Capacidades Técnicas, Legales y de Gestión Para Equipos Blue Team y Red Team

Alvaro Ivan Vasquez Tovar

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería - ECBTI

Especialización En Seguridad Informática

2024

Resumen

Este trabajo aborda el fortalecimiento de las capacidades técnicas, legales y de gestión de los equipos Blue Team y Red Team en el ámbito de la ciberseguridad. Se examina la legislación colombiana relevante, las estrategias de análisis de riesgos y la evaluación de vulnerabilidades en infraestructuras TI teniendo en cuenta el desarrollo del seminario especializado.

***Palabras clave*:** Ciberseguridad, Pentesting, Hardenización, Vulnerabilidades, Exploit.

Abstract

This work addresses the strengthening of the technical, legal, and management capacities of Blue Team and Red Team in the field of cybersecurity. It examines relevant Colombian legislation, risk analysis strategies, and vulnerability assessment in IT infrastructures.

Keywords**:** Cybersecurity, Pentesting, Hardening, Vulnerabilities, Exploit.

Tabla de Contenido

Lista de Ilustraciones

Glosario

Ciberdelincuente: Persona que utiliza sus conocimientos para cometer delitos informáticos.

CVE: Identificador único asignado a las vulnerabilidades.

Equipos Azules (Blue Teams): Equipos diseñados para la prevención y defensa de ataques cibernéticos.

Equipos Rojos (Red Teams): Equipos diseñados para realizar pruebas de ataques cibernéticos controlados.

TI: Tecnología de la información

Monitoreo Continuo: Proceso de supervisión constante de la red y los sistemas para detectar actividades sospechosas o no autorizadas.

IDS/IPS (Intrusion Detection System/Intrusion Prevention System): Sistemas utilizados para detectar y prevenir intrusiones en la red. IDS detecta y alerta sobre posibles intrusiones, mientras que IPS puede bloquearlas automáticamente.

Análisis de Vulnerabilidades: Evaluación sistemática de los sistemas para identificar y clasificar las vulnerabilidades de seguridad.

Gestión de Parches: Proceso de actualización de software para corregir vulnerabilidades y mejorar la seguridad.

Respuesta a Incidentes: Conjunto de procedimientos y acciones para manejar y mitigar los efectos de un incidente de seguridad.

Pruebas de Penetración: Simulaciones controladas de ataques cibernéticos para identificar y explotar vulnerabilidades en los sistemas.

Ingeniería Social: Técnica utilizada para manipular a las personas y obtener información confidencial mediante engaños.

Simulación de Ataques: Proceso de recrear ataques cibernéticos reales para evaluar la efectividad de las defensas de seguridad.

Explotación de Vulnerabilidades: Uso de técnicas y herramientas para aprovechar las debilidades en los sistemas y obtener acceso no autorizado.

Cumplimiento Normativo: Asegurarse de que todas las actividades de seguridad cumplan con las leyes y regulaciones aplicables.

Protección de Datos: Implementación de políticas y procedimientos para proteger la información personal y sensible.

Introducción

En el contexto de la ciberseguridad moderna y como en el desarrollo de este seminario especializado bajo los supuestos en relación con la empresa ficticia “CyberFort Technologies”, la protección de la información y las infraestructuras tecnológica es crucial para las organizaciones. Este informe técnico examina las capacidades técnicas, legales y de gestión necesarias para los equipos Blue Team y Red Team.

El equipo Blue Team se especializa en la defensa proactiva y la mitigación de amenazas, utilizando herramientas y estrategias avanzadas para salvaguardar los sistemas de información. Por su parte, el Red Team lleva a cabo simulaciones de ataques reales para detectar vulnerabilidades y evaluar la efectividad de las defensas implementadas.

Además, este informe aborda la legislación vigente en Colombia sobre protección de datos y delitos informáticos, proporcionando un marco normativo esencial para la operación de estos equipos. Se explorará la metodología ISSAF y herramientas utilizadas en pruebas de penetración (pentesting) y auditorías de seguridad, destacando las mejores prácticas para mantener la integridad, confidencialidad y disponibilidad de la información.

Objetivos

Objetivo General

Fortalecer las capacidades técnicas, legales y de gestión de los equipos Blue Team y Red Team mediante la implementación de estrategias avanzadas de contención, análisis de riesgos y evaluación de vulnerabilidades en la infraestructura TI.

Objetivos Específicos

Reconocer elementos prácticos y legales en el desarrollo de equipos rojos y azules.

Evaluar un acuerdo de confidencialidad según la ley 1273 de 2009 de Colombia y normas éticas profesionales en la práctica de equipos rojos y azules.

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI según el escenario planteado.

Desarrollo del Informe

Leyes y Decretos Colombianos Sobre Delitos Informáticos

Mediante la Ley 1273 de 2009 se establece el bien Jurídico tutelado de la protección de la información y de los datos, así mismo, modifica el código de penal al adicionar el Título VII BIS denominado "De la Protección de la información y de los datos"

Se legisla con relación a:

- Los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos
- Los atentados informáticos y otras infracciones
- Tipificando y estableciendo las sanciones frente a los delitos informáticos, buscando garantizar la protección integral de los sistemas de información y comunicaciones

Por otra parte, existen decretos que buscan establecer normas, métodos y/o procedimientos que regulan y garantizan el uso de las tecnologías de la información y la protección de datos personales:

- Decreto 333 de 2014: Implementado en entidades públicas y privadas.
- Decreto 1078 de 2014: Implementado en entidades del sector Salud.
- Decreto 1702 de 2012: Implementado en la administración pública.

Metodología de Pentesting

Es el proceso por el cual se realizan pruebas de penetración, mediante ataques a diferentes sistemas y entornos con el fin de identificar y prevenir posibles fallos, vulnerabilidades o errores del sistema. Mediante el uso de métodos de penetración se establecen los pasos para realizar dicho pentest. Una de las metodologías es ISSAF en la cual se realiza en 3 etapas y 9 pasos:

Etapa 1. Planeación y preparación: Se realiza el contrato donde se especifiquen las responsabilidades todas las partes interesadas, así como los garantes legales y se establecen lineamientos para la auditoria.

Se establecen alcances, metodologías de trabajos, enfoques de trabajo, rutas de escalamiento, contactos y se aceptan los casos de prueba.

Etapa 2. Evaluación: Cuenta con nueve pasos dentro de la auditoria.

- Recolección de información: Se recolecta toda la información posible sobre el objetivo a auditar, esto puede realizarse a través de medios informáticos públicos o a través de las herramientas dispuestas por la entidad.
- Mapeo de red: Se realiza escaneo de la red, identificando su posible tipología, vulnerabilidades, puertos y servicios expuestos entre otros mediante diversas herramientas para el escaneo de redes.
- Identificación de vulnerabilidades: Mediante el uso de la información recolectada, el auditor valida las vulnerabilidades encontradas y selecciona una de ellas para realizar la explotación, estas vulnerabilidades pueden ser seleccionadas según las publicadas y conocidas como CVE o CERT.
- Penetración: Mediante la explotación de vulnerabilidades y explotación de diversos vectores de ataque se realiza la intrusión logrando el control a mayores niveles jerárquicos. Estas acciones podrán realizarse mediante diversas herramientas o actividades que considere el auditor, de esta forma, encontrar las vulnerabilidades que puedan poner en riesgo a la organización. Por otra parte, cada acción que se realice y cada hallazgo encontrado, deberá ser documentado detalladamente para la toma de decisiones.

- Obtener acceso y escalar privilegios: Mediante los ataques de penetración, ataques de diccionario, ataques de fuerza bruta, configuraciones que permiten ejecución de comandos del sistema, usuarios sin contraseña, entre otros, es posible escalar privilegios gracias a la falta de controles establecidos para la seguridad de la información tales como firewall, IDS/IPS, capacitación al talento humano y algunos otros más, haciendo que la obtención de privilegios como administrador sea más difícil.
- Enumeración: Se pretende encontrar todas las vulnerabilidades del sistema, mediante validación del tráfico de red, correos, cookies de sesión, texto plano o contraseñas cifradas, entre otros.
- Comprometer usuario/sitios remotos: Los diferentes vectores de ataque, puertas traseras y demás hechos de seguridad comprometen la seguridad de la información y dar acceso no autorizados, comprometiendo accesos remotos al sistema y canales de comunicación.
- Mantener acceso: Al obtener resultados exitosos en las intrusiones a los sistemas, es posible dejar accesos ocultos como Back Door, de esta forma se pueden instalar script, rootkits o exploit, entre otros, así, se pueden evidenciar riesgos que podrían ser aprovechados por atacantes externos.
- Cubrir huellas: Para este paso es importante tener en cuenta las condiciones estipuladas inicialmente, si el auditor debe reestablecer el sistema sin ningún tipo de modificación, es importante tener claridad de cada actuación que se realizó para dejar todo en total orden eliminando toda evidencia de los procesos realizados, de lo contrario, el sistema se deja tal cual el resultado de las pruebas realizadas, con el fin de dejar evidencia de estos.

Etapa 3. Reporte, limpieza y destrucción: Se realiza el reporte de las acciones realizadas junto con los hallazgos

ISSAF indica que se deben reportar los incidentes inmediatamente se presentan de forma verbal y escrita, con el fin de analizar el impacto que podría tener en el sistema y tomar decisiones de las acciones para mitigarlos.

