alta
    - Muy alta
6. ¿Cuánto interés tienes en ciberseguridad?
    - Escala de 1 a 5
7. ¿Conoces la matriz MITRE ATT&CK?
    - Sí
    - No
8. ¿Has utilizado herramientas de hacking ético como Kali Linux, Metasploit o Wireshark?
    - Sí

- No

9. ¿Qué esperas aprender en este cyber range?

10. ¿Crees que este tipo de plataformas ayudan a mejorar habilidades en ciberseguridad?
    - Sí
    - No

Elaborado por: Ing. Edison Fuentes	Aprobado por director: MSc. Fabián Cuzme

Anexo F. Tabulación de resultados de la encuesta previa

Se presenta la tabulación de las respuestas obtenidas en la encuesta realizada.

1. ¿Cuál es tu nivel de conocimiento en seguridad cibernética?

Figura 35

Gráfica pregunta 1 – Encuesta previa a entrenamiento

Nota. Figura elaborada por el autor

2. ¿Has participado anteriormente en competencias CTF o entornos de entrenamiento similares?

Figura 36

Gráfica pregunta 2 - Encuesta previa a entrenamiento

Nota. Figura elaborada por el autor

3. ¿Qué áreas de seguridad cibernética conoces o has practicado? (Marca todas las que apliquen)

Figura 37

Gráfica pregunta 3 - Encuesta previa a entrenamiento

Nota. Figura elaborada por el autor

4. ¿Qué esperas aprender o mejorar con el uso de la plataforma CTF?

Tabla 17

Tabulación pregunta 4 - Encuesta previa a entrenamiento

Categoría	Frecuencia (número de respuestas)
Mejorar en ciberseguridad y encontrar vulnerabilidades	1
Conocimientos de ciberseguridad y mitigación de ataques	1
Explorar nuevos temas de ciberseguridad	1
Otras respuestas	6

Nota. Tabla elaborada por el autor

5. ¿Cómo calificarías tu confianza actual para resolver desafíos de seguridad cibernética?

Figura 38

Gráfica pregunta 5 - Encuesta previa a entrenamiento

Nota. Figura elaborada por el autor

6. ¿Cuánto interés tienes en ciberseguridad?

Tabla 18

Tabulación pregunta 6 - Encuesta previa a entrenamiento

Nivel de interés	Frecuencia (número de respuestas)
5	7
4	3
3	0
2	0
1	0
Promedio	4.7

Nota. Tabla elaborada por el autor

7. ¿Conoces la matriz MITRE ATT&CK?

Figura 39

Gráfica pregunta 7 - Encuesta previa a entrenamiento

Nota. Figura elaborada por el autor

8. ¿Has utilizado herramientas de hacking ético como Kali Linux, Metasploit o Wireshark?

Figura 40

Gráfica pregunta 8 - Encuesta previa a entrenamiento

Nota. Figura elaborada por el autor

9. ¿Qué esperas aprender en este cyber range?

Tabla 19

Tabulación pregunta 9 - Encuesta previa a entrenamiento

Categoría	Frecuencia (número de respuestas)
Aprender nuevas habilidades en ciberseguridad	2
Uso de herramientas de ciberseguridad	2
Hacking ético	1
Obtención de Flags	1
Análisis de Malware	1
Aplicación práctica de conocimientos	1

Nota. Tabla elaborada por el autor

10. ¿Crees que este tipo de plataformas ayudan a mejorar habilidades en ciberseguridad?

Figura 41

Gráfica pregunta 10 - Encuesta previa a entrenamiento

Nota. Figura elaborada por el autor

Anexo G. Encuesta posterior al entrenamiento

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

Carrera de ingeniería en Telecomunicaciones

Proyecto: Desarrollo de un entorno seguro Capture The Flag (CTF) con integración de escenarios de ciberataques basados en mitre att&ck como estrategia de prevención de ciberataques. Caso de estudio: universidad técnica del norte

Objetivo: El objetivo de esta encuesta es evaluar la efectividad y utilidad de la plataforma CTF (Capture The Flag) en la mejora de la conciencia y habilidades en seguridad cibernética. Tus respuestas ayudarán a comprender cómo el entrenamiento en esta plataforma impacta en tu aprendizaje y preparación para enfrentar desafíos de ciberseguridad.

Indicaciones generales

- Responde con sinceridad y detenimiento.
- No hay respuestas correctas o incorrectas; tu opinión es valiosa.
- Las encuestas son anónimas.
- Completa la encuesta antes y después de utilizar la plataforma CTF.

