Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Javier Felipe Quijano Rodríguez

Asesor

Ing. Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI)

Especialización en Seguridad Informática

2025

Esta página opcional

_____

Eduvin Trigos Sánchez

_____ _____

Jurado Jurado

2025

Dedicatoria

Con amor dedico este trabajo a mi Madre, María Isabel Rodríguez, que con su carisma y comprensión me acompañó en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones de hijo, que con su apoyo, consagración y paciencia disminuyo mis tareas en el hogar permitiéndome una entrega más tranquila en el estudio y trabajo.

Agradecimientos

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

Resumen

El informe detalla las estrategias de los equipos Red Team y Blue Team en CyberFort Technologies, abarcando desde los conceptos básicos hasta la ejecución de pruebas de intrusión y la contención de ataques.

Se analizan aspectos como la legislación colombiana sobre delitos informáticos, el proceso de pentesting, las herramientas de ciberseguridad y la configuración de entornos de trabajo.

También se discuten la ética y legalidad en las prácticas de ciberseguridad, así como las responsabilidades de los profesionales en este campo.

Además, se explora la simulación de ataques, la identificación de vulnerabilidades y las medidas de prevención y respuesta ante incidentes de seguridad.

El documento destaca la importancia de la colaboración entre los equipos Red Team y Blue Team, el uso de herramientas especializadas y el cumplimiento de las normativas vigentes para garantizar la seguridad en el entorno digital.

***Palabras clave*:** BlueTeam, Ciberseguridad, Legislación, Pentesting, RedTeam

.

Abstract

The report details the strategies of the Red Team and Blue Team at CyberFort Technologies, covering everything from basic concepts to the execution of penetration testing and the containment of attacks.

Aspects such as Colombian legislation on cybercrime, the pentesting process, cybersecurity tools, and the configuration of work environments are analyzed.

The ethics and legality of cybersecurity practices are also discussed, as well as the responsibilities of professionals in this field.

Furthermore, the simulation of attacks, the identification of vulnerabilities, and prevention and response measures for security incidents are explored.

The document highlights the importance of collaboration between the Red Team and Blue Team, the use of specialized tools, and compliance with current regulations to ensure security in the digital environment

***Keywords*:** BlueTeam, Cybersecurity, Legislation, Pentesting, RedTeam

Tabla de contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Acuerdo de Confidencialidad: Contrato que obliga a una o ambas partes a mantener en secreto cierta información.

Aislamiento de sistemas: Acción de desconectar o segregar un sistema comprometido de la red para prevenir la propagación de un ataque.

Análisis de registros: Proceso de examinar detalladamente los archivos que documentan la actividad de sistemas y aplicaciones para detectar anomalías o incidentes.

Aplicación vulnerable: Software con fallos de seguridad que pueden ser explotados.

Ataque en tiempo real: Agresión cibernética que se desarrolla y ejecuta de manera inmediata, requiriendo una respuesta simultánea.

Blue Team: Equipo de seguridad encargado de la defensa proactiva de los sistemas de una organización, implementando medidas preventivas contra ataques.

Ciberdelincuencia: Actividades ilícitas que se llevan a cabo en el entorno digital.

Ciberespionaje: Acceso no autorizado a datos confidenciales en sistemas de información.

Ciberseguridad: Prácticas y tecnologías diseñadas para proteger sistemas informáticos y datos de ataques cibernéticos.

Controles CIS: Conjunto de prácticas y directrices de seguridad informática ampliamente reconocidas, diseñadas para establecer una base de seguridad efectiva.

COPNIA: Consejo Profesional Nacional de Ingeniería.

CVE (Common Vulnerabilities and Exposures): Sistema para identificar, definir y nombrar vulnerabilidades de seguridad.

Datos personales: Información vinculada a una persona natural determinada o determinable.

Equipo de Respuesta a Incidentes (IR): Grupo especializado responsable de identificar, contener, erradicar y recuperarse de incidentes de seguridad.

Escalada de privilegios: Proceso de obtener derechos de acceso superiores a los inicialmente concedidos en un sistema.

Exploit: Fragmento de código o técnica que aprovecha una vulnerabilidad en un sistema para ejecutar acciones no autorizadas.

Falla de seguridad: Vulnerabilidad o error en un sistema que puede ser aprovechado para comprometer su seguridad.

Fuga de información: Divulgación no autorizada de datos confidenciales a individuos o entidades no autorizadas.

Hacking Ético: Práctica de utilizar técnicas de hacking con fines defensivos y legales.

Hardenización: Proceso de asegurar un sistema o aplicación mediante la configuración de sus defensas, como parches y filtrado de puertos, especialmente después de un incidente.

Ley 1273 de 2009: Conocida como la Ley de Delitos Informáticos que protege la información y los datos personales de los ciudadanos**.**

Ley 1581 de 2012: Ley que establece el régimen general de protección de datos personales.

Payload: Parte de un exploit que realiza la acción maliciosa.

Pentesting: Proceso de evaluar la seguridad de un sistema informático simulando ataques.

Red Team: Equipo de ciberseguridad que simula ataques a los sistemas de una organización para identificar vulnerabilidades.

SIEM: Sistema que centraliza y analiza registros de diversas fuentes para correlacionar eventos, generar alertas de seguridad y facilitar la investigación forense.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada por una amenaza.

Introducción

Este trabajo detalla las etapas y consideraciones clave en la ciberseguridad, enfocándose en las estrategias y acciones de los equipos Red Team y Blue Team. Inicialmente, se establecen los conceptos fundamentales, el marco legal colombiano sobre delitos informáticos y la configuración de entornos de trabajo para pruebas de penetración.

Se profundiza en la importancia de la ética y la legalidad en las actividades de ciberseguridad, analizando escenarios de riesgo, acuerdos de confidencialidad y el rol de los profesionales en la protección de la información.

Posteriormente, se aborda la ejecución de pruebas de intrusión, simulando ataques para identificar vulnerabilidades en sistemas Windows, y se explica el proceso de escalamiento de privilegios y la demostración de pruebas de concepto.

Finalmente, se examinan las estrategias de contención de ataques informáticos en tiempo real, el análisis de registros, el aislamiento de sistemas y las funciones de los equipos Blue Team y de respuesta a incidentes, así como el uso de herramientas SIEM y los controles CIS para fortalecer la postura de seguridad.

Justificación

El presente trabajo se justifica en la necesidad de proporcionar una comprensión integral y aplicada de las estrategias de los equipos Red Team y Blue Team en el ámbito de la ciberseguridad, abordando tanto los fundamentos teóricos como las habilidades prácticas esenciales para la protección de la información y los sistemas.

Se reconoce la importancia de analizar el marco legal y ético que rige las actividades de ciberseguridad en Colombia, así como de comprender los procesos de pruebas de penetración y el uso de herramientas especializadas para la identificación y explotación de vulnerabilidades.

Además, se justifica la necesidad de desarrollar habilidades para la contención de ataques informáticos en tiempo real, el análisis de registros y la implementación de medidas de "hardenización" para fortalecer la postura de seguridad de las organizaciones.

En última instancia, esta guía busca formar profesionales de la ciberseguridad altamente capacitados y éticamente responsables, capaces de enfrentar los desafíos del panorama digital actual y contribuir a la protección de los activos de información de las organizaciones.

Objetivos

Objetivo General

Analizar las estrategias y acciones de los equipos Red Team y Blue Team en el ámbito de la ciberseguridad, considerando los aspectos legales, éticos y técnicos involucrados en la identificación, explotación y contención de amenazas informáticas.

Objetivos Específicos

Evaluar el marco legal que regula las actividades de ciberseguridad en Colombia, incluyendo la legislación sobre delitos informáticos y protección de datos personales; por otro lado, los procesos y herramientas utilizados en las pruebas de penetración (pentesting).

Establecer el marco ético de los acuerdos y contratos relacionados con la ciberseguridad, así como los principios éticos que deben guiar la conducta de los profesionales del área.

Investigar una fuga de información en un equipo Windows de la organización, identificando la vulnerabilidad explotada y demostrando la escalada de privilegios mediante la creación de un usuario administrador.

Analizar los aspectos críticos de la ciberseguridad, incluyendo la contención de ataques, estrategias de prevención y respuesta, la función de los equipos Blue Team y de Respuesta a Incidentes, el valor de los Controles CIS, la importancia de los sistemas SIEM, las medidas de "hardenización" y la relevancia de la informática forense.

Capítulo 1 Objetivo específico 1

Marco legal que regula las actividades de ciberseguridad en Colombia

Ley 1273 de 2009 (Función Pública, 2009)

Delitos relacionados con la tecnología, que busca la protección de la información, los datos y los sistemas informáticos. Define castigos, como penas de cárcel y multas, para quienes cometan estos delitos.

Entre algunos de los delitos se encuentran:

> El acceso no autorizado a sistemas informáticos, con o sin medidas de seguridad (Artículo 269a).
>
> La obstrucción del funcionamiento normal de los sistemas informáticos, datos o redes de telecomunicaciones. (Artículo 269b).
>
> Algunos escenarios en las que las penas por estos delitos se agravan son cuando se cometen contra sistemas del gobierno o del sector financiero, por funcionarios públicos, abuso de confianza, revelando información confidencial, con fines terroristas o por personas encargadas de la administración de la información (Artículo 269H).

Ley 1581 de 2012 (Función Pública, 2012)

Regula el derecho de las personas a conocer, actualizar y corregir la información personal recopilada sobre ellas en bases de datos o archivos.

Principios para el tratamiento de datos personales, conteniendo la seguridad de la información (alteraciones, pérdidas, accesos no autorizados, entre otros) y confidencialidad (reserva de la información, incluso terminada la relación con el tratamiento de los datos).

Sanciones que la Superintendencia de Industria y Comercio puede imponer por el incumplimiento de esta ley (multas, suspensión de actividades y cierre temporal de operaciones).

Ley 1621 de 2013 (Función Pública, 2013)

Define la acción de los organismos del Estado para la recolección, procesamiento, análisis y difusión de información, para la protección de los derechos, prevención y combatir las amenazas contra la seguridad nacional, entre otros.

Regulación del monitoreo del espectro y la interceptación de comunicaciones privadas, siguiendo los requisitos de la Constitución y el Código de Procedimiento Penal.

Solicitar la colaboración de entidades públicas y privadas con organismos de inteligencia.

