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

Carlos Javier Perez Marin

Tutor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Especialización en Seguridad Informática

2024

Resumen

El presente trabajo asociado al Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, muestra de manera sintetizada las labores realizadas a lo largo de su duración, donde se identificaron las características de cada uno de los equipos mediante la aplicación de un caso de estudio. La pretensión con este documento no es la de detallar paso a paso las actividades realizadas, sino la de generar a nivel más abstracto cuales son los aspectos más importantes de las funciones realizadas por cada equipo y establecer tanto a partir del conocimiento teórico generado en las revisiones documentales como en la experiencia adquirida mediante la practica de laboratorio desarrollada, cuales pueden ser las estrategias generales a nivel de ciberseguridad que se pueden adoptar en las organizaciones a fin de mejorar su postura de seguridad.

De igual manera, transversalmente se menciona la importancia de la colaboración entre los equipos de Red Team y Blue Team mediante la estrategia de Purple Team, como una forma de medir la eficacia en las acciones de los dos equipos, adquirir conocimiento en ambas partes mediante la retroalimentación de las acciones y llevar a la mejora continua de los procesos para asi fortalecer la defensa de la organización.

Tabla de Contenido

Glosario

CIS: Acrónimo del Center for Internet Security, entidad independiente que genera controles y documentos de buenas prácticas de seguridad para su aplicación en equipos, sistemas operativos y aplicaciones.

DDoS: Acrónimo de Distributed Denial of Service. Se establece como un ataque de denegación de servicios hacia objetivos, el cual es generado desde varios orígenes distintos de tráfico.

Equipo Azul (BLUE TEAM): Equipo de seguridad informática que tiene como objetivo realizar la ejecución de las labores de defensa, mediante una vigilancia constante de los comportamientos y eventos que se presentan en los sistemas de una organización a fin de detectar desviaciones que puedan afectar a los activos de información y realizar la respuesta frente a un incidente en caso de requerirse.

Equipo Rojo (RED TEAM): Equipo de seguridad informática encargado de las labores ofensivas mediante la simulación de comportamientos que puede realizar un actor malicioso, lo cual sirve para determinar tanto la postura de seguridad de los activos de información como la efectividad de las labores del equipo de blue team y de las medidas defensivas de la organización.

NVD: Acrónimo de National Vulnerability Database. Repositorio del gobierno de EE.UU mantenido por el NIST, que almacena información de fallas/debilidades a nivel de software y hardware que pueden comprometer la seguridad de activos de información.

Pentesting: Actividad donde aplicada una metodología especifica, se realiza la detección y explotación de vulnerabilidades en un activo de información a fin de identificar el nivel de riesgo de este.

RCE: Acrónimo de Remote Code Execution. Vulnerabilidad de nivel crítico y técnica de ataque que permite que un actor malicioso pueda realizar la ejecución de comandos desde una ubicación remota, tomando control de un objetivo.

TTP: Acronimo de Tactics, Techniques and Procedures. En el ámbito de la ciberseguridad, se refiere a la forma de describir el patrón de comportamiento de un actor malicioso para comprometer un activo de información.

Lista de Figuras

Lista de Apéndices

Introducción

Teniendo en cuenta que la premisa máxima de la seguridad informática es la de proteger los activos de información, este trabajo se enfoca en mostrar como las actuaciones de los equipos de Blue Team y Red Team dentro de las organizaciones, sirven para cumplir dicho propósito, esto a partir de las estrategias de carácter ofensivo y defensivo que se despliegan en cada uno de sus frentes. Sin embargo, cabe mencionar que estas operaciones no deben verse como esfuerzos aislados, sino que deben tratarse como procesos complementarios entre sí, que andan en constante retroalimentación y que llevan a la mejora continua de la postura de seguridad de la organización.

En este documento se observarán cuáles son los aspectos relevantes de cada uno de los equipos a partir de la visión brindada en el desarrollo del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, al igual que recomendaciones para el planteamiento de estrategias para mejorar la postura de seguridad de las organizaciones a partir de la experiencia adquirida en el programa académico.

Objetivos

Objetivo General

Realizar la generación de estrategias de seguridad frente a las vulnerabilidades y debilidades identificadas en una infraestructura de IT de una organización.

Objetivos Específicos

Identificar los aspectos relevantes de los equipos de Red Team y Blue Team que permitan el desarrollo de estrategias de seguridad a partir de lo observado en el desarrollo del seminario especializado.

Generar recomendaciones para implementar estrategias que permitan llevar a la mejora de la postura de seguridad de las organizaciones a partir de la aplicación de los conocimientos teóricos y prácticos adquiridos en el seminario especializado.

Contenido del Trabajo

Aspectos que aporten al desarrollo de estrategias de Red Team y Blue Team

De acuerdo con el desarrollo de las etapas anteriores del Seminario de Especialización donde se especificaron los fundamentos legales, éticos y operativos de los equipos de Red Team y Blue Team en un escenario donde se requiere hacer una investigación de un incidente ocurrido en una entidad pública, actividad a cargo de un proveedor de seguridad al cual estamos asignados como expertos en seguridad, es posible sintetizar diversos aspectos relevantes de lo observado, asi:

Aspectos Legales y Éticos de la actuación de los equipos de Blue Team/Red Team

Dentro de las primeras dos etapas se identificaron a nivel Colombia, cuales aspectos legales se deben tener en cuenta para el desarrollo de las funciones básicas de los equipos de Red/Blue Team, dada la sensibilidad de la información que puede ser manejada, las actividades que se pueden desarrollar y las implicaciones jurídicas de estas actuaciones.

Importante aquí la mención de dos normas relevantes a observar en una actividad que se desarrolle en territorio colombiano o incluso de manera remota para un cliente cuyo domicilio comercial sea Colombia:

- Ley 1273 de 2009: Como lo menciona textualmente dicha ley, se introduce el termino jurídico de “protección de información y datos” dentro del código penal colombiano así como se tipifican los 9 delitos más comunes que pueden darse en activos de información como lo son: el acceso abusivo a un sistema informático, la obstaculización ilegitima de un sistema informático o red de comunicación, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales, la suplantación de sitios web para obtener datos personales, el hurto utilizando medios informáticos y la transferencia no consentida de activos. Si bien no está especificado en la ley directamente, la Fiscalía General de la Nación en su documento Cartilla Metodológica de Atención de delitos informáticos (Fiscalía General de la Nación, s.f.), explica cuáles pueden ser los modos en los cuales los delincuentes pueden cometer los delitos expuestos en la Ley 1273 de 2009, donde se incluyen desde los ataques DDoS, el uso de virus y ransomware, la explotación de vulnerabilidades hasta los diversos ataques que hacen aprovechamiento de las distintas técnicas de Ingeniería Social.

- Ley 1581 de 2012: Denominada la “Ley de protección de datos personales” (Congreso de la República de Colombia, 2012), es una norma que especifica como se desarrolla el derecho otorgado a los ciudadanos respecto al conocimiento, actualización y modificación de la información que se recoge de estos. Se establece en esta norma, los principios para el tratamiento de los datos personales, las categorías de datos, los derechos que tienen los ciudadanos respecto al manejo de los datos personales, las obligaciones de las personas/entidades que manejan datos, los mecanismos establecidos

para vigilancia y control de las entidades, así como las sanciones por la no observancia de la ley.

De acuerdo con las necesidades del cliente u organización a la cual se esté desarrollando la actividad, es importante validar que no se requiera una adherencia normativa adicional como lo puede ser la observancia de la ISO 27001 u otras normas de compliance, asi como el cumplimiento de la política de seguridad de la información (en caso de existir para la organización objetivo).

Es de destacar igualmente, que, para el caso de Colombia, las actividades de ingeniería deben estar sujetas al Código de Ética emanado por el COPNIA (COPNIA, 2015), sobre todo en aspectos como:

- Articulo 31 parágrafo f. (deberes generales de los profesionales)
- Articulo 34 parágrafo a. (prohibiciones especiales a los profesionales respecto de la sociedad)
- Artículo 35, parágrafo b. (deberes de los profesionales para con la dignidad de sus profesiones)

Ahora bien, para plasmar todos estos requerimientos legales de una forma clara y concisa al momento previo de la realización de la actividad se recomienda la suscripción de un acuerdo de confidencialidad entre proveedor y cliente como se indica por parte de autores como Romero, Figueroa y Vera (Romero Castro et al., 2018, p. 51), donde se deben delimitar las acciones que puede adelantar la empresa con la información confidencial y establecer las consecuencias de carácter penal/económico que puede sufrir el proveedor de seguridad en caso de que se haga mal

uso de esta. Un buen ejemplo de un modelo adecuado de un acuerdo de confidencialidad puede ser el que expone el INCIBE (INCIBE, 2021) donde se establecen claramente las responsabilidades de las partes, acciones que se pueden ejecutar y medidas/controles a aplicar por parte del proveedor para garantizar que la información recopilada no vaya a caer en manos indebidas.