Es importante que todo sea debidamente documentado, de esta forma, en el informe final estarán consignadas cada uno de los hallazgos y las recomendaciones realizadas, así como plasmar las herramientas utilizadas y los tiempos de ejecución en cada una de las pruebas realizadas.

Un ejemplo de herramientas usadas en el pentesting es Metasploit, la cual permite poner a prueba las diferentes vulnerabilidades que puedan tener los sistemas informáticos y lo hace por medio de las siguientes funciones:

- Escaneo y recopilación de información: Metasploit utiliza herramientas como nmap para realizar el escaneo de puertos e identificación de puertas de entrada a los sistemas
- Identificación y explotación de vulnerabilidades: Identifica que vulnerabilidades están presentes en un sistema y que están publicadas en CVE, de esta menara identifica como explotar dicha vulnerabilidad.
- Escalada de privilegios: Cuenta con software que permite la elevación de privilegios como administrador en diferentes sistemas operativos tales como Linux y Windows.
- Instalación de puertas traseras: Basado en códigos maliciosos o payloads, instala puertas traseras o backdoors en el equipo víctima, para poder robar información confidencial.
- Fuzzing: Automatiza el ingreso de valores aleatorios que pueden ser inesperados o erróneos en la entrada de los sistemas con el fin de identificar fallos que permitan el ingreso a un dispositivo o red.

- Evasión de sistemas antivirus: Metasploit contiene herramientas que permite la ofuscación de código o escribir código malicioso que no le permite al sistema de defensa ser detectado.
- Eliminación de registros de rastros: Con sus herramientas permite la eliminación de registros o rastros en los logs de los sistemas operativos impactados.

Definición de Herramientas y Servicios en Línea de Ciberseguridad.

Herramientas:

Metasploit. es un Software de código abierto u open source, que viene instalado en los sistemas Kali Linux y que contiene más de 900 exploit. Esta es de las herramientas que más se utiliza dentro del hacking ético o de equipos rojos. Este permite poner a prueba las diferentes vulnerabilidades que puedan tener los sistemas informáticos y lo hace por medio de las siguientes funciones:

- Escaneo y recopilación de información: Metasploit utiliza herramientas como nmap para realizar el escaneo de puertos e identificación de puertas de entrada a los sistemas
- Identificación y explotación de vulnerabilidades: Identifica que vulnerabilidades están presentes en un sistema y que están publicadas en CVE, de esta menara identifica como explotar dicha vulnerabilidad.
- Escalada de privilegios: Cuenta con software que permite la elevación de privilegios como administrador en diferentes sistemas operativos tales como Linux y Windows.
- Instalación de puertas traseras: Basado en códigos maliciosos o payloads, instala puertas traseras o backdoors en el equipo víctima, para poder robar información confidencial.

- Fuzzing: Automatiza el ingreso de valores aleatorios que pueden ser inesperados o erróneos en la entrada de los sistemas con el fin de identificar fallos que permitan el ingreso a un dispositivo o red.
- Evasión de sistemas antivirus: Metasploit contiene herramientas que permite la ofuscación de código o escribir código malicioso que no le permite al sistema de defensa ser detectado.
- Eliminación de registros de rastros: Con sus herramientas permite la eliminación de registros o rastros en los logs de los sistemas operativos impactados.

Nmap. es una herramienta de auditoría de seguridad y exploración de red de código abierto. Mediante el uso de paquetes IP en su forma original permite identificar qué equipo están disponibles en la red, los servicios y sus versiones presentes, sistemas operativos y sus versiones, cortafuegos y filtros de paquetes, escaneo de vulnerabilidades y diversas más características.

Entre los resultados obtenidos podemos encontrar listas de puertos y protocolos con sus servicios y estados con las versiones de cada uno de ellos. De igual forma, llega a mostrar nombres de DNS, direcciones de MAC y tipos de dispositivos.

Nmap Permite:

- Especificar objetivos como escanear un IP especifica, parte de una red, segmentos o la red completa mediante el método CIDR y el uso de diversos comandos.

- Analizar 65535 puertos, entre los que encontramos más de 1660 puertos TCP y cada uno de sus 6 estados, permitiendo obtener información confiable y precisa de su estado.

- A los atacantes identificar las vulnerabilidades de los puertos y servicios presentes en cada uno de los equipos activos en la red gracias a su capacidad de detección de versiones y detalle en cada equipo.

- analiza más de 1500 huellas resguardadas en sus bases de datos para identificar los sistemas operativos, las cuales son comparadas con los resultados arrojados de paquetes TCP y UDP en el escaneo.

Por otra parte, mediante el uso avanzado y la experiencia en Nmap, es posible evadir cortafuegos e IDS, ya que los usos básicos ya están filtrados o bloqueados por algunos sistemas, haciendo más difícil realizar el análisis de la red.

OpenVAS (Open Vulnerability Assessment Scanner). es una herramienta de código abierto diseñada para evaluar y corregir debilidades de seguridad en infraestructuras tecnológicas al identificar y gestionar vulnerabilidades de seguridad de los sistemas y redes minimizando los riesgos.

Gracias a su excelente interfaz gráfica, a más de 50mil test y datos de vulnerabilidades actualizadas diariamente por la comunidad, expertos y la misma empresa permite:

- Realizar pruebas autenticadas.
- Realizar pruebas no autenticadas.
- Ejecutar protocolos de internet de bajo y alto nivel, así como protocolos industriales.
- Ajustar exploraciones de rendimientos personalizados a gran escala.
- Implementar cualquier tipo de prueba de vulnerabilidad.

OpenVAS cuenta con excelente documentación junto con una gran comunidad por foros y en la web, que brinda tutoriales y apoyo con la exploración de vulnerabilidades.

Servicios en línea:

ExploitDB. Es una base de datos de shellcodes, exploits, aplicaciones web, vulnerabilidades 0-days, artículos de seguridad, informes de vulnerabilidades y tutoriales que se encuentra en línea la cual es constantemente actualizada y totalmente disponible

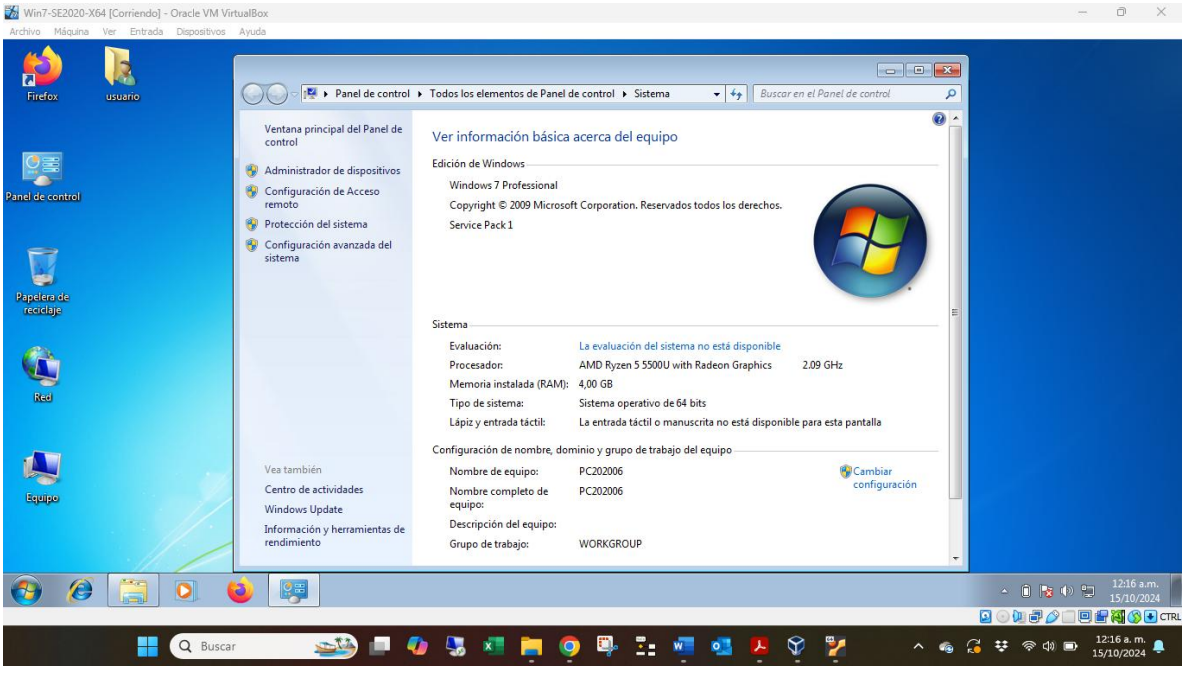
CVE. Lista de vulnerabilidades y exposiciones de seguridad informática divulgadas públicamente en donde se realiza su debida identificación CVE-ID por la corporación MITRE y el Departamento de Seguridad Nacional de EEUU.

Creada como un diccionario estándar de ciberseguridad para identificar y categorizar las vulnerabilidades encontradas por las organizaciones, facilitando la comunicación e intercambio de información entre las diferentes herramientas y organizaciones.

Implementación de Montaje del Banco de Trabajo para evidencia práctica.

Se cuenta con un equipo con procesador AMD Ryzen 5 de 2.09 GHz, 4 GB de RAM, disco duro de 50 GB y SO Windows 7 profesional de 64 bits, el montaje se realiza en la máquina virtual VirtualBox.