1. ¿Cómo calificarías la facilidad de uso de la plataforma CTF?
    - Muy difícil
    - Difícil
    - Neutral
    - Fácil
    - Muy fácil
2. ¿Qué áreas de seguridad cibernética practicaste durante el entrenamiento? (Marca todas las que apliquen)
    - Criptografía
    - Análisis de malware
    - Explotación de vulnerabilidades

- Forense digital
- Otros: _____

3. ¿Consideras que el entrenamiento mejoró tus habilidades en seguridad cibernética?
    - Sí, significativamente
    - Sí, un poco
    - No estoy seguro
    - No, no mejoró
4. ¿En qué áreas específicas sientes que mejoraste? (Describe brevemente)

---

5. ¿Cómo calificarías tu nivel de conciencia sobre amenazas cibernéticas después del entrenamiento?
    - Muy baja
    - Baja
    - Neutral
    - Alta
    - Muy alta
6. ¿Qué aspectos de la plataforma CTF consideras que podrían mejorarse?

---

7. ¿Recomendarías esta plataforma a otros estudiantes?
    - Sí
    - No
    - Tal vez

Elaborado por:	Aprobado por director:
Ing. Edison Fuentes	MSc Fabián Cuzme

Anexo H. Tabulación de resultados de la encuesta posterior

1. ¿Cómo calificarías la facilidad de uso de la plataforma CTF?

Figura 42

Gráfica pregunta 1 - Encuesta posterior al entrenamiento

Nota. Figura elaborada por el autor

2. ¿Qué áreas de seguridad cibernética practicaste durante el entrenamiento?

Figura 43

Gráfica pregunta 2 - Encuesta posterior al entrenamiento

Nota. Figura elaborada por el autor

3. ¿Consideras que el entrenamiento mejoró tus habilidades en seguridad cibernética?

Figura 44

Gráfica pregunta 3 - Encuesta posterior al entrenamiento

Nota. Figura elaborada por el autor

4. ¿En qué áreas específicas sientes que mejoraste? (Describe brevemente)

Tabla 20

Tabulación pregunta 4 - Encuesta posterior al entrenamiento

Categoría	Frecuencia (número de respuestas)
Análisis de vulnerabilidades	4
Identificación de vulnerabilidades	2
Explotación de vulnerabilidades	1
Seguridad y mitigación de vulnerabilidades	1
Seguridad de puertos	1

Nota. Tabla elaborada por el autor

5. ¿Cómo calificarías tu nivel de conciencia sobre amenazas cibernéticas después del entrenamiento?

Figura 45

Gráfica pregunta 5 - Encuesta posterior al entrenamiento

Nota. Figura elaborada por el autor

6. ¿Qué aspectos de la plataforma CTF consideras que podrían mejorarse?

Tabla 21

Tabulación pregunta 6 - Encuesta posterior al entrenamiento

Categoría	Frecuencia (número de respuestas)
Ninguna mejora necesaria	3
Incluir más retos en la plataforma	1
Agregar video tutoriales y guías	1
Explicación de ataques antes de realizarlos	1
Mayor competitividad con otros grupos	1
Incorporar más comandos avanzados en Linux	1
No mencionó mejoras específicas	1

Nota. Tabla elaborada por el autor

7. ¿Recomendarías esta plataforma a otros estudiantes?

Figura 46

Gráfica pregunta 7 - Encuesta posterior al entrenamiento

Nota. Figura elaborada por el autor

Anexo I. Informe de participantes en el entrenamiento

UNIVERSIDAD TÉCNICA DEL NORTE
Facultad de Ingeniería y Ciencias Aplicadas
PLATAFORMA CTF
ENTRENAMIENTO

Estudiantes: Esteban Vizcaíno, Nahim Gómez

16 de marzo de 2025

1. Nombre de la práctica

Entrenamiento de vulnerabilidades mediante el uso de plataformas CTF.

2. Objetivos

El objetivo de esta práctica es fortalecer las habilidades en ciberseguridad mediante la resolución de retos en plataformas CTF (Capture The Flag). Específicamente, se busca:

- Desarrollar la capacidad de identificación de vulnerabilidades en sistemas y aplicaciones.
- Aplicar herramientas de análisis de seguridad como Nmap, Hydra y técnicas de escaneo de puertos.
- Explorar métodos de explotación de servicios vulnerables, como FTP con acceso anónimo y servidores web desprotegidos.
- Mejorar la comprensión de técnicas de enumeración, fuerza bruta y escalamiento de privilegios.
- Familiarizarse con buenas prácticas de seguridad ofensiva y defensiva en entornos controlados.

