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

Leonardo Cortes Fuquene

Grupo: 202337164_8

Presentado a:

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización Seguridad Informatica

2025

Resumen

El informe técnico documenta las actividades, estrategias y aprendizajes obtenidos durante un seminario de profundización en ciberseguridad, centrado en los equipos Red Team y Blue Team. A través de laboratorios controlados, se simularon ataques reales y se aplicaron técnicas de defensa, permitiendo comprender los roles ofensivos y defensivos en la protección de activos informáticos.

Se analizan aspectos éticos y legales, destacando cláusulas contractuales que vulneran la Ley 1273 de 2009 y principios del COPNIA. Se ejecutaron pruebas de intrusión utilizando herramientas como Nmap y Metasploit, explotando vulnerabilidades en sistemas Windows. Además, se proponen medidas de hardening, segmentación de red, uso de SIEM y políticas de seguridad para prevenir ataques.

El informe también diferencia entre Blue Team y equipos de respuesta a incidentes, y destaca la importancia de herramientas como pfSense, Wazuh y Cisco ISE para la contención de amenazas. Finalmente, se promueve la colaboración entre equipos ofensivos y defensivos bajo un enfoque Purple Team, fomentando una cultura de ciberseguridad continua.

Palabras Clave: Red Team. Blue Team. Simulación. Etica Profesional. Kali Linux.

Abstract

The technical report documents the activities, strategies and lessons learned during an in-depth cybersecurity seminar focused on the Red Team and Blue Team. Through controlled laboratories, real attacks were simulated and defense techniques were applied, allowing to understand the offensive and defensive roles in the protection of IT assets.

Ethical and legal aspects were analyzed, highlighting contractual clauses that violate Law 1273 of 2009 and COPNIA principles. Intrusion tests were executed using tools such as Nmap and Metasploit, exploiting vulnerabilities in Windows systems. In addition, hardening measures, network segmentation, use of SIEM and security policies to prevent attacks are proposed.

The report also differentiates between Blue Team and incident response teams, and highlights the importance of tools such as pfSense, Wazuh and Cisco ISE for threat containment. Finally, it promotes collaboration between offensive and defensive teams under a Purple Team approach, fostering a continuous cybersecurity culture.

Keywords: Red Team. Blue Team. Simulation. Professional Ethics. Kali Linux.

Glosario

Activos: Bienes tangibles o intangibles que poseen valor para la organización, como información, sistemas, infraestructura tecnológica o recursos humanos.

Amenazas: Causas potenciales de incidentes no deseados que pueden dañar activos de la organización. (ISO/IEC 27000)

Análisis Forense Digital: Proceso de recolección, preservación, análisis y presentación de evidencia digital con el fin de investigar incidentes de seguridad.

Botnet: Red de dispositivos comprometidos controlados remotamente mediante malware, utilizada para ejecutar ataques coordinados como DDoS o propagación de otros códigos maliciosos.

Blue Team: Equipo encargado de la defensa activa de los sistemas de información. Monitorea, detecta y responde a amenazas, asegurando la integridad, disponibilidad y confidencialidad de los activos.

Herramientas: Conjunto de recursos físicos o lógicos utilizados para proteger los activos de información, como firewalls, antivirus, IDS/IPS, entre otros.

Pentesting: Simulación controlada de ataques para identificar vulnerabilidades en sistemas, redes o aplicaciones.

Ransomware: Tipo de malware que cifra la información del sistema infectado y exige un rescate, generalmente en criptomonedas, para su recuperación.

Red Team: Equipo que simula ataques reales utilizando técnicas, tácticas y procedimientos similares a los de actores maliciosos, con el fin de evaluar la efectividad de las defensas de la organización.

Riesgo: Probabilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo en un activo. (ISO/IEC 27000)

Seguridad de la Información: Conjunto de prácticas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC 27000)

Vulnerabilidad: Debilidad en un sistema, proceso o control que puede ser explotada por una amenaza para comprometer la seguridad de los activos.

Tabla de contenido

Tabla de ilustraciones

Introducción

El presente informe tiene como objetivo documentar las actividades desarrolladas en el seminario de profundización sobre equipos estratégicos en ciberseguridad. A lo largo del curso, se llevaron a cabo laboratorios controlados que permitieron simular escenarios reales en los que intervienen los equipos Red Team y Blue Team. Estas prácticas facilitaron la comprensión de los procesos, capacidades y alcances de cada equipo dentro de una organización, así como su contribución al fortalecimiento de la seguridad informática.

Objetivos

Objetivo General

Elaborar un informe técnico que documente las actividades, estrategias y aprendizajes obtenidos durante el seminario de profundización sobre los equipos Red Team y Blue Team.

Objetivos Específicos

Formular recomendaciones prácticas orientadas al fortalecimiento de la postura de ciberseguridad en las organizaciones, basadas en las experiencias del seminario.

Documentar con evidencia el desarrollo de las actividades realizadas, como soporte del proceso de aprendizaje y validación de resultados.

Evaluar el impacto de las prácticas realizadas en los laboratorios controlados sobre la comprensión de los roles ofensivos y defensivos en ciberseguridad.

Desarrollo de la actividad

2.1 Actuación Etica y Legal

2.1.1 ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo?

En el anexo 2, se evidencian varias fragmentos ilegales e irregulares, como son:
La alta gerencia debe revisar los contratos que están próximos a firmarse y en los cuales es consciente que lo realizo un abogado que fue despedido por procesos ilícitos. Esto demuestra que el contrato puede contener clausulas inapropiadas o ilegales.

En la falta de esta revisión, se puede encontrar inconsistencias en los acuerdos de confidencialidad, por lo que se considera un riesgo de seguridad de la información y derechos de empleados.

