CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

FABIAN ANDRÉS PÉREZ RUIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2023

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

FABIAN ANDRÉS PÉREZ RUIZ

M.Sc. JOHN F. QUINTERO T.
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

RESUMEN

El reporte técnico generado por el "Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team" de la UNAD describe las acciones y rasgos de los equipos interdisciplinarios Red Team y Blue Team en el entorno empresarial, demostrando su relevancia en la prevención y reducción de ataques informáticos.

El informe se organiza en 5 fases que parten de los principios fundamentales de seguridad informática, llegando hasta la socialización de las actividades desplegadas, las cuales partieron de un caso de estudio simulado para ilustrar las herramientas y procedimientos técnicos inherentes a estos equipos.

Las organizaciones colombianas sufren impactos económicos, de productividad y de seguridad cuando son objeto de ciberataques[1]. Por ello, es importante comprender los riesgos asociados con la ciberdelincuencia y la relevancia del trabajo de los equipos de ciberseguridad red team y blue team, el primero busca explotar las vulnerabilidades de seguridad mientras que el segundo se enfoca en proteger los sistemas contra esos ataques; Ambos equipos son importantes para garantizar la seguridad de una organización y se complementan entre sí para proporcionar una estrategia de seguridad completa y eficaz.

la implementación de los equipos Red Team y Blue Team es detectar las vulnerabilidades más importantes y crear un plan de acción para reducir los riesgos y vulnerabilidades en la infraestructura de tecnología de la información de las empresas en Colombia.

[1] Más de 54.000 denuncias de ciberdelitos se registraron a cierre del tercer trimestre de 2022. (2022, diciembre 7). CCIT - Cámara Colombiana de Informática y Telecomunicaciones. https://www.ccit.org.co/noticias/crecieron-28-las-denuncias-de-ciberataques-a-redes-de-telecomunicaciones/

CONTENIDO

TABLA DE ILUSTRACIONES

GLOSARIO

ACCESO NO AUTORIZADO: Entrada en un sistema informático o red sin haber obtenido la debida autorización previa por parte del propietario o administrador. En este sentido, se considera una actividad ilícita y puede ser sancionada por la ley en función de la gravedad de la acción.

ANTIVIRUS: Software que ha sido desarrollado específicamente para identificar, prevenir y eliminar virus y otros programas maliciosos de un sistema informático o red

ATAQUE INFORMÁTICO: Acto deliberado que tiene como objetivo comprometer la seguridad de un sistema o red informática. Estos ataques suelen aprovecharse de vulnerabilidades y debilidades del sistema para acceder a información confidencial o causar daños en la infraestructura tecnológica.

AUTENTICACIÓN: Proceso de verificación de la identidad de un usuario o sistema con el fin de autorizar el acceso a recursos protegidos. Es una medida de seguridad que asegura que solo usuarios autorizados tengan acceso a la información y recursos del sistema

COPNIA: Entidad encargada de la regulación y supervisión de la práctica profesional de la ingeniería en el país. Su objetivo principal es garantizar la ética y calidad en el ejercicio de la ingeniería, así como proteger los intereses del público en general.

CIBERSEGURIDAD: Conjunto de estrategias y medidas adoptadas para proteger los sistemas y redes informáticas de posibles ataques y amenazas, mediante la implementación de técnicas y herramientas especializadas para prevenir, detectar y responder a incidentes de seguridad.

EXPLOIT: código malicioso o técnica que aprovecha una vulnerabilidad en un sistema o aplicación para comprometer la seguridad y permitir que un atacante obtenga acceso no autorizado o realice acciones maliciosas..

FIREWALL: Herramienta de seguridad informática que actúa como una barrera entre una red privada y una red pública. Su función principal es analizar el tráfico de red entrante y saliente para permitir o bloquear el acceso a la red privada según las políticas de seguridad establecidas.

INFORMACIÓN: Conjunto organizado de datos con el propósito de transmitir un mensaje específico o generalizado. La información se compone de elementos estructurados de manera lógica para que puedan ser interpretados por un receptor.

MALWARE : Software malicioso, que se desarrolla con el objetivo de dañar, controlar o tomar control de los sistemas o redes informáticas. Estos programas maliciosos suelen estar diseñados para realizar acciones dañinas, tales como robo de información, espionaje, o toma de control de los sistemas infectados.

PHISHING: Estrategia de ingeniería social que se utiliza para obtener información confidencial, en la que se emplean correos electrónicos o sitios web falsos con el objetivo de engañar a los usuarios. Mediante esta técnica, los atacantes buscan hacerse pasar por entidades de confianza para obtener datos sensibles como nombres de usuario, contraseñas, información financiera o de identidad, entre otros.

SEGURIDAD DE LA INFORMACIÓN : Conjunto de medidas, políticas, prácticas y procedimientos diseñados para proteger la información confidencial y crítica contra el acceso no autorizado, la divulgación, la destrucción, la alteración y otros riesgos que puedan afectar su disponibilidad, integridad y confidencialidad.

VULNERABILIDAD: Debilidad o defecto presente en un sistema o red informática que puede ser utilizado por un atacante para explotar su seguridad y obtener acceso no autorizado a información confidencial, interrumpir el funcionamiento normal del sistema o causar daños en la infraestructura tecnológica.

INTRODUCCIÓN

El presente informe técnico ha sido elaborado con el propósito de presentar una contextualización de los conceptos de ciberseguridad desde el enfoque normativo y jurídico colombiano, abordado una serie de preguntas relacionadas con las leyes de seguridad de la información de este país, especialmente la ley 1273 de 2009, se realiza un análisis personal sobre la aceptación de una oferta laboral en la empresa caso de estudio denominada WhiteHouse Security, considerando la firma de una cláusula de confidencialidad y la realización de tareas asignadas.

Se incluye un análisis del caso de espionaje del ejército colombiano conocido como Operación Andrómeda Buggly, que es relevante en el contexto de la ciberseguridad en Colombia.

En cuanto a la ejecución de pruebas de intrusión, se describe el proceso detallado para encontrar vulnerabilidades en el sistema operativo Windows 7 x64, partiendo de una situación problema planteada en el escenario y la realización de pruebas de intrusión desde el sistema operativo Kali Linux.

como estudiante, he tenido la oportunidad de profundizar en los temas de ciberseguridad, aplicando mis conocimientos en la práctica, lo cual ha sido una experiencia enriquecedora y desafiante.

El informe técnico cubre una amplia variedad de temas relacionados con la ciberseguridad, desde la definición de conceptos hasta la descripción de características y diferencias en cuanto a la contención de ataques informáticos; Espero que este informe contribuya a enriquecer el conocimiento de los lectores interesados en el tema de la ciberseguridad.

JUSTIFICACIÓN

Es fundamental tener un conocimiento profundo de los conceptos básicos y la normativa en torno a la seguridad informática, especialmente en nuestro País; Por lo tanto, es de gran importancia investigar y comprender las definiciones técnicas y jurídicas, las cuales proporcionan una base sólida para ejercer la profesión en seguridad informática.

Es fundamental tener un conocimiento profundo de las normativas colombianas en torno a la seguridad informática y actuar de manera adecuada como empleado tanto en el sector público como privado para evitar cometer delitos que podrían tener consecuencias graves para el desempeño del ingeniero. En este sentido, en Colombia se encuentran vigentes la "Ley 1273 de 2009" y el "Código de Ética" establecido por la entidad COPNIA, los cuales regulan y establecen parámetros éticos en nuestra profesión

El día de hoy, las empresas han convertido en prioridad el salvaguardar los activos de información, con el fin de asegurar su disponibilidad, integridad y confidencialidad.

Para este aseguramiento, es preciso contar con herramientas y personal altamente capacitado en los temas de seguridad informática; En este informe se han recopilado diversas herramientas y elementos necesarios para poder realizar esta tarea con altos niveles de calidad y eficacia, con el objetivo de abordar los desafíos que se presentan en el ámbito de la seguridad informática y garantizar la protección de la información de las empresas.[2]

[2] Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades (1.ª ed.). Editorial Científica 3Ciencias. https://doi.org/10.17993/IngyTec.2018.46

OBJETIVOS

1.1 OBJETIVO GENERAL

Generar una descripción detallada del proceso involucrado en los escenarios propuestos para las actividades del equipo Blue Team y Red Team.

1.2 OBJETIVOS ESPECÍFICOS

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.
- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.
- Reconocer la relevancia de los equipos de ciberseguridad en las empresas para prevenir y contener ataques Informáticos.
- Formular recomendaciones y conclusiones, que aporten a mejorar las estrategias usadas por RedTeam & BlueTeam

2 ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

2.1 DENTRO DEL MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES REDACTE CON SUS PROPIAS PALABRAS QUE LEGISLACIÓN "LEYES, DECRETOS" EXISTEN ACTUALMENTE Y LAS CARACTERÍSTICAS PRINCIPALES DE CADA LEY.

En Colombia, los delitos informáticos están regulados por la Ley 1273 de 2009, que establece un marco legal para la prevención y el castigo de los delitos informáticos y electrónicos en el país

LEY 1273 DE 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."[3]

Artículo 269A	La utilización inapropiada de los sistemas informáticos puede llevar a consecuencias graves. Cuando una persona, que no se encuentra autorizada o no cumple con los términos acordados, accede a un sistema informático protegido o no seguro, o permanece en él en contra de la voluntad de los encargados de administrarlo, está violando las políticas de seguridad informática y puede enfrentar cargos legales
Artículo 269B	La obstrucción ilegal de sistemas informáticos o redes de

[3] POLICIA NACIONAL. Trámites, servicios e información. [en línea]. 10 febrero 2022 Consultado: 11 de febrero de 2023. Disponible en internet: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

	telecomunicaciones es una actividad que puede tener serias consecuencias. Cuando alguien impide o dificulta el funcionamiento normal de sistemas informáticos, datos almacenados en ellos o redes de telecomunicaciones sin autorización, está violando las políticas de seguridad informática y puede enfrentar cargos legales. Es importante respetar las normas establecidas para garantizar el correcto funcionamiento de estos sistemas y redes.
Artículo 269C	La interceptación de datos informáticos sin autorización previa puede ser considerada una actividad ilegal. Cuando una persona interfiere en la transmisión de datos informáticos o en las señales electromagnéticas que se emiten durante el proceso, sin una orden judicial previa, y sin contar con la autorización de los propietarios de los sistemas involucrados, está vulnerando los derechos de privacidad y seguridad de los usuarios y puede enfrentar cargos legales.
Artículo 269D	Causar daños a sistemas informáticos sin autorización previa puede ser considerado un delito. Cuando una persona destruye, daña, borra, deteriora, altera o suprime datos informáticos, sistemas de procesamiento de información, sus partes lógicas o componentes sin tener autorización, está violando las políticas de seguridad informática y puede enfrentar cargos legales.
Artículo 269E	Producir, transportar, distribuir o vender malware u otros programas informáticos que puedan causar

	daños a sistemas informáticos sin autorización previa puede ser considerado un delito. Cuando una persona obtiene, envía, introduce o extrae programas informáticos maliciosos dentro del territorio del país sin autorización, está violando las políticas de seguridad informática y puede enfrentar cargos legales.
Artículo 269F	La violación de datos personales puede ser considerada un delito. Cuando una persona obtiene, recopila, sustrae, ofrece, vende, permuta, envía, compra, intercepta, divulga, modifica o utiliza claves personales contenidas en documentos, archivos, bases de datos o medios análogos sin tener derecho a hacerlo, está vulnerando la privacidad y seguridad de los usuarios y puede enfrentar cargos legales.
Artículo 269G	La suplantación de identidad en un sitio web con el fin de obtener datos personales puede ser considerada un delito. Cuando una persona diseña, desarrolla, transmite, vende, ejecuta, programa o envía páginas electrónicas, enlaces o pop-ups con fines ilícitos y sin tener derecho a hacerlo, está vulnerando la privacidad y seguridad de los usuarios y puede enfrentar cargos legales.
Artículo 269H	Las penas establecidas por las disposiciones de este título pueden ser aumentadas entre la mitad y las tres cuartas partes. Este incremento en las penas tiene como objetivo

	agravar la sanción impuesta al infractor, en función de la gravedad del delito y las circunstancias específicas del caso.
Artículo 269I	El robo por medios informáticos y similares es considerado un delito. Cuando una persona vulnera las medidas de seguridad informática manipulando sistemas informáticos, redes de sistemas electrónicos y realizando los actos previstos en la ley, está cometiendo un delito y puede enfrentar cargos legales.
Artículo 269J	La transferencia involuntaria de bienes es considerada un delito. Cuando una persona realiza operaciones informáticas o utiliza medios similares para transferir activos sin el consentimiento de un tercero, con ánimo de lucro y en perjuicio del mismo, está vulnerando la propiedad y puede enfrentar cargos legales.

Ley 527 de 1999

la misma fue firmada y expedida en la república de Colombia en el año 1999 el 18 de agosto la cual trata sobre la reglamentación del acceso y uso de datos, comercio electrónico y firmas digitales por último se estableció cuáles serán las entidades certificadas para tales fines y otras disposiciones

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, también del comercio electrónico, de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 962 de 2005

Fue expedida en la república de Colombia el día 8 de julio del 2005, por medio de la cual se establecieron disposiciones legales en base a los trámites administrativos

de los organismos y entidades del Estado particularmente para los que son funcionarios públicos.

Ley 1341 de 2009

Fue expedida en la república de Colombia el día 30 de julio del 2009, "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones."[4]

Ley 1581 de octubre 17 de 2012

Fue expedida en la república de Colombia del día 17 de octubre del año 2012, por medio de la cual se prohíbe la trasferencia de datos a países que no tiene regulados la protección de datos. "Esta prohibición **NO** REGIRÁ cuando se trate de: Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia."

Decreto 1377 de 2013

En 2013 se emitió una regulación en Colombia que complementa la Ley 1581 de 2012. Esta regulación tiene como finalidad establecer los procedimientos para que todas las personas tengan acceso a la información que se ha recopilado sobre ellas en bases de datos o archivos, y puedan actualizar o corregir dicha información de acuerdo con los derechos y garantías constitucionales establecidos en el artículo 15 de la Constitución.

DOCUMENTO COMPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL

"La política nacional de seguridad digital, objeto de este documento, cambia el enfoque tradicional al incluir la GESTIÓN DEL RIESGO como uno de los elementos más importantes para abordar la seguridad digital. • Las estrategias para alcanzar su objetivo principal son: Fortalecer las capacidades de las múltiples partes interesadas, para: • Identificar • Gestionar • Tratar • Mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital."[5]

---

[4] COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones Ley 1341 de 2009 [online]. MINTIC, julio 30 del 2009. Consultado el 11 de febrero de 2023. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913 11

[5] JARAMILLO, Alejandro. CONPES 3854copyright © 2016, fireeye, inc. all rights reserved. de la protección reactiva a la respuesta proactiva junto a fireeye. [en línea]. 2014 Consultado: 09

DOCUMENTO COMPES 3995 POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL

“El documento contiene un análisis de la situación actual del país respecto a la seguridad digital, en el que se destacan las debilidades existentes y se establecen los objetivos de la política propuesta. Asimismo, se presenta un Plan de Acción a corto plazo para los próximos dos años, con medidas concretas para: (i) mejorar las capacidades de seguridad digital de los ciudadanos, el sector público y el sector privado; (ii) actualizar el marco de gobernanza en materia de seguridad digital; y (iii) analizar la adopción de modelos, estándares y marcos de trabajo en seguridad digital, prestando especial atención a las nuevas tecnologías para preparar al país ante los desafíos de la llamada Cuarta Revolución Industrial”[6]

2.2 EN EL MUNDO DE LA CIBERSEGURIDAD EXISTEN PROCESOS DEFINIDOS PARA PODER EJECUTAR DE FORMA ORGANIZADA LO QUE SE CONOCE COMO PRUEBAS DE PENETRACIÓN O PENTESTING; USTED COMO FUTURO EXPERTO DEBERÁ REDACTAR CON SUS PALABRAS Y DEFINIR CADA UNA DE LAS ETAPAS DEL PENTESTING, DENTRO DE LA DEFINICIÓN INCORPORARÁ UN EJEMPLO DE UNA HERRAMIENTA QUE SE UTILICE PARA CADA UNA DE LAS ETAPAS DEL PENTESTING.

proceso de evaluación de seguridad que busca identificar las vulnerabilidades y debilidades en un sistema o aplicación informático. El objetivo principal es simular un ataque malintencionado para evaluar la efectividad de los controles de seguridad actuales y determinar el impacto potencial de un ataque exitoso.

El pentesting es realizado por profesionales de seguridad cibernética, que utilizan una combinación de herramientas automatizadas y técnicas manuales para simular un ataque y evaluar la capacidad del sistema o aplicación para resistir la explotación. Los resultados del pentesting se utilizan para identificar y corregir las debilidades de seguridad y mejorar la defensa contra ataques reales.