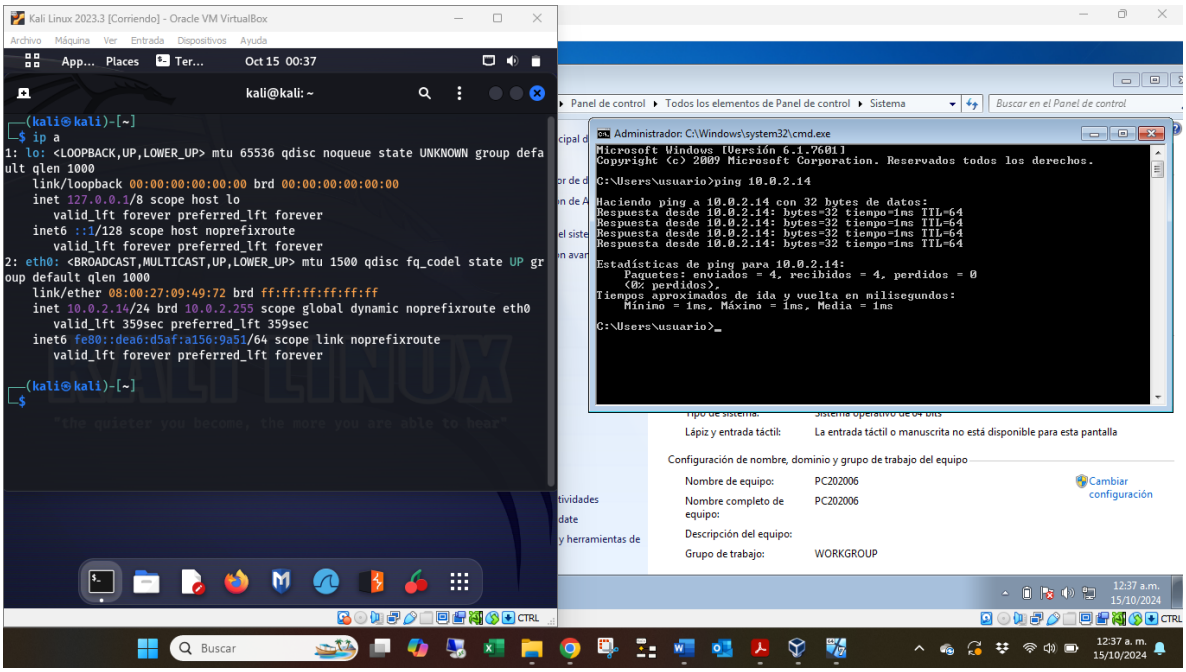
Ilustración 1
Win7-SE2020-X64.ova



Fuente. Propio

Ilustración 2

Ping de Windows 7 a Maquina Kali Linux 10.0.2.14



Fuente. Propio

Situaciones de Procesos Ilegales y No Ético Que Se Pueden Presentar en Acuerdos de Confidencialidad.

Los siguientes textos son parte de un acuerdo de confidencialidad en donde existen diversos procesos y obligaciones que están en contra de la ley y la ética profesional.

- Se obliga a no divulgar directa, indirecta… la información confidencial o sobre procesos ilegales dentro de CyberFort Technologies no podrán ser divulgados.
- Información Confidencial: Cualquier información societaria, técnica… datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.
- No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

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

Artículos De La Ley 1273 de 2009 Que Se Podrían Vulnerar Según las Situaciones Anteriores.

- "se obliga a no divulgar directa, indirecta… la información confidencial o sobre procesos ilegales dentro de CyberFort Technologies no podrán ser divulgados." La NO divulgación de procesos ilegales evidenciados, convierte a la parte receptora en cómplice de incurrir en actos penalizados en la ley 1273 de 2009 (en uno o todos sus artículos), así como faltar a los principios éticos de trasparencia, responsabilidad e integridad establecidos por el COPNIA.
- "Información Confidencial: Cualquier información societaria, técnica… datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos" Aunque esta información si es confidencial, se podría presentar que la información obtenida no sea de propiedad de la empresa y el tener conocimiento que posiblemente ha sido obtenida de forma ilegal y no dar aviso del posible acto delictivo, convierte al receptor en cómplice de incurrir en actos penalizados en la ley 1273 de 2009 (Artículo 269A Acceso abusivo a un sistema informático, Artículo 269C Interceptación de datos informáticos, Artículo 269E Uso de software malicioso para la obtención de la información, Artículo 269F Violación de datos personales, Artículo 269G Suplantación de sitios web para capturar datos personales, Artículo 269I Hurto por medios informáticos y semejantes), así como faltar a los principios éticos de trasparencia, responsabilidad e integridad establecidos por el COPNIA, aunque no haya participado en la obtención de los datos.

- “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.” Esta obligaría al Receptor a incurrir en la violación de la ley 1273 de 2009 (Artículo 269A Acceso abusivo a un sistema informático, Artículo 269C Interceptación de datos informáticos, Artículo 269E Uso de software malicioso para la obtención de la información, Artículo 269F Violación de datos personales, Artículo 269I Hurto por medios informáticos y semejantes), así como la ley 1581 de 2012 y faltar a los principios éticos de trasparencia, responsabilidad e integridad establecidos por el COPNIA.
- “Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.” La NO denuncia la información ilegal, convierte a la parte receptora en cómplice de incurrir en actos penalizados en la ley 1273 de 2009 (en uno o todos sus artículos), así como faltar a los principios éticos de trasparencia, responsabilidad e integridad establecidos por el COPNIA.

Tomar acciones ante delitos informáticos establecidos en la ley 1273 de 2009 y la ley 1581 de 2012 hace parte del actuar ético como ingeniero.

¿Se Recomendaría Firmar Un Acuerdo Bajo Las Anteriores Condiciones?

No es recomendable aplicar a un trabajo bajo las anteriores condiciones, teniendo en cuenta que sus cláusulas van en contra de los principios éticos profesionales establecidos en el COPNIA de trasparencia, responsabilidad e integridad al pretender prohibir las denuncias de procesos y/o situaciones ilegales que se evidencien.

Artículos de ley 842 de 2003 que entran en conflicto con algunas cláusulas son:

- Artículo 15 Sanciona a los profesionales que incurran en prácticas ilícitas.

- Artículo 31 Los ingenieros deben denunciar todo delito y faltas contra el código ético de los que tuviese conocimiento.
- Artículo 35 Denunciar trasgresiones que obliguen a los ingenieros a no respetar las disposiciones legales y éticas profesionales.

Igualmente, algunas de las cláusulas incitan a cometer delitos penalizados en las leyes 1273 de 2009 y 1581 de 2012 las cuales regulan los delitos informáticos en Colombia y exigen NO denunciar dichos actos delictivos.

Análisis Frente a Casos de "Ciberespionaje Y Ética"

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

R/ Las empresas de ciberseguridad no necesariamente deben tener acceso a información sensible de sus clientes en el desarrollo de una auditoria, estaría más orientado a conocer la estructura de la información que se maneja sin acceder a los datos. Por otra parte, es importante realizar acuerdos robustos para restringir el acceso a la información confidencial, especificando claramente responsabilidades y limitaciones, también, es importante establecer controles para el acceso de la información tomando registro de los ingresos y autenticación de multifactor.

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

R/ Establecer roles de jerarquía que garanticen el uso restringido a la información en cada proyecto, implementar políticas y procedimientos que permitan establecer responsables, realizar

auditorías continuas de los trabajos realizados, capacitar continuamente a los especialistas frente al código de ética profesional y leyes, implementar monitoreo para detectar actividades sospechosas en tiempo real, controlar el uso de dispositivos tecnológicos no autorizados.

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

R/ Es importante que los gobiernos y organizaciones, una vez han evidenciado que se han cometido delitos de ciberseguridad, deben:

- Desistir del contrato con la empresa de ciberseguridad.
- Iniciar acciones legales (civiles y penales) en contra del personal y la empresa contratante, así como denunciar ante las autoridades competentes para que realicen las acciones e investigaciones pertinentes.
- Iniciar un estudio o auditoría interna para evaluar las afectaciones e impacto del ataque, así como tomar las medidas correctivas necesarias para prevenir vectores de ataque y puertas trasera abiertas.
- Informar a posibles terceros afectados para prevenir ataques y mayores afectaciones.
- Fortalecer políticas de ciberseguridad que permitan restaurar la confianza de los afectados.
- Fortalecer el monitoreo frente a ataques de ciberseguridad.

Evidencia Practica de Acciones Realizadas Por un Equipo Red Team en Ambiente Controlado.

