Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de Magister en Ciberseguridad

AUTOR/ES:

Carvajal Perez Christopher Alexander

Guambaña Macas Jorge Luis

Paguay Espinosa Erick Fabian

TUTOR/ES:

Iván Reyes Chacón

Alejandro Cortés López

Análisis de vulnerabilidades mediante Hacking Ético a una red interna aplicando técnicas como escalada de privilegios

Quito - Ecuador

REINVENTEMOS EL FUTURO

Certificación de autoría

Nosotros, Guambaña Macas Jorge Luis, Paguay Espinosa Erick Fabian, Carvajal Pérez Christopher Alexander declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firma del graduando
Guambaña Macas Jorge Luis

Firma del graduando
(Carvajal Perez Christopher alexander)

Firma del graduando
Paguay Espinosa Erick Fabian

Autorización de Derechos de Propiedad Intelectual

Nosotros, Guambaña Macas Jorge Luis, Paguay Espinosa Erick Fabian, Carvajal Pérez Christopher Alexander en calidad de autores del trabajo de investigación titulado **Análisis de vulnerabilidades mediante hacking ético a una red interna aplicando técnicas como escalonamiento de privilegios**, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, (noviembre 2024)

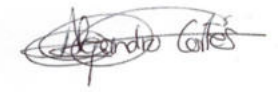
Firma del graduando
Guambaña Macas Jorge Luis

Firma del graduando
(Carvajal Perez ChristopherAlexander)

Firma del graduando
Paguay Espinosa Erick Fabian

APROBACIÓN DE DIRECCIÓN Y COORDINACIÓN DEL PROGRAMA

Nosotros, **Alejandro Cortés López e Iván Reyes Chacón,** declaramos que: Jorge Guambaña, Erick Paguay, Alexander Carvajal, son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



Alejandro Cortés L.

Maestría en Ciberseguridad

Iván Reyes Ch.

Maestría en Ciberseguridad

DEDICATORIA

El presente proyecto de titulación está dedicado a mis familiares por el apoyo brindado en mis estudios, a mis docentes por compartir sus conocimientos y estar siempre al pendiente a resolver cualquier inquietud y Dios por darme sabiduría, salud y permitirme haber llegado a este momento tan importante de mi formación profesional.

Jorge Guambaña, Erick Paguay, Alexander Carvajal

AGRADECIMIENTOS

Agradezco principalmente a Dios por permitirme haber compartido tan buenas experiencias en mis estudios de maestría, gracias a los docentes de la universidad UIDE por compartir sus conocimientos y a mi tutora Lina que siempre estuvo al pendiente para resolver cualquier inquietud.

Agradezco también a quien lee este apartado de mi proyecto de titulación y por permitir que mis experiencias y conocimientos formen parte de su información mental.

Jorge Guambaña, Erick Paguay, Alexander Carvajal

RESUMEN

Con el avance tecnológico y el aumento de dispositivos conectados al internet multiplica los vectores de ataque hacia los sistemas informáticos. En respuesta se realizó un análisis con enfoque de caja gris a la red interna de Mastercleans S.A., realizada desde una estación Kali Linux, se identificaron 7 vulnerabilidades que comprometen la confidencialidad, integridad y disponibilidad de los sistemas de la organización clasificadas por el score CVSS. El análisis fue enfocado hacia la infraestructura de Active Directory de la organización. La cadena de ataque inicio comprometiendo el servidor CASTELLBLACK, el cual no tenía el protocolo SMB firmado, y por ende fue susceptible a ataques de envenenamiento NTLM vía NBT-NS y LLMNR, permitiendo la captura de hashes NTLM incluyendo los del usuario Administrator, y crackearlos con la heramienta hashcat. Se aplicaron técnicas como Pass the Hash que facilito el acceso administrativo al equipo sin credenciales en texto plano. También fue posible la carga de una webshell hacia un sitio web alojado en un servidor IIS que permitió la ejecución remota de código (RCE). Para la escalada de privilegios se abusó del permiso SetImpersonatePrivilege del usuario apppool y se usó la herramienta Petit Potato para escalar privilegios hasta NT Authority\System, además se pudo evadir la solución de Windows Defender aplicando técnicas de ofuscación. Se recomienda que Mastercleans implemente un plan de remediación urgente para abordar los hallazgos críticos y altos, seguido de una evaluación más profunda de Active Directory para fortalecer la seguridad, dificultar ataques y mejorar la detección y respuesta ante actividades sospechosas.

Palabras Claves**:** SSH, vulnerabilidades, escalada de privilegios, RCE, CVSS

ABSTRACT

Technological advancements and the increase in internet-connected devices are multiplying the attack vectors on computer systems. In response, a gray-box analysis was performed on the internal network of Mastercleans S.A., carried out from a Kali Linux workstation. Seven vulnerabilities were identified that compromise the confidentiality, integrity, and availability of the organization's systems, classified by the CVSS score. The analysis focused on the organization's Active Directory infrastructure. The attack chain began by compromising the CASTELLBLACK server, which did not have the signed SMB protocol and was therefore susceptible to NTLM poisoning attacks via NBT-NS and LLMNR, allowing the capture of NTLM hashes, including those of the Administrator user, and cracking them with the hashcat tool. Techniques such as Pass the Hash are applied, which facilitates administrative access to the computer without plaintext credentials. A webshell was also uploaded to a website hosted on an IIS server, enabling remote code execution (RCE). Privilege escalation was achieved by abusing the SetImpersonatePrivilege permission of the apppool user, using the Petit Potato tool to escalate privileges to NT Authority\System. The Windows Defender solution was also evaded by applying obfuscation techniques. Mastercleans recommends implementing an urgent remediation plan to address the critical and high findings, followed by a more in-depth assessment of Active Directory to strengthen security, hinder attacks, and improve detection and response to suspicious activity.

Keywords: *SSH, vulnerabilities, privilege escalation, RCE, CVSS*

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

Capítulo 1: Introducción

La evolución constante de las tecnologías de información da lugar al surgimiento de nuevas amenazas cibernéticas, en el contexto empresarial es indispensable contar con una infraestructura tecnológica capaz de enfrentar ataques cibernéticos. Este proyecto se enfoca en identificar fallos de seguridad que una pequeña empresa pueda tener en su red interna.

1. Planteamiento Del Problema E Importancia Del Estudio

1.1. Definición del proyecto

El proyecto se centrará en realizar un análisis de las vulnerabilidades presentes en una red interna de una organización utilizando técnicas de hacking ético. El objetivo principal es identificar posibles puntos débiles que puedan ser explotados por atacantes malintencionados externos o por miembros de la institución con intenciones maliciosas y probar métodos de escalamiento de privilegios para evaluar la capacidad de un atacante de obtener acceso administrativo y comprometer la seguridad de la red.

Este análisis incluirá varias fases: el reconocimiento de la red, la identificación y explotación de vulnerabilidades, y la implementación de técnicas de escalamiento de privilegios "*Es una situación que ocurre cuando un usuario malicioso explota una vulnerabilidad la cual le permite obtener acceso privilegiado a recursos que, por defecto, no debería tenerlos".* (Laprovittera, 2024)

Se utilizarán herramientas y metodologías reconocidas en el campo de la ciberseguridad para garantizar un análisis riguroso y preciso.

Al final del proyecto, se presentará un informe detallado que incluirá las vulnerabilidades encontradas, el impacto potencial de cada una, las técnicas de escalamiento utilizadas y las recomendaciones para mitigar los riesgos identificados. Este informe servirá como una guía para mejorar la seguridad de la red interna de la organización y protegerla contra posibles ataques futuros, ya sea de fuentes externas o internas.

1.2. Alcance del proyecto

El proyecto abarca el análisis de la red interna de la organización, incluyendo servidores, estaciones de trabajo, dispositivos de red, sistemas de almacenamiento y aplicaciones internas. Se realizarán actividades de reconocimiento, identificación y explotación de vulnerabilidades, así como la implementación de técnicas de escalamiento de privilegios, excluyendo sistemas y aplicaciones externas, dispositivos móviles personales y redes inalámbricas fuera del alcance de la red interna. Todo el trabajo se realizará con el

consentimiento de la organización, garantizando la confidencialidad y el cumplimiento de normativas de ciberseguridad. Se utilizarán herramientas como nmap, netexec, hashcat, smbclient y bloodhound para identificar vulnerabilidades críticas y proponer soluciones, culminando en un informe detallado de los hallazgos y recomendaciones.

1.3. Naturaleza o tipo de proyecto

Este proyecto es de carácter técnico y aplicado dentro del ámbito de la ciberseguridad, centrado en utilizar metodologías de hacking ético para evaluar la seguridad de la red interna de una organización. Se emplearán técnicas avanzadas de análisis y explotación de vulnerabilidades para identificar debilidades en los sistemas y procesos de seguridad. El proyecto combina conocimientos teóricos de ciberseguridad con habilidades prácticas en el uso de herramientas y técnicas de análisis de vulnerabilidades y escalamiento de privilegios.

Desarrollado en un entorno controlado y autorizado, el proyecto asegura el cumplimiento de estándares éticos y legales. Su enfoque es tanto exploratorio como evaluativo, buscando no solo documentar las vulnerabilidades presentes sino también evaluar su impacto potencial y proponer medidas correctivas. El objetivo final es proporcionar información valiosa para mejorar la postura de seguridad de la organización, previniendo posibles ataques y fortaleciendo la protección de datos y recursos críticos.

1.4. Objetivos

Objetivo general

Identificar vulnerabilidades en una red interna mediante la implementación de técnicas de hacking ético, con un enfoque especial en el escalamiento de privilegios.

Objetivo especifico

- Realizar un reconocimiento completo de la red interna de la organización que permita identificar posibles vectores de ataque para acceso inicial.
- Identificar y explotar vulnerabilidades conocidas en infraestructuras tecnológicas basadas en directorio activo (Microsoft) utilizando herramientas de seguridad ofensiva.
- Revisar las políticas de contraseñas, la implementación de la autenticación multifactor, los mecanismos de autorización basados en roles y la gestión de privilegios.
- Realizar pruebas de evasión hacia herramientas de seguridad integradas en sistemas

operativos Windows.

- Identificar y explotar vulnerabilidades en aplicaciones web alojadas en servidores IIS
- Probar técnicas de escalamiento de privilegios para evaluar la capacidad de un atacante para obtener acceso administrativo.
- Clasificar vulnerabilidades identificadas mediante el score obtenido en cvss.
- Soluciones y recomendaciones para mitigar las vulnerabilidades encontradas.

1.5 Justificación e importancia del trabajo de investigación.

Dado el incremento de las amenazas cibernéticas y su creciente sofisticación debido a la implementación en muchos de los casos de herramientas de inteligencia artificial en sus ataques, es crucial que las organizaciones realicen evaluaciones de vulnerabilidades periódicamente para proteger sus activos de información y recursos esenciales. Este proyecto se enfoca en el análisis de vulnerabilidades y técnicas de escalamiento de privilegios mediante hacking ético, para identificar fallas que podrían ser explotadas por atacantes, ya sean externos o internos. Detectar y mitigar estas vulnerabilidades proactivamente es fundamental para evitar pérdidas financieras, daños a la reputación y compromisos de datos confidenciales.

Este trabajo de investigación es vital por varias razones. Primero, mejora la seguridad de la red al identificar y corregir vulnerabilidades críticas. Segundo, ayuda a prevenir ataques internos como el escalamiento de privilegios, proporcionando una comprensión detallada de cómo un atacante podría obtener acceso administrativo. Además, el presente proyecto de titulación cumple con la legislación ecuatoriana, que exige a las entidades implementar un sistema de gestión de seguridad de la información con un análisis de vulnerabilidades periódico, evitando sanciones y fortaleciendo la confianza de clientes y socios. Finalmente, el proyecto ofrece formación valiosa para el personal de tecnologías de la información y proporciona recomendaciones para la mejora continua de la infraestructura de seguridad, fortaleciendo la resiliencia frente a amenazas cibernéticas.

En este presente trabajo se busca detallar la evolución de las amenazas, destacar cómo las amenazas cibernéticas se vuelven cada vez más sofisticadas y cómo los atacantes utilizan nuevas técnicas para explotar vulnerabilidades. Calcular un impacto en la reputación de esta forma explicar cómo un incidente de seguridad puede dañar la reputación de una organización y afectar su relación con clientes y socios. Mediante un cumplimiento normativo mencionar

las regulaciones y estándares de seguridad que aplican a tu organización y cómo este proyecto contribuye a cumplir con ellos.

2. PERFIL DE LA ORGANIZACIÓN.

2.1. NOMBRE, ACTIVIDADES, MERCADOS SERVIDOS Y PRINCIPALES CIFRAS

2.1.1. Nombre de la empresa

Mastercleans S.A

2.1.2. Misión, visión, valores

Misión: Mastercleans S.A es una empresa dedicada al servicio de la sociedad que se encarga de Facilitar los procesos de aseo, limpieza y desinfección de nuestros clientes.

Visión: Ser la mejor empresa que provea servicios relacionados a la solución de limpieza y desinfección para bienestar y comodidad de nuestros beneficiados.

Valores: Disciplina, Honestidad, Honradez

2.1.3. Actividades, marcas, productos y servicios

Actividades: Toda clase de limpieza de su hogar o de su empresa

Marcas: Cascade. Dawn. Lysol. Clorox. Affresh.

Productos: Desinfectantes, aromatizantes, limpia vidrios, escobas, trapeadores, abrillantadoras entre otras, todo lo relacionado a la necesidad del cliente.

2.1.4. Ubicación de la sede

La Sede de la empresa se encuentra ubicada en la ciudad de Quito

2.1.5. Ubicación de las operaciones

La empresa cuenta con diferentes sedes es así que se encuentra en la ciudad de Quito, Guayaquil y Ambato.

2.1.6. Propiedad y forma jurídica

La empresa Mastercleans S.A es una sociedad cooperativa la que esta constituidas por varias personas en este caso consta de 4 personas que son hermanos

2.1.7. Mercados servidos o ubicación de sus actividades de negocio

La empresa maneja el mercado servido en base a 2 parámetros

1.-Producto. La empresa cuenta únicamente con productos importados de mercados americanos asi como con máquinas americanas para el servicio

2.-Punto de vista geográfico. La empresa se encuentra prestando servicios en 3 ciudades de las más recurridas Quito, Guayaquil, Ambato

2.1.8. Tamaño de la organización

La organización consta de 50 empleados

2.1.9. Información sobre empleados y otros trabajadores

La empresa cuenta con

03 guardias de seguridad

01 gerente

01 subgerente

01 coordinador de Operaciones

01 coordinador de Talento Humano

01 coordinador de Bienestar social

01 coordinadores Financieros

02 coordinadores de Marketing

40 trabajadores designados a las actividades

2.1.11. Principales cifras, ratios y números que definen a la empresa

La empresa cuenta con un ingreso de $10.000 mensuales en base a los diferentes contratos que maneja

Tiene un egreso en insumos de $3000 mensuales.