---

de febrero de 2023. Disponible en internet: https://www.minambiente.gov.co/images/tecnologias-de-la-informacion-y-comunicacion/pdf/conpes_3854_politica_nacional_seguriad_digital.pdf

[6] PROGRESO. Confianza y Seguridad Digital. Documento CONPES 3995 Consejo Nacional de Política Económica y Social (CONPES) [en línea]. Consultado: 09 de febrero de 2023. Disponible en internet: http://www.fundacionmicrofinanzasbbva.org/revistaprogreso/confianza-seguridad-digital-documento-conpes-3995/

Es importante destacar que el pentesting solo debe ser realizado con el permiso previo y autorización del propietario del sistema o aplicación, y debe seguir una metodología estricta para evitar dañar el sistema o aplicación durante el proceso de evaluación.

Fases de pentesting

1. **FASE: RECOPILACIÓN DE INFORMACIÓN / ENUMERACIÓN**

La recopilación de información involucra la obtención de información previa sobre el sistema o aplicación a ser evaluado, incluyendo la topología de red, la versión de software, los servicios en ejecución.

La enumeración se refiere a la identificación de los recursos y servicios activos en el sistema o aplicación, como servidores, puertos abiertos, servicios de correo electrónico.

La recopilación de información y la enumeración proporcionan una visión general de los componentes y recursos del sistema permiten a los profesionales de seguridad informática identificar posibles puntos débiles y objetivos de ataque.

Es fundamental respetar los términos y condiciones acordados previamente con el propietario del sistema y seguir una metodología rigurosa para evitar dañar el sistema durante el proceso de evaluación.

En esta etapa, se emplean algunas de las herramientas más populares, tales como:

Nmap: herramienta de código abierto que se utiliza para explorar redes, realizar inventario de dispositivos y servicios, y detectar vulnerabilidades.

Whois: permite consultar información sobre el propietario de un dominio o dirección IP.

nslookup: utilidad de línea de comandos que se utiliza para obtener información de resolución de nombres de dominio (DNS) de un servidor DNS

theHarvester: una herramienta de recopilación de información que busca información en diferentes fuentes, incluyendo motores de búsqueda, redes sociales, y directorios de correo electrónico.

Metasploit: una plataforma de pruebas de penetración que incluye numerosas herramientas de recopilación de información y enumeración, así como la capacidad de llevar a cabo pruebas de explotación.

2. FASE: ANÁLISIS DE VULNERABILIDADES

Se trata de ejecutar todas las acciones posibles para poner en riesgo el objetivo, sus usuarios o su información.

En esta fase se utilizan diversas herramientas que son comúnmente empleadas.:

Nessus herramienta de escaneo de vulnerabilidades que se utiliza para evaluar y detectar vulnerabilidades en sistemas y redes

OWASP ZAP (Zed Attack Proxy) es una herramienta gratuita y de código abierto utilizada para identificar y explotar vulnerabilidades en aplicaciones web. Proporciona una amplia gama de funcionalidades, incluyendo la inyección de payloads, la identificación de vulnerabilidades conocidas, la exploración de sitios web y la realización de pruebas de seguridad automatizadas y manuales.

Burp Suite proporciona un conjunto integral de herramientas para interactuar y manipular solicitudes HTTP, automatizar pruebas de seguridad y realizar otras actividades para identificar y explotar vulnerabilidades en aplicaciones web. Las herramientas proporcionadas por Burp Suite incluyen un proxy de interceptación, un escáner de aplicaciones web, una herramienta de intrusión, una herramienta de repetición entre otras

3. FASE: EXPLOTACIÓN DE VULNERABILIDADES

La explotación de vulnerabilidades se refiere al proceso de aprovechar una debilidad en un sistema o aplicación informático para ganar acceso no autorizado o causar daños.
Durante esta fase, se llevan a cabo acciones para comprometer los sistemas objetivos mediante la explotación de vulnerabilidades identificadas o el uso de credenciales obtenidas previamente. Para ello, se utilizan diversas herramientas como OpenVAS, Nessus, BeEF, Metasploit Framework, Routersploit, PowerSploit, SPARTA, Xarp y SQLMap.

4. FASE: POST EXPLOTACIÓN

En la fase de post-explotación se busca mantener y expandir el acceso conseguido a un sistema vulnerable, pudiendo incluir la instalación de malware persistente, la extracción de información sensible y la manipulación de sistemas y aplicaciones.

Para llevar a cabo esta fase, se utilizan diversas herramientas, entre las que se destacan:

- Empire
- Enumdb
- Mimikatz
- Poet
- Pwnat
- TheFatRat

Es importante tener en cuenta que esta fase no siempre es aplicable, dependiendo de la naturaleza del objetivo y la información obtenida en fases anteriores.

5. FASE: REPORTE

Documento detallado que resume los resultados de una prueba de penetración (pentesting). Este informe incluye información sobre los objetivos y metodologías utilizadas durante el pentesting, así como los resultados y las recomendaciones para corregir las vulnerabilidades identificadas.
Se sugiere registrar las soluciones de seguridad apropiadas para abordar las deficiencias de seguridad detectadas en etapas anteriores. Esto puede ayudar a nuestro cliente o a la organización afectada a corregir las vulnerabilidades identificadas.

Entre las herramientas utilizadas para crear informes de vulnerabilidades se encuentran:

- Metasploit Framework
- OWASP ZAP
- Nessus
- OpenVAS

2.3 LAS HERRAMIENTAS DE CIBERSEGURIDAD SON DE VITAL IMPORTANCIA, ADEMÁS QUE EXISTE UN GRAN ABANICO DE POSIBILIDADES DE HERRAMIENTAS EXISTENTES Y SOFTWARE ESPECIALIZADO PARA DESARROLLAR HERRAMIENTAS PROPIAS. USTED COMO FUTURO EXPERTO DEBE DEFINIR Y EXPLICAR LAS SIGUIENTES HERRAMIENTAS:

• **Metasploit**

Metasploit es un framework de seguridad informática que se utiliza para realizar pruebas de penetración y evaluaciones de seguridad. Fue desarrollado por H.D.

Moore y se lanzó por primera vez en 2003 como una herramienta de seguridad gratuita y de código abierto.

Metasploit proporciona una plataforma centralizada para realizar pruebas de penetración, incluyendo la explotación de vulnerabilidades, la creación y utilización de exploits y la generación de payloads maliciosos.

• Nmap

Nmap es una herramienta de escaneo de red de código abierto que se utiliza para mapear redes y recopilar información sobre sistemas y dispositivos conectados a ellas. Nmap es un acrónimo que significa "Network Mapper".

Se pueden realizar escaneos de red para recopilar información sobre los sistemas y dispositivos conectados, incluyendo su dirección IP, sistema operativo, servicios en ejecución y otros detalles importantes.

• OpenVas

Es un marco de pruebas de penetración de código abierto que se utiliza para evaluar la seguridad de sistemas y redes. Proporciona una variedad de herramientas y utilidades para el escaneo de vulnerabilidades y la evaluación de riesgos.

Permite realizar evaluaciones exhaustivas de seguridad para identificar y evaluar las vulnerabilidades en sistemas y redes , escaneos de puertos, detección de software desactualizado.

OpenVAS cuenta con una base de datos actualizada de vulnerabilidades, lo que permite a los usuarios detectar de manera efectiva vulnerabilidades conocidas y evaluar su posible impacto en la seguridad de sus sistemas y redes.

Servicios en línea:

• ExploitDB

Base de datos que contiene información sobre vulnerabilidades y exploits de seguridad de software que se utilizan en el desarrollo y pruebas de herramientas de seguridad en el ámbito de la seguridad informática.

La base de datos contiene una amplia variedad de exploits para diferentes plataformas, sistemas operativos y aplicaciones, y es actualizada regularmente con los últimos descubrimientos y desarrollos. Algunos de los exploits incluidos son para

sistemas operativos como Windows y Linux, navegadores web, aplicaciones de mensajería, entre otros.
https://www.exploit-db.com/

• **CVE**

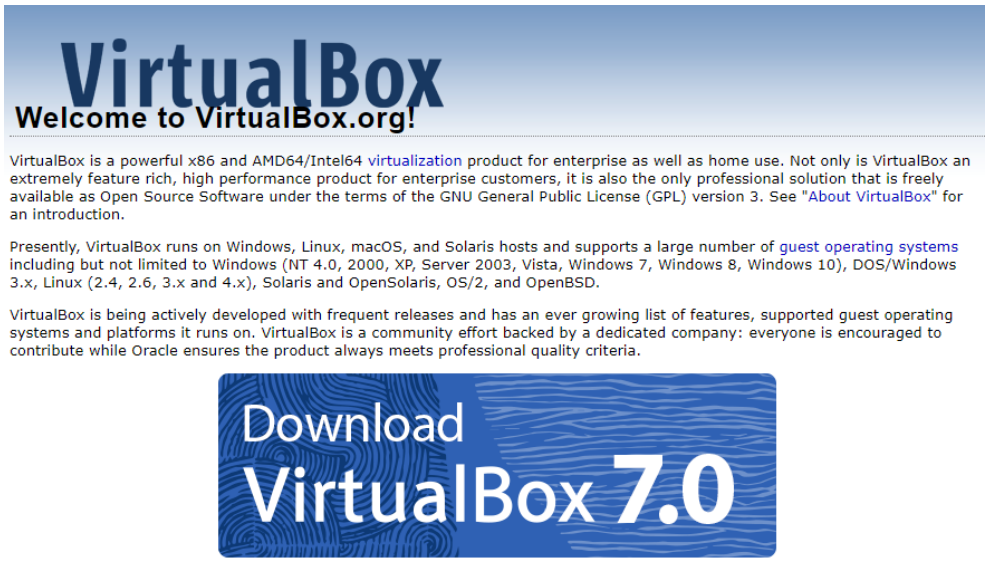
Es un diccionario público que contiene información sobre vulnerabilidades de seguridad de software. Cada entrada en CVE identifica una vulnerabilidad única y se utiliza como un estándar para compartir información sobre vulnerabilidades entre diversas herramientas y organizaciones.
https://cve.mitre.org/

2.4 PARA FINALIZAR ESTA ACTIVIDAD ES IMPORTANTE QUE USTED RECONOZCA, ANALICE Y CONFIGURE "BANCO DE TRABAJO" LO SOLICITADO EN EL ANEXO 1 – ESCENARIO 1 SOBRE EL CUAL DEBERÁ TRABAJAR ACTIVIDADES QUE CONTIENEN UN ALTO GRADO DE TECNICIDAD. LO SOLICITADO EN EL ANEXO 1

– escenario 1 es lo siguiente:

- **Paso A**: Descargar la herramienta virtualizadora "VirtualBox" en su última versión.

Ilustración 1. Descarga máquina virtual



Fuente: propia

En mi caso realizare las pruebas en Proxmox 7.3

Ilustración 2. Descarga Proxmox

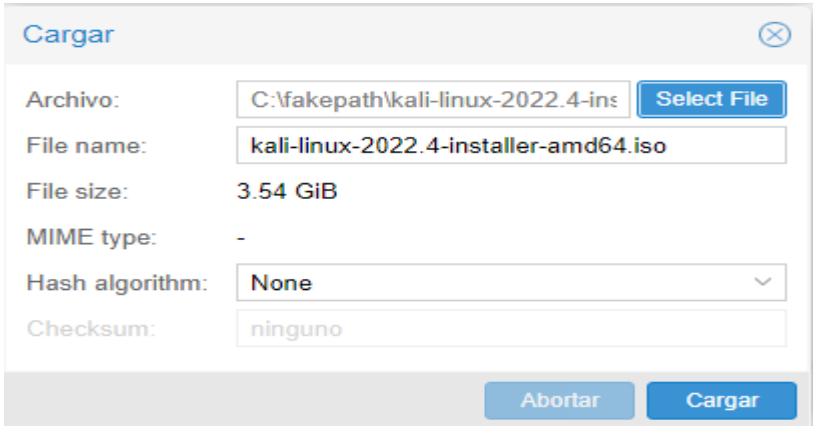
Fuente: propia

- **Paso B:**

Debido a que los foros no se abrieron en tiempos establecidos, se decidió implementar proxmox para poder llevar a cabo el laboratorio ya que no se tenían las OVA necesarias.

Como siguiente paso, se subirán las imágenes de los sistemas operativos que se van a virtualizar.

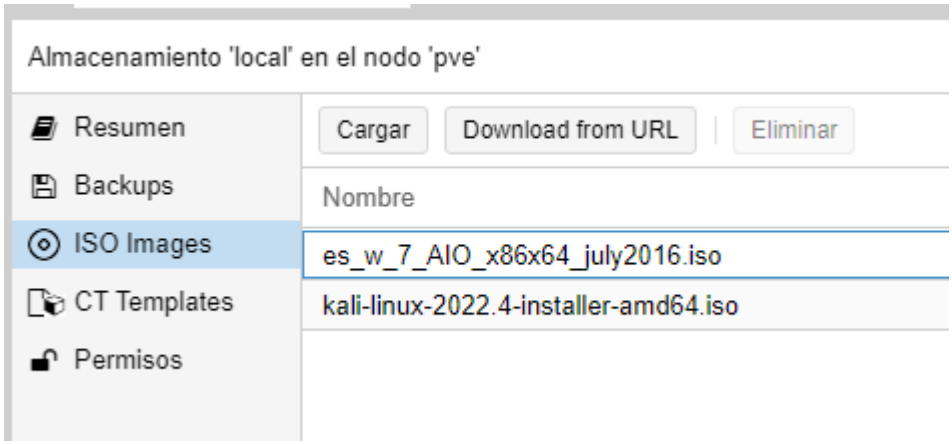
Ilustración 3. Carga ISO en Proxmox



Fuente: propia

A continuación observamos las dos imágenes en el servidor proxmox , y procedo a realizar la instalación de los dos Sistemas operativos .

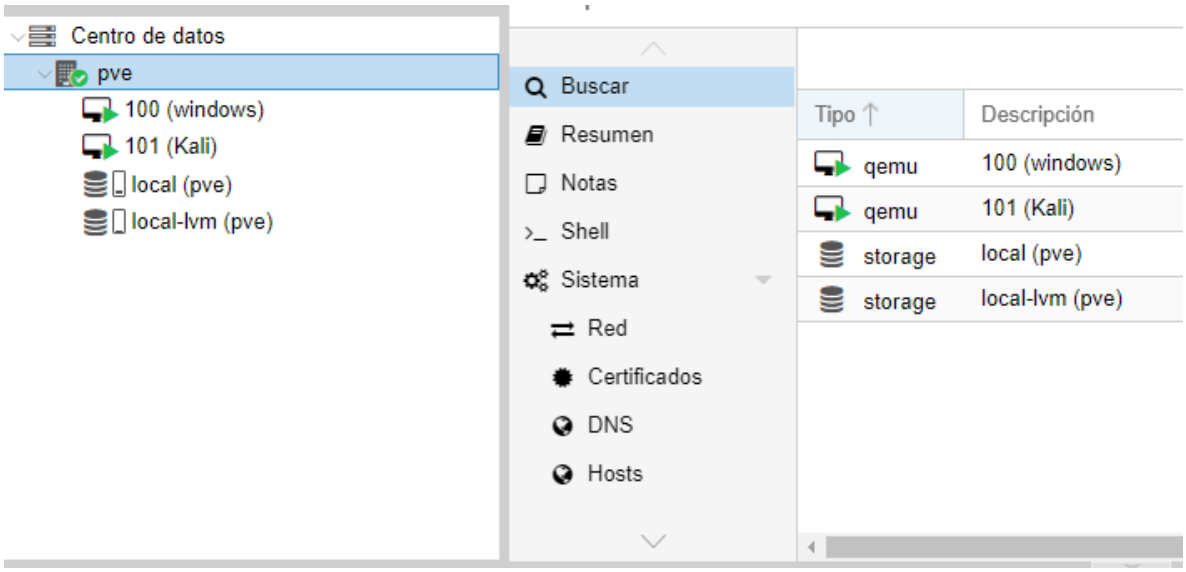
Ilustración 4.imágenes ISO



Fuente: propia

Observamos las dos maquinas virtuales corriendo (Windows y Kali)

Ilustración 5. Máquinas Virtuales Instaladas

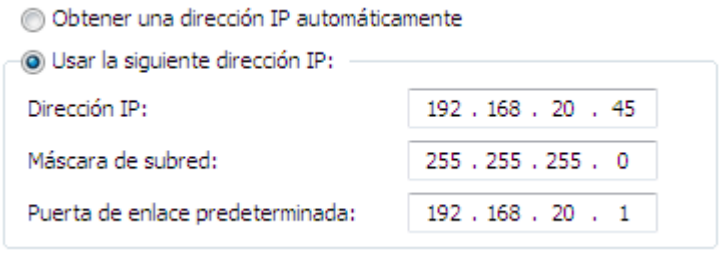


Fuente: propia

- **Paso C:** Es necesario verificar la comunicación entre cada una de las máquinas con Windows y la máquina de Kali Linux. Es importante recordar no encender las tres máquinas simultáneamente para evitar la sobrecarga de los recursos del equipo host. Lo recomendable es encender primero una máquina con Windows y luego encender la máquina de Kali Linux.