En resumen, se puede inferir que la evolución regulatoria en ciberseguridad en Colombia ha sido objeto de un análisis profundo que sigue en desarrollo (Jiménez-Almeira & López, 2023).

Proceso de pruebas de penetración, etapas y herramientas

Etapa I - Planeación

Entrega de información inicial para delimitación en la obtención de pruebas, acuerdo firmado entre el experto en seguridad informática y la organización, definición de grupo de trabajo, cronograma, rutas de escalamientos, reuniones abiertas, entre otros. El método escogido es de acuerdo con el tipo de análisis. Área de Innovación y Desarrollo. (2018).

Caja Negra. Análisis de los resultados de ejecución de herramientas en la investigación de vulnerabilidades, no se conoce el funcionamiento interno del objetivo.

Caja Blanca. Estudio con conocimiento del objetivo en búsqueda de vulnerabilidades, examinándolo por medio del ciclo de desarrollo del Software (SDLC) combinado con las normas de la familia ISO 27000, entre otros.

Caja Gris. Combinación de los dos anteriores tipos de análisis.

Las actividades por realizar en esta fase son:

- Lectura de documentación teórica-técnica y clasificación de información de la empresa, presentación de documentos y toma de decisiones.
- Instalación y configuración de máquina virtual, servidores necesarios y herramientas.

Herramienta por utilizar.

Kali Linux. Es un sistema operativo adaptable a los diferentes enfoques de las pruebas de penetración, puede combinar técnicas de caja negra y caja blanca de tal forma que se puede tener un contexto completo de la seguridad de un sistema. Se puede

combinar con herramientas de hardware como: Pineapple, Rubber Ducky, Lan Turtle, entre otros.

Etapa II - Evaluación

Recolección de Información. Búsqueda de información de determinada organización y/o individuo, motores de búsqueda, emails, redes sociales, documentos internos o públicos y registro de ingreso, visitas, entre otros.

Se identifican los elementos más sensibles:

Para empresas. Nombre, empleados, rol, datos de contacto, proveedores tecnológicos y de negocio (tecnologías usadas, localización, plataformas).

Para personas. Presencia en la web (dominios, e-mails, números de teléfono) y ubicaciones físicas (oficinas, centros de datos, almacenes).

Herramienta por utilizar.

Maltego. Herramienta de fuentes abiertas (OSINT) y análisis forense, que recopila y muestra información desde diversas fuentes públicas como registros DNS, redes sociales, bases de datos de direcciones IP, entre otros.

Mapeo de la Red. Diseñar un mapeo de red del objetivo, el cual consiste en acceder sin autorización para: encontrar equipos (routers, firewall), puertos, servicios, aplicativos, software y versiones.

Herramienta por utilizar.

Nmap. Conocida como la navaja suiza de los pentesters, permite el escaneo en un rango de direcciones IP para la identificación de servicios, detección de sistema operativo, puertos, entre otros.

Identificación de vulnerabilidades. Determinación de vulnerabilidades y en concordancia con la información de los 2 puntos previos, posteriormente correlacionar las mismas y enumerarlas para encaminar un ataque.

Herramienta por utilizar.

Nessus. Escáner de vulnerabilidades que cuenta con un amplio tablero de control que facilita la identificación de debilidades en sistemas y aplicaciones.

Intrusión. Evasión de controles de seguridad y escalamiento de privilegios, mediante pruebas y obteniendo puntos de acceso sin autorización, verificándolos y probándolos.

Herramienta por utilizar.

Metasploit. Framework que cuenta con exploits para distintas vulnerabilidades, por medio de la cual se podría ganar el acceso a cuentas de usuario (combinaciones de user/password, ataques de diccionario, fuerza bruta,) explotando configuraciones por defecto de fabricantes, visualización del comportamiento de

usuarios y/o sitios remotos para tener el acceso con privilegios en red interna, ocultación de archivos y borrado de logs del sistema, entre otros.

Etapa III. Presentación de informes

Se exponen las vulnerabilidades encontradas de acuerdo con su criticidad de tal forma que la organización cuente con: resumen de gestión, alcance del estudio, herramientas utilizadas, fechas y tiempos, resultados de pruebas efectuadas y recomendaciones, todo lo anterior para mejorar la reproducibilidad y el entretenimiento en los ejercicios de ciberseguridad (Besson et al., 2023).

Herramienta por utilizar.

Dradis CE (Community Edition). Framework para la generación de informes durante el pentesting, para organizar y documentar las evidencias mediante el trabajo en colaboración de varias personas, así como la integración con herramientas como Nmap y Nessus.

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. A continuación, se definen y explican las siguientes herramientas:

Metasploit. Framework usado tanto por los Red Teams como Blue Teams, permite crear software malicioso en diversidad formatos a través del módulo ENCODERS, como payloads, para el despliegue en otros sistemas.

Cuando se cuenta con conocimientos en Scripting, la ejecución, bien sea por acción del usuario o de un proceso, puede evadir el antivirus.

Algunos otros módulos y funcionalidades que implementan son:

Auxiliares (auxiliary): Funciones para ejecución sobre un equipo como inicio de sesión, escáner de puertos, herramientas de denegación de servicios, fuzzers, entre otros.

De explotación (exploits): Procedimientos que por medio de payloads se toma el control de un equipo.

Generadores de no operación (nops): Código capaz de generar instrucciones NOP40 para los códigos maliciosos.

De post-explotación (post): Acciones que permiten el mantenimiento del acceso, escalamiento de privilegios, pruebas sobre la máquina, entre otras, cuando ya se ha alcanzado la explotación.

Nmap. A través de la escritura de comandos, ejecutados en paralelo, se logra la automatización para su uso.

Escanear varios objetivos: -nmap target1,target2,etc

Escanear un fichero con hosts: -nmap iL [list.txt]

Escanear una subred completa: -nmap host/máscara

OpenVas. Framework con diferentes de servicios y herramientas para el escaneo y gestión de vulnerabilidades. Entre sus características principales se encuentran:

- ✓ Usa una base de datos actualizada de pruebas de vulnerabilidad (NVTs) con el fin de identificar fallas de seguridad conocidas.

- ✓ Provee informes detallados de vulnerabilidades y recomendaciones para su corrección.
- ✓ OpenVAS es un software de código abierto, lo que significa que es gratuito y puede ser modificado y adaptado a las necesidades específicas de cada usuario.

Servicios en línea.

ExploitDB. Es una plataforma online que opera como un repositorio público, con exploits para fallos de seguridad conocidos, estos códigos son aportados por la comunidad y disponibles gratuitamente para interesados en la seguridad informática, permitiendo la ejecución de pruebas de penetración de acuerdo con el enfoque en que se esté orientando.

CVE (Common Vulnerabilities and Exposures). Es un sistema de identificación de vulnerabilidades de seguridad informática. Cuenta con una lista de registros, en donde cada uno de ellos contiene los detalles de una vulnerabilidad.

Funciona como un estándar en la manera que se informan y comparten la información de vulnerabilidades entre distintas herramientas, bases de datos y organizaciones.

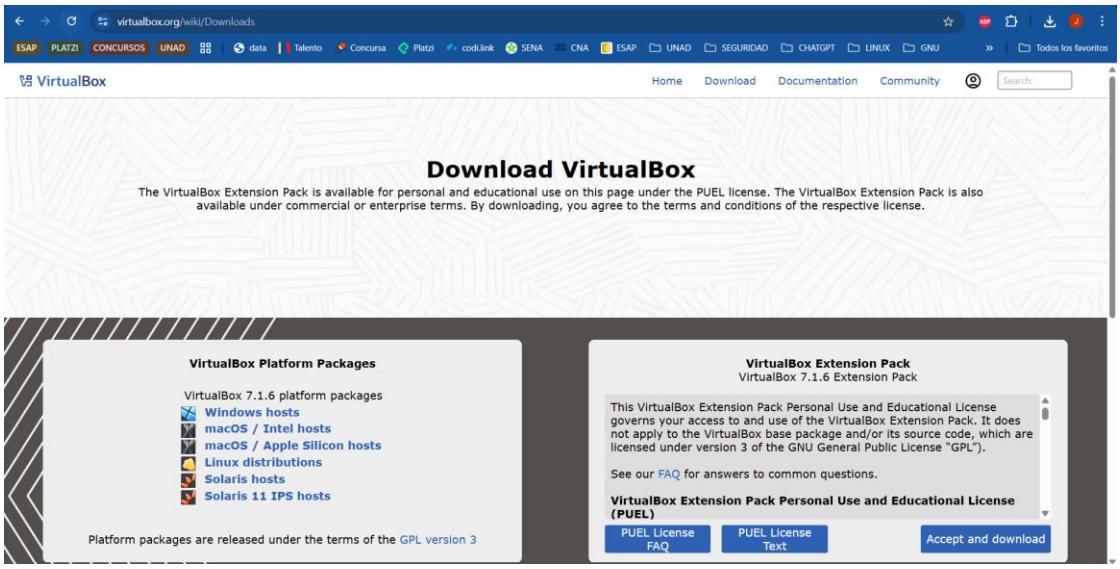
Cada vulnerabilidad y exposición tiene un identificador CVE único. El formato es CVE-YYYY-NNNN, donde YYYY es el año en que se publicó y NNNN es un número secuencial.

Configuración del Banco de Trabajo

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

Figura 1

Descarga VirtualBox y Extension Pack desde de la Página Web Oficial

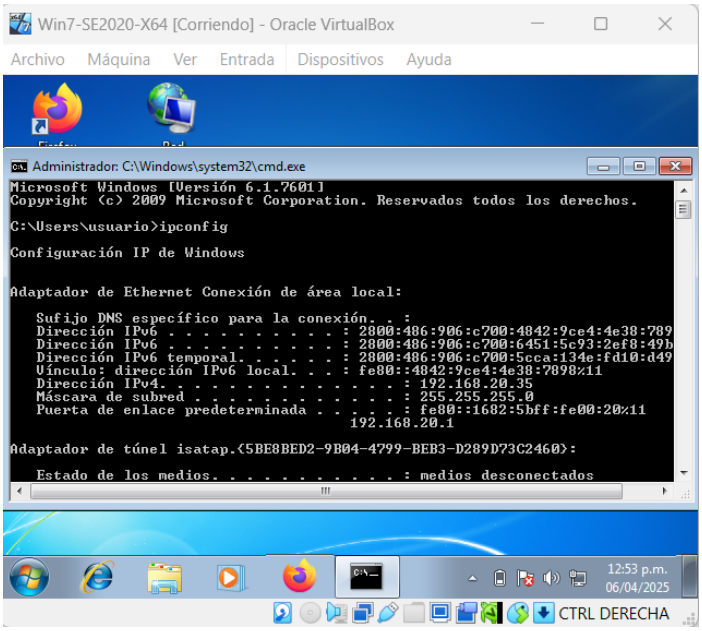


Fuente. VirtualBox (2025). Sitio Web oficial Virtualbox.org. Tomado de https://www.virtualbox.org/wiki/Downloads

Paso B. Una vez se realice apertura del foro para el desarrollo de la actividad ingrese al enlace: RedTeam&BuleTeam2024, el cual contiene lo requerido para el montaje del banco de trabajo, las imágenes en formato *.OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un sistema operativo windows y un sistema operativo Kali Linux.

