CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

DIDIER HERNANDO MORALES MOSQUERA

Asesor

EVER LUIS ARROYO BARON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA

2024

Resumen

En este documento se recorre toda la experiencia del seminario especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team el cual aborda, entre otros temas, el marco legal y ético que regula las actividades de Red Team en Colombia, destacando diversas leyes y normativas que son relevantes para la ciberseguridad y la protección de datos. Además hace un recorrido por las etapas de una prueba de penetración, entrega un reporte de una prueba de concepto de ataque sobre una maquina involucrada en un incidente de fuga de información desde la perspectiva de un integrante de Red Team, hace un análisis de esta prueba de concepto desde el punto de vista de Blue Team y elabora una serie de recomendaciones para mitigar las vulnerabilidades y riesgos encontrados. Por último, presenta un conjunto de estrategias para mejorar la colaboración y efectividad entre el Red Team y el Blue Team y diferentes métodos para medir la efectividad de las estrategias de los equipos.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Glosario

Ataque: Acción maliciosa realizada por un atacante con el objetivo de comprometer la seguridad de un sistema, red o dispositivo, ya sea para robar información, causar daños o interrumpir servicios.

Blue Team: Grupo de profesionales de la ciberseguridad que se encargan de defender y proteger los sistemas y redes de una organización contra ataques y amenazas.

Catálogo de Servicios: Documento que describe los servicios ofrecidos por un departamento o empresa, incluyendo detalles sobre su funcionamiento, características y beneficios para los usuarios.

CVE (Common Vulnerabilities and Exposures): Sistema de referencia que proporciona identificadores únicos para vulnerabilidades conocidas en software y hardware, facilitando la comunicación sobre problemas de seguridad.

DHCP (Dynamic Host Configuration Protocol): Protocolo que permite a los dispositivos en una red obtener automáticamente configuraciones IP y otros parámetros necesarios para comunicarse en la red.

Dirección IP: Número único asignado a cada dispositivo conectado a una red que utiliza el Protocolo de Internet para identificar y localizar dicho dispositivo.

EFS (Encrypting File System): Sistema de archivos que permite el cifrado de archivos en sistemas operativos Windows, protegiendo así la información sensible almacenada en el disco duro.

Elevación de Privilegios: Técnica utilizada por atacantes para obtener niveles más altos de acceso a un sistema del que originalmente poseían, permitiéndoles realizar acciones no autorizadas.

Endurecimiento (Hardening): Proceso de asegurar un sistema informático reduciendo sus vulnerabilidades mediante la eliminación de funciones innecesarias, aplicación de parches y ajustes en la configuración.

Escaneo: Actividad que consiste en analizar un sistema o red para identificar vulnerabilidades y debilidades que podrían ser explotadas por atacantes.

Firewall: Dispositivo o software que controla el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas, protegiendo así redes y sistemas contra accesos no autorizados.

Fuga de Información: Situación en la cual datos sensibles son expuestos o robados sin autorización, a menudo como resultado de un ataque cibernético o una mala gestión de la seguridad.

Framework: Conjunto estructurado de herramientas, prácticas y estándares utilizados para abordar problemas específicos dentro del ámbito del desarrollo o la ciberseguridad.

IPS (Intrusion Prevention System): Sistema diseñado para detectar y prevenir ataques en tiempo real al analizar el tráfico de red y tomar acciones automáticas para bloquear amenazas.

Kali Linux: Distribución del sistema operativo Linux diseñada específicamente para pruebas de penetración y auditorías de seguridad, que incluye numerosas herramientas para evaluar la seguridad informática.

Meterpreter: Herramienta avanzada utilizada en pruebas de penetración que permite a los atacantes ejecutar comandos en sistemas comprometidos, facilitando el control remoto.

NAT (Network Address Translation): Método utilizado para modificar las direcciones IP en los encabezados de los paquetes mientras están en tránsito a través de un router, permitiendo múltiples dispositivos en una red local compartir una única dirección IP pública.

Parche de Seguridad: Actualización diseñada para corregir vulnerabilidades específicas en software o sistemas operativos, mejorando así su seguridad general.

RDP (Remote Desktop Protocol): Protocolo desarrollado por Microsoft que permite a los usuarios conectarse a otro ordenador a través de una red utilizando una interfaz gráfica remota.

Internet Storage Name Service: Protocolo utilizado para asignar nombres legibles por humanos a direcciones IP dentro del contexto del almacenamiento en red, facilitando la gestión y acceso a recursos compartidos.

SIEM (Security Information and Event Management): Sistema que proporciona análisis en tiempo real sobre alertas generadas por aplicaciones y hardware, permitiendo la recopilación y análisis centralizado de datos relacionados con la seguridad.

Vulnerabilidad: Debilidad o fallo en un sistema, aplicación o proceso que puede ser explotado por atacantes para comprometer su integridad, confidencialidad o disponibilidad.

Introducción

En el contexto actual de ciberseguridad, las organizaciones enfrentan un panorama de amenazas en constante evolución, donde los ataques cibernéticos se vuelven cada vez más sofisticados y difíciles de detectar. Para proteger sus activos digitales y garantizar la integridad, confidencialidad y disponibilidad de la información, es fundamental implementar estrategias efectivas que empleen e integren equipos de Red Team y Blue Team.

El Red Team se encarga de simular ataques reales, identificando vulnerabilidades y debilidades en la infraestructura de seguridad de la organización. Por otro lado, el Blue Team se centra en la defensa, monitoreando y respondiendo a incidentes de seguridad para proteger los sistemas y datos críticos. El trabajo de estos dos equipos no solo mejora la preparación ante ciberamenazas, sino que también fomenta una cultura organizacional centrada en la seguridad.

El presente documento presenta un resumen de lo desarrollado durante el seminario especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team incluyendo un conjunto de estrategias diseñadas para optimizar las interacciones entre el Red Team y el Blue Team, promoviendo una defensa proactiva y una respuesta efectiva ante incidentes.

Objetivos

Objetivo General

Formular estrategias de contención de ciberataques mediante la implementación de equipos Red Team y Blue Team.

Objetivos Específicos

Mostrar el marco legal vigente en Colombia para las pruebas de penetración teniendo en cuenta la protección de datos personales y las leyes sobre delitos informáticos.

Evaluar la seguridad de un sistema informático proporcionado mediante la ejecución de ataques controlados.