Desde la maquina Windows configuramos la IP

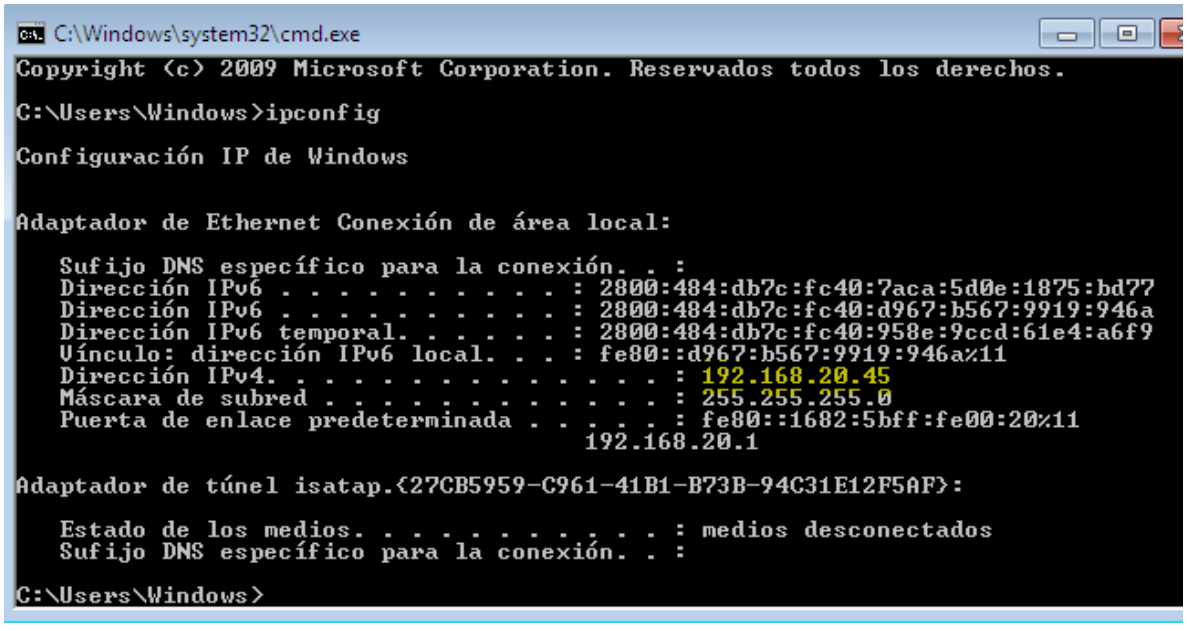
Ilustración 6. configuración IP estática



Fuente: propia

Desde la consola de comandos verificamos la IP configurada

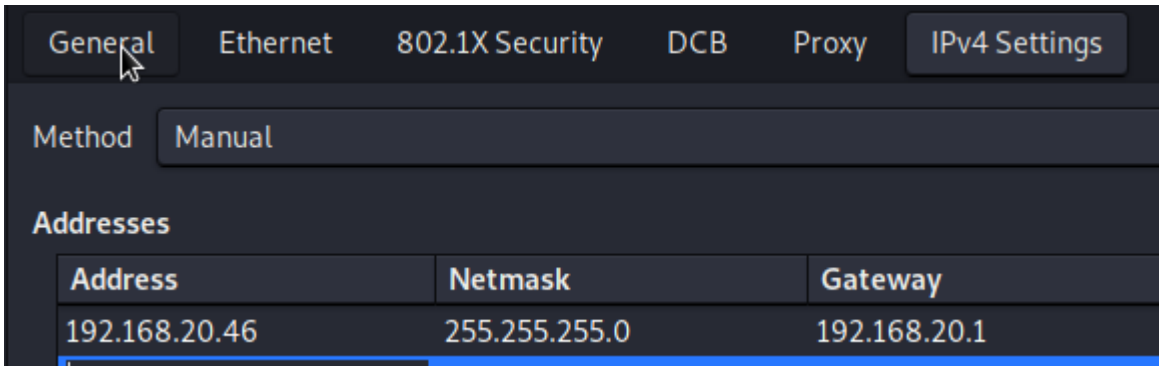
Ilustración 7. verificación IP



Fuente: propia

Desde la maquina Kali configuramos la IP

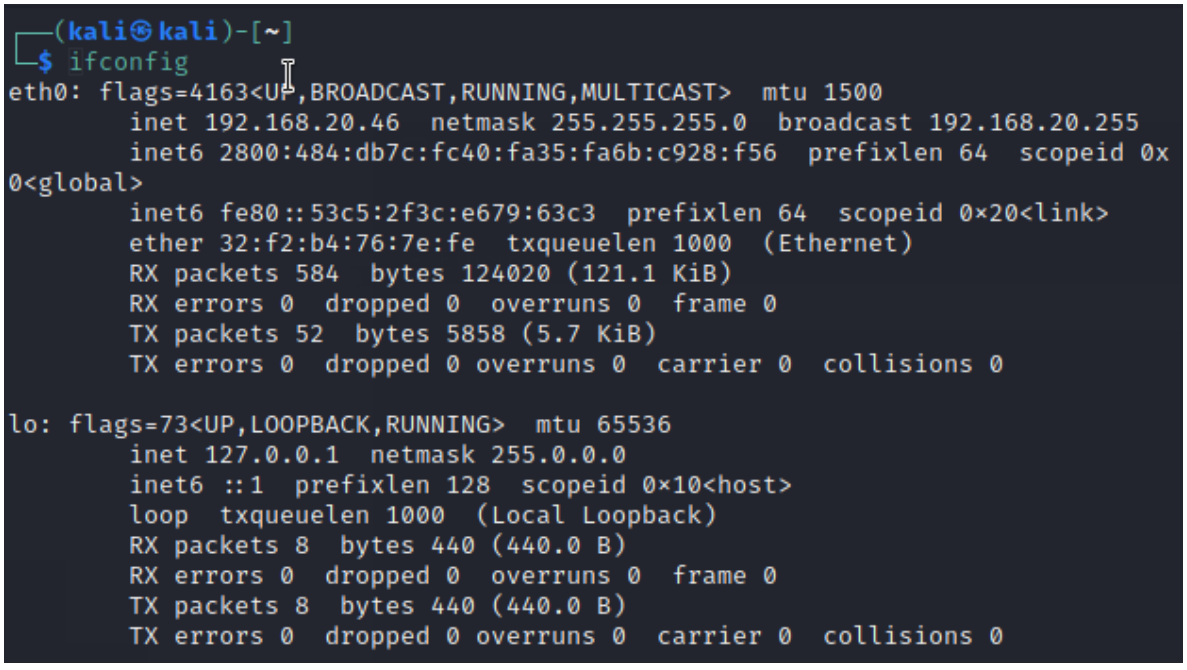
Ilustración 8. configuración IP estática



Fuente: propia

Desde la terminal verificamos la IP configurada

Ilustración 9. verificación IP



Fuente: propia

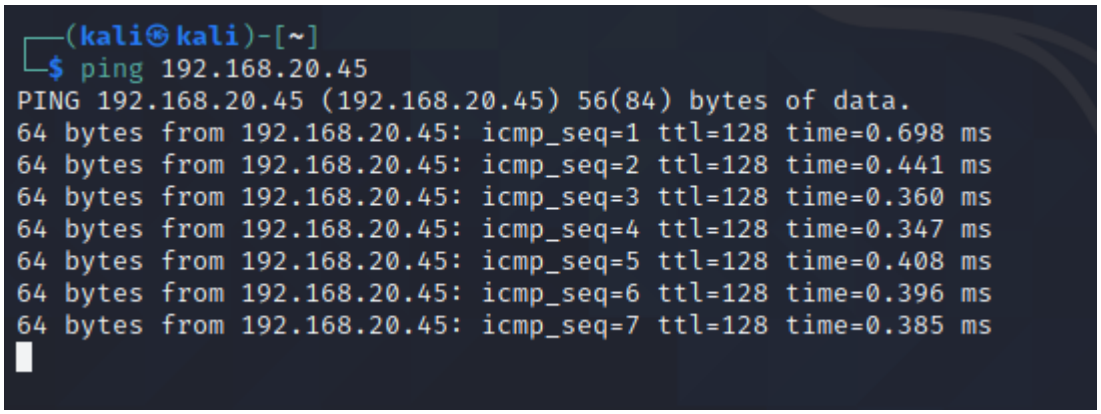
Desde la maquina Windows realizamos ping a la maquina Kali

Ilustración 10. Ping Maquina Kali

Fuente: propia

Desde la maquina kali realizamos ping a la maquina Windows

Ilustración 11. Ping Maquina windows 7

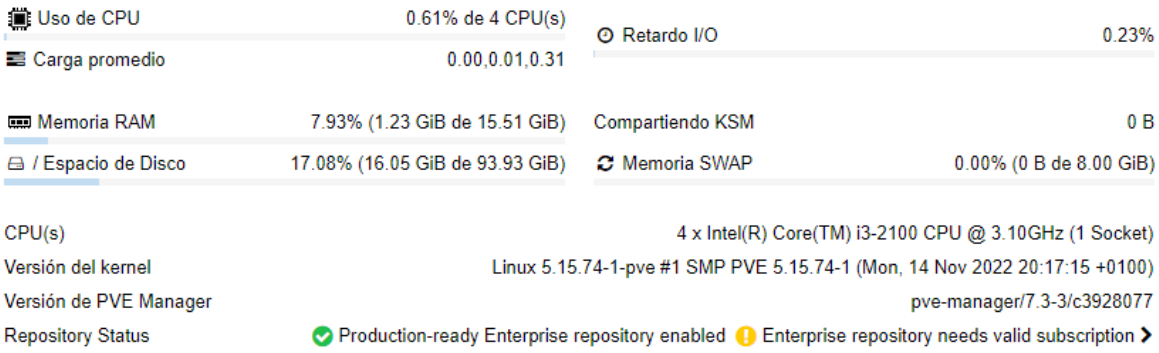


Fuente: propia

- **Paso D:** Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Hardware de la PC PROXMOX

Ilustración 12. Hardware Maquina anfitriona



Fuente: propia

Hardware Máquina virtual Kali Linux

Ilustración 13. Hardware Máquina virtual Kali Linux

Fuente: propia

Hardware Máquina virtual Windows 7

Ilustración 14. Hardware Máquina virtual Windows 7

Memoria	2.00 GiB
Procesadores	1 (1 sockets, 1 cores)
BIOS	Por defecto (SeaBIOS)
Pantalla	Por defecto
Machine	pc-i440fx-7.1
Controlador SCSI	VirtIO SCSI single
Disco Duro (ide0)	local-lvm:vm-100-disk-0,size=32G
Dispositivo CD/DVD (ide2)	local:iso/es_w_7_AIO_x86x64_july2016.iso,media=cdrom,size=6907688K
Dispositivo de red (net0)	e1000=1A:18:1B:E1:37:6B,bridge=vmbr0,firewall=1

Fuente: propia

3 ETAPA 2 ACTUACIÓN ÉTICA Y LEGAL

De manera individual usted deberá leer el problema que se encuentra en el anexo 2 – Escenario 2, además deberá leer y analizar el anexo 3 – Acuerdo para generar la solución a las siguientes preguntas orientadoras:

3.1 ¿UNA VEZ LEÍDO EL ANEXO 2 – ESCENARIO 2 Y EL ANEXO 3 - ACUERDO USTED LOGRA EVIDENCIAR ALGÚN PROCESO ILEGAL Y NO ÉTICO QUE SE ESTÉ ESTIPULANDO EN DICHO ACUERDO? DEBERÁ ARGUMENTAR SU RESPUESTA Y SEÑALAR LOS FRAGMENTOS ILEGALES DEL ANEXO ACUERDO EN CASO DE EXISTIR ALGUNA IRREGULARIDAD.

ANEXO 2 - Escenario

1. La organización WhiteHouse Security utiliza un **contrato elaborado por un abogado que fue despedido por encontrar procesos ilícitos**, lo que sugiere que la empresa podría estar involucrada en prácticas poco éticas o ilegales.

   Además, **la alta gerencia no revisó los contratos**, lo que indica una falta de diligencia por parte de la empresa.

2. La organización aprovecha una serie de problemas internos para **clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión,** lo que parece ser una forma poco ética de seleccionar a los nuevos empleados. Además, la empresa espera que los equipos trabajen bajo esta característica, lo que puede conducir a prácticas poco éticas o incluso ilegales en el proceso.

3. La organización solicita que se proyecte la **instalación de dos máquinas virtuales por medio de virtualbox**, lo que sugiere que la empresa puede estar utilizando tecnología sin licencia, lo que también es ilegal.

ANEXO 3 - Acuerdo

Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.

Respuesta: Esta cláusula va más allá de lo permitido por las leyes de protección de datos, ya que impide que la información confidencial o sobre procesos ilegales dentro de la empresa sea divulgada, incluso a las autoridades legales competentes. Esto permite llegar a sugerir que la empresa está intentando encubrir posibles delitos o prácticas ilegales, lo que es contrario a la ética empresarial y a la ley colombiana.

Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

   Parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

   Respuesta: Esta cláusula presenta varios aspectos que pueden ser considerados ilegales y no éticos.

   Al establecer que la información confidencial incluye cualquier información sobre procesos ilegales dentro de Whitehouse Security, lo que sugiere que la organización podría estar involucrada en actividades ilícitas.

   La cláusula menciona que la información confidencial incluye datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos", esto señalaría que la organización podría estar realizando actividades de espionaje o hackeo, lo cual es ilegal y antiético.

   La cláusula establece que los empleados de Whitehouse Security se comprometen a no divulgar cualquier información que no sea pública y sea conocida por ellos durante el proceso de selección de personal. Esto puede pensarse como un acto ilegal, ya que los empleados podrían tener acceso a información que no deberían conocer durante el proceso de selección, tales como datos sobre otros candidatos qué podrían ser considerados como información sensible.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Respuesta: Esta cláusula no establece límites precisos sobre qué tipo de información se considerará confidencial y de dónde vendrá, se está dando pie a la posibilidad de que información personal y propiedad intelectual de los candidatos a la organización WhiteHouse Security sean conseguidas y utilizadas sin su consentimiento. Esto puede ser considerado un proceso ilegal y no ético ya que se estaría violando el derecho a la privacidad de los candidatos, así como su propiedad intelectual.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora de la información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

Ítem 1- Mantener la información confidencial segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

Respuesta: *no ofrece garantías para la protección de los derechos de los trabajadores y su privacidad, así como también podría ser una violación de los derechos de propiedad intelectual de los empleados.*

Ítem 2- Proteger la información confidencial, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Whitehouse Security, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

Respuesta: *restringir la información solo a ciertas personas puede permitir la ocultación de conductas ilegales o poco éticas en la empresa*

Ítem 3- No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

Respuesta: *Como especialistas en seguridad informática, nuestra ética profesional nos impone la responsabilidad de reportar a las autoridades competentes cualquier actividad de espionaje sospechosa, ya que la ley colombiana considera que la omisión de esta acción constituye un delito..*

Ítem 4- Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

Respuesta: *La ética profesional que tenemos como especialistas en seguridad informática nos obliga a denunciar ante las autoridades competentes cualquier actividad sospechosa de espionaje, ya que la ley colombiana considera que no hacerlo constituye un delito.*

Ítem 8- Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

Respuesta : *La empresa desea que el empleado sea directamente involucrado ante las autoridades competentes y que asuma la totalidad de los cargos, con el fin de eximir a la compañía de cualquier responsabilidad.*

Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo**. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security

Respuesta : O*bliga a una de las partes a renunciar a su derecho a la justicia y a la protección de sus intereses legales y confidenciales. Además, deja a la otra parte exenta de responsabilidad incluso en caso de incumplimiento o violación del acuerdo.*

3.2 SI LA RESPUESTA ES AFIRMATIVA Y USTED ENCONTRÓ ALGÚN PROCESO ILEGAL EN EL ANEXO 3 - ACUERDO ACUERDO DEBERÁ MENCIONAR QUE ARTÍCULOS DE LA LEY 1273 SE PODRÍAN VULNERAR EN DICHO ACUERDO Y ESPECIFICAR PORQUÉ VULNERA ARTÍCULOS DE LA LEY 1273.

artículos de la ley 1273 que se vulnera y por que

Primera. Objeto: Al obligar al empleado a no denunciar y convertirse en cómplice de actividades criminales, la empresa está violando el artículo **269F** de la **Ley 1273 de 2009**. Asimismo, al manipular información privada y confidencial sin la autorización expresa del propietario, la empresa está cometiendo un delito según el artículo **269H de la Ley 1273 de 2009**.

Esta acción puede resultar en una pena de prisión de hasta tres años y en la inhabilitación para ejercer la profesión.

Esta cláusula es contraria a la ley que establece que cualquier persona que tenga conocimiento de actividades ilícitas relacionadas con sistemas de información debe denunciarlas ante las autoridades competentes.

