Capacidades Técnicas, Legales Y De Gestión Para Equipos

Blue Team Y Red Team

JOHN ALEJANDRO CASTRO RAMOS

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

Ibagué 30 noviembre 2024

Resumen

En un contexto digital en constante evolución, la ciberseguridad se ha vuelto fundamental para proteger los sistemas y datos críticos de las organizaciones. Este documento se centra en el papel de las herramientas y servicios especializados en ciberseguridad, primero analizando la legislación colombiana en materia de ciberseguridad, segundo analizar las implicaciones éticas y legales y por último analizar que es pentesting para posterior realizar en el ámbito de las pruebas de penetración (pentesting) y la evaluación de vulnerabilidades dentro de los escenarios entregados en este diplomado por la empresa CyberFort Technologies. Se analizan herramientas esenciales como Metasploit, Nmap y OpenVAS, que permiten a los profesionales de la seguridad en Red Team y Blue Team identificar y explotar vulnerabilidades en redes y sistemas y buscar la mitigación de estas.

Las empresas de ciberseguridad, al realizar auditorías, tienen acceso a información confidencial de sus clientes. Este acceso debe ser cuidadosamente regulado y supervisado para evitar el uso indebido o explotación de la información, como ocurrió en el caso de CyberFort Technologies. La implementación de mecanismos de control, como la segmentación de funciones y auditorías independientes, es esencial para prevenir abusos y garantizar que la información sea utilizada solo para los fines autorizados.

Lo anterior nos permite identificar y exponer las debilidades o fallos de seguridad en un sistema informático al simular ataques cibernéticos. Los desafíos en seguridad informática

permiten utilizar métodos y técnicas conocidas como "técnicas de intrusión" para tratar de penetrar en un sistema de la misma manera que lo haría un equipo de Red Team y mecanismos de defensa que se emplearían para mitigar las intrusiones como un equipo blue Team lo haria.

Palabras clave: Ciberseguridad, Intrusión, Pentesting

Tabla de contenido

Lista de Figuras

Glosario

- **Auditoría de seguridad**: Proceso de evaluación de la infraestructura digital de una organización con el objetivo de identificar vulnerabilidades, amenazas y riesgos, con el fin de mejorar la seguridad y proteger la información confidencial.
- **Backdoor:** Puerta trasera. Programa o dispositivo que permite acceder a un sistema de forma oculta.
- **Blue Team:** Equipos que realiza un análisis de sistemas de información para garantizar la seguridad, identificar fallas de seguridad, verificar la efectividad de cada medida de seguridad y asegurarse de que todas las medidas de seguridad continúen siendo efectivas después de la implementación.
- **Ciberseguridad:** Conjunto de prácticas y tecnologías destinadas a proteger sistemas, redes y datos de ataques cibernéticos.
- **COPNIA:** Consejo Profesional Nacional de Ingeniería de Colombia. Es la entidad que regula el ejercicio de la ingeniería en el país y establece un código de ética para los ingenieros, exigiendo responsabilidad, integridad y transparencia en sus actividades profesionales.
- **CVE (Common Vulnerabilities and Exposures)**: Sistema de identificación estándar para vulnerabilidades de seguridad en software y hardware, que proporciona identificadores únicos para cada vulnerabilidad.

- **Explotación:** Acción de aprovechar una vulnerabilidad para obtener acceso no autorizado a un sistema
- **ExploitDB**: Base de datos en línea que contiene una colección de exploits y pruebas de concepto para vulnerabilidades conocidas, útil para investigadores y profesionales de la seguridad.
- **Kali Linux:** Distribución de Linux especializada en pruebas de penetración, que incluye una amplia gama de herramientas para hacking ético.
- **Escalada de privilegios:** Proceso de obtener mayores privilegios dentro de un sistema comprometido, como pasar de un usuario normal a un administrador.
- **Ley 1273 de 2009 (Colombia):** Legislación colombiana que regula y sanciona los delitos informáticos y la protección de la información en medios digitales, estableciendo penalidades para actos como el acceso abusivo a sistemas informáticos, interceptación de datos, y daño a la información.
- **Ingeniería social:** Técnica que manipula a las personas para que revelen información confidencial o realicen acciones que beneficien al atacante.
- **Hacking ético:** Práctica de utilizar las mismas técnicas que los hackers malintencionados, pero con fines autorizados y legales, para identificar y corregir vulnerabilidades.
- **Nmap:** Herramienta de red utilizada para descubrir hosts y servicios en una red, así como para detectar vulnerabilidades.

- **Metasploit:** Framework de explotación que permite a los pentesters identificar y explotar vulnerabilidades en sistemas remotos.
- **Malware:** Software malicioso diseñado para causar daño a un sistema informático.
- **OpenVAS**: Sistema de evaluación de vulnerabilidades de código abierto que permite realizar análisis de seguridad en redes y aplicaciones, generando informes sobre los problemas identificados
- **Pentesting:** Prueba de penetración. Consiste en simular un ataque cibernético a un sistema informático para identificar vulnerabilidades y evaluar su seguridad.
- **Red Team:** Estrategia de seguridad en la que un equipo simula ataques cibernéticos contra otro equipo que defiende la red.
- **Vulnerabilidad:** Debilidad o fallo en un sistema que puede ser explotado por un atacante.
- **Vulnerabilidad cero-day:** Vulnerabilidad desconocida para el proveedor del software y para el público en general.
- **VirtualBox:** Software de virtualización que permite ejecutar múltiples sistemas operativos en una sola máquina física.

Introducción

las empresas que ofrecen servicios de auditoría y protección de datos manejan información altamente sensible de sus clientes. Esta relación implica un nivel elevado de confianza, ya que la información expuesta durante estos procesos puede incluir detalles críticos sobre infraestructuras, políticas internas, e incluso datos estratégicos de defensa, como fue el caso del incidente reportado en CyberFort Technologies. En este contexto, es esencial que las empresas y sus empleados operen con el más alto estándar ético y legal, cumpliendo con las normativas nacionales e internacionales que regulan la protección de la información y los delitos cibernéticos. Sin embargo, la explotación indebida del acceso privilegiado, como el uso de herramientas avanzadas de análisis forense con fines no autorizados o la venta de información confidencial, puede derivar en graves violaciones de la confianza, afectando tanto a los clientes como a la integridad de la industria.

En el dinámico panorama de la ciberseguridad, las pruebas de penetración (pentesting) se han convertido en una herramienta indispensable para evaluar la postura de seguridad de los sistemas informáticos. Al simular ataques reales, los pentesting permiten identificar vulnerabilidades y debilidades antes de que sean explotadas por actores maliciosos.

En este ejercicio práctico iniciaremos con un análisis de la normatividad colombiana vigente, para posteriormente hacer un análisis de las actuaciones éticas y legales, con esta información podemos proceder con un entorno virtualizado con VirtualBox para llevar a cabo un pentesting basándonos en un equipo Red Team, para este ejercicio no hemos enfocado en una máquina Windows 7

infectada con el malware hipotético "Rejjeto". Utilizando Kali Linux, una distribución de Linux especializada en pruebas de penetración, exploraremos las diferentes fases de un ataque cibernético, desde la recopilación de información hasta la obtención y escalada de privilegios.

Con el análisis anterior no es posible identificar y exponer las debilidades o fallos de seguridad en un sistema informático, esto nos brindará la oportunidad de aplicar conocimientos teóricos y prácticos en un entorno controlado, permitiendo desarrollar habilidades en diversas técnicas de hacking ético. Es decir, como expertos en seguridad informática utilizan una serie de métodos y técnicas (conocidas como "técnicas de intrusión").

En este escenario de laboratorio y ya con el informe de la intrusión, nos permite como equipo Blue Team iniciar las técnicas y medidas que nos permitirán mitigar las vulnerabilidades y fallos presentados por el equipo Red Team.

Justificación

El presente documento busca fomentar el desarrollo de habilidades como lo es el análisis de documentación legal colombiana en materia de ciberseguridad y su componente ético y moral y el análisis de vulnerabilidades, explotación de vulnerabilidades, escalada de privilegios y documentación de hallazgos, en aras de poder mitigar las vulnerabilidades encontradas y posteriormente buscar una posible preparación para certificaciones para obtener certificaciones en seguridad informática como Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), entre otras.

Objetivos

Objetivo general

El objetivo principal de este pentesting es evaluar la seguridad de una máquina Windows 7 infectada con un malware, identificando las vulnerabilidades presentes y posteriormente evaluar la efectividad de las medidas de seguridad implementadas.

Objetivos específicos

- Identificar los riesgos éticos y legales asociados al acceso a información confidencial durante auditorías de seguridad en empresas de ciberseguridad, basándose en incidentes como el de CyberFort Technologies
- Implementar herramientas de evaluación de vulnerabilidades como Nmap, Legión y Metasploit para identificar, analizar y explotar debilidades en redes y sistemas, garantizando una evaluación integral de la seguridad.
- Recopilar información sobre la máquina víctima (Windows 7) a través de técnicas de reconocimiento activo y pasivo.
- Identificar los servicios en ejecución y los puertos abiertos en la máquina víctima
- Explorar vulnerabilidades conocidas en Windows 7 y en los servicios en ejecución.
- Intentar obtener acceso a la máquina víctima explotando las vulnerabilidades identificadas.
- Buscar formas de obtener privilegios de administrador.

- Identificar las mejores prácticas para la establecer la mitigación de estas vulnerabilidades.

Desarrollo del Informe

Guía de actividades y rúbrica de evaluación – Etapa 1 Conceptos equipos de Seguridad

Dentro del aparte importante nos solicitan que dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

Ley 1273 de 2009

Esta ley es pionera en Colombia en la lucha contra los delitos informáticos. Establece una categoría especial de delitos llamada "delitos contra la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas informáticos" Entre sus principales características están:

- **Protección de datos**: Penaliza el acceso, uso, eliminación o modificación no autorizada de datos personales y sistemas informáticos.
- **Ciberdelitos**: Tipifica acciones como el acceso abusivo a sistemas informáticos, la interceptación de datos, la utilización de software malicioso (como virus) y el fraude informático.

- **Sanciones**: Establece sanciones penales que pueden incluir multas y penas privativas de la libertad dependiendo de la gravedad del delito.
- **Pilar fundamental:** Esta ley es considerada el punto de partida para la regulación de los delitos informáticos en Colombia.
- **Nuevos tipos penales:** Introdujo nuevos tipos penales relacionados con la protección de la información y los datos, como el acceso abusivo a sistemas informáticos, la interceptación de datos y la destrucción de información.
- **Bien jurídico tutelado:** Creó un nuevo bien jurídico tutelado: la protección de la información y los datos.

Ley Estatutaria 1581 de 2012

También conocida como la **Ley de Protección de Datos Personales**, esta ley establece el marco normativo general para el manejo, almacenamiento y protección de datos personales en Colombia.

Algunas de sus principales características son:

- **Principios de protección de datos**: Los datos personales deben ser tratados con principios como legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad.

- **Derechos de los titulares**: Las personas tienen el derecho de conocer, actualizar y rectificar la información que las empresas o instituciones manejan sobre ellas.
- **Responsabilidad de los responsables del tratamiento**: Empresas e instituciones deben garantizar la confidencialidad de los datos y obtener el consentimiento previo y explícito de los titulares antes de recolectar o tratar su información.
- **Registro Nacional de Bases de Datos**: Las empresas y entidades públicas que manejen grandes volúmenes de datos deben inscribir sus bases de datos ante la **Superintendencia de Industria y Comercio**.
- **Principios:** Establece principios como la finalidad, la calidad, la libertad, la transparencia, el acceso y la seguridad en el tratamiento de los datos.
- **Autoridad de control:** Crea la Superintendencia de Industria y Comercio como la autoridad de control encargada de velar por el cumplimiento de la ley.

Decreto 1377 de 2013 - Reglamentario de la Ley 1581 de 2012

Este decreto reglamenta aspectos prácticos de la **Ley 1581 de 2012**. Enfoca sus disposiciones en el manejo adecuado de la información personal, estableciendo obligaciones más claras para las empresas e instituciones que tratan estos datos.

Algunas características clave incluyen:

- **Obtención de consentimiento**: Precisa cómo debe solicitarse y documentarse el consentimiento de los titulares de los datos.
- **Políticas de privacidad**: Requiere que las empresas establezcan políticas internas de protección de datos, que deben estar disponibles para los titulares.
- **Plazos para la actualización de datos**: Define los plazos y procedimientos para actualizar, rectificar o suprimir datos cuando así lo solicite el titular.

Ley 1928 de 2018 - Protección frente a la utilización indebida de datos personales en bases de datos

Con el auge de las plataformas digitales y las bases de datos masivas, esta ley refuerza las medidas de control para prevenir el uso indebido de datos personales. Su foco principal es la protección frente al uso no autorizado de datos para actividades comerciales o de mercadeo, sin el consentimiento del titular.

Decreto 886 de 2014 - Habeas Data Financiero

Este decreto reglamenta aspectos específicos del manejo de datos personales relacionados con la información crediticia y financiera, enfocándose en la protección de los derechos de los consumidores en relación con sus datos financieros. Las principales características son:

- **Rectificación de información financiera**: Los usuarios tienen derecho a solicitar la corrección de información inexacta sobre su historial crediticio.
- **Plazos para la permanencia de datos**: Regula cuánto tiempo puede permanecer la información negativa en las bases de datos de las centrales de riesgo.