Tiene un egreso en Sueldos del personal de $4000 mensuales.

Tiene una Ganancia neta de $3000 mensuales.

2.1.12. Modelo de negocio

La empresa maneja 01 modelo de gestión

La vente directa que es el ofrecimiento al cliente explicándole los beneficios que ofrece de manera directa o a su vez por medios del marketing

2.1.13. Grupos de interés internos y externos

Grupo de interés interno: Gerente, subgerente que son los encargados de verificar el correcto funcionamiento

Grupo de interés externo: Clientela que a su vez busca excelente calidad y cómodos precios

2.1.14. Otros datos de interés

La empresa está proyectándose a 1 año extender sus sucursales a las ciudades de Cuenca, Puyo y Riobamba

La empresa se encuentra realizando planificaciones para que sus trabajadores se comiencen a capacitar en tema de Aseo con certificaciones norteamericanas

Capítulo 2: Marco Teórico

Ciberseguridad

La ciberseguridad hace referencia a la seguridad de la información digitalizada, nos ayuda a mantener seguro los datos contra ataques, daño o accesos no autorizados. Autores como (SAYAGO HEREDIA, 2021), (Voutssas, 2010) definen a la seguridad informática como "el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización". Según, (Parra Bolaños, 2024) la ciberseguridad es "un conjunto de acciones, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos" con la finalidad de proteger los datos de una organización de terceros. El concepto de cultura de ciberseguridad según (Ghirardotti & Renna, 2022) "se refiere al conocimiento, creencias, percepciones, actitudes, suposiciones, normas y valores de las personas con respecto a la ciberseguridad y cómo se manifiestan en el comportamiento de las personas con las tecnologías de la información."

La seguridad informática según, (Pons Gamon, 2017) involucra aspectos importantes como la integridad de los datos, indispensable para garantizar que una información sea fiable; sin embargo la constante evolución tecnológica da origen a nuevas amenazas y para contrarrestar es necesario aplicar buenas prácticas actualizadas como las estipuladas en la norma ISO 27000(Organización internacional de normalización), este organismo internacional indica que la seguridad informática debe mantener la confidencialidad, integridad y disponibilidad de la información mediante un enfoque de gestión de riesgos con el fin de aplicar los controles adecuados.

"El hacking ético es una disciplina que las empresas de seguridad privada pueden adoptar dentro de sus servicios de consultoría para a ser frente a las exigencias de la actualidad en materia de ciberseguridad." (Guevara, 2022)

"El hacking consiste en acceder desde algún lugar del ciberespacio a un ordenador privado valiéndose de deficiencias en los sistemas de seguridad" (Sanchez Dávila, 2019), utilizan las mismas técnicas que los intrusos, pero sin dañar ni robar información. (Giannone, Amatriain, Rodríguez, & Merlino, 2018)

Como parte de la gestión de riesgo es evaluar las vulnerabilidades de un sistema de información para el caso de estudio se tomará la parte activa de la ciberseguridad aplicando hacking ético a una red local utilizando técnicas de escalada de privilegios.

Escalada de privilegios

La escalada de privilegios según (CyberZaintza, s.f.)"es la acción de explotar un error o mala configuración para permitir a un supuesto atacante obtener más permisos y un mayor nivel de acceso a sistemas o aplicaciones de lo que pretendían sus administradores."

"Cuando las funcionalidades asociadas al control de acceso son deficientes, un atacante puede, a menudo, comprometer la aplicación completa, tomando el control de la funcionalidad de administración y teniendo acceso a datos sensibles que pertenecen a otros usuarios" (Romaniz, 2008).

Comúnmente esta técnica de hacking ético es utilizada para obtener acceso a la red en un nivel mayor, obteniendo permisos y controles adicionales sobre los recursos del sistema. "Si la PC de un empleado carece del software de seguridad más reciente, puede infectar otras máquinas a través de la red de la empresa" (Zaidman, 2017)

Existen dos tipos de escalada, puede ser vertical u horizontal.

Escalada vertical: se considera cuando el atacante obtiene permisos adicionales como por ejemplo los de administrador.

Escalada horizontal: se considera cuando el atacante se mantiene en mismo nivel, sin embargo, puede visualizar información que no debería estar disponible para él.

En la actualidad existen muchas aplicaciones en el área de seguridad de la información que son útiles para detectar vulnerabilidades en sistema o en una red, para ambientes de prueba es necesario utilizar plataformas de virtualización como virtual Box.

Virtual Box

"Oracle VirtualBox es una aplicación de virtualización multiplataforma. Esto significa que amplía las capacidades de su equipo actual para que pueda ejecutar múltiples sistemas operativos en múltiples máquinas virtuales (VM) simultáneamente." (VirtualBox, 2025)

Kali Linux

"Kali Linux es una distribución basada en GNU/Linux Debian, destinado a auditorias de seguridad y pruebas de penetración avanzadas" (Caballero Quezada, 2025)

Python

Según (Gonzales Duque, 2025) es un lenguaje de programación creado por Guido van Rossum a principios de los años 90 cuyo nombre está inspirado en el grupo de cómicos ingleses "Monty Python". Es un lenguaje similar a Perl, pero con una sintaxis muy limpia y que favorece un código legible. Se trata de un lenguaje interpretado o de script, con tipado dinámico, fuertemente tipado, multiplataforma y orientado a objetos.

Netdiscover

Según (Kali, 2024)es una herramienta de reconocimiento de direcciones activas/pasivas, desarrollada principalmente para redes inalámbricas sin servidor DHCP, durante el wardriving. También se puede utilizar en redes concentradas/conmutadas.

Nmap

Según (Orebaugh & Pinkard, 2011) Nmap, o Mapeador de Redes, es una herramienta gratuita de código abierto disponible bajo la Licencia Pública General GNU publicada por la Free Software Foundation. Es utilizada principalmente por administradores de red y profesionales de seguridad informática para analizar redes corporativas en busca de hosts activos, servicios específicos o sistemas operativos específicos.

NETEXEC

Según (Chandel, 2024) " Ofrece una amplia gama de funciones para la enumeración de Active Directory, la validación de credenciales, los ataques Kerberos y la escalada de privilegios". Permite a los administradores supervisar, controlar y optimizar la infraestructura de red de manera eficiente.

SMBCLIENT

Según (Red Hat,Inc., 2024) "Permite acceder a los recursos compartidos de un servidor SMB, de forma similar a un cliente FTP de línea de comandos." Es esencial para el control de recursos en redes, presenta una interfaz que agiliza la conexión y a su vez la copia de datos.

IMPACKET

Según (IMPACKET, 2023) “Es una colección de clases de Python para trabajar con la red protocolos. se centra en proporcionar información de bajo nivel acceso programático a los paquetes y para algunos protocolos.”

HASHCAT

Según (Hascat, 2023) “Es la utilidad de recuperación de contraseñas más rápida y avanzada del mundo, que admite cinco modos de ataque únicos para más de 300 algoritmos de hash altamente.” Es conocido por su capacidad para usar la GPU línea por lo que el procesamiento es realmente rápido, ideal para auditar seguridad de contraseñas.

XFREERDP

Es un cliente de software libre de RDP que según (FreeRDP, 2023) “Esta herramienta proporciona una implementación completa del protocolo RDP, permitiendo la conexión a escritorios remotos en entornos Windows y Linux”.

POWERVIEW

Es una herramienta de post-explotación de Windows utilizada que según (PowerSploit, s.f.) “permite a los usuarios realizar consultas sobre la infraestructura de Active Directory, incluyendo la enumeración de usuarios, grupos y relaciones de confianza, lo que es esencial para identificar vectores de ataque."

Según, (Chicaiza, 2019) es una herramienta para la evaluación y gestión de vulnerabilidades, así lo indica en su sitio web además que ayuda a exponer y cerrar las brechas de seguridad prioritarias que colocan a los negocios en riesgo.

Esta plataforma ofrece cobertura de análisis para un grupo mayoritario de activos de TI considerados entre ellos:

- Dispositivos de red
- Dispositivos móviles
- Sistemas operativos
- Actualización de controladores hasta paquetes de productividad de office.

Metasploit

Es un marco de pruebas que según, (De la Cruz Gámez, 2022) “ayuda a los equipos de seguridad a hacer más que simplemente verificar vulnerabilidades, administrar evaluaciones de seguridad y mejorar la concienciación sobre seguridad”

Mapeo de Red

Es un proceso que según (ProgressWhatsUp Gold, 2023) “Es utilizado para descubrir y visualizar la conectividad de red física y virtual a través de un grupo de Tareas que facilitan la creación de un mapa de red.”

Vector de Ataque

Es un medio que según (Dávila, 2021) “un hacker malicioso puede hacerle llegar un malware a una víctima”.

Tipos de ejecución

Según, (López de Jimenez, 2016) los tipos de ejecución se divide en tres partes prueba de caja negra, prueba de caja blanca y prueba de caja gris. Los test de penetración se basan en la detección de vulnerabilidades para fortalecer el sistema objetivo, (Hajdarevic & Dzaltur, 2015)

Prueba de caja negra: el atacante no tiene idea del sistema que va atacar y solo se dedica en recopilar información. “Son pruebas ofensivas que simulan de la forma más real, un posible ataque por un cibercriminal” (Lazo Canazas, 2021).

Prueba de caja blanca: el atacante realiza pruebas de penetración exhaustivas en base a la información brindada. “En este nivel se puede llegar incluso a tener como punto de inicio del análisis, el código fuente de la aplicación web” (Lazo Canazas, 2021).

Prueba de caja gris: el atacante realiza pruebas de penetración al sistema en base a la limitada información proporcionada por el dueño del sistema.

“Las pruebas de penetración son procesos para detección de vulnerabilidades que se aplican hacia un sistema o dispositivo específico, llamado también objetivo de análisis” (Hualpa Oscas, 2022).

Capítulo 3. Metodología para el Análisis de Vulnerabilidades en la Red Interna de Mastercleans S.A. mediante Técnicas de Hacking Ético

Cuando se realizan pruebas de pentesting o Ethical Hacking es necesario llevarlas a cabo implementando metodologías basadas en marcos de ciberseguridad robustos como NIST o OSSTMM, en donde se dé cobertura completa a cada fase. En este ejercicio controlado se utilizó una metodología que está apegada al estándar OSSTMM, cuya metodología consta de las siguientes etapas.

Figura 1

Metodología OSSTMM

Nota: Metodología basada en OSSTMM.

1. **Recolección de información.**

En esta fase es totalmente pasiva, es decir no se está interactuando con los servidores, entre las actividades se realiza se tiene:

- Búsquedas mediante OSINT.
- Registros DNS, Whois, reverse whois,
- Búsqueda de inversa de imágenes, DNS, whois.
- Correos de empleados en redes sociales
- Fugas de credenciales.
- Código expuesto en servidores de terceros (GitHub, Gitlab)

- Archivos históricos.

2. **Enumeración.**

En esta etapa se interactúa con los objetivos, algunas actividades se tienen:

- Escaneo de puertos, servicios, OS.
- Identificación de usuarios.
- Identificación de infraestructura tecnológica
- Escaneo de vulnerabilidades.

3. **Análisis de vulnerabilidades**

En esta fase se investiga a fondo cual es el camino más factible para poder comprometer la organización.

- Modelado de infraestructura
- Identificación de ataques
- Identificación de fallos conocidos

4. **Explotación.**

Con las vulnerabilidades identificadas y validadas, la cuarta fase implicará la explotación controlada de dichas vulnerabilidades basado en el estándar de ejecución de pruebas de penetración que son descritas según (Chuqui Quille & Orellana González, 2023)

En esta fase se explota las vulnerabilidades identificadas en pasos anteriores, entre ello tenemos:

- Ataques hacia recursos de red
- Explotando fallos conocidos
- Fuerza bruta hacia servicios
- Ataques hacia aplicaciones web
- Ataques hacia aplicaciones cliente/servidor
- Ataques enfocados en active directory
- Técnicas de captura de trafico
- Extracción de evidencias

- Escalada de privilegios
- Saltando entre redes (pivoting)
- Saltando soluciones de seguridad Firewalls, IDS, IPS.

5. **Documentación.**

   Documentación de hallazgos encontrados.

- Generación de pre-informe con fallos muy críticos.
- Generaciones informes técnicos
- Generación informes ejecutivos
- Presentación de resultados.

FASE DE RECONOCIMIENTO

La primera fase se enfoca en la recopilación de información sobre la red interna de Mastercleans S.A., incluyendo servidores, estaciones de trabajo, dispositivos de red, y sistemas de almacenamiento que soportan las actividades clave de la empresa. Utilizando herramientas como Nmap que según (Moncho Terol, s.f.) “permite encontrar información específica y a menudo oculta en Internet”.

Como es una prueba hacia una red interna, este paso se lo va a saltar, en entornos reales se debe seguir esta etapa, que es fundamental para tener éxito en las pruebas de penetración.

FASE DE ENUMERACIÓN.

Para poder utilizar los nombres de hosts es importante agregar los siguientes DNS en el archivo /etc/hosts

Figura 2

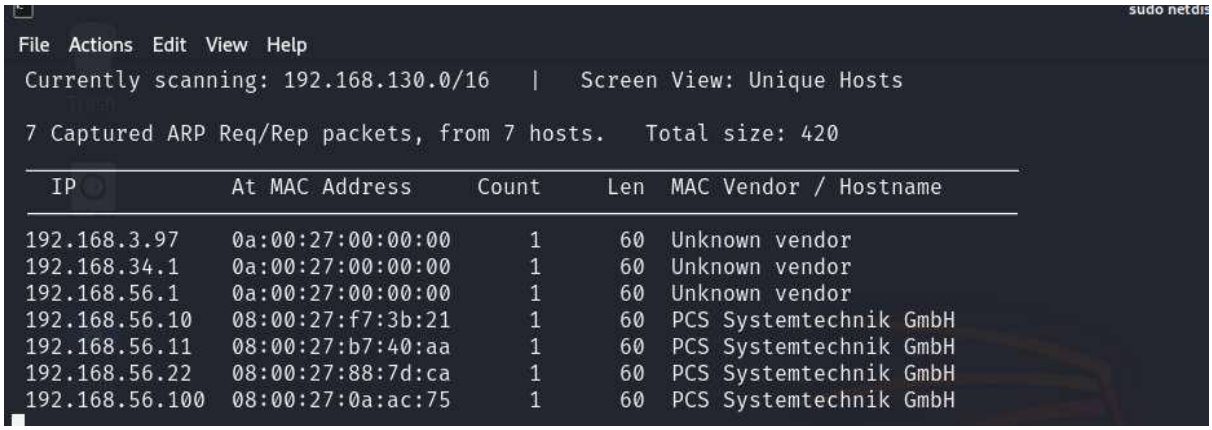
Herramienta netdiscover

Nota: Visualización de los dominios en la red.