En el Anexo 3 se evidencian varias fragmentos ilegales e irregulares, como son:
"No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros." Esto está indicando al empelado a abstenerse a denunciar actividades sospechosas de espionaje o ilícitas que pueda observar, por lo cual se considera ilegal. La aceptación de esta cláusula puede comprometer la integridad de los empleados al obligarlos a ocultar actividades ilegales, exponiéndolos a sanciones legales y éticas.

"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas." El acuerdo obliga a la parte receptora a no divulgar información confidencial e ilegal. Esto es éticamente cuestionable y puede ser ilegal, ya que protege actividades ilícitas bajo el manto de la confidencialidad.

Compromete la integridad de los empleados al obligarlos a ocultar información ilegal, exponiéndolos a sanciones legales y éticas.

"Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento." La empresa CyberFort es la responsable ante las autoridades de la información que se encuentre en su poder y no el empleado. Por lo cual esto se evidencia como una forma en evadir la responsabilidad legal.

"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." Por la evidencia del párrafo anterior, la empresa debe ser la responsable de la información que se encuentre en la compañía. Por lo cual no es ético y se puede considerar ilegal que el empelado sea el responsable de la información y liberando de cualquier responsabilidad a la empresa CyberFort Technologies.

La aceptación de cláusulas ilegales puede comprometer la integridad tanto de los empleados como de la compañía de varias maneras. La inclusión de cláusulas abusivas o que puedan afectar las leyes actuales, pueden dañar la reputación de la compañía, esto afectando la atracción de nuevo personal y afectar la relación con los clientes. Esto adicional puede ocurrir en multas y sanciones por el incumplimiento de normativas legales, afectando de forma critica la continuidad de la empresa por gastos no contemplados que pueden afectar su correcto funcionamiento. Por ultimo los empleados pueden demandar a la empresa por este tipo de cláusulas.

Con el fin de abordar lo anteriormente mencionado, se debe implementar varios aspectos como lo son: La revisión de los contratos por un área especializada, la cual pueda identificar y

eliminar cláusulas que no están de acuerdo con el código ética y legal. Se debe establecer políticas claras sobre la denuncia de actividades ilegales y la protección a denunciantes. En algunas organizaciones se opta por contratar a externos para evaluar y mejorar las practicas de contratación y confidencialidad.

2.1.2 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: Esto implica el acceso no autorizado a sistemas informáticos. Esto hace referencia a que el acuerdo menciona la prohibición de denunciar activades sospechosas de espionaje o apropiación de información de terceros, por lo cual comprende que se podría permitir que se mantenga el acceso abusivo, sin consecuencias legales.

Artículo 269C: Interceptación de datos informáticos: La cláusula que obliga a no denunciar información ilegal podría incluir la interceptación de datos informáticos sin autorización judicial, lo cual es una violación directa de este artículo y agrava la situación. Artículo 269F: Violación de datos personales: La prohibición de divulgar información confidencial e ilegal puede incluir la manipulación o uso indebido de datos personales, lo cual vulnera este artículo. La protección de los datos personales es fundamental en todos los aspectos. Artículo 269D: Daño Informático: La responsabilidad impuesta a la parte receptora en caso de allanamiento podría implicar la destrucción o alteración de datos informáticos para evitar la detección de actividades ilegales, lo cual vulnera este artículo. La cláusula que exime de

responsabilidad a CyberFort Technologies podría incentivar el daño informático para proteger la empresa.

Artículo 269E: Uso de software malicioso: La prohibición de denunciar actividades ilegales podría incluir el uso de software malicioso, por lo cual permite que se perpetúe el uso de software dañino.

2.1.3 ¿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?

No. No aplicaría este trabajo por varios aspectos legales y basado en el Código de ética para ingenieros de COPNIA.

De acuerdo con el código de ética del COPNIA, debemos actuar con integridad y honestidad en todas nuestras actividades profesionales, por lo cual aceptar este trabajo en el cual hay cláusulas que prohíben denunciar actividades ilegales va en contra a la integridad y honestidad anteriormente mencionada. Al prohibir denunciar las actividades ilegales estamos incumpliendo el artículo 32, el cual nos exige el cumplimiento de todas las leyes y regulaciones aplicables, por lo que se consideraría una violación directa a este principio. Por otro lado, en el artículo 36 menciona que debemos ser responsables de nuestras acciones y decisiones, por lo cual aceptar este trabajo, podría implicar responsabilidad legal y ética en caso de que se descubra actividades ilícitas. Esto conlleva a no aceptar el trabajo por lo cual se indaga que la empresa puede fomentar practicas ilegales y no éticas lo cual afectaría la reputación y dignidad de mi profesión.

2.1.4 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.

El incidente en CyberFort Technologies muestra prácticas ilegales y no éticas, las cuales comprometieron la reputación de la empresa. Los empleados usaron su acceso para recopilar información confidencial sin permiso y luego vendieron esa información en la darknet, esto es ilegal y muy poco ético. Por mejorar procesos y buscar nuevas amenazas, no se debió a utilizar el acceso autorizado para obtener y sacar información a la cual no se tenía acceso. Legalmente, están violando varias leyes, como las de protección de datos y ciber espionaje, por lo cual se rompe la confianza con el cliente actuando de forma deshonesta. En las leyes que se puede estar incurriendo y que están relacionadas con el ciber espionaje, encontramos la ley PATRIOT, la cual fue promulgada en 2001, Esta ley, promulgada en 2001, amplía las capacidades de vigilancia y recopilación de datos por parte de las agencias de seguridad nacional para prevenir actos de terrorismo. Incluye disposiciones que permiten la interceptación de comunicaciones y el acceso a registros financieros y de Internet. Adicional encontramos el reglamento general de protección de datos RGPD, este establece normas estrictas sobre la recopilación, almacenamiento y uso de datos personales, por otra parte, obliga a las empresas a obtener el consentimiento explícito de los individuos antes de procesar sus datos y a implementar medidas de seguridad adecuadas.