3. Marco Teórico

Las plataformas CTF (Capture The Flag) son entornos diseñados para la práctica de seguridad informática mediante la resolución de desafíos que simulan escenarios del mundo real. Estos desafíos pueden incluir el análisis de tráfico, explotación de vulnerabilidades y obtención de privilegios en sistemas comprometidos.
Algunas de las herramientas utilizadas en esta práctica incluyen:

3.1. Nmap

Nmap (Network Mapper) es una herramienta de código abierto utilizada para el escaneo de redes y detección de servicios. Permite descubrir puertos abiertos, versiones de software y configuraciones de seguridad.

3.2. Hydra

Hydra es una herramienta utilizada para ataques de fuerza bruta en servicios autenticados. Permite probar múltiples combinaciones de usuario y contraseña en protocolos como SSH, FTP y HTTP.

1

3.3. Fuerza Bruta y Enumeración

Las técnicas de fuerza bruta consisten en probar sistemáticamente combinaciones de credenciales hasta encontrar una válida. La enumeración es el proceso de obtener información útil sobre el sistema objetivo, como nombres de usuarios y configuraciones de servicio.

3.4. Escalamiento de Privilegios

El escalamiento de privilegios ocurre cuando un atacante, tras obtener acceso a un sistema con privilegios bajos, explota una vulnerabilidad para obtener acceso de administrador o root. Esto puede lograrse mediante la manipulación de archivos de configuración, explotación de vulnerabilidades del sistema operativo o credenciales mal protegidas.

4. Desarrollo

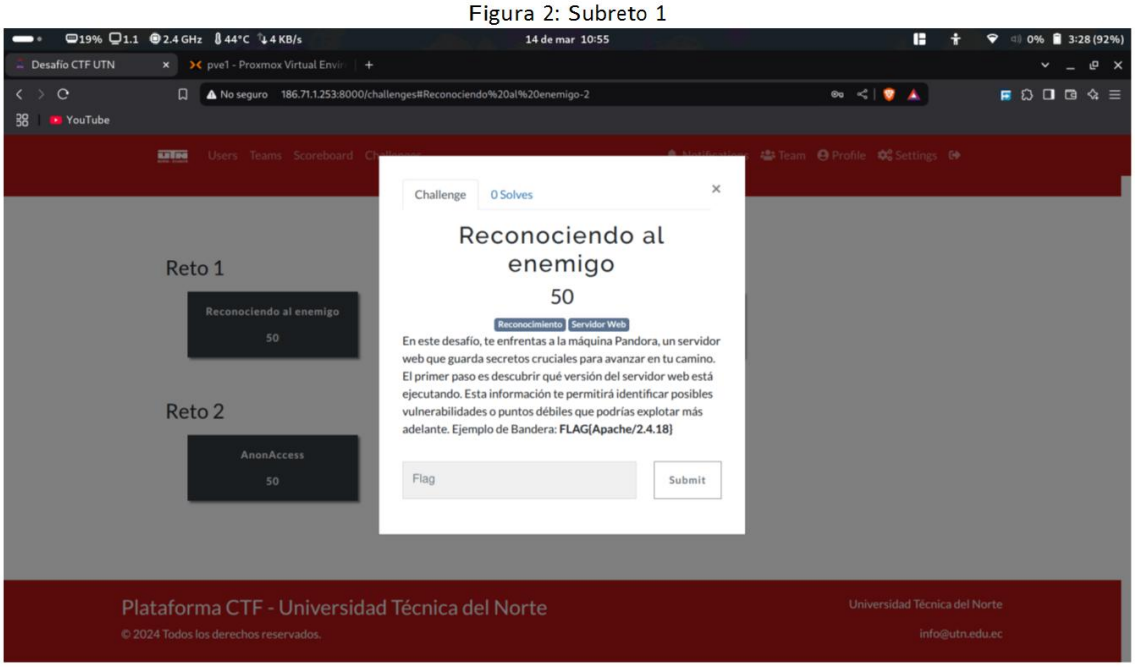
4.1. Reto 1

El primer reto estaba conformado por 3 subretos en los cuales el objetivo era encontrar la FLAG.

El primer subreto tenia como objeivo realizar un escaneo de puertos al servidor mediante la herramienta Nmap, se realizo un escaneo de los puertos 21, 22, 3306, 80. Al terminar el escaneo se encontró la versión del servidor web la cual fue la FLAG para completar el primer subreto.