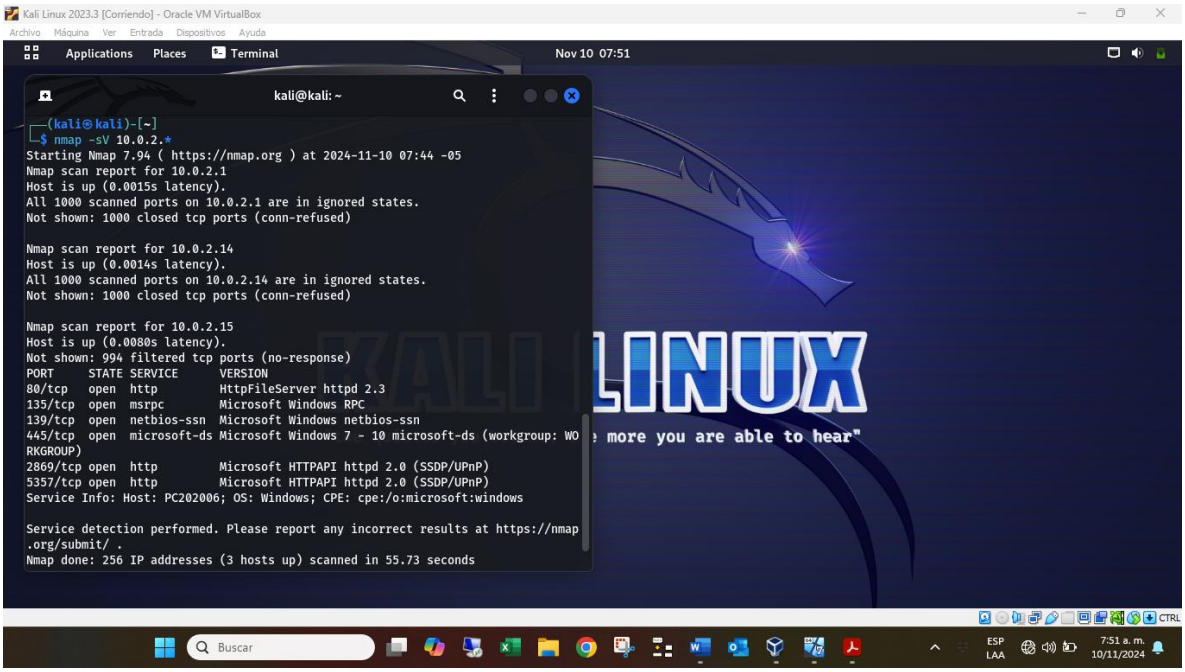
Se realiza el montaje del entorno seguro para la realización de las pruebas (maquina atacante Kali Linux y Maquina Copia del servidor Windows 7).

En el servidor Windows 7 se evidencia la instalación de la aplicación HTTP File Server 2.3 la cual utiliza el puerto 80 para la transferencia de datos.

Una vez iniciadas las maquinas en el mismo entorno de red se realiza escaneo de equipos y versiones de software activos y vulnerables desde Kali Linux mediante la herramienta NMAP con el comando nmap -sV 10.0.2.*

Ilustración 3

Escaneo de red (Equipos y Versiones de Software)



Fuente. Propio

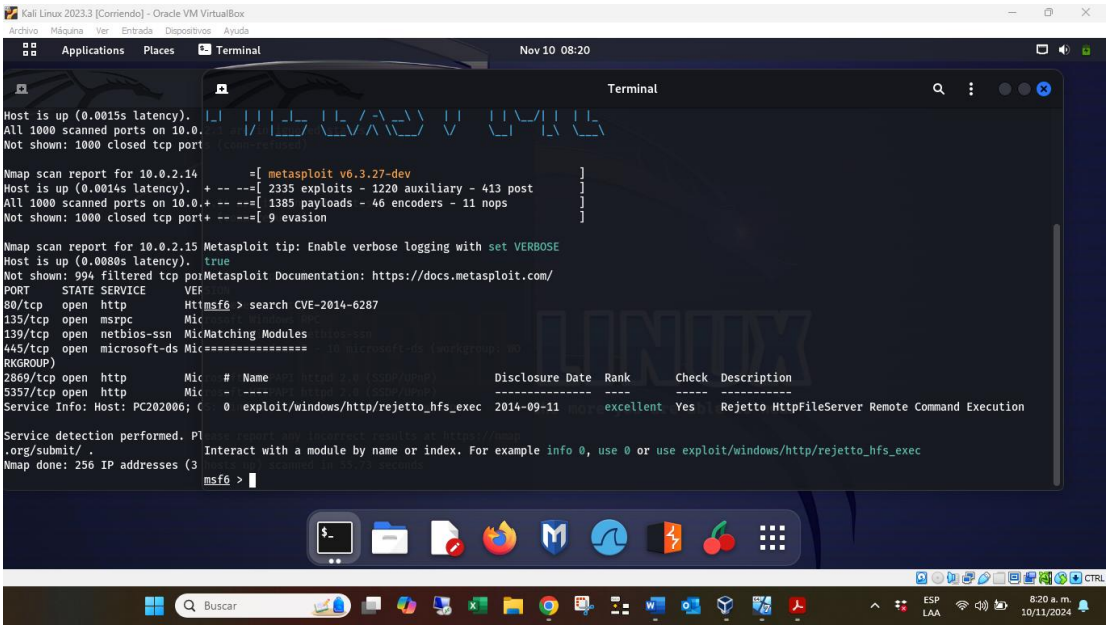
Se evidencia la maquina objetivo con IP 10.0.2.15, la cual cuenta con diversos puertos abiertos los cuales podrían presentar diversas vulnerabilidades. Entre los puertos abiertos se encuentra el puerto 80 con la versión de software “HttpFileServer httpd 2.3”.

Al identificar la versión expuesta se realiza investigación de las posibles vulnerabilidades en la base de datos de cve.mitre.org. Como resultado se encuentra la vulnerabilidad CVE-2014-6287 la cual muestra una vulnerabilidad de ejecución de comando remoto.

Se procede a la búsqueda de Exploit de la vulnerabilidad con el comando “search CVE-2014-6287” en la herramienta Metasploit en Kali Linux.

Ilustración 4

Búsqueda de Exploits CVE-2014-6287



Fuente. Propio

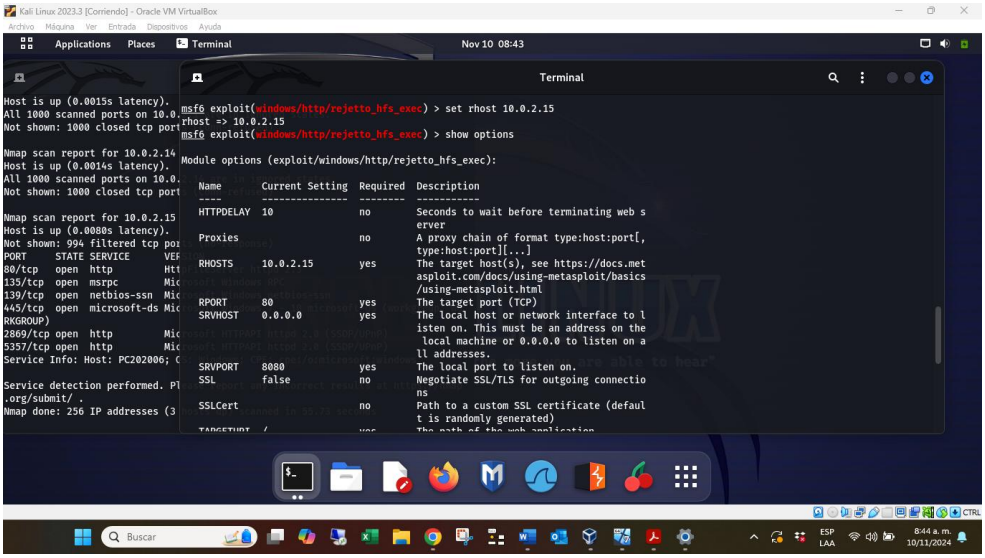
Se evidencia el exploit rejetto_hfs_exec.

Mediante el comando use 0 se realiza la ejecución del exploit.

Seguidamente se realiza la configuración de los parámetros necesarios para iniciar la intrusión mediante el comando set rhost 10.0.2.15, lo cual permite orientar el ataque a la maquina especifica la cual presenta la vulnerabilidad.

Ilustración 5

Configuración para la explotación de vulnerabilidades

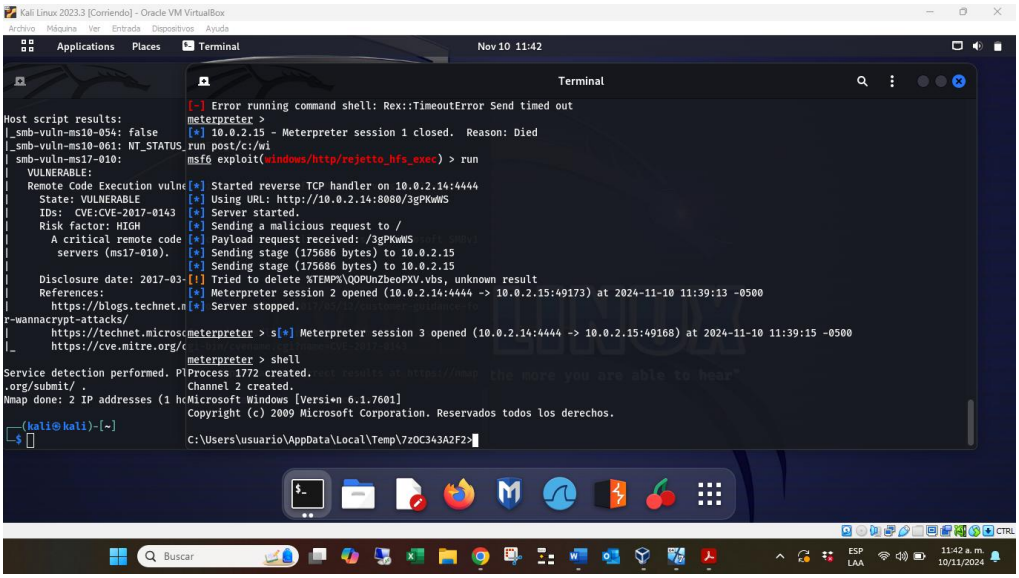


Fuente. Propio

Con el comando “run” se ejecuta el exploit el cual abre una puerta al eludir los filtros de seguridad del servidor HFS para tomar control remoto de la maquina objetivo, posteriormente se ejecuta el comando “shell” para ingresar a modo comandos de Windows 7.