Segunda. Definición de información confidencial: ***Artículos 269C y 269H de la Ley 1273 de 2009*** ,cuando alguien se apropia de información, accede a sistemas de información y lleva a cabo la interceptación de datos sin la autorización correspondiente, está cometiendo un delito que puede conllevar graves consecuencias penales y económicas..

Al obligar al empleado a no denunciar estos delitos, es cómplice se expone a estas penas

Tercera. Origen de la información confidencial: ***artículos 269i y 269h de la ley 1273 de 2009*** en esta cláusula, ya que manipula información de terceros sin su consentimiento a través de herramientas informáticas y también recopila información personal de los candidatos sin autorización en los procesos de selección.

Cuarta. Obligaciones de la parte receptora:

Esta cláusula vulnera varios artículos de la Ley 1273 de 2009: el **269A** por referencia al espionaje y receptación de información, el **269C** por la interceptación de información, el **269F** por la violación de información empresarial y personal, y el **269H** por la captura de información sin autorización y su uso para beneficio propio. El empleado al callar y no denunciar, es cómplice y se expone a graves consecuencias penales y económicas.

Octava. Solución de controversias: ***Artículo 269f,*** ya que la compañía está obligando al receptor a no denunciar cualquier información ilegal o confidencial encontrada en sus manos y a eximir a la compañía de cualquier responsabilidad legal y penal.

3.3 ¿EXISTIENDO PROCESOS POCO CONFIABLES EN EL ANEXO 3 – ACUERDO? ¿USTED COMO EXPERTO EN CIBERSEGURIDAD APLICARÍA A ESTE TRABAJO EN THE WHITEHOUSE, DONDE LA ORGANIZACIÓN DISPONE DE UN SUELDO DE $15.000.000 DE PESOS COLOMBIANOS MENSUALES Y CONTRATO VITALICIO?

Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.

Respuesta: ***NEGATIVA***, La oferta laboral ofrece un salario atractivo y un contrato vitalicio, lo cual da indicios a que se realizarán actividades delictivas que pueden llevar a graves consecuencias como la prisión y la pérdida de la licencia profesional. No es justificable aceptar este tipo de empleo que atenta contra la privacidad de las personas y va en contra de las leyes que rigen nuestro país. Es importante ser consecuentes con el código de ética de la entidad COPNIA, se debe ser consecuente con el código de ética y las leyes , lo cual es fundamental para evitar graves consecuencias, como la destitución, la anulación de títulos, multas y cárcel[7].

3.4 DEBERÁ BUSCAR LA NOTICIA DEL CASO "OPERACIÓN ANDROMEDA BUGGLY" EN LA CIUDAD DE BOGOTÁ, Y REDACTAR SU PUNTO DE VISTA TENIENDO EN CUENTA LAS IMPLICACIONES LEGALES Y ÉTICAS QUE ALLÍ SE PUDIERON GENERAR.

Considero que en el "Caso Andrómeda Buggly" en la ciudad de Bogotá, se logra evidenciar la necesidad de la articulación entre entidades públicas y privadas en Colombia, en el tema de la seguridad informática y el hacking ético del país.

Aunque hay un esfuerzo constante en este ámbito, todavía hay mucho por hacer para minimizar las brechas legales, técnicas y de personal calificado.

El gobierno también debe mostrar una voluntad de trabajar por el bien común en lugar de intereses particulares. Solo así se podrán lograr avances significativos en la protección de la privacidad y seguridad de los ciudadanos en el entorno digital.

En Colombia, hay una gran cantidad de especialistas en seguridad informática que buscan contribuir al bien común y al servicio comunitario. La falta de oportunidades laborales y de regulación en el campo de la seguridad informática ha llevado a muchos profesionales a buscar oportunidades en otros países.

En este contexto, la empresa Andromeda Buggly realizó un reclutamiento de personal con el objetivo de aprovechar al máximo el conocimiento de los expertos en seguridad informática y hacking ético. Si bien esta estrategia produjo resultados positivos, también hubo consecuencias negativas, como la violación de normas y la comisión de delitos informáticos debido a la falta de experiencia y conocimiento en la materia. Es importante destacar que la normatividad actual del Estado colombiano establece medidas claras para prevenir este tipo de situaciones y garantizar la seguridad informática en el país. Por tanto, se requiere una mayor regulación y formación en seguridad informática para evitar estos problemas en el futuro.

[7] Código de ética | Copnia. (s. f.). Recuperado 23 de febrero de 2023, de https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

la seguridad informática y el hacking ético son cada vez más importantes a nivel mundial, y es necesario que se unan las fuerzas de todas las ramas judiciales del estado y entidades privadas para aprovechar a los expertos en beneficio del bien común, buscando la integridad, confidencialidad y disponibilidad de la información del estado.[8]

4 ETAPA 3 EJECUCIÓN PRUEBAS DE INTRUSIÓN

De manera individual usted deberá leer el problema que se encuentra en el anexo 4 – escenario 3 referente a equipo Redteam y por medio del banco de trabajo configurado previamente deberá dar respuesta a las siguientes preguntas orientadoras:

4.1 DESCRIBA DE MANERA ESPECÍFICA LAS HERRAMIENTAS SOFTWARE QUE UTILIZÓ PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3 ENFOCADO A REDTEAM. DEBERÁ ADJUNTAR EVIDENCIA DE LOS COMANDOS UTILIZADOS Y RESULTADOS QUE ARROJÓ CADA HERRAMIENTA UTILIZADA, ESTAS HERRAMIENTAS DEBEN ESTAR CLASIFICADAS SEGÚN LOS PASOS DE UN PENTESTING.

Ilustración 15. Herramienta Nmap

Fuente: Nmap | Kali Linux Tools. (s. f.). Kali Linux. Recuperado 9 de marzo de 2023, de https://www.kali.org/tools/nmap/

[8] Peñarredonda, J. L. (2015, diciembre 9). Detrás de Buggly: La historia de la fachada Andrómeda • ENTER.CO. ENTER.CO. https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Nmap, también conocido como "Network Mapper", es una herramienta de código abierto ampliamente utilizada para la exploración de redes y la identificación de hosts y servicios en una red determinada.

Entre las principales características de Nmap se incluyen:

Escaneo de puertos: Nmap puede escanear una amplia gama de puertos en un host y descubrir qué puertos están abiertos, cerrados o filtrados. Esto puede ayudar a identificar servicios y aplicaciones que se ejecutan en un host determinado.

Detección de sistemas operativos: Nmap puede detectar el sistema operativo que se está ejecutando en un host en función de las respuestas que recibe de las sondas enviadas durante el escaneo.

Escaneo de redes: Nmap puede escanear una red entera y descubrir qué hosts están activos y cuáles están inactivos. También puede identificar los sistemas operativos de los hosts y los servicios que se ejecutan en cada host.

Detección de vulnerabilidades: Nmap puede ser utilizado para detectar vulnerabilidades en los sistemas y servicios que se ejecutan en los hosts. Para hacer esto, Nmap utiliza scripts personalizados que se ejecutan durante el escaneo y que buscan señales de vulnerabilidades conocidas.

Personalización: Nmap ofrece una gran cantidad de opciones de personalización y configuración. Los usuarios pueden personalizar el comportamiento de Nmap para adaptarse a sus necesidades específicas.

Interfaz de usuario: Nmap se puede utilizar tanto desde la línea de comandos como a través de una interfaz de usuario gráfica. La interfaz de usuario permite a los usuarios seleccionar opciones de escaneo y visualizar los resultados en un formato fácil de entender.[9]

En esta actividad se utilizó scripts para comprobar vulnerabilidades las más conocidas en este caso son

- Auth: ejecuta todos sus scripts disponibles para autenticación
- Default: ejecuta los scripts básicos por defecto de la herramienta
- Discovery: recupera información del target o víctima
- External: script para utilizar recursos externos

[9] Guía de referencia de Nmap (Página de manual). (s. f.). Recuperado 9 de marzo de 2023, de https://nmap.org/man/es/index.html#man-description

- Intrusive: utiliza scripts que son considerados intrusivos para la víctima o target
- Malware: revisa si hay conexiones abiertas por códigos maliciosos o backdoors (puertas traseras)
- Safe: ejecuta scripts que no son intrusivos
- Vuln: descubre las vulnerabilidades más conocidas
- All: ejecuta absolutamente todos los scripts con extensión NSE disponibles[10]

Ilustración 16. Metasploit-framework

Fuente: *Metasploit-framework | Kali Linux Tools*. (s. f.). Kali Linux. Recuperado 9 de marzo de 2023, de https://www.kali.org/tools/metasploit-framework/

Metasploit es un marco de pruebas de penetración de código abierto utilizado para probar la seguridad de los sistemas informáticos y encontrar vulnerabilidades.

Metasploit proporciona una amplia variedad de herramientas y técnicas que permiten a los usuarios llevar a cabo pruebas de penetración y explotar vulnerabilidades. La plataforma incluye módulos que permiten la identificación de vulnerabilidades, la generación de payloads y la ejecución de exploits.

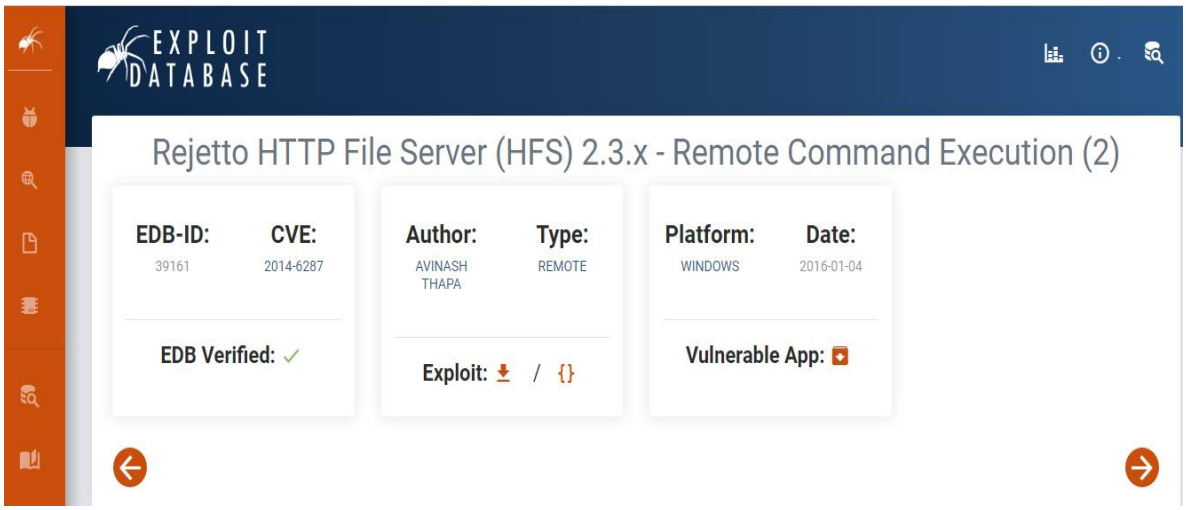
También se pueden personalizar los módulos para adaptarse a las necesidades específicas de las pruebas de penetración.[11]

[10] Auditando con Nmap y sus scripts para escanear vulnerabilidades. (2015, febrero 12). WeLiveSecurity. https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

[11] Metasploit | Penetration Testing Software, Pen Testing Security. (s. f.). Metasploit. Recuperado 9 de marzo de 2023, de https://www.metasploit.com/

Rejetto v.2.3 es una versión de HFS (HTTP File Server), que es un servidor web gratuito y de código abierto que permite a los usuarios compartir archivos a través de Internet utilizando el protocolo HTTP.
En algunas fuentes confiables se evidencian alertas sobre la vulnerabilidad presente en la aplicación Rejetto v. 2.3

Ilustración 17. Vulnerabilidad Rejetto - exploit-db

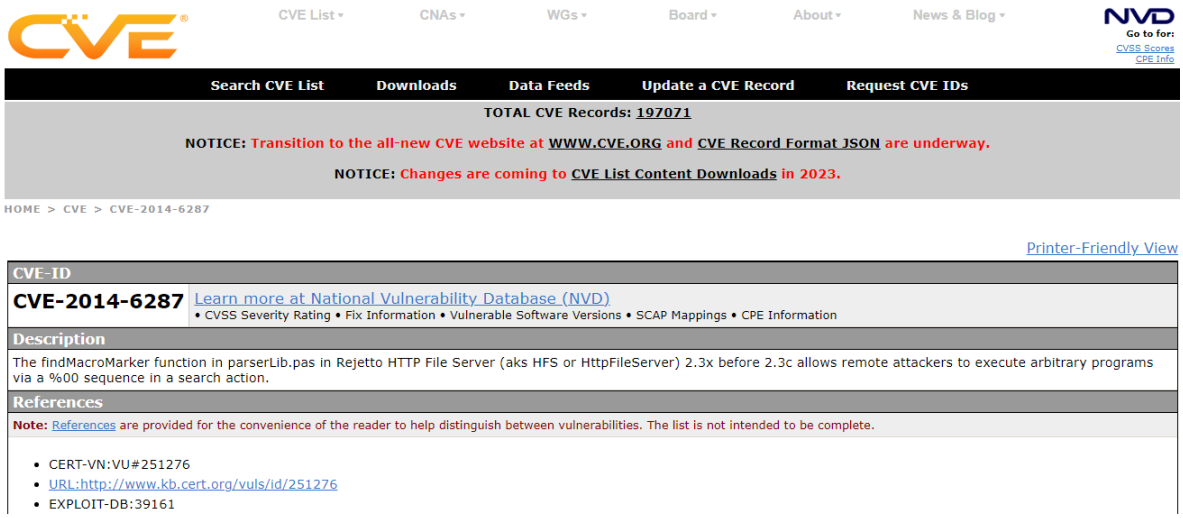


Fuente: Thapa, A. (2016, enero 4). *Rejetto HTTP File Server (HFS) 2.3.x—Remote Command Execution (2)*. Exploit Database. https://www.exploit-db.com/exploits/39161

Ilustración 18. Vulnerabilidad Rejetto - incibe-cert

Fuente: *CVE-2020-13432*. (2020, junio 8). INCIBE-CERT. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-13432

Ilustración 19. Vulnerabilidad Rejetto – CVE



Fuente: *CVE - CVE-2014-6287*. (s. f.). Recuperado 9 de marzo de 2023, de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

4.2 A CONTINUACIÓN, LISTE Y DESCRIBA LOS DATOS E INFORMACIÓN DEL ANEXO 4 ESCENARIO 3 QUE LE FUERON DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 7 X64.

La información del anexo 4, escenario 3, que ayudaron a identificar el fallo de seguridad fueron:

- Equipo con sistema operativo Windows 7 X64 , sistema que no cuenta las actualizaciones de software de Windows Update que ayudan a proteger tu equipo ya no están disponibles para el producto desde el 14 de enero de 2020 [12]

- Se ha producido una fuga de información en un equipo que cuenta con la aplicación Rejetto v. 2.3 instalada

- Se ha identificado un exploit que podría conducir a la apertura de una Shell reversa y la creación de una sesión de meterpreter

- Falla de seguridad

- Escalamiento de privilegios

4.3 ¿QUÉ HERRAMIENTA UTILIZÓ PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA "MÁQUINA WINDOWS 7"? ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

- Con la herramienta ipconfig se identifica la IP de la máquina victima que para este caso es la IP: 192.168.20.49

- Con la herramienta netstad se identifica los puertos que están abiertos y que se encuentran en estado LISTENING.

[12] El soporte de Windows 7 finalizó el 14 de enero de 2020—Soporte técnico de Microsoft. (s. f.). Recuperado 9 de marzo de 2023, de https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finaliz%C3%B3-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962

- Al emplear la herramienta Nmap se identifica los servicios que la máquina tiene corriendo y a su vez el puerto por donde se puede atacar.

- La “aplicación rejetto v.2.3” tiene abierto “el puerto 80”

4.4 EXPLIQUE CON SUS PALABRAS Y DE MANERA ESPECÍFICA CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64), HAGA USO DE GRÁFICOS PARA EXPLICAR EL ATAQUE.

Un shell inverso es una técnica utilizada en seguridad informática para obtener acceso a un sistema remoto. En lugar de establecer una conexión directa desde el sistema atacante al sistema objetivo, el objetivo es quien inicia la conexión hacia el atacante.