Éticamente, están rompiendo la confianza del cliente y actuando de manera deshonesta. Para una empresa de ciber seguridad el código de ética debe guiar las practicas de acuerdo a estándares y normativas internacionales, en las cuales encontramos varios casos como lo son: ISO27001, la cual es una norma internacional que proporciona un marco para la gestión de

seguridad de le información, incluyendo la implementación de controles de seguridad y la evaluación de riesgos. Otra normativa que se puede contemplar es la NIS2 Directiva sobre seguridad de las redes y sistemas de información, la cual establece requisitos para la ciberseguridad en sectores claves. Es acá la importancia de recalcar desde la alta gerencia de la empresa, primero validar el contrato con sus empleados y verificar los anexos que se encuentran en los mismos. Es importante asegurarse de que los empleados que tienen roles críticos y tareas sensibles sean profesionales, éticos y estén comprometidos con los valores de la empresa. Por último, es importante la implementación del código de ética, el cual debe contener los siguientes aspectos: Capacitación continua, auditorías internas, políticas de manejo de información confidencial y trasparencia.

2.2 Ejecución pruebas de intrusión

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

VirtualBox: Es una herramienta de virtualización de código abierto desarrollada por Oracle, que permite crear y ejecutar máquinas virtuales en distintos sistemas operativos (Windows, Linux, macOS). Con VirtualBox, los usuarios pueden simular otros sistemas operativos dentro de su equipo físico, facilitando pruebas, laboratorios y entornos seguros para prácticas de ciberseguridad o desarrollo sin afectar el sistema principal.

Una vez realizada la instalación de VirtualBox 7.1.6, se realiza el cargue de la maquinas con las que procederemos a trabajar en este laboratorio las cuales son: Kali Linux y la versión de la maquina involucrada con el nombre Win7-SE2020-X64.

Win7-SE2020-X64: Imagen con sistema operativo vulnerable.

Kali Linux: Es una distribución de Linux basada en Debian, diseñada especialmente para pruebas de penetración, auditorías de seguridad y análisis forense digital. Desarrollada y mantenida por Offensive Security, Kali incluye una amplia gama de herramientas preinstaladas para tareas como escaneo de redes, explotación de vulnerabilidades, ingeniería inversa y pruebas de contraseñas, convirtiéndola en una de las plataformas preferidas por profesionales en ciberseguridad.

NMAP: Es una herramienta de código abierto utilizada para el escaneo y mapeo de redes. Permite descubrir hosts activos, servicios disponibles, puertos abiertos y características del sistema operativo en dispositivos conectados a una red. Dentro de la maquina con Kali Linux, abrimos una terminal y ejecutamos el comando *nmap –version* este comando nos permitirá evidenciar la versión de Nmap que tenemos instalada.

Metasploit Framework: Es un framework de código abierto utilizado para desarrollar, probar y ejecutar exploits contra sistemas vulnerables. Es una de las herramientas más poderosas en ciberseguridad ofensiva, ya que permite automatizar ataques, obtener acceso remoto a sistemas, escalar privilegios y generar pruebas de concepto (PoC) en entornos controlados.

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

En el anexo 4, se indica que se encuentra una aplicación vulnerable en Windows la cual tiene asociado un exploit el cual permite un acceso a Shell remoto, escalación de privilegios y una creación de usuarios tipo administrador. Esto junto con un Nmap desde el Kali Linux nos abre la puerta a que el puerto 445 se puede acceso con el Shell remoto Meterpreter.

Adicional a primera instancia sabemos que la maquina no cuenta con actualizaciones y un sistema operativo el cual ya que no tiene soporte por fabricante. Lo anterior abre a que sea mucho más vulnerable la máquina.

Por ultimo y no menos importante, se evidencio que el firewall se encuentra desactivado, lo que nos permite de una forma mucho más fácil identificar puertos y forma de conexión a la máquina de una forma más sencilla.

2.2.3 ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows"? ¿Qué puerto abre la aplicación específica en el anexo?

Como se evidencio en el primer paso, las herramientas utilizadas fueron:

NMAP: El cual se utilizó para realizar un escaneo de puertos y servicios en la máquina de Windows. Esto evidencio el puerto utilizado 445 se encontraba potencialmente vulnerable.

Metasploit Framework: La cual fue utilizada para explorar y explotar vulnerabilidades en servicios SMB. Se utilizo el exploit exploit/windows/smb/ms17_010_eternalblue.
Para la creación del usuario con permisos de administrador se utilizó la prueba de concepto PoC.

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

En el ataque realizado, evidenciamos que el equipo de la organización compromete varios aspectos importantes ya que el atacante una vez detectado el puerto y con las herramientas anteriormente descritas como fueron Nmap y Metasploit, puede acceder a archivos, servicios e incluso privilegios con credenciales, lo que permite tener un control total de la máquina y otras en la misma red. Con la creación del usuario administrador, en un entorno corporativo con dominio, se puede acceder fácilmente permitiendo control de múltiple equipos de la organización. Además, una vez establecida la persistencia en la máquina comprometida, es

posible lanzar ataques adicionales desde este punto hacia otros sistemas o redes conectadas, ampliando considerablemente el alcance de la intrusión