Ley 2108 de 2021 - Ley de "Habeas Data"

Esta ley fortalece el derecho de las personas a acceder, actualizar y rectificar la información que sobre ellas exista en bases de datos, con énfasis en proteger los datos sensibles (como los relativos a la salud, religión, vida sexual, entre otros).

Ley 2015 de 2020 - Transacciones Electrónicas y Comercio Electrónico

Si bien no está centrada exclusivamente en delitos informáticos o protección de datos, esta ley aborda aspectos sobre la seguridad en las transacciones electrónicas, impulsando una mayor regulación sobre los sistemas de pago electrónico y la necesidad de medidas preventivas para evitar fraudes cibernéticos.

Otras leyes y decretos relevantes

- **Código Penal:** Contiene disposiciones penales relacionadas con delitos informáticos, complementando lo establecido en la Ley 1273 de 2009.
- **Decretos reglamentarios:** Existen diversos decretos que reglamentan las leyes mencionadas, estableciendo procedimientos y requisitos específicos.

Guía de actividades y rúbrica de evaluación – Etapa 2 Actuación ética y legal

Se establecieron varios puntos a tratar de los cuales se discutieron de la siguiente manera:

1. ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 – Acuerdo: acuerdo, deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

El acuerdo de confidencialidad proporcionado menciona varias cláusulas que parecen restringir la denuncia de procesos ilegales o actividades sospechosas. Estas restricciones podrían vulnerar ciertos artículos de la Ley 1273 de 2009 de Colombia, que se refiere a la protección de la información y los datos en medios informáticos y sanciona conductas relacionadas con ataques a la integridad de los sistemas de información.

A continuación, se detallan algunos artículos que podrían estar siendo vulnerados:

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

El acuerdo menciona que la parte receptora en el punto 3, 4 y punto 9 (Anexo 3 - Acuerdo), no puede denunciar actividades como "espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros" o ilegal. Si estas actividades implican acceso no autorizado a sistemas informáticos, el acuerdo podría estar promoviendo la omisión de una obligación legal de denuncia, lo que contravendría el artículo 269A de la Ley 1273.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

El acuerdo prohíbe la divulgación de "datos de chuzadas, interceptación de información"clausula 2 punto 2 (Anexo 3 - Acuerdo). Si la parte receptora tiene conocimiento de actividades de interceptación ilegal de datos y se le impide denunciarlo, esto estaría en conflicto directo con la obligación de reportar este tipo de conductas bajo la Ley 1273, en particular el artículo que sanciona la interceptación de datos sin autorización.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Aunque no se menciona explícitamente, si el acuerdo encubre procesos ilegales dentro de la empresa que pudieran causar daños a sistemas informáticos o afectar la integridad de la información, la omisión de denunciar dichas actividades podría contribuir indirectamente a la vulneración de este artículo.

Artículo 269E (Uso de software malicioso):

Si el acuerdo cubre actividades relacionadas con el uso o desarrollo de software malicioso (como malware), la prohibición de denuncia también podría ser una infracción de este artículo.

En resumen, el acuerdo intenta restringir la denuncia de actividades potencialmente ilegales, lo que podría estar vulnerando la Ley 1273 en varios aspectos, especialmente en lo que respecta a la protección de la integridad de los sistemas informáticos y la obligación de reportar conductas ilícitas que afectan a la seguridad informática.

Desarrollo del punto 2 Etapa 2 Actuación ética y legal

2. ¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo, ¿usted como experto en ciberseguridad aplicaría a este trabajo en CyberFort Technologies, donde la organización dispone de un contrato vitalicio?

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

Como experto en ciberseguridad, no recomendaría aplicar a este trabajo en CyberFort Technologies, debido a los aspectos poco confiables del acuerdo presentado, incluso con la oferta de un contrato vitalicio. El acuerdo contiene varias cláusulas que podrían limitar la ética profesional y la obligación de denunciar prácticas ilegales o inseguras, como la prohibición de denunciar espionaje o la apropiación de información confidencial e ilegal (Anexo 3 - Acuerdo).

El Código de Ética de COPNIA para ingenieros establece principios claros de responsabilidad, transparencia y protección del interés público. Según el artículo 33 del código, un ingeniero debe "abstenerse de actuar en circunstancias en las cuales el ejercicio profesional pueda verse comprometido por restricciones ilegales o contrarias a la ética profesional." Además, el artículo 34 recalca la responsabilidad de un ingeniero de proteger la información confidencial, pero siempre bajo los principios de ética y legalidad.

El acuerdo en cuestión no solo contraviene principios fundamentales de seguridad de la información, sino que también limita la denuncia de actividades ilegales, lo cual podría poner en riesgo la reputación del profesional y exponerlo a implicaciones legales. Aceptar una posición en estas condiciones no solo comprometería mi integridad profesional, sino que también podría ser incompatible con los valores éticos estipulados por COPNIA.

Desarrollo del punto 3 Etapa 2 Actuación ética y legal

3. Deberá analizar el caso problema “Ciberespionaje y Ética en CyberFort Technologies” (Anexo 7 - Escenario 2), redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar y dar respuesta los siguientes interrogantes:

El incidente descrito en CyberFort Technologies, donde empleados utilizaron su acceso privilegiado para recopilar y vender información confidencial durante una auditoría de seguridad, plantea serias implicaciones tanto legales como éticas. Este tipo de situaciones puede erosionar la confianza no solo entre las empresas de ciberseguridad y sus clientes, sino también en todo el ecosistema de seguridad digital.

¿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, durante una auditoría, deben tener acceso a información sensible para identificar vulnerabilidades y mitigar riesgos. Sin embargo, este acceso debe estar estrictamente limitado y supervisado. El propósito debe ser claro: proteger, no explotar. La confianza entre cliente y proveedor se basa en el principio de que la información sensible será utilizada únicamente para los fines especificados y no será explotada para beneficio propio o terceros, como ocurrió en el caso de CyberFort (Anexo 7 - Escenario 2).

Para garantizar que este acceso no sea explotado, se deben implementar estrictos acuerdos de confidencialidad, además de auditorías internas y externas independientes que aseguren que el acceso se usa exclusivamente para lo que fue autorizado. Cualquier desviación de estas normas podría generar violaciones a leyes como la Ley 1273 de 2009 de Colombia, que regula los delitos informáticos, como el acceso abusivo a sistemas y la interceptación de datos

¿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?

Las empresas de ciberseguridad deben contar con mecanismos de supervisión robustos para evitar que los empleados utilicen herramientas avanzadas de análisis forense esto otorga a las

empresas de ciberseguridad un poder considerable para investigar incidentes y proteger los sistemas con fines no autorizados o poco éticos. Estos mecanismos pueden incluir:

- **Control de accesos y monitoreo en tiempo real**: Se debe restringir quién puede acceder a datos sensibles y cómo se accede a ellos, con sistemas que registren toda la actividad.

- **Revisión y auditoría por terceros**: Evaluaciones externas que verifiquen que las herramientas y el acceso se utilicen de manera legítima.

- **Separación de funciones**: Ningún empleado debe tener acceso completo o sin supervisión a todas las herramientas o datos. Este tipo de segmentación minimiza el riesgo de abuso.

Programas de concienciación ética y responsabilidad: Formación constante en ética profesional y responsabilidad para los empleados, basada en códigos como los de COPNIA, que enfatizan la integridad en la profesión.

Mecanismos clave:

1. Políticas y Procedimientos Claros:

- **Política de uso aceptable:** Definir claramente los usos permitidos y prohibidos de las herramientas, incluyendo restricciones sobre el acceso a datos, la realización de análisis no autorizados y la divulgación de información confidencial.
- **Procedimientos operativos estándar (SOP):** Establecer procedimientos detallados para el uso de las herramientas, incluyendo la autorización de análisis, la documentación de los hallazgos y la gestión de las evidencias.

2. Supervisión Humana y Tecnológica:

- **Monitoreo de actividad:** Implementar sistemas de monitoreo que registren el acceso a las herramientas, las consultas realizadas y las acciones llevadas a cabo.
- **Análisis de logs:** Revisar periódicamente los logs para detectar patrones de uso inusuales o actividades sospechosas.
- **Auditorías internas:** Realizar auditorías internas regulares para evaluar el cumplimiento de las políticas y procedimientos, e identificar posibles vulnerabilidades.

3. Gestión de Acceso:

- **Control de acceso basado en roles (RBAC):** Otorgar a cada empleado solo los permisos necesarios para realizar sus tareas.
- **Autenticación de dos factores:** Exigir una autenticación de dos factores para acceder a las herramientas y sistemas sensibles.

- **Registro de acceso:** Mantener un registro detallado de todos los accesos a las herramientas y sistemas.

4. **Formación y Concienciación:**

- **Capacitación continua:** Impartir formación regular a los empleados sobre ética profesional, privacidad de datos y las implicaciones legales del uso indebido de las herramientas.
- **Códigos de conducta:** Establecer códigos de conducta claros que reflejen los valores de la empresa y las expectativas en materia de ética profesional.

5. **Tecnologías de Prevención:**

- **Detección de anomalías:** Utilizar herramientas de detección de anomalías para identificar comportamientos inusuales en los sistemas.
- **Sistemas de prevención de intrusiones (IPS):** Implementar IPS para proteger las herramientas y los sistemas contra ataques externos.
- **Encriptación de datos:** Proteger los datos sensibles mediante encriptación.

6. Mecanismos de Denuncia:

- **Canales anónimos:** Establecer canales seguros y anónimos para que los empleados puedan denunciar posibles irregularidades.
- **Protección a denunciantes:** Garantizar la protección de los denunciantes contra represalias.

7. Evaluaciones de Riesgo:

- **Análisis de riesgos:** Realizar evaluaciones de riesgo periódicas para identificar las amenazas potenciales y tomar las medidas necesarias para mitigarlas.

8. Colaboración con Fuerzas del Orden:

- **Comunicación abierta:** Establecer canales de comunicación claros con las fuerzas del orden para reportar cualquier actividad criminal.

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

Cuando se descubre que una empresa de ciberseguridad ha cometido actos de ciberespionaje, los gobiernos y organizaciones deben actuar rápidamente para restaurar la confianza. Algunas medidas apropiadas incluyen:

Rescisión inmediata del contrato y sanciones legales: La violación de la confidencialidad y la comisión de ciber espionaje deben ser perseguidas judicialmente, con sanciones acordes a la legislación vigente, tanto penal como civil.

- **Investigación exhaustiva:** Es esencial llevar a cabo una investigación independiente y transparente para determinar el alcance del ciber espionaje, identificar a los responsables y comprender los motivos detrás de estos actos.

Comunicación abierta: Informar de manera clara y transparente a todas las partes involucradas, incluyendo al público en general, sobre los hallazgos de la investigación y las medidas que se están tomando.

Terminación del contrato: Rescindir de inmediato el contrato con la empresa implicada y prohibirle participar en futuros proyectos gubernamentales o corporativos.

Sanciones legales: Aplicar las sanciones legales correspondientes a la empresa y a los individuos involucrados, según las leyes y regulaciones vigentes.

Divulgación transparente: Informar de manera clara y abierta sobre lo ocurrido y las medidas tomadas puede ayudar a restaurar la confianza de otros clientes y partes interesadas.

- **Revisión de los procesos de contratación**: Implementar mecanismos más rigurosos para evaluar y seleccionar a las empresas de ciberseguridad, incluyendo verificaciones de antecedentes, auditorías de seguridad y evaluaciones de cumplimiento normativo.

Fortalecimiento de las medidas de seguridad: Aumentar las inversiones en seguridad cibernética, tanto a nivel gubernamental como organizacional, para proteger los sistemas y datos sensibles.

- **Mayor transparencia**: Promover la transparencia en las operaciones de las empresas de ciberseguridad y exigirles que cumplan con estándares internacionales de ética y seguridad.

- **Colaboración internacional**: Fomentar la cooperación entre los gobiernos y organizaciones internacionales para establecer normas y estándares comunes en materia de ciberseguridad y prevenir futuros incidentes de este tipo.

- **Educación y concienciación**: Impartir capacitación a los empleados sobre las mejores prácticas de seguridad cibernética y concienciar a la población sobre los riesgos del ciber espionaje.

Implementación de controles más estrictos: Las organizaciones deben revisar sus políticas de contratación y auditoría de terceros, reforzando los requisitos de seguridad y supervisión para evitar que situaciones similares se repitan.

- **Supervisión continua**: Establecer mecanismos de supervisión y auditoría regulares para las empresas de ciberseguridad contratadas, con el fin de detectar cualquier actividad sospechosa.

- **Requisitos de certificación**: Exigir a las empresas de ciberseguridad que obtengan certificaciones reconocidas en el sector y que demuestren su compromiso con la seguridad.

- **Creación de un marco regulatorio**: Desarrollar un marco regulatorio sólido y actualizado que establezca los requisitos mínimos de seguridad para las empresas de ciberseguridad y que imponga sanciones severas por el incumplimiento de las normas.

Reparación y compensación: Ofrecer una compensación adecuada por los daños causados, tanto económicos como reputacionales, y tomar medidas concretas para mitigar los efectos del espionaje.

Guía Unidad 2 Fase 3 -Ejecución de pruebas de intrusión

Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Red Team. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

Pasos del Pentesting

A. Configuración del Entorno:

- **Instalación de VirtualBox**: Se realiza la instalación del VirtualBox en su última versión.