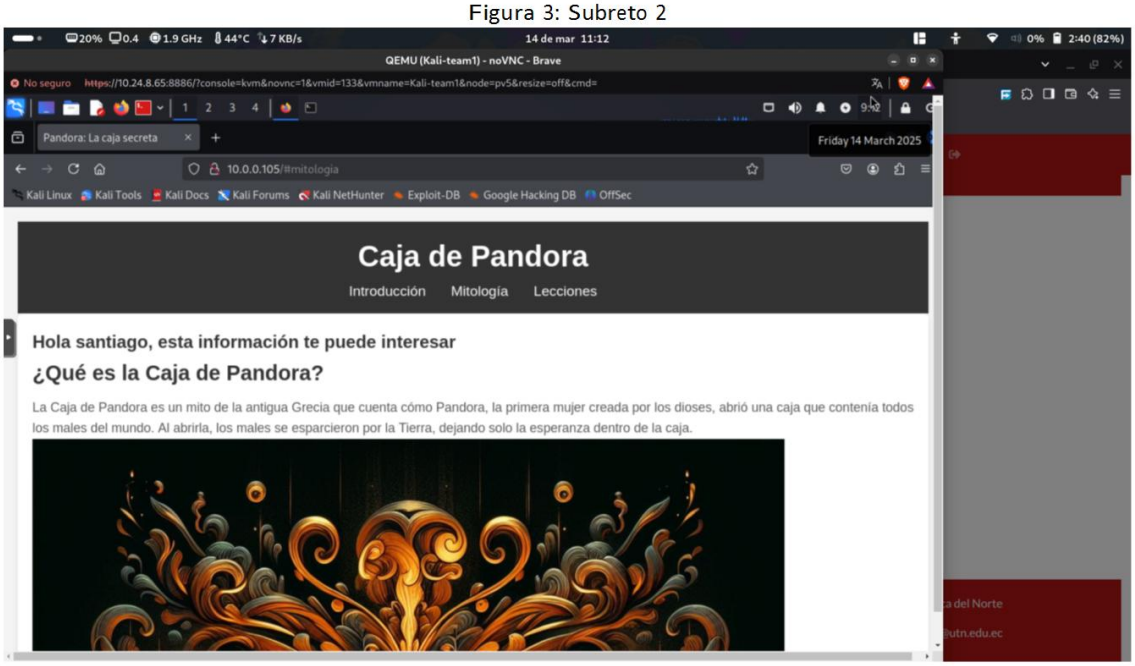
Figura 1: Escaneo de Puertos

Figura 2: Subreto 1



Para poder encontrar la FLAG del segundo subreto ingresamos a la pagina web del servidor y mediante inspeccionar elemento del navegador se reviso el código html y se encontró la FLAG al final del mismo.

Figura 3: Subreto 2



El tercer subreto consistía en utilizar hydra y un diccionario de contraseñas para poder encontrar una clave que correspondiera al usuario ”Santiago”para poder acceder a una base de datos MySQL, una vez obtenida la contraseña de la base de datos accedimos a la tabla de usuarios donde conseguimos el usuario y contraseña de un