Figura 1

Ciclo de vida de un ataque

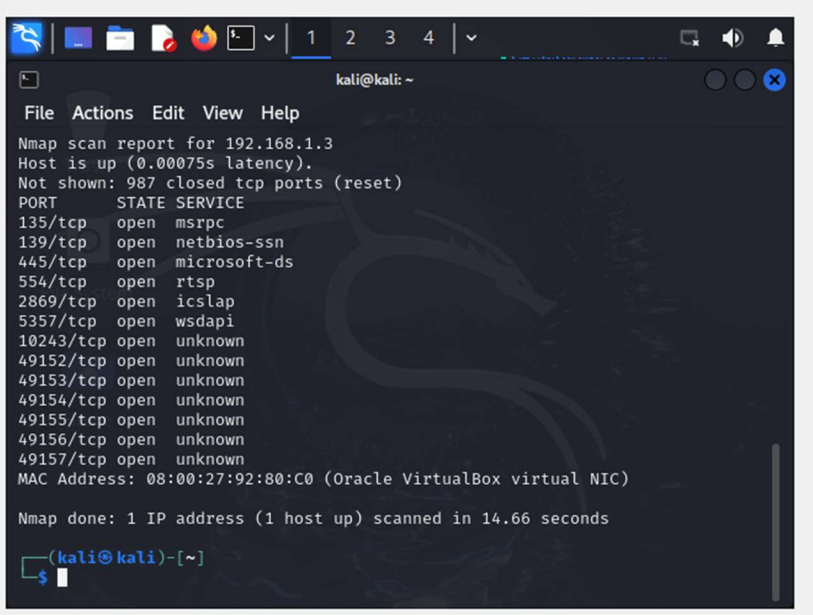
*Fuente. Imagen tomada de: Red Team Ops. (s.f.). Red Team Operations Attack Lifecycle LinkedIn. Recuperado el 4 de mayo de 2025, de https://www.linkedin.com/in/**[usuario]/posts/[id-de-la-publicación]***

2.2.5 Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Una vez tengamos las maquinas configuradas para que tengan comunicación entre Windows y Kali Linux. Paso configuración explicado en el punto 5 del presente trabajo, procederemos a ejecutar el comando *nmap 192.168.1.3*. Este comando nos muestra a continuación los puertos abiertos:

Figura 2

Verificar puertos NMAP.



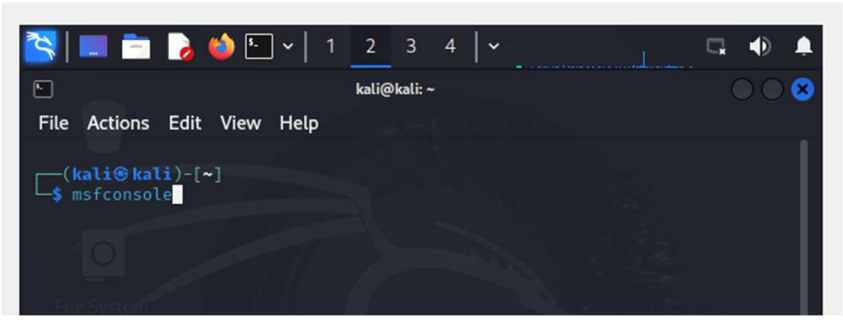
Fuente. Elaboracion propia

Evidenciamos en el escaneo que el puerto 445/tcp se encuentra abierto. Este puerto es asignado a NetBIOS, Network Basic Input / Output System y hace que la red sea vulnerable a los ataques de los piratas informático.

Desde la consola de Kali, ejecutamos el comando *msfconsole* el cual nos ejecuta Metasploit:

Figura 3.

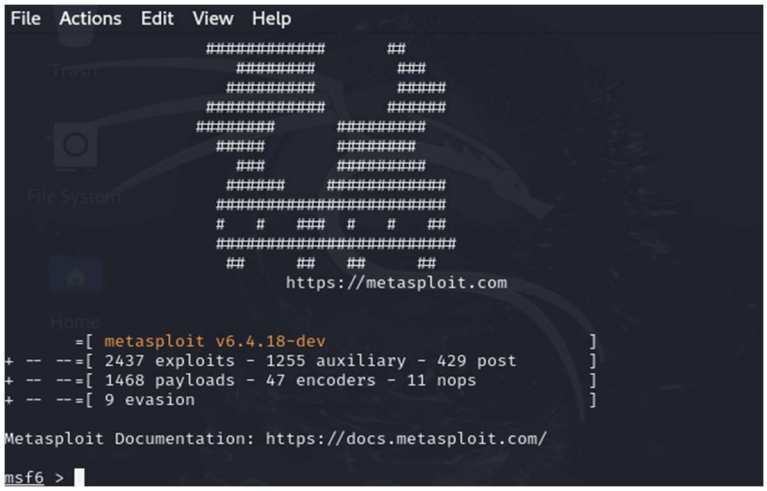
Ejecución comando msfconsole



Fuente. Elaboracion propia

Figura 4.

Inicio metasploit

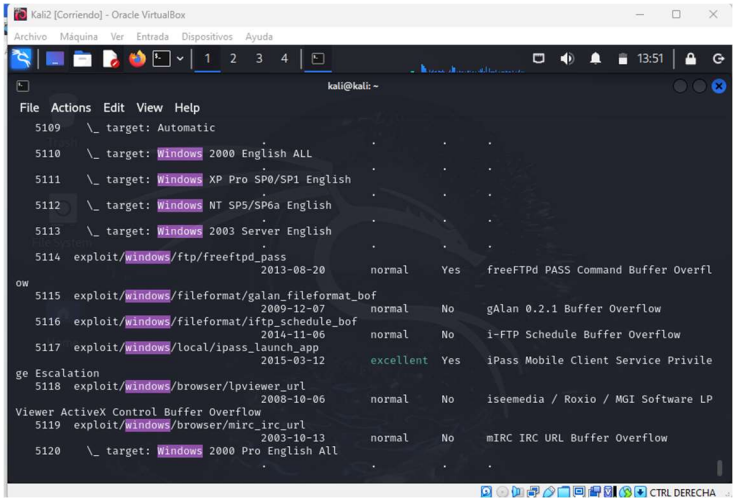


Fuente. Elaboración propia

Con el comando *search windows* podemos encontrar la ruta de los exploit que se encuentran en la maquina:

Figura 5

Ejecución comando search windows

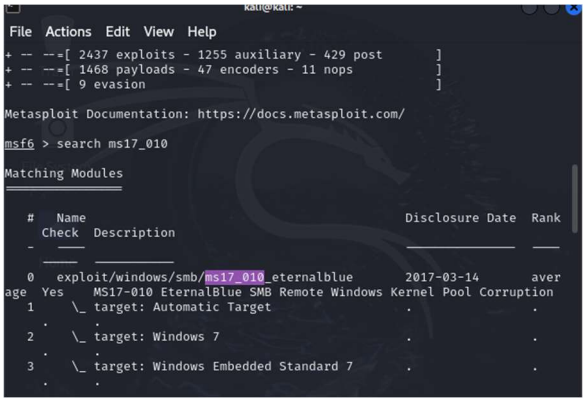


Fuente. Elaboración propia

En una búsqueda avanzada buscamos en exploit ms17_010_eternalblue con el comando *search ms17_010*:

Figura 6.