Dentro del ejercicio realizado en el Seminario de Profundización se encontraron serias deficiencias en el acuerdo de confidencialidad revisado dado que no se cumplía el código de ética del COPNIA como la ley 1273 de 2009, por lo que se pudo concluir que se carecía de un marco legal que pudiera sustentar las actuaciones técnicas y hacia que estas fueran susceptibles a consecuencias de carácter legal.

Adicional a esto, se indica otro documento importante a suscribir el cual es el RoE (Rules of Engagement), el cual sirve para delimitar las acciones, técnicas y procedimientos que pueden ejecutar los equipos de Red Team (principalmente) y Blue Team, lo cual va a servir para determinar el alcance de cada uno de ellos y que estas acciones no vayan en contravía de las disposiciones legales del sitio donde se esté desarrollando la actividad. La importancia de este documento es resaltada por Rehberger ((Rehberger, 2020, p. 23-25), quien indica que es necesaria la suscripción del documento para garantizar la debida diligencia en las actividades.

Aspectos Técnicos de los Equipos de Red Team

Dentro del desarrollo del seminario especializado las actividades de Red Team se delimitaron a realizar una réplica en una copia forense del compromiso realizado por parte del

actor malicioso a la máquina de la entidad estatal, como se muestra en los siguientes pasos del proceso de pentesting:

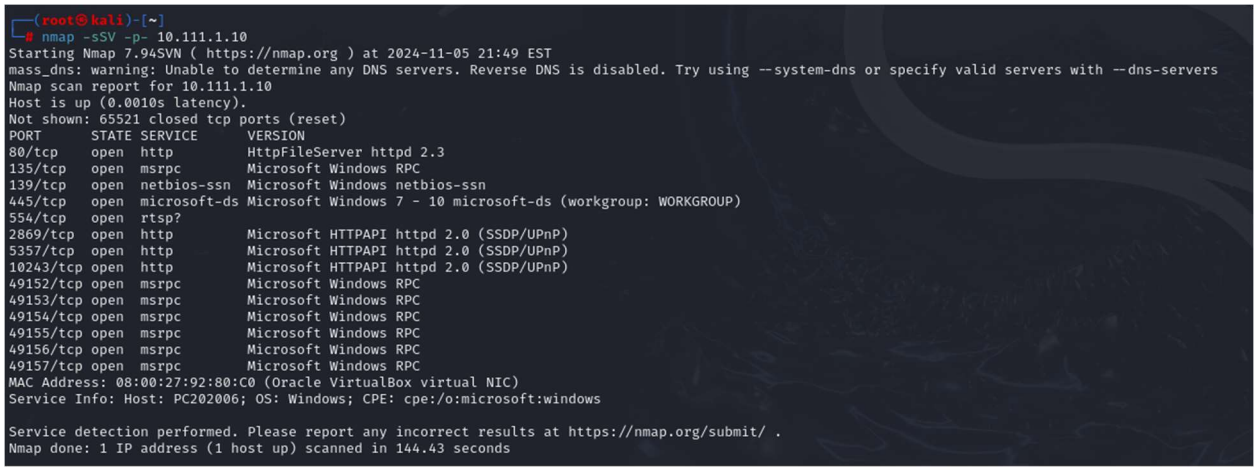
Descubrimiento y Enumeración de puertos.

Teniendo en cuenta lo indicado en el anexo 4 – escenario 3, se procedió a realizar una revisión de los puertos abiertos en la maquina replica a fin de conocer cuál fue la posible superficie de ataque identificada por el actor malicioso.

La herramienta elegida para esto fue nmap, donde mediante el comando nmap -sSV -p- 10.111.1.10 se hizo el escaneo de puertos pertinente encontrando lo que se muestra en la figura 1.

Figura 1

Ejecución de escaneo de puertos con detección de versiones de servicios en nmap



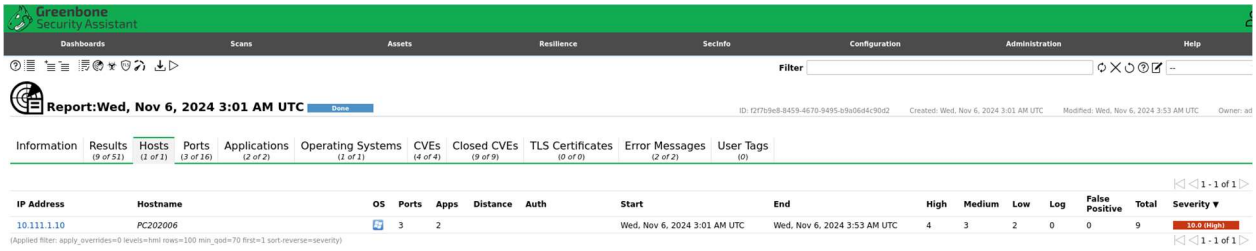
Nota: Elaboración propia

Escaneo de Vulnerabilidades.

Una vez se determinaron los puertos abiertos en el equipo, se procedió a realizar un escaneo de vulnerabilidades a los servicios identificados, apoyado por la herramienta Greenbone Security Assistant o GVM(antiguo OpenVAS) como se muestra en la figura 2.

Figura 2

Escaneo de vulnerabilidades a máquina victima

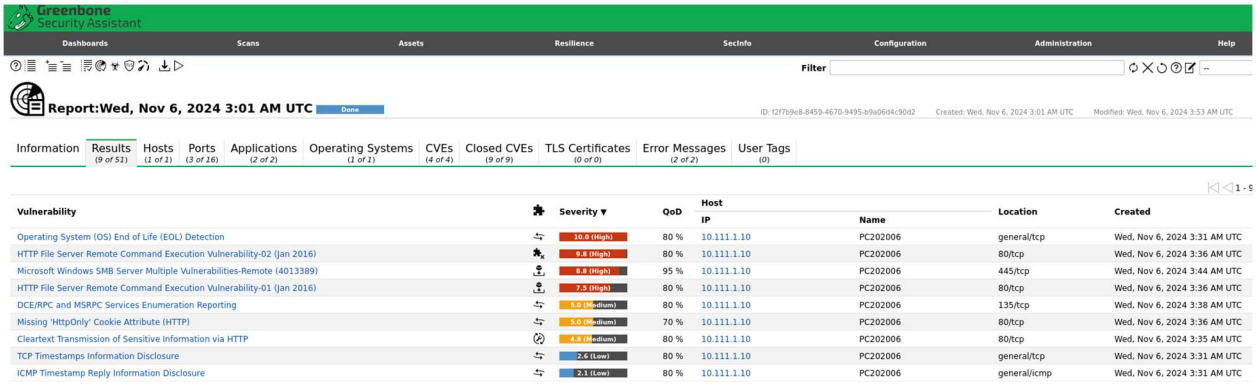


Nota: Elaboración propia

Al verificar los resultados del escaneo, se encontraron cuatro vulnerabilidades relevantes para el análisis, una indicando el estado de obsolescencia del sistema operativo, otra indicando múltiples vulnerabilidades a nivel del protocolo SMB y dos relacionadas con el servicio ejecutado en el puerto tcp/80 como se muestra en la figura 3.

Figura 3

Vulnerabilidades identificadas en maquina victima por parte de GVM



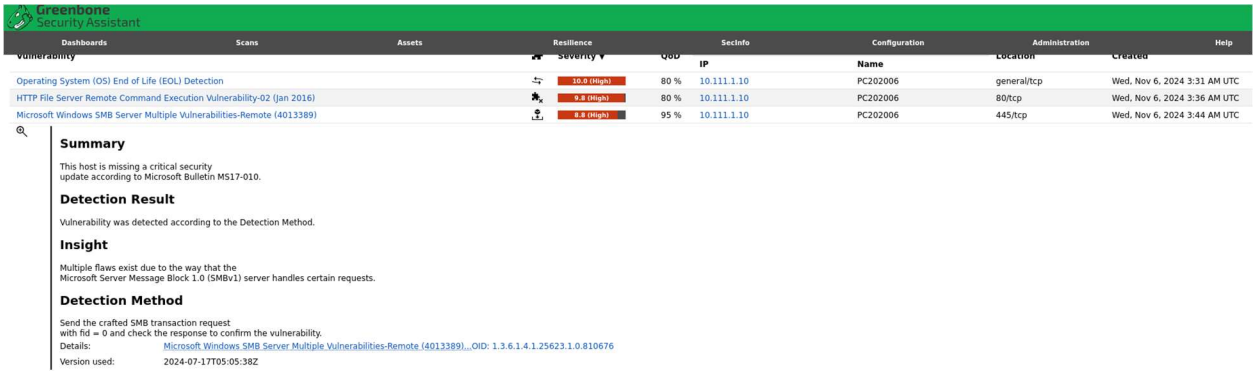
Nota: Elaboración propia

Dado lo anterior, se consideró relevante la revisión a profundidad de las vulnerabilidades del protocolo SMB y las identificadas en el puerto tcp/80. Inicialmente revisando la vulnerabilidad del protocolo SMB reportada por la aplicación GVM, se identificaron dos detalles fundamentales como se muestra en la figura 4:

- Falta de aplicación de parche de seguridad del boletín MS17-010 (Corrección de
- Posible uso de SMBv1.