Figura 2

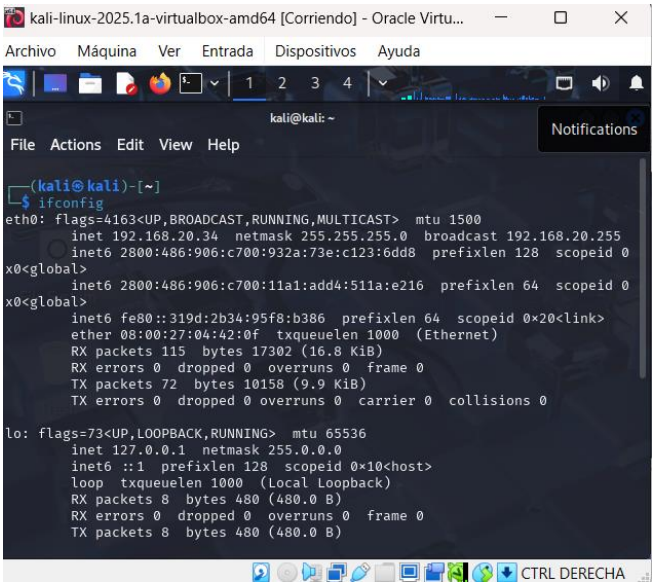
Máquina Virtual de Windows 7 iniciada



Fuente. Creada por el autor

Figura 3

Máquina Virtual de Kali Linux iniciada

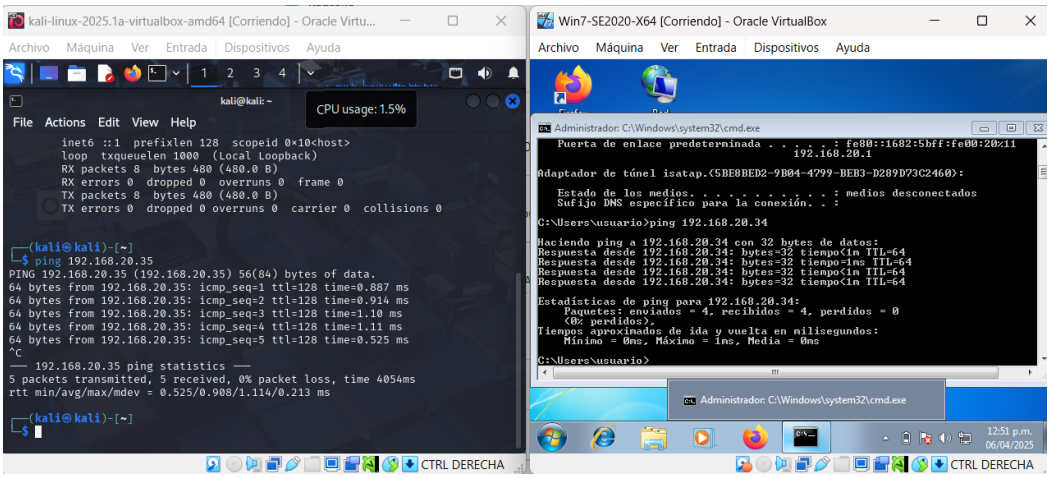


Fuente. Creada por el autor

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

Figura 4

Validación de comunicación entre máquinas virtuales iniciadas

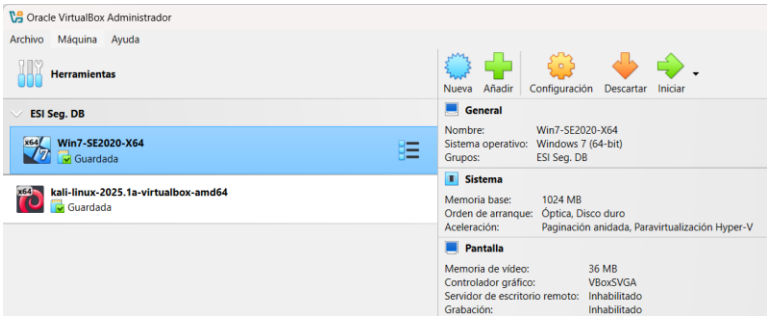


Fuente. Creada por el autor

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

Figura 5

Montaje del banco de Trabajo



Fuente. Creada por el autor

Características técnicas de hardware de la Máquina Virtual con Kali Linux

Nombre. kali-linux-2025.1a-virtualbox-amd64

Sistema operativo. Debian (64-bit)

Memoria base. 2048 MB

Procesadores. 2

Orden de arranque. Disco duro, Óptica

Aceleración. Paginación anidada, PAE/NX, Paravirtualización KVM

Memoria de vídeo. 128 MB

Servidor de escritorio remoto. Inhabilitado

Dispositivo IDE secundario 0. [Unidad óptica] Vacío

Puerto SATA 0. kali-linux-2025.1a-virtualbox-amd64.vdi (Normal, 80,09 GB)

Adaptador 1. Intel PRO/1000 MT Desktop (Adaptador puente, «Realtek PCIe GbE Family Controller»)

Características técnicas de hardware de la Máquina Virtual con Windows 7

Nombre. Win7-SE2020-X64

Sistema operativo. Windows 7 (64-bit)

Grupos. ESI Seg. DB

Memoria base. 1024 MB

Orden de arranque. Óptica, Disco duro

Aceleración. Paginación anidada, Paravirtualización Hyper-V

Memoria de vídeo. 36 MB

Servidor de escritorio remoto. Inhabilitado

Grabación. Inhabilitado

Puerto SATA 0. Win7-SE2020-X64-disk001.vdi (Normal, 50,00 GB)

Adaptador 1. Intel PRO/1000 MT Desktop (Adaptador puente, «Realtek PCIe GbE Family Controller»)

Capítulo 2 Objetivo específico 2

Legalidad y ética de los acuerdos y contratos relacionados con la ciberseguridad

Las evidencias de algunos procesos ilegales y no éticos que se estipularon en acuerdos de contratos suministrados como ejemplo, muestran algunos procesos ilegales y no éticos como:

Ejecución de contratos por parte de un abogado que fue despedido al ser sorprendido en procesos ilegales, sin haber hecho una revisión de los documentos elaborados incluyendo los acuerdos de confidencialidad, dada la premura en la inclusión de los equipos Red & Blue, además de dejar a discreción de los interesados en acceder en la contratación la firma de dicha documentación.

La competencia del trabajo bajo presión bajo las condiciones del ítem anterior puede inducir al error, sugiriendo mala fe por parte de la organización.

La información de un contrato no debe ser confidencial, a nivel público la información de un contrato debe ser publicada de forma transparente, así como la no divulgación de procesos ilegales.

Estas irregularidades están centradas en la intención de la empresa de eludir responsabilidades legales, silenciando a los empleados a cerca de actividades ilícitas y definiciones confusas de "información confidencial".

Se destacan algunos fragmentos específicos del acuerdo:

Ambigüedad en el concepto de "Información Confidencial"

> **Fragmento (Cláusula Segunda, numeral 2).** *"...datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos..."*
>
> Datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos, definidos como "información confidencial" es cuestionable éticamente, la información sobre la empresa puede ser legítimamente confidencial, pero la inclusión de actividades ilegales infiere que la organización podría estar involucrada en ellas y busca protegerse a través de un acuerdo.

Obligación de la no denuncia de actividades ilegales

> **Fragmento (Cláusula Cuarta, numeral 3).** *"...No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros..."*
>
> Es deber de los ciudadanos colombianos denunciar los delitos. Estipular que un empleado no denuncie las actividades como por ejemplo un espionaje, va en contra del orden justo, adicionalmente que va en contra de los principios éticos de transparencia y legalidad, fundamentales en las relaciones laborales y empresariales.

Prohibir denunciar y publicar información Ilegal

Fragmento (Cláusula Cuarta, numeral 4). *"…Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas…"*

No se debe imponer a una persona la obligación de mantener silencio sobre la comisión de delitos. Esto induce a la impunidad y facilita la ocurrencia de actividades ilícitas dentro de la organización.

Exención de responsabilidades empresariales

Fragmento (Cláusula Octava). *"…Las partes se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies..."*

Abuso al sugerir medios alternativos no claros que puedan ser actos de corrupción, a través de algún tipo de dádiva, además de intentar eximir a CyberFort de su responsabilidad legal y penal en caso de que se maneje información ilegal, atentando a los principios de equidad y justicia.

Por otro lado, algunos artículos de la ley 1273 (Función Pública, 2009) vulnerados en los acuerdos son:

En Cláusula Segunda, numeral 2. presunta vulneración en datos secretos como 'datos de chuzadas (269F), interceptación de información (269C), accesos abusivos a sistemas informáticos (269A).

Artículo 269F. Violación de datos personales. al clasificar la información sobre "chuzadas" como confidencial, podría estar intentando proteger la divulgación de acciones a la referencia de este artículo.

Artículo 269C. Interceptación de datos informáticos. sin una orden judicial es un delito, no se puede legitimar una actividad ilegal enmascarándola como "confidencial", adicionalmente si la organización ejecuta esta tarea y prohíbe al empleado revelar esa información, está obstaculizando la aplicación de la ley.

Artículo 269A. Acceso abusivo a un sistema informático. Si la empresa realiza interceptación de información y el acuerdo impide la denuncia, se estaría entorpeciendo la aplicación de la ley.

En Cláusula Octava. mecanismos alternativos (269H Numeral 5) de solución de conflictos cualquier diferencia (269H Numeral 7) que surja con motivo de la ejecución del

presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies (269H Numeral 3,8).