Figura 5: Descifrado de contraseña para .^nonymous”mediante Hydra

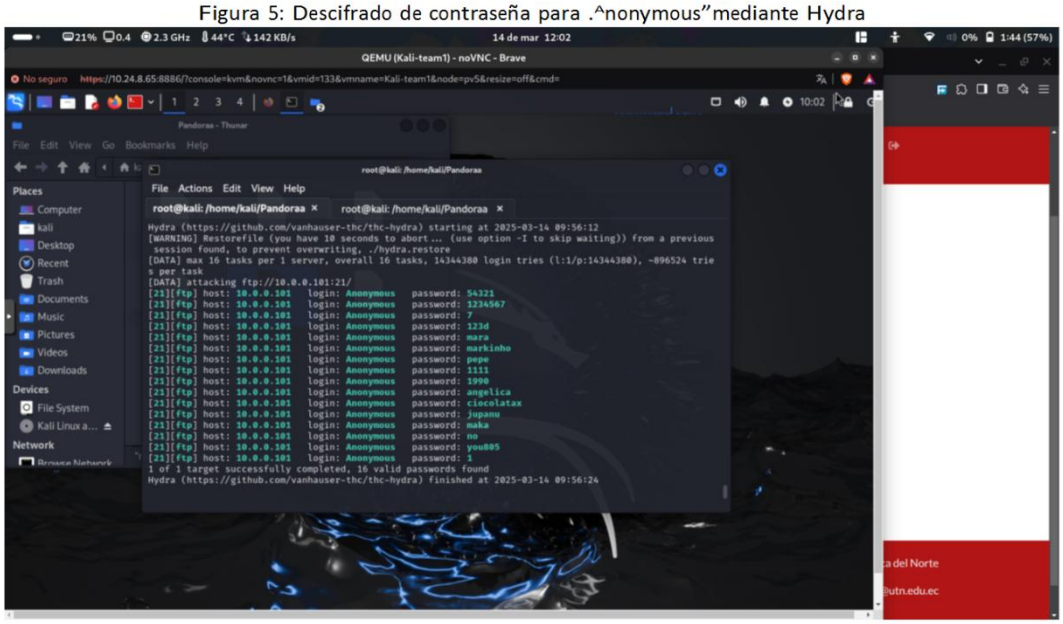
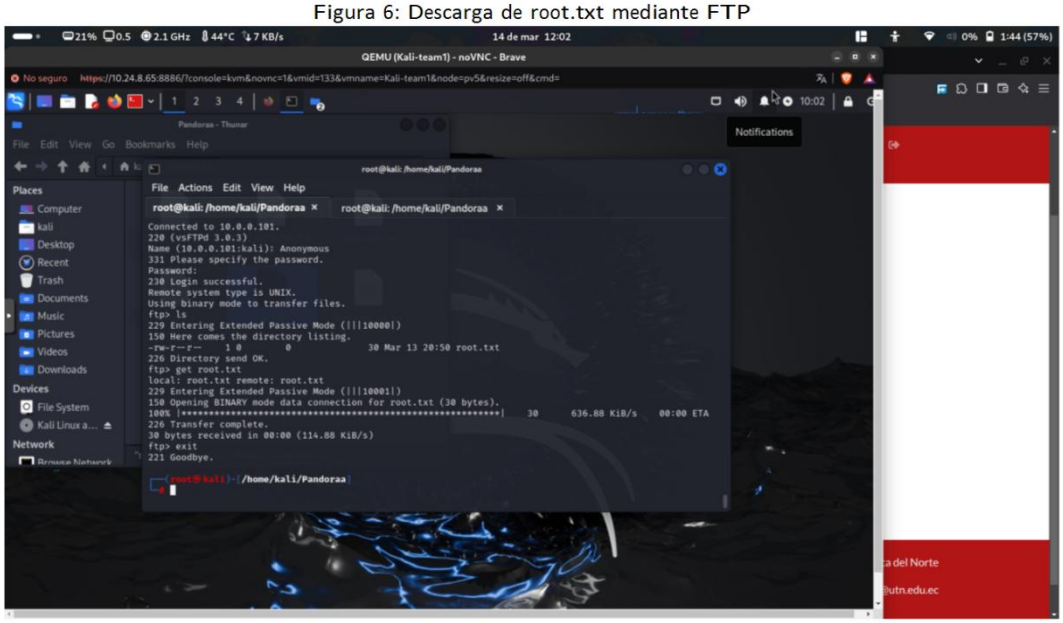


Figura 6: Descarga de root.txt mediante FTP



5. Resultados

Durante la práctica, se lograron completar los retos planteados en la plataforma CTF, obteniendo las respectivas FLAGS como evidencia de la explotación exitosa de vulnerabilidades. Los resultados obtenidos fueron los siguien-

tes:

- Se identificaron puertos abiertos y servicios vulnerables mediante escaneo con Nmap.
- Se extrajo información sensible desde el código fuente de páginas web mediante técnicas de inspección de elementos.
- Se utilizó Hydra para realizar ataques de fuerza bruta exitosos sobre servicios FTP y SSH.
- Se accedió a bases de datos MySQL y se extrajeron credenciales que permitieron el acceso al sistema objetivo.
- Se logró escalar privilegios hasta obtener acceso root, permitiendo la visualización de archivos protegidos que contenían las FLAGS.

Estos resultados demuestran la efectividad de las herramientas y técnicas utilizadas para la identificación y explotación de vulnerabilidades en entornos controlados.

Figura 7: Resultados

6. Conclusiones

La práctica de retos CTF permite mejorar las habilidades en seguridad informática de manera controlada y didáctica. A través de los retos realizados, se identificaron vulnerabilidades comunes en servidores web y servicios FTP, destacando la importancia de aplicar medidas de seguridad como:

- Mantener los sistemas actualizados para evitar vulnerabilidades explotables.
- Restringir accesos a servicios críticos, como la autenticación anónima en FTP.
- Implementar políticas de contraseñas seguras para evitar ataques de fuerza bruta.
- Monitorizar el tráfico y registros del sistema para detectar accesos no autorizados.

El uso de herramientas como Nmap e Hydra fue clave para la identificación de vulnerabilidades y explotación de sistemas, demostrando la importancia de conocer estas técnicas tanto para pruebas de penetración como para la defensa de infraestructuras. Finalmente, se concluye que la formación continua en ciberseguridad es fundamental para enfrentar los desafíos en el ámbito de la seguridad informática actual.

Anexo J. Manuales de resolución de los retos 1 y 2

INGENIERÍA EN TELECOMUNICACIONES

MANUAL DE RESOLUCIÓN RETO 1

Máquina Pandora

Estudiante:

Período Académico:

Nombre del escenario: Máquina Pandora

Objetivos del escenario: Aplicar técnicas de reconocimiento, análisis de servicios y escalada de privilegios para comprender una máquina vulnerable, accediendo a tres banderas tipo CTF.