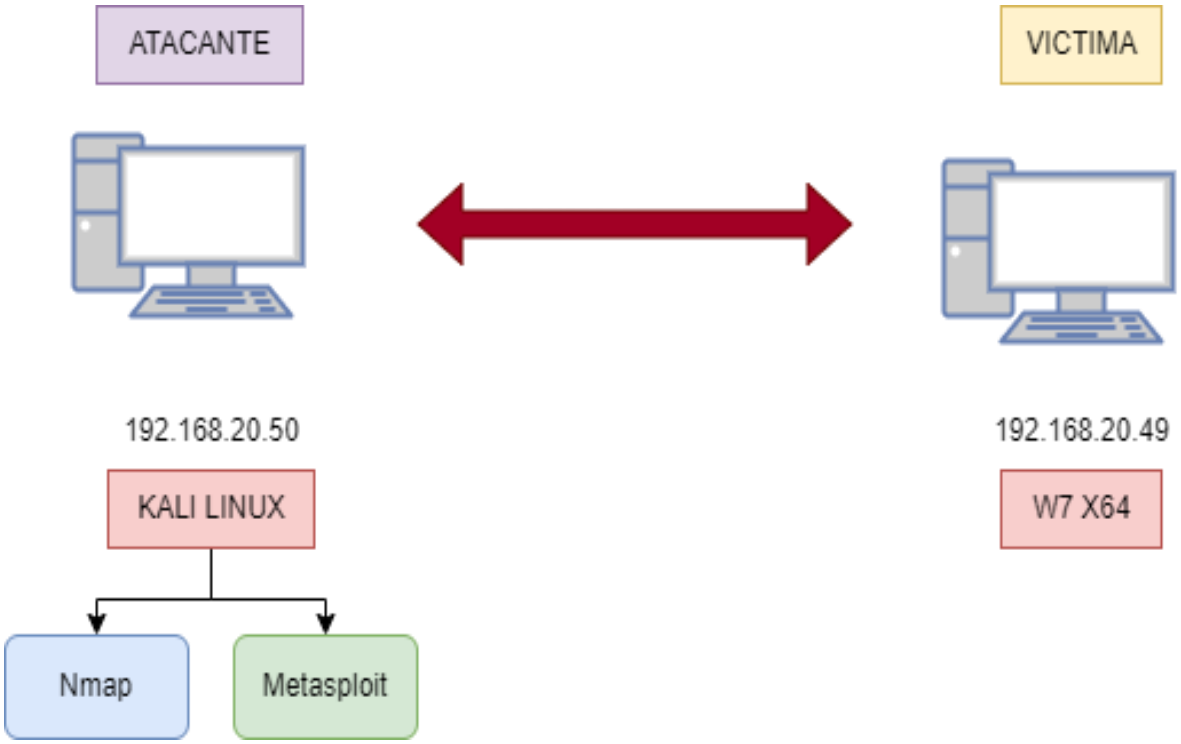
Esto se logra mediante la ejecución de un programa malicioso en este caso aplicación rejetto v.2.3, la cual se encarga de establecer una conexión de red de vuelta al sistema atacante. Una vez que se ha establecido la conexión, el atacante puede utilizar una línea de comandos remota en el sistema objetivo para realizar acciones maliciosas, como instalar software malicioso adicional, robar información, o realizar cambios en el sistema objetivo.
La técnica del shell inverso es utilizada a menudo porque permite a los atacantes evadir los sistemas de detección de intrusiones y los firewalls al utilizar una conexión de red de salida legítima desde el sistema objetivo hacia el atacante.[13]

Sumado a esto la maquina con Windows 7 x64 no cuenta con las actualizaciones de software de Windows Update que ayudan a proteger el equipo ya no están disponibles para el producto desde el 14 de enero de 2020 [14]

Ilustración 20. Descripción ATAQUE

[13] KeepCoding, R. (2022, noviembre 10). ¿Cómo ejecutar una shell inversa? | KeepCoding Tech School. https://keepcoding.io/blog/como-ejecutar-una-shell-inversa/

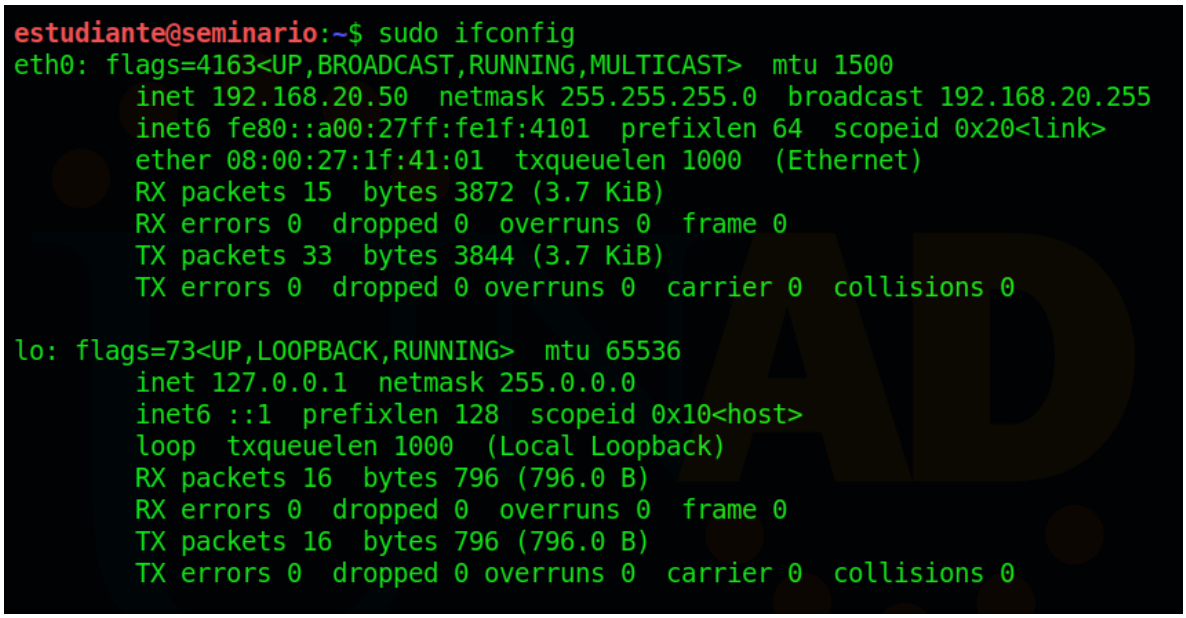
[14] El soporte de Windows 7 finalizó el 14 de enero de 2020—Soporte técnico de Microsoft. (s. f.). Recuperado 9 de marzo de 2023, de https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finaliz%C3%B3-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962



Fuente: Propia

4.5 DOCUMENTE CADA UNO DE LOS PASOS QUE EJECUTÓ Y SUS RESPECTIVAS EVIDENCIAS PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS.

Ilustración 21.Consulta IP Kali Linux



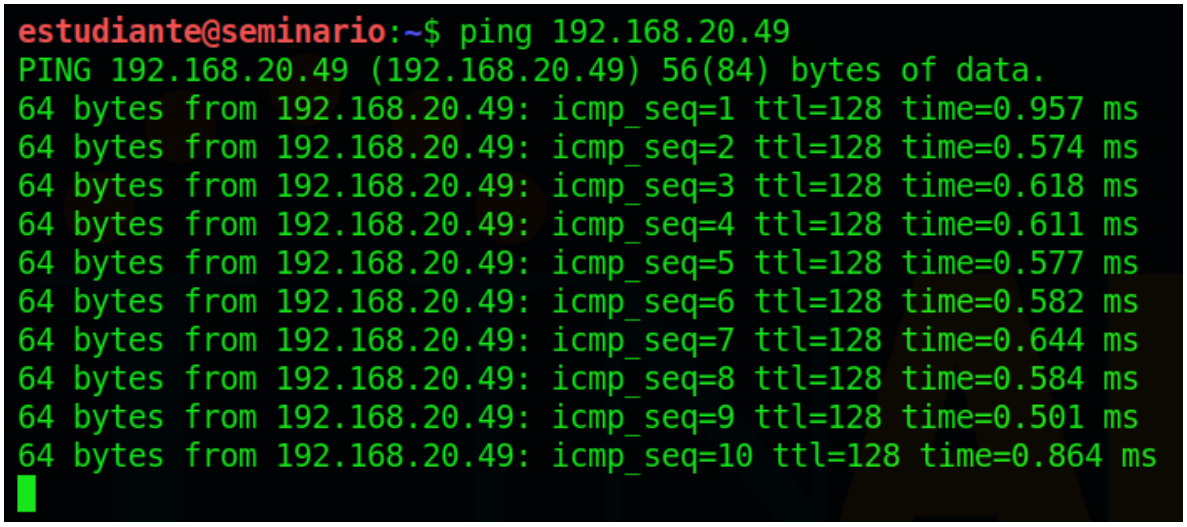
Fuente: Propia

Consultamos la IP del HOST con Kali Linux

Ilustración 22. Consulta IP Host Windows 7 x64

Fuente: Propia
Consultamos la IP del HOST CON Windows 7 X64

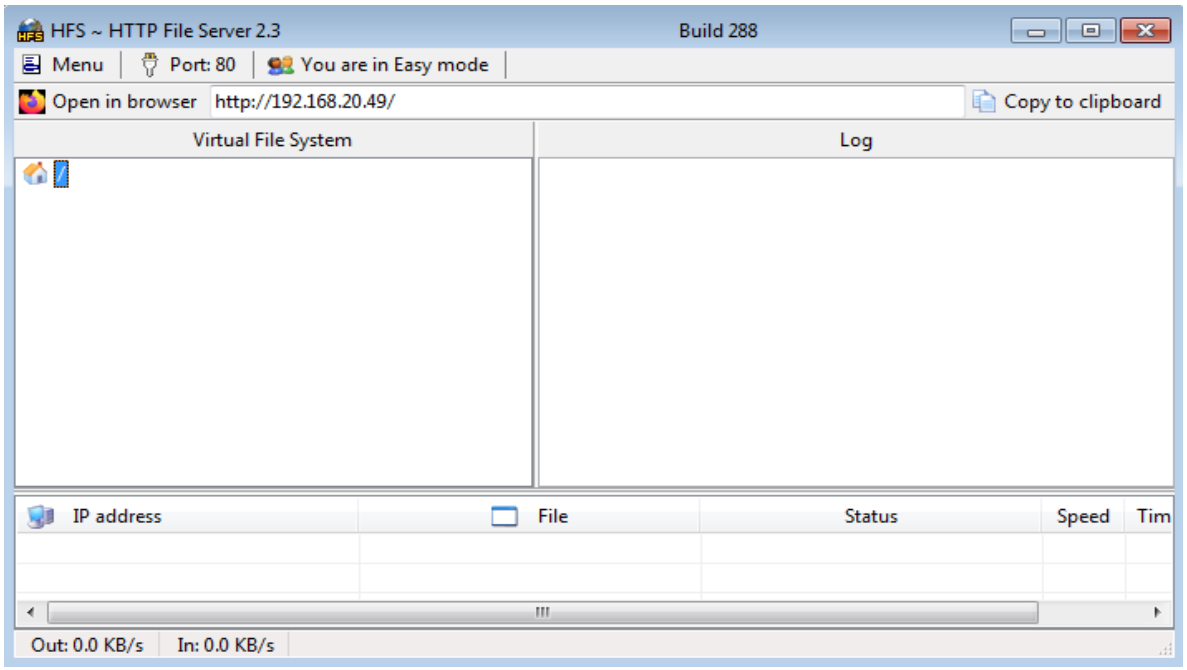
Ilustración 23. Verificación comunicación y respuesta mediante Ping



Fuente: Propia

Verifico conectividad mediante ping desde la maquina Linux

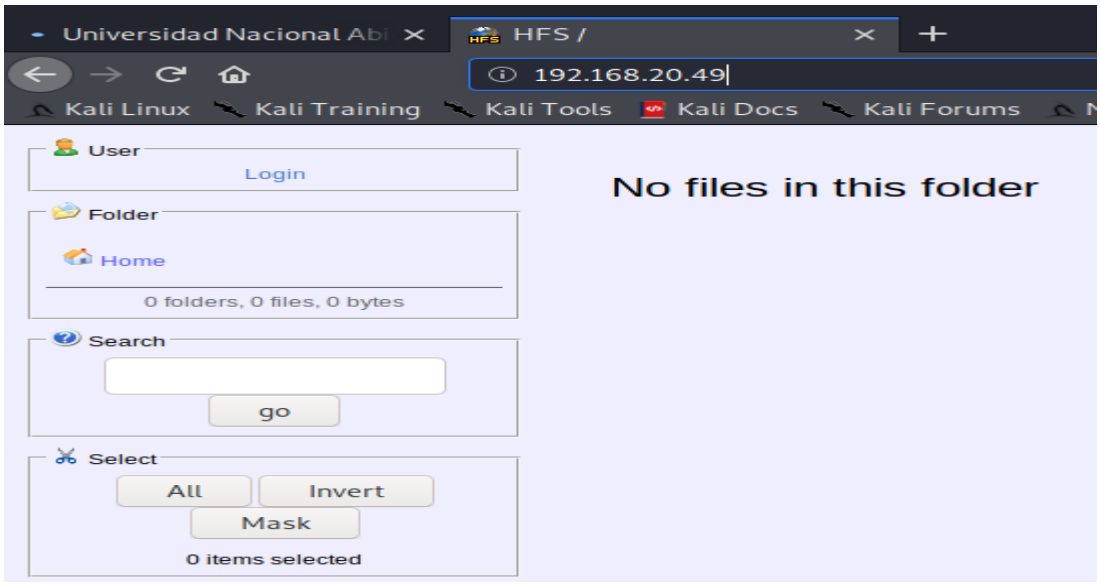
Ilustración 24. Instalación de software rejetto v.2.3



Fuente: Propia

Instalación de software rejetto v.2.3 con el objetivo de experimentar lo que dice la actividad y encontrar el punto de fuga de información.

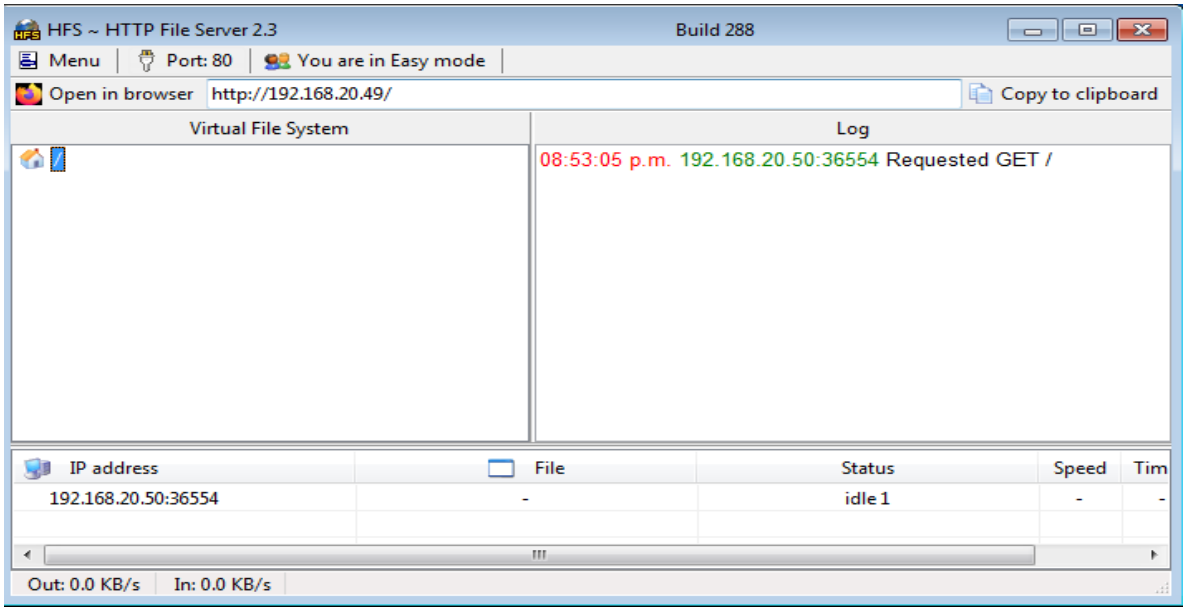
Ilustración 25. browser en host Kali Linux