Para realizar el descubrimiento de activos que están conectados en la misma red se utilizó la herramienta netdiscover, el resultado es el siguiente.

Figura 3

Ejecución de la herramienta Netdiscover

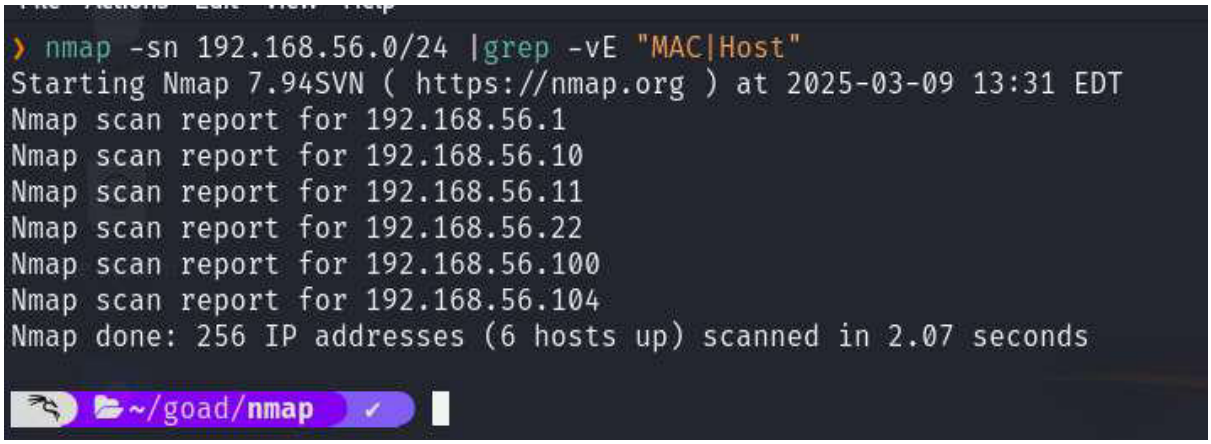


Nota: Se visualiza los activos levantados en la red.

Se realizó un escaneo para identificar todas las direcciones IP activas dentro segmento de red interna, que es 192.168.56.0/24, para ello se usó el siguiente comando de nmap, esto realizó un escaneo ICMP para identificar IP activas, las IP que son del AD son 192.168.56.10 192.168.56.11 y 192.168.56.22, además la del equipo kali (atacante) 192.168.56.104.

Figura 4

Herramienta Nmap



Nota: Se visualiza las ip activas en el segmento de red 192.168.56.0/24

Con las direcciones IP activas identificadas el siguiente paso fue escanear los puertos abiertos en cada HOST, de la misma manera se utilizó la herramienta nmap. Y se guardó la salida en los 3 tipos diferentes de extensiones.

Comando ejecutado al HOST 192.168.56.10

Figura 5

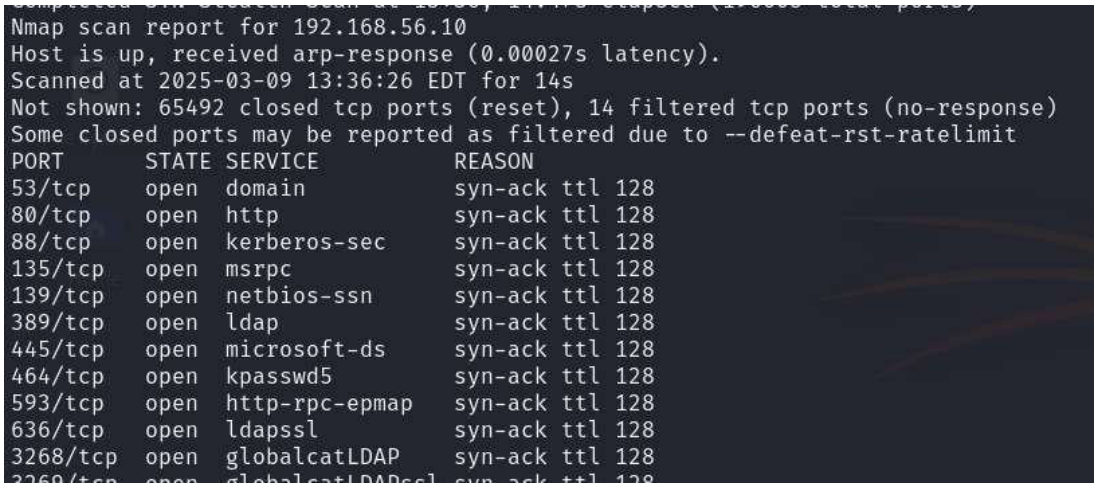
Herramienta para escanear puertos abiertos en la red 192.168.56.10

Nota: Se visualiza el comando ejecutado para escanear los puertos abiertos

Resultados obtenidos del escaneo.

Figura 6

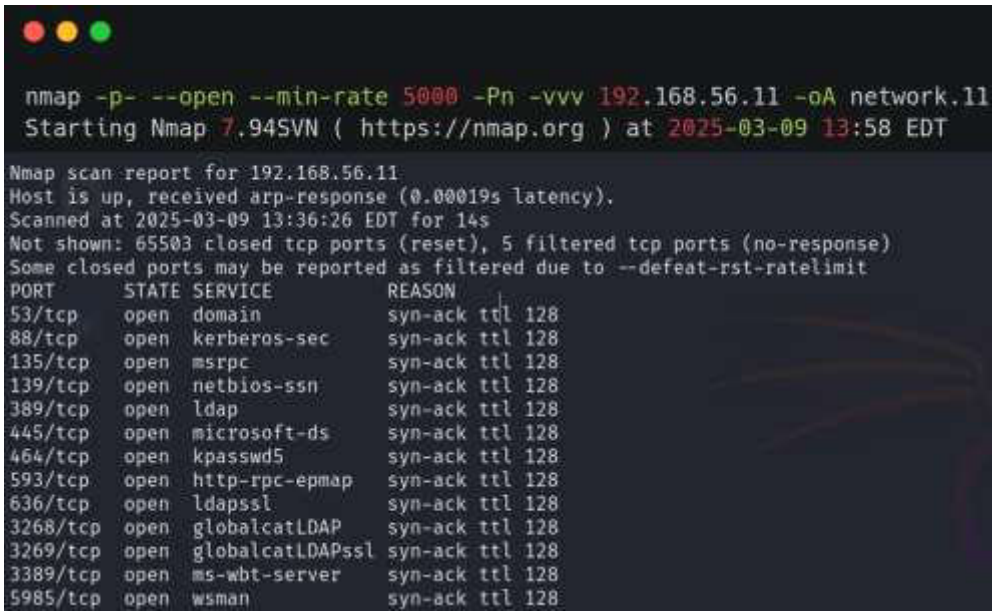
Resultados del escaneo a la red 192.168.56.10



Nota: Se visualiza los puertos abiertos y los servicios que se ejecutan en la red 192.168.56.10

Figura 7

Ejecución del escaneo al HOST 192.168.56.11



Nota: Se visualiza los puertos y servicios que se ejecutan en la red 192.168.56.11

Figura 8

Ejecución del escaneo al Host 192.168.56.22

```
Nmap scan report for 192.168.56.22
Host is up, received arp-response (0.00022s latency).
Scanned at 2025-03-09 13:36:26 EDT for 14s
Not shown: 65516 closed tcp ports (reset)
PORT      STATE SERVICE       REASON
80/tcp    open  http          syn-ack ttl 128
135/tcp   open  msrpc         syn-ack ttl 128
139/tcp   open  netbios-ssn   syn-ack ttl 128
445/tcp   open  microsoft-ds  syn-ack ttl 128
1433/tcp  open  ms-sql-s      syn-ack ttl 128
3389/tcp  open  ms-wbt-server syn-ack ttl 128
5985/tcp  open  wsman         syn-ack ttl 128
5986/tcp  open  wsmans        syn-ack ttl 128
47001/tcp open  winrm         syn-ack ttl 128
49664/tcp open  unknown       syn-ack ttl 128
```

Nota: Se visualizan los puertos y servicios ejecutados en la red 192.168.56.22

Luego de identificar todos los puertos abiertos el siguiente paso es averiguar cuál es la versión de cada servicio que se está ejecutando en cada servidor, de la misma manera la herramienta por excelencia es nmap, ejecutado de la siguiente manera, se guardó el reporte en formato HTML para mejorar la visualización.

Figura 9

Versión de servicios en la red 192.168.56.10

Nota: Se visualiza la versión de los servicios ejecutados en la red 192.168.56.10

Figura 10

Versión de servicios en la red 192.168.56.11

Nota: Se visualiza la versión de los servicios ejecutados en la red 192.168.56.11

Figura 11

Versión de servicios en la red 192.168.56.22

Nota: Se visualiza la versión de los servicios ejecutados en la red 192.168.56.22

FASE DE ANÁLISIS

Se identificó que la infraestructura completa depende de la tecnología de Microsoft Directorio Activo lo que orienta los esfuerzos de ataque hacia esta tecnología ampliamente utilizada. Los vectores de explotación se detallan a continuación.

- Ataques hacia protocolos comunes, se identificaron y explotaron fallos conocidos hacia servicios/puertos: FTP, SMB, RDP, KERBEROS, NTLM, NETBIOS.
- Identificación y explotación de permisos mal asignados a usuarios y grupos.
- Identificación y explotación de aplicaciones web vulnerables, se analizaron aplicaciones web alojadas en el servidor IIS en busca de fallos conocidos como inyecciones SQL, o carga de archivos maliciosos.
- Se intentó obtener y crackear contraseñas débiles o reutilizadas en el ecosistema de Windows AD, utilizando técnicas como los ataques conocidos: AS-REP roasting, Kerberoasting, y pass the hash contra el protocolo Kerberos y NTLM.
- Acceso indebido a recursos compartidos, se inspeccionaron unidades de red o carpetas compartidas.
- Explotación de fallos por configuraciones incorrectas, se identificó errores comunes en el Directorio Activo, como políticas de grupo (GPOs) mal definidas.
- Se intentó saltarse las soluciones de seguridad integradas por defecto en Windows.

FASE DE EXPLOTACIÓN

Enumeración de equipos mediante netexec.

Se identificó las versiones de los OS, además se pudo analizar si los mismos están firmados para SMB, en este caso el equipo 192.168.56.22 no está firmado.

Figura 12

Enumeración con netexec

Nota: Se visualiza las versiones de sistemas operativos que no se encuentran firmados por smb

Enumeración de recursos compartidos.

Mediante una sesión nula, se enumeró recursos hacia todos los equipos en la red 192.168.56.0/24

Figura 13

Enumeración de recursos

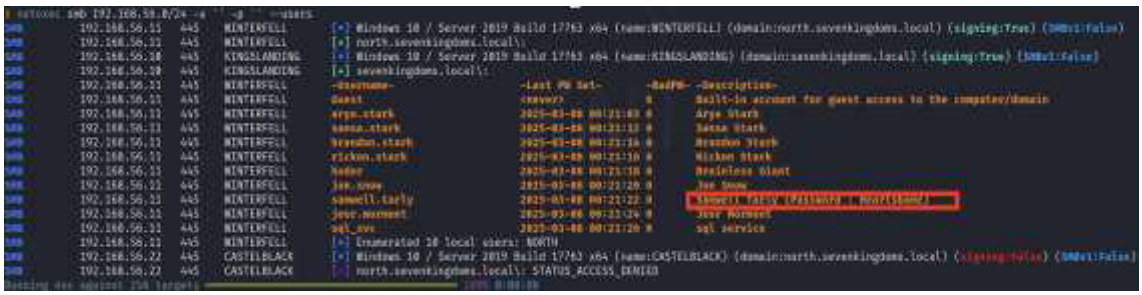
Nota: Se visualiza los recursos en los equipos de la red 192.168.56.0

Enumeración de usuarios en todo el segmento de red.

Se identificó que el HOST 192.168.56.11 enumeró usuarios enviándole una sesión nula(usuario y contraseña vacío), se ha identificado una contraseña del usuario samell.tarly que está en la descripción del usuario.

Figura 14

Numeración de usuarios con netexec.



Nota: Se visualiza los usuarios en la red 192.168.56.0

Enumeración de política de contraseñas.

Con la herramienta netexec fue posible enumerar como está definida la política de contraseñas del dominio, y con esta información se pudo crear patrones para los diccionarios de fuerza bruta.

Figura 15

Numeración de políticas de contraseña

Nota: Se visualiza las políticas de contraseña en el equipo 192.168.56.11

Resumen de enumeración de usuarios.

Figura 16

Usuarios en la red 192.168.56.11

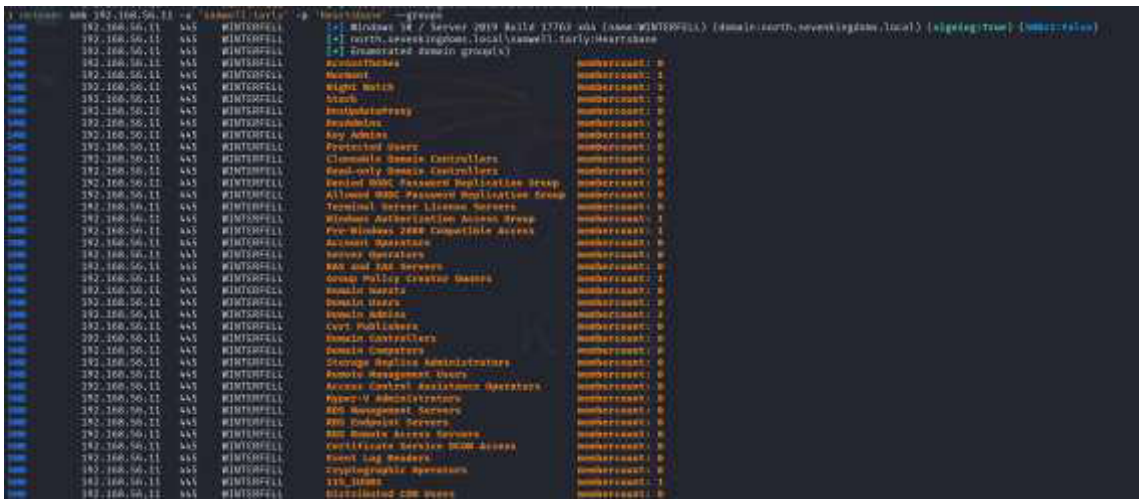
Nota: vista resumen de los usuarios encontrados con netexec.