Materiales y equipos:

- Computador personal o de laboratorio
- Máquinas atacantes, vulnerables virtualizadas
- Plataforma CTFd

Pasos del reto:

Paso 1: Conectarse a la red de Eduroam y acceder al entorno de Proxmox de CITEL (IP: 10.24.8.65:8886) para conectarse a la máquina atacante (Kali Linux) con las credenciales proporcionadas por el instructor.

Paso 2: Acceder a la plataforma CTFd (IP: 186.71.1.253:8000) y visualizar los desafíos del Reto 1 como se muestra en la Figura 47.

Figura 47

Desafíos de Reto 1

Nota. Se puede apreciar que para este reto se encuentran disponibles 3 banderas.

Paso 3: Resolver la primera bandera "Reconociendo al enemigo" (ver Figura 48)

Figura 48

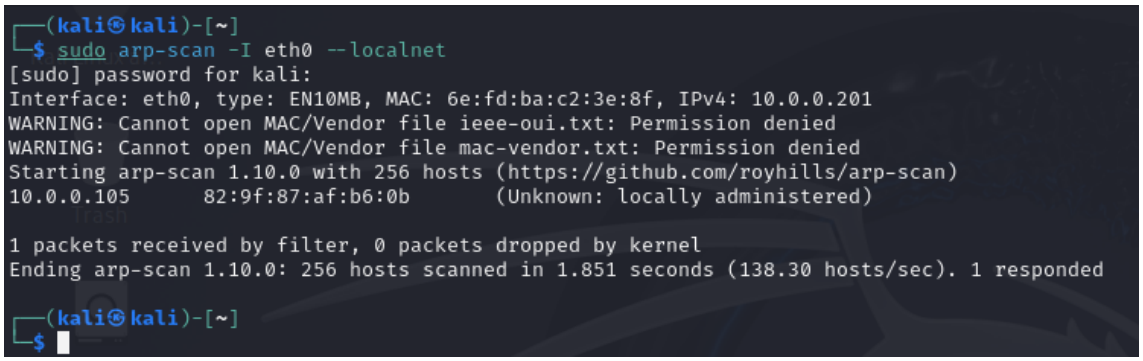
Primer desafío (Reconociendo al enemigo)

Nota. En este primer desafío es necesario conocer la versión del servidor web de la máquina vulnerable.

Paso 4: Desde la máquina de Kali, se puede buscar la versión de Apache, al realizar un escaneo de puertos y servicios, previamente identificando la dirección IP de la máquina vulnerable asignada (ver Figura 49).

Figura 49

Reconocimiento IP de máquina vulnerable

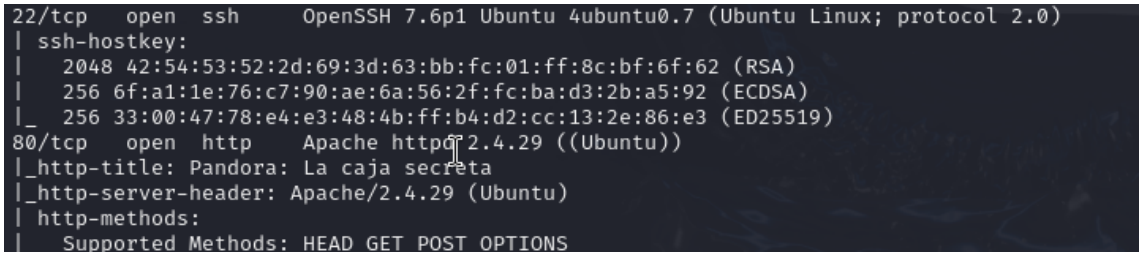


Nota. El comando "*arp-scan -I eth0 –localnet*" busca todos los dispositivos conectados a la misma red local (LAN).

Paso 5: Determinar qué servicios están abiertos (ver Figura 50).

Figura 50

Servicios activos en máquina vulnerable 1



Nota. El comando "nmap -sV 10.0.0.201" muestra que servicios están activos en una máquina Linux.

Con esta información ya se podría resolver la primera bandera.