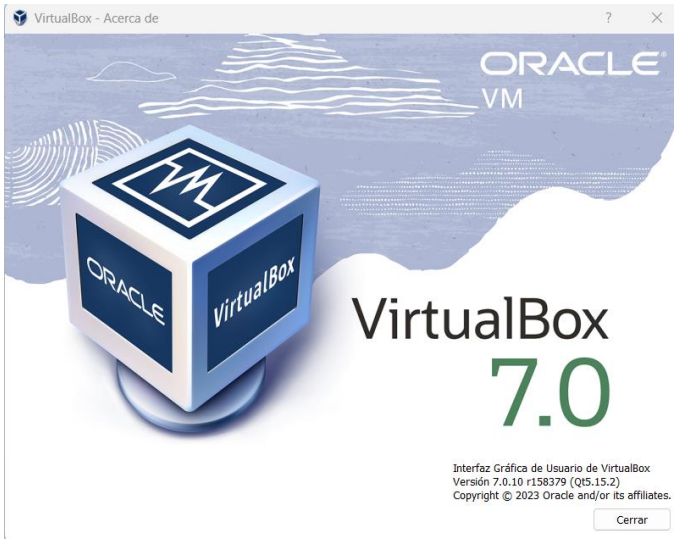

Ilustración 1 VirtualBox 7.0, fuente propia (2024)

- **Creación de máquinas virtuales:**

- **Máquina atacante (Kali Linux):** Se configura una máquina virtual con Kali Linux como sistema operativo.

Ilustración 2- Kali Linux, funte propia (2024)

- **Máquina víctima (Windows 7):** Se Instala Windows 7 y se simula la infección con "Rejjeto".

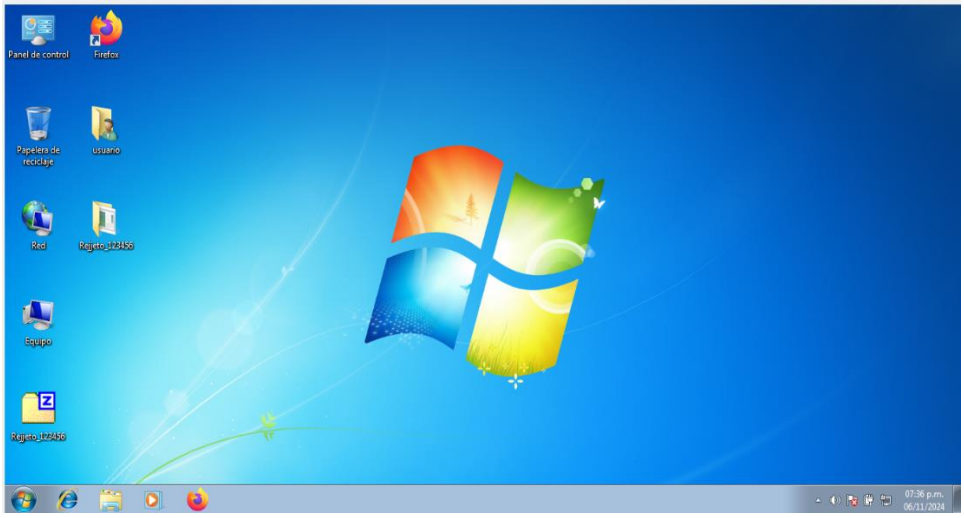

Ilustración 3 -Windows 7, fuente propia (2024)

Una vez instalado el servicio se procede a abrir el programa que se utiliza con un servidor de archivos HTTP File Server que nos abre un puerto determinado o que se modificar de acuerdo con lo mostrado en la figura

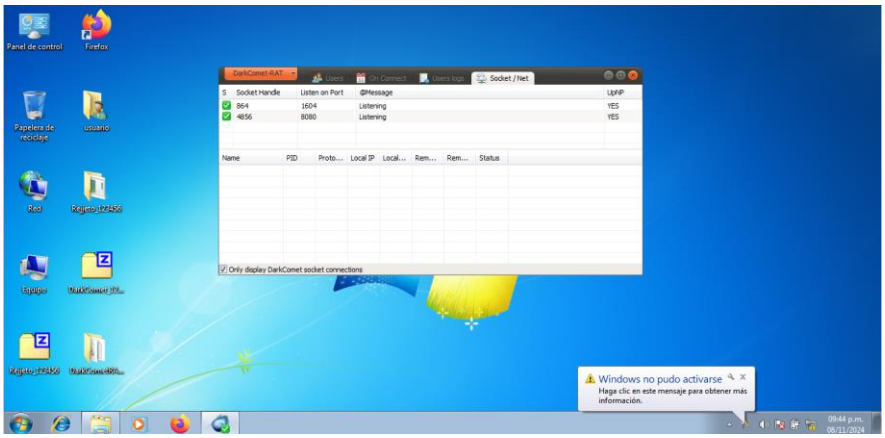

Ilustración 4- DarkComect-RAT

- Máquina virtual GNS3: GNS3 (Graphic Network Simulator-3), es un simulador gráfico de red lanzado en 2008, que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellas

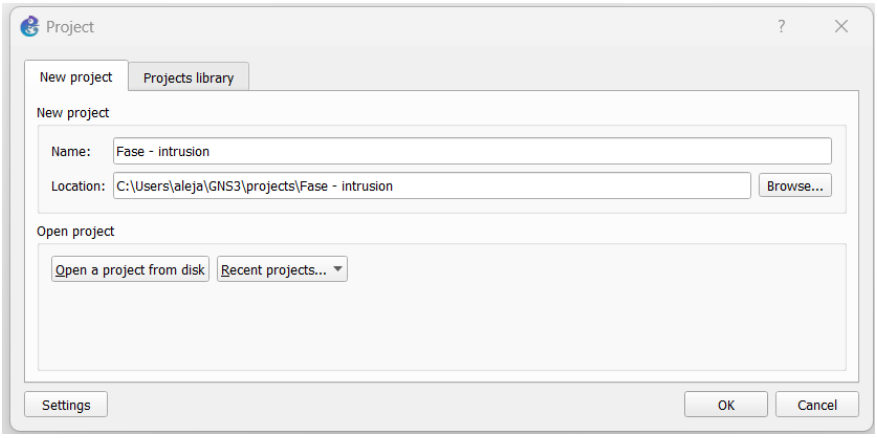

Ilustración 5- Nuevo Proyecto GNS3, fuente propia (2024)

Para la guía se utiliza como nuevo proyecto nombrado Fase- Intrusión y se elabora una red que nos permita simular la topología de red y el ataque.

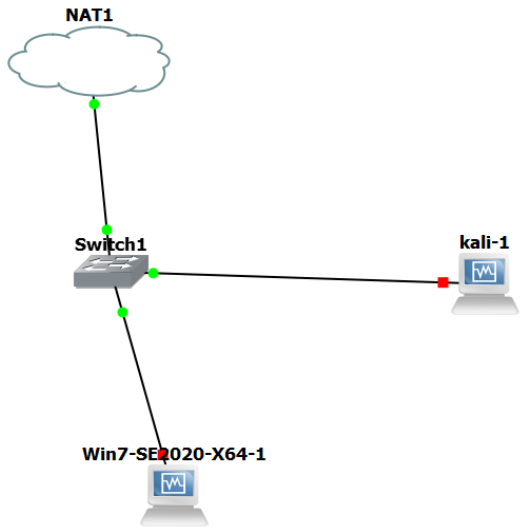

Ilustración 6- Red GNS3, fuente propia (2024)

Se agregan los sistemas operativos instalados en VirtualBox y se crea la red como se muestra en la imagen y se verifica la conexión entre ellos.

- **Configuración de redes**: Configura las redes virtuales para que ambas máquinas puedan comunicarse entre sí.

  Obtenemos desde GNS3 la dirección que se va a tener por defecto las maquinas a trabajar

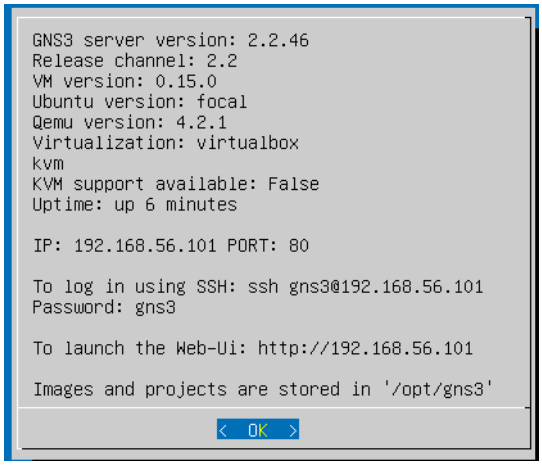

Ilustración 7- Ip GNS3, fuente propia (2024)

Utilizamos el comando # ifconfig desde Kali Linux y podemos obtener la dirección de red

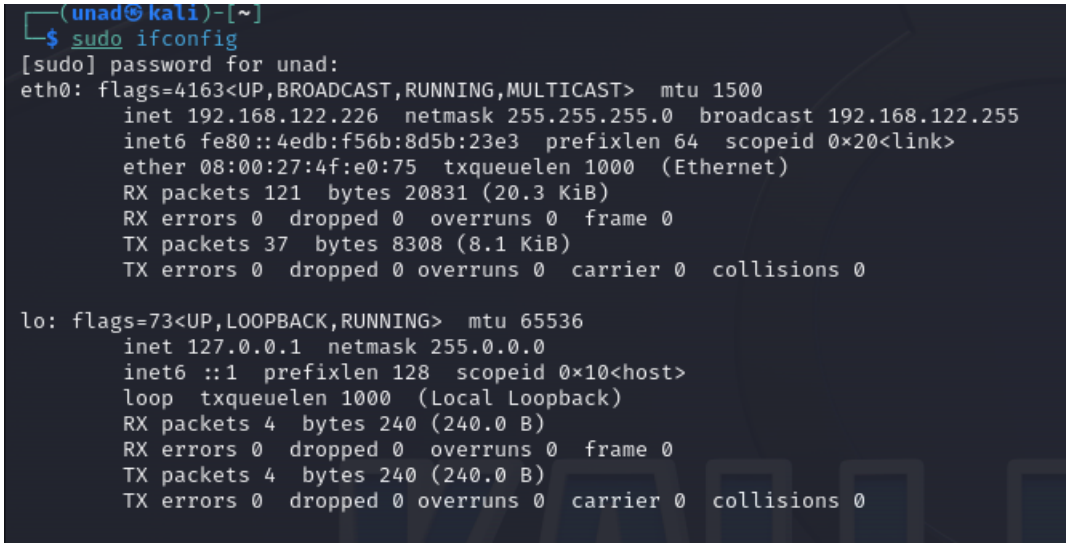

Ilustración 8- Ip Kali Linux, fuente propia (2024)

Para Windows podemos utilizar la herramienta de red para poder visualizar la dirección ip o con el comando # ipconfig /all podemos visualizar por consola la dirección ip.

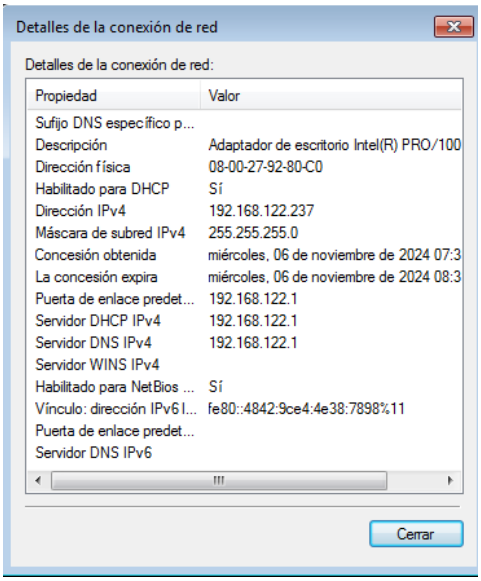

Ilustración 9- Ip Windows 7, fuente propia (2024)

A. Reconocimiento:

- Escaneo de puertos: Utilizamos herramientas como Nmap y legion para identificar los puertos abiertos en la máquina víctima.

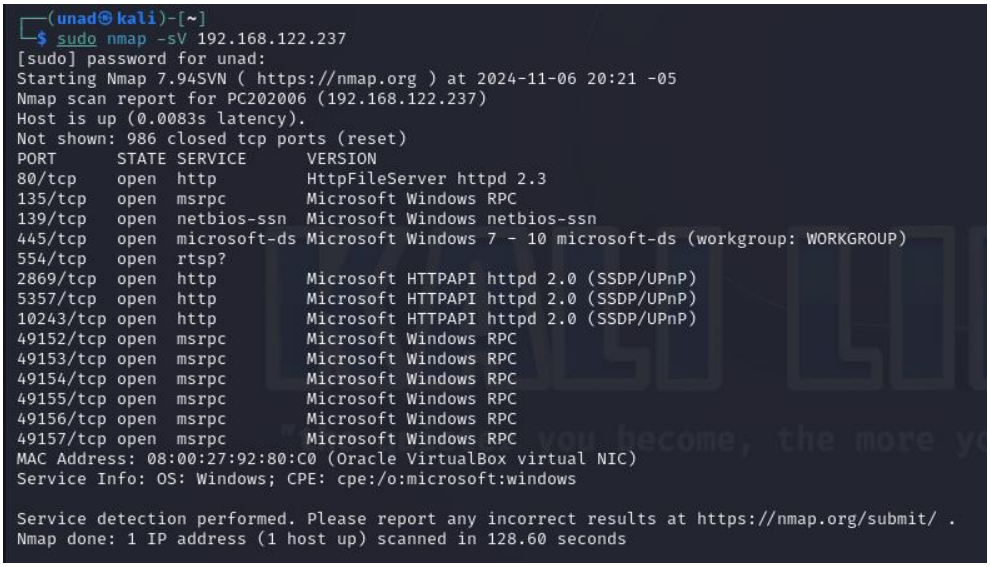

Ilustración 10- Scaneo nmap, fuente propia (2024)

- **Enumeración de servicios:** Identifica los servicios que están en ejecución en la máquina víctima y busca vulnerabilidades conocidas asociadas a ellos.