Enumeración de usuarios con credenciales

Con el usuario samell.tarly que se ha encontrado es posible enumerar más información del dominio **nort**.**sevenkingdoms**.**local**, estos son los grupos que perecen al dominio, y los miembros asociados a cada uno.

Figura 17

Enumeración de usuarios con credenciales

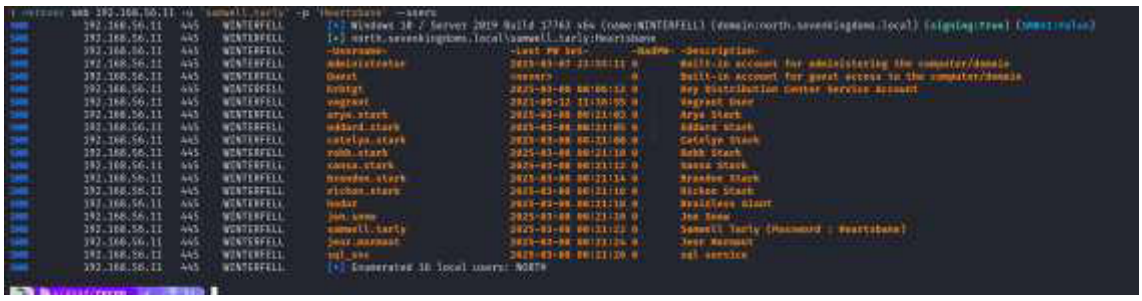


Nota: se visualiza listado de usuarios que se pueden logear en el dominio 192.168.56.11

Enumeración de todos los usuarios del dominio con credenciales, se identificó más usuarios debido a que se está probando con un usuario autenticado al dominio.

Figura 18

Usuarios del dominio



Nota: Se visualiza los usuarios del dominio con credenciales

Enumeración de recursos compartidos

Una técnica para tomar en cuenta, cuando se envían sesiones nulas, hacerlo con alguna cadena en el valor del parámetro, como “noexisteuser”, mediante esto se identificó los recursos compartidos en el dominio north, en este escenario se tuvo acceso de lectura a IPC$ y recurso all.

Figura 19

Enumeración de recursos compartidos

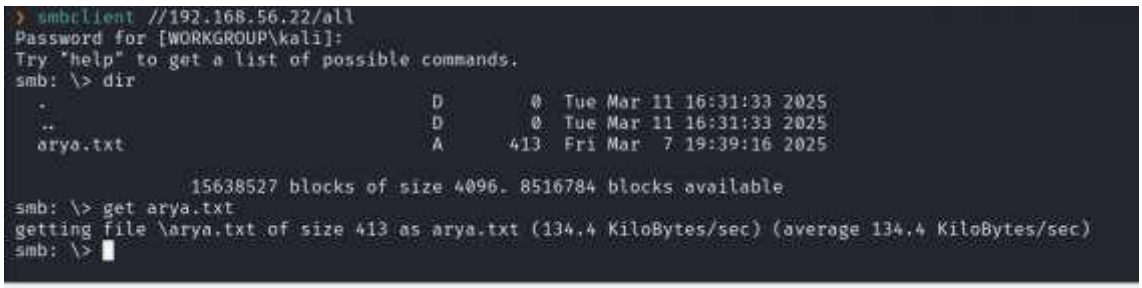
Nota: se visualiza los recursos compartidos en el dominio.

Descarga de recursos compartidos mediante smbclient

Para revisar los archivos compartidos se utilizó la herramienta smbcclient, cuando solicita un usuario y contraseña se debe dejar vacío.

Figura 20

Herramienta smbclient



Nota: se visualiza la descarga de archivos compartidos en la red 192.168.56.22

El archivo que se descargó se muestra a continuación, es común encontrar recursos compartidos en infraestructuras, específicamente en servidores que sirven para compartir recursos en la red interna y en muchas ocasiones se puede acceder a estos recursos con sesiones nulas, es decir no se debe ingresar credenciales.

Figura 21

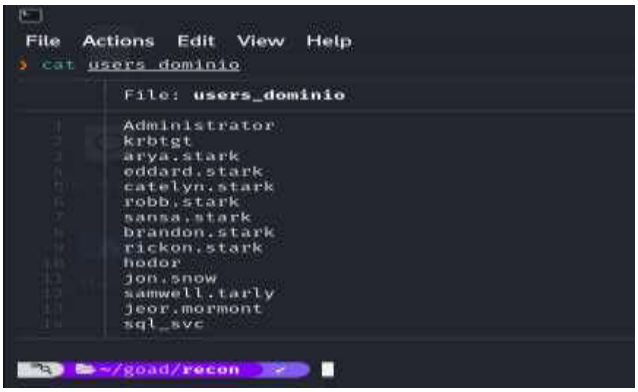
Archivo compartido arya.txt

Nota: Se visualiza el contenido del archivo arya.txt

Luego de haber obtenido la lista completa de usuarios del directorio activo, un método de ataque común en estos sistemas de Microsoft consiste en investigar si dichos usuarios tienen activa la opción don't pre auth. Esto significa que no se exige una autenticación previa mediante el protocolo Kerberos, el cual desempeña un papel clave en los procesos de validación de identidad en Windows.

Figura 22

Usuarios identificados del dominio north.sevenkingdoms.local



Nota: se visualiza el listado de usuarios del dominio que tienen la opción activa don’t pre auth

Ataque as-rep roast

Comando que permitió identificar usuarios vulnerables a este ataque, se identificó a un usuario llamado brandon.stark.

Figura 23

Ataque as-rep roast

Nota: Se visualiza el usuario vulnerable brandon.stark

Crackeo de hashes mediante hashcat

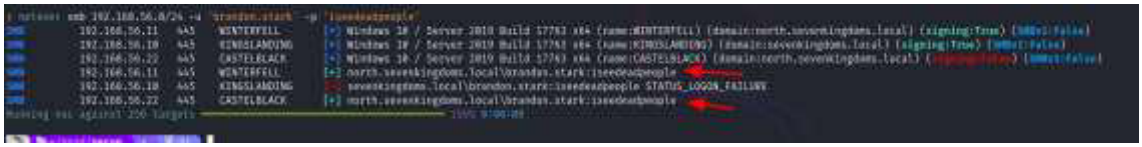
Figura 24

Herramienta hashcat

Nota: Para crackear este hash se utilizó el siguiente comando, con el módulo 18200 identifica el tipo de algoritmo de cifrado

Figura 25

Validación de credenciales mediante netexec.



Nota: Se visualiza los hashes validos en el dominio.

En este punto se consiguió 2 cuentas del dominio con credenciales válidas, es muy importante realizar “password spray” con los usuarios identificados, es decir probar como usuario el propio usuario, y como contraseña de la misma manera.

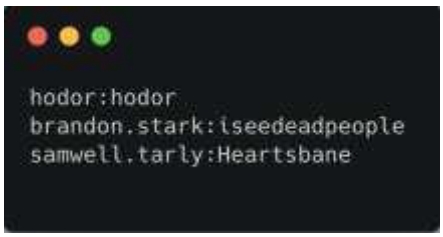
Figura 26

Password spray

Nota: Se visualiza los resultados de probar la contraseña el mismo usuario.

Figura 27

Usuarios identificados



Nota: Se identificaron en total 3 usuarios en el proceso de explotación

CVSS SCORE.

Figura 28

Análisis en CVSS score

Nota: resultados de la vulnerabilidad explotada en CVSS score

Ataque kerberoasting

En un directorio activo se tienen configuradas cuentas de servicio, y hay ocasiones que usuarios normales son asignados a un servicio (SPN), para consultar estas cuentas vulnerables que se llaman kerberoasteables se utilizó la suite de herramientas de impacket.

Figura 29

Herramienta impacket

Nota: Se identificaron las siguientes cuentas kerberoasteables.

De la misma manera se crackeo el hash obtenido, y se obtuvo una nueva cuenta de usuario con su respectiva credencial en texto plano.

Figura 30

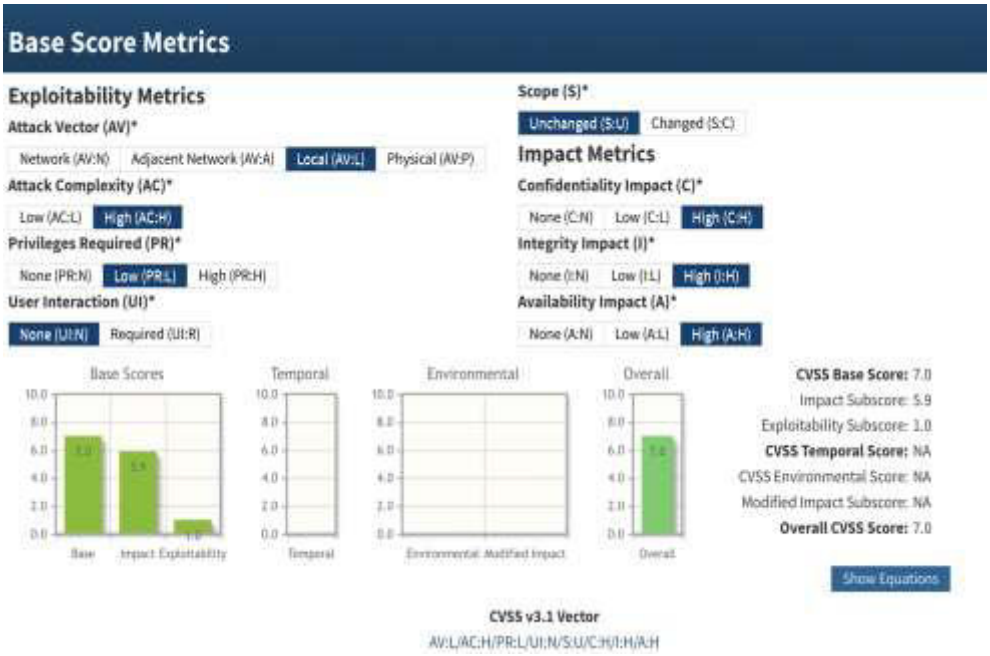
Crackeo de hash

Nota: Resultados del crackeo de hash obtenido con la herramienta impacket

Score CVSS

Figura 31

Análisis de vulnerabilidad en CVSS score



Nota: resultados de la vulnerabilidad explotada según el score CVSS.

Enumeración de recursos compartidos

Utilizando un listado válido de usuarios y contraseñas, se revisó recursos compartidos en todos los segmentos de red, se idéntico un recurso compartido llamado public, en donde se tiene permiso de lectura y escritura, para esto se utilizó la herramienta de netexec.

Figura 32

Herramienta netexec para revisar recursos compartidos

Nota: se visualiza los recursos compartidos en la red 192.168.56.10

Se accedió al recurso compartido y no se identificó ninguna información que aporte al ejercicio.

Figura 33

Recurso compartido en la red 192.168.56.22

Nota: se ingresa al recurso compartido en la carpeta “public”, sin embargo, no se encuentra ninguna información que aporte al trabajo.

CSVV Score

Figura 34

Análisis de la vulnerabilidad en CVSS score

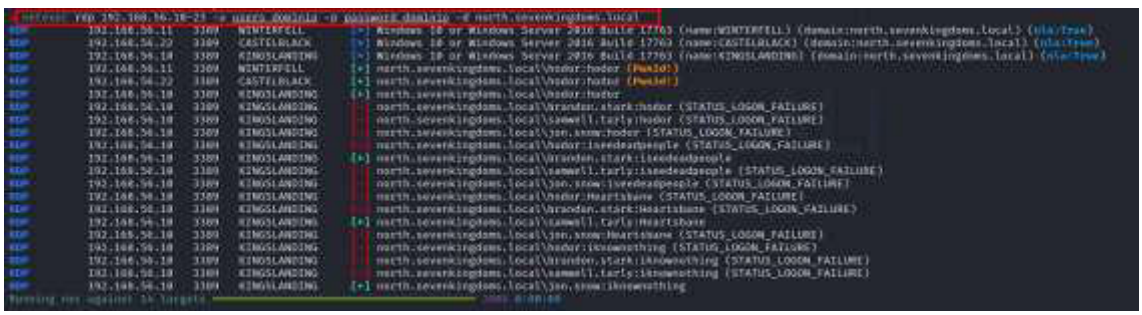
Nota: Se visualiza el score obtenido luego de analizar la vulnerabilidad en CVSS score

ACCESO MEDIANTE RDP A SERVIDORES.

Como la infraestructura está basada en Windows active directory, con las credenciales que se obtuvieron se probó acceso mediante protocolo RDP que sirve para acceso remoto. La cuenta “hodor” tuvo acceso mediante este protocolo al HOST 192.168.56.11 y 192.168.56.22, esto porque se identificó que sale PWn3d! en la herramienta netexec.

Figura 35

Acceso RDP

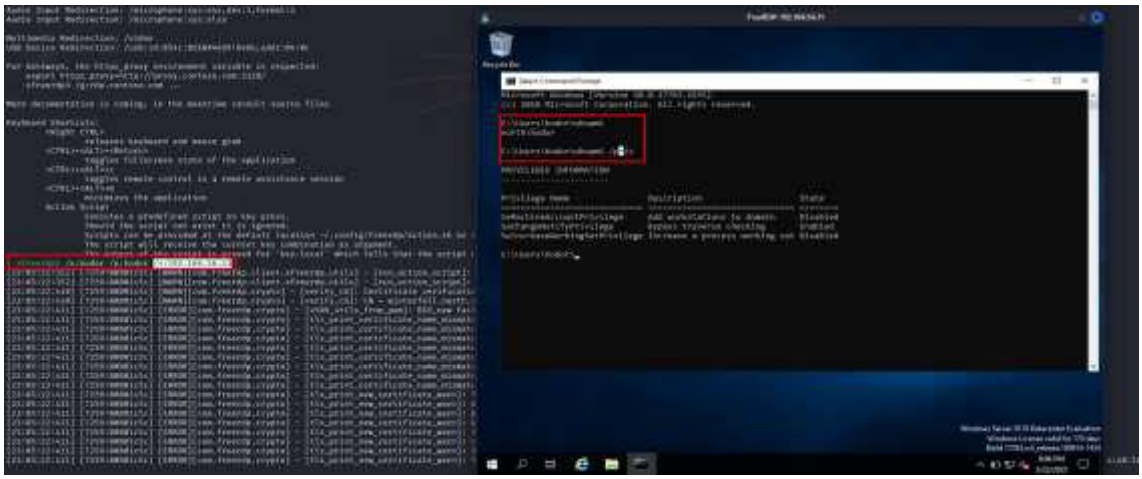


Nota: Vista de usuarios enumerados en la red interna

Se accedió al servidor 192.168.56.11 mediante una conexión RDP y las credenciales del usuario “hodor” utilizando la herramienta xfreerdp, además se enumeró los privilegios que este usuario posee en el servidor.