Busqueda exploit ms17_010_eternalblue

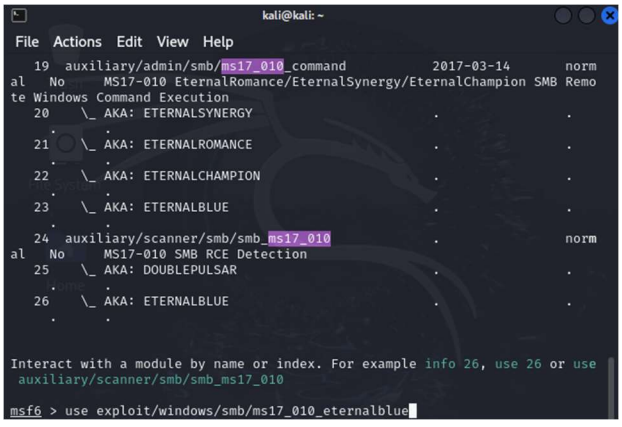


Fuente. Elaboración propia

Seleccionamos el exploit con el comando *use exploit/windows/smb/ms17_010_eternalblue*

Figura 7

Selección exploit exploit/Windows/smb/ms17_010_eternalblue

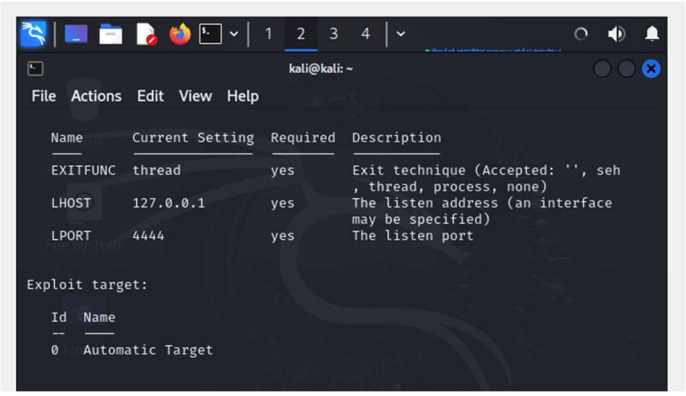


Fuente. Elaboración propia

Con el comando *show options* podemos visualizar las opciones:

Figura 8

Ejecución comando show



Fuente. Elaboración propia

Una vez entro del sploit procedemos a cambiar dos parámetros RHOST y LHOST. Para modificar el parámetro RHOST utilizamos el comando *set LHOST* en este punto colocamos la dirección IP de la maquina a atacar, en este caso 192.168.1.3

Figura 9

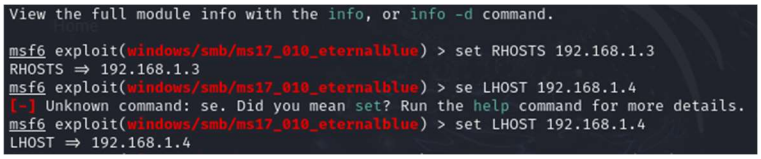
Modificación RHOSTS

Fuente. Elaboración propia

Con el comando *set LHOST* colocamos la dirección de la maquina local, en este caso la 1921.168.1.4:

Figura 10

Modificicación LHOST

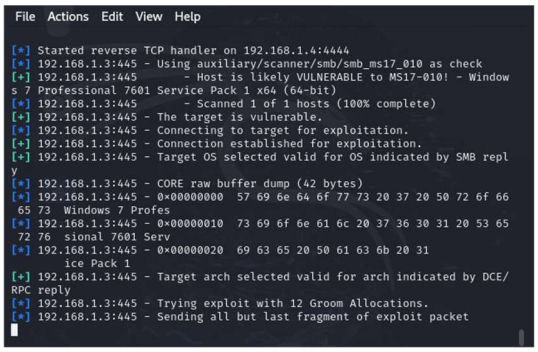


Fuente. Elaboración propia

Luego que tenemos todo configurado escribimos el comando exploit el cual explota la vulnerabilidad, esto nos genera una Shell Reversa y una sesión del meterpreter, ahora estamos en el equipo de la víctima. Ejecutamos el exploit con el comando *exploit* :

Figura 11

Ejecución vulnerabilidad



Fuente. Elaboración propia

Una vez se confirme conexión con la maquina Windows. Se procede a crear el usuario solicitado en el anexo mediante PoC. Para esto utilizamos el siguiente comando: *execute -f cmd.exe -i -H -c -a "/c net user LeonardoCortes 1234 /add"* en el cual LeonardoCortes es el nombre del usuario y el 1234 es la contraseña de la cuenta.