Fuente: Propia

Desde browser en host Kali Linux, accedemos a la IP del Host Con Windows 7x&4

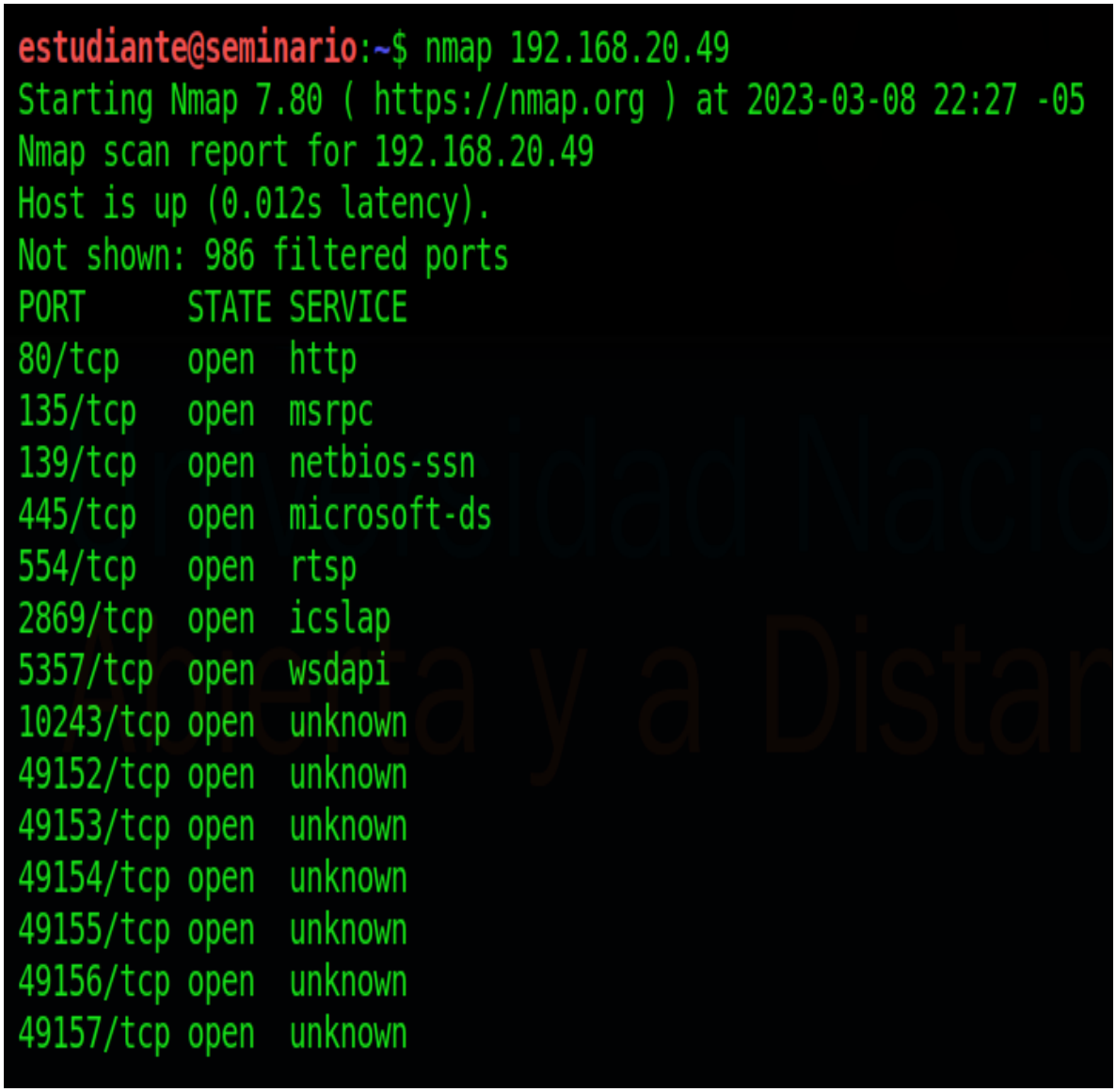
Ilustración 26. Respuesta host victima



Fuente: Propia

Respuesta desde host victima

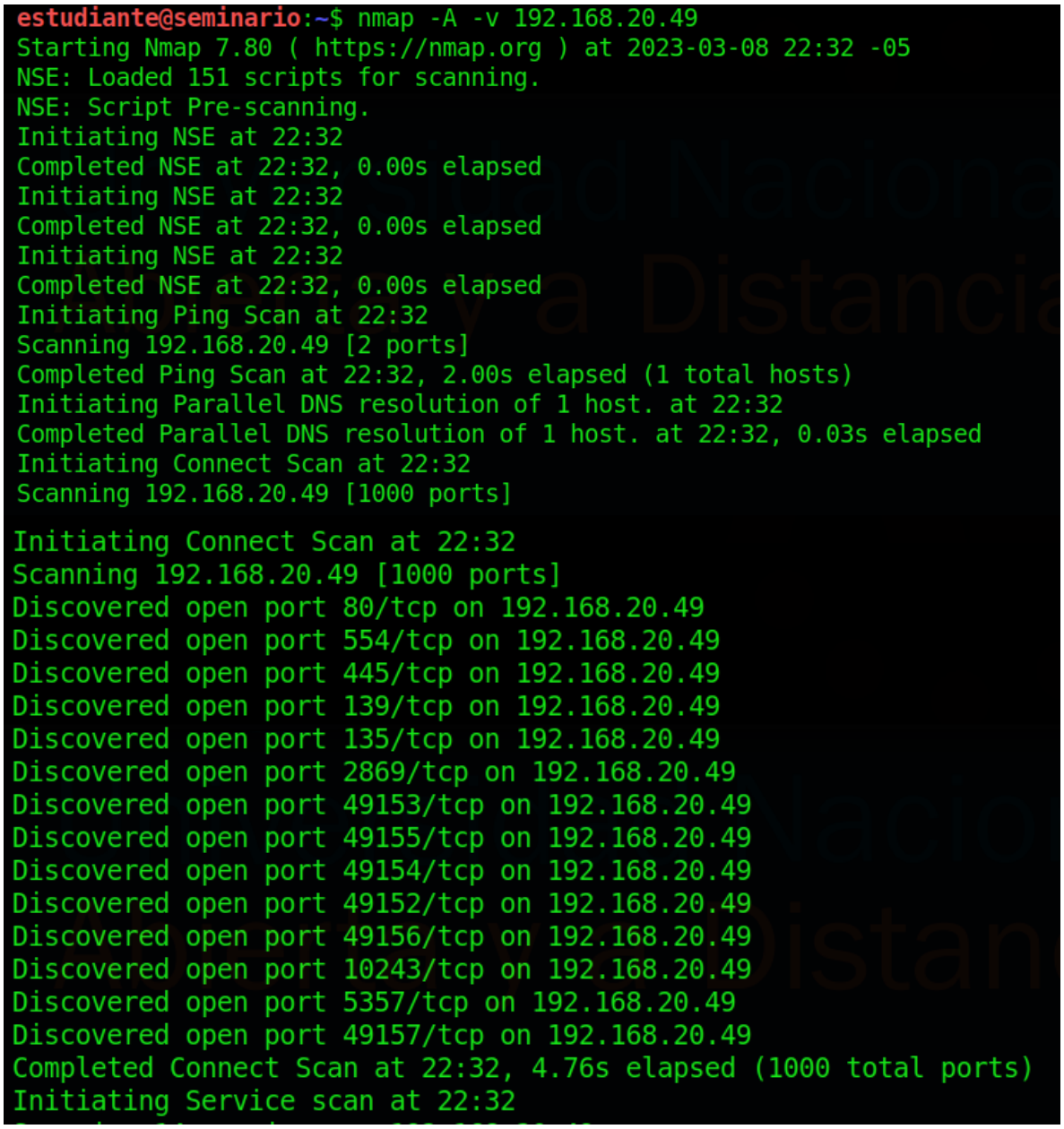
Ilustración 27. Escaneo Nmap



Fuente: Propia

Escaneo de los puertos mediante Nmap, Se observa el puerto 80 abierto.

Ilustración 28. Escaneo con Nmap -A -v


estudiante@seminario:~$ nmap -A -v 192.168.20.49
Starting Nmap 7.80 (https://nmap.org) at 2023-03-08 22:32 -05
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:32
Completed NSE at 22:32, 0.00s elapsed
Initiating NSE at 22:32
Completed NSE at 22:32, 0.00s elapsed
Initiating NSE at 22:32
Completed NSE at 22:32, 0.00s elapsed
Initiating Ping Scan at 22:32
Scanning 192.168.20.49 [2 ports]
Completed Ping Scan at 22:32, 2.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:32
Completed Parallel DNS resolution of 1 host. at 22:32, 0.03s elapsed
Initiating Connect Scan at 22:32
Scanning 192.168.20.49 [1000 ports]
Initiating Connect Scan at 22:32
Scanning 192.168.20.49 [1000 ports]
Discovered open port 80/tcp on 192.168.20.49
Discovered open port 554/tcp on 192.168.20.49
Discovered open port 445/tcp on 192.168.20.49
Discovered open port 139/tcp on 192.168.20.49
Discovered open port 135/tcp on 192.168.20.49
Discovered open port 2869/tcp on 192.168.20.49
Discovered open port 49153/tcp on 192.168.20.49
Discovered open port 49155/tcp on 192.168.20.49
Discovered open port 49154/tcp on 192.168.20.49
Discovered open port 49152/tcp on 192.168.20.49
Discovered open port 49156/tcp on 192.168.20.49
Discovered open port 10243/tcp on 192.168.20.49
Discovered open port 5357/tcp on 192.168.20.49
Discovered open port 49157/tcp on 192.168.20.49
Completed Connect Scan at 22:32, 4.76s elapsed (1000 total ports)
Initiating Service scan at 22:32

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
|_http-title: HFS /
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 micros
oft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found

49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h40m02s, deviation: 2h53m13s, median: 1s
| nbstat: NetBIOS name: PC202006, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:
27:92:80:c0 (Oracle VirtualBox virtual NIC)
| Names:
|   PC202006<00>         Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   PC202006<20>         Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1
)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: PC202006
|   NetBIOS computer name: PC202006\x00
```

```
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: PC202006
|   NetBIOS computer name: PC202006\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-03-08T22:34:11-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-03-09T03:34:09
|_  start_date: 2023-03-09T02:45:13

NSE: Script Post-scanning.
Initiating NSE at 22:35
Completed NSE at 22:35, 0.00s elapsed
Initiating NSE at 22:35
Completed NSE at 22:35, 0.00s elapsed
Initiating NSE at 22:35
Completed NSE at 22:35, 0.00s elapsed
```

Fuente: Propia

Escaneo con Nmap -A -v

Se utiliza para realizar un escaneo agresivo de una red y obtener información detallada sobre los sistemas objetivo.

Aquí se explica el significado de las opciones utilizadas en el comando:

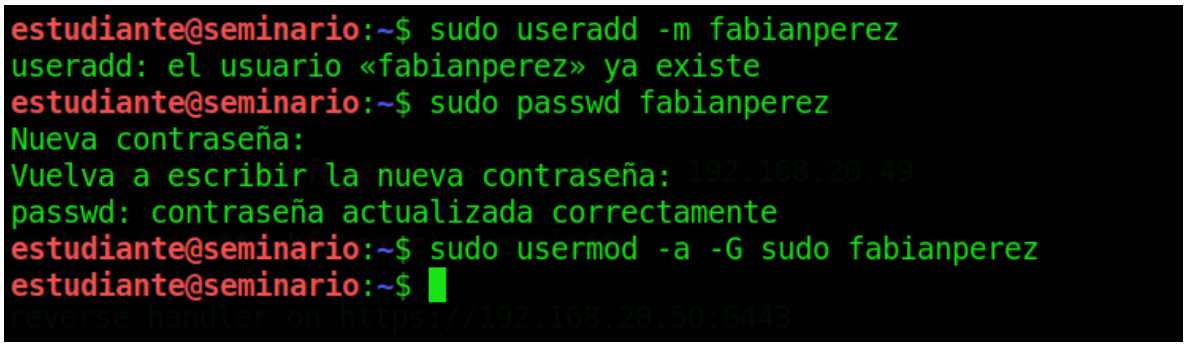
-A: Habilita el modo agresivo. Esta opción activa la detección de sistemas operativos, la detección de versiones, el escaneo de scripts y el trazado de ruta (traceroute).

-v: Aumenta el nivel de verbosidad. Esta opción aumenta la cantidad de detalles que muestra nmap durante el escaneo.

Al combinar estas opciones, nmap realizará un escaneo exhaustivo de los sistemas objetivo, identificando el sistema operativo, los puertos abiertos y los servicios que se ejecutan en esos puertos. También intentará detectar las versiones de los

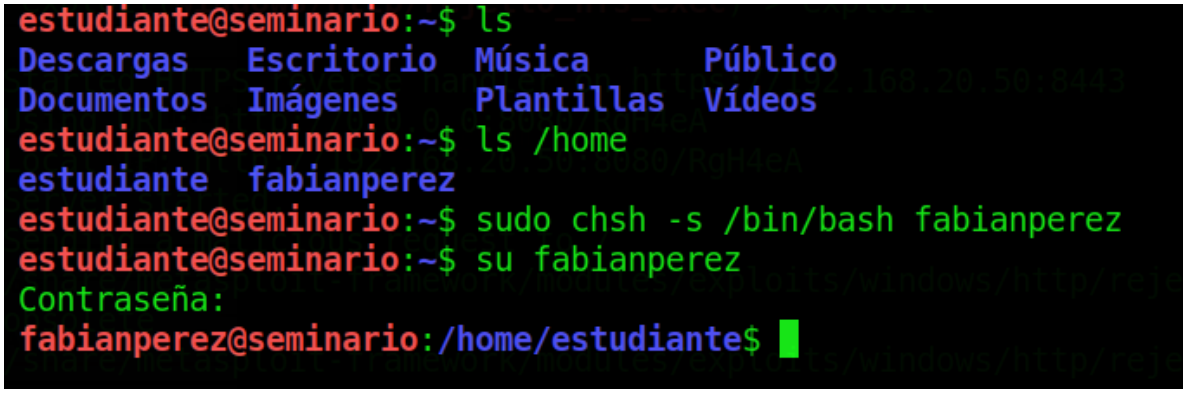
servicios y del sistema operativo, y ejecutará un conjunto de scripts predeterminados para identificar posibles vulnerabilidades.

Ilustración 29. Creación usuario en Kali Linux



Fuente: Propia

Ilustración 30. Shell kali linux

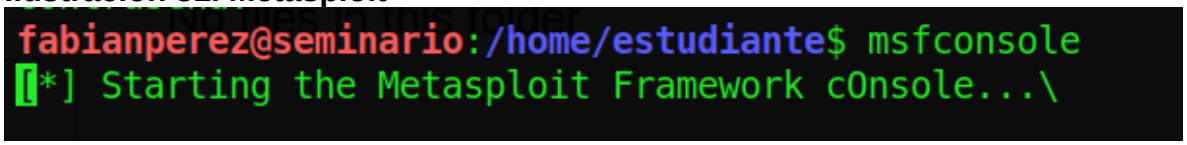


Fuente: Propia

Se crea el usuario en Kali Linux con privilegios de administrador con el comando sudo o **usermod -a -G sudo fabianperez**. A su vez el usuario es agregado a la Shell para que sea visible en la terminal con el siguiente comando de Kali Linux: **chsh -s /bin/bash fabianperez**

Inicio y uso de la herramienta Metasploit en Kali Linux

Ilustración 31. Metasploit

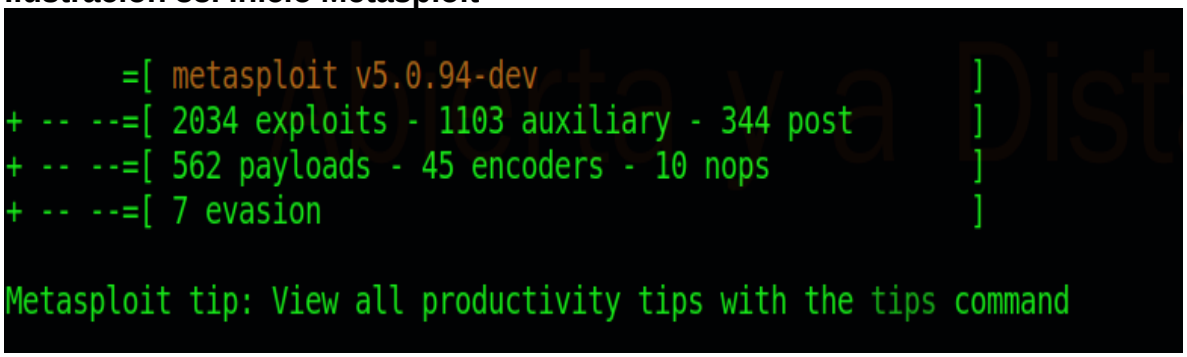


Fuente: Propia

Ilustración 32. Logo MetasPloit

Fuente: Propia

Ilustración 33. Inicio Metasploit



Fuente: Propia

Ilustración 34. Busqueda httpFileServer o Rejetto

```
msf5 > search httpFileServer

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check
  Description
   -  ----                                      ---------------  ----       -----
  -----------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes
  Rejetto HttpFileServer Remote Command Execution
```

Fuente: Propia

Ilustración 35. Uso exploit