Ilustración 6

Ejecución de exploit y acceso a comandos del sistema Win7

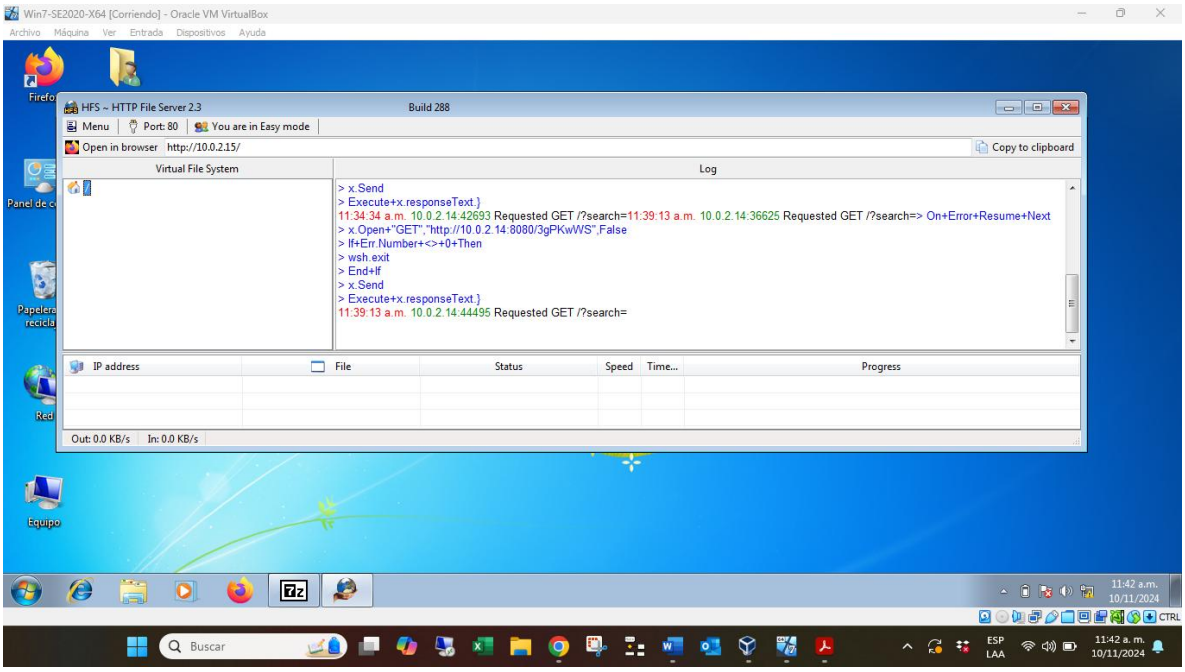


Fuente. Propio

Se toma evidencia de la aplicación HFS (la cual es vulnerable) donde evidencia que el sistema está registrando transferencia de datos y requerimientos por parte de la maquina atacante.

Ilustración 7

Evidencia de transacción de datos en la aplicación HFS



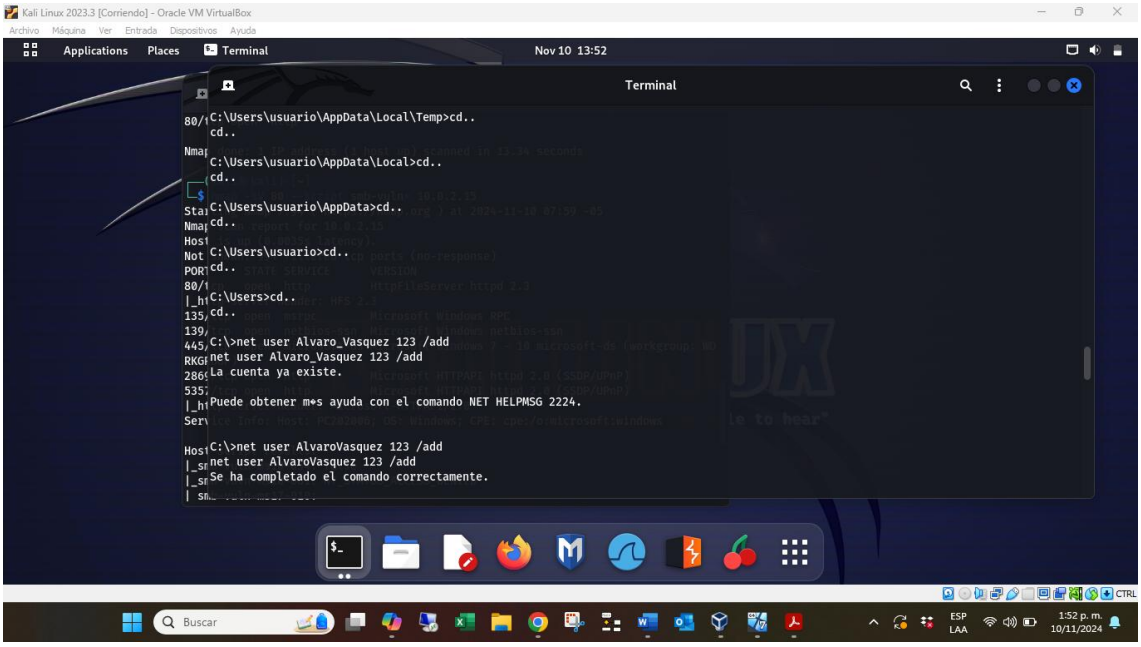
Fuente. Propio

Una vez establecido el control remoto de la maquina objetivo, se evidencia que abre el acceso en la carpeta de Temp Local, ubicada en el disco C.

Mediante el comando “cd..” ejecutado 5 veces llegamos a la raíz del disco “C:” desde donde se realiza la ejecución del comando “net user AlvaroVasquez 123 /add”, el cual permite en la maquina vulnerable crear un usuario del sistema de nombre “AlvaroVasquez” y contraseña “123” conforme siguiente imagen.

Ilustración 8

Ejecución comandos creación nuevo usuario desde maquina atacante

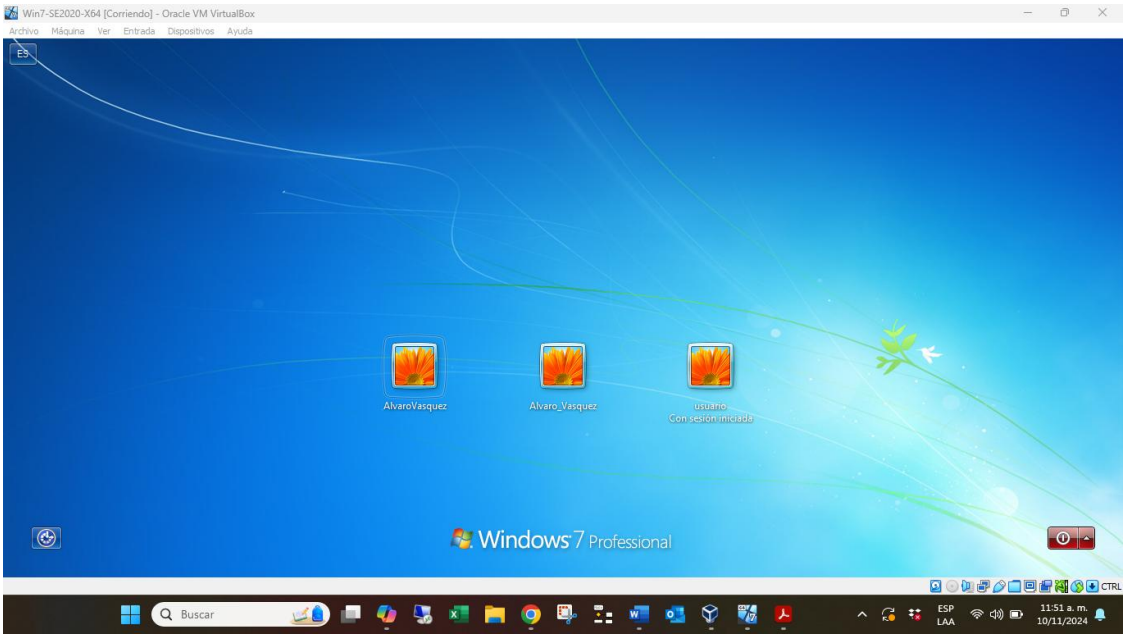


Fuente. Propio

Ahora encontramos evidencia de usuario creado en la maquina Windows 7.