> ***Artículo 269H. Circunstancias de agravación punitiva.*** aumento de la pena por presunto:
>
> - *Numeral 5:* El uso de mecanismos alternativos podrían ser prebendas para obtener provecho por parte del empleado o un tercero como el abogado privado y la misma organización.
>
> - *Numeral 7:* Atento contra la buena fé del empleado siendo instrumentalizado, aludiendo la resolución ante cualquier tipo de problema en ejecución del contrato.

Numeral 3 y 8: Aprovechamiento de la confianza depositada tanto en la organización como en el empleado, así como responsables de la administración y control de la información.

Alienando el código de ética del COPNIA para ingenieros, se puede completar la argumentación brindada con la existencia de procesos poco confiables en el contrato

No sería ético aceptar un trabajo en CyberFort Technologies, a pesar del salario alto y el contrato vitalicio. Esta decisión la argumento en el Código de Ética, COPNIA. (s.f.):

Artículo 31 del Código de Ética, violación de los deberes y obligaciones profesionales, en literales b y f. dónde trabajar para una empresa que promueve la no denuncia de actividades ilegales (evidenciado en el acuerdo) implica el fallo a este deber, al servirse ocultar información relevante para la justicia.

El Artículo 32, literal b. al laborar para una organización que busca encubrir delitos informáticos, constituiría en cierta forma la tolerancia a dichas actividades. Además, los literales c y j, dónde al intentar resolver mediante los “mecanismos alternativos”, puede ser considerado como una posible dádiva; por otro lado, si bien es cierto, es menos directo, el salario alto y el contrato vitalicio podrían interpretarse a modo de un "beneficio injustificado" que induciría al profesional a pasar por alto irregularidades éticas y legales.

El Artículo 53, literal e. podría considerarse como falta gravísima, dónde el profesional se involucre en encubriendo los delitos de CyberFort Technologies, atentando contra clientes de la empresa y autoridades del sector.

De acuerdo con las implicaciones legales y éticas generadas en el contrato, se pueden responder los siguientes interrogantes.

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

La ejecución de una auditoría de seguridad implica generalmente el acceso a información sensible de sus clientes con el fin de evaluar exhaustivamente vulnerabilidades. Sin embargo, este acceso debe estar restringido a lo necesario y con un manejo de máxima confidencialidad, para generar un equilibrio entre la necesidad de acceso a información sensible y la protección de los intereses y privacidad del cliente.

***Límites al acceso de información sensible*.**

Necesidad. Acceso a la información que sea estrictamente necesaria en cumplimiento con los objetivos de la auditoría.

Alcance. El alcance del acceso debe ser lo suficientemente claro en el acuerdo de servicio, especificando en detalle qué tipo de información se accederá, sistemas qué se examinarán y actividades que se realizarán.

Consentimiento Informado. Los clientes deben comprender claramente qué información se accederá, el por qué, cómo se utilizará y protegerá.

Minimización de Información. Implementación de medidas para minimizar la cantidad de información a la que se accede, por ejemplo, uso de técnicas de anonimización o seudonimización, también limitación del acceso a sistemas o bases de datos.

Uso Adecuado del Acceso.

Acuerdos de confidencialidad. Acuerdos legalmente vinculantes entre la empresa auditora y sus empleados, así como con el cliente, también la definición detallada

de qué es considerado como información confidencial, cómo debe ser protegida y las consecuencias de una fuga.

Controles de acceso estrictos. Controles que limiten quién dentro de la empresa puede acceder a la información del cliente, bajo el principio del mínimo privilegio, entregando a sus empleados únicamente permisos de acuerdo con el rol para la ejecución de sus actividades.

Supervisión. Las tareas del equipo auditor deben ser supervisadas desde el nivel central, para hacer cumplir los límites en el acceso a la información del cliente en concordancia con los acuerdos establecidos con el mismo.

Procesos y procedimientos internos. Internamente la empresa auditora debe contar con políticas y procedimientos detallados sobre el manejo de la información de los clientes, en lo que respecta a la recopilación, almacenamiento, uso, transferencia y eliminación de datos.

Ética. Los auditores deben recibir capacitación periódicamente en ética profesional, confidencialidad y protección de datos, recalcando la importancia de la confianza del cliente y las consecuencias de las violaciones éticas y legales.

Transparencia. Transparencia con el cliente sobre las tareas ejecutadas, informarle sobre cualquier hallazgo importante e incidentes ocurridos.

Responsabilidad. La organización auditora deberá asumir responsabilidades por cualquier uso indebido o no autorizado de la información del cliente, establecimiento de mecanismos para abordar PQRS con resolución justa y oportuna.

¿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?.

Tomando como apoyo la Ley 1581 de 2012, (Función Pública, 2012)**,** CONPES 3995, Departamento Nacional de Planeación (2020), y los controles CIS en su versión 8, Center for Internet Security. (2021, Mayo), en aras de prevenir el uso indebido de herramientas de análisis forense, las empresas de ciberseguridad deben implementar componentes de supervisión y control con aspectos éticos y de gestión:

Controles de Acceso y Auditoría.

Acceso basado en roles y privilegios mínimos. Ejecución de sistemas de control dónde cada empleado tenga acceso únicamente a las herramientas de análisis forense y datos necesarios para su función.

Autenticación multifactor (MFA). MFA requerido para el acceso a aplicaciones forenses, específicamente aquellas con capacidades de impacto alto, logrando añadir una capa más de seguridad y mitigando el riesgo de acceso no autorizado.

Auditoría de accesos. Registro detallado de quién accede a qué herramientas e información, marca de tiempo y qué acciones se efectuaron. Estos registros deben ser revisados con periodicidad alta para detectar anomalías o tareas sospechosas.

Políticas con procesos y procedimientos detallados.

Política de uso aceptable (PUA o AUP). Uso aceptable de las herramientas, qué acciones están permitidas y las consecuencias de violaciones a lo prohibido.

Procedimientos operativos estándar (POE). POE detallados para las actividades de ciberseguridad y en auditorías forenses, esto engloba la cadena de custodia de la evidencia, manejo de datos sensibles y protocolos de comunicación.

Minimización de información. Recopilación y análisis solo de los datos absolutamente necesarios para las investigaciones, evitando la recopilación de información irrelevante o excesiva. Esto se alinea con parte de los principios de la Ley 1581 de 2012, a cerca de la protección de datos personales.

Supervisión y Capacitación.

Supervisión constante. En tareas de alto impacto y en espacial para investigaciones forenses, el monitoreo en tiempo real es válido para la identificación de comportamientos inusuales.

Retroalimentación de actividades. La ejecución de actividades de retroalimentación para la revisión de los procedimientos seguidos y el cumplimiento de las políticas, con apoyo de control interno, deben ser independientes y objetivas.

Supervisión de proveedores. El contrato de proveedores y aplicaciones para investigaciones forenses, deben ser estrictamente supervisados y alineados con el cumplimiento de los mismos estándares éticos y legales que la organización.

Responsabilidad. Definir claramente una cadena de responsabilidad, quién es responsable de qué acciones y quién supervisa el uso de las herramientas forenses.

Actualización Legal. Estar día a día con las mejores prácticas y cambios en la legislación, en lo que respecta a protección de datos y delitos informáticos.

Capacitación en ética. Formación continua a los empleados sobre principios éticos en la ciberseguridad, importancia de la privacidad y consecuencias en el uso indebido de aplicaciones en las acciones que ejecuten. Adicionalmente la adopción de un código de conducta que defina los valores y principios éticos (incluido el respeto por la privacidad) que deben guiar el comportamiento de los empleados.

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

Cuando un gobierno u organización descubre que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje, se deben tomar medidas como:

Contención.

Investigación. Investigación interna y externa con el fin de determinar el alcance del ciberespionaje, identificar responsables y evaluar las afectaciones.

Aislamiento. Aislar los sistemas y datos afectados para prevenir una mayor filtración de información y preservar la evidencia.

Notificación a las autoridades. Informar a las autoridades competentes, iniciando un proceso legal.

Sanciones.

Acciones legales. Iniciar acciones legales contra la empresa de ciberseguridad y sus responsables, buscando compensación por daños causados.

Sanciones contractuales. Aplicar las sanciones estipuladas en el contrato y remuneración económica por las afectaciones.

Inhabilitación. Considerar la inhabilitación de la empresa para futuros contratos

Remediación.

Auditoría de seguridad. Ejecutar una auditoría de seguridad completa de los sistemas para identificar y corregir vulnerabilidades.

Fortalecimiento de la seguridad. Implementar medidas de seguridad adicionales, siguiendo marcos como los Controles CIS, para la prevención de futuras intrusiones.

Revisión de políticas. Actualizar las políticas y procedimientos de seguridad para incluir lecciones aprendidas y prevenir incidentes.

Entre las medidas para la restauración de la confianza y prevenir sucesos similares.

Rendición de cuentas para comunicar con transparencia las acciones tomadas y resultados de la investigación.

Ofrecer compensación a las partes afectadas.

Compartir lecciones aprendidas y mejores prácticas con entre organizaciones para la prevención de incidentes análogos**.**

Revisión de los procesos de selección y contratación de los proveedores, verificando su reputación.

Contratos robustos con acuerdos contractuales detallados que definan el alcance, responsabilidades y acciones legales ante incumplimientos.

Implementar supervisión y auditoría externas para verificar el cumplimiento de los proveedores.