Establecer un marco ético para el desempeño de la actividad de ciber seguridad en la ejecución de pruebas de penetración y auditoría de Red Team.

Brindar recomendaciones para mejorar la postura de seguridad de una organización mediante el análisis posterior de un ejercicio de Red Team y Blue Team.

Marco legal para el desarrollo de actividades de Red Team

Dentro del marco legal colombiano acerca de delitos informáticos y protección de datos personales podemos encontrar las siguientes leyes, decretos y normas que delimitan el alcance de los equipos de Red Team:

Constitución Política de Colombia, Artículo 15 (Derecho a la intimidad)

El Artículo 15 establece que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, los cuales deben ser respetados por el Estado. Además, se garantiza el derecho a conocer, actualizar y rectificar información personal en bases de datos. La correspondencia y otros medios de comunicación privada son inviolables, salvo en casos de orden judicial. Este artículo también menciona que la recolección y tratamiento de datos deben respetar las libertades consagradas en la Constitución.

Ley 23 de 1982, Ley 44 de 1993, Ley 1915 de 2018 (Derechos de autor)

Estas leyes regulan los derechos de autor en Colombia. La Ley 23 de 1982 establece el marco general para la protección de obras literarias y artísticas. La Ley 44 de 1993 introduce modificaciones para fortalecer estos derechos, incluyendo la protección de programas de ordenador. La Ley 1915 de 2018 actualiza y refuerza las disposiciones sobre derechos de autor, adaptándolas a las nuevas tecnologías y promoviendo el acceso a la cultura.

Ley 527 de 1999 (Firma digital)

La Ley 527 regula el uso de la firma digital en Colombia, estableciendo su equivalencia legal con la firma manuscrita. Se busca facilitar la autenticación de documentos electrónicos y garantizar la integridad y confidencialidad de la información transmitida digitalmente. Esta ley también promueve el uso seguro de medios electrónicos en las transacciones comerciales.

Ley 594 de 2000 (Ley general de archivo)

La Ley General de Archivo establece normas para la gestión documental en entidades públicas y privadas, asegurando la conservación y acceso a documentos. Promueve la organización, preservación y consulta de archivos, garantizando el derecho a la información pública y la transparencia administrativa.

Ley 1266 de 2008 (Habeas Data)

Esta ley regula el habeas data, que protege el derecho a conocer, actualizar y rectificar información personal en bases de datos. Establece los procedimientos para el manejo responsable de datos personales por parte de entidades públicas y privadas, así como sanciones por su uso indebido.

Ley 1221 del 2008, Decreto 0884 del 2012 (Teletrabajo)

La Ley 1221 establece las condiciones para el teletrabajo en Colombia, promoviendo su regulación para asegurar derechos laborales. El Decreto 0884 complementa esta ley al definir aspectos técnicos y operativos del teletrabajo, garantizando condiciones adecuadas para los trabajadores.

Ley 1273 de 2009 (Protección de datos y telecomunicaciones en el código penal)

Esta ley introduce modificaciones al código penal colombiano para incluir delitos relacionados con la protección de datos y las telecomunicaciones. Busca sancionar conductas que vulneren la privacidad y seguridad de los datos personales en entornos digitales.

Ley 1581 de 2012, Decreto 1377 de 2013, Decreto 886 de 2014, Decreto 1074 de 2015 (Protección de datos personales)

Estas normas establecen un marco integral para la protección de datos personales en Colombia. La Ley 1581 define principios básicos sobre el manejo responsable de datos

personales. Los decretos complementan esta ley al establecer procedimientos para el registro y tratamiento adecuado de bases de datos.

Ley 1928 de 2018, Convenio de Budapest (Ciberdelincuencia)

La Ley 1928 ratifica el Convenio sobre Ciberdelincuencia, promoviendo una cooperación internacional efectiva contra delitos informáticos. Se enfoca en mejorar las capacidades del Estado para prevenir y sancionar delitos relacionados con tecnologías digitales.

CONPES 3701 de 2011 (Ciberseguridad y Ciberdefensa)

Este documento establece lineamientos estratégicos para fortalecer la ciberseguridad y ciberdefensa en Colombia. Busca proteger infraestructuras críticas frente a amenazas cibernéticas mediante políticas públicas coordinadas entre diferentes sectores del gobierno.

CONPES 3854 de 2016 (Política Nacional de Seguridad Digital)

La Política Nacional busca establecer un marco integral para garantizar la seguridad digital en Colombia. Incluye estrategias para proteger información sensible del Estado y promover un entorno digital seguro para ciudadanos y empresas.

Marco Ético para el desarrollo de actividades de Red Team

Un marco ético para el desempeño de la actividad de ciberseguridad en el contexto de ejercicios de penetración y auditoría es fundamental para garantizar que las acciones realizadas sean responsables, transparentes y respetuosas con los derechos de las personas y las organizaciones. Por ello existen unos principios clave que deben guiar este tipo de actividades:

- Consentimiento Informado: Es requisito esencial el obtener el consentimiento explícito de la organización antes de llevar a cabo cualquier prueba de penetración o auditoría. Esto asegura que todas las partes involucradas comprendan tanto el alcance cómo los objetivos y los métodos utilizados en el ejercicio, promoviendo de ese modo una continua relación de confianza.
- Transparencia: Los profesionales de ciberseguridad que hacen parte de los equipos tanto Red Team cómo Blue Team deben ser claros sobre sus intenciones y métodos. Esto incluye comunicar de manera efectiva y oportuna los hallazgos y recomendaciones resultantes del ejercicio para permitir que la organización pueda tomar decisiones conscientes sobre cómo mitigar las vulnerabilidades identificadas.
- Confidencialidad: Respetar la privacidad y la confidencialidad de la información a la que se tiene acceso durante el ejercicio es vital. Los datos sensibles deben ser protegidos adecuadamente y no pueden ser divulgados sin autorización, asegurando de ese modo que se cumplan las regulaciones pertinentes sobre protección de datos.
- Responsabilidad: Los profesionales deben asumir la responsabilidad por sus acciones durante el ejercicio. Esto implica actuar con total integridad, cumplir con

las normas legales y éticas, y estar dispuestos a rendir cuentas por cualquier incidente o hallazgo que pueda surgir.

- Integridad: Mantener un alto estándar de integridad profesional es esencial. Esto significa actuar de manera honesta y ética en todas las interacciones, evitando cualquier práctica que pueda comprometer la seguridad o la reputación de la organización.