Ilustración 9

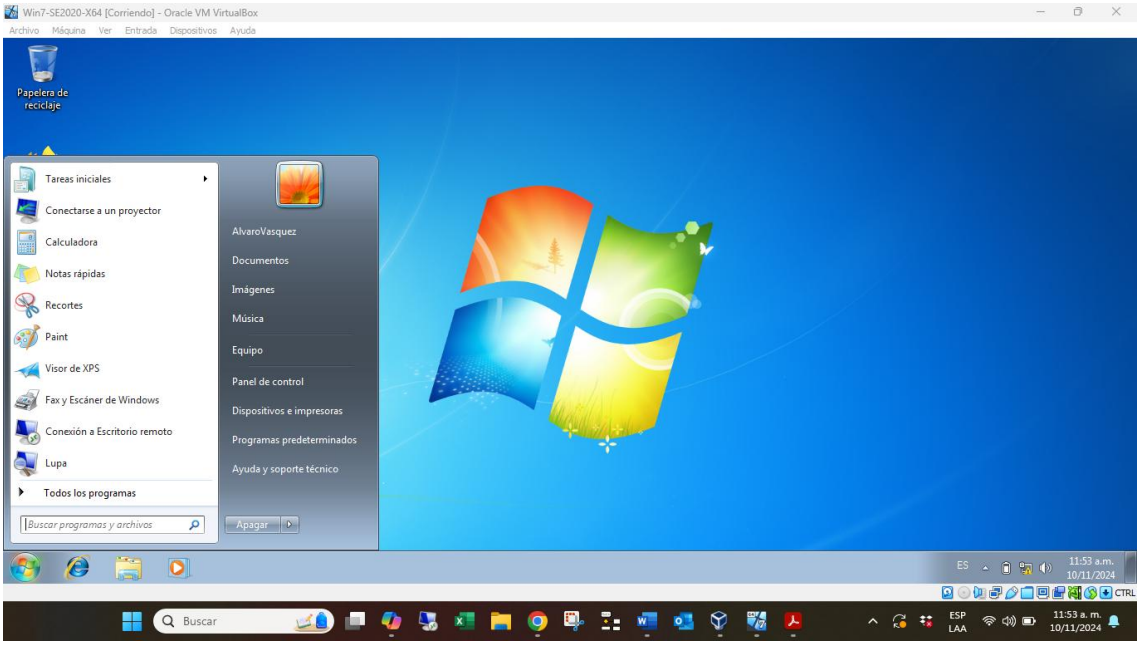
Confirmación creación del usuario en maquina Win7



Fuente. Propio

Ilustración 10

Inicio de sesión nuevo usuario AlvaroVasquez



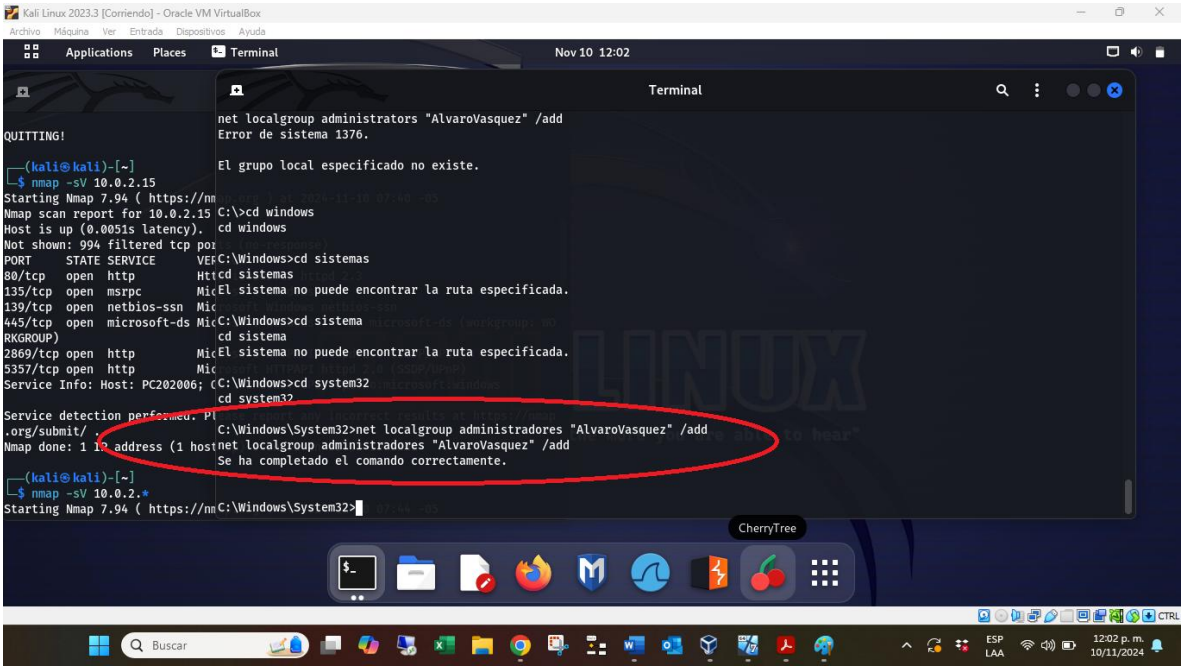
Fuente. Propio

De igual forma, mediante el uso de comandos nos permite ubicarnos en la carpeta de “cd Windows\System32” demostrando que se tiene acceso a cualquier información del sistema.

Adicionalmente, aun más delicado, permite realizar configuración del usuario creado como administrador “net localgroup administradores “AlvaroVasquez” /add” dejando aún más vulnerable la maquina objetivo conforme se evidencia en las siguientes ilustraciones.

Ilustración 11

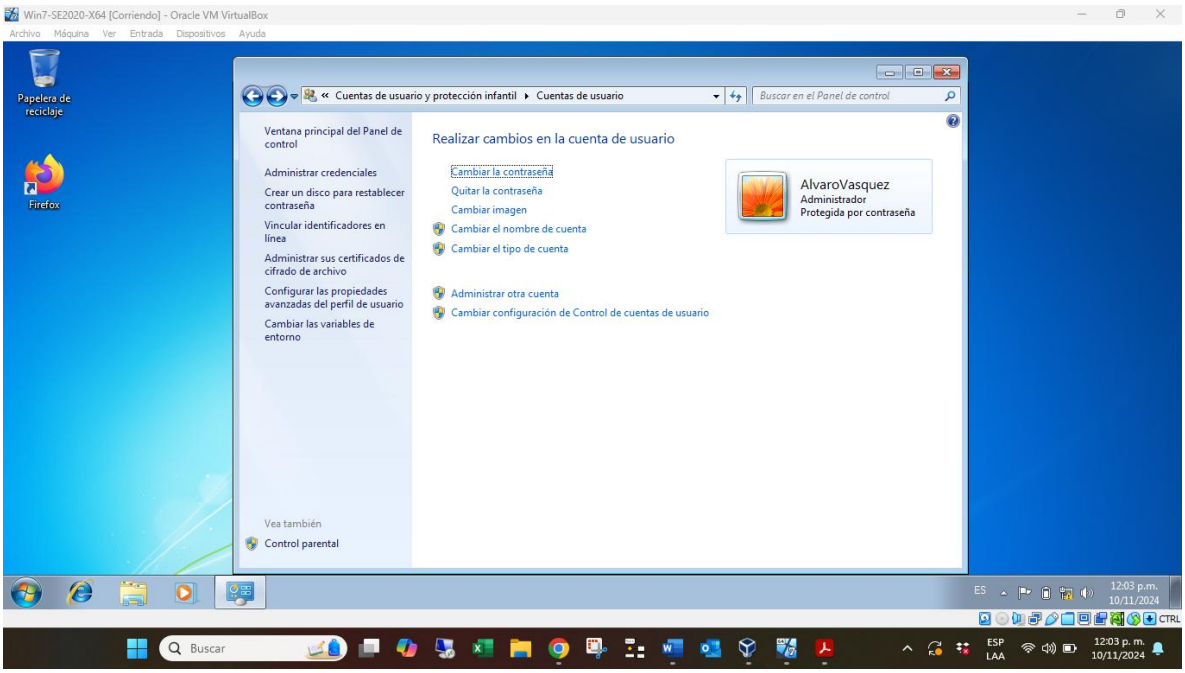
Configuración de usuario AlvaroVasquez como administrador



Fuente. Propio

Ilustración 12

Evidencia usuario AlvaroVasquez administrador maquina Windows 7



Fuente. Propio

Se confirma la intrusión exitosa desde la maquina Kali Linux a la maquina Windows 7 por la aplicación HFS la cual mantiene el puerto 80 abierto para su funcionamiento sin restricciones, permitiendo que se realice creación de usuario y configuración del usuario como administrador evidenciando un alto grado de vulnerabilidad.

Algunos Datos Tenidos en Cuenta Para Identificar Fallas de Seguridad

- La fuga de información que ha sufrido la empresa nos da a entender que existe una o más puertas abiertas por la cual se está accediendo remotamente al equipo.
- La aplicación detectada como vulnerable bajo Windows nos permite validar mediante el escaneo de puertos y versiones de software presentes en el equipo objetivo e investigar las vulnerabilidades según los resultados del escaneo.
- El saber que existe un exploit que permite acceso a través de shell evidencia que es una vulnerabilidad ya conocida e identificable.