Por medio de la herramienta nmap se realiza la búsqueda de acuerdo con los comandos establecidos por la herramienta que nos permiten realizar la búsqueda en la dirección Ip objetivo, en este caso utilizaremos el comando # nmap -f -- script vuln 192.168.122.237, este script me permite visualizar las diferentes vulnerabilidades que posteriormente pueden ser aprovechadas y explotadas.

Recopilación de información: Busca información pública sobre la máquina víctima (si fuese un escenario real) utilizando herramientas de búsqueda de shodan, censys, etc.

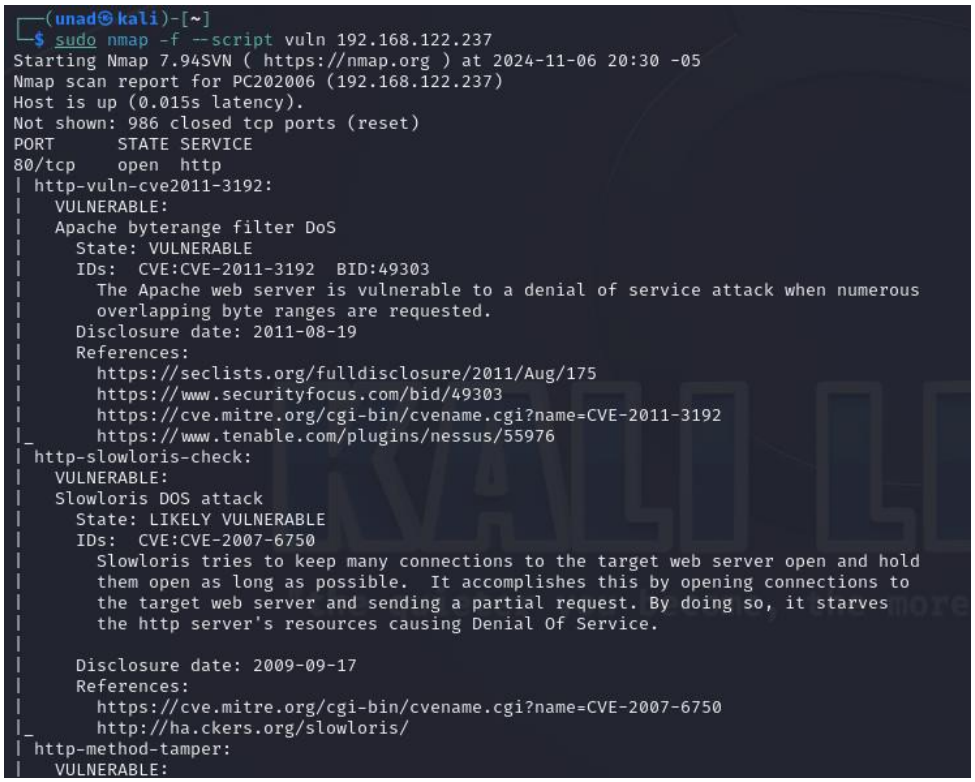

Ilustración 11-nmap vulnerabilidades, fuente propia (2024)

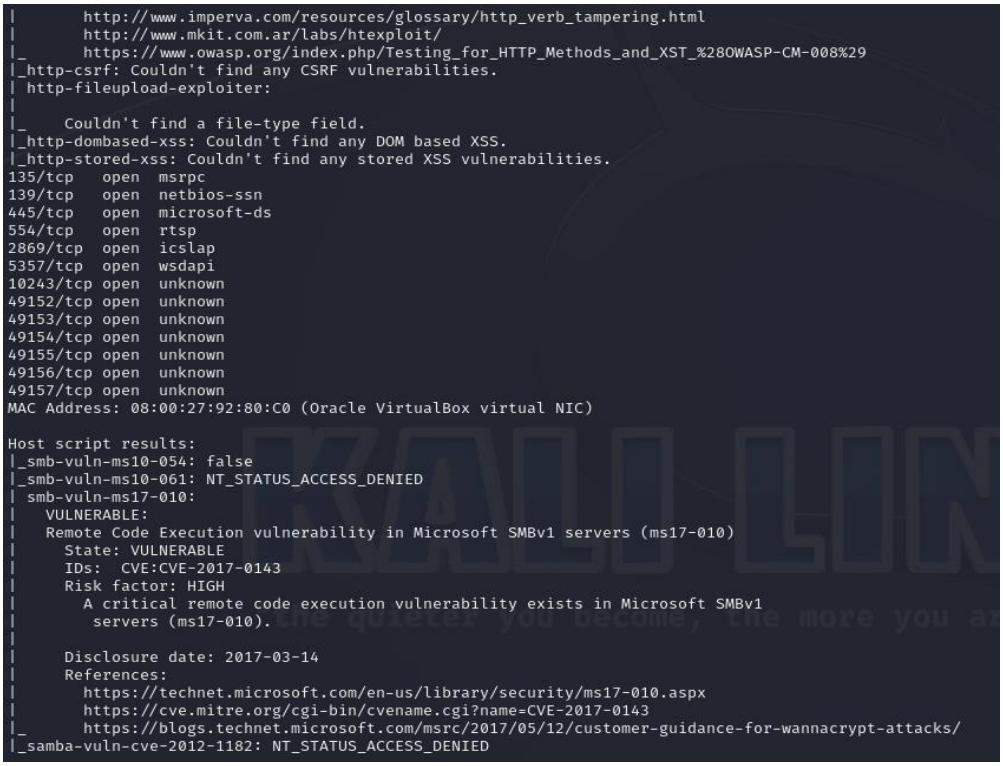

Ilustración 12 - nmap vulnerabilidades, fuente propia (2024)

Desarrollo del punto 2

1. A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows.

- **Enumeración de servicios:** Identificamos todos los servicios en ejecución en la máquina comprometida. Esto nos permitió tener una idea de qué aplicaciones o procesos podrían estar expuestos.
- **Análisis de puertos abiertos:** Utiliza herramientas como Nmap y legión para escanear los puertos abiertos en la máquina. Esto nos permite identificar servicios que podrían ser vulnerables.
- **Búsqueda de procesos sospechosos:** Revisamos la lista de procesos en ejecución buscando nombres de archivos o procesos asociados a DarkComet o a otros malware conocidos.

Desarrollo del punto 3

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

La segunda herramienta utilizada es Legión, por lo general, la herramienta Legión viene preinstalada con Kali Linux, pero, si necesitamos instalarla, podemos ejecutar el siguiente comando # sudo apt-get install legion -y.

Legión es una herramienta de pruebas de penetración de red de código abierto, super extensible y semiautomatizada que ayuda en el descubrimiento, el reconocimiento y la explotación.

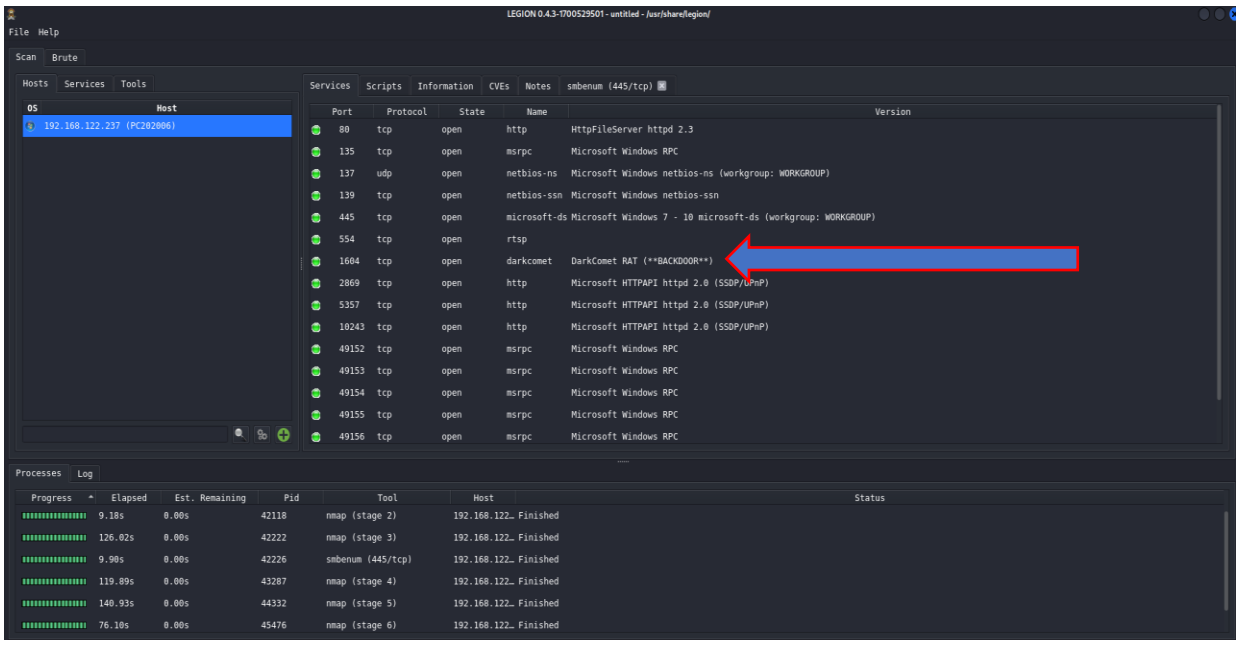

Ilustración 13- Legion, fuente propia (2024)

Se realiza la búsqueda de acuerdo con la información suministrada por Nmap con la dirección ip de nuestro sistema Windows 7 vulnerable, la dirección 192.168.122.237 donde podemos observar en la imagen 13 los servicios que se encontraron vulnerables entre esos el **puerto 1604** abierto con

el protocolo Tcp abierto darkcomet RAT, entre los otros servicios abierto con su respectivo protocolo

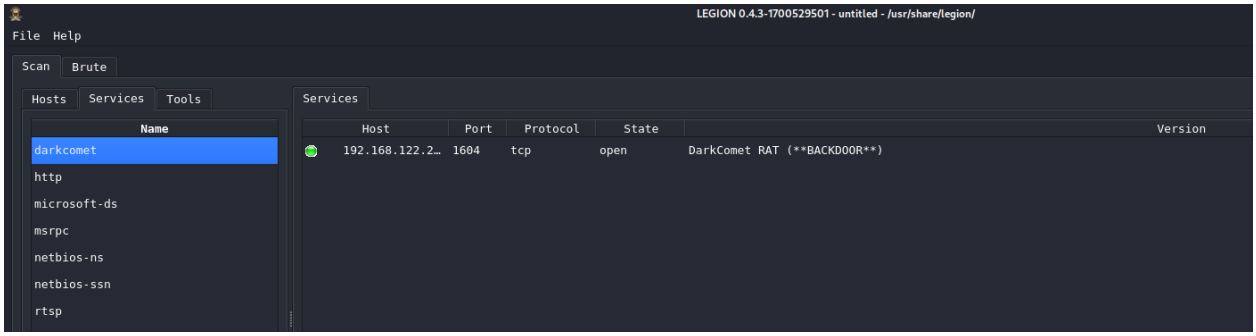

Ilustración 14- Legión servicio Darcomet, fuente propia (2024)

Por servicios se selecciona el nombre darkcomet y se verifica el servicio del cual se va a aprovechar la vulnerabilidad

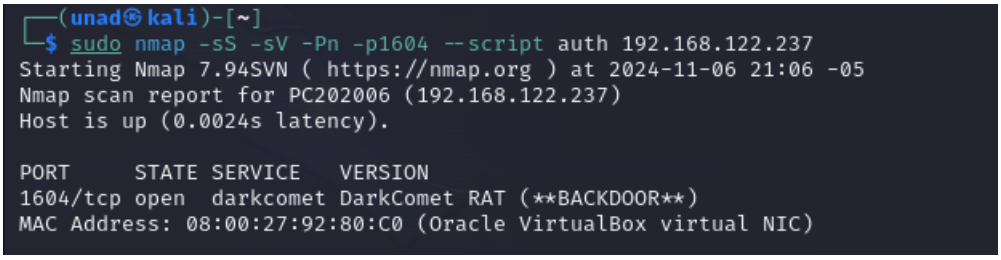

Ilustración 15- Nmap puerto 1608, fuente propia (2024)

Con la herramienta nmap se realiza un escaneo con el puerto seleccionado y se verifica lo arrojado por legión.

Una vez identificado el puerto y el servicio se realiza la explotación de vulnerabilidades conocidas Se identifica una vulnerabilidad específica asociada a DarkComet o al sistema operativo, se intenta explotarla para confirmar los hallazgos.

Desarrollo del punto 4

3. Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows), haga uso de gráficos para explicar el ataque.

B. **Obtención de acceso:**

- **Explotación de vulnerabilidades:** Una vez identificadas las vulnerabilidades, se utiliza herramientas como Metasploit para explotarlas y obtener un acceso inicial a la máquina víctima.