Capítulo 3 Objetivo específico 3

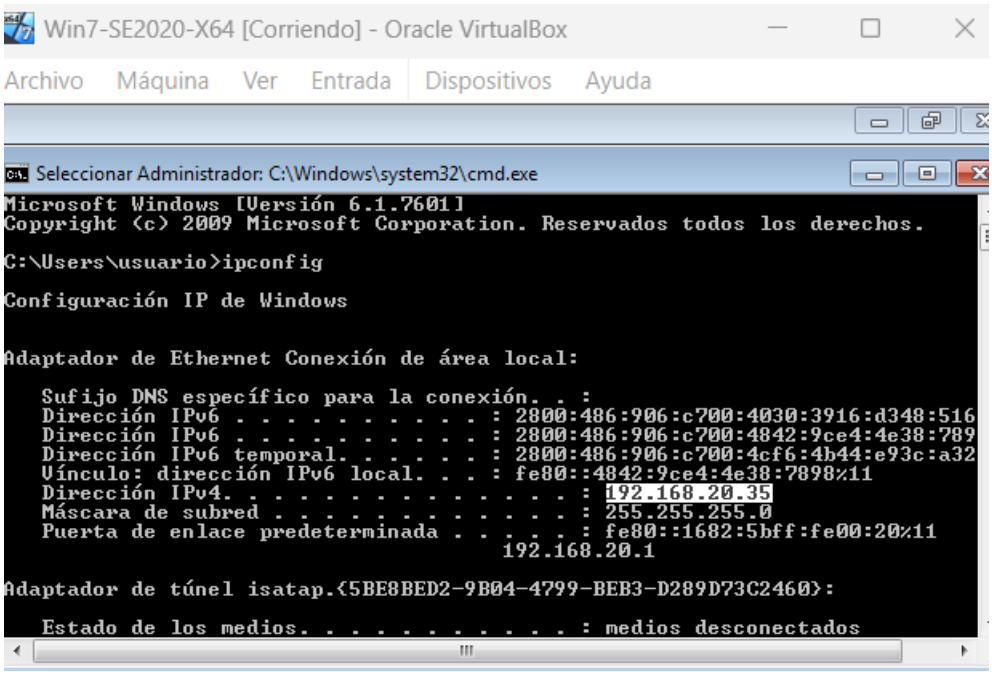
Documentación de comandos y resultados obtenidos de acuerdo con el análisis de una fuga de información en un equipo Windows

Reconocimiento

Paso A. Se valida la dirección ip de la máquina objetivo anexo 4 – escenario 3.

Figura 6

Máquina objetivo del anexo 4 – escenario 3



Nota. Creada por el autor

Paso B. A través del sistema operativo Kali Linux se ejecutó la herramienta Nmap para realizar el reconocimiento de la red e identificación de la máquina objetivo:

Figura 7

Reconocimiento de la red e identificación de la máquina objetivo

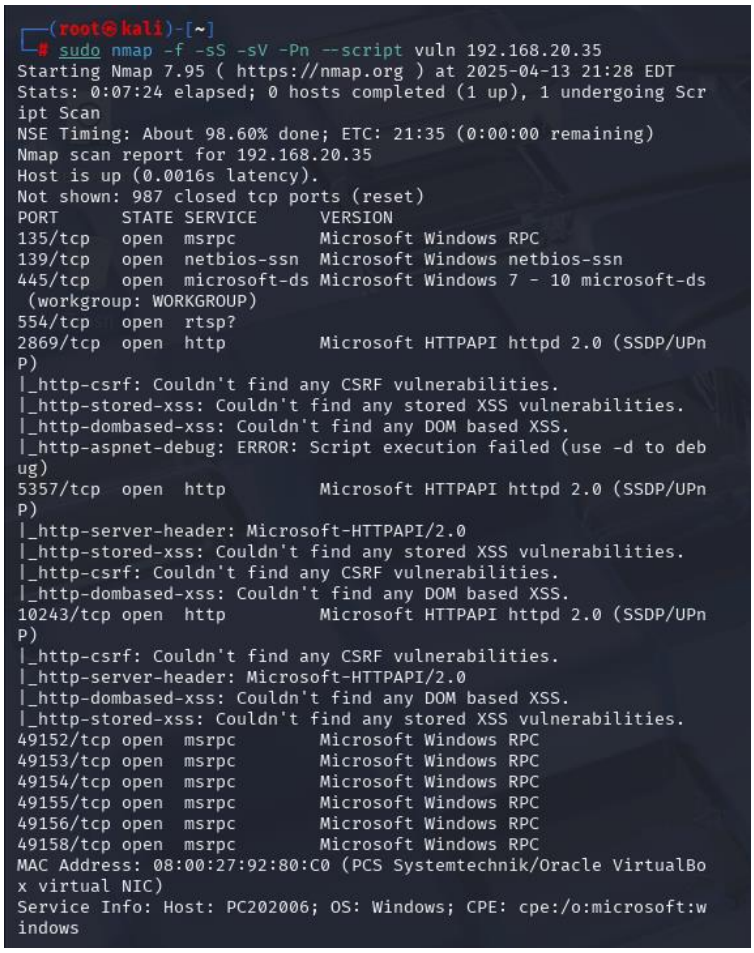
Nota. Creada por el autor

Se pueden visualizar puertos, servicios, estados y versiones de los sistemas operativos de los equipos conectados a la red, identificando la máquina objetivo del anexo 4 – escenario 3.

Paso C. Con el fin de identificar las vulnerabilidades de la máquina objetivo, se ejecuta, desde el super usuario, el comando de la aplicación de Nmap en el terminal de Kali Linux apuntando a la ip de la misma:

Figura 8

Identificación de vulnerabilidades con Nmap



Nota. Creada por el autor

Comando: sudo nmap -f -sS -sV -Pn --script vuln 192.168.20.35

-f: Fragmenta los paquetes de escaneo en partes más pequeñas para tratar de evadir IDS o firewall que bloquean paquetes de gran tamaño.

-sS: SYN Scan (Half-Open Scan). Tipo de escaneo sigiloso.

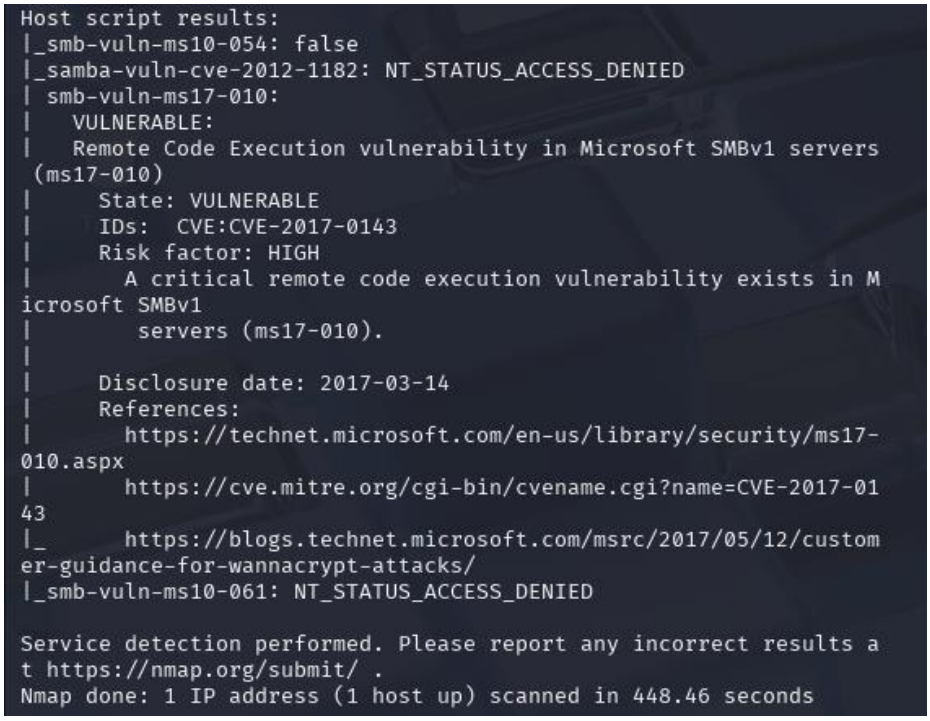
-sV: Determina la versión de los servicios que están ejecutándose.

-Pn: Cuando se ejecuta el escaneo, generalmente Nmap envía pings para definir si el objetivo se encuentra activo, al adicionar este parámetro a la instrucción, esta tarea inicial se desactiva.

--script vuln: Conjunto de secuencia de comandos NSE (Nmap Scripting Engine) para la búsqueda de vulnerabilidades comunes:

Figura 9

Resultados de vulnerabilidades encontradas



Nota. Creada por el autor

Explotación

Paso D. Desde el sistema operativo Kali Linux, en el terminal de superusuario se ejecuta la herramienta Metasploit Framework:

Figura 10

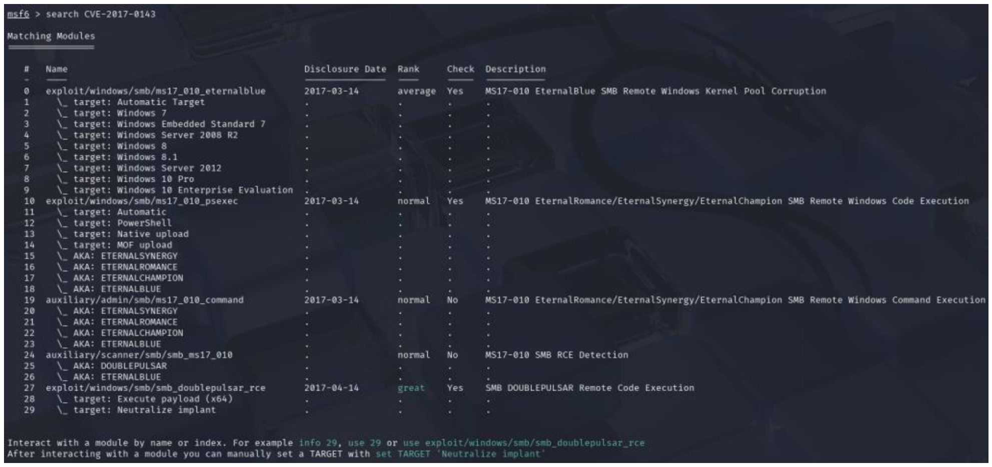
Metasploit Framework

Nota. Creada por el autor

Paso E. Con la instrucción search se realiza la búsqueda de la vulnerabilidad hallada en el paso C y validar la existencia de módulos que permitan explotarla. Entre las opciones, se selecciona la primera (0):

Figura 11

Instrucción search CVE-2017-0143

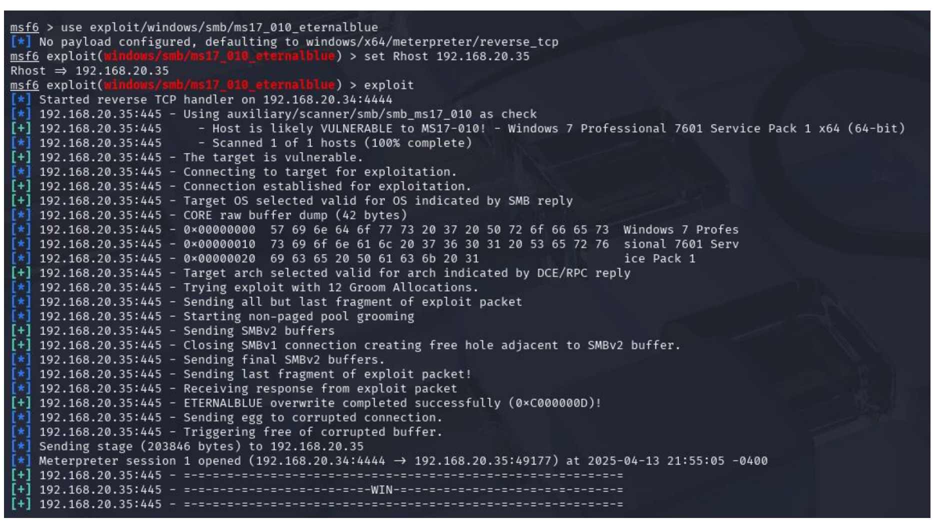


Nota. Creada por el autor

Paso F. Usando la instrucción Rhost apuntando a la ip de la máquina objetivo, se explota la vulnerabilidad e inicia el Meterpreter:

Figura 12

Instrucción Rhost sobre ip objetivo



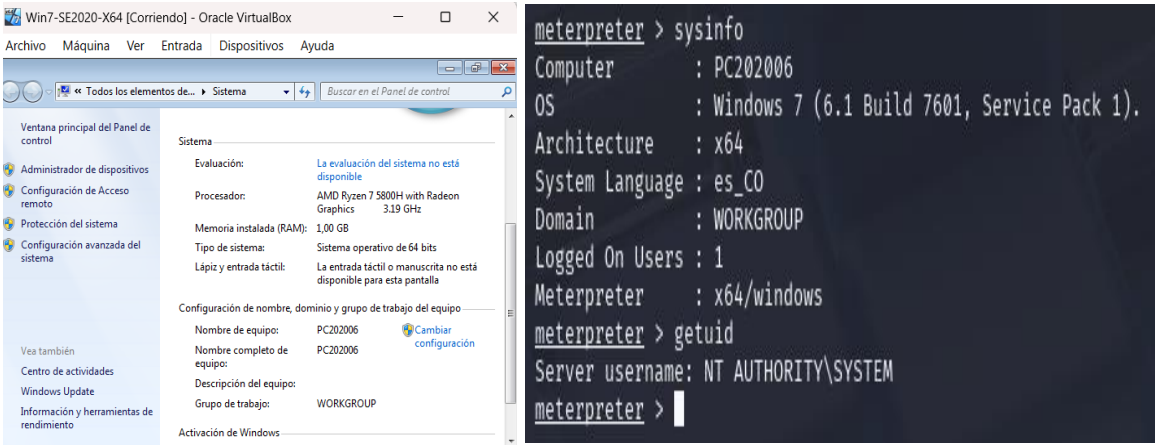
Nota. Creada por el autor

Post-Explotación

Paso G. Una vez en la máquina objetivo, se ejecuta SYSINFO para validar información de la misma y GETUID para los privilegios, al ser SYSTEM se puede continuar, sin la necesidad de escalar privilegios:

Figura 13

Validación de ingreso a máquina objetivo

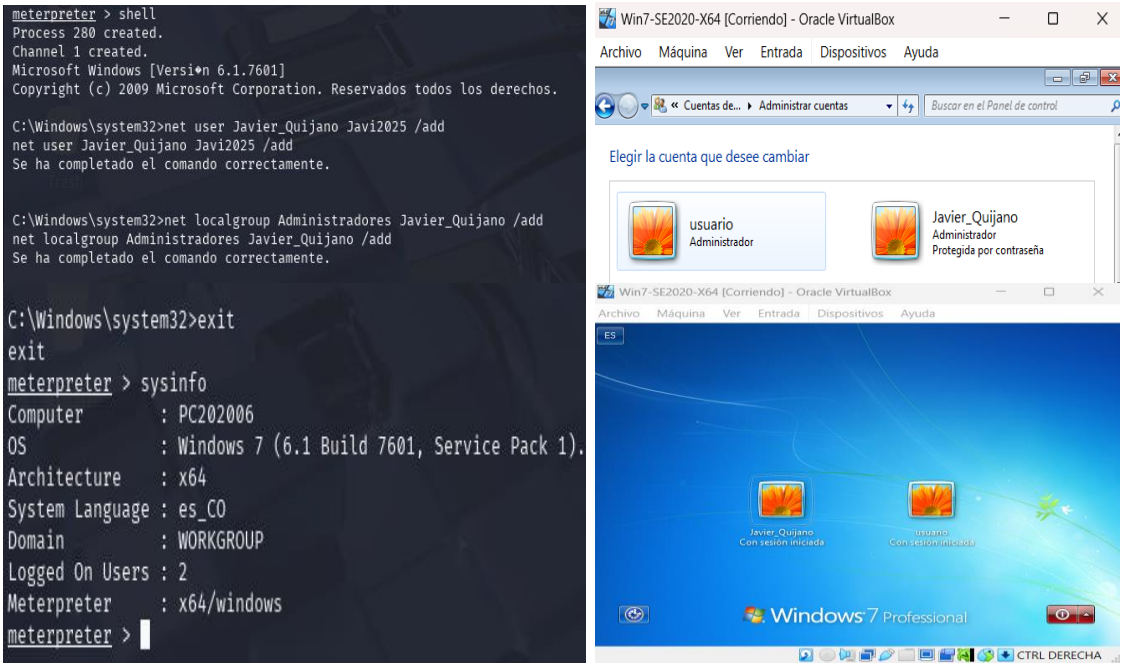


Nota. Creada por el autor

Paso H. Con Shell se ingresa a la consola de Windows de la máquina objetivo y se crea el usuario Javier_Quijano con contraseña (Javi2025), otorgándole privilegios de administrador. Luego se abre el Administrador de Cuentas de la máquina objetivo y se observa la cuenta de usuario creada desde Kali Linux. Adicionalmente se inicia la sesión y con SYSINFO dentro de Kali Linux, se visualiza que aparece otro usuario logeado:

Figura 14

Creación usuario con privilegios de administrador



Nota. Creada por el autor

Datos e información de ayuda para la identificación del fallo de seguridad específico hallado en la máquina Windows.

Sistema operativo. Equipo por medio del cual se genera la fuga de información tiene instalada una aplicación vulnerable bajo Windows.

Vulnerabilidad en Aplicativo. Aplicación que aparentemente cuenta con un exploit que estaría permitiendo el acceso sin autorización a través de consola.

Creación de usuario no autorizado. Escalamiento de privilegios a través de la creación de un usuario tipo administrador que permitiría la modificación de otros usuarios y archivos de sistema.

En resumen, La información clave es la presencia de una aplicación vulnerable en el sistema Windows, la existencia de un exploit para esa aplicación, y la posibilidad de usar esa vulnerabilidad para obtener acceso al sistema y aumentar los privilegios

La herramienta usada para poder identificar los fallos de seguridad fue Nmap.

Se utilizó Nmap específicamente con el script "vuln" para la búsqueda de vulnerabilidades conocidas, además de –sV, para detección de servicios con sus versiones y puertos abiertos, obteniendo información sobre posibles agujeros de seguridad que podrían ser explotados en un ataque.

El puerto que abre la aplicación vulnerable es el puerto 445. Este puerto está asociado con el servicio Microsoft-DS, que es Microsoft Windows SMB (Server Message Block), afectado en versiones de Windows no actualizadas y permitiendo el uso de exploits para ganar acceso al sistema. (Microsoft, 2017).

¿Cómo afecta el ataque a la máquina Windows?

El ataque está enfocado en la explotación de una vulnerabilidad presente en el protocolo Server Message Block (SMB) de Windows, en el puerto 445, haciendo uso del exploit conocido como EternalBlue (Avast, 2020):

Reconocimiento (Nmap). Herramienta Nmap para realizar un escaneo de la máquina Windows objetivo, identificando que el puerto 445 está abierto.
Al ejecutar el --script vuln, se encuentra la vulnerabilidad MS17-010, (Google, 2017).

Explotación (Metasploit). Usando el framework Metasploit, desde el sistema operativo Kali Linux, se selecciona el módulo exploit (exploit/windows/smb/ms17_010_eternalblue), para luego establecer con RHOST, la dirección IP de la máquina objetivo.

Se ejecuta el exploit, el cuál aprovecha una falla en la forma en que SMB maneja determinadas operaciones de memoria, permitiendo la sobreescritura de la memoria y ejecución de código.

Post-Explotación (Meterpreter). A través de Meterpreter, payload dentro de Metasploit que proporciona un control extenso sobre un sistema comprometido, se pueden ejecutar diferentes acciones, como:

Recopilación de información del sistema (sysinfo, getuid).

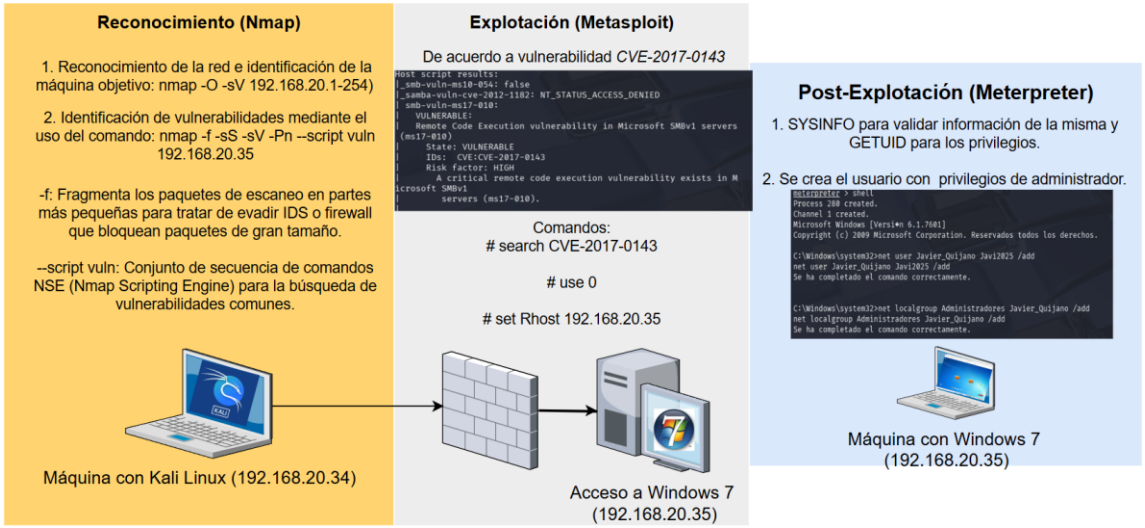
Ejecución de comandos en la consola del pc víctima.