Figura 36

Herramienta netdiscover



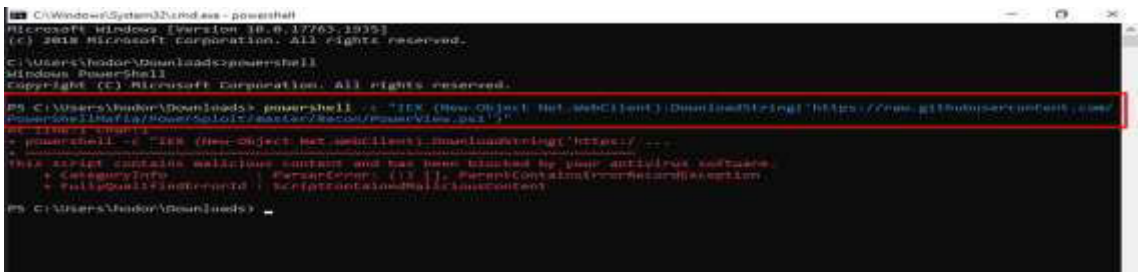
Nota: Detección de dispositivos conectados en red mediante Netdiscover

Se accedió al servidor con un usuario válido del dominio y se enumeró las DACL que son configuraciones de permisos para grupos, usuarios, carpetas, etc, además se buscó la manera de abusar de estos permisos para poder escalar privilegios, utilizando la herramienta llamada PowerView, como el equipo tuvo activado el Windows Defender, bloqueo este proceso.

Bloqueo de la herramienta AMSI de Windows Defender.

Figura 37

Nmap



Nota: Escaneo de direcciones IP activas en red interna con Nmap

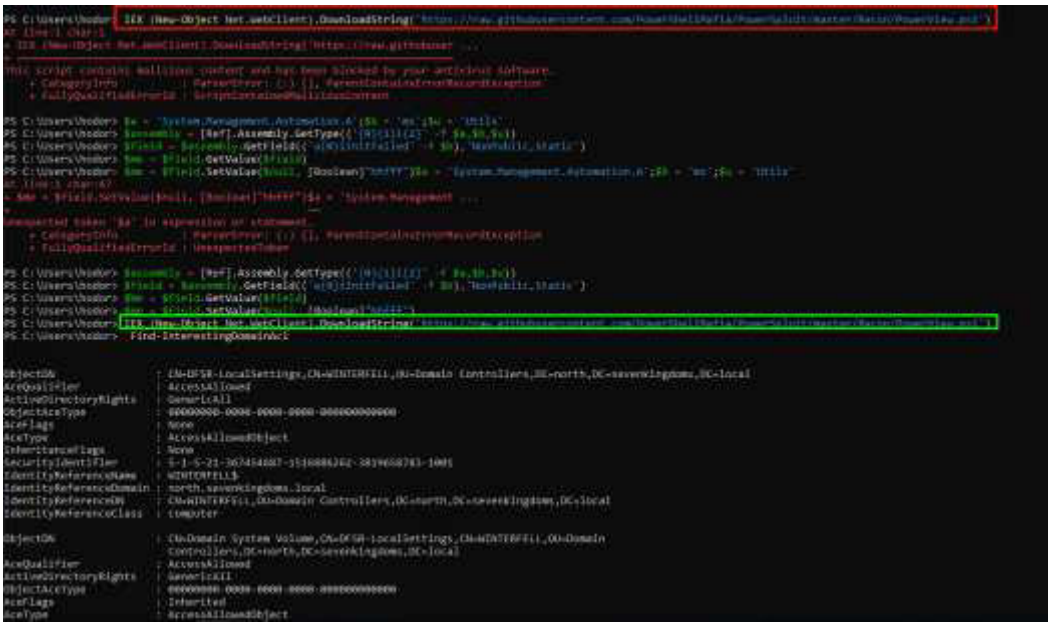
Las empresas no solo cuentan con soluciones tradicionales como antivirus, si no que implementan herramientas como EDR o EXDR que protegen activamente contra amenazas avanzadas. Se logró saltarse la solución de Windows defender, se utilizó el siguiente código que interrumpe la ejecución de AMSI y por ende se pudo ejecutar los códigos maliciosos.

Bypass de Windows Defender

Se enumeraron las DACLS configuradas mediante la herramienta PowerView y se saltó la protección de la solución AMSI.

Figura 38

Bypass windows defender



Nota: Resultado de escaneo de puertos abiertos en host 192.168.56.10

Hasta este punto del ejercicio, se tiene múltiples credenciales válidas del directorio activo, se ha enumerado DACLS del AD, la idea es poder acceder al AD mediante un usuario con altos privilegios, puede ser un Domain Admin, o buscar la manera de escalar privilegios mediante configuraciones incorrectas, grupos, DACLS, o explotar alguna vulnerabilidad que permita escalar privilegios.

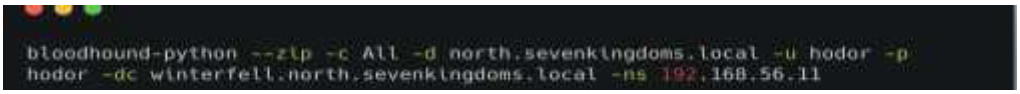
Uso de la herramienta BloodHound

Se utilizó la herramienta bloodhound que permitió obtener todo el esquema completo del AD, y mediante esto permitió identificar la forma más factible de poder escalar privilegios en el dominio, es posible utilizar la herramienta directamente desde Kali, o estando dentro de un equipo que se tenga acceso.

Se ha extraído los objetos de 2 dominios, 1. north.sevenkingdoms.local y sevenkingdoms.local

Figura 39

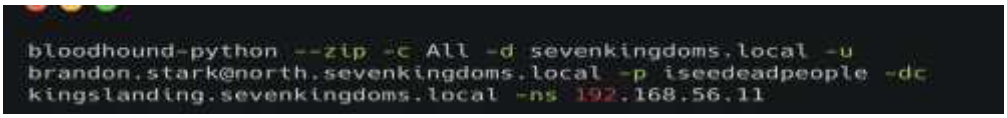
Dominio north



Nota: Servicios detectados en el servidor 192.168.56.10

Figura 40

Dominio sevenkingdoms



Nota: Servicios detectados en el servidor 192.168.56.11

Ejecución de comandos para obtener información de todos los objetos del Directorio activo.

Figura 41

Servicios en el directorio activo

Nota: Servicios detectados en el servidor 192.168.56.22

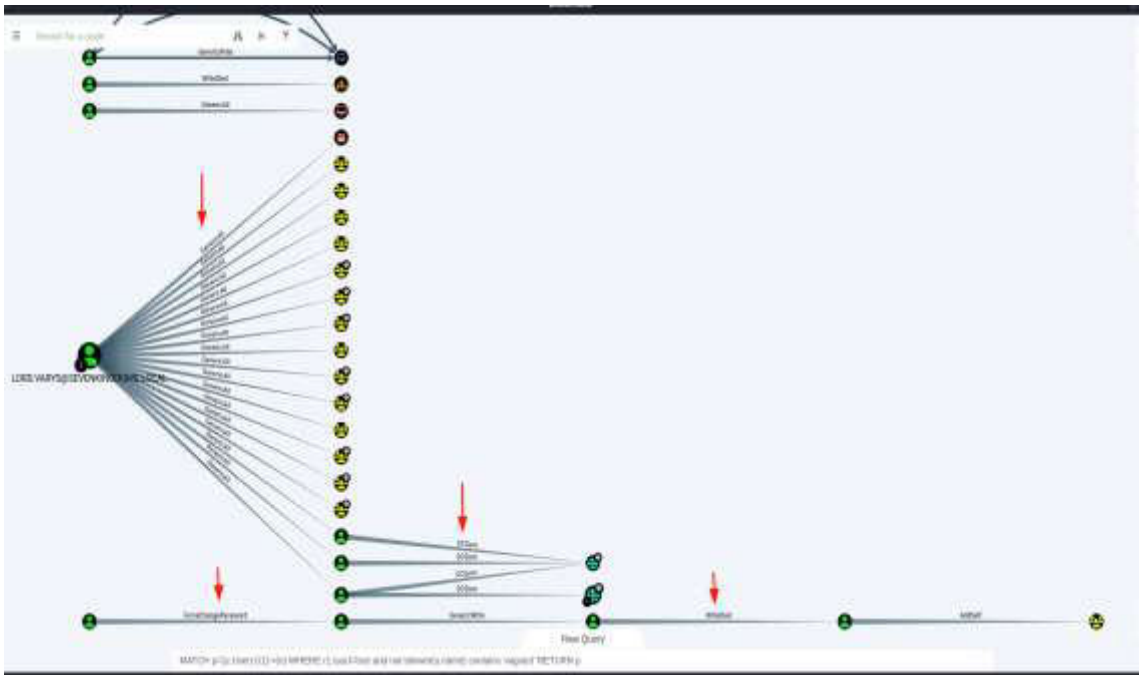
El archivo que se generó se basa en todos los objetos del Directorio activo, que son usuarios, grupos, GPOS, DACLS, etc. Bloodhound ayudó a recolectar toda la información, pero para poder visualizar esto de una mejor manera se utilizó la herramienta grafica llamada neo4j.

Uso de herramienta neo4j.

Estas son las DACLS configuradas en los diferentes usuarios identificadas mediante bloodhound.

Figura 42

Herramienta Neo4j



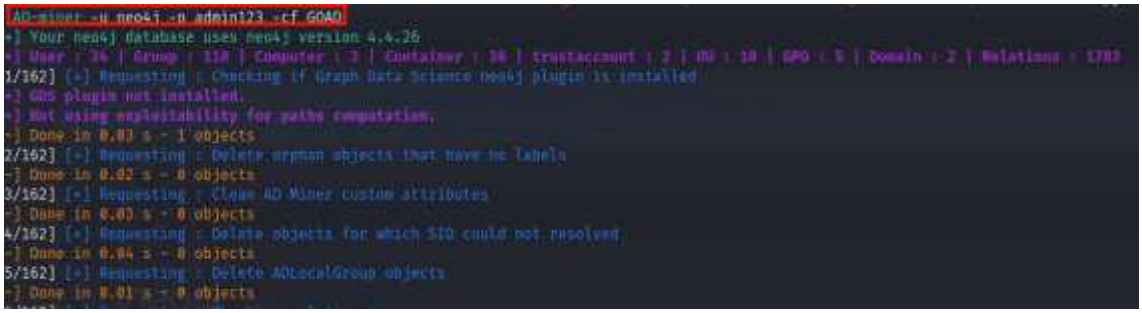
Nota: Versión de servicios expuestos en host 192.168.56.10

Uso de herramienta ADMiner

Existe una herramienta llamada ADMiner para poder visualizar de manera gráfica como poder escalar privilegios con la información obtenida mediante bloodhound y la generación de vías para movimiento lateral.

Figura 43

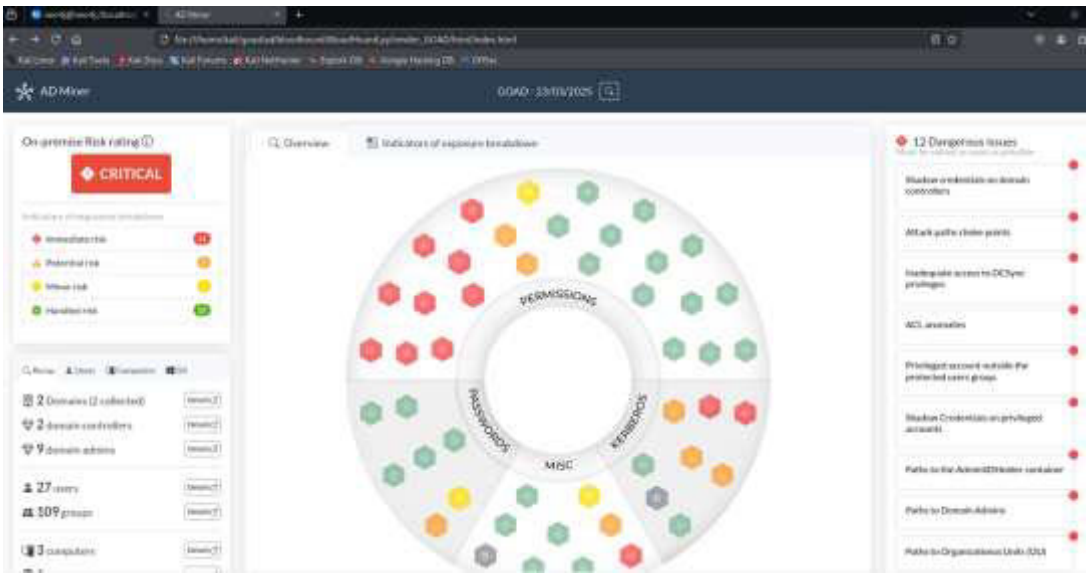
Herramienta adminer



Nota: Enumeración de usuarios mediante sesión nula

Figura 44

Gráficos mediante Adminer.



Nota: Enumeración de política de contraseñas del dominio

Ataque - Envenamiento de tráfico DNS, NBTS, LLMR

Cuando un servidor Windows no tiene el protocolo SMB firmado es posible realizar ataques de envenenamiento de tráfico DNS, NBTS, LLMR, y por ende capturar los hashes de los usuarios que interactúan con aplicaciones que usan estos protocolos, si las credenciales son débiles es posible crackearlos mediante hashcat.

Se han identificado los siguientes servidores que no tiene firmado este protocolo.