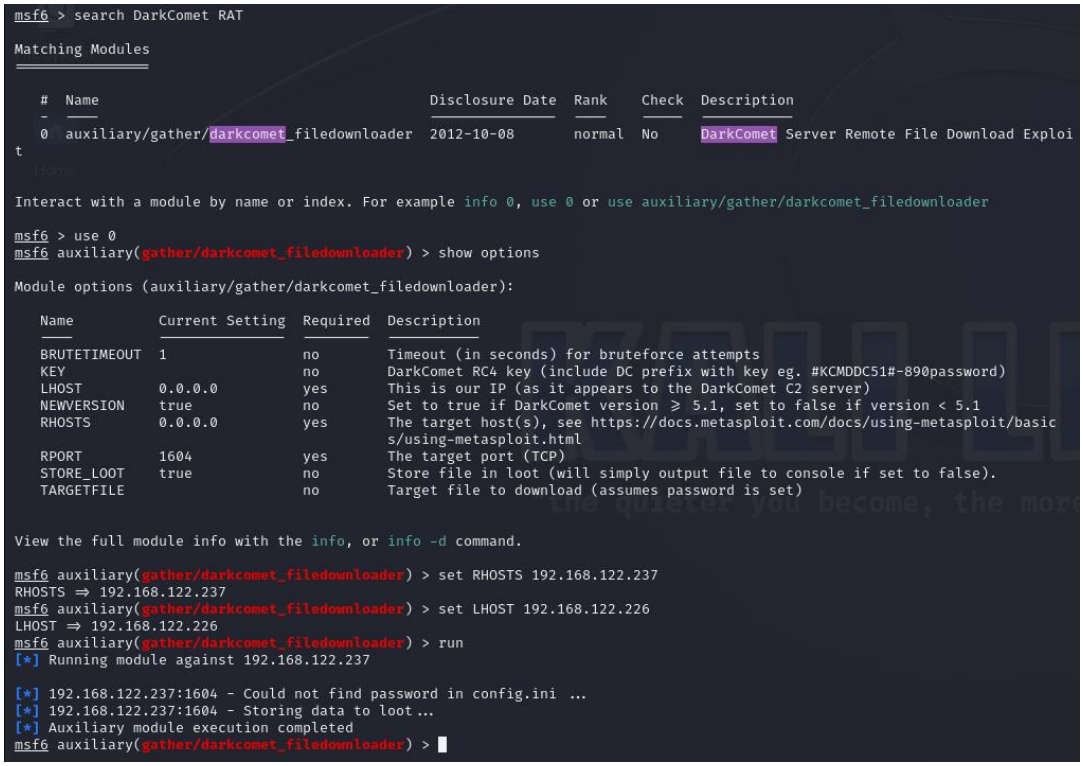

Ilustración 16 -Metasploit, fuente propia (2024)

Una vez identificado el puerto y el servicio se utiliza la herramienta para la búsqueda de vulnerabilidades, en este caso utilizamos el comando #search Darkcomet para que la herramienta nos oriente en su base de datos de exploit como podemos aprovecharla.

En este caso nos arroja un resultado el # exploit/Windows/http/rejjeto_hfs_ejec, con su respectiva descripción lo que nos orienta a que podemos utilizar este exploit para nuestro ejercicio.

Posteriormente utilizamos con el comando # use 0 el exploit y se selecciona, una vez seleccionado el exploit a utilizar lo configuramos con el comando # show options que nos emite introducción la dirección Ip de nuestro objetivo con el comando # set RHOST (dirección Ip), posteriormente ejecutamos nuestro exploit con el comando run y verificamos que corra de manera correcta, como se muestra en la ilustración No 16

C. **Escalada de privilegios:**

- **Buscar vulnerabilidades locales:** Una vez dentro del sistema, buscamos vulnerabilidades locales que permitan obtener privilegios de administrador.

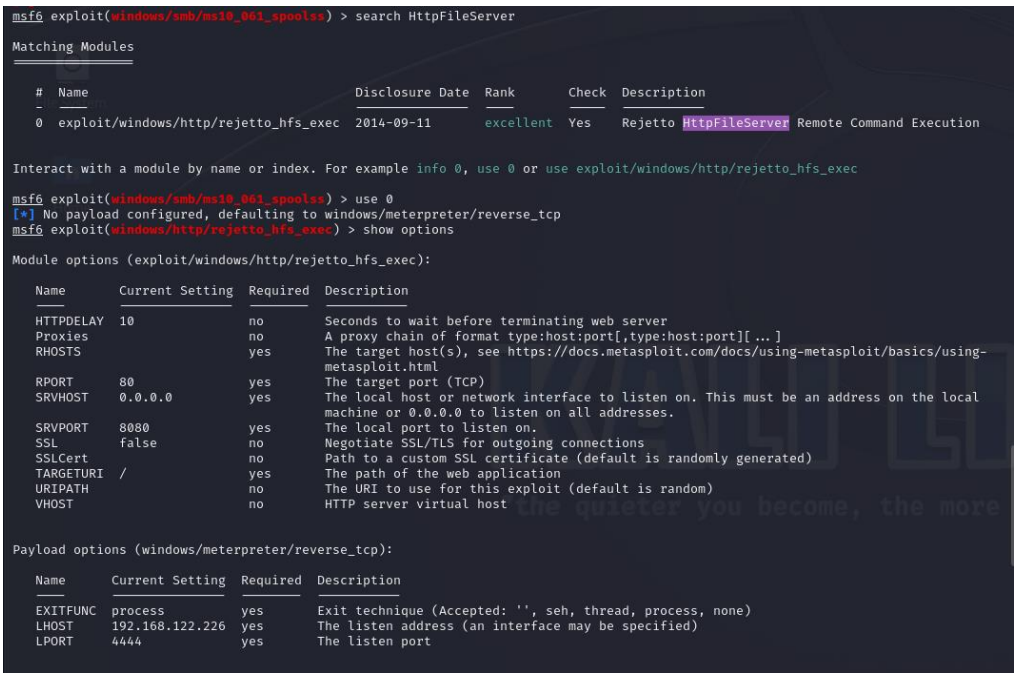

Ilustración 17- Utilizando el exploit, fuente propia (2024)

Ya se aprovechó la vulnerabilidad Darkcomet y al ser un servicio HttpFileServer utilizamos el comando search HttpFileServer lo cual al realizar la búsqueda nos permite encontrar un exploit en la base de datos, utilizamos con el comando # use 0, el exploit y configuramos el mismo como se mostró en la anterior imagen

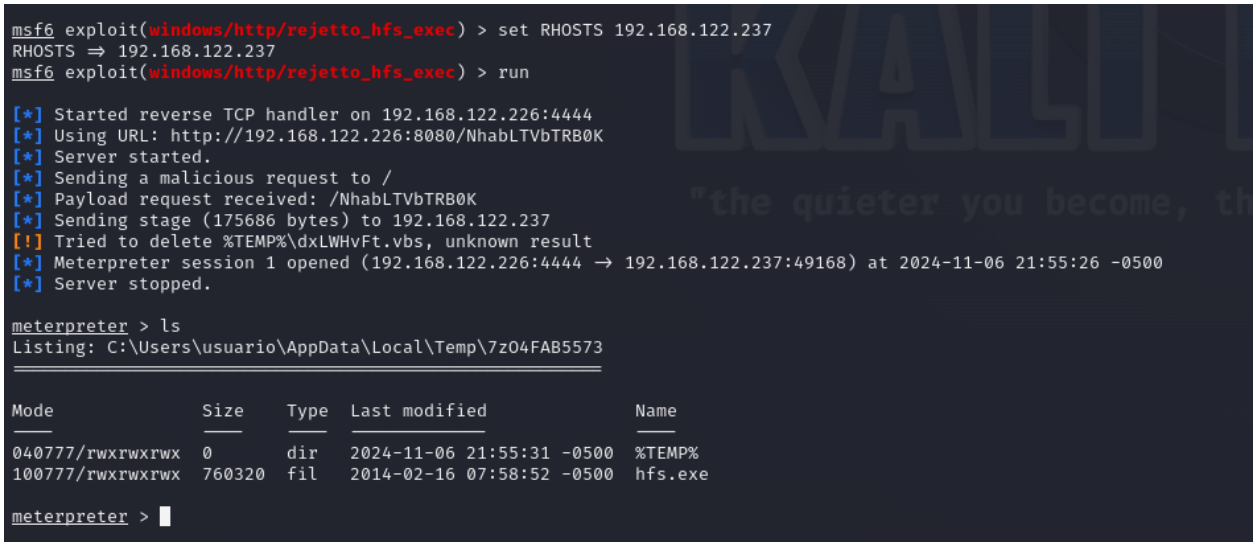

Ilustración 18-Corriendo vulnerabilidad, fuente propia (2024)

Al ejecutar el exploit se puede verificar que montamos una sesión llamada **meterpreter,** mostrando el direccionamiento y los puertos que se utilizaron para crear una sesion1

Ya en la sesión se utiliza el comando #ls que nos permite verificar la lista de archivos en la sesión que queda alojada en la dirección c:\user\usuario\AppData\Local\Temp

Mantenimiento del acceso:

Backdoors: Instala un backdoor en el sistema para mantener el acceso remoto

```
meterpreter > ls
Listing: C:\
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2020-06-26 23:05:04 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2020-06-26 23:04:42 -0500  Archivos de programa
040777/rwxrwxrwx  0      dir   2009-07-14 00:08:56 -0500  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-13 22:20:08 -0500  PerfLogs
040555/r-xr-xr-x  4096   dir   2020-06-26 23:54:12 -0500  Program Files
040555/r-xr-xr-x  4096   dir   2020-06-26 23:53:09 -0500  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2020-06-26 23:53:08 -0500  ProgramData
040777/rwxrwxrwx  0      dir   2020-06-26 23:04:43 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2024-11-06 21:03:19 -0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2020-06-27 00:10:21 -0500  Users
040777/rwxrwxrwx  16384  dir   2020-06-27 00:41:48 -0500  Windows
000000/----------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2009-07-14 00:08:56 -0500  All Users
040555/r-xr-xr-x  8192   dir   2020-06-26 23:04:42 -0500  Default
040777/rwxrwxrwx  0      dir   2009-07-14 00:08:56 -0500  Default User
040555/r-xr-xr-x  4096   dir   2011-04-12 04:10:43 -0500  Public
100666/rw-rw-rw-  174    fil   2009-07-13 23:54:24 -0500  desktop.ini
040777/rwxrwxrwx  0      dir   2020-06-27 00:09:17 -0500  semi
040777/rwxrwxrwx  8192   dir   2020-06-26 23:05:12 -0500  usuario

meterpreter > mkdir johncastro
Creating directory: johncastro
meterpreter > ls
Listing: C:\Users
=================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2009-07-14 00:08:56 -0500  All Users
040555/r-xr-xr-x  8192   dir   2020-06-26 23:04:42 -0500  Default
040777/rwxrwxrwx  0      dir   2009-07-14 00:08:56 -0500  Default User
040555/r-xr-xr-x  4096   dir   2011-04-12 04:10:43 -0500  Public
100666/rw-rw-rw-  174    fil   2009-07-13 23:54:24 -0500  desktop.ini
040777/rwxrwxrwx  0      dir   2024-11-06 22:35:01 -0500  johncastro
040777/rwxrwxrwx  0      dir   2020-06-27 00:09:17 -0500  semi
```

Ilustración 19- Creación de usuario Windows 7, fuente propia (2024)

Ya dentro del sistema y conociendo la ruta donde nos encontramos, nos devolvemos en la ruta donde se encuentra la carpeta User de usuarios del sistema y creamos la carpeta con el comando # mkdir johncastro.