Creación de nuevos usuarios y escalamiento de privilegios.

Extracción de información confidencial.

Figura 15

Afectación del ataque a la máquina Windows



Nota. Creada por el autor

Capítulo 4 Objetivo específico 4

Determinación de las acciones iniciales a realizar ante un ataque en tiempo real, especificando indagaciones y procedimientos técnicos.

Ante un ataque en tiempo real, la prioridad absoluta es obtener una información rápida y precisa de la situación para contener la amenaza y mitigar el daño para la recopilación y el análisis de información:

Verificación

Confirmar la realidad de ataque y no una falsa alarma. Implica revisar las alertas de los IDS y/o SIEM, este último permitiría correlacionar eventos de diferentes medios (firewalls, servidores, endpoints) que validen algún tipo de actividad irregular.

Examinar logs de sistema y aplicaciones en búsqueda de errores inusuales o actividades sospechosas. Herramientas como Systeminfo y Hostname son importantes en Windows.

Enfoque con MITRE ATT&CK. Búsqueda de patrones que se alineen con las tácticas de TA0001 (Initial Access) como T1566 ("Phishing"), T1190 "Exploit Public-Facing Application) o TA0002 (Execution) como T1059 (Command and Scripting Interpreter). También TA0004 (Privilege Escalation), uso de exploits para obtener derechos de administrador, o TA0007 (Discovery), uso de herramientas para el mapeo de red, MITRE. (s.f.).

Contención

Una vez identificados los sistemas afectados, aislarlos de la red para prevenir la propagación, implicando la desconexión de los segmentos de red o firewalls para bloquear el tráfico.

Implementar reglas de firewall estrictas para el bloqueo del tráfico y comunicaciones de los atacantes, esto incluye el bloqueo de direcciones IP, dominios o puertos específicos.

Uso de antivirus o reinstalación de sistemas comprometidos.

Enfoque con MITRE ATT&CK. TA0005 (Defense Evasion), donde los atacantes intentan evadir la detección y TA0008 (Lateral Movement), para el aislamiento de los sistemas, dificultan el movimiento lateral del atacante. Así mismo interrumpir el TA0011 (Command and Control), MITRE. (s.f.).

Análisis Forense

Recolección de datos volátiles de la memoria RAM, puede existir información que se perdería al apagar el sistema. Uso de aplicaciones como Volatility (para análisis de memoria) y Regripper (para análisis de registro).

Copias forenses de medios de almacenamiento de los sistemas afectados.

Enfoque con MITRE ATT&CK. Ayuda a detectar técnicas como TA0006 (Credential Access), obtención de contraseñas en la memoria, o TA0003 (Persistence) en T1505.006, si el malware está cargado en la RAM, MITRE. (s.f.).

Documentación

Documentar cada paso, incluyendo la hora de inicio del ataque, sistemas afectados y acciones tomadas.

Apegarse a una cadena de custodia, le da un acto profesional para mantener la integridad de la evidencia.

Medidas de hardenización necesarias para evitar la incidencia

Con el fin de enriquecer medidas hardenización, se alineará con los CIS Controls v8, Center for Internet Security. (2021, Mayo), para proporcionar una estructura más clara y delimitada de las medidas a tomar:

CIS Control 1-2: Control de Activos de Hardware y Software. La gestión de un inventario detallado de los activos, tanto de hardware como de software, es prioritario para la identificación de elementos no autorizados, no actualizados o no parcheados que los atacantes podrían explotar.

CIS Control 3: Protección de Datos. Identificación, clasificación, protección y gestión de la información correctamente etiquetada como sensible, confidencial y pública, es esencial para la mitigación del impacto anta la exfiltración de data.

CIS Control 4: Configuración Segura de Activos. La implementación de configuraciones seguras juega un papel primordial en la reducción de la superficie de ataque y prevención en la explotación de configuraciones por defecto.

CIS Control 5-6: Administración de Cuentas y Control de Accesos. Gestión de un programa de gestión integral de identidades y accesos (IAM) para las cuentas de usuario

y sus privilegios, es importante en la prevención de accesos no autorizados, escalamiento y el movimiento lateral. Un control de acceso basado en roles y la autenticación multifactor (MFA) reduce el riesgo de acceso no acreditado a información y funciones críticas.

CIS Control 7-8: Gestión Continua de Vulnerabilidades y Registros de Auditoría. El escaneo proactivo y corrección de vulnerabilidades de manera en combinación con el análisis de registros de auditoría es importante para la detección temprana, investigación de incidentes y comprensión del alcance del ataque.

CIS Control 11: Recuperación de Datos. Prácticas cruciales para la restauración efectiva de los sistemas a un estado seguro después de un ataque, específicamente en casos de ransomware: copias de seguridad automatizadas e instancias aisladas de recuperación de información.

CIS Control 14: Concienciación en Seguridad y Mejores Prácticas. La capacitación de los usuarios a cerca de amenazas reduce el riesgo ante la ingeniería social como también mejores prácticas en manejo de datos, reconocimiento y notificación de incidentes.

CIS Control 17: Gestión de Respuesta a Incidentes. Establecimiento de un plan para la detección, respuesta y recuperación de ataques efectiva a incidentes con protocolos de comunicación, asignación de roles claves, responsabilidades y ejercicios constantes.

Diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos.

Estas son las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos descritos en la siguiente tabla:

Tabla 1

Diferencias entre Blue Teams y Equipo de Respuesta a incidentes

Blue Teams	**Equipo de Respuesta a incidentes**
Enfoque proactivo que busca la prevención de ataques, monitoreo de amenazas potenciales, fortalecimientos de defensas y mantenimiento de la postura de seguridad.	Enfoque reactivo cuando se produce un incidente de seguridad, de forma rápida y eficiente para minimizar el daño y restaurar las operaciones.
- Monitoreo de infraestructura de TI en busca de anomalías - Configuración de dispositivos para seguridad informática - Actualización de sistemas - Implementación de políticas de seguridad.	- Investigación del incidente. - Contención, erradicación, recuperación de los sistemas, - Aprendizaje en prevención de posibles nuevos ataques. - Análisis forense, gestión de crisis y comunicación efectiva.
Controles CIS v8 asociados: - Control 4: Configuración segura HW/SW - Control 6: Implementación de controles de acceso	Controles CIS v8 asociados: - Control 8: Análisis de registros de auditoría para una investigación forense, que permita determinar el alcance, causa raíz y el vector de ataque.

- Control 7: Gestión de vulnerabilidades - Control 13: Monitoreo y Defensa de la red - Control 14: Concienciación y capacitación de usuarios	- Control 11: Restauración de datos -Control 17: Gestión de repuesta a incidentes con procedimientos, roles definidos, capacitación y comunicaciones
Responsabilidades: - Seguridad de redes (firewalls, protocolos) - Sistemas operativos (Propietario y GPL) - Análisis de vulnerabilidades - IDS, IPS, SIEM, entre otros - Gestión de identidades y accesos (IAM) - Cifrado de información	Responsabilidades: - Análisis forense (Recuperación de datos, análisis de RAM, entre otros.) - Gestión de crisis (decisiones bajo presión) - Comunicación efectiva (con roles claves y responsables) - Conocimiento profundo de MITRE ATT&CK (comprensión del atacante) - Leyes y normas como posible guía o asociación (ISO 27037, Ley 1273 de 2009, Ley 1621 de 2013, entre otros).

Nota. Elaboración propia

El papel del CIS "Center For Internet Security" dentro de un equipo Blueteam

Trabajar CIS permite contar con un cuadro amplio para tratar variedad de puntos básicos y críticos en el fortalecimiento de la seguridad en determinada organización, al servir como una

guía integral de mejora desde su configuración inicial en los sistemas hasta la recuperación ante incidentes de seguridad. Entre su contenido para emplear se puede encontrar:

CIS Benchmarks. Uso de los Benchmarks que proporcionan guías de configuración detalladas y probadas por la comunidad que colabora con CIS, ayudando al hardening, (Eslami et al., 2023).

CIS Controls. Revisar los controles CIS establecen un conjunto de acciones de seguridad para implementar y gestionar las defensas de ciberseguridad de forma más organizada, tomando como foco las acciones que tienen mayor importancia.

Herramientas de Evaluación. Con el propósito de auditar la configuración de los sistemas y al compararla con los Benchmarks, permite identificar desviaciones en mejores prácticas y vulnerabilidades potenciales.

Pentesting. Los CIS Controls se podrían tomar como base para el diseño pruebas de penetración más encaminadas.

Monitoreo. Servir de guía sobre la implementación de un monitoreo efectivo (por ejemplo, el Control 8, Registros de Auditoría), en la configuración de sistemas de registro en un SIEM para la detección de actividades inusuales que podrían indicar un ataque.

Normatividad. Los Controles CIS están alineados con otros marcos y normativas de seguridad (como NIST e ISO 27001), facilitando demostrar el cumplimiento normativo y la adopción de las mejores prácticas en seguridad.

Funciones y características principales de lo que es un SIEM.

Entre las Funciones Principales de un SIEM, Red Hat. (2023, 21 de septiembre) se encuentran

Recolección. Recopilar y almacenar registros de seguridad de la infraestructura de TI en una organización: firewalls, servidores, IDS, aplicaciones, entre otros.

Análisis. Analizar de la data recopilada para identificar patrones, anomalías y posibles amenazas.

Monitoreo. Monitorear continuamente de actividades y generación de alertas en tiempo real cuando se detectan eventos sospechosos o que violen las reglas de seguridad predefinidas.

Informes. Generar informes de seguridad para cumplir con regulaciones y estándares.

Análisis Forense. Ayudar en investigaciones forenses al proporcionar un registro detallado de los eventos de seguridad, contribuyendo a la reconstrucción de la secuencia de eventos en un ataque.

Características Principales de un SIEM

Centralización. Vista unificada de la seguridad, facilitando la identificación de amenazas.

Detección Avanzada. Anomalías y aprendizaje automático, para identificación de amenazas complejas y/o que evolucionen, incluyendo amenazas internas y ataques de Cero Day.

Correlación de Eventos. Identificar patrones maliciosos que podrían no ser evidentes al analizar los registros de forma individual, permitiendo relacionar eventos aparentemente no relacionados y detectar ataques complejos.

Automatización. Automatizar tareas de recopilación de registros, análisis y generación de informes, mejorando la eficiencia del trabajo.