Paso 6: Resolver la siguiente bandera “Pandora la caja secreta” (ver Figura 51)

Figura 51

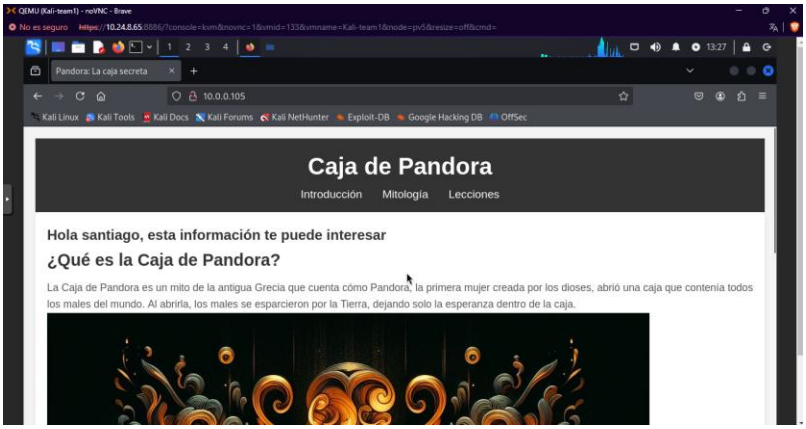
Segundo desafío (La caja secreta)

Nota. Figura elaborada por el autor.

Paso 7: Analizar el texto del reto, al encontrar el servicio de HTTP, sugiere que existe una página web, por lo que se debería visitar la IP 10.0.0.105 y analizar dicha página (ver Figura 52).

Figura 52

Página web de la máquina vulnerable 1

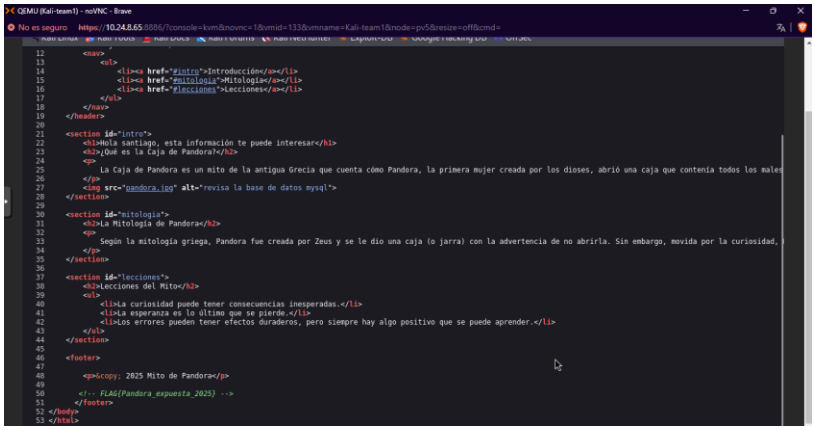


Nota. Analizar información visible en la página.

Se identifica un nombre “santiago” posiblemente un usuario en el sistema. Una buena costumbre es analizar el código fuente de la página (ver Figura 53). En este caso es posible encontrar la bandera.

Figura 53

Código fuente de la página web

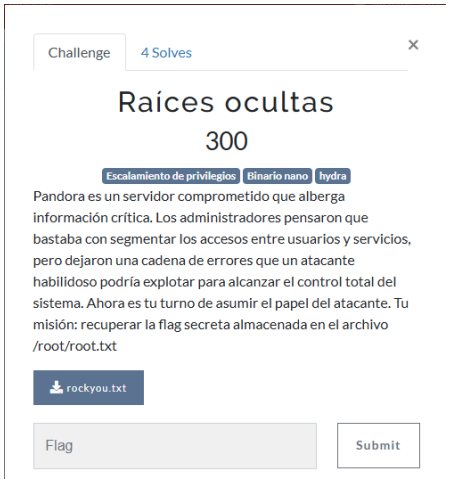


Nota. Al final del código es posible identificar la bandera que soluciona este desafío.

Paso 8: Resolver la última bandera “Raíces ocultas”

Figura 54

Tercer desafío "Raíces ocultas"



Nota. Se puede apreciar en la imagen que se adjunta un diccionario de claves llamado *“rockyou.txt”*.

Paso 9: Con la información obtenida anteriormente, se recomienda hacer uso del diccionario “rockyou” para buscar una contraseña para el usuario “santiago”. Intenta atacar a los servicios detectados previamente. Como recomendación no siempre la contraseña está al inicio del diccionario.

Paso 10: Una vez encontrada la clave de “santiago”, acceder a la base de datos en busca de más credenciales, esta vez de un usuario que pueda acceder por ssh al sistema.

Paso 11: Al encontrar el nuevo usuario, conectarse por ssh a la máquina víctima.

Paso 12: Realizar escalada de privilegios, se puede hacer uso del binario /bin/nano.

Paso 13: Una vez como root, se puede localizar la última bandera.