Herramienta Utilizada Para Poder Identificar Los Fallos De Seguridad De La "Máquina Windows"

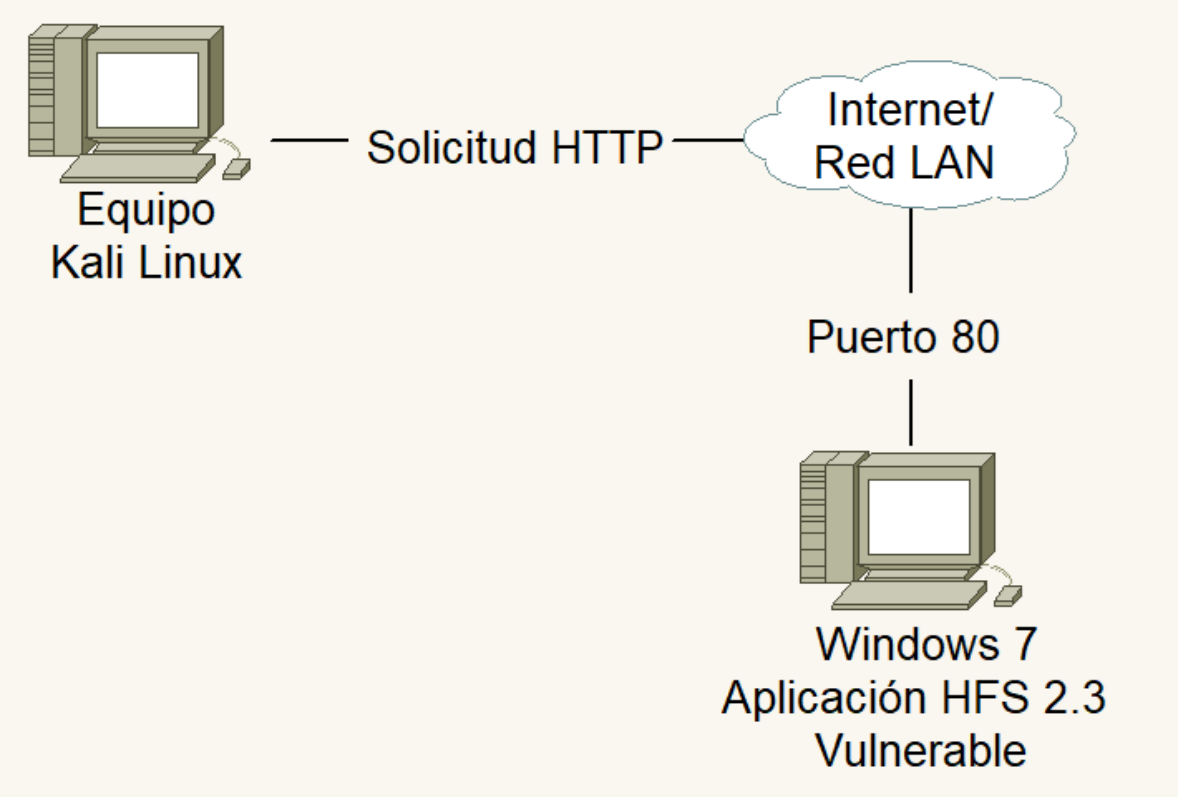
Se utilizó la herramienta NMAP con el comando nmap -sV 10.0.2.*, la cual mostró que en la maquina Windows de IP 10.0.2.15 el puerto 80 se encuentra abierto mediante la versión de software "HttpFileServer httpd 2.3", esto permitió investigar en la base de CVE las posibles vulnerabilidades presentes y el exploit de ataque, logrando de esta forma realizar un ataque exitoso.

Afectación Del Ataque Realizado

Este ataque permite acceder remotamente a símbolo del sistema de Windows desde la maquina atacante y ejecutar diversos comandos afectando la integridad del sistema, de tal forma que podría tener control total del sistema, ataques de denegación de servicio DoS, hurto de información, instalación malwares y daños al sistema a través de eliminación o modificación de archivos críticos.

Ilustración 13

Topología de Red de Ataque



Fuente. Propio

Acciones Por Parte de Blue Teams Frente un Ataque Cibernético en un Ambiente Controlado

Las primeras indagaciones y acciones a realizar durante un ataque informático en tiempo real el cual afecta una maquina Windows 7 son:

- **Identificación del ataque**: Mediante la implementación de herramientas con licencia GPL como Wireskark y Snort, podremos analizar y detectar actividad sospechosa en la red y hacía que host está dirigida.
    - Wireshark permitirá analizar el tráfico de red en tiempo real y de esta forma identificar patrones irregulares evidenciando el ataque.
    - Snort permitirá evidenciar las alertas generadas por el ataque al realizar actividades sospechosas como el escaneo de puertos, intento de explotación de vulnerabilidades y el tráfico malicioso
- **Contención del ataque**: Se procede inmediata al aislamiento de la maquina afectada retirándola de la red de forma física y lógica evitando la propagación del ataque y riesgos adicionales. Adicionalmente se procede por medio de Firewall al bloqueo de IPs y puertos para prevenir más ataques en la red.
- **Análisis Forense**: Con este análisis estableceremos el alcance del ataque, con el uso de herramientas como Autopsy la cual nos permitirá validar registros logs y evidenciar si se ha borrado información, analizar registros y obtener información detallada del sistema atacado, de igual forma, se realiza análisis mediante la herramienta RegRipper la cual también nos permitirá evidencias cuentas de usuarios creadas, cambios en la configuración del sistema y en las políticas de seguridad.

- **Mitigación y Recuperación**: Mediante el uso de la herramienta Autopsy se realizará recuperación de la información comprometida, se eliminarán usuarios creados durante el ataque, se realizará ejecución de antivirus y antivirus y antimalware para eliminar cualquier infección o amenaza que pudiese estar en el sistema, por otra parte, se implementarán nuevas políticas de seguridad con el fin de mitigar los riesgos. De ser necesario se podrá hacer uso de recuperación del sistema mediante el uso de Backup seguro.
- **Implementación de mejora**: Mediante la implementación de OpenVas se realiza escaneo a la red para encontrar y corregir vulnerabilidades en los sistemas, además, se implementarán parches y actualizaciones necesarias para corregir dichas vulnerabilidades junto con capacitación en ciberseguridad a usuarios.
- **Documentación y reporta**: Posterior a un ataque informático es crucial para identificar la causa del ataque, evaluar el impacto, mejorar las estrategias de seguridad, cumplir con normativas y regulaciones, y capacitar al personal para futuros incidentes. Esta documentación proporciona transparencia y se convierte en una herramienta importante para la implementación de mejoras continuas y fortalecer la postura de seguridad de la información.

Diferencias Entre un Equipo Blueteam y un Equipo de Respuesta A Incidentes Informáticos

Un equipo Blue Team se dedica a fortalecer y proteger de manera proactiva la infraestructura de TI mediante la implementación de medidas preventivas y el monitoreo continuo. Utilizan herramientas de detección de intrusiones para identificar y neutralizar amenazas antes de que comprometan la red, también aplican estrategias de endurecimiento de sistemas, asegurando que todas las configuraciones y parches estén actualizados para mitigar

vulnerabilidades conocidas. Este equipo está encargado de realizar pruebas de penetración internas y auditorías de seguridad periódicas para evaluar y mejorar continuamente la seguridad.

Un equipo de Respuesta a Incidentes Informáticos (IR Team) actúa de manera reactiva frente a los incidentes de seguridad. Se enfoca en la contención, erradicación y recuperación de los sistemas comprometidos posterior a un ataque. Utilizan técnicas de análisis forense para investigar la causa y el impacto del ataque, también documentan el incidente y las lecciones aprendidas para mejorar la preparación y respuesta ante futuros ataques asegurando una recuperación rápida y eficaz de los sistemas afectados.

Que Implementar de CIS "Center For Internet Security" Dentro de un Blue Teams

Se recomienda utilizar el Center for Internet Security (CIS) para acceder a los CIS Controls con el fin de implementar las prácticas recomendadas, priorizadas y simplificadas que fortalecerán la seguridad de nuestra infraestructura. Además, emplearía las guías de CIS Benchmarks para aplicar configuraciones específicas que se ajusten a las necesidades de la empresa, asegurando así la protección de nuestros sistemas frente a amenazas cibernéticas.

Por otra parte, implementaría la herramienta CIS-CAT Lite para realizar escaneos y evaluaciones detalladas de la configuración de nuestros sistemas, verificando el cumplimiento con los estándares establecidos en los CIS Benchmarks. Esta herramienta permite identificar y corregir configuraciones inseguras, asegurando que los sistemas cumplan con las mejores prácticas de seguridad cibernética.

Funciones y Características Principales de lo Que es un SIEM

Un Security Information and Event Management (SIEM) tiene como funciones principales la recolección, normalización y análisis de eventos de seguridad provenientes de diferentes fuentes en una red. Permite la correlación de estos eventos para identificar patrones de ataque y generar alertas en tiempo real sobre posibles amenazas. Un SIEM también facilita la investigación forense post-incidente al centralizar los logs y eventos, y proporciona herramientas para el reporte de cumplimiento normativo. En resumen, su principal función es mejorar la capacidad de detección y respuesta ante incidentes de seguridad al consolidar y analizar datos de múltiples fuentes.

Las características principales de un SIEM incluyen la capacidad de integración con diversos dispositivos y aplicaciones para una recolección de logs centralizada, la normalización de datos para facilitar su análisis, y motores de correlación avanzados que permiten identificar actividades sospechosas, también suelen ofrecer dashboards personalizables, herramientas de reporte robustas, y capacidades de respuesta automatizada ante incidentes. La escalabilidad para manejar grandes volúmenes de datos y la capacidad de generar informes detallados para cumplimiento regulatorio también son características cruciales de estas plataformas.