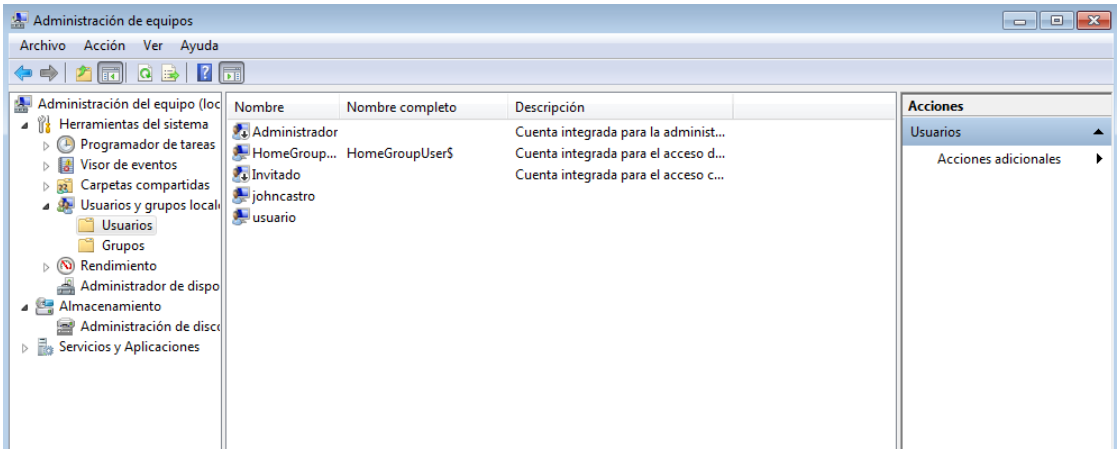

Ilustración 20- Usuario creado Windows 7, fuente propia (2024)

Escalamos privilegios en la maquina victima con el comando #getprivs # getuit

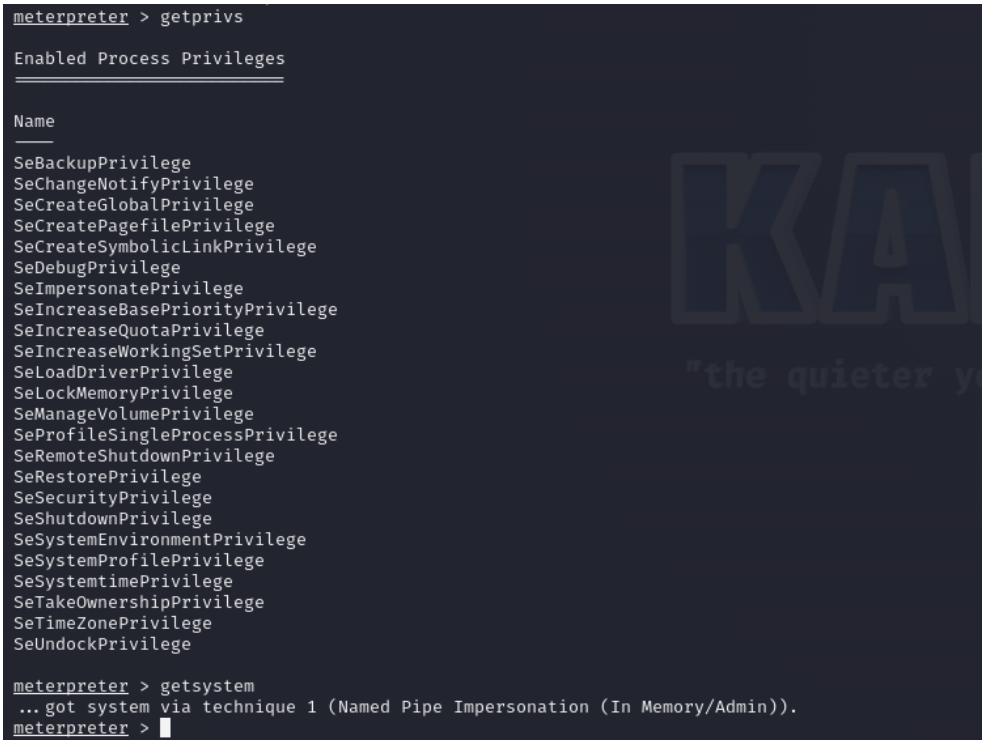

Ilustración 21- Escalada de privilegios, fuente propia (2024)

Con el comando Shell iniciamos sesión como en terminal de Windows y creamos el usuario con el comando # net user johncastro /add

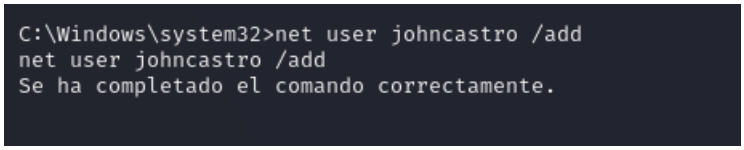

Ilustración 22- creación usuario Windows, fuente propia (2024)

Ya con los privilegios desde la terminal Shell en Windows se verifica el grupo con al comando # net localgroup lo que nos muestra el listado de privilegios, posterior a verificar el grupo se ingresa el comando # net localgroup Administradores johncastro /add, lo que nos permite escalar los privilegios y tener un acceso completo del sistema.

```
C:\Users\usuario\AppData\Local\Temp\7zO4FAB5573>net localgroup
net localgroup

Alias para \\PC202006

-------------------------------------------------------------------------------
*Administradores
*Duplicadores
*HomeUsers
*IIS_IUSRS
*Invitados
*Lectores del registro de eventos
*Operadores criptogr♦ficos
*Operadores de configuraci♦n de red
*Operadores de copia de seguridad
*Usuarios
*Usuarios avanzados
*Usuarios COM distribuidos
*Usuarios de escritorio remoto
*Usuarios del monitor de sistema
*Usuarios del registro de rendimiento
Se ha completado el comando correctamente.


C:\Users\usuario\AppData\Local\Temp\7zO4FAB5573>net localgroup Administradores johncastro /add
net localgroup Administradores johncastro /add
Se ha completado el comando correctamente.
```

Ilustración 23- Creando privilegios, fuente propia (2024)

Ilustración 24- Usuario Administrador Windows, fuente propia (2024)

Como se muestra en la ilustración 24, se puede confirmar que se ha creado el usuario y que se le han creado los privilegios de administrador.

Unidad 3 - Etapa 4 Contención de ataques informáticos

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

Si detectara un ataque en tiempo real en un sistema Windows 7, seria crucial actuar rápidamente para contener la amenaza y minimizar los daños. presentaría una serie de pasos y consideraciones técnicas:

Aislamiento del Sistema:

- **Desconectar de la red:** Lo primero seria aislar el sistema comprometido de la red para evitar la propagación del malware a otros equipos. Desconectaría el cable de red o desactivaría la conexión Wi-Fi.
- **Desactivar servicios no esenciales:** Detendría todos los servicios no esenciales para reducir la superficie de ataque.
- **Activar o verificar el firewall de Windows:** Se activa o se verifica que conexiones se pueden permitir.

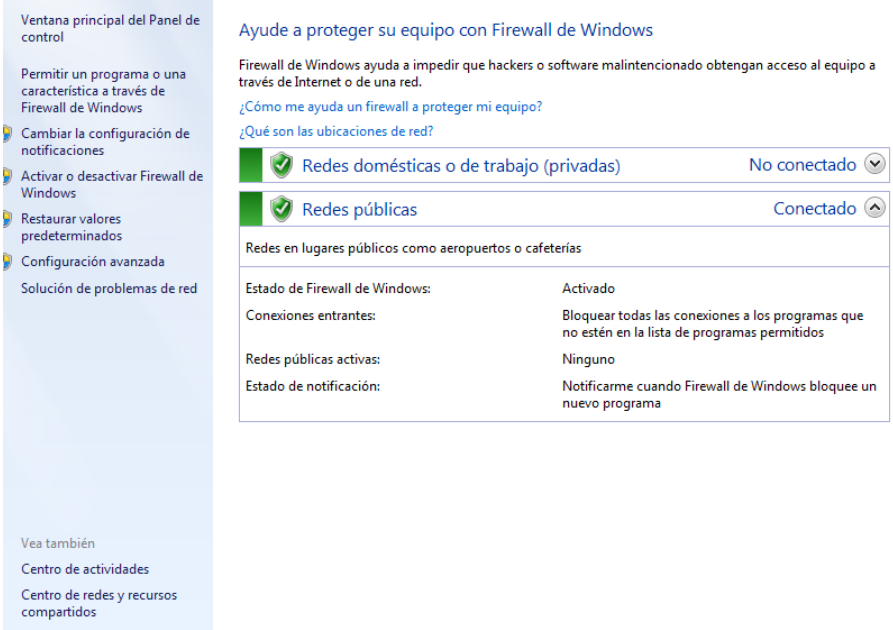

Ilustración 25 - Activar Firewall, fuente propia (2024)

Iniciar el Modo Seguro:

- **Reiniciar en modo seguro:** Reiniciaría el sistema en modo seguro con funciones de red. Esto cargará un conjunto mínimo de controladores y servicios, dificultando la actividad del malware o ataque.

Análisis del Sistema:

- **Buscar procesos sospechosos:** Utilizaría el Administrador de tareas (Ctrl+Shift+Esc) para identificar procesos desconocidos o que consumen recursos excesivos.

- **Verificar archivos de registro:** Revisaría los archivos de registro del sistema (eventvwr.msc) para encontrar entradas relacionadas con el ataque, como intentos de acceso no autorizados, errores de inicio de sesión o cambios en la configuración del sistema.
- **Buscar archivos modificados:** Compara los archivos del sistema con copias de seguridad o con un sistema limpio para identificar archivos que hayan sido modificados o añadidos por el malware.

Eliminar el Malware:

- **Utilizar un antivirus actualizado:** Ejecutaría un análisis completo del sistema con un antivirus actualizado.
- **Eliminar archivos maliciosos:** Identifica y elimina los archivos maliciosos encontrados en el análisis.
- **Quitar claves de registro:** Elimina las claves de registro creadas por el malware.

Restaurar el Sistema:

- **Utilizar un punto de restauración:** Utilizaría un punto de restauración creado antes de la infección, restáuralo para volver el sistema a un estado anterior.

Cambiar contraseñas:

- **Cambiar contraseñas de cuentas:** Cambia las contraseñas de todas las cuentas que hayan podido ser comprometidas, incluyendo las de correo electrónico y otros servicios en línea, cuentas de usuario.

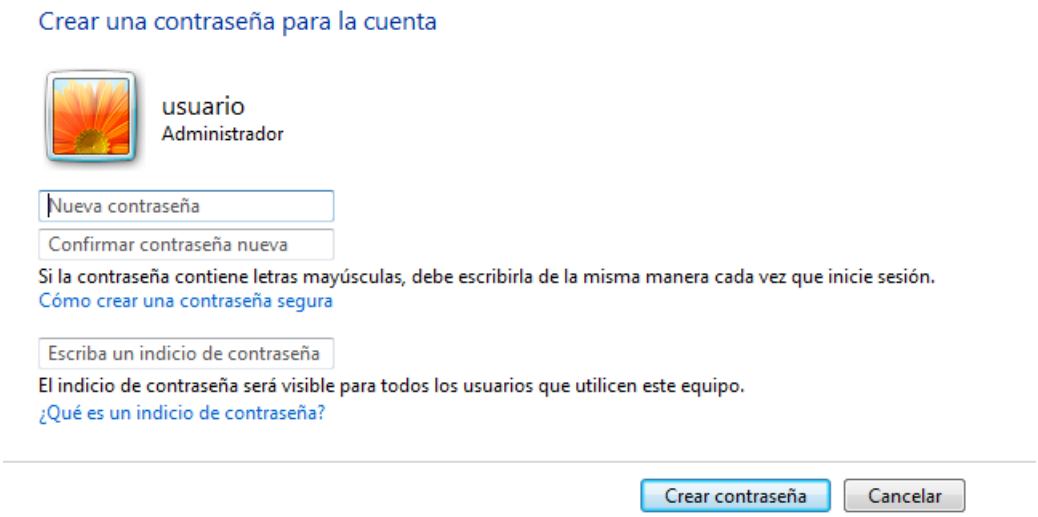

Ilustración 26 - Crear Contraseñas, fuente propia (2024)

7. Informar y documentar:

- **Documentar los pasos:** Documenta todos los pasos realizados durante la investigación y eliminación del malware.

- **Informar al equipo de seguridad:** Informa al equipo Red Team de seguridad de la organización sobre el incidente para que puedan tomar las medidas necesarias para prevenir futuros ataques.

Consideraciones Adicionales con Windows 7:

- **Vulnerabilidades conocidas:** Asegúrate de que Windows 7 esté actualizado con todos los parches de seguridad disponibles.
- **Software de terceros:** Deshabilita o elimina cualquier software de terceros que no sea esencial, ya que podría contener vulnerabilidades.
- **Análisis forense:** Si el ataque ha sido especialmente grave, realizaría un análisis forense completo del sistema para identificar la causa raíz y prevenir futuros ataques.

Para el caso concreto se instala autopsy en la máquina que ha sido vulnerada y se verifica en los informes que ha pasado sospechoso en nuestro sistema arrojando la instalación del malware y la creación de la cuenta de usuario.

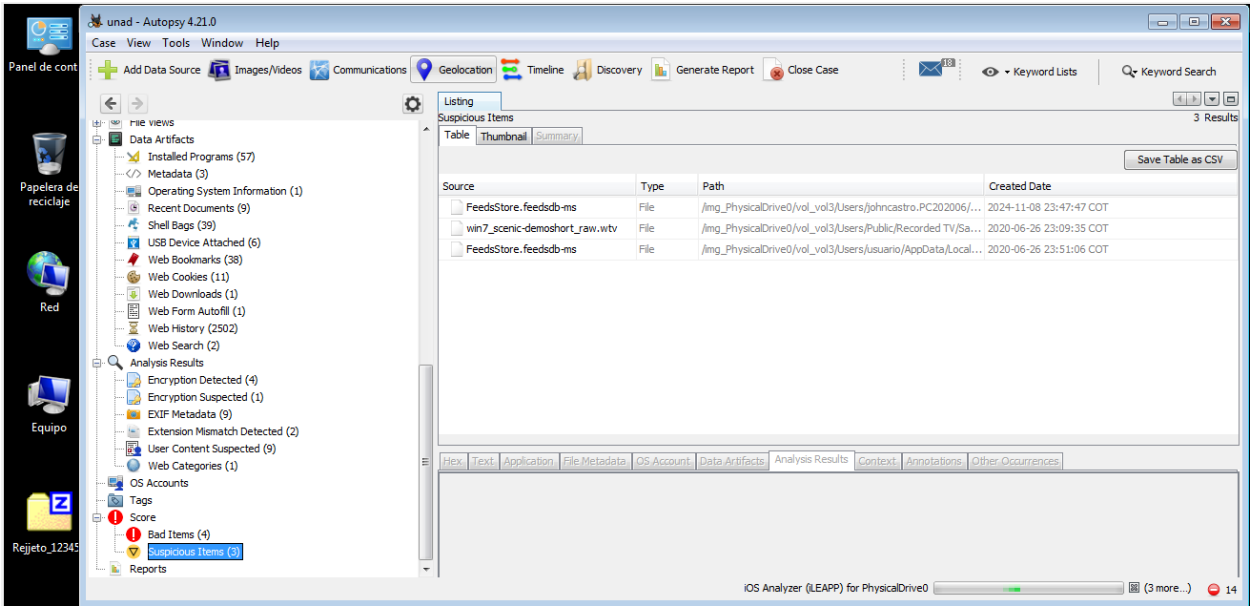

Ilustración 27 - Informe Autopsy, fuente propia (2024)

De esta manera se logra identificar que nuestro sistema se encuentra comprometido y fue vulnerado.