Figura 45

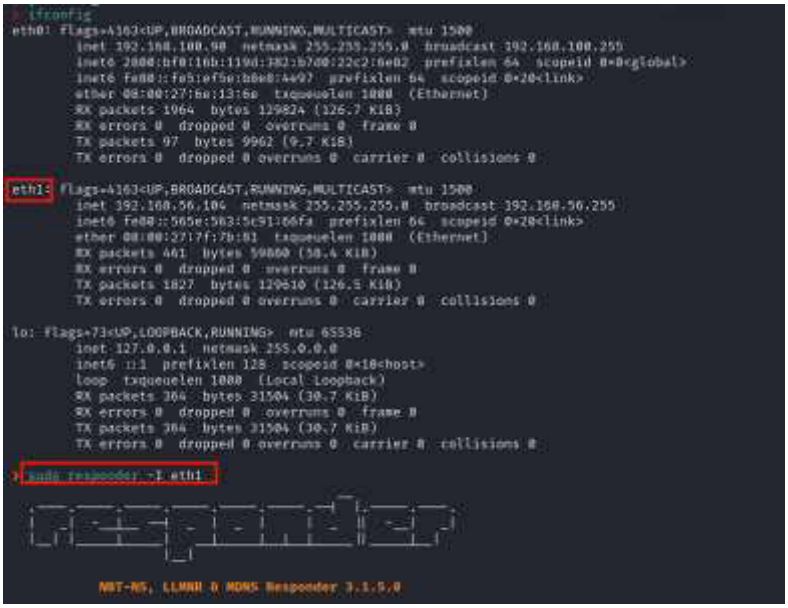
Envenenamiento al tráfico

Nota: Enumeración de grupos y usuarios del dominio con credenciales válidas

Ejecución de la herramienta responder que permite envenenar el tráfico, se debe elegir la interfaz de red, en este caso eth1 que pertenece a la red 192.168.56.24/0

Figura 46

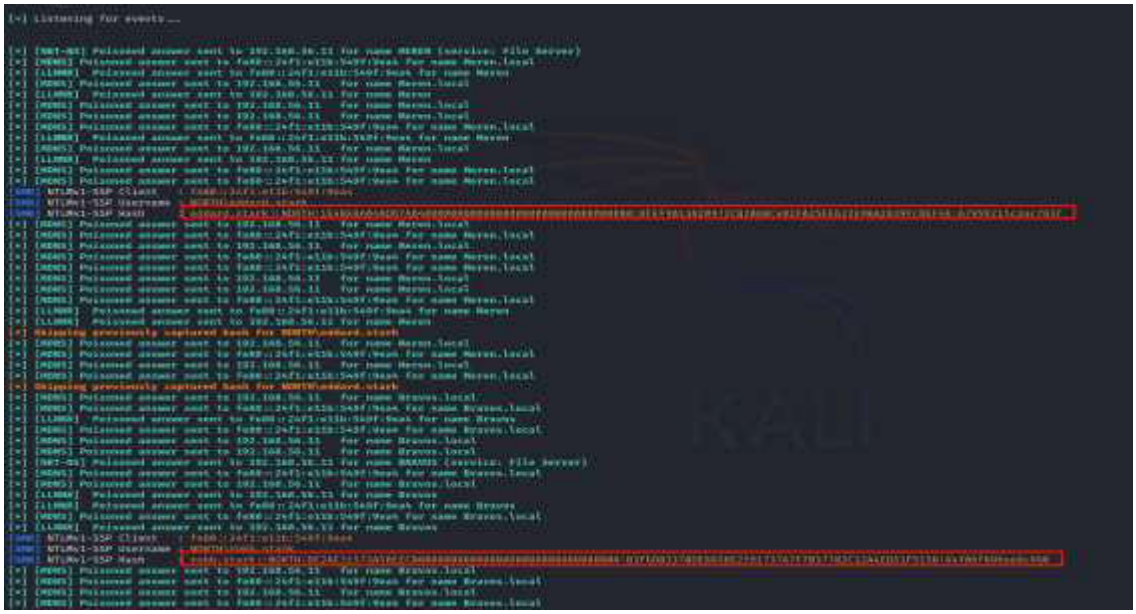
Herramienta netexec



Nota: Recursos compartidos identificados usando netexec

Figura 47

Hashes NTLM obtenidos



Nota: Archivo descargado desde recurso compartido abierto

Figura 48

SCORE CVSS

Nota: Usuario vulnerable al ataque AS-REP Roasting

Crackeo de hashes NTLM

Crackeo de hashes pertenecientes al usuario robb.stark

Figura 49

Crackeo de hashes NTLM

Nota: Crackeo exitoso de hash Kerberos con Hashcat

Con las credenciales obtenidas del crackeo, se consiguió acceso total al dominio de winterfell, esto debido a que cuando se pasó las credenciales en la herramienta netexec, ¡se visualiza un mensaje de pwn3d! que significa que el usuario tiene privilegios o se tiene acceso de Administrador al dominio.

Figura 50

Visualización de credenciales

Nota: Enumeración de privilegios de usuario dentro del servidor comprometido

Obtención de Hashes de todos los usuarios del dominio.

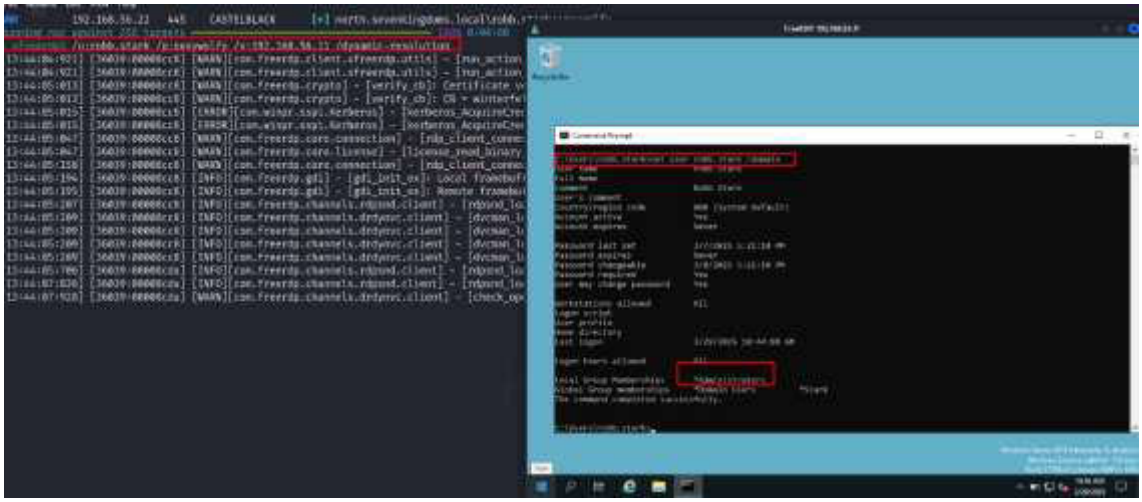
Cuando un usuario es Administrador puede obtener todos los hashes de los usuarios del dominio que es la base de datos NTDS, solamente disponible en los controladores de Dominio, en este caso del dominio north.seventking.local, estos hashes son NTLM y sirven

para hacer pass the hash, que significa poder acceder a un equipo mediante este hash, sin proporcionar ninguna credencial.

Acceso de administrador al dominio mediante RDP usando la herramienta xfreerdp.

Figura 51

Herramienta xfreerdp



Nota: Vista de DACLS obtenidas con PowerView en entorno comprometido

Ataque NLTM Relay.

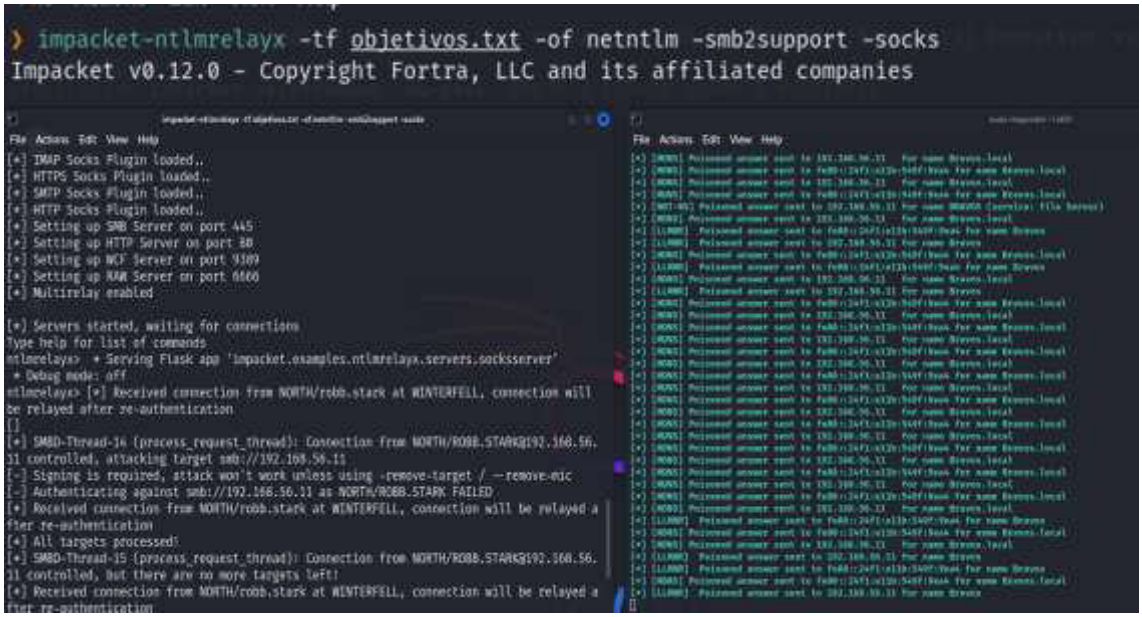
El ataque NTLM Relay es una técnica que permite interceptar y redirigir las credenciales de un usuario que usa el protocolo NTLM para autenticarse en una red Windows. Mediante este ataque el atacante intercepta la comunicación entre el cliente y el servidor, en lugar de intentar crackear los hashes, se utiliza para autenticarse en otros sistemas. Esto permite al atacante acceder a recursos como si fuera el usuario legítimo, sin necesidad de conocer su contraseña.

Herramienta para realizar NTLM Relay.

Una de las herramientas por excelencia para realizar este ataque se llama impacket.

Figura 52

Herramienta NTLM relay

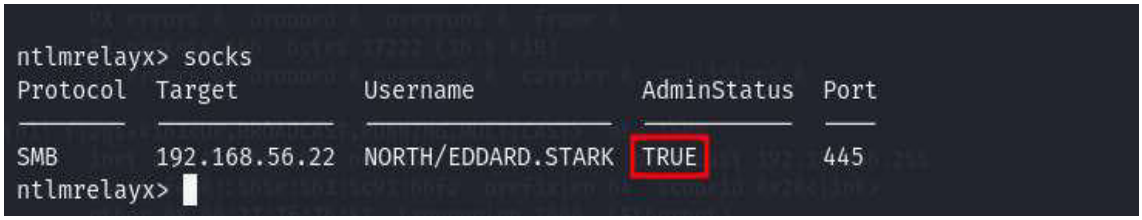


Nota: Mapa de relaciones en Active Directory generado por ntlmrelay

Equipo que permitió hacer el túnel mediante proxychains, para que funcione el usuario al que se envenenó el tráfico debe tener acceso de Administrator.

Figura 53

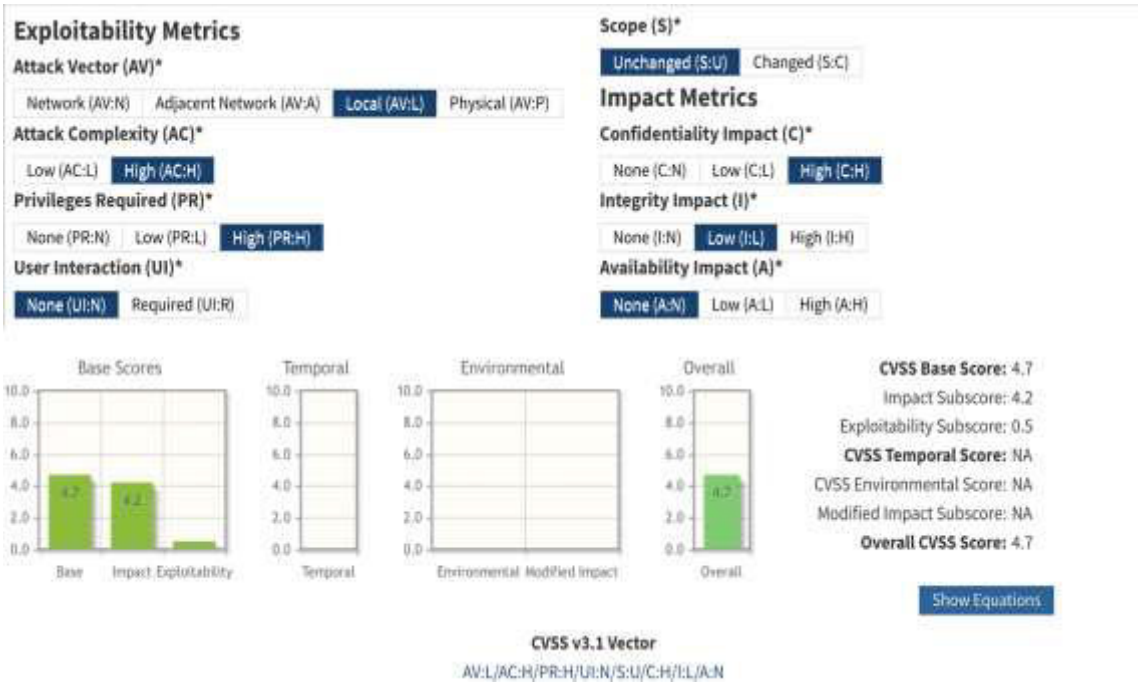
Proxychains



Nota: se visualiza el envenenamiento al usuario con permisos de administrador

Figura 54

Score CVSS



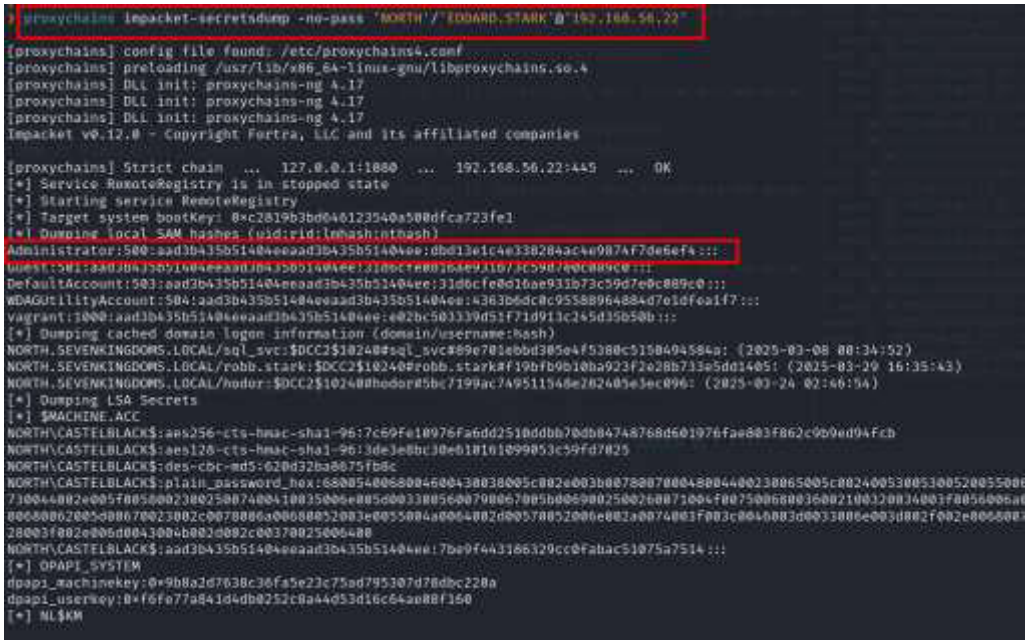
Nota: score obtenido de la vulnerabilidad en cvss

Extracción de Hashes de LSASS y Dominio

Se utilizó proxychains que permitió realizar un túnel y así poder extraer la lsass, es decir los usuarios del equipo local, se pudo extraer estos hashes, en este caso incluida la del usuario Administrator que es el más importante, además es posible obtener los hashes de los usuarios que están en el caché del equipo.