Figura 4

Detalle de vulnerabilidad identificada en servicio SMB – maquina victima

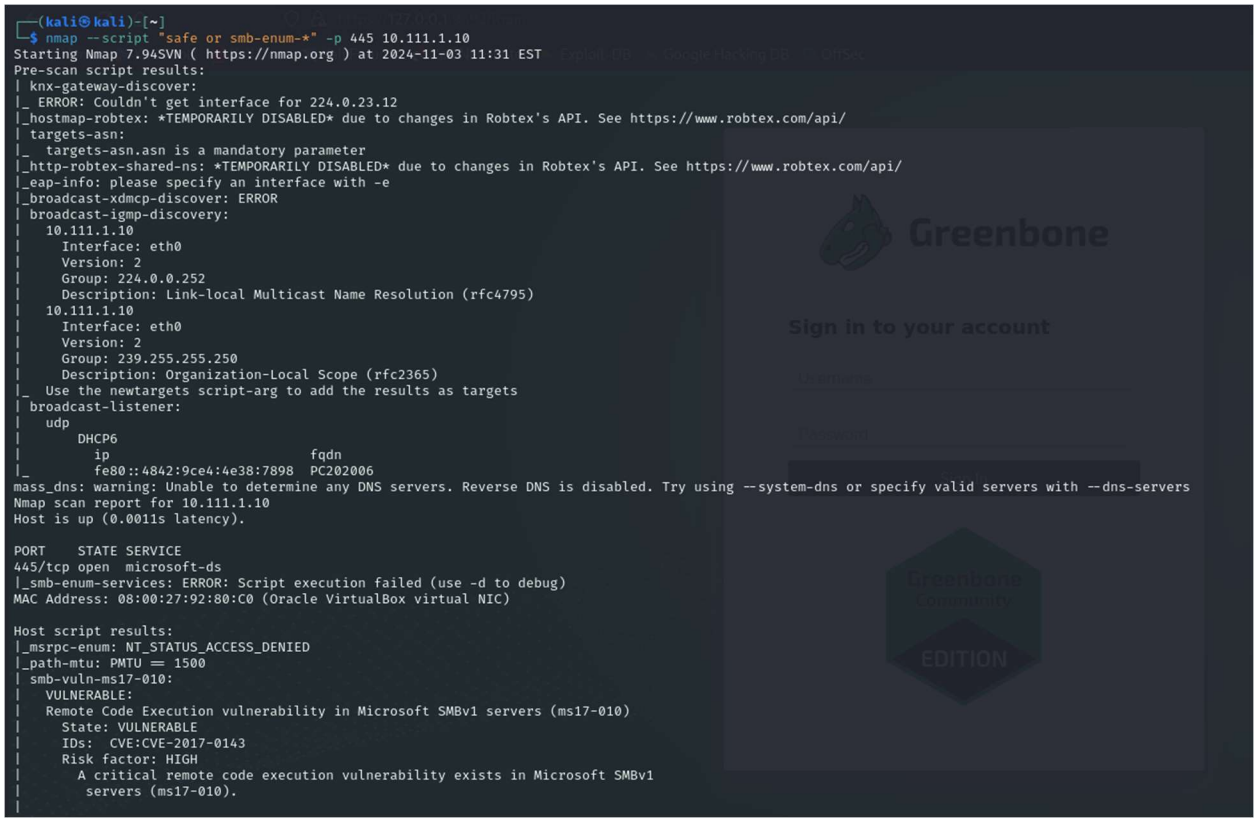


Nota: Elaboración propia

A fin de verificar los hallazgos en el escaneo, se ejecutó de nuevo nmap con unos parámetros puntuales (--script “safe or smb-enum-*”), encontrando que efectivamente el objetivo utiliza SMBv1 y adicionalmente se detecta el servicio SMB como vulnerable a los CVE-2017-0143, CVE-2017-0144 que permite que se pueda hacer ejecución remota de comandos (RCE) como se muestra en la figura 6. Cabe destacar que estas vulnerabilidades son las que fueron explotadas en su momento mediante el exploit EternalBlue y que fueron aprovechadas en el ciberataque denominado WannaCry en el 2017.

Figura 5

Detalle de ejecución de scripts smb de nmap en maquina victima

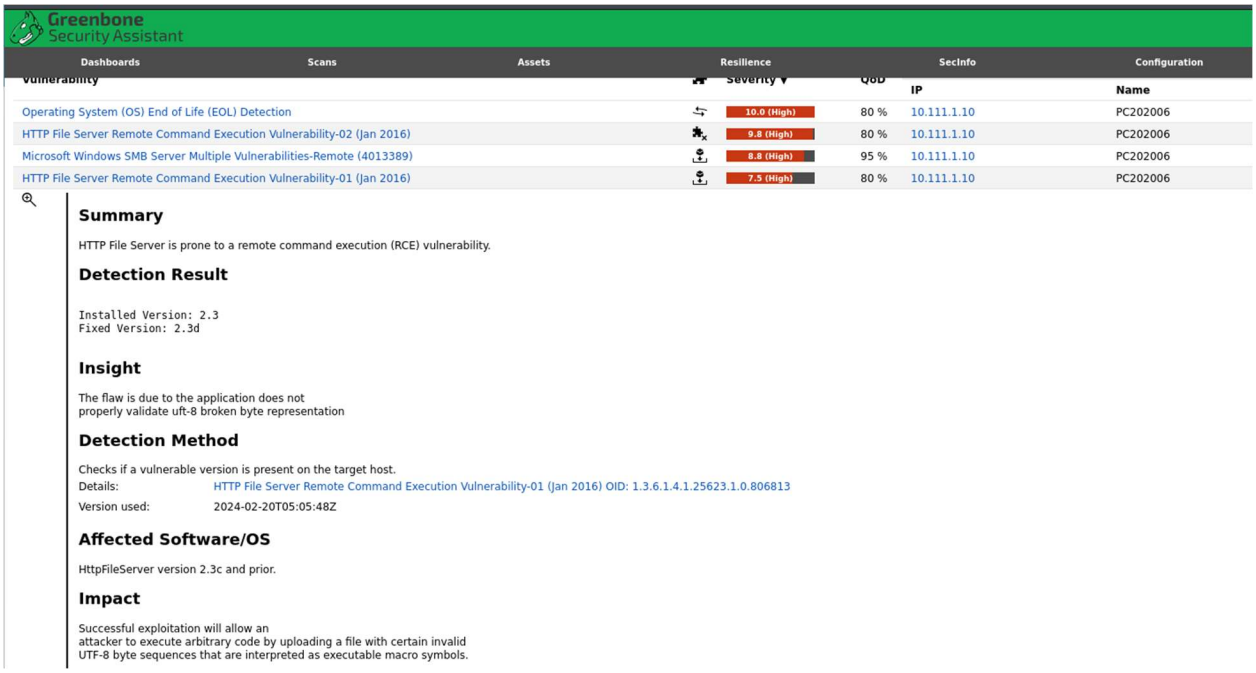


Nota: Elaboración propia

Por otra parte, las vulnerabilidades de nivel alto identificadas en el puerto tcp/80 están relacionadas con la versión de la aplicación HTTP File Server (para el caso del activo analizado, la 2.3), la cual es susceptible a ejecución remota de comandos (CVE-2014-6287, CVE-2014-7226), como se puede observar en la figura 6.

Figura 6

Detalle de vulnerabilidades identificadas por GVM en servicio HTTP File Server (tcp/80) de maquina victima