```
msf5 > use 0
```

Fuente: Propia

Ilustración 36.Uso exploit

```
msf5 > use 0
msf5 exploit(windows/http/rejetto_hfs_exec) >
```

Fuente: Propia

Ilustración 37. Uso exploit

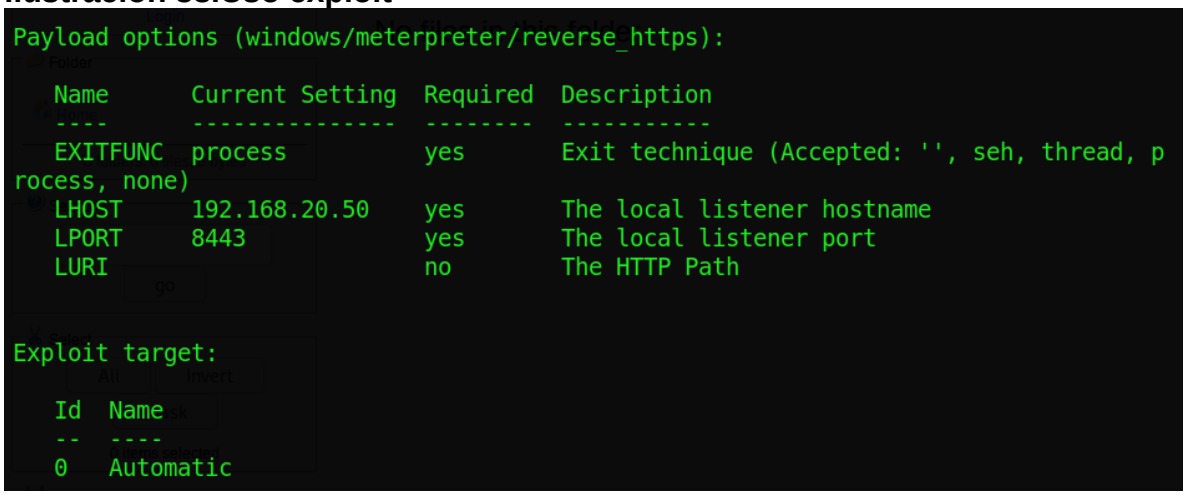
```
msf5 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web serv
er
   Proxies                     no        A proxy chain of format type:host:port[,typ
e:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier,
or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to list
en on. This must be an address on the local machine or 0.0.0.0 to listen on all addr
esses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default i
s randomly generated)
```

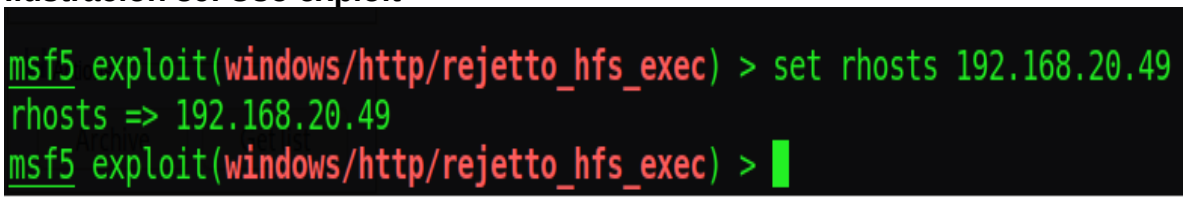
Fuente: Propia

Ilustración 38.Uso exploit



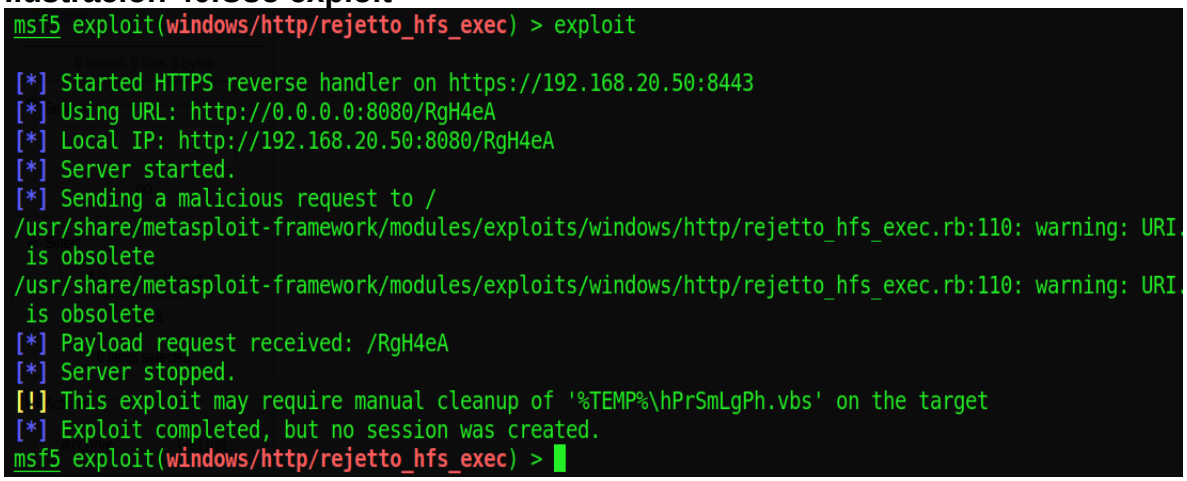
Fuente: Propia

Ilustración 39. Uso exploit



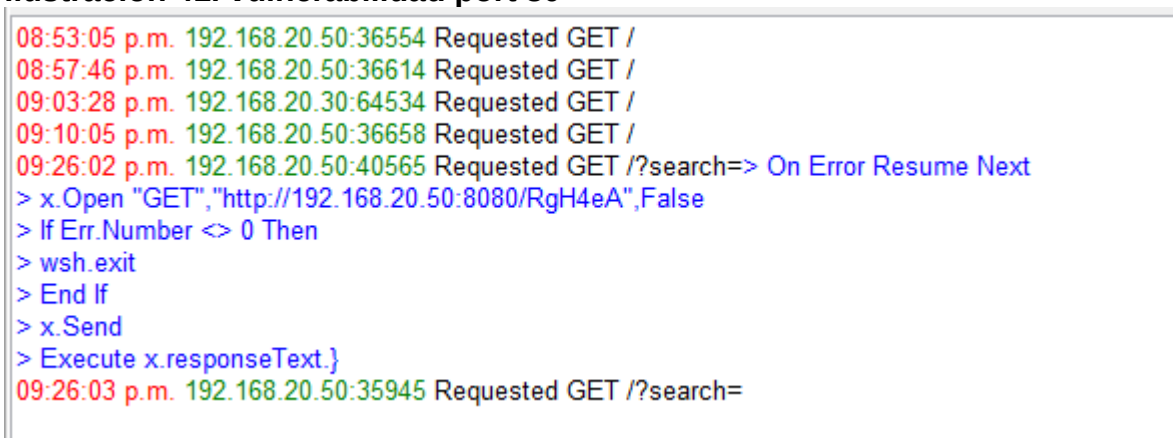
Fuente: Propia

Ilustración 40.Uso exploit



Fuente: Propia

Ilustración 41. vulnerabilidad port 80



Fuente: Propia

Con este último proceso se comprobó que se logró ingresar de manera remota desde Kali Linux a Windows 7 x64 por medio del exploit y se conoció la vulnerabilidad que hay en el puerto 80.

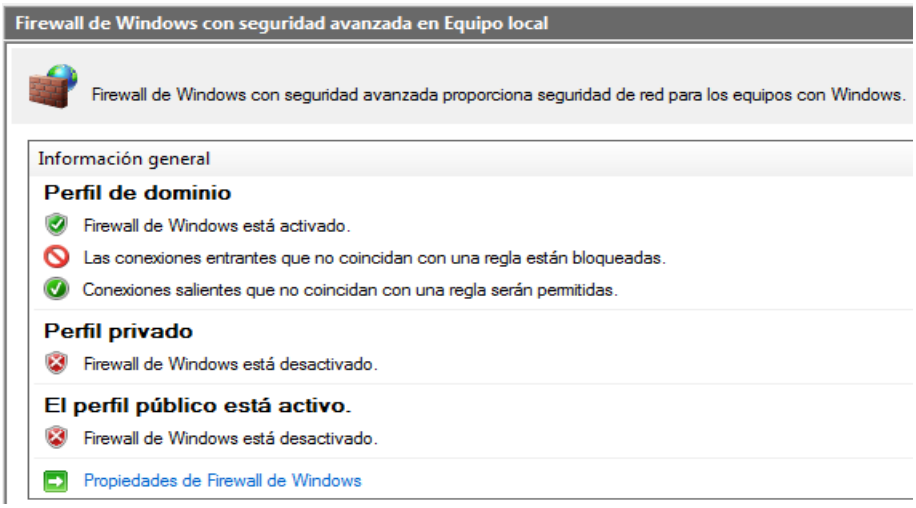
5 ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

5.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

En primer lugar, se debe validar con el equipo Red Team el tipo de ataque que se está presentando, los activos informáticos que impacta este ataque, e identificar las vulnerabilidades que presenta el sistema.

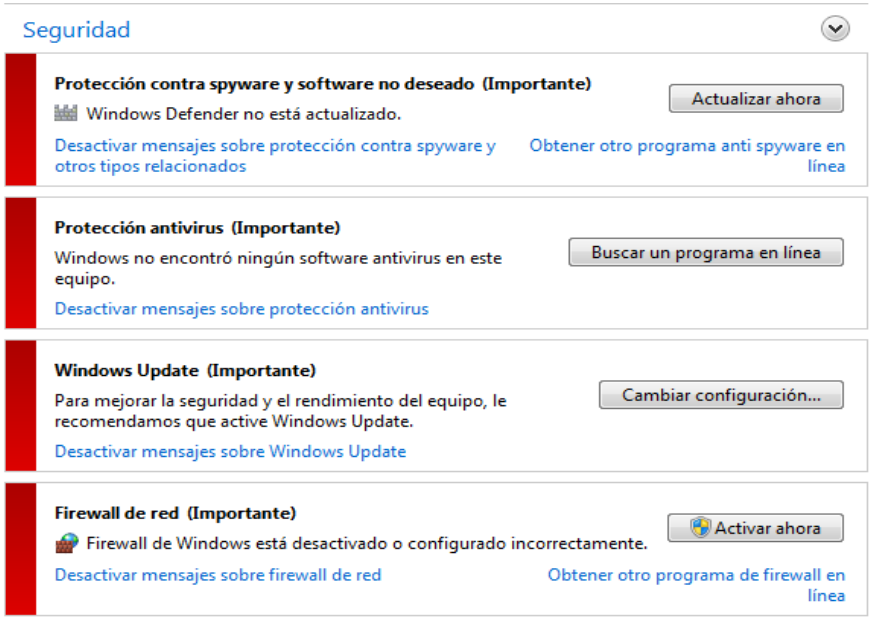
Se evidencia que un equipo con sistema operativo Windows 7 X64 se encuentra con antivirus y firewalls desactivados, procedimiento que se dio en la etapa anterior.

Ilustración 42. Firewall Desactivado Host W7x64



Fuente : Propia

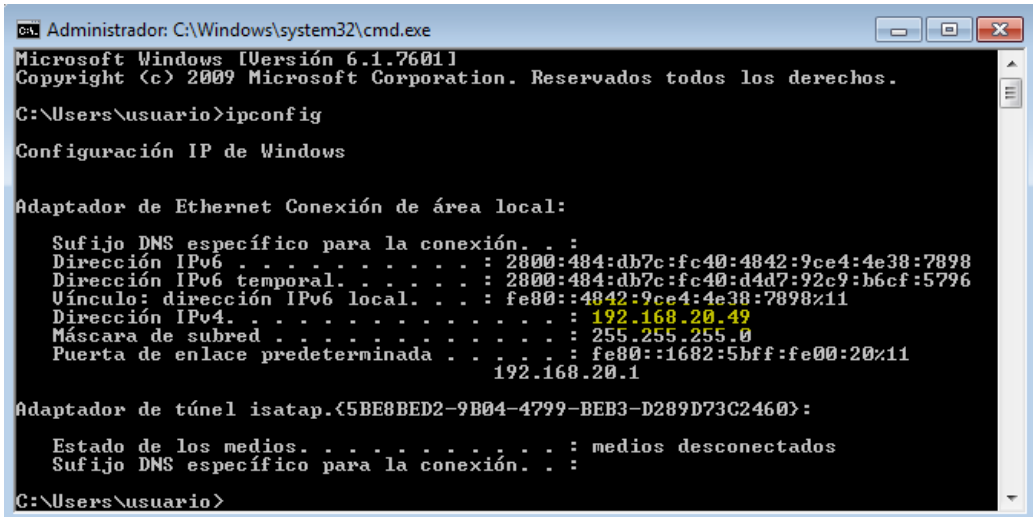
Ilustración 43. Seguridad Host W7x64



Fuente: Propia

Recolección de información de las vulnerabilidades que presenta la red, y estado de la conexión de red del host implicado en el incidente, para realizar aislamiento

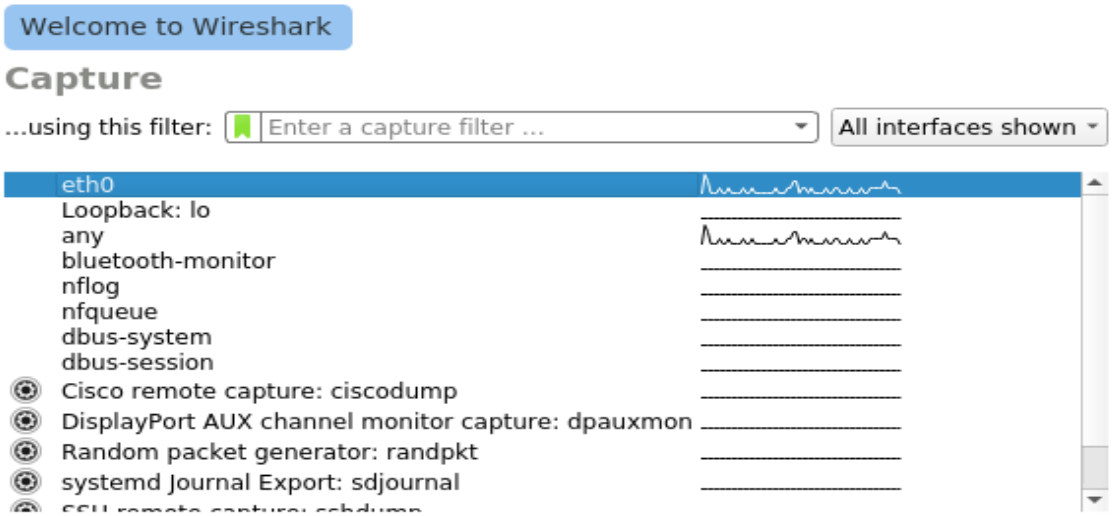
Ilustración 44. IP Host W7x64



Fuente: Propia

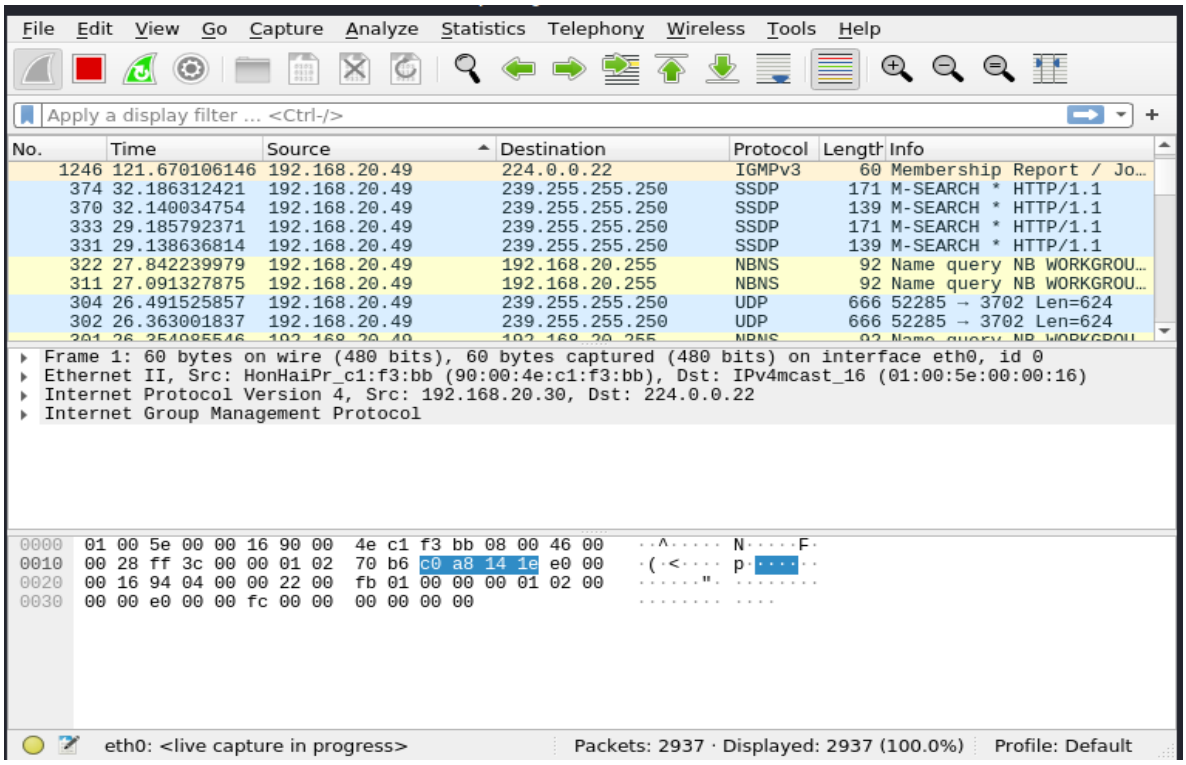
Correr un sniffer desde el host con Kali lunux para capturar el tráfico de información que ingresa y sale a través de la red, en este caso utilizare la herramienta Wireshark.

Ilustración 45. Interface Wireshark



Fuente: Propia

Ilustración 46. Captura Paquetes Wireshark



Fuente: Propia

Al utilizar el sniffer puedo tener claridad de lo que está sucediendo y el tipo de ataque al cual nos estamos enfrentando en el host con Windows 7 X64.

Posteriormente se debe habilitar firewall y antivirus, además se deben correr los parches de actualización del sistema operativo.

El equipo Red Team realizo el informe de vulnerabilidades encontradas en el host con Windows 7 X64 y se procede a cerrar puertos encontrados en la etapa anterior con la herramienta NMAP

5.2 ¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM QUÉ MEDIDAS DE HARDENIZACIÓN PROPONDRÍA PARA QUE EL ATAQUE NO SE REPITA?

Instalación de parches y actualizaciones de seguridad: tener políticas y cronograma para la aplicación regular de parches y actualizaciones de seguridad al sistema operativo y al software, para minimizar las vulnerabilidades conocidas.

Configuración de ajustes de seguridad: configurar ajustes de seguridad como controles de acceso, cortafuegos y sistemas de detección de intrusos puede ayudar a prevenir accesos y ataques no autorizados.

Aplicación de contraseñas y autenticación seguras: las contraseñas seguras y los mecanismos de autenticación, como la autenticación multifactor, pueden dificultar que los atacantes accedan al sistema, así como el deshabilitar los usuarios por default al realizar la instalación de sistemas operativos.

Reducción de la superficie de ataque: mediante la realización de políticas, procedimientos y buenas prácticas el deshabilitar los servicios innecesarios y eliminar el software innecesario puede reducir la superficie de ataque del sistema.

Copias de seguridad Periódicas: práctica importante para proteger los datos y garantizar que no se pierdan en caso de un ciberataque, error humano, fallo del hardware o cualquier otro problema.[15]

5.3 ¿DESCRIBA CON SUS PALABRAS LAS DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS?"

Son dos tipos de equipos de ciberseguridad los cuales poseen diferentes roles y responsabilidades en la protección y respuesta a amenazas informáticas.

El equipo Blue Team tiene como principal objetivo detectar, prevenir y mitigar las amenazas informáticas antes de que ocurran. Esto se lleva a cabo mediante un constante monitoreo a la infraestructura de la empresa, es el responsable de realizar, desarrollar y documentar pruebas de vulnerabilidades, políticas y procedimientos se seguridad. además, pueden implementar medidas de seguridad como firewalls, sistemas de detección de intrusiones

Por otro lado, un equipo de respuesta a incidentes informáticos es el responsable de responder a los incidentes de seguridad cuando ocurren, este quipo tiene como objetivo minimizar el impacto del incidente y restaurar la operatividad de los sistemas de la empresa; este equipo se encarga de investigar, recopilar las causas del incidente, además de recolectar pruebas para reportarlo a las autoridades y realizar el análisis forense

El equipo Blue Team es defensivo y proactivo en la seguridad de la organización, y el equipo de respuesta a incidentes informáticos es reactivo en la seguridad de la organización[16].

5.4 ¿Si dentro de un equipo Blue Team le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

[15] Hardening informático ¿Qué es? (s. f.). Recuperado 21 de marzo de 2023, de https://www.ciset.es/publicaciones/blog/746-hardening

[16] Suárez, P. (2021, julio 29). El CSIRT y el trabajo de un BlueTeam. Escuela tecnológica especializada en programación, ciberseguridad, XR, IoT, IA y blockchain | CODE SPACE. https://codespaceacademy.com/blog/csirt-trabajo-blueteam/

El Center for Internet Security es una organización sin fines de lucro que se dedica a mejorar la seguridad informática a nivel mundial. Lo utilizaría para mejorar la postura de seguridad informática de la empresa; El CIS ofrece un conjunto de controles de seguridad críticos y prácticas recomendadas que pueden ayudar a fortalecer la seguridad de la infraestructura y los sistemas de la organización.

Utilizaría los recursos y herramientas de CIS para implementar los controles de seguridad críticos en la organización, como podrían ser : la identificación y autenticación de usuarios, la monitorización y análisis de eventos, configuraciones seguras, como estudiante de especialización en seguridad informática, aprovecharía los recursos y herramientas de CIS para mejorar la capacidad del equipo Blue Team en la detección y prevención de amenazas informáticas lo cual permite fortalecer la seguridad de la organización [17]

5.5 Explique y redacte las funciones y características principales de lo que es un SIEM.

Se puede definir un SIEM, como un sistema de administración de seguridad de la información que se encarga de recolectar y analizar información proveniente de diversas fuentes como registros de eventos, registros de seguridad, vulnerabilidades, entre otros, con el fin de identificar posibles amenazas y anomalías en la red de una organización.[18]

Las funciones principales de un SIEM son:

Recopilación y correlación de datos: recopila información de diferentes fuentes y correlaciona los eventos para detectar patrones de comportamiento.

Análisis de comportamiento: utiliza algoritmos y análisis estadísticos para identificar comportamientos anómalos en la red.

Detección de amenazas: detecta amenazas de seguridad mediante la identificación de patrones y anomalías en la red.

Respuesta a incidentes: proporciona información detallada y contexto a los equipos de respuesta a incidentes para tomar decisiones informadas.

---

[17] CIS. (s. f.). CIS. Recuperado 21 de marzo de 2023, de https://www.cisecurity.org

[18] ¿Qué es SIEM? | Seguridad de Microsoft. (s. f.). Recuperado 21 de marzo de 2023, de https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

Cumplimiento normativo: ayuda a cumplir con los requisitos de cumplimiento normativo mediante la recopilación y análisis de datos.

Las principales características de un SIEM son:

Recopilación de datos: recopila datos de diferentes fuentes, como registros de eventos, registros de seguridad, vulnerabilidades, etc.

Correlación de eventos: correlaciona eventos para detectar patrones de comportamiento y anomalías.

Análisis de comportamiento: utiliza algoritmos y análisis estadísticos para identificar comportamientos anómalos en la red.

Dashboard e informes: Permiten el monitoreo y estado de seguridad de la red mediante informes y tableros de información

Integración: se integra con otros sistemas de seguridad de la información para proporcionar una solución de seguridad completa.

5.6 Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Firewalls: Los firewalls son una herramienta esencial de contención de ataques informáticos permite filtrar el tráfico de red y bloquear los accesos no autorizado a los sistemas. Estos dispositivos actúan como una barrera de protección entre la red interna y el mundo exterior, y pueden ser hardware o software.
Los firewalls pueden ser configurados para permitir o denegar el acceso a ciertos puertos, protocolos y direcciones IP, y pueden ser personalizados a la medida de las necesidades de la organización

Sistemas de prevención de intrusiones (IPS): Herramienta de contención de ataques informáticos que se utiliza para monitorear el tráfico de red en busca de actividades sospechosas o maliciosas. Estos sistemas utilizan una combinación de técnicas de detección de intrusiones y análisis de tráfico para identificar y bloquear posibles amenazas antes de que puedan causar daño. Los IPS pueden ser hardware o software, y pueden ser configurados para bloquear automáticamente el tráfico de red malicioso o enviar alertas a los equipos de seguridad para una respuesta manual.