Figura 55

Herramienta LSASS



Nota: Extracción de Hashes de LSASS y Dominio

Ataque Pass the Hash

Esta técnica permitió ingresar como administrador al equipo local 192.168.56.22 sin tener una credencial en texto plano.

Figura 56

Herramienta pass the hash

Nota: con esta técnica se logró ingresar al equipos local 192.168.56.22

Score CVSS

Figura 57

SCORE CVSS

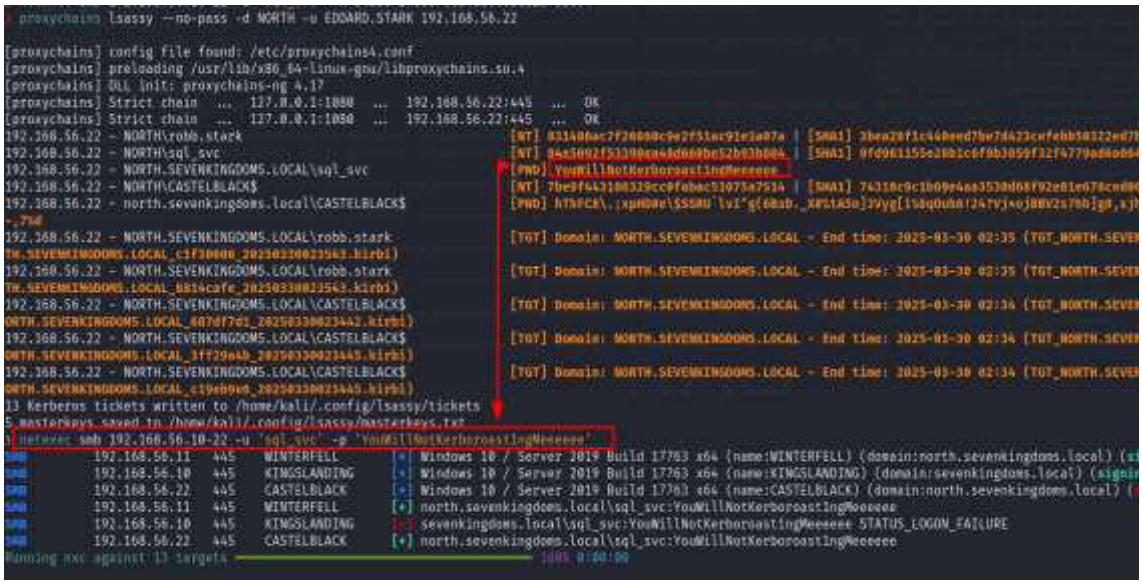
Nota: score obtenido de la vulnerabilidad en cvss

Lsassy

Se utilizó lsassy para obtener las credenciales almacenadas del proceso lsass, la información de las cuentas de dominio se almacena en el proceso LSASS, por lo que hacer un volcado de este proceso pudo brindar más cuentas de dominio y privilegios.

Figura 58

Lsassy

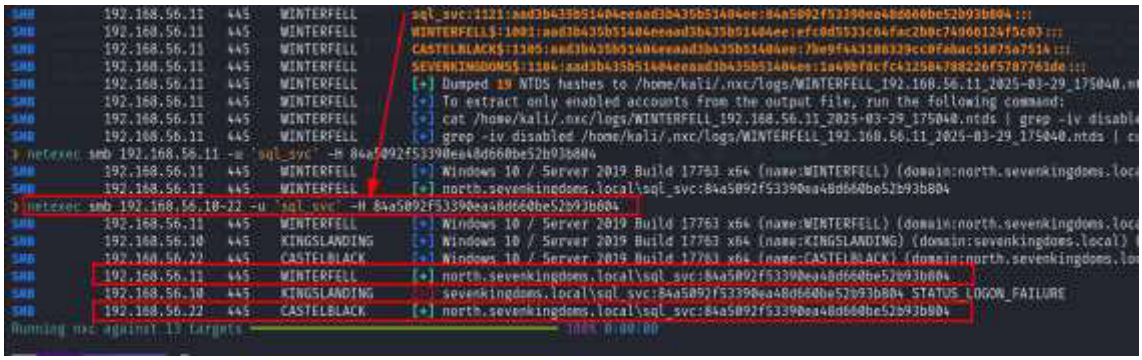


Nota: Vista del ingreso de lsassy

Pass the hash en una de las cuentas obtenidas, cuando se visualiza el signo (+) es porque la cuenta es válida dentro del dominio.

Figura 59

Ejecución de pass the hash



Nota: Vista de la cuenta obtenida mediante Pass the hash

Ejercicio- Escalada de privilegios

La cuarta fase se enfocará en la evaluación de las capacidades de un atacante para escalar privilegios dentro de la red interna. Se intentará elevar privilegios desde cuentas de usuario estándar a privilegios administrativos que según (IBM, 2021) “otorgan a los usuarios y a los grupos permisos para ejecutar operaciones globales y crear objetos”, utilizando técnicas manuales y automatizadas. Esto es crucial para determinar si un atacante podría comprometer completamente la red y acceder a sistemas críticos que gestionan la provisión de productos como desinfectantes y abrillantadoras, esenciales para la misión de Mastercleans S.A.

Subida de Archivos Conduce a RCE

En el servidor de destino se identificó el siguiente sitio web que solicitó subir un archivo, donde se verificó que es posible subir una webshell(código malicioso que permite interactuar con el servidor donde está alojado un sitio web)

El siguiente código está programado en aspx y permitió interactuar con el servidor de aplicación.

Figura 60

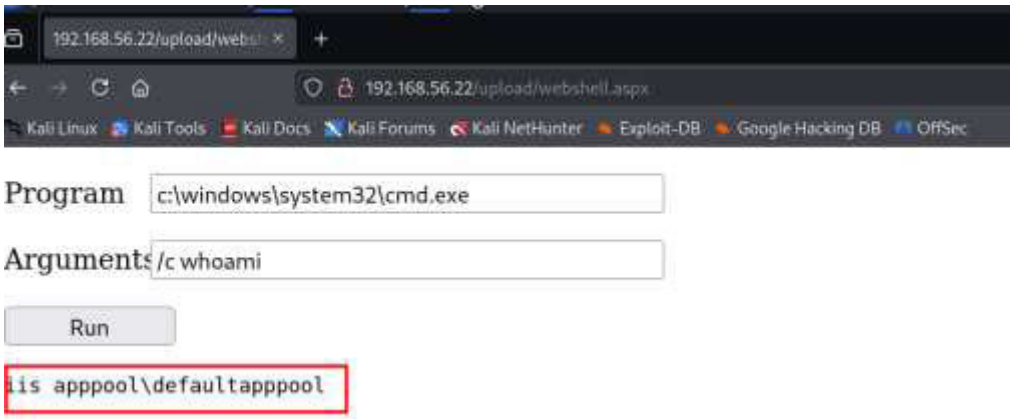
Código programado en aspx

Nota: Vista del código aspx

Se comprometió el servidor, fue posible ejecutar comandos en el servidor remoto, además se identificó cual usuario está corriendo el servicio web.

Figura 61

Servidor comprometido

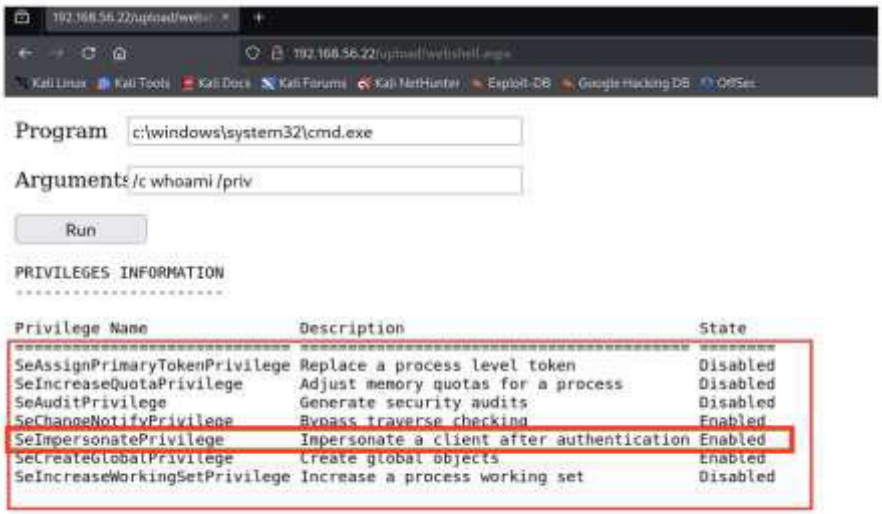


Nota: Vista del servidor comprometido

Privilegios del usuario defaultpppol en el servidor, el objetivo es escalar privilegios al usuario nt autority system, privilegio similar a root en servidores linux.

Figura 62

Privilegios de usuario en el servidor



Nota: Vista del usuario defaultppol

Abuso de privilegios SetImpersonatePrivilege

Este privilegio está asignado al usuario apppool, y permitió un proceso de impersonar a otro usuario, es decir, tomar su identidad de seguridad temporalmente.

Reverse + Bypass de AMSI mediante shell en base64

Se utilizó una herramienta que permite generar una carga útil para realizar una conexión reversa desde el sitio web hacia el servidor, y que a su vez no sea detectado por la solución Windows Defender (este código fue ejecutado en el equipo Windows, mediante la web shell)

Figura 63

Shell en base64

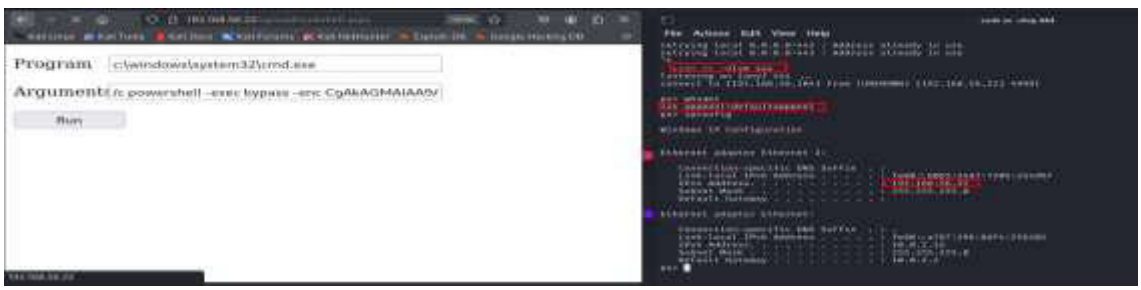
Nota: Vista de la web shell

Conexión mediante netcat hacia el servidor IIS.

Se accedió al servidor usando la herramienta netcat(ejecutada en el equipo kali), y se obtuvo una sesión interactiva con el servidor IIS.

Figura 64

Conexión netcat



Nota: Vista de la conexión de netcat

Uso de software para escala de privilegios.

Para escalar privilegios se utilizó Petit Potato un software que ya encuentra compilado para ejecutarlo, esto permitió la escalada de privilegio hacia el usuario NT authority system.

Figura 65

Software Petit Potato

Nota: Vista del uso Petit Potato

Score CVSS.

Figura 66

Análisis en CVSS score

Nota: Se visualiza el score obtenido en CVSS luego de analizar la vulnerabilidad.

Ejercicio - Movimiento Lateral

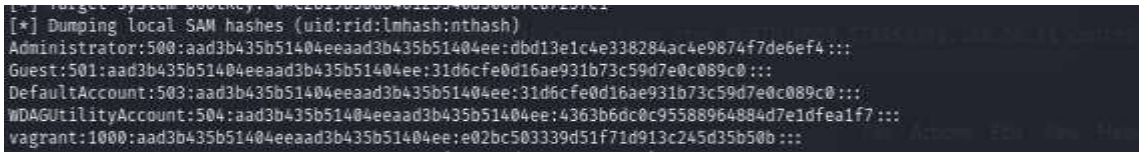
Antes de saltar de un ordenador a otro se debe conocer los secretos (contraseñas, o hashes) de la máquina que poseemos.

- Windows tiene muchos secretos diferentes almacenados en diferentes lugares.
- Se utilizó impacket secretsdump.py
- Base de datos del Administrador de cuentas de seguridad (SAM)

La herramienta secretdump recuperó los hashes SAM, la cual contiene:

Figura 67

Herramienta secretdump



Nota: Ingreso a secretdump

Se accedió al equipo local como usuario Administrator mediante pass the hash con la herramienta netexec.

Figura 68

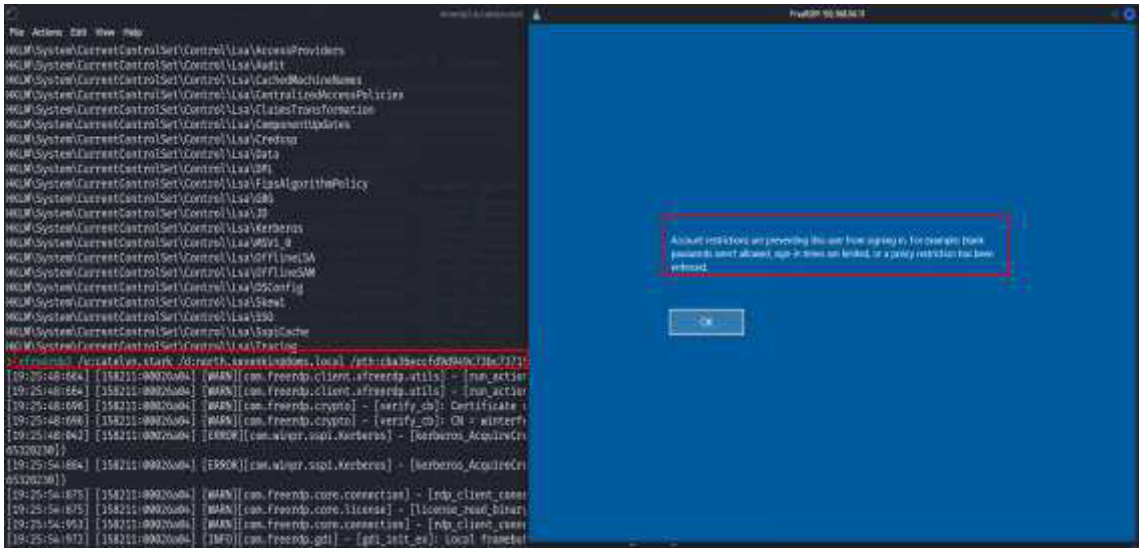
Herramienta netexec

Nota: Ingreso con netexec, a usuario administrador

La técnica de ataque “pass the hash” no es posible realizarlo para conectarse mediante RDP, Microsoft tiene una restricción cuando un usuario intenta acceder mediante el hash respectivo de su contraseña, esta protección se llama Restricted Admin.