Herramientas de contención de ataques informáticos

NGFW (Firewalls de Próxima Generación). Hardware que incorpora funcionalidades activas de contención. Inspeccionan el tráfico a un nivel más profundo (capa de aplicación) y pueden identificar comportamientos maliciosos en tiempo real, tomando medidas inmediatas para contenerlo, que incluye:

Bloqueo de direcciones IP, puertos y terminación de sesiones. Interrumpiendo la comunicación entre el atacante y los sistemas comprometidos, además de su aislamiento.

Cuarentena de hosts. Aislamiento del sistema comprometido.

Implementación de reglas de firewall dinámicas. Creación de reglas temporales para el bloqueo de patrones de tráfico específicos asociados con el ataque.

HIPS (Sistemas de Prevención de Intrusiones en Host). Software que se instala en un endpoint y monitorea la actividad del sistema en busca de comportamientos inusuales, de encontrarlos aplica medidas de contención como:

> ***Aislamiento o terminación de procesos sospechosos.*** Restringe acciones que un proceso malicioso puede estar realizando, a través de limitar el acceso a otros recursos del sistema, comunicación con otros procesos y la modificación de archivos.
>
> ***Restauración de archivos.*** Revirtiendo cambios ejecutados por el proceso malicioso a partir de copias de seguridad o snapshots.
>
> ***Bloqueo de la comunicación de red.*** Impidiendo que el proceso se comunique con otros dispositivos conectados.

Plataforma SOAR (Security Orchestration, Automation, and Response). Software que integran diferentes herramientas de seguridad y automatizan los flujos de trabajo para la respuesta a incidentes por medio de playbooks (guías detalladas que definen las acciones a seguir). Cuando alguna herramienta de detección alerta sobre una probabilidad de amenaza, SOAR puede activar automáticamente un playbook de contención con acciones en múltiples sistemas y herramientas para limitar el impacto del ataque, por ejemplo:

Aislamiento de endpoints. Uso de comandos remotos para la desconexión de un sistema comprometido de la red.

Bloqueo de usuarios y cuarentena de emails. Inhabilitación de cuentas de usuario probablemente comprometidos, así como mover correos electrónicos sospechosos de las bandejas de entrada de los usuarios.

Aplicación de reglas de firewall. Modificando las reglas del firewall para el bloqueo del tráfico.

Análisis Avanzado. Utilización de machine learning e IA, para reducir el tiempo en identificación de patrones.

Ejecución de scripts para remediación. Automatización de tareas de limpieza en sistemas afectados.

Documentación y Comunicación. Generación de documentación del incidente y comunicación real-time con las partes interesadas.

Conclusiones

La ciberseguridad requiere un enfoque integral que no solo abarque la identificación y explotación de vulnerabilidades, sino también una profunda consideración de los marcos legales y éticos, esenciales para la operación responsable de los equipos Red Team y Blue Team.

La comprensión y aplicación del marco legal colombiano, incluyendo las leyes sobre delitos informáticos y protección de datos personales, son cruciales para los profesionales de la ciberseguridad, ya que guían las metodologías y herramientas utilizadas en pruebas de penetración y otras actividades de seguridad.

La investigación y demostración práctica de la explotación de vulnerabilidades, como la escalada de privilegios en un entorno Windows, son fundamentales para evidenciar el riesgo real de las fallas de seguridad y la importancia de una adecuada gestión de incidentes y hardenización.

La eficacia en la ciberseguridad depende de la colaboración entre equipos defensivos (Blue Team, IR), el seguimiento de estándares como los Controles CIS, el uso de herramientas de monitoreo (SIEM) y la aplicación de la informática forense para asegurar una postura defensiva robusta y una respuesta adecuada ante cualquier tipo de ataque.

Recomendaciones

El análisis de las estrategias y acciones de los equipos Red Team y Blue Team en el ámbito de la ciberseguridad, considerando aspectos legales, éticos y técnicos, permite formular las siguientes recomendaciones para la identificación, explotación y contención de amenazas informáticas:

Cumplimiento Legal y Ético Continuo

Para Red Team y Blue Team

Asegurar que todas las actividades, desde el pentesting hasta la respuesta a incidentes, se realicen dentro de los límites de la legislación colombiana vigente, incluyendo la Ley 1273 de 2009 sobre delitos informáticos y la Ley 1581 de 2012 sobre protección de datos personales. Esto implica obtener consentimientos informados explícitos y documentados antes de cualquier prueba de penetración o acceso a información sensible.

Para la Organización

Realizar auditorías legales periódicas de los acuerdos y contratos de ciberseguridad para identificar y eliminar cláusulas abusivas o que contravengan la normativa legal, como aquellas que impidan la denuncia de actividades ilícitas. Es crucial que los contratos no contengan ambigüedades en la definición de "información confidencial" que puedan encubrir actividades ilegales.

Principios Éticos y Profesionalismo

Para Profesionales de Ciberseguridad

Adherirse estrictamente al Código de Ética de COPNIA para ingenieros, que prohíbe el encubrimiento de delitos y el aprovechamiento indebido de la confianza. No aceptar trabajos que impongan la obligación de mantener silencio sobre la comisión de delitos o que ofrezcan beneficios injustificados que comprometan la ética profesional.

Para la Organización

Fomentar una cultura organizacional basada en la transparencia, la integridad y el respeto por la ley. Esto incluye la implementación de políticas claras que promuevan la denuncia de irregularidades y protejan a los empleados que actúen conforme a la ética y la legalidad.

Metodología de Pentesting Rigurosa

Implementar un proceso de pentesting bien definido que incluya fases de planeación, evaluación (recolección de información, mapeo de red, identificación de vulnerabilidades) y explotación, culminando con la presentación de informes detallados.

Documentación Detallada de Vulnerabilidades

Documentar minuciosamente los comandos utilizados, los resultados obtenidos y las evidencias de la explotación de vulnerabilidades, como la creación de usuarios con privilegios elevados. Esto es crucial para que el Blue Team pueda comprender el impacto del ataque y aplicar las medidas correctivas.

Investigación y Contención de Fugas de Información

Implementar SIEM (Security Information and Event Management) para la recolección, análisis y monitoreo continuo de registros de seguridad. Esto permite la detección temprana de anomalías, correlación de eventos y generación de alertas en tiempo real, lo cual es fundamental para identificar ataques en curso, como fugas de información.

Enfoque Holístico de la Ciberseguridad

La ciberseguridad eficaz requiere un enfoque integral que combine la prevención, la detección, la respuesta y la recuperación. Esto implica la colaboración constante entre los equipos Red Team (simulación de ataques) y Blue Team (defensa) para identificar debilidades y fortalecer las defensas.

Capacitación, Concienciación Continua y Confianza Digital

La capacitación de los profesionales en el uso de herramientas especializadas y metodologías de pentesting es esencial. Asimismo, la concienciación de los usuarios sobre las amenazas de ciberseguridad reduce significativamente el riesgo de ataques basados en ingeniería social.

Tecnología y Procesos Robustos

La implementación de sistemas SIEM, firewalls de próxima generación (NGFW), HIPS y plataformas SOAR son indispensables para una detección, análisis y contención de ataques eficiente en tiempo real. Estos deben complementarse con planes de respuesta a incidentes bien definidos y prácticas de "hardenización" continua.

Referencias Bibliográficas

Avast, de 18 de junio, ¿Qué es EternalBlue y por qué el exploit MS17-010 sigue siendo relevante? (2020). https://www.avast.com/es-es/c-eternalblue

ÁREA DE INNOVACIÓN Y DESARROLLO. (2018). Introducción A La Seguridad Informática y el Análisis De Vulnerabilidades. CAPÍTULO IV: METODOLOGÍAS DE ANÁLISIS DE VULNERABILIDADES, p. 52.

Besson, P.-V., Brisse, R., Orsini, H., Sanchez, A., & Tong, V. V. T. (2023). CERBERE: Cybersecurity Exercise for Red and Blue team Entertainment, REproducibility. Proceedings - 2023 IEEE International Conference on Big Data, BigData 2023

Center for Internet Security. (2021, Mayo). Controles CIS Versión 8. Recuperado el 11 de abril de 2025, de https://learn.cisecurity.org/cis-controls-download-v8.pdf.

COPNIA. (s.f.). Código de Ética, para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Recuperado el 11 de abril de 2025, de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

Departamento Nacional de Planeación (2020). Documento CONPES 3995, Política Nacional De Confianza Y Seguridad Digital, Recuperado el 11 de abril de 2025, de https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

Eslami, M., Knechtel, J., Sinanoglu, O., Karri, R., & Pagliarini, S. (2023). Benchmarking Advanced Security Closure of Physical Layouts: ISPD 2023 Contest. Proceedings of the International Symposium on Physical Design, pp. 256–264.

Google, de 26 de Mayo, SMB Exploited: WannaCry Use of "EternalBlue". (2017). https://cloud.google.com/blog/topics/threat-intelligence/smb-exploited-wannacry-use-of-eternalblue/

Jiménez-Almeira, G. A., & López, D. E. (2023). Cybersecurity and Integral Security: an analysis of regulatory progress in Colombia | Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 2023(E62), pp. 16–31.

Ley 1273, de 5 de enero, de la protección de la información y de los datos. (2009). Artículos 269A, 269B, 269H. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492.

Ley 1341, de 30 de julio, de principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones. (2009). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913.

Ley 1581, de 17 de octubre, de disposiciones generales para la protección de datos personales. (2012). Artículos 4, 23. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

Ley 1621, de 17 de abril, de normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal. (2013). Artículos 2, 17, 42. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706.

Microsoft, de 14 de marzo, Actualización de seguridad para Microsoft Windows SMB Server (4013389). (2017). https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010

MITRE. (s.f.). Enterprise tactics, Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access. Recuperado el 8 de mayo de 2025, de https://attack.mitre.org/tactics/enterprise/

Red Hat. (2023, 21 de septiembre). *What is security information and event management (SIEM)?* Recuperado de https://www.redhat.com/en/topics/security/what-is-SIEM

Apéndices

Apéndice A

Enlace público del video en una hoja como apéndice del documento

Enlace público del video

Enlace al video de sustentación

Fuente. https://youtu.be/mD6wahgj3XY

Apéndice B

Resultado de prueba anti plagio Turnitin

Enlace resultado de prueba anti plagio Turnitin

Enlace al resultado de prueba anti plagio Turnitin

Fuente. Resultado_reporte_antiplagio_Turnitin.pdf