INGENIERÍA EN TELECOMUNICACIONES

MANUAL DE RESOLUCIÓN RETO 2

Servicio FTP Expuesto

Estudiante:

Período Académico:

Nombre del escenario: Servicio FTP Expuesto

Objetivos del escenario: Aprender a usar herramientas de monitoreo de red para detectar servicios expuestos, como FTP.

Materiales y equipos:

- Computador personal o de laboratorio
- Máquinas atacantes, vulnerables virtualizadas
- Plataforma CTFd

Pasos del reto:

Paso 1: Conectarse a la red de Eduroam para tener acceso a la máquina atacante (Kali Linux).

Paso 2: Acceder a la plataforma CTFd para visualizar el reto.

Figura 55

Desafío Reto 2

Nota. El nombre del desafío indica que está relacionado con el acceso anónimo

Paso 3: Identificar la dirección IP de la máquina vulnerable.

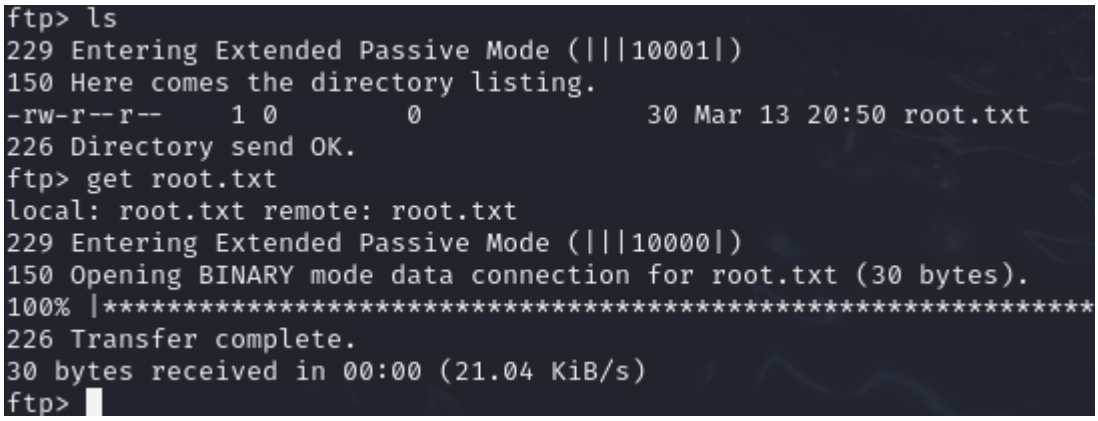
Paso 4: Establecer que servicios se encuentran abiertos.

Paso 5: Analizar resultados y ver el servicio FTP expuesto con el login por usuario anónimo permitido.

Paso 6: Conexión al servicio FTP. Ingresar con el usuario anónimo y contraseña. Listar archivos disponibles. Obtener el archivo. (ver Figura 56)

Figura 56

Acceso a servicio ftp

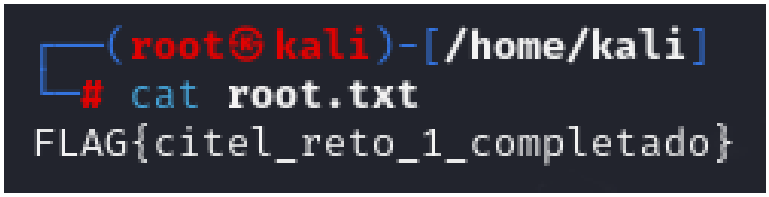


Nota. Con el comando "*ls*" se listan los archivos ubicados en el servidor de ftp, además con "*get nombre_archivo*" se puede descargar el archivo correspondiente para su posterior análisis.

Paso 9: Obtención de bandera (ver Figura 57).

Figura 57

Flag reto 2



Nota. En la imagen se puede apreciar el formato de la bandera que debe ser colocado en la plataforma CTFd para validar la solución del reto y obtener el puntaje establecido.

Anexo K. Registro fotográfico del Entrenamiento

Figura 58

Exposición Cyber Range - CTF UTN

Nota. Figurada elaborada por el autor

Figura 59

Equipo 1 – archlovers

Nota. Figurada elaborada por el autor

Figura 60

Equipo 2 - error 404

Nota. Figurada elaborada por el autor

Figura 61

Equipo 3 – CrushesUTN

Nota. Figurada elaborada por el autor

Figura 62

Equipo 4 – secNet

Nota. Figurada elaborada por el autor

Figura 63

Estudiantes usando la plataforma CTFd

Nota. Figurada elaborada por el autor

Figura 64

Estudiantes realizando desafíos de seguridad informática

Nota. Figurada elaborada por el autor

Figura 65

Grupo de participantes en Cyber Range UTN

Nota. Se puede apreciar en la imagen a los participantes e instructor del evento Cyber Range UTN.