Figura 69

Protección restricted admin



Nota: Vista de error de ingreso, mediante protección Restricted Admin

Fue posible saltarse esta protección, cambiando el valor del registro.

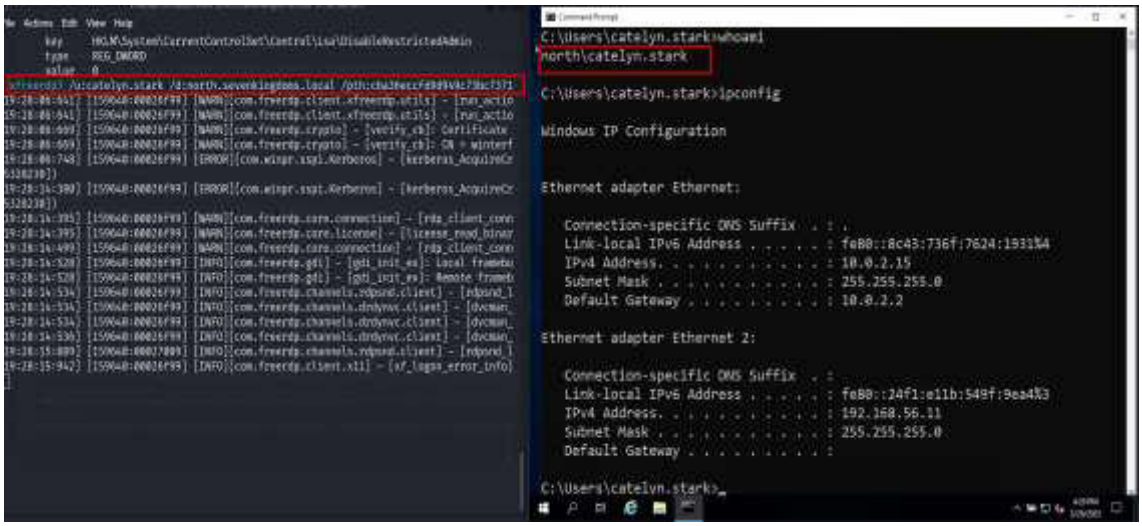
Figura 70

Anulación de la proteccion restricted admin

Nota: Vista del cambio de valores

Figura 71

Se accedió al servidor 192.168.56.11



Nota: Vista de servidores utilizando impacket secretsdump.py

Capítulo 4. Análisis De Resultados

Los resultados obtenidos de las técnicas aplicadas presentan vulnerabilidades que permiten el acceso al servidor y comprometer su funcionamiento; entre ellas, la subida de archivos que conduce a la ejecución de código de manera remota. Este tipo de vulnerabilidad es considerada critica con puntaje de 10 según la evaluación en Score CVSS.

Score CVSS

Figura 72

Análisis de vulnerabilidad en CVSS score

Nota: se visualiza el score más alto obtenido luego de analizar la vulnerabilidad que afecta directamente al servidor.

También fue posible realizar el movimiento lateral, para este ejercicio se necesitó conocer el hash de la maquina víctima. El comando aplicado para este ataque fue “pass the hash”, sin embargo, debido a la restricción de Microsoft no era posible conectarse; para esto se tuvo que saltar esta protección llamada Restricted Admin modificando su valor de registro según la Figura 29, de esta manera fue posible conectarse mediante RDP como se visualiza en la Figura 30.

Tabla 1

Resumen de vulnerabilidades basadas en CVSS Score

Nombre de vulnerabilidad	Escore De Criticidad	Tiempo de Remediación
AS-REP Roasting	6.2 (Medio)	30 días
Kerberoasting	7.0 (Alto)	20 días
NTLM Relay	4.7 (Medio)	30 días
Envenenamiento LLMNR/NBT-NS	7.7 (Alto)	20 días
Pass The Hash	10.0 (Crítico)	5- 15 días
Subida de Archivos + RCE	10.0 (Crítico)	5- 15 días
Escalada de Privilegios SetImpersonatePrivilege	10.0 (Crítico)	5- 15 días

Nota: esta tabla muestra de manera resumida los valores obtenidos según el sistema de puntuación CVSS Score para estimar el impacto de una vulnerabilidad.

Tabla 2

Tiempos de Remediación de vulnerabilidades, SLA

Impacto de vulnerabilidad	Tiempo de Remediación
Critica	5- 15 días
Alta	20 días
Medio	30 días
Baja	3 meses

Nota: en esta tabla se visualiza los tiempos de remediación según el nivel de impacto de la vulnerabilidad.

Para ejecutar la fase técnica, se implementó el proyecto de código abierto llamado GOAD (Game of Active Directory). Esta iniciativa facilitó el despliegue de manera automática del entorno realista usando tecnologías de Microsoft, este laboratorio fue indispensable para llevar a cabo las evaluaciones de seguridad controladas aplicando diferentes técnicas ofensivas, además el laboratorio se complementa con el uso de herramientas de código abierto.

Se ha elegido el laboratorio GOAD basado en Windows Active Directory debido a que un gran número de compañías dentro del ranking Fortune 500 emplean esta tecnología desarrollada por el gigante Microsoft, dicha solución resulta indispensable para gestionar, administrar dispositivos, cuentas de usuario y demás elementos de infraestructuras tecnológicas críticas.

Capítulo 5. Conclusiones

5.1. Conclusiones generales

Tras el análisis a la red interna de la empresa MasterCleans se evidenció 7 vulnerabilidades que según su score de criticidad en CVSS se clasifican como bajos y altos; en consecuencia, los tiempos de remediación van desde los 5 días hasta los 3 meses para las vulnerabilidades menos críticas. La explotación exitosa de estas vulnerabilidades podría permitir a los atacantes obtener acceso no autorizado a los sistemas internos, escalar privilegios y comprometer la integridad, confidencialidad y disponibilidad de la información.

MasterCleans necesita realizar mejoras en sus sistemas y dede basarse en el score obtenido en cvss y el impacto al negocio que permite a la empresa priorizar que vulnerabilidad debe ser atendida en menos tiempo, para las críticas se estima plazos de 5 días y para las bajas hasta 3 meses. Además, la capacitación del personal en temas de seguridad informática es fundamental para reducir el riesgo de incidentes y garantizar que se sigan las mejores prácticas de seguridad.

5.2. Conclusiones específicas

- Mediante las herramientas de seguridad ofensiva se identificó la red completa de la organización y permitió obtener información relevante para el proceso como puertos abiertos, versión de sistemas operativos.

- Se explotaron vulnerabilidades como password spray, Kerberoaring, pass the hash enfocadas hacia sistemas operativos Windows

- Se reviso las políticas de contraseñas aplicadas hacia los usuarios del directorio activo, se evidencio que la longitud de contraseña es de 5 caracteres y fue posible crakear hashes ntlm y de kerberos mediante hash cat.

- Mediante la ofuscación de código fue posible saltarse la solución amsi de Windows defender

- Fue posible subir un archivo malicioso en un sitio web alojado en servidor de la empresa lo que permitió ejecutar comandos en el sistema.

- Mediante la enumeración de permisos asignados hacia el usuario apppool permitió utilizar la herramienta peti potato para escalar privilegios hacia nt autority system.

- Se identifico vulnerabilidades críticas, altas y medias además se las clasifico de acuerdo el score cvss que se basa en el impacto y como afecta a la confidencialidad, integridad y disponibilidad de la información de la empresa

- Se estableció tiempos de remediación (SLA) para cada vulnerabilidad identificada dependiendo su criticidad de acuerdo al score cvss y cómo afecta al negocio.

Referencias

Caballero Quezada, A. E. (31 de 03 de 2025). *elhacker.info.* Obtenido de elhacker.info: https://elhacker.info/manuales/Hacking%20y%20Seguridad%20informatica/0197-hacking-con-kali-linux.pdf

Chandel, R. (28 de 12 de 2024). *Artículos sobre piratería informática*. Obtenido de https://www.hackingarticles.in/active-directory-pentesting-using-netexec-tool-a-complete-guide/

Chicaiza, V. (2019). Metodología abierta de testeo en Seguridad NESSUS. *Nexos Científicos, 3*(1), 35-41. Obtenido de http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index

CyberZaintza. (s.f.). Obtenido de Escalada de privilegios: https://www.ciberseguridad.eus/ciberglosario/escalada-de-privilegios

Dávila, V. (2021). *Studocu*. Obtenido de https://www.studocu.com/es-ar/document/universidad-nacional-de-la-rioja/seguridad-informatica/vectores-de-ataque/40393938

De la Cruz Gámez, E. (2022). Ethical Hacking to remote systems using Metasploit and Kali Linux. *IEEE*, 224-226. doi:10.1109/CIMPS57786.2022.10035712

FreeRDP. (2023).

Ghirardotti, M. S., & Renna, J. I. (2022). Auditoría y ciberseguridad. *Audit.AR, 2*(1), 7. doi:https://doi.org/10.24215/27188647e014

Giannone, A., Amatriain, H. G., Rodríguez, D., & Merlino, H. (2018). Método de inclusión de Hacking ético en el proceso de testing de software. *XXIV Congreso Argentino de Ciencias de la Computación (La Plata, 2018).* (págs. 542-541). La Plata: Red de Universidades con Carreras en Informática (RedUNCI). Obtenido de http://sedici.unlp.edu.ar/handle/10915/73243

Gonzales Duque, R. (2025). *Python para todos.* Santiago: Universida santiago de campostela. Obtenido de https://persoal.citius.usc.es/eva.cernadas/informaticaparacientificos/material/libros/Python%20para%20todos.pdf

Guevara, L. A. (2022). El hacking ético como servicio conexo de consultoría en seguridad por parte de las empresas de seguridad privada. *Universidad Militar Nueva Granada*, 17. Obtenido de http://hdl.handle.net/10654/40525

Hajdarevic, K., & Dzaltur, V. (2015). Internal penetration testing of Bring Your Own Device (BYOD) for preventing vulnerabilities exploitation. *IEEE*, 1-6. doi:10.1109/ICAT.2015.7340506

Hascat. (2023). *Advanced Password Recovery*. Obtenido de https://hashcat.net/wiki/doku.php?id=hashcat

Hualpa Oscas, R. R. (2022). *EVALUACIÓN DE EFECTIVIDAD DE LAS PRUEBAS DE PENETRACIÓN INTERNAS CONTRA EL ESCALAMIENTO DE PRIVILEGIOS DE USUARIO.* Lima: Repositorio institucional de la Universidad de Lima. Obtenido de https://hdl.handle.net/20.500.12724/17430

IBM. (03 de agosto de 2021). *Privilegios de administrador*. Obtenido de https://www.ibm.com/docs/es/psfa/7.1.0?topic=model-administrator-privileges

IMPACKET. (2023). Obtenido de https://github.com/fortra/impacket?tab=readme-ov-file

Kali. (23 de 05 de 2024). *netdiscover | Herramientas de Kali Linux*. Obtenido de netdiscover | Herramientas de Kali Linux: https://www.kali.org/tools/netdiscover/

Laprovittera, C. (enero de 17 de 2024). *Hacking Web – Escalada de Privilegios*. Obtenido de https://achirou.com/hacking-web-escalada-de-privilegios/#:~:text=El%20escalamiento%20de%20privilegios%20es,por%20defecto%2Cno%20deber%C3%ADa%20tenerlos.

Lazo Canazas, J. G. (2021). *IOC – Intrusion Operation Center.* Lima: Repositorio institucional de la Universidad de Lima. Obtenido de https://hdl.handle.net/20.500.12724/19251

López de Jimenez, R. E. (2016). Pentesting on Web Applications using Ethical. *IEEE*, 1-6. doi:10.1109/CONCAPAN.2016.7942364

Orebaugh, A., & Pinkard, B. (2011). *Nmap in the Enterprise.* Ucrania: Elsevier Science. Obtenido de https://www.google.com.ec/books/edition/Nmap_in_the_Enterprise/VjgezB784XIC?hl=es&gbpv=0

Parra Bolaños, E. A. (2024). El rol de la ciberseguridad en las ciudades inteligentes. *Repositorio Institucional Universidad Piloto de Colombia*, 8. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/13768

Pons Gamon, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO*(20), 89-93. doi:10.17141/urvio.20.2017.2563

PowerSploit. (s.f.). Obtenido de https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon/PowerView

ProgressWhatsUp Gold. (13 de Diciembre de 2023). Obtenido de https://www.whatsupgold.com/es/blog/what-network-mapping-what-good-for

Red Hat,Inc. (2024). *Red Hat Documentation*. Obtenido de https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/8/html/deploying_different_types_of_servers/assembly_using-the-smbclient-utility-to-access-an-smb-share_assembly_using-samba-as-a-server#assembly_using-the-smbclient-utility-to-access-an-sm

Romaniz, S. C. (2008). Seguridad de aplicaciones web: vulnerabilidades en los controles de acceso. *XIV Congreso Argentino de Ciencias de la Computación* (pág. 14). Argentina: Repositorio institucional de la UNLP. Obtenido de http://sedici.unlp.edu.ar/handle/10915/21581

Sanchez Dávila, M. A. (2019). HACKING ETICO: IMPACTO EN LA SOCIEDAD. *Repositorio Institucional Universidad Piloto de Colombia*, 8. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/4919

SAYAGO HEREDIA, J. (2021). Ciberseguridad en ecuador y latinoamerica. *KillKana Tecnica, 5*(1), 7-8. Obtenido de https://doi.org/10.26871/killkanatecnica.v5i1.957

VirtualBox. (31 de 03 de 2025). *VirtualBox.org.* Obtenido de VirtualBox.org: https://www.virtualbox.org/manual/topics/Introduction.html#intro-starting

Voutssas, J. (06 de abril de 2010). *Investigación Bibliotecnològica*. Obtenido de Preservación documental digital y seguridad informática: http://rev-ib.unam.mx/ib/index.php/ib/article/view/21416/20180

Zaidman, E. (2017). Seguridad informática ¿Vulnerabilidades técnicas o errores humanos? *Econo*(14), 26-28. Obtenido de http://sedici.unlp.edu.ar/handle/10915/61109

ANEXOS

LABORATORIOS:

https://1024terabox.com/s/1fZAOiodrxiD43m7skCvtuA