Desarrollo del punto 2

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team, qué medidas de hardenización propondría para que el ataque no se repita?

Dentro del ejercicio propuesto se realizó un ataque desde Kali Linux con un equipo Windows 7 vulnerable con DarkComet que es un potente RAT (Remote Access Trojan) que permite a atacantes tomar el control remoto de un sistema comprometido. Al atacar el sistema Windows 7,

que ya no cuenta con soporte oficial de Microsoft, se aprovechó las vulnerabilidades conocidas y configuraciones por defecto que pueden ser explotadas fácilmente.

Medidas de Hardenización Propuestas

Para prevenir ataques como DarkComet y fortalecer la seguridad de un sistema Windows 7, se propone implementar las siguientes medidas de hardenización:

Actualizaciones y Mantenimiento

- **Parches de seguridad:** A pesar de que Windows 7 ya no recibe actualizaciones oficiales, es fundamental instalar todos los parches de seguridad disponibles para las aplicaciones y software instalados, especialmente aquellos con vulnerabilidades conocidas.
- **Actualizaciones de antivirus:** Mantener el antivirus actualizado y realizar escaneos regulares.
- **Deshabilitar servicios innecesarios:** Deshabilitar servicios de Windows y aplicaciones de terceros que no sean esenciales para reducir la superficie de ataque.

Configuración de Red

- **Firewall:** Activar y configurar el firewall de Windows para bloquear puertos innecesarios y permitir solo el tráfico necesario.

- **VPN:** Utilizar una VPN para cifrar el tráfico de red y proteger la conexión a internet.
- **Segmentación de red:** Si es posible, segmentar la red para limitar el impacto de una posible infección.

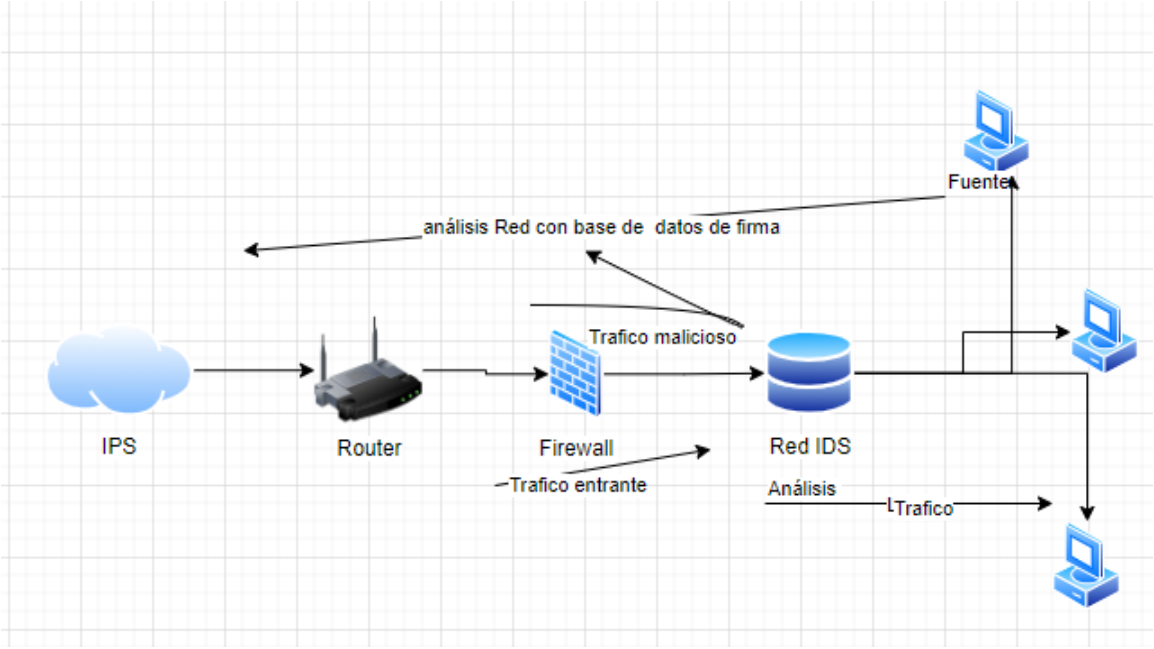

Ilustración 28 - Cambios en la Red, fuente propia (2024)

Controles de Acceso

- **Contraseñas fuertes:** Implementar políticas de contraseñas robustas, exigiendo contraseñas largas y complejas.
- **Autenticación multifactor:** Utilizar la autenticación multifactor para agregar una capa adicional de seguridad al proceso de inicio de sesión.

- **Control de cuentas de usuario:** Configurar el control de cuentas de usuario (UAC) para solicitar permisos de administrador antes de realizar cambios en el sistema.

Seguridad Física

- **Control de acceso físico:** Restringir el acceso físico a los equipos para evitar manipulaciones no autorizadas.
- **Prevención de dispositivos externos:** Implementar políticas para controlar el uso de dispositivos externos como memorias USB.

Detección y Respuesta a Incidentes

- **Sistemas de detección de intrusiones (IDS):** Implementar un IDS para monitorear el tráfico de red y detectar actividades sospechosas.
- **Planes de respuesta a incidentes:** Desarrollar un plan detallado para responder a incidentes de seguridad de manera rápida y eficaz.
- **Realizar copias de seguridad:** Realizar copias de seguridad regulares de los datos importantes para facilitar la recuperación en caso de un ataque exitoso.
- **Análisis de vulnerabilidades:** Realizar análisis de vulnerabilidades periódicamente para identificar y corregir debilidades en el sistema.

- **Monitoreo continuo:** Monitorear continuamente el sistema en busca de cualquier actividad sospechosa.

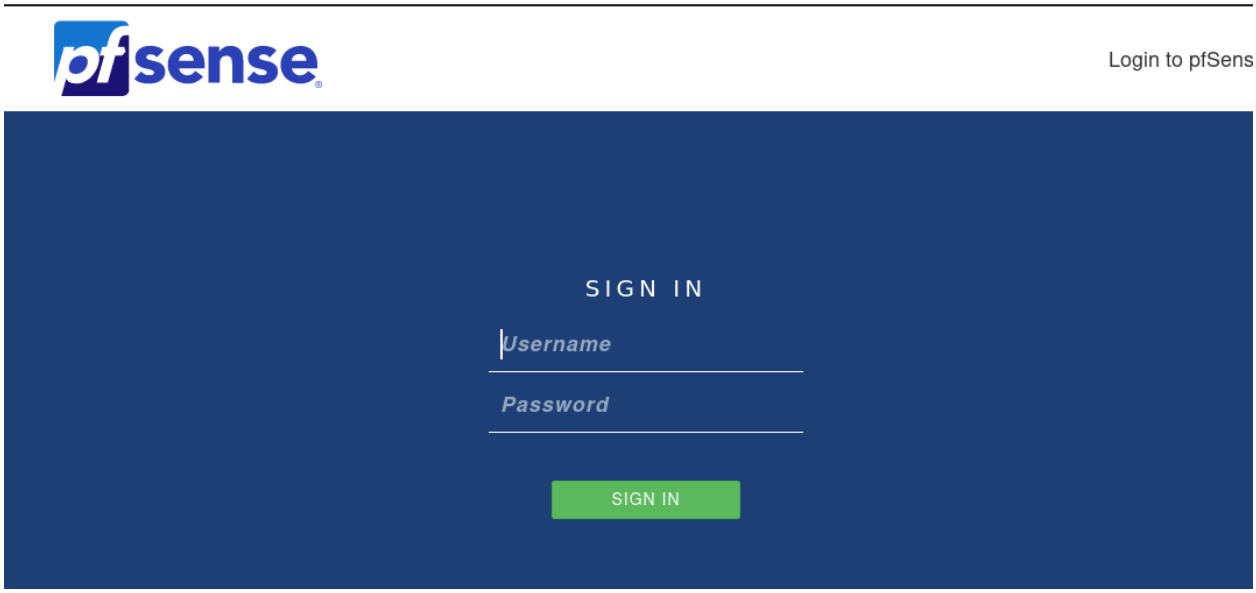

Ilustración 29 - Pfsense, fuente propia (2024)

En este ejercicio y como propuesta se instala una herramienta open source como Pfsense que nos permite tener un firewall e Implementar un IDS para monitorear el tráfico de red y detectar actividades sospechosas.

Migración a un Sistema Operativo Moderno

pesar de estas medidas, la mejor manera de protegerse contra ataques como DarkComet es migrar a un sistema operativo moderno y con soporte, como Windows 10. Los sistemas operativos más recientes incluyen características de seguridad más robustas y reciben actualizaciones de seguridad de forma regular.

Desarrollo del punto 3

3. ¿Describa con sus palabras las diferencias entre un equipo BlueTeam y un equipo de respuesta a incidentes informáticos?

Ambos equipos desempeñan un papel crucial en la ciberseguridad, pero tienen enfoques y responsabilidades ligeramente diferentes:

Equipo Blue Team (Equipo Azul)

- **Enfoque proactivo:** Se centra en la prevención de incidentes de seguridad.
- **Actividades:**
  - **Monitoreo continuo:** Vigila constantemente los sistemas y redes en busca de anomalías o actividad sospechosa.

- **Análisis de amenazas:** Identifica y evalúa las amenazas potenciales que podrían afectar a la organización.
- **Implementación de controles de seguridad:** Configura firewalls, sistemas de detección de intrusiones (IDS), y otras medidas de seguridad para proteger los sistemas.
- **Capacitación de usuarios:** Educa a los empleados sobre las mejores prácticas de seguridad para reducir el riesgo de ataques.
- **Objetivo principal:** Mantener la seguridad de la organización de manera continua y proactiva, reduciendo la probabilidad de sufrir un incidente.

Equipo de Respuesta a Incidentes Informáticos

- **Enfoque reactivo:** Se activa cuando se detecta un incidente de seguridad.
- **Actividades:**
  - **Detección de incidentes:** Identifica y confirma la ocurrencia de un incidente de seguridad.
  - **Contención:** Aísla el incidente para evitar que se propague a otros sistemas.
  - **Erradicación:** Elimina la amenaza y restaura los sistemas a un estado seguro.
  - **Análisis:** Investiga el incidente para determinar su causa raíz y aprender de él.
  - **Recuperación:** Restaura los datos y sistemas afectados.
  - **Comunicación:** Informa a las partes interesadas sobre el incidente y las acciones tomadas.

- **El equipo Blue Team** es como un guardia de seguridad que patrulla un edificio, buscando posibles intrusos y tomando medidas preventivas.
- **El equipo de respuesta a incidentes** es como un equipo de bomberos que responde a un incendio, conteniendo el fuego, apagándolo y evaluando los daños.

Desarrollo del punto 4

4. ¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "¿Center For Internet Security", usted lo utilizaría para qué fin?

El CIS (Center for Internet Security) es una organización sin fines de lucro que proporciona estándares y mejores prácticas de seguridad cibernética ampliamente reconocidos en la industria. Si como miembro de un equipo Blue Team te indicaran trabajar con CIS, podrías aprovechar sus recursos para diversos fines:

1. **Establecer una Línea Base Segura:**

- **CIS Benchmarks:** Estos benchmarks te ofrecen una guía detallada para configurar de forma segura sistemas operativos, aplicaciones y dispositivos de red. Al utilizarlos como

punto de partida, puedes asegurar que tu infraestructura cumple con los estándares de seguridad más altos.

- **Identificación de vulnerabilidades:** Comparando la configuración actual de tu sistema con los CIS Benchmarks, podrás identificar rápidamente las configuraciones que no cumplen con las mejores prácticas y, por lo tanto, son más vulnerables a ataques.

2. **Priorizar las Medidas de Seguridad:**

- **CIS Controls:** Los CIS Controls te brindan una lista priorizada de acciones defensivas que puedes implementar para proteger tu organización contra las amenazas cibernéticas más comunes y peligrosas. Al seguir estos controles, puedes enfocar tus esfuerzos en las medidas de seguridad más importantes.

3. **Demostrar Cumplimiento Normativo:**

- **Marcos regulatorios:** Muchos marcos regulatorios, como PCI DSS, HIPAA y NIST, hacen referencia a los CIS Controls o Benchmarks. Al utilizar estos estándares, puedes demostrar que tu organización cumple con los requisitos legales y regulatorios aplicables.

4. Mejorar la Colaboración entre Equipos:

- **Lenguaje común:** El CIS proporciona un lenguaje común y un marco de referencia para que los equipos de seguridad, TI y otros departamentos se comuniquen de manera efectiva sobre los riesgos y las medidas de seguridad.
- **Mejores prácticas compartidas:** Al utilizar los mismos estándares, los equipos pueden colaborar de manera más eficiente y compartir conocimientos.