Es de resaltar que, de no cumplir el marco ético, además de los potenciales delitos que puedan ser imputados al profesional de seguridad, también puede tener consecuencias a nivel profesional ya que puede llevar incluso a la cancelación definitiva de la matricula profesional (Ley 842 de 2003, Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Etica Profesional y se dictan otras disposiciones).

Supervisión y control

Lamentablemente confiar en la ética no es suficiente. Las empresas de ciberseguridad deben tener acceso controlado a información sensible durante auditorías, limitado a lo necesario para cumplir con su mandato. Este acceso debe estar claramente definido en los contratos y acuerdos de servicios, especificando qué datos pueden ser accedidos y con qué fines. Para garantizar que este acceso no sea explotado indebidamente, se deben implementar políticas de privacidad y confidencialidad robustas, junto con auditorías regulares que evalúen el cumplimiento de estas políticas.

Además, para evitar el uso indebido de herramientas avanzadas de análisis forense, las empresas de ciberseguridad deberían adoptar varios mecanismos de supervisión tales como:

- Auditorías Internas Regulares: Evaluaciones periódicas del acceso y uso de datos sensibles para detectar actividades inusuales.
- Supervisión Continua: Implementar sistemas que monitoricen en tiempo real las acciones de los empleados y el acceso a información crítica.
- Capacitación y Concienciación: Programas regulares para educar a los empleados sobre la ética profesional y las implicaciones legales del ciber espionaje.
- Controles de Acceso Rigurosos: Limitar el acceso a información sensible solo a aquellos empleados que realmente lo necesiten para realizar su trabajo.

Etapas de una prueba de penetración

Un pentesting (pruebas de penetración) es un conjunto de pruebas en la que se ejecutan ataques sobre una plataforma específica para identificar vulnerabilidades en sistemas y redes. Tanto los ataques cómo la profundidad de las pruebas debe ser pactada con el propietario de la plataforma con anticipación.

Las etapas de un pentesting serían las siguientes:

1. Planificación y Preparación: En esta fase inicial, se definen los objetivos del pentest y se establece el alcance del proyecto. Se determina qué sistemas serán evaluados, los métodos a utilizar y los límites que no se deben cruzar. Esta etapa es crucial para asegurar que todas las partes involucradas tengan expectativas claras sobre el proceso y sus resultados.
2. Reconocimiento: Esta etapa implica la recopilación de información sobre el objetivo. Se utilizan técnicas tales cómo la recopilación de dominios, IPs, puertos y servicios, el uso de herramientas como Google Dorks y la obtención de metadatos y datos de terceros de fuentes abiertas.
3. Análisis de Vulnerabilidades: En esta fase, se analiza la información recopilada para identificar posibles vulnerabilidades. Se utilizan herramientas automáticas y manuales para descubrir puntos débiles que podrían ser explotados por un atacante.
4. Explotación: Aquí es donde se llevan a cabo los ataques. Los pentesters intentan explotar las vulnerabilidades identificadas para evaluar el nivel de acceso que podrían obtener los atacantes reales. Esta fase busca demostrar cómo se pueden comprometer los sistemas procurando usualmente no causar un daño real.

5. Post-explotación: Después de haber explotado el sistema, se evalúa el nivel de acceso obtenido y qué información sensible ha sido expuesta. Esta fase ayuda a entender el impacto real que un ataque exitoso podría tener en la organización.
6. Informe y Recomendaciones: La última etapa consiste en compilar un informe detallado que documente las vulnerabilidades encontradas, cómo fueron explotadas y recomendaciones para mitigar esos riesgos. Este informe es esencial para que la organización pueda implementar mejoras en su seguridad.

Las pruebas de penetración pueden ser de los siguientes tipos dependiendo de la cantidad de información que se le entregue al Pentester:

- Caja blanca: En este caso el responsable de la plataforma a probar entrega toda la información sobre esta, como cuentas de usuario, arquitectura, direccionamiento IP, etc. En algunos casos incluso se entrega el código fuente de las aplicaciones que se ejecutan en la infraestructura. Esto permite probar lo que sucedería si se sufre un ataque interno por parte de alguien que conoce a la perfección el sistema objetivo.
- Caja gris: Aquí se tendría una información parcial del sistema objetivo tales como nombres de cuentas, direccionamiento IP e información global de los sistemas a probar.
- Caja negra: En este caso se tendría solo una información básica sobre la empresa objetivo lo que permite probar el alcance que tendría cualquiera con una conexión a Internet.

Red Team: Prueba de concepto de ataque

Antecedentes

La misión del equipo de Red Team en esta PoC consistió en identificar el medio o proceso a través del cual se estaban generando fugas de información dentro de la organización, específicamente en uno de sus equipos de cómputo. La información inicial que tenía el equipo indicaba que la máquina donde se producía la fuga contaba con una aplicación vulnerable instalada en un sistema operativo Windows. Se sospechaba que esta aplicación estaba asociada a un exploit que podía permitir el acceso a través de un Shell, así como la escalación de privilegios u otros tipos de ataque. Además, durante la investigación, también se examinó la posibilidad de un escalamiento de privilegios mediante la creación de un usuario con privilegios de administrador en el sistema.

Para esto se entregó al Red Team una imagen de máquina virtual del equipo afectado la cual se procedió a montar en un entorno de laboratorio donde se pudiera ejecutar la prueba de concepto. La prueba ejecutada fue de tipo Caja blanca ya que se tuvo acceso local total a la máquina atacada para comprobar de primera mano la efectividad y los efectos del ataque.

Metodología Usada

La metodología usada para esta prueba de concepto fue extraída de la sugerida por el framework MITRE ATT&CK sobre la cual se aplicaron las siguientes etapas:

- Reconocimiento mediante escaneo activo
- Acceso inicial
- Escalamiento de privilegios
- Persistencia

Dado que el escenario planteado está limitado a un entorno de laboratorio conocido con un solo equipo no fue necesario aplicar las demás etapas del framework.

Herramientas utilizadas

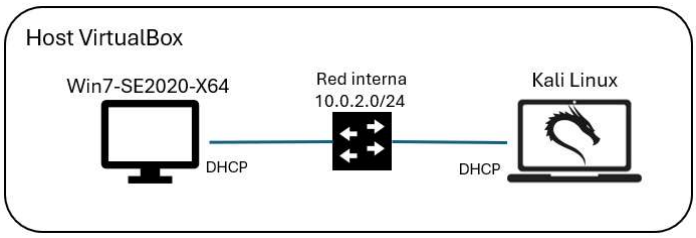
Para ejecutar la prueba de concepto del ataque se emplearon las siguientes herramientas:

- Oracle VirtualBox para la ejecución de las máquinas virtuales.
- Máquina virtual con Kali Linux 2024.3
- Programa NMAP para hacer el escaneo activo de direcciones IP y puertos.
- La herramienta Metasploit que permite ejecutar módulos de ataques ya conocidos.
- El módulo de Metasploit windows/http/rejetto_hfs_rce_cve_2024_23692 para explotar la vulnerabilidad hallada.
- La herramienta Meterpreter para lograr ejecutar una Shell reversa en la maquina atacada.
- El módulo de Metasploit Incognito para la creación de un usuario administrador.

Preparación del banco de trabajo

Se configuró el banco de trabajo dentro de un sistema de ejecución de máquinas virtuales montado sobre Oracle VirtualBox. En este se configuró una red NAT con el segmento de red 10.0.2.0 el cual asigna direcciones IP mediante DHCP. En esa red se conectaron dos máquinas virtuales: la máquina virtual para analizar, llamada Win7-SE2020-X64 y una máquina virtual ejecutando Kali Linux.

Ilustración 1 - Arquitectura laboratorio

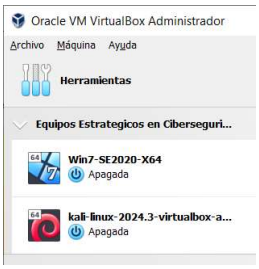


Fuente: Elaboración propia

Se configuraron dos máquinas virtuales sobre VirtualBox:

- Win7-SE2020-X64
- Kali-Linux-20204.3-virtualbox-amd64

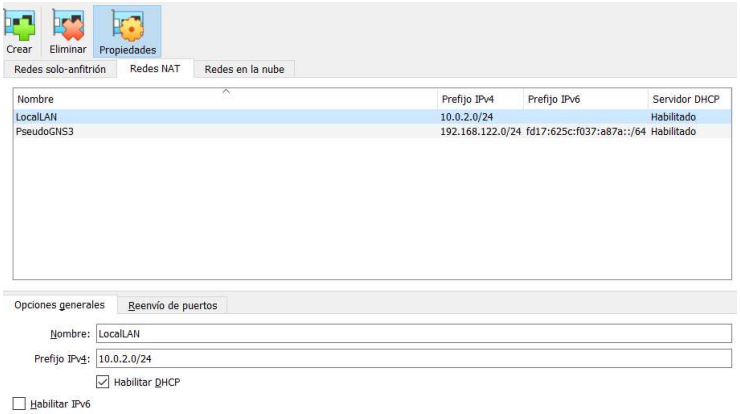
Ilustración 2 - Montaje de banco de trabajo



Fuente: Elaboración propia

Además, se definió una red NAT llamada LocalLAN para conectar los dos equipos. Esta red cuenta con un DHCP con la red 10.0.2.0/24 tal como se detalla en la imagen anexa.

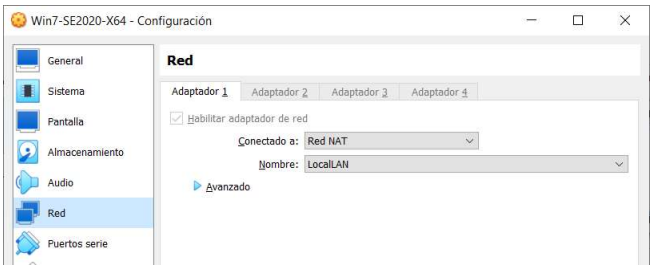
Ilustración 3 - Red banco de trabajo



Fuente: Elaboración propia

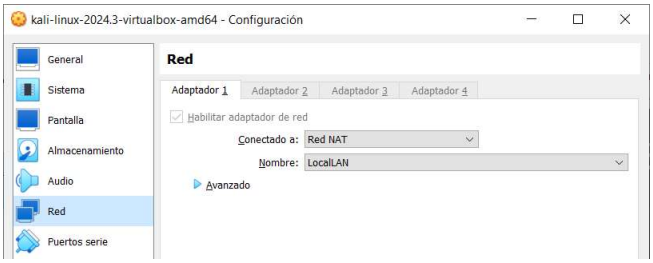
Cada máquina virtual se configuró para conectarse a la red NAT especificada.

Ilustración 4 - Configuración de red VM Windows



Fuente: Elaboración propia

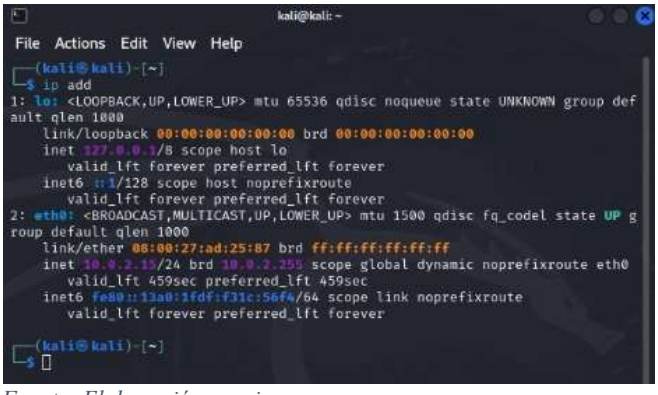
Ilustración 5 - Configuración de red VM Kali



Fuente: Elaboración propia

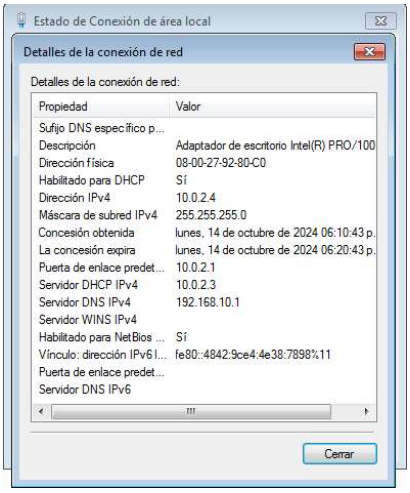
Se verifica que ambas máquinas tengan dirección IP de la red asignada.

Ilustración 6 - Dirección IP Kali



Fuente: Elaboración propia

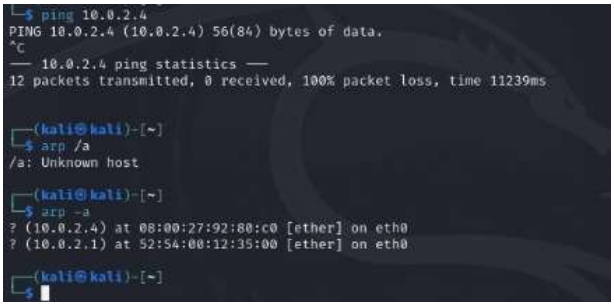
Ilustración 7 - Dirección IP Windows



Fuente: Elaboración propia

Se hace una prueba de ping desde la VM Kali y se comprueba que la MAC de la VM Windows sea resuelta por ARP de este.

Ilustración 8 - Evidencia conexión Kali - Windows



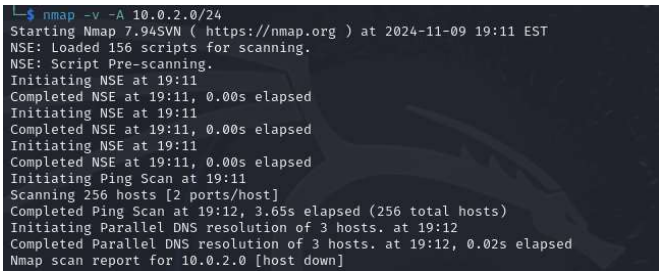
Fuente: Elaboración propia

Ejecución del ataque

Reconocimiento

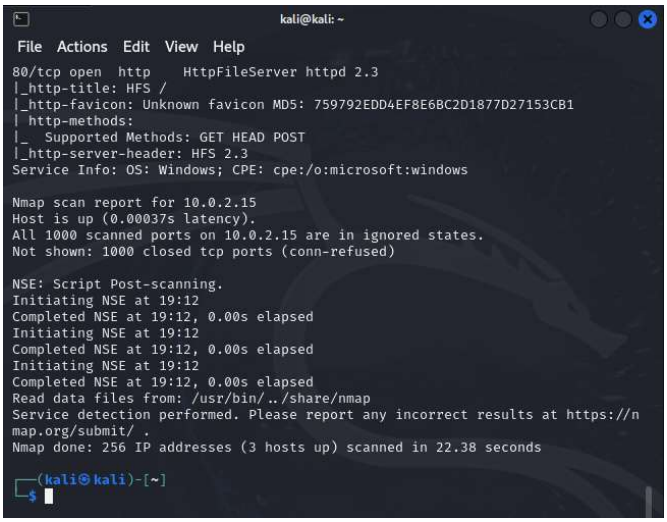
Inicialmente se procedió a escanear la red para determinar la dirección IP de la VM a analizar.

Ilustración 9 - Escaneo de red 1



Fuente: Elaboración propia

Ilustración 10 - Escaneo de red 2



Fuente: Elaboración propia

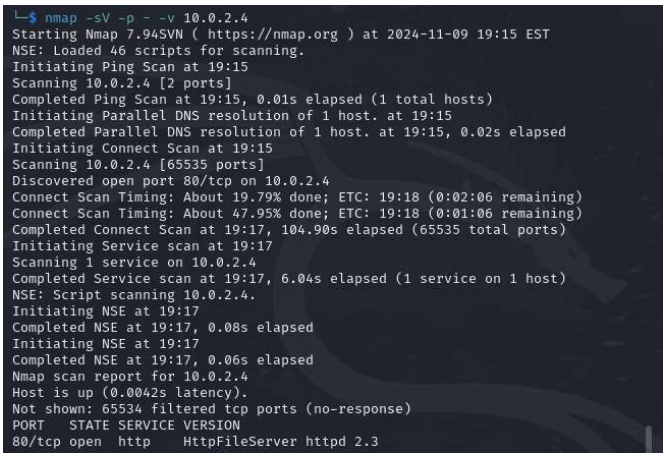
Después de determinar la dirección IP del computador Win7-SE2020-X64 (10.0.2.4), se realizó un escaneo del equipo para determinar que puertos y servicios estaban abiertos, hallándose los siguientes:

Tabla 1 - Puertos abiertos

Puerto	Estado	Servicio	Versión
80/tcp	Abierto	http	HttpFileServer httpd 2.3

Fuente: Elaboración propia

Ilustración 11 - Escaneo de servicios



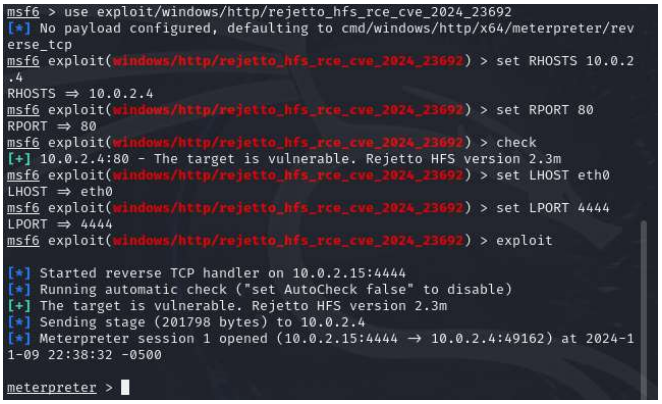
Fuente: Elaboración propia

Acceso inicial

Se realizó una investigación en internet del puerto compatible con HTTP para determinar el tipo de servicio. El puerto corresponde a un servidor de archivos web llamado Rejetto HFS cuya versión 2.3 es vulnerable a un ataque de inyección de plantillas RCE identificado con el CVE-2024-23692.

Se verificó en MITRE (2024) la documentación de la vulnerabilidad donde se evidenció que existe un módulo de Metasploit que permite explotar la vulnerabilidad antes mencionada por lo cual se procedió a cargar y ejecutar el módulo en Metasploit el cual logró abrir una Shell de Meterpreter.

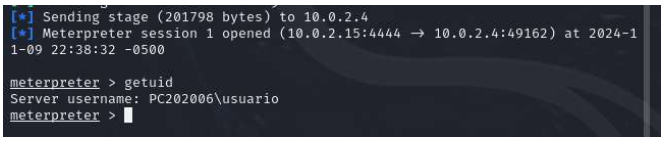
Ilustración 12 – Carga del exploit



Fuente: Elaboración propia

Posteriormente, se procedió a verificar con cual usuario local se ejecutó la Shell de Meterpreter encontrando que el usuario era **PC202006\usuario**

Ilustración 13 – Verificación del usuario



Fuente: Elaboración propia

Se ejecutó el comando ***sysinfo*** para dejar evidencia del equipo al cual se logró la conexión.

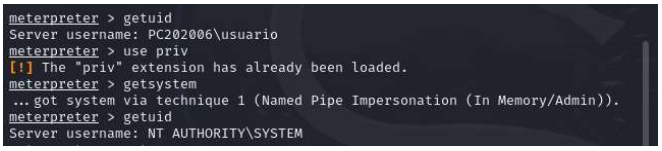
Ilustración 14 – Sysinfo

Fuente: Elaboración propia

Elevación de privilegios

Después de lograr ejecutar exitosamente la Shell de Meterpreter en la maquina virtual analizada se procedió a ejecutar el comando ***getsystem*** exitosamente para lograr la elevación de privilegios, obteniendo de ese modo acceso como **NT AUTHORITY\SYSTEM**.

Ilustración 15 – Elevación de privilegios



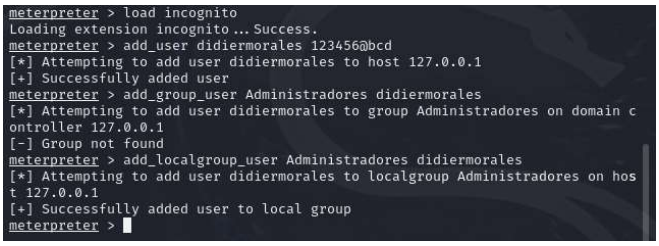
Fuente: Elaboración propia

Persistencia

Luego de lograr la elevación de privilegios, se cargó el módulo ***incognito*** para crear el usuario solicitado en la Prueba de Concepto. Sobre este módulo se ejecutaron los comandos

add_user para crear el usuario y **add_localgroup_user** para hacer el usuario miembro del grupo Administradores.

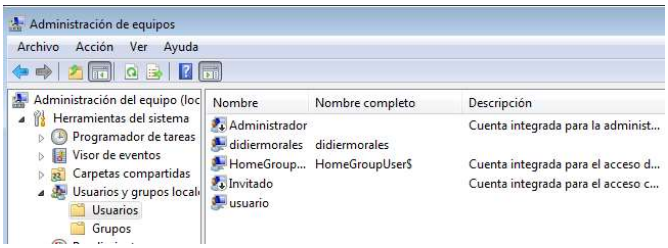
Ilustración 16 – Creación del usuario local



Fuente: Elaboración propia

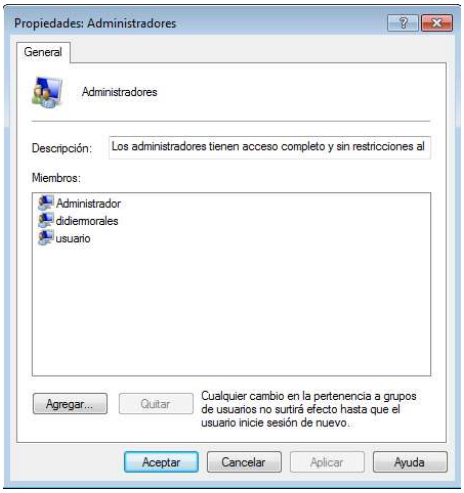
Posterior a esto, se accedió localmente a la consola de la maquina virtual analizada para comprobar que efectivamente se hubiese creado el usuario con la respectiva membresía al grupo Administradores, verificando que efectivamente así había sucedido.

Ilustración 17 – Verificación del usuario local



Fuente: Elaboración propia

Ilustración 18 – Grupo administradores



Fuente: Elaboración propia

Descripción del ataque

El CVE-2024-23692 es una vulnerabilidad crítica de ejecución remota de código (RCE) que afecta al servidor de archivos HTTP (HFS) de Rejetto versión 2.3m. Esta vulnerabilidad permite enviar solicitudes HTTP especialmente diseñadas para ejecutar comandos arbitrarios. Esta vulnerabilidad puede ser explotada por un atacante remoto sin necesidad de estar autenticado.

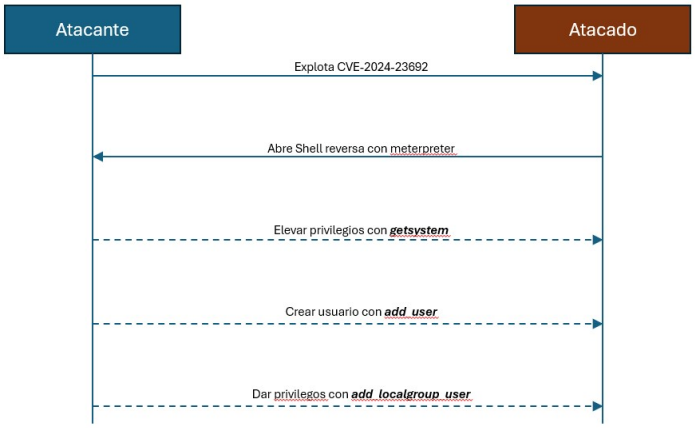
Por otra parte, la maquina atacada tiene un sistema operativo no soportado desde enero de 2020 por lo que no se cuenta con actualizaciones lo que la pone en riesgo de todo tipo de ataques entre los que se encuentran:

- CVE-2021-43233. Vulnerabilidad de RCE sobre RDP.
- CVE-2021-43217. Vulnerabilidad sobre el sistema de archivos cifrados EFS.
- CVE-2021-43215. Vulnerabilidad de RCE sobre Internet Storage Name Service (iSNS).

El ataque ejecutado consistió en explotar la vulnerabilidad de RCE con identificación CVE-2024-23692, lo que permitió abrir una sesión de Meterpreter con los privilegios del usuario que lo ejecutó en el sistema Windows. Posteriormente se ejecutó la elevación de privilegios mediante suplantación de tuberías nombradas (*Named Pipe Impersonation*). Por último, se creó el usuario y se otorgaron privilegios de administrador mediante el módulo incognito.

En el siguiente diagrama se puede observar el orden del ataque:

Ilustración 19 – Descripción del ataque



Fuente: Elaboración propia

Blue Team: Recomendaciones sobre el escenario planteado

Hallazgos y falencias

Al analizar el escenario como parte del Blue Team se pudieron observar múltiples falencias que facilitaron la ejecución de los ataques entre las que se encuentran:

- La organización no cuenta con un catálogo de servicios instalados que facilite el descubrimiento de nuevas vulnerabilidades de manera temprana y proactiva
- Se siguen usando sistemas operativos no soportados y sin parches de seguridad
- No tienen mecanismos de Firewall e IPS que mitiguen la ejecución de ataques contra la plataforma
- No hay procesos de endurecimiento, o hardening, de sistema operativo y servicios al menos en las máquinas que están expuestas a Internet.
- No cuentan con sistemas de centralización de eventos, aún menos con sistemas de correlación de estos (SIEM).

Recomendaciones para endurecimiento

Cómo primera medida, se recomienda hacer actualización del sistema operativo al menos a Windows 10 ya que el sistema operativo actual (Windows 7) no cuenta con soporte ni actualizaciones desde enero de 2020.

Al nuevo equipo se le aplicarían las recomendaciones de *CIS Microsoft Windows 10 Stand-alone Benchmark* versión 3.0.0.

El servicio que está escuchando sobre el puerto 80 corresponde a un servidor de archivos web llamado Rejetto HFS cuya versión 2.3 es vulnerable a un ataque de inyección de plantillas RCE CVE-2024-23692 y ya no está siendo soportado por sus creadores. En este caso se recomienda eliminar el software ya que aún no hay un reléase estable del programa en la versión

3.0 o al menos reemplazarlo por el reléase 0.54.0 que ya cuenta con el parche para la vulnerabilidad RCE.

En caso de requerir mantener el servicio se debería limitar el acceso al puerto 80 solo a las direcciones IP que requieren consumirlo de tal modo que no quede expuesto públicamente a cualquiera. Adicionalmente el servicio debería ejecutarse con el mínimo nivel de privilegio posible.

Se recomienda incluir un sistema de SIEM dentro de la solución para que centralice eventos de sistema y seguridad y en este configurar alarmas para detectar, entre otros, la administración de cuentas y otros eventos recomendados por el manual CIS.

Otras recomendaciones generales serían configurar un IPS y Firewall para proteger el segmento de red donde se encuentra el equipo y activar la firma o regla para bloqueo del ataque con CVE-2024-23692.

Conclusiones

Contar con un equipo de Red Team y Blue Team es crucial para que las organizaciones no solo identifiquen y mitiguen vulnerabilidades, sino que también desarrollen una cultura sólida de seguridad cibernética que les permita adaptarse y responder eficazmente a las amenazas en constante evolución ya que obliga a las organizaciones a estar en un estado de constante alerta y mitigar vulnerabilidades de manera prioritaria y proactiva. Esto también permite contar con detección y respuesta rápida a incidentes sean generados por el Red Team o por atacantes externos y la mejora continua de las políticas de seguridad y en los controles implementados en las defensas de la organización.

Por otra parte, la efectividad de una estrategia que involucra a equipos de Red Team y Blue Team se evalúa mediante simulaciones prácticas, análisis detallados, revisiones colaborativas y un enfoque continuo en la capacitación y mejora. Estos métodos ayudan a asegurar que la organización esté bien preparada para enfrentar amenazas cibernéticas reales.

Recomendaciones

Las siguientes recomendaciones están diseñadas para mejorar la efectividad y cohesión entre el Red Team y el Blue Team, optimizando las estrategias de defensa y ataque dentro de una organización. Al implementar estas prácticas, buscamos fortalecer la postura de seguridad en general, aumentar la resiliencia ante ataques y alimentar un ambiente de colaboración que beneficie a toda la organización:

- Fomentar la Colaboración Continua: Establecer sesiones regulares de intercambio de información y estrategias entre el Red Team y el Blue Team. Esta interacción permite a ambos equipos aprender de las tácticas y técnicas utilizadas, mejorando así la preparación y respuesta ante amenazas reales.
- Implementar Ejercicios de Simulación: Realizar ejercicios de simulación de ciberataques, donde el Red Team pueda ejecutar ataques controlados mientras el Blue Team defiende. Esto no solo ayuda a identificar vulnerabilidades, sino que también permite evaluar la efectividad de las respuestas del equipo defensor.
- Desarrollar un Programa de Capacitación Cruzada: Crear un programa donde los miembros del Blue Team reciban formación en técnicas ofensivas del Red Team y viceversa. Esto aumenta la comprensión mutua de las estrategias defensivas y ofensivas, facilitando una respuesta más integrada ante incidentes.
- Utilizar Herramientas de Automatización: Implementar herramientas que automaticen la detección y respuesta a incidentes, permitiendo al Blue Team centrarse en la estrategia y análisis en lugar de tareas repetitivas. El Red Team también puede beneficiarse de herramientas automatizadas para realizar pruebas de penetración más eficientes.

- Establecer Metas Comunes: Definir objetivos claros y comunes para ambos equipos, alineando sus esfuerzos hacia la mejora continua de la ciberseguridad organizacional lo que fomenta un sentido de unidad y colaboración en lugar de competencia entre los equipos.
- Recopilar y Analizar Datos Post Ejercicio: Después de cada ejercicio conjunto, recopilar datos sobre el rendimiento de ambos equipos y analizar los resultados para identificar áreas de mejora. Esta retroalimentación es muy importante para ajustar tácticas y estrategias en futuras interacciones.
- Promover una Cultura de Seguridad: Fomentar una cultura organizacional que valore la ciberseguridad en todos los niveles, asegurándose de que todos los empleados comprendan su papel en la defensa contra amenazas cibernéticas. Esto además incluye capacitaciones regulares sobre concienciación en seguridad, lo que permite complementar los esfuerzos del Red Team y Blue Team.

Referencias Bibliográficas

Alcarria, P. (2024). Ciberseguridad proactiva: La importancia del Blue Team | OpenWebinars. OpenWebinars.net. Recuperado de https://openwebinars.net/blog/ciberseguridad-proactiva-la-importancia-del-blue-team/

Almatisse. (2023). Las Etapas de un Pentesting y su Propósito: Un Escudo para las Empresas. Linkedin. https://es.linkedin.com/pulse/las-etapas-de-un-pentesting-y-su-prop%C3%B3sito-escudo-para-empresas

Awati, R. (2023). What is Common Vulnerabilities and Exposures (CVE)? | Definition from TechTarget. TechTarget. https://www.techtarget.com/searchsecurity/definition/Common-Vulnerabilities-and-Exposures-CVE

BID & OEA. (2020). Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe (2). Banco Interamericano de Desarrollo - BID. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Center for Internet Security. (2024). CIS. CIS Center for Internet Security. Recuperado de https://www.cisecurity.org

Center for Internet Security. (2024). CIS Microsoft Windows 10 Stand-alone Benchmark. CIS - Center for Internet Security.

Ciberseguridad.com. (S/F). Guía completa sobre controles de seguridad CIS | Ciberseguridad. ciberseguridad.com. Recuperado de https://ciberseguridad.com/herramientas/controles-seguridad-cis/

Cloudflare. (2024). Cartera de productos de servicios para aplicaciones de Cloudflare. Cloudflare.com. Recuperado de https://www.cloudflare.com/es-es/application-services/products/

Cloudflare. (2024). ¿Estás siendo blanco de un ataque? | Soporte de emergencia 24/7. Cloudflare.com. Recuperado de https://www.cloudflare.com/es-es/under-attack-hotline/

Código de Ética Profesional. Ley 842 de 2003. 9 de octubre de 2003 (Colombia).

Colombia, MinTIC. (2016). Guía de gestión de riesgos. Ministerio de Tecnologías de la Información y Comunicaciones -MINTIC. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Dezso, R. (2023). Metasploit Tutorial 2024: The Complete Beginners Guide. StationX.Net. https://www.stationx.net/metasploit-tutorial/

ElevenPaths. (s/f). Ocho siglas relacionadas con las vulnerabilidades (I): CVE. Telefónica Tech. Recuperado el 14 de octubre de 2024, de https://telefonicatech.com/blog/ocho-siglas-relacionadas-con-las-6

Fewer, S. (2024). Rejetto HTTP File Server (HFS) 2.x—Unauthenticated RCE exploit module (CVE-2024-23692) by sfewer-r7 · Pull Request #19240 · rapid7/metasploit-framework. GitHub. https://github.com/rapid7/metasploit-framework/pull/19240

Greenbone AG. (s/f). OpenVAS - Open Vulnerability Assessment Scanner. Greenbone OpenVAS. https://openvas.org/

Hasan, M. (2022). Metasploit Tutorial for Beginners—Basics to Advanced. NoobLinux. https://nooblinux.com/metasploit-tutorial/

Hernandez, M. (2022). Pentesting con OWASP: Fases y metodología. Blog de hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Holdsworth, J., & Kosinski, M. (2024). ¿Qué es la respuesta a incidentes? | IBM. IBM.com. Recuperado de https://www.ibm.com/es-es/topics/incident-response

IBM. (2021). ¿Qué es un ciberataque? | IBM. Recuperado de https://www.ibm.com/es-es/topics/cyber-attack

IBM. (S/F). ¿Qué es la gestión de eventos e información de seguridad (SIEM)? IBM.com. Recuperado de https://www.ibm.com/mx-es/topics/siem

Instituto Nacional de Ciberseguridad. (S/F). Guía de ciberataques. incibe.es. Recuperado de https://www.incibe.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

lupita@microbit.com. (2023). ¿Qué es NMAP? | Genuino Cloud. Genuino Cloud | Correo electrónico corporativo. https://genuinocloud.com/blog/que-es-nmap/

MinTIC. (2016). Guía para la Implementación de Seguridad de la Información en una MIPYME. Ministerio de Tecnologías de la Información y Comunicaciones -MINTIC. https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

MITRE. (2024). CVE - CVE-2024-23692. CVE - CVE-2024-23692. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23692

Microsoft Corp. (2024). Windows 7—Microsoft Lifecycle. Microsoft Learn. Recuperado de https://learn.microsoft.com/es-es/lifecycle/products/windows-7

MITRE. (2024). CVE - CVE-2024-23692. CVE - CVE-2024-23692. Recuperado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23692

NE Digital. (S/F). ¿Qué significa SIEM y cómo funciona? nedigital.com. Recuperado de https://www.nedigital.com/es/blog/siem-de-microsoft

NIST. (2024). NVD - CVE-2024-23692. NVD - CVE-2024-23692. https://nvd.nist.gov/vuln/detail/CVE-2024-23692

NMAP.ORG. (s/f). Guía de referencia de Nmap (Página de manual). Guía de referencia de Nmap. https://nmap.org/man/es/index.html

OffSec Services Limited. (S/F). OffSec's Exploit Database Archive. About Exploit Database. https://www.exploit-db.com/

Ramírez, B. (2016). Medición de madurez de ciberseguridad en pymes colombianas. https://repositorio.unal.edu.co/handle/unal/57956

Rapid7. (s/f). Meterpreter getsystem | Metasploit Documentation. Metasploit Documentation. https://docs.rapid7.com/metasploit/meterpreter-getsystem/

Rapid7. (s/f). Python Extension. Metasploit Documentation Penetration Testing Software, Pen Testing Security. https://rapid7.github.io/metasploit-framework/docs/using-metasploit/advanced/meterpreter/python-extension.html

Revista UNIR. (2020). Red Team, Blue Team y Purple Team: Funciones y diferencias. Universidad Internacional de La Rioja. Recuperado de https://www.unir.net/revista/ingenieria/red-blue-purple-team-ciberseguridad/

Snort. (2024). Snort—Rule Docs—SID 1:63771. Snort.org. Recuperado de https://www.snort.org/rule-docs/1-63771

SOPHOS. (2024). IPS Signature Update Release Note Version: 18.22.16. SOPHOS. Recuperado de https://docs.sophos.com/releasenotes/output/en-us/nsg/IPSReleaseNotes/7.22.16_s.pdf

Team, O. (s/f). Privilege Escalation—Metasploit Unleashed. OffSec. Recuperado de https://www.offsec.com/metasploit-unleashed/privilege-escalation/

Apéndices

Apéndice A - *URL del video de sustentación*

El video de sustentación se encuentra en la siguiente dirección: https://youtu.be/GrdpUJKVKl0