Nota: Elaboración propia

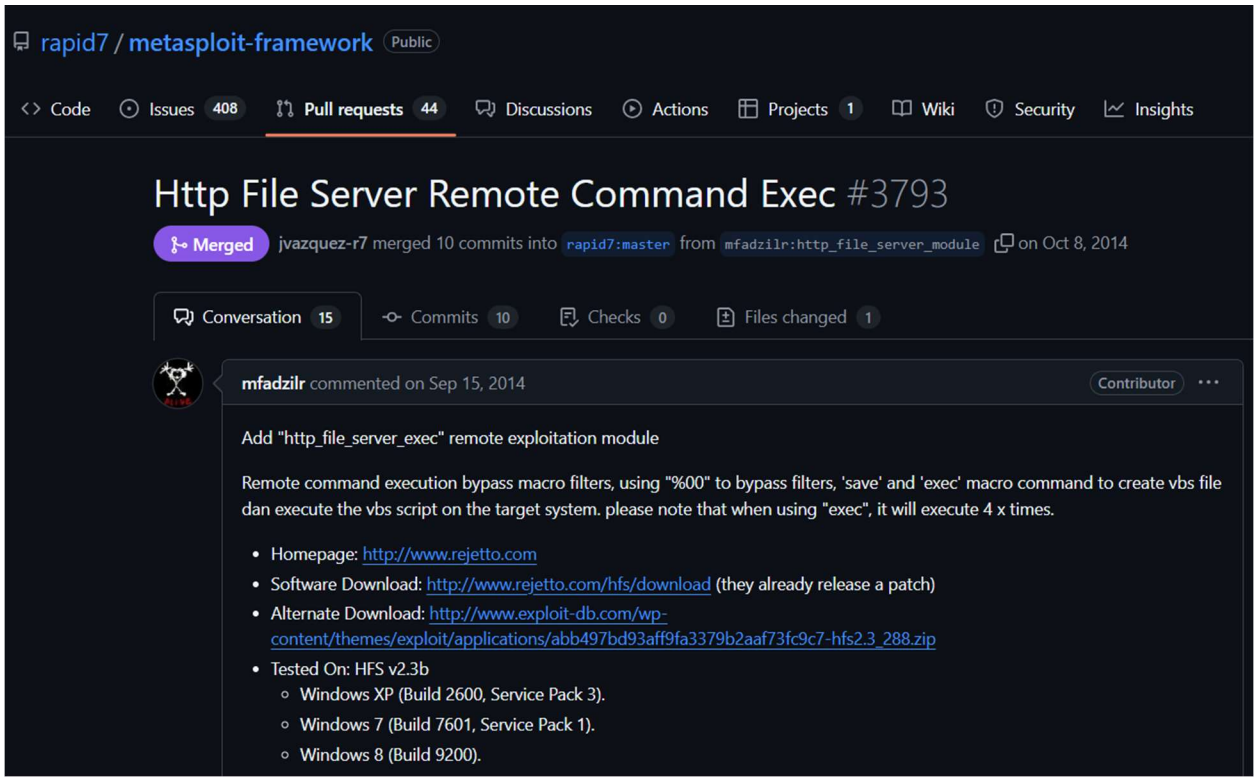
Tal y como lo indica el NIST en la NVD (NVD, 2021), la vulnerabilidad afecta a las versiones 2.3x de la aplicación, debido a un fallo en el manejo de expresiones regulares en una librería usada por esta. Al enviar una búsqueda con los caracteres “%00” (null byte) y comandos de la aplicación, la aplicación ejecutará este ultimo de forma directa en el activo evaluado. Como se menciona igualmente en la NVD, la vulnerabilidad fue resuelta por el fabricante en las versiones 2.3c y posteriores.

Explotación.

Para la fase de explotación, se realizó la búsqueda de exploits públicos para las vulnerabilidades detectadas en la fase anterior del proceso de pentesting, encontrando que tanto para el CVE-2017-0143 (SMB) como para los CVE-2014-6287, CVE-2014-7226 (HTTP File Server) existen exploits que ya están incluidos en el framework Metasploit como se muestra en la figura 7.

Figura 7

Reporte en github de Metasploit de inclusión de exploit para vulnerabilidad en Rejetto



Nota: Elaboración propia

A fin de validar la información encontrada, se hizo la revisión directa en la herramienta tanto de la existencia del exploit EternalBlue para las vulnerabilidades de SMB como para las

vulnerabilidades del servicio HTTP File Server. Como se observa en las figuras 8 y 9, hay existencia de dichos exploits en Metasploit.

Figura 8

Resultado de búsqueda de exploit SMB en Metasploit

Nota: Elaboración propia

Figura 9

Resultado de búsqueda de exploit de aplicación Rejetto HTTP File Server en Metasploit

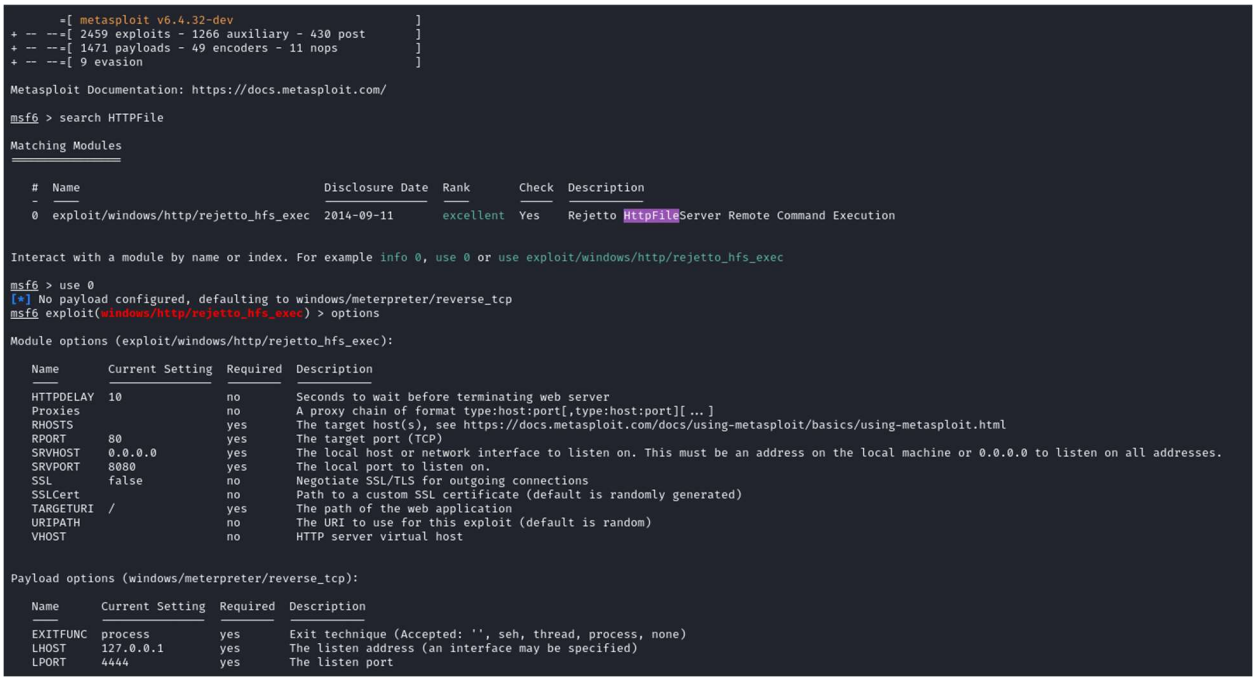
Nota: Elaboración propia

Se realizó la prueba con el exploit de la aplicación Rejetto HTTP File Server, donde al seleccionarlo y verificar las opciones disponibles en Metasploit mediante la ejecución del

comando *options*, se pueden personalizar varios valores como el objetivo (RHOSTS, para este caso el 10.111.1.10), el puerto de la aplicación (RPORT – para este caso, el tcp/80) y demás como la ruta de la aplicación y si se va a utilizar un proxy para acceder al equipo víctima. Adicional a esto, para la apertura de la sesión remota se requiere configurar la dirección IP del equipo que estará a la escucha de la apertura de la shell de tipo reverse_tcp en el equipo víctima y el puerto por donde se estará escuchando, que por defecto asigna el tcp/444. Se puede observar en la figura 10, lo mencionado anteriormente.

Figura 10

Opciones de exploit HTTP File Server RCE - Metasploit

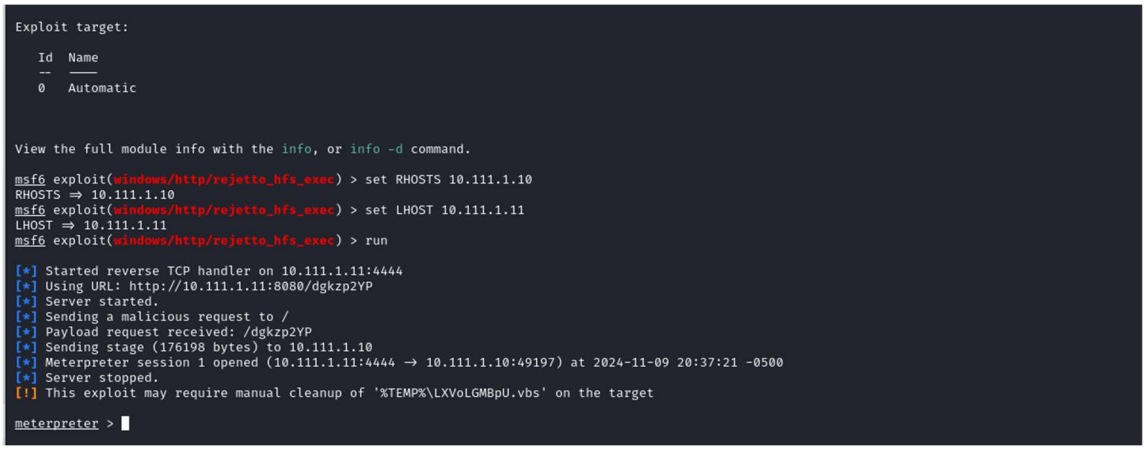


Nota: Elaboración propia

Al configurar los parámetros de RHOSTS, LHOST y ejecutar el exploit mediante el comando run, se pudo observar que se abrió una sesión de tipo Meterpreter en la maquina objetivo como se muestra en la figura 11.