Figura 12

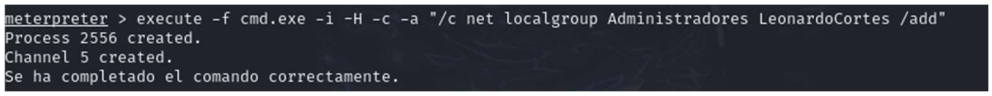
Ejecución comando creación usuario

Fuente. Elaboración propia

El anterior comando, crea el usuario estándar. Para asignarle permisos de administrador utilizamos: *execute -f cmd.exe -i -H -c -a "/c net localgroup Administradores LeonardoCortes /add"*

Figura 13

Ejecucion comando asignación roles administrador

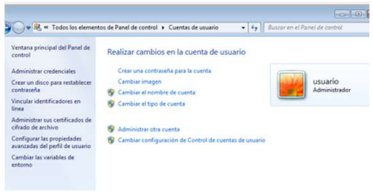


Fuente. Elaboración propia

En las evidencias que se muestran a continuación, evidenciamos el proceso antes y después de crear el usuario:

Figura 14

Evidencia usuarios default



Fuente. Elaboración propia

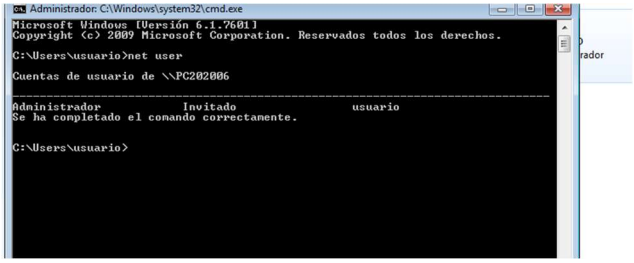
Figura 15

Evidenicia creación usuario Leonardo Cortes

Fuente. Elaboración propia

Figura 16

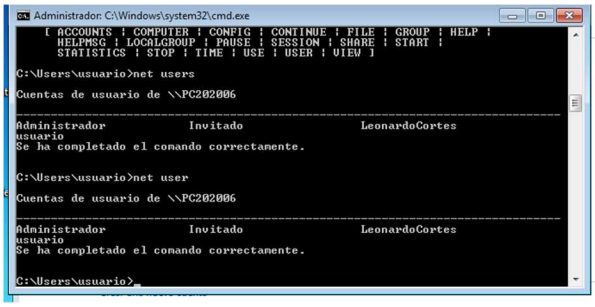
Ejecución comando net user



Fuente. Elaboración propia

Figura 17

Ejecución comando net users con evidencia roles administrador



Fuente. Elaboración propia

De esta manera podemos identificar los pasos que se ejecutaron para llevar a cabo el ataque que del cual se fue víctima por los delincuentes que se aprovecharon de una vulnerabilidad y lograron obtener todo el control de esta máquina Windows 7 X64.

2.3 Contención de ataques informaticos

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

Lo primero es identificar el ataque, las maquinas que están comprometidas, las maquinas que pueden verse afectadas y poder aislarlas de inmediato. Esto con el fin de evitar la propagación y mitigar el impacto en la organización.

De acuerdo con lo anterior, para le proceso de aislamiento se deben desconectar las máquinas de cualquier tipo de red, tanto wifi o cableada. No se deben apagar los equipos, ya que esto podría eliminar evidencia volátil crucial, como procesos en ejecución o conexiones activas. La máquina debe permanecer encendida, pero sin conexión a internet, permitiendo así un análisis posterior de la memoria y del tráfico de red.

Una vez aislado el sistema, se puede proceder con la recolección de evidenica y análisis en tiempo real. Para ello se puede utilizar la herramienta Wireshark o TCPView, que nos ayudan a validar las conexiones de red, tráfico sospechoso y conexiones a IPS no autorizadas. Para un posterior análisis de registros de sistema se puede utilizar la herramienta Event Viewer, el cual nos puede dar información de intentos de sesión fallidos, ejecución de scripts, entre otros servicios. En la maquina afectada y mediante la opción de services.msc, se pueden evidenciar tareas programadas del ataque.

Se debe garantizar el cambio de credenciales, tanto en las cuentas locales, como en las cuentas de dominio. Esto garantizando protección en filtración de credenciales. Con la información recolectada se debe realizar los informes técnicos y fortalecer las políticas de seguridad de la organización.

Una vez tengamos un informe técnico, y si se requiere la conexión de la maquina en un ambiente controlado, se debe garantizar la instalación de todas las actualizaciones a nivel de Windows. Activación de Firewall.

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

Fortalecer el sistema operativo, garantizando la instalación de las ultimas actualizaciones y parches. Desactivación de servicios como telnet, RDP, entre otros. Activación de firewall de Windows para facilitar el tráfico entrante y saliente, instalación de antivirus y antimalware en las máquinas para un análisis en tiempo real. Se debe validar la instalación de un EDP de control de puertos de los equipos.

Se debe garantizar que las maquinas no cuenten por permisos de administración local, esto de acuerdo con el principio de mínimo de privilegios. Si la organización cuenta con un controlador de dominio, se debe programar auditorias y generar procesos de administración de cuentas, en el cual se especifique vigencia de cada una de las cuentas, políticas de contraseñas, y procesos de desactivación de estas. Se debe implementar MFA a todas alas cuentas de la organización.

A nivel de Red, se segmentaria la red, esto por niveles de confianza o áreas. Se debe implementar un firewall local y perimetral, en el cual se pueda bloquear puertos y protocolos no

utilizados o innecesarios. Por ultimo se debe garantizar el monitoreo con soluciones IDS/IPS para prevenir y detectar actividades maliciosas en la red. Establecer alertas automáticas ante comportamientos anómalos, intentos de acceso no autorizados o cambios de configuraciones críticas.

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

El equipo Blueteam, es el grupo encargado de una defensa proactiva en la organización. Su principal tarea es prevenir detectar y mitigar las amenazas antes de que perjudiquen y causen daño a los activos de la organización. Este equipo realiza las actividades de monitoreo de registros a nivel de sistemas y redes. Implementa los controles y configuraciones a nivel de Firewalls, IPS/IPS, entre otros. Debe garantizar que los equipos de las organizaciones se encuentren con las ultimas actualizaciones de los fabricantes, esto aplica para los equipos de red a nivel de infraestructura. Gestiona las políticas de seguridad y concienciación del personal. Simula ataques defensivos con el fin de validar procedimientos, políticas estén actualizados frente a un ataque real.