Antivirus empresarial: Herramienta de contención de ataques informáticos que se utiliza para proteger los sistemas de una organización contra virus, malware y otras amenazas informáticas. Estos programas se ejecutan en los sistemas de los usuarios y en los servidores de la red, y utilizan una variedad de técnicas de detección de amenazas, como análisis de firmas, heurística y análisis de comportamiento, para detectar y bloquear malware. Los antivirus empresariales también pueden ser configurados para actualizar automáticamente las definiciones de virus y para programar exploraciones regulares de los sistemas para detectar amenazas.[19]

[19] 10 tipos de incidentes de seguridad y cómo manejarlos | Computer Weekly. (s. f.). ComputerWeekly.es. Recuperado 21 de marzo de 2023, de https://www.computerweekly.com/es/tutoriales/10-tipos-de-incidentes-de-seguridad-y-como-manejarlos

VIDEO DE SUSTENTACIÓN

https://youtu.be/tA8VosPWkf4

Ilustración 47. Video Sustentación

Fuente: Propia

CONCLUSIONES

Colombia ha logrado avances significativos en temas tecnológicos y normatividad sobre delitos informáticos, pero aún hay aspectos pendientes en términos de protección de la información y los sistemas informáticos. Es esencial que las empresas inviertan en equipos de ciberseguridad interdisciplinarios para garantizar la estabilidad y el correcto funcionamiento de sus activos informáticos y protegerlos de posibles ataques informáticos.

Todas las empresas, sin importar su tamaño o sector, deben preocuparse por la seguridad informática; Es esencial invertir en equipos de ciberseguridad interdisciplinarios para asegurar la estabilidad y el funcionamiento adecuado de los sistemas de red de la organización y protegerlos de posibles ataques informáticos.

La prevención es clave para evitar ataques informáticos. Las empresas deben contar con procesos, actividades y herramientas actualizadas para evitar que ocurran, o en su defecto, tener las fortalezas necesarias para responder y atacar eficazmente en caso de un posible ataque cibernético.

Es importante que los especialistas en ciberseguridad estén actualizados y tengan conocimientos sólidos sobre las herramientas de contención de ataques informáticos más robustas. Esto les permitirá desempeñar su labor de manera eficaz y reconocida, y proteger los sistemas de red de sus organizaciones de forma más efectiva

La ética es clave para la integridad del empleado y la reputación de la empresa, mientras que la falta de ética puede tener consecuencias desfavorables.

La realización de pruebas de intrusión en redes de datos es una práctica necesaria para identificar las vulnerabilidades en los sistemas y corregirlas. Esto ayuda a mejorar la seguridad, proteger los datos y sistemas de posibles ataques cibernéticos.

Mantener los sistemas operativos actualizados con las últimas actualizaciones del fabricante es esencial para evitar vulnerabilidades y posibles ataques informáticos. Los sistemas operativos desactualizados pueden ser altamente vulnerables a ataques cibernéticos, por lo que es importante actualizarlos regularmente.

RECOMENDACIONES

- Implementar políticas de seguridad claras y específicas que aborden aspectos como la gestión de contraseñas, el acceso a información confidencial, la seguridad física de los equipos, entre otros. Además, es importante que estas políticas sean comunicadas de manera efectiva a todo el personal y se les brinde la capacitación necesaria para cumplirlas correctamente.

- Realizar auditorías y revisiones periódicas de los sistemas y procesos de seguridad para identificar posibles vulnerabilidades y áreas de mejora. Es importante que se establezcan protocolos claros de seguimiento y resolución de problemas.

- Implementar soluciones tecnológicas que permitan proteger la información y los sistemas de la organización, como firewalls, sistemas de detección de intrusiones, encriptación de datos, entre otros.

- Establecer un plan de respuesta a incidentes de seguridad que contemple la identificación rápida de la situación, la contención del problema, la investigación de la causa y la recuperación de los sistemas afectados.

- Promover una cultura de seguridad en la organización, en la que se fomente la conciencia de los riesgos cibernéticos y se incentive la participación de todo el personal en la prevención y mitigación de estos riesgos.

- Identificar los activos de información críticos que tiene la organización y protegerlos adecuadamente. Para ello, se deben llevar a cabo evaluaciones de riesgos y análisis de impacto en el negocio.

- Realizar pruebas de intrusión y análisis de vulnerabilidades: para identificar las vulnerabilidades existentes en los sistemas y aplicaciones de la organización, es recomendable realizar pruebas de intrusión y análisis de vulnerabilidades. Estas pruebas deben ser realizadas por expertos en seguridad informática y se deben llevar a cabo de manera periódica.

- Mantener los sistemas y aplicaciones de la organización actualizados con las últimas versiones de software y parches de seguridad. Esto ayuda a reducir las vulnerabilidades y mejorar la protección contra amenazas de seguridad.

BIBLIOGRAFÍA

10 tipos de incidentes de seguridad y cómo manejarlos | Computer Weekly. (s. f.). ComputerWeekly.es. Recuperado 21 de marzo de 2023, de https://www.computerweekly.com/es/tutoriales/10-tipos-de-incidentes-de-seguridad-y-como-manejarlos

A Rising Tide: New Hacks Threaten Public Technologies - Security Roundup - Trend Micro FR. (s. f.). Recuperado 21 de marzo de 2023, de https://www.trendmicro.com/vinfo/fr/security/research-and-analysis/threat-reports/roundup/a-rising-tide-new-hacks-threaten-public-technologies

Auditando con Nmap y sus scripts para escanear vulnerabilidades. (2015, febrero 12). WeLiveSecurity. https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

Ciberseguridad, P. (2022, marzo 21). *¿Cuál Son La 5 Fases Del Pentesting? - Ciberseguridad*. https://ciberseguridadbidaidea.com/fases-del-pentesting/

CIS. (s. f.). CIS. Recuperado 21 de marzo de 2023, de https://www.cisecurity.org
CVE - CVE-2014-6287. (s. f.). Recuperado 9 de marzo de 2023, de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

CVE-2020-13432. (2020, junio 8). INCIBE-CERT. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-13432

El soporte de Windows 7 finalizó el 14 de enero de 2020—Soporte técnico de Microsoft. (s. f.). Recuperado 9 de marzo de 2023, de https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finaliz%C3%B3-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962

Guía de referencia de Nmap (Página de manual). (s. f.). Recuperado 9 de marzo de 2023, de https://nmap.org/man/es/index.html#man-description

Hardening informático ¿Qué es? (s. f.). Recuperado 21 de marzo de 2023, de https://www.ciset.es/publicaciones/blog/746-hardening

KeepCoding, R. (2022a, noviembre 3). *¿Qué es una shell inversa? | KeepCoding Tech School*. https://keepcoding.io/blog/que-es-una-shell-inversa/

KeepCoding, R. (2022b, noviembre 10). *¿Cómo ejecutar una shell inversa? | KeepCoding Tech School*. https://keepcoding.io/blog/como-ejecutar-una-shell-inversa/

LEY 1273 DE 2009. (s. f.). Recuperado 11 de febrero de 2023, de https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699

Metasploit | Penetration Testing Software, Pen Testing Security. (s. f.). Metasploit. Recuperado 9 de marzo de 2023, de https://www.metasploit.com/

Metasploit-framework | Kali Linux Tools. (s. f.). Kali Linux. Recuperado 9 de marzo de 2023, de https://www.kali.org/tools/metasploit-framework/

MINTIC Colombia—Transparencia. (s. f.). MINTIC Colombia. Recuperado 12 de febrero de 2023, de http://www.mintic.gov.co/portal/715/w3-propertyvalue-111092.html

Nmap | Kali Linux Tools. (s. f.). Kali Linux. Recuperado 9 de marzo de 2023, de https://www.kali.org/tools/nmap/

pve—Proxmox Virtual Environment. (s. f.). Recuperado 12 de febrero de 2023, de https://192.168.20.42:8006/#v1:0:=node%2Fpve:4:5::::::

¿Qué es SIEM? | Seguridad de Microsoft. (s. f.). Recuperado 21 de marzo de 2023, de https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

¿Qué es un firewall? (s. f.). Cisco. Recuperado 21 de marzo de 2023, de https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (1.ª ed.). Editorial Científica 3Ciencias. https://doi.org/10.17993/IngyTec.2018.46

SIEM Implementation: Guide to Security Information & Event Management. (s. f.). Recuperado 21 de marzo de 2023, de https://www.controlscan.com/siem-datasheet/

Solano, A. A. (s. f.). *rm—Borrar ficheros y /o directorios*. Recuperado 12 de febrero de 2023, de https://cambiatealinux.com/rm-borrar-ficheros-directorios

Soluciones de seguridad de endpoints para empresas | Kaspersky. (s. f.). Recuperado 21 de marzo de 2023, de https://latam.kaspersky.com/small-to-medium-business-security

Suárez, P. (2021, julio 29). El CSIRT y el trabajo de un BlueTeam. *Escuela tecnológica especializada en programación, ciberseguridad, XR, IoT, IA y blockchain | CODE SPACE*. https://codespaceacademy.com/blog/csirt-trabajo-blueteam/

Thapa, A. (2016, enero 4). *Rejetto HTTP File Server (HFS) 2.3.x—Remote Command Execution (2)*. Exploit Database. https://www.exploit-db.com/exploits/39161

What is an Intrusion Prevention System? (s. f.). Palo Alto Networks. Recuperado 21 de marzo de 2023, de https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

What is Intrusion Prevention System? | *VMware Glossary*. (s. f.). VMware. Recuperado 21 de marzo de 2023, de https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html

What is Security Information and Event Management (SIEM)? | *IBM*. (s. f.). Recuperado 21 de marzo de 2023, de https://www.ibm.com/topics/siem

https://www.openit.com.ar/wp-content/uploads/2019/02/clement-h-544786-unsplash.png