4. **Validar la Eficacia de las Medidas de Seguridad:**

- **Evaluación continua:** Puedes utilizar los CIS Benchmarks para evaluar de forma periódica la eficacia de tus medidas de seguridad y realizar ajustes según sea necesario.

Desarrollo Punto 5

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

SIEM, acrónimo de Security Information and Event Management (Gestión de Información y Eventos de Seguridad), es una solución de software que centraliza y correlaciona datos de seguridad de diversas fuentes en una organización. Imagina que es un centro de control que monitorea constantemente tu red, buscando patrones sospechosos y alertando de posibles amenazas.

Funciones Principales de un SIEM:

- **Recolección de Datos:** Un SIEM recopila datos de una amplia variedad de fuentes, como firewalls, sistemas operativos, aplicaciones, dispositivos de red y registros de seguridad.
- **Normalización de Datos:** Transforma los datos de diferentes formatos en un formato común, lo que facilita su análisis y correlación.
- **Análisis de Datos:** Emplea algoritmos avanzados para analizar los datos en busca de patrones anómalos, correlacionar eventos y detectar amenazas potenciales.
- **Detección de Amenazas:** Identifica comportamientos sospechosos, como intentos de intrusión, malware y ataques de denegación de servicio.
- **Generación de Alertas:** Genera alertas en tiempo real cuando se detectan amenazas, permitiendo a los equipos de seguridad responder rápidamente.
- **Investigación de Incidentes:** Proporciona herramientas para investigar a fondo los incidentes de seguridad, identificando la causa raíz y el alcance del ataque.
- **Generación de Informes:** Crea informes detallados sobre el estado de seguridad de la organización, las amenazas detectadas y las acciones tomadas.

Características Principales de un SIEM:

- **Consolidación de Datos:** Reúne datos de múltiples fuentes en una única plataforma.

- **Correlación de Eventos:** Identifica relaciones entre diferentes eventos para detectar ataques complejos.
- **Análisis en Tiempo Real:** Permite detectar amenazas a medida que ocurren.
- **Escalabilidad:** Se adapta a organizaciones de cualquier tamaño y complejidad.
- **Personalización:** Permite configurar reglas y alertas personalizadas para adaptarse a las necesidades específicas de cada organización.
- **Integración con Otras Herramientas:** Se integra con otras herramientas de seguridad, como sistemas de detección de intrusiones (IDS) y herramientas de respuesta a incidentes.
- **Visualización:** Ofrece interfaces gráficas intuitivas para visualizar los datos y las amenazas.

Beneficios de Utilizar un SIEM:

- **Detección temprana de amenazas:** Identifica ataques antes de que causen daños significativos.
- **Respuesta más rápida a incidentes:** Reduce el tiempo de detección y respuesta a incidentes.
- **Mejor comprensión de los riesgos:** Proporciona una visión holística de la postura de seguridad de la organización.

- **Cumplimiento normativo:** Ayuda a cumplir con los requisitos de diversas normativas de seguridad.
- **Reducción de costos:** Evita pérdidas económicas causadas por incidentes de seguridad.

Desarrollo Punto 6

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

Las herramientas de contención de ataques informáticos son esenciales para mitigar las amenazas y proteger los sistemas. A continuación, te presento tres herramientas clave, tanto de hardware como de software, que cumplen esta función:

Herramientas de Contención de Ataques Informáticos

1. Firewalls:

- **Definición:** Un firewall es un sistema de seguridad que monitorea el tráfico de red entrante y saliente, permitiendo o bloqueando datos según un conjunto de reglas de seguridad.

- **Funcionamiento:** Actúa como un filtro, examinando cada paquete de datos que entra o sale de una red. Si el paquete cumple con las reglas, se permite el paso; de lo contrario, se bloquea.
- **Tipos:**
  - **Firewalls de hardware:** Dispositivos físicos que se instalan en la red para protegerla.
  - **Firewalls de software:** Aplicaciones que se ejecutan en un sistema operativo y protegen un dispositivo individual o una red más pequeña.

- **Características clave:**
  - **Filtrado de paquetes:** Analiza los paquetes de datos para determinar si deben ser permitidos o bloqueados.
  - **Stateful inspection:** Mantiene un estado de las conexiones para tomar decisiones más inteligentes sobre el tráfico.
  - **NAT (Network Address Translation):** Oculta las direcciones IP internas de una red.

2. Sistemas de Detección y Prevención de Intrusiones (IDS/IPS):

- **Definición:** Los IDS y IPS son sistemas diseñados para detectar y prevenir ataques a redes informáticas.
- **Funcionamiento:**

- **IDS:** Monitorea el tráfico de red en busca de patrones que indiquen un ataque y genera alertas.
- **IPS:** Además de detectar, los IPS pueden tomar medidas para bloquear el ataque, como descartar paquetes o bloquear conexiones.

- **Tipos:**
- **Basados en firmas:** Buscan patrones conocidos de ataques.
- **Basados en anomalías:** Detectan desviaciones del comportamiento normal de la red.

- **Características clave:**
- **Análisis de tráfico:** Examinan el contenido de los paquetes de datos en busca de firmas de ataque.
- **Generación de alertas:** Avisan al administrador de seguridad sobre actividades sospechosas.
- **Medidas de mitigación:** Pueden bloquear el tráfico malicioso o aislar sistemas comprometidos.

3. Sistemas de Prevención de Pérdida de Datos (DLP):

- **Definición:** Los DLP son sistemas diseñados para identificar, monitorear y proteger datos confidenciales dentro de una organización.

- **Funcionamiento:** Analizan el contenido de los archivos, correos electrónicos y otros datos para identificar información sensible y prevenir su fuga.
- **Características clave:**
  - **Clasificación de datos:** Identifica y clasifica los datos según su sensibilidad.
  - **Monitoreo de dispositivos:** Rastrea los dispositivos USB y otros medios de almacenamiento para evitar la copia de datos no autorizada.
  - **Encriptación:** Protege los datos en tránsito y en reposo.
  - **Prevención de fugas de datos:** Bloquea la transmisión de datos confidenciales a destinos no autorizados.

Otras herramientas importantes:

- **Antivirus y antimalware:** Detectan y eliminan software malicioso.
- **Sistemas de gestión de eventos de seguridad (SEM):** Centralizan y correlacionan los eventos de seguridad de toda la organización.
- **HSM (Hardware Security Module):** Módulos de hardware que almacenan claves criptográficas de forma segura.

Conclusiones

Los profesionales y empresas de ciberseguridad deben adherirse a altos estándares de conducta, como los establecidos por normativas como la Ley 1273 de 2009 y el Código de Ética de COPNIA, que exigen un comportamiento responsable y transparente al manejar información sensible.

Los actos de ciberespionaje, como el perpetrado por empleados de CyberFort, tienen graves implicaciones legales y profesionales. Las organizaciones que cometen o facilitan estos actos deben enfrentar sanciones legales severas, además de perder la confianza de sus clientes y del sector. Para restaurar esa confianza, es necesario que las empresas y gobiernos establezcan medidas de reparación, incluyendo la divulgación transparente de los incidentes y la adopción de controles más estrictos en futuras auditorías.

Los gobiernos y organizaciones deben actuar rápidamente cuando descubren que una empresa de ciberseguridad ha cometido actos de ciberespionaje, como en el caso de CyberFort Technologies. Las acciones deben incluir la rescisión del contrato, sanciones legales, y la implementación de políticas que aseguren que estos incidentes no se repitan. Además, es fundamental establecer protocolos de respuesta que permitan restaurar la confianza y proteger la reputación de las instituciones afectadas.

La confianza en el sector de la ciberseguridad depende no solo de la competencia técnica, sino también del compromiso con principios éticos y legales. Las empresas deben operar dentro de un marco de integridad, y tanto gobiernos como organizaciones deben ser diligentes al establecer controles y responder ante cualquier violación que comprometa la seguridad y confidencialidad de la información.

La Importancia de la Ciberseguridad y las Herramientas Especializadas: En un entorno digital cada vez más complejo, las organizaciones y profesionales necesitan estar bien equipados para enfrentar amenazas emergentes. Herramientas como Metasploit, Nmap y OpenVAS son fundamentales para identificar y explotar vulnerabilidades, lo que permite realizar pruebas de penetración eficaces. Estas herramientas ayudan a simular ataques reales, proporcionando un diagnóstico preciso de las debilidades en sistemas y redes, y permitiendo una respuesta proactiva.

Las pruebas de penetración siguen un proceso bien definido que abarca desde el reconocimiento inicial hasta la explotación y la remediación de vulnerabilidades. La correcta implementación de este proceso es vital para evaluar la seguridad de los sistemas. Además, la integración de herramientas específicas en cada fase, como Nmap para el escaneo y Metasploit para la explotación, asegura que el análisis de seguridad sea profundo y eficiente.

Bases de Datos de Vulnerabilidades: ExploitDB y CVE: El acceso a bases de datos como ExploitDB y CVE es crucial para mantener un sistema actualizado frente a amenazas conocidas. Estas bases permiten a los profesionales de seguridad estar al tanto de vulnerabilidades recientes y exploits disponibles, mejorando significativamente la capacidad de respuesta ante incidentes de seguridad.

La creación de un laboratorio de pruebas de ciberseguridad en un entorno virtual, utilizando GNS3 para simular redes y sistemas, es una estrategia eficaz para llevar a cabo pentesting y evaluaciones de vulnerabilidades en un entorno controlado. Este montaje, con la interacción entre Kali Linux y Windows en red clase C, permite una evaluación detallada y simulaciones realistas, facilitando la mejora de las habilidades técnicas.

El correcto funcionamiento de un laboratorio de pruebas de ciberseguridad requiere un hardware robusto, con un procesador potente, suficiente memoria RAM y almacenamiento rápido. Estos recursos aseguran que las simulaciones y análisis de vulnerabilidades se realicen sin interrupciones y con resultados confiables.

La configuración de redes virtuales es esencial para realizar pruebas en un entorno seguro. La asignación adecuada de direcciones IP y la configuración de servicios en las máquinas virtuales permiten realizar pruebas de penetración, ataques y análisis de tráfico con el propósito de identificar posibles fallas de seguridad.

Este banco de trabajo con GNS3, Kali Linux y Windows en red C ofrece un entorno controlado ideal para simular ataques reales y mejorar las habilidades en ciberseguridad. La capacidad de integrar herramientas especializadas, junto con una configuración de red realista, permite realizar pruebas de vulnerabilidades, monitoreo de tráfico y evaluación de respuestas ante posibles amenazas.

Realizamos un pentesting en un entorno virtual como VirtualBox que nos permite practicar y mejorar tus habilidades de hacking ético de manera segura y controlada. Al seguir estos pasos y utilizando las herramientas adecuadas y expuestas en este documento, podrás identificar las vulnerabilidades en un sistema y proponer medidas para mejorar su seguridad del entorno donde se encuentre trabajando o estudiando.

Referencias

Nmap: The network mapper - Free Security Scanner. (s/f). Nmap.org. Recuperado el 14 de octubre de 2024, de https://nmap.org/

Lee, J., Greenbone, A. G., & Feilner, M. (2024, septiembre 25). Vulnerability management. Greenbone; Greenbone AG. https://www.greenbone.net/en/

Metasploit - penetration testing tool. (s/f). Rapid7. Recuperado el 14 de octubre de 2024, de https://www.rapid7.com/products/metasploit/

Exploit Database. (s/f). Exploit-db.com. Recuperado el 14 de octubre de 2024, de https://www.exploit-db.com/

Cve - cve. (s/f). Mitre.org. Recuperado el 14 de octubre de 2024, de https://cve.mitre.org/

(S/f). Normas-iso.com. Recuperado el 14 de octubre de 2024, de https://www.normas-iso.com/iso-27001/

Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. (s/f). Senado de la República de Colombia. Recuperado el 14 de octubre de 2024, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012]. (s/f). Senado de la República de Colombia. Recuperado el 14 de octubre de 2024, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Decreto 1377 de 2013 - Gestor Normativo. (s/f). Gov.co. Recuperado el 14 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1928_2018]. (s/f). Senado de la República de Colombia. Recuperado el 14 de octubre de 2024, de http://secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

(S/f). Raspberrypi.com. Recuperado el 14 de mayo de 2024, de https://www.raspberrypi.com/software/

Al-Sarawi, S. F., Anjum, A., & Kurien, S. (2020). Intrusion detection systems (IDS) for the Internet of Things (IoT): State-of-the-art and future directions. Journal of Network and Computer Applications, 160, 102560. doi: 10.1016/j.jnca.2020.102560

Choo, K.-K. R., & Han, G. (2021). Lightweight intrusion detection systems for resource-constrained IoT devices. Sustainable Computing: Informatics and Systems, 31, 100639. doi: 10.1016/j.suscom.2021.100639

National Institute of Standards and Technology (NIST). (2020). Interconnecting smart devices: Security considerations.

Cve - cve. (s/f). Mitre.org. Recuperado el 14 de octubre de 2024, de https://cve.mitre.org/

Exploit Database. (s/f). Exploit-db.com. Recuperado el 14 de octubre de 2024, de https://www.exploit-db.com/

(S/f). Normas-iso.com. Recuperado el 14 de octubre de 2024, de https://www.normas-iso.com/iso-27001/

Anexos

- Enlace Video https://youtu.be/95Zfd3uDYRQ