Mientras que el equipo de respuesta a incidentes informáticos entra en acción cuando ya ha ocurrido el incidente o ataque informático. Por lo cual este equipo la tarea principal es contener, investigar y en lo posible recuperar los sistemas afectados. Como tareas identifican y clasificación del ataque. Contención de este para evitar la propagación en mas equipos de la organización. Eliminar del malware o vector del ataque, por lo cual es el encargado de la

recuperación de los sistemas y restauración de los servicios que se vieron afectados. Por último, este equipo elabora el informe post incidente y recomendaciones para la organización.

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

Se debe utilizar para establecer, evaluar, reforzar la postura de seguridad de los sistemas y redes de la organización. Se utilizarían estas guías con el fin de configurar sistemas de forma segura, evaluar y mejorar el cumplimiento de estándares, implementar controles de seguridad efectivos y reducir riesgos y mejorar la resiliencia ante ataques.

Adicional, con estas guías se puede generar el proceso de auditar configuraciones actuales de los sistemas e implementar controles técnicos, aplicar configuraciones seguras en los equipos de la organización y estandarizar la seguridad en todos los dispositivos.
Estas implementaciones nos ayudan a reducir la probabilidad de incidentes y mejorar la capacidad de detección y respuesta mediante registros y controles de acceso.

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

Un SIEM – Security Information and Event Management, es una herramienta la cual permite recopilar, analizar, visualizar y correlacionar y visualizar eventos de ciberseguridad, generados por diferentes dispositivos dentro de una infraestructura IT como lo son; Firewall, servidores, etc.

Entre las funciones de un SIEM encontramos por parte del cumplimiento normativo la ayuda para cumplir con las regulaciones ISO 27001 PCI-DSS entre otras, esto ayudando a mantener los registros detallados y trazabilidad de eventos. Centraliza los logs de múltiples

dispositivos, lo que permite tener una visión unificada de la actividad en toda la red. Analiza todos los eventos recopilados para la identificación de patrones maliciosos lo que nombramos la correlación de eventos. Utiliza reglas y análisis de comportamiento para la detección de incidentes de seguridad en tiempo real, la cual se puede integrar con inteligencia de amenazas, lo cual ayuda para la identificación de IPs maliciosas, malware conocidos entre otros.
Adicional, permite la configuración de alertas automáticas, las cuales se pueden configurar por corros, dashboards o otros sistemas los cuales envían la notificación una vez se detectan comportamientos anómalos o incluso violaciones de políticas. Ofrece la opción de dashboards interactivos, en los cuales se pueden personalizar los reportes para monitorear el estado de seguridad en tiempo real.

En las características de un SIEM encontramos:
Centralización, la cual unifica los registros de múltiples fuentes en un solo lugar.
Escalabilidad, lo que permite adaptarse a infraestructuras pequeñas o grandes.
Automatización, Automatiza la detección y respuesta a los incidentes.
Integración, permite conectar con otros sistemas de seguridad como EDR, Firewall, etc.
Personalización lo que permite definir reglas, alertas y reportes según las necesidades del negocio.

2.3.5 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.

pfSense: Es una distribución basada en FreeBSD que actúa como un firewall y router de nivel empresarial. Es ampliamente utilizada por organizaciones que buscan una solución robusta

y gratuita para proteger su red. Puede actuar como un punto de control centralizado para contener amenazas antes de que lleguen a los sistemas internos.

Capacidades de contención:

Bloqueo de IPs maliciosas en tiempo real.

Segmentación de red mediante VLANs y reglas de acceso.

Limitación de ancho de banda para mitigar ataques de denegación de servicio (DoS).

VPN segura para aislar accesos remotos.

Integración con Snort o Suricata para contención automática basada en detección de amenazas.

Wazuh: Es una plataforma de seguridad que combina capacidades de SIEM, HIDS (Host-based Intrusion Detection System) y EDR. Aunque su enfoque principal es la detección, permite ejecutar acciones de contención automatizadas. Permite contener amenazas directamente desde el agente instalado en el endpoint, sin necesidad de intervención manual inmediata.

Capacidades de contención:

Bloqueo de procesos maliciosos mediante scripts personalizados.

Aislamiento de endpoints al detectar comportamientos anómalos.

Desactivación de cuentas comprometidas automáticamente.

Control de dispositivos USB y ejecución de comandos remotos para detener amenazas.

Permite contener amenazas directamente desde el agente instalado en el endpoint, sin necesidad de intervención manual inmediata.

Cisco Identity Services Engine (ISE) – NAC: Cisco ISE es una solución de Network Access Control (NAC) que permite definir políticas de acceso dinámicas basadas en la identidad, el estado del dispositivo y su comportamiento. Permite contener amenazas desde el punto de entrada a la red, evitando que dispositivos comprometidos interactúen con recursos críticos.

Capacidades de contención:

Poner en cuarentena dispositivos sospechosos automáticamente.

Desconectar dispositivos no autorizados o que no cumplan con políticas de seguridad.

Aplicar políticas de acceso diferenciadas según el nivel de riesgo del dispositivo.

Integración con soluciones de detección para actuar en tiempo real ante amenazas.

2.4 Socialización Informe Tecnico

2.4.1 Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam.

El desarrollo de estrategias para equipos Red Team y Blue Team requiere un enfoque integral que combine técnicas ofensivas y defensivas con una planificación táctica clara. El Red Team debe diseñar estrategias basadas en la emulación de amenazas reales, utilizando técnicas como el reconocimiento pasivo, explotación de vulnerabilidades, movimientos laterales y persistencia, apoyándose en herramientas como Cobalt Strike o Metasploit. Estas acciones deben estar alineadas con objetivos específicos, como evaluar la resiliencia de los sistemas o probar la respuesta ante incidentes. Por otro lado, el Blue Team debe implementar estrategias centradas en la visibilidad y la respuesta, como el despliegue de sistemas SIEM, la creación de reglas de detección personalizadas, el análisis de comportamiento y la gestión de vulnerabilidades. Además, ambos equipos deben colaborar bajo un enfoque Purple Team, donde se diseñan ejercicios coordinados que permiten ajustar las defensas en tiempo real, mejorar la detección y fortalecer la postura de seguridad organizacional. Esta sinergia estratégica no solo mejora la preparación ante ataques reales, sino que también promueve una cultura de ciberseguridad continua y adaptativa.