Herramientas de Contención de Ataques Informáticos "Hardware o Software"

- Cisco ASA: Actúa como una barrera entre la red interna y externa, bloqueando tráfico no autorizado basado en reglas predefinidas.
- Cisco Identity Services Engine (ISE): Restringe el acceso a la red solo a dispositivos que cumplen con políticas de seguridad específicas, conteniendo dispositivos no autorizados.

- MikroTik RouterOS: Utiliza técnicas como VLANs para aislar segmentos de la red, limitando la capacidad de propagación de un atacante dentro de la infraestructura de la organización.
- Docker: Usa técnicas como contenedores o micro-segmentación para aislar aplicaciones, evitando que un ataque en una aplicación afecte a otras.

Conclusiones

Como especialistas en ciberseguridad es importante el claro conocimientos y cumplimiento de las leyes y decretos que rigen la seguridad de la información y los datos personales, de tal forma que podamos garantizar un desarrollo ético y profesional con integridad, transparencia y responsabilidad.

El no denunciar actos delictivos, acarrea graves sanciones para quienes las cometen y/o son cómplices de las éstas.

Como especialistas en ciberseguridad evidencio falla de seguridad debido a la no actualización y parcheo de la aplicación HFS 2.3 y la falta de controles en puertos abiertos, toda vez que también se evidencia el puerto 445/tcp abierto el cual presenta vulnerabilidad y permite acceso remoto a los atacantes.

Las vulnerabilidades encontradas son graves, toda vez que exponen la integridad de los sistemas y la información que allí reposa.

La implementación de IPS y políticas de seguridad robustas en firewall, permitirían un mayor control para mitigar ataques exitosos.

Implementar auditorias internar y pruebas de penetración periódicas permitirían encontrar fallas de seguridad anticipándose a los ciberatacantes, logrando corregir las vulnerabilidades encontradas.

Las herramientas de seguridad como los firewalls, sistemas IDS/IPS y el sandboxing son esenciales para detectar y contener amenazas en tiempo real. La combinación de medidas proactivas (como el uso de CIS Controls y CIS Benchmarks) con medidas reactivas (como las herramientas de contención y la respuesta a incidentes) es crucial para mantener una infraestructura segura y resiliente frente a ataques cibernéticos.

Herramientas como CIS-CAT Lite permiten la evaluación continua del cumplimiento de los sistemas con las mejores prácticas de seguridad. Esta evaluación regular es fundamental para identificar y corregir configuraciones inseguras, asegurando que los sistemas se mantengan alineados con los estándares de seguridad reconocidos y protegiendo así contra nuevas amenazas.

Es crucial implementar una estrategia de gestión integral que incluya la identificación, evaluación, priorización y remediación de estas. Utilizar herramientas de escaneo de vulnerabilidades, como Nessus o OpenVAS, permite detectar y evaluar puntos débiles en los sistemas. Una vez identificadas, las vulnerabilidades deben ser priorizadas según su criticidad y el impacto potencial en la organización. La aplicación de parches y actualizaciones de software es una medida esencial para mitigar estas vulnerabilidades. Además, realizar pruebas de penetración regularmente ayuda a asegurar que las medidas de seguridad implementadas sean efectivas y que no haya nuevas vulnerabilidades expuestas. Esta gestión proactiva y continua es fundamental para mantener la integridad y seguridad de los sistemas frente a posibles amenazas.

Recomendaciones

Algunas medidas de Hardenización que se recomiendan implementar frente a el escenario planteado son:

- Actualizar el Software: La vulnerabilidad CVE-2014-6287 permite la ejecución remota de código de comandos, para mitigar este riesgo, es importante actualizar la herramienta a su versión más reciente de HFS, la cual tendrá corregida esta vulnerabilidad.
- Configuración de Seguridad: Configurar las herramientas de transferencia de datos o como en este caso HFS, para restringir el acceso solo a usuarios autorizados y limitar las funciones disponibles al deshabilitar funciones innecesarias, implementar Control de Acceso Basado en Roles para asegurar que solo usuarios autorizados puedan acceso a ciertas funciones y configurar listas de IP para permitir solo conexiones desde direcciones IP de confianza.
- Monitoreo Continuo: Implementar herramientas de monitoreo como OSSEC para la detección de intrusiones en tiempo real, la cual permitirá analizar registros de logs y detectar comportamientos inusuales, permitiendo una respuesta rápida ante cualquier intento de explotación de vulnerabilidades.
- Firewall, Antivirus y Antimalware: Configurar un firewall robusto para filtrar el tráfico en la red. Utilizar un antivirus y Antimalware para escanear y eliminar amenazas potencialmente introducidas durante el ataque.
- Auditoría Regular: Implementar auditorías de seguridad periódicas utilizando herramientas como OpenVAS para identificar y corregir vulnerabilidades.

Otras recomendaciones generales son:

Para el Blue Team, es esencial implementar herramientas de monitoreo y detección de intrusiones como Snort y Suricata, que permiten identificar amenazas en tiempo real. También

deben realizar evaluaciones periódicas de vulnerabilidades utilizando herramientas como OpenVAS y Nmap, además de gestionar los parches de manera efectiva con soluciones como GLPI y OCS Inventory. Además, es crucial desarrollar y practicar planes de respuesta a incidentes, para lo cual herramientas como OSSEC y Wazuh pueden ser muy útiles.

El Red Team debe enfocarse en realizar pruebas de penetración con herramientas como Metasploit y Aircrack-ng, y utilizar técnicas de ingeniería social para evaluar la preparación del personal, empleando herramientas como SET (Social-Engineer Toolkit). También es importante simular ataques reales utilizando plataformas como Kali Linux, que incluye una amplia gama de herramientas de seguridad GPL, y desarrollar exploits personalizados con herramientas como ExploitDB.

En cuanto a las capacidades legales, el Blue Team debe asegurarse de cumplir con todas las leyes y regulaciones locales e internacionales, utilizando herramientas como OpenSCAP. También deben implementar políticas y procedimientos para proteger los datos personales y sensibles, para lo cual herramientas como VeraCrypt pueden ser útiles.

Para la gestión, el Blue Team debe desarrollar una estrategia de seguridad a largo plazo, invertir en la formación continua del personal y fomentar la colaboración entre departamentos. El Red Team debe realizar evaluaciones de riesgos, mantener una comunicación clara con el Blue Team y otros stakeholders, y revisar y actualizar regularmente sus técnicas y herramientas.

Referencias Bibliográficas

GOV.CO, Ley 1273 de 2009, [Online], Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492&form=MG0AV3

OpenWebinars, Qué es Metasploit framework, [Online], Disponible en https://openwebinars.net/blog/que-es-metasploit/

GEEKFLARE, Las 11 mejores herramientas SIEM para proteger a su organización de ciberataques, [Online], Disponible en https://geekflare.com/es/best-siem-solutions/

GEEKSFORGEEKS, OpenVAS : Evaluación de seguridad, [Online], Disponible en https://www.geeksforgeeks.org/security-assessment-openvas/?form=MG0AV3

EXPLOTI DATABASE, Acerca de la base de datos de exploits, [Online], Disponible en https://www.exploit-db.com/about-exploit-db

CIBERSEGURIDAD, ¿Qué es CVE? Explicación de las vulnerabilidades y exposiciones comunes, [Online], Disponible en https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/?form=MG0AV3

IBM, ¿Qué es el marco MITRE ATT&CK?, [Online], Disponible en https://www.ibm.com/es-es/topics/mitre-attack

Policía Nacional, Normatividad sobre delitos informáticos [Online], Disponible en https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos#:~:text=Art%C3%ADculo%20269A%3A%20Acceso%20abusivo%20a,el%20leg%C3%ADtimo%20derecho%20a%20excluirlo

GOV.CO, Ley 1581 de 2012, [Online], Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

COPNIA, LEY 842 DE 2003, [Online], Disponible en https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

COPNIA, Código de ética, [Online], Disponible en https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica?form=MG0AV3

CVE, CVE-2014-6287, [Online], Disponible en https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

Packet storm, HttpFileServer 2.3.x Remote Command Execution, [Online], Disponible en https://packetstormsecurity.com/files/128243/HttpFileServer-2.3.x-Remote-Command-Execution.html

KALI, regripper, [Online], Disponible en https://www.kali.org/tools/regripper/

Center For Internet Security, CIS Controls, [Online], Disponible en https://www.cisecurity.org/controls?form=MG0AV3

Center For Internet Security, CIS Benchmarks List, [Online], Disponible en https://www.cisecurity.org/cis-benchmarks?form=MG0AV3

Cibernosgroup, Pasos a seguir ante un ataque informático, [Online], Disponible en https://www.grupocibernos.com/blog/pasos-a-seguir-ante-un-ataque-informatico

Axity, ¿como reaccionar ante un ataque cibernético?, [Online], Disponible en https://axity.com/comunidad-axity/como-reaccionar-ante-un-ataque-cibernetico/

KEEPCODING,¿Qué es OSSEC? ?, [Online], Disponible en https://keepcoding.io/blog/que-es-ossec/

Anexos

Anexo A

Capacidades Técnicas, Legales y de Gestión Para Equipos Blue Team y Red Team

En este video se expone el desarrollo del informe técnico correspondiente al Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. El video se encuentra en el siguiente enlace: https://youtu.be/W_3bOOrdm04