Figura 11

Configuración de parámetros de exploit y ejecución de este - Metasploit

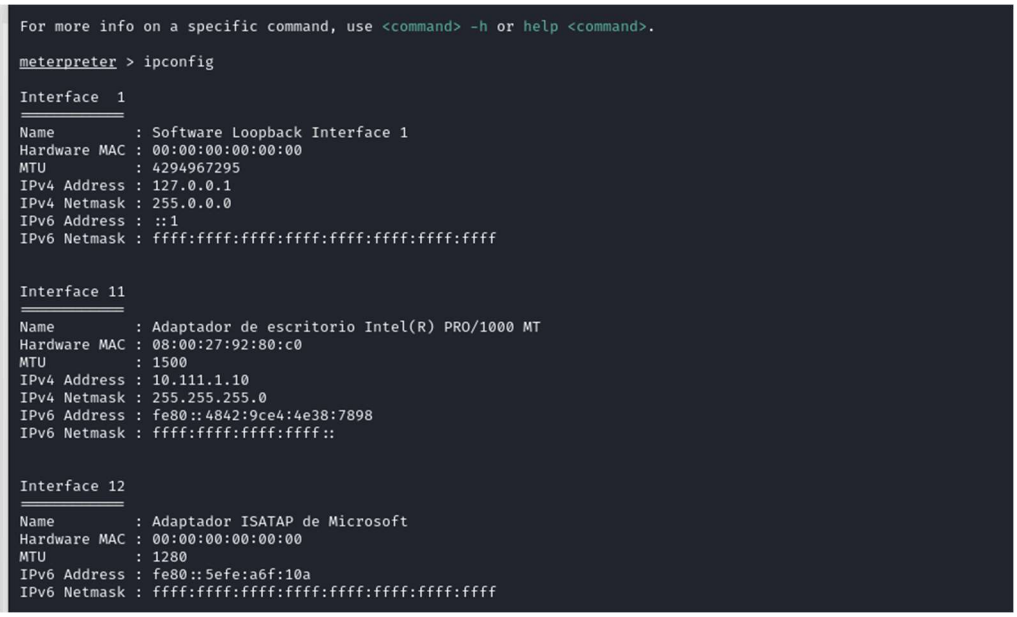


Nota: Elaboración propia

Una vez abierta la sesión meterpreter, se validó que se estuviera dentro del objetivo mediante el comando ipconfig, donde nos mostró las interfaces de red del equipo donde se abrió la sesión y confirmando la intrusión en el equipo victima (10.111.1.10) tal y como se observa en la figura 12.

Figura 12

Ejecución de comando ipconfig en sesión meterpreter establecida por exploit



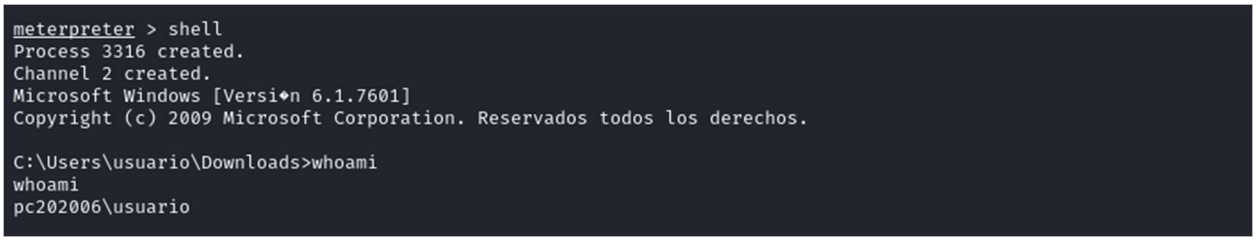
Nota: Elaboración propia

Escalamiento de privilegios.

Teniendo una sesión de meterpreter desde el paso anterior de explotación y generada una Shell mediante el comando s*hell*, se validó el usuario con el cual se tenía abierta esta. Esto se pudo realizar mediante la ejecución el comando whoami. Como se muestra en la figura 13, el usuario fue uno local en la maquina PC202006 llamado *usuario.*

Figura 13

Escalamiento de sesión meterpreter a Shell interactiva y validación de usuario con el que se creó la conexión.



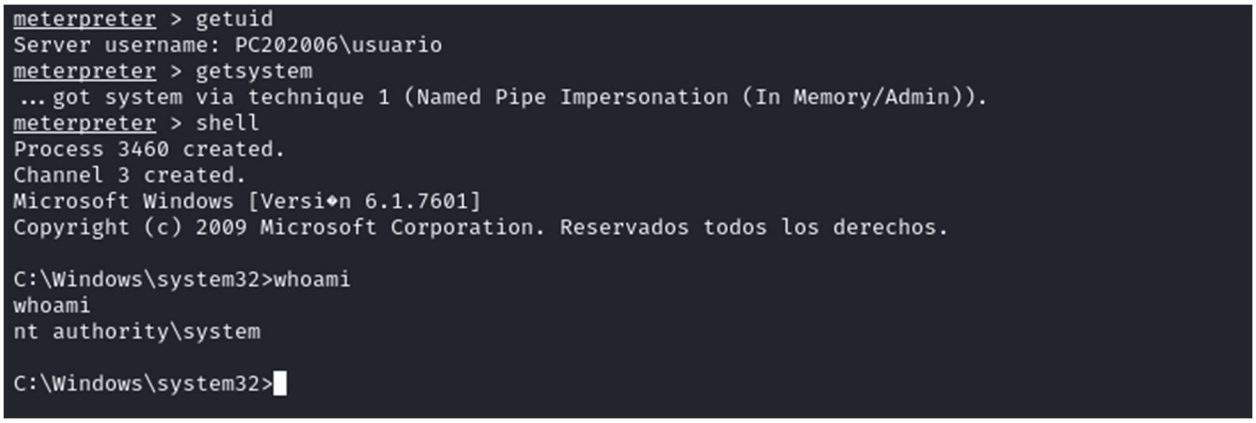
Nota: Elaboración propia

Volviendo a la sesión de meterpreter, dentro de los comandos que se podían ejecutar dentro de esta según la ayuda de Metasploit, estaba uno destinado a validar si se podía escalar privilegios hacia el usuario SYSTEM. La cuenta SYSTEM o como NT AUTHORITY SYSTEM como se conoce de forma completa, es una cuenta de carácter especial que tiene privilegios aún más altos que los que puede tener un usuario administrador de forma local.

Al ejecutar el comando getsystem, se indicó que la tarea fue exitosa y al lanzar de nuevo la Shell interactiva, se realizó la validación del usuario con el que se estaba ejecutando esta, se encontró que el usuario era NT AUTHORITY\SYSTEM, con lo cual se pudo escalar privilegios dentro del sistema, como se muestra en la figura 14.

Figura 14

Escalamiento de privilegios mediante meterpreter, apertura de Shell interactiva y validación de usuario de la sesión



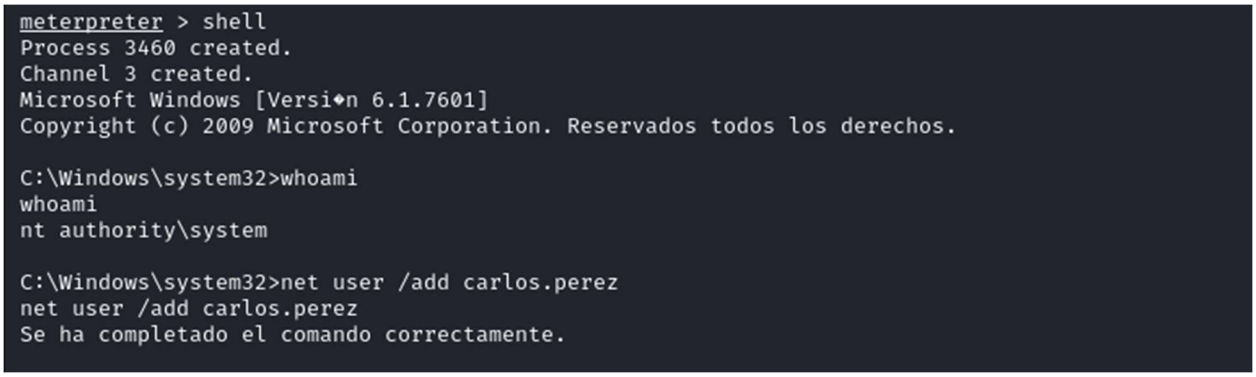
Nota: Elaboración propia

Persistencia.

Una vez logrado tener privilegios elevados como SYSTEM, se realizó la creación de un usuario local y se agregó al grupo de Administradores, como se muestra en las figuras 15 y 16, demostrando el riesgo critico que tiene la vulnerabilidad explotada en la aplicación Rejetto HTTP File Server.

Figura 15

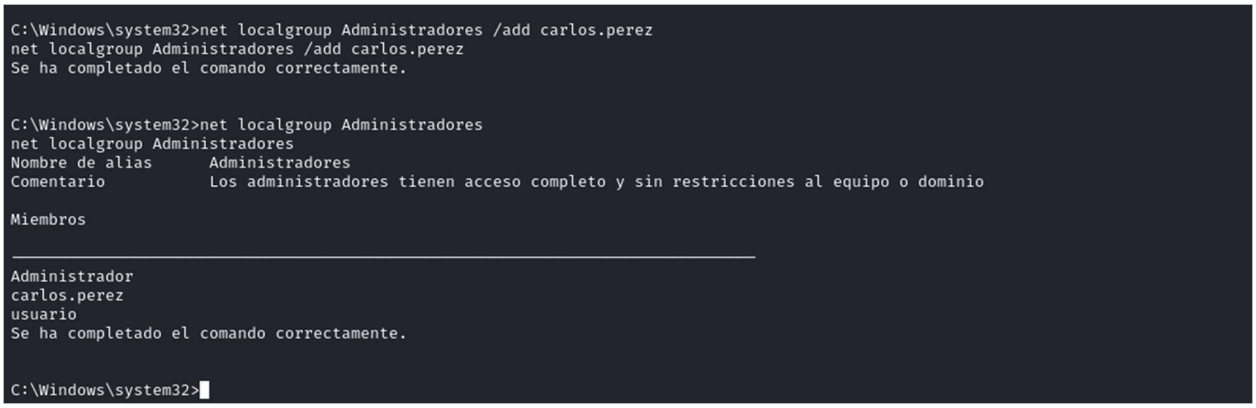
Creación de usuario local en maquina victima mediante Shell interactiva desde maquina atacante



Nota: Elaboración propia

Figura 16

Adición de usuario local a grupo de administradores y validación de este en Shell interactiva



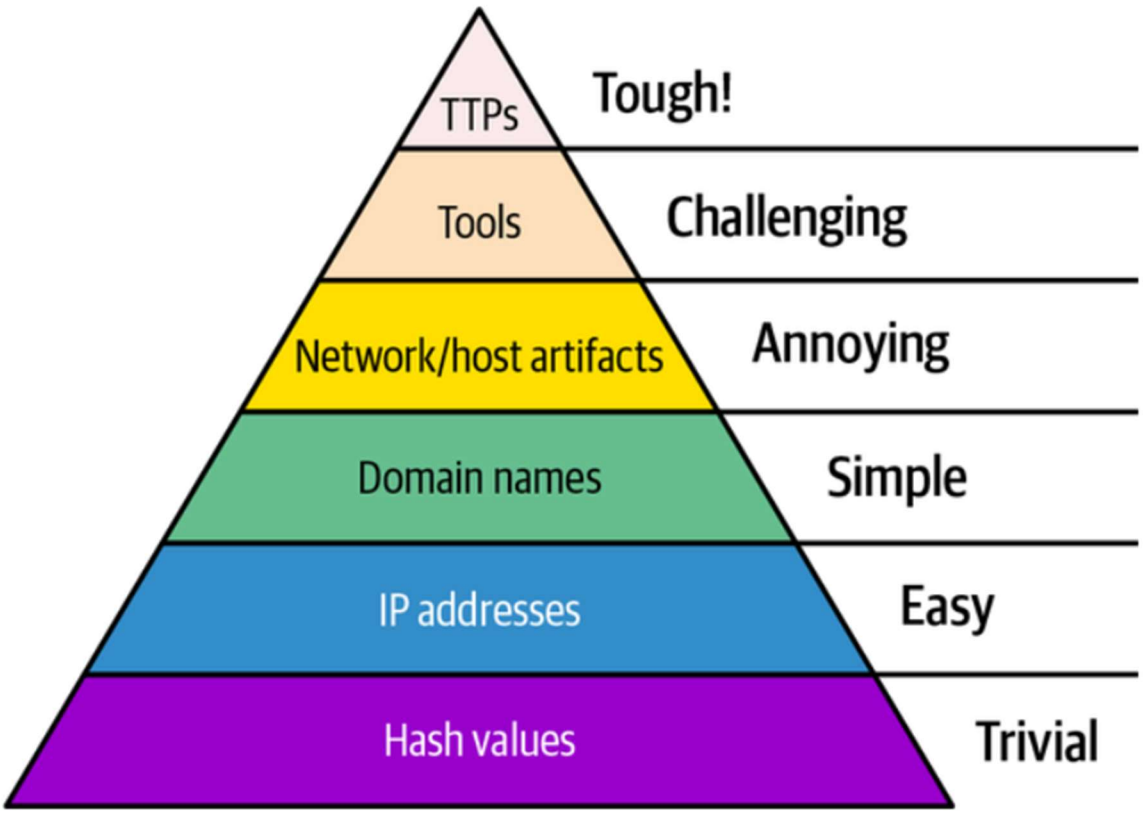
Nota: Elaboración propia

De acuerdo con la actividad realizada, se pueden mencionar aspectos importantes de los equipos de Red Team dentro de las organizaciones:

- Las actividades que realizan son útiles para conocer no solo las debilidades de los activos protegidos, sino también el verdadero impacto de la explotación de las vulnerabilidades que se encuentren estos, lo cual sirve para mostrar a la alta dirección la importancia de realizar acciones de mitigación y/o remediación de estas.
- Las operaciones de Red Team adicional a las actividades básicas de pentesting, se encargan de realizar investigación de posibles adversarios o actores maliciosos (inteligencia de amenazas) que pueden comprometer la infraestructura o servicios de la organización, lo que implica llegar a conocer TTP (Tácticas, Técnicas y Procedimientos) asi como las herramientas usadas por estos, es decir su comportamiento. Como menciona Selmanaj (Selmanaj, 2024, p. 12-13) al conocer el comportamiento del adversario y aplicar la pirámide de dolor de Bianco (ver figura 17) al momento de defender los activos, es decir no ir solo al tradicional bloqueo de IP/URL, hashes o dominios que se conoce; el costo de la operación del actor malicioso se hará cada vez mucho más alto, ya que al identificar/bloquear herramientas o al hacer que las TTP utilizadas por ellos sean inútiles, este tendrá que modificar su comportamiento por completo, lo cual implicará un cambio de estrategia (costo en tiempo) así como la consecución de nuevas herramientas (costo monetario).

Figura 17

Pirámide de Dolor de Bianco



Nota: Adaptado de David Bianco's Pyramid of Pain por Selmanaj, D. (2024). Adversary Emulation With MITRE ATT&CK: Bridging the Gap Between the Red and Blue Teams

- Adicional a la investigación, se debe realizar por parte de los equipos Red Team la parte de simulación de adversarios. Esto implica que se evalúen las defensas de la organización (Blue Team) en cuanto a las medidas actuales de protección implementadas en los activos relevantes o susceptibles a ser blanco de ataques, los

procesos de detección y por supuesto la respuesta de estos. Todo esto, mediante la replicación del comportamiento de los posibles actores maliciosos. Esto proporcionará valiosa retroalimentación continua de los posibles puntos de mejora a nivel defensivo que se deben aplicar en la organización, dado el carácter evolutivo de los actores maliciosos y las formas en las cuales pueden comprometer la seguridad de la información de las empresas. Resaltar aquí que es importante que para la simulación de las actividades, no debe haber aviso de estas a los equipos Blue Team, ya que se pierde el carácter de estas.

- Tener en cuenta las diferencias entre las actividades de escaneo de vulnerabilidades, análisis de vulnerabilidades, pentesting y red team, ya que cada una entrega una salida diferente y tienen niveles distintos de complejidad, siendo la actividad de "*Red Teaming"*, la que más se acerca a la evaluación completa de la fortaleza defensiva de la organización.

Algo muy importante a adicionar dentro de los procesos de Red Team a ejecutar en las organizaciones es que no solo se deben tener en cuenta las amenazas externas sino también las que pueden provenir de atacantes internos o *insiders***.**

Aspectos Técnicos de los Equipos de Blue Team

Como actividad posterior a la realizada por parte del Red Team y tomando como referencia la documentación de la vulnerabilidad aprovechada en el ejercicio del seminario

especializado, así como las acciones realizadas para la explotación de esta, se propusieron las siguientes medidas para evitar la reincidencia en la afectación, asi:

- De acuerdo con las recomendaciones del fabricante, en lo posible utilizar la última versión de la aplicación Rejetto HFS (v3), dado que utilizar una versión de la familia 2.3 o 2.4 hace que el sistema sea susceptible a una vulnerabilidad reciente (CVE-2024-23692) que también permite la ejecución remota de comandos sin requerirse credenciales de usuario. Al igual que la vulnerabilidad explotada en el ejercicio de Red Team, esta vulnerabilidad reciente ya tiene exploits públicos. Cabe anotar que la mínima versión de sistema operativo requerida para ejecutar la versión 3 de Rejetto HFS es Windows 8.1 o Windows Server 2012.

Dado que la acción de remediación principal no sería posible de aplicar en el sistema operativo evaluado, se recomiendan las siguientes acciones de mitigación, lo cual indica que, si bien la vulnerabilidad va a seguir presente, se minimizará el riesgo de explotación de esta.

- Instalación de una herramienta de detección de intrusiones ya sea a nivel de la red (tipo SNORT) o a nivel del equipo con un agente (Wazuh). Esto permitirá que se pueda realizar un proceso de detección y contención más adecuado, dada la falta de herramientas de seguridad en el equipo analizado.
- Realizar la configuración de AppLocker mediante la creación de políticas que permita establecer bloqueo para la ejecución de scripts (en el caso del ejercicio de Red Team, el

exploit ejecuta un archivo .vbs que ejecuta una petición que trae el payload para realizar la conexión entre la víctima y el atacante)

- Aplicar las recomendaciones de CIS Benchmark (CIS Security, 2020) para Windows 7 respecto al punto de User Account Control (UAC) a fin de fortalecer la seguridad respecto a los archivos ejecutables.
- Realizar la revisión de parches faltantes de sistema operativo, teniendo en cuenta que en el ejercicio de Red Team se encontró que el equipo es susceptible a Eternal Blue (Vulnerabilidades de SMBv1).
- A fin de mejorar el perfil de seguridad de la información de la organización, realizar la implementación de herramientas de seguridad en la red como Firewalls para control de trafico y segmentación de la red, SIEM para la recopilación y correlación adecuada de eventos de los diferentes activos, asi como agente de EDR/XDR en los dispositivos.

Adicional a lo anterior, para términos de las acciones para su ejecución en caso de presentarse un ataque, lo ideal en este punto es que se tenga un procedimiento adecuado para la revisión y detección de un ataque por parte un actor malicioso, lo cual lleve a su aplicación de forma organizada a fin de permitir las actividades de contención e investigación posterior. Para este efecto, las acciones a realizar estarían enmarcadas en lo mencionado por el NIST (NIST, 2012) en su guía de manejo de incidentes de seguridad, lo indicado por ICONTEC (ICONTEC, 2024) en la ISO/IEC 27035, así como lo mencionado en la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (MINTIC, 2016), como se indica a continuación:

- Identificar la naturaleza del evento que indica un comportamiento anómalo identificado en el equipo afectado (aumento de consumo de recursos del equipo, cifrado de archivos, aumento inusual en el tráfico de red, caída del servidor, alertas de antivirus (si bien para el caso evaluado no existe una herramienta instalada, es necesario monitorearla en caso de que exista), u otras actividades anormales que puedan detectarse.
- Evaluar a partir de la identificación del evento y su categorización, la afectación en el activo
- Revisar las conexiones de red a servicios/procesos existentes en el equipo, a fin de identificar si existe alguna anomalía que pueda indicar una variación frente a la línea base normal de funcionamiento.
- Revisar los procesos en ejecución en el equipo en busca de anomalías (ej: nombres anormales de procesos (aleatorios como en el caso de lo visto en el laboratorio)) que indiquen una variación frente a los procesos normales que se deberían observar en el dispositivo.
- Revisar los logs del sistema a fin de identificar eventos que puedan indicar modificaciones no autorizadas en el sistema operativo (creación de usuarios, eliminación de usuarios, elevaciones de privilegios, eliminación de logs, ejecución de scripts (ej: PowerShell)).
- Realizar la recolección de la mayor cantidad de evidencia en el momento del ataque que permita posteriormente la investigación del incidente y la generación del informe respectivo que permita tomar las acciones correctivas para minimizar la reincidencia del evento malicioso.

- Tomar las acciones a fin de contener el evento malicioso y evitar la posible propagación a otros equipos de la red, las cuales pueden ser el aislamiento de la maquina afectada, el bloqueo de direcciones IP maliciosas o aplicación de firmas en dispositivos de seguridad perimetral o el bloqueo de cuentas comprometidas.

Es indispensable que dentro de toda la actividad se realice la documentación necesaria y exigida en el procedimiento de atención de incidentes a fin de que sirva como insumo para la fase de lecciones aprendidas que se realiza post incidente.

Siendo lo anterior hay que resaltar que de acuerdo con la revisión documental (Sehgal & Thymianis, 2023, p. 13-14), el equipo de Blue Team está orientado a realizar como tarea principal, el monitoreo y vigilancia constante de los activos de información por medio de las herramientas de seguridad que se dispongan en la organización, así mismo apoya en el establecimiento de controles de seguridad mediante la recomendación de estos de acuerdo con los riesgos que pueden afectar los activos de información protegidos y las vulnerabilidades detectadas en estos. Por otra parte, también se encargan de la planeación de la respuesta ante ataques con el equipo de respuesta a incidentes, observando las lecciones aprendidas y las conclusiones generadas de actividades previas, así como la generación de guías de respuesta (playbooks).

Como se puede ver, hay un carácter preventivo en las actividades del equipo de Blue Team, sin embargo, su existencia no se puede ver como la de una entidad aislada, sino que debe interactuar con el Red Team a fin de complementar su estrategia y enriquecer las actividades

defensivas de la organización. por lo cual es importante dentro del presente trabajo mencionar el concepto de *Purple Team*.

El equipo purpura o Purple Team es una forma de unir las capacidades de los equipos de Blue Team y Red Team no solo como personas sino también como una forma de ver la ciberseguridad como un todo, conllevando a la colaboración entre partes y a la realización de actividades para mejorar los equipos y, por ende, la seguridad de la información de la organización. Este proceso continuo, conlleva a que haya investigaciones previas de TTP de actores maliciosos gracias a las capacidades de ciber inteligencia (ya sea integradas al Blue Team como parte interna o como equipo separado), se ejecuten dichas TTP por parte del equipo Red Team, se documenten los resultados obtenidos en los dos equipos y posteriormente se identifiquen cuales fueron las brechas de seguridad identificadas para su priorización de acuerdo con el nivel de criticidad de los activos afectados. Una vez se hace la implementación de medidas (que puedan subsanarse prontamente) para remediar las brechas de seguridad por parte del equipo Blue Team, posteriormente se hacen nuevas pruebas para validar la efectividad de estas por parte del equipo Red Team. Para las remediaciones o mejoras dentro del proceso de defensa que requieran mayor tiempo, se debe establecer un plan con actividades puntuales y tiempos estimados para su ejecución, lo cual va a permitir su medición posterior.

Es importante que en pos de la mejora continua buscada se retroalimente por parte de los dos equipos, que oportunidades de enriquecer el proceso se pueden observar y por supuesto, que aprendizaje se obtuvo de lado y lado, ya que tanto el equipo Red Team obtendrá conocimiento de como funciona la parte defensiva y que acciones debería buscar aplicar para evadir defensas, como el equipo Blue Team obtendrá conocimiento de cual es el comportamiento de un posible actor malicioso en un ataque real.

Autores como Moreno Garcia (Moreno Garcia, 2022, p. 119), Routin, Thoores y Rossier (Routin et al., 2022, p. 26), Oakley (Oakley, 2019) y Dale (Dale, 2020) coinciden en resaltar la relevancia de la colaboración estratégica entre los equipos de Blue/Red Team, mediante la coordinación de las acciones ofensivas y defensivas a fin de perfeccionar los esfuerzos realizados y así obtener los resultados esperados en busca del mejoramiento de la postura de seguridad de la organización.

Recomendaciones para el planteamiento de estrategias para endurecer los aspectos de seguridad en una organización

Es fundamental tener muy presente que la ciberseguridad en las organizaciones tiene tres pilares fundamentales: las personas, los procesos y la tecnología. Sin involucrar estos tres elementos al tiempo no puede existir una estrategia coherente de ciberseguridad ya que esta debe tener un enfoque sistémico; por ejemplo: ¿De que puede servir un dispositivo de seguridad cuando no existe un procedimiento adecuado para monitorearlo y gestionar los eventos que se presenten? ¿De qué sirve decir en una empresa que tienen certificación ISO 27001 cuando sus empleados tienen contraseñas básicas que pueden ser adivinadas en un ataque simple por diccionario?

Las anteriores son apenas dos ejemplos de situaciones donde la ciberseguridad en las empresas carece de integración entre sus partes, quedando asi brechas que deben ser resueltas.

Siendo lo anterior se proponen las siguientes recomendaciones a fin de mejorar la postura de seguridad de cualquier organización, teniendo como base la estrategia de defensa en profundidad que integra los 3 elementos mencionados con anterioridad, así:

- Definir e implementar una política de seguridad de la información en la organización de preferencia ajustada a estándares como ISO 27001:2022, que este soportada por políticas adicionales, procesos y procedimientos documentados y bien definidos. Esto implica el apoyo de la alta gerencia para su implementación y la capacitación a los integrantes para que haya adherencia a la política establecida.
- Implementar una política de gestión de eventos e incidentes dentro de la organización que permita realizar un proceso de respuesta a estos, ya sea de forma directa o realizada por un tercero.
- Establecer políticas de gestión de accesos e identidad que estén orientadas al principio del "mínimo privilegio" en los dispositivos, aplicaciones y sistemas de la organización.
- Realizar la definición e implementación de líneas base de seguridad y controles para los dispositivos, equipos y aplicaciones que integran la infraestructura de la organización, basado en buenas practicas como las indicadas por el CIS.
- Programar la validación de reglas configuradas en los dispositivos de seguridad y red con una periodicidad mínima de una vez por semestre para garantizar que estas estén ajustadas a los requerimientos establecidos a nivel de seguridad.
- Mantener documentación actualizada de la infraestructura de la organización en cuanto a su topología, direccionamiento, información de direccionamiento IP, sistemas operativos

y servicios, lo cual facilitará el trabajo del equipo de Blue Team y CSIRT al momento de la respuesta frente a un ataque.

- Realizar el proceso adecuado de gestión de riesgos de los activos críticos de la compañía (identificación, evaluación, planes de acción) a fin de determinar la vigencia de las estrategias de protección de estos y aplicar las actualizaciones necesarias según sea el caso.
- Realizar las campañas necesarias de concientización en seguridad de la información a los empleados de la organización para mitigar los riesgos asociados a comportamientos de los usuarios.
- Ejecutar procesos adecuados de selección de personal, identificando personas con suficientes criterios técnicos, éticos y profesionales para adelantar las labores de Red Team o Blue Team.
- Establecer políticas para la ejecución periódica de los planes de mantenimiento y actualización de dispositivos, equipos y aplicaciones, a fin de minimizar los riesgos operativos y de seguridad que se pueden presentar por la falta de aplicación de parches.
- Tener implementado un servicio de backup para los elementos críticos de la organización y definir las políticas necesarias para definir este proceso
- A fin de implementar una base para el servicio de monitoreo, tener un SIEM en el entorno que permita recolectar logs de los elementos importantes de la red como son los servidores, el antimalware (EDR/XDR), equipos de conectividad, IPS/IDS y firewall.
- Realizar evaluaciones periódicas de seguridad en los activos mediante la conducción de pruebas de escaneos/análisis de vulnerabilidades y pruebas de pentesting que permitan

medir el nivel de riesgo de los activos relevantes frente a las vulnerabilidades que están en continuo descubrimiento.

- Realizar pruebas de Purple Team que permitan medir las capacidades defensivas de la organización a fin de determinar las fortalezas y los puntos de mejora a aplicar a fin de mejorar la respuesta frente a las amenazas que se identifiquen.
- Realizar la observancia de la normatividad legal del país donde se esté desarrollando la actividad de Blue Team/Red Team. Importante aquí que se firmen los acuerdos de confidencialidad necesarios al igual que establecer claramente las RoE que permitan delimitar las acciones a desarrollar en las actividades, las responsabilidades civiles, comerciales y penales, así como la observancia de las políticas de la organización.

Conclusiones

De acuerdo con el conocimiento adquirido en el trascurso del seminario especializado mediante las revisiones documentales del tema tratado y su puesta en práctica, se pueden generar las siguientes conclusiones

La actuación de los equipos de Blue Team/Red Team se debe realizar observando la normatividad legal del país donde se esta realizando las actividades, si bien en Colombia existen leyes como la 1273 de 2009 y la 1582 de 2012, en cada país existe su normatividad establecida para la protección de datos y la definición de la ocurrencia de delitos informáticos. Es por esto que, los contratos, acuerdos de confidencialidad y las reglas de compromiso deben definir las labores en concordancia con la parte legal correspondiente.

En el contexto actual de ciberseguridad, ya no es posible contemplar la actuación de los equipos de Red Team y Blue Team como entidades separadas en las organizaciones, debido al carácter complementario de las actividades de cada uno; razón por la cual el concepto de Purple Team toma fuerza como estrategia para mejorar el desempeño de los equipos y por ende de las medidas defensivas a través de la prueba de los procedimientos de detección, respuesta y contención, así como el fortalecimiento de la parte investigativa mediante la identificación de amenazas a través de la ciber inteligencia.

Las estrategias de seguridad en las organizaciones deben ser de carácter integral, incorporando a estas los tres pilares de la ciberseguridad: las personas, los procesos y la tecnología. Pretender no contar con alguno de ellos, puede ocasionar que se creen brechas en las estrategias y van a perder su efectividad para la protección de la seguridad de la información.

Por otra parte, la implementación de estrategias como “Defensa en Profundidad”, “Zero Trust”, así como la adecuada gestión de riesgos en la organización dentro de ciclos de evaluación, retroalimentación y mejora continua, va a permitir el fortalecimiento de la seguridad en la organización, adaptándose así al cambiante panorama de amenazas que presenta el mundo actual.

Recomendaciones

Dentro de las recomendaciones se reitera lo mencionado en el apartado de "Recomendaciones para el planteamiento de estrategias para endurecer los aspectos de seguridad en una organización", asi:

- Definir e implementar una política de seguridad de la información en la organización de preferencia ajustada a estándares como ISO 27001:2022, que este soportada por políticas adicionales, procesos y procedimientos documentados y bien definidos. Esto implica el apoyo de la alta gerencia para su implementación y la capacitación a los integrantes para que haya adherencia a la política establecida.

- Implementar una política de gestión de eventos e incidentes dentro de la organización que permita realizar un proceso de respuesta a estos, ya sea de forma directa o realizada por un tercero.

- Establecer políticas de gestión de accesos e identidad que estén orientadas al principio del "mínimo privilegio" en los dispositivos, aplicaciones y sistemas de la organización.

- Realizar la definición e implementación de líneas base de seguridad y controles para los dispositivos, equipos y aplicaciones que integran la infraestructura de la organización, basado en buenas practicas como las indicadas por el CIS.

- Programar la validación de reglas configuradas en los dispositivos de seguridad y red con una periodicidad mínima de una vez por semestre para garantizar que estas estén ajustadas a los requerimientos establecidos a nivel de seguridad.

- Mantener documentación actualizada de la infraestructura de la organización en cuanto a su topología, direccionamiento, información de direccionamiento IP, sistemas operativos y servicios, lo cual facilitará el trabajo del equipo de Blue Team y CSIRT al momento de la respuesta frente a un ataque.

- Realizar el proceso adecuado de gestión de riesgos de los activos críticos de la compañía (identificación, evaluación, planes de acción) a fin de determinar la vigencia de las estrategias de protección de estos y aplicar las actualizaciones necesarias según sea el caso.

- Realizar las campañas necesarias de concientización en seguridad de la información a los empleados de la organización para mitigar los riesgos asociados a comportamientos de los usuarios.

- Ejecutar procesos adecuados de selección de personal, identificando personas con suficientes criterios técnicos, éticos y profesionales para adelantar las labores de Red Team o Blue Team.

- Establecer políticas para la ejecución periódica de los planes de mantenimiento y actualización de dispositivos, equipos y aplicaciones, a fin de minimizar los riesgos operativos y de seguridad que se pueden presentar por la falta de aplicación de parches.

- Tener implementado un servicio de backup para los elementos críticos de la organización y definir las políticas necesarias para definir este proceso

- A fin de implementar una base para el servicio de monitoreo, tener un SIEM en el entorno que permita recolectar logs de los elementos importantes de la red como son los servidores, el antimalware (EDR/XDR), equipos de conectividad, IPS/IDS y firewall.

- Realizar evaluaciones periódicas de seguridad en los activos mediante la conducción de pruebas de escaneos/análisis de vulnerabilidades y pruebas de pentesting que permitan medir el nivel de riesgo de los activos relevantes frente a las vulnerabilidades que están en continuo descubrimiento.

- Realizar pruebas de Purple Team que permitan medir las capacidades defensivas de la organización a fin de determinar las fortalezas y los puntos de mejora a aplicar a fin de mejorar la respuesta frente a las amenazas que se identifiquen.

- Realizar la observancia de la normatividad legal del país donde se esté desarrollando la actividad de Blue Team/Red Team. Importante aquí que se firmen los acuerdos de confidencialidad necesarios al igual que establecer claramente las RoE que permitan delimitar las acciones a desarrollar en las actividades, las responsabilidades civiles, comerciales y penales, así como la observancia de las políticas de la organización.

Referencias bibliográficas

CIS. (2020, 31 de marzo). *CIS Microsoft Windows 7 Workstation Benchmark - v3.2.0. CIS - Center for Internet Security*. https://learn.cisecurity.org/l/799323/2020-06-16/sscq?_gl=1*1fbs7ch*_ga*ODM3NzI2MDkwLjE3MzIzMjc5NTA.*_ga_3FW1B1JC98*MTczMjMyNzk0OS4xLjEuMTczMjMyOTk4OC4wLjAuMA..*_gcl_au*NTU0MTY5NDUzLjE3MzIzMjc5NTIuMzgyNjA3NjYuMTczMjMyNzk4NS4xNzMyMzI4MDA3*_ga_N70Z2MKMD7*MTczMjMyNzk0OS4xLjEuMTczMjMyOTk4OC42MC4wLjA.

Congreso de la Republica. (s.f.). *Ley 1581 de 2012 - Gestor Normativo. Función Pública*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

COPNIA. (2015). *Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares.* https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Dale, C. (2020). *Red, Blue and Purple Teams: Combining Your Security Capabilities for the Best Outcome. Cyber