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

Para fortalecer la seguridad en una organización, es fundamental plantear estrategias integrales que aborden tanto aspectos técnicos como humanos. Se recomienda iniciar con una evaluación de riesgos para identificar activos críticos y posibles vulnerabilidades, seguido de la implementación de una defensa en profundidad que combine controles perimetrales, internos y de monitoreo. La gestión de identidades debe basarse en el principio de mínimo privilegio y autenticación multifactor, mientras que la actualización constante de sistemas y parches reduce la exposición a amenazas conocidas. La capacitación continua del personal en buenas prácticas de ciberseguridad es clave para mitigar errores humanos, y debe complementarse con políticas claras y planes de respuesta a incidentes bien definidos. Además, realizar pruebas de penetración y ejercicios de Red Teaming permite evaluar la efectividad de las defensas, y la colaboración entre equipos técnicos y administrativos asegura una cultura de seguridad sólida y sostenible.

Conclusiones

A través del laboratorio controlado, se logró simular un ataque real y aplicar técnicas de intrusión, lo que fortaleció las habilidades técnicas en herramientas como Nmap, Metasploit y VirtualBox.

Se evidenció la necesidad de actuar bajo principios éticos y legales, especialmente en contextos donde se manejan datos sensibles y se ejecutan pruebas de seguridad. La identificación de cláusulas ilegales en contratos refuerza la importancia de la revisión jurídica en entornos corporativos.

La implementación de medidas de hardening, segmentación de red, monitoreo con SIEM y políticas de seguridad robustas son esenciales para prevenir y contener amenazas.

Recomendaciones

Fomentar la colaboración entre Red Team y Blue Team para mejorar continuamente las defensas mediante ejercicios coordinados y retroalimentación mutua.

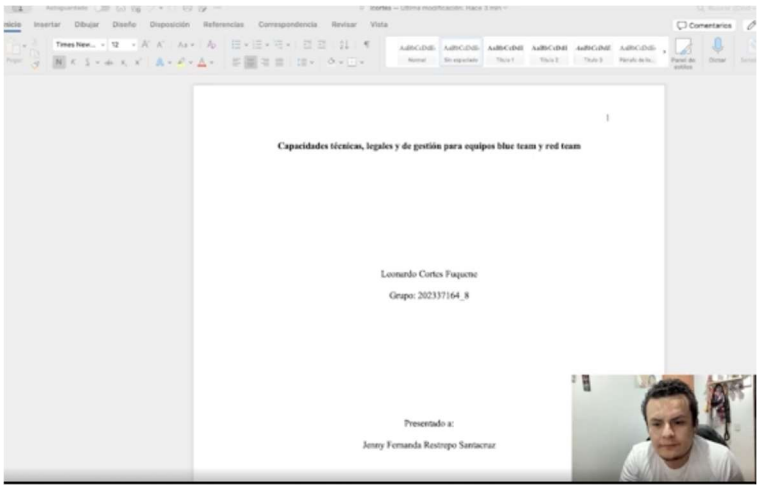
Garantizar que todos los sistemas operativos y aplicaciones cuenten con las últimas actualizaciones de seguridad para reducir la superficie de ataque.

Capacitar continuamente al personal en buenas prácticas, concienciación sobre amenazas y procedimientos de respuesta ante incidentes.

Asegurar que los acuerdos laborales y de confidencialidad estén alineados con la legislación vigente y los principios éticos, evitando cláusulas que comprometan la integridad de los empleados.

Enlace video sustentación

https://youtu.be/WptqdP1-CwQ



Referencias Bibliográficas

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.
https://www.wiley.com/en-us/Security+Engineering

Bejtlich, R. (2013). The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press.
https://nostarch.com/nsm

Cole, E. (2017). Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization. Syngress.
https://www.amazon.com/Advanced-Persistent-Threat

Conklin, A., White, G., Williams, D., Davis, R., & Cothren, C. (2018). Principles of Computer Security: CompTIA Security+ and Beyond (5th ed.). McGraw-Hill Education.
https://www.amazon.com/Principles-Computer-Security

Grimes, R. A. (2017). Hacking the Hacker: Learn from the Experts Who Take Down Hackers. Wiley.
https://www.wiley.com/en-us/Hacking-the-Hacker

Harris, S. (2019). CISSP All-in-One Exam Guide (8th ed.). McGraw-Hill Education. https://www.amazon.com/CISSP-All-One-Guide

ISO/IEC. (2018). ISO/IEC 27001:2018 - Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization. https://www.iso.org/standard/73906.html

Ley 1273 de 2009. Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – la protección de la información y de los datos – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. Diario Oficial No. 47.426. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Northcutt, S., & Novak, J. (2002). Network Intrusion Detection (3rd ed.). New Riders. https://www.amazon.com/Network-Intrusion-Detection

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/94/final

SANS Institute. (2021). Blue Team Operations: Defensive Techniques and Tools.

https://www.sans.org

Skoudis, E., & Liston, T. (2006). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (2nd ed.). Prentice Hall. https://eu.pearson.com/counter-hack-reloaded

Stewart, J. M., Chapple, M., & Gibson, D. (2021). CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide (9th ed.). Wiley. https://www.wiley.com/en-us/ISC2-CISSP

Zeltser, L. (2020). Digital Forensics and Incident Response: A Practical Guide to Deploying Digital Forensic Solutions. Packt Publishing. https://www.packtpub.com/en-us/product/digital-forensics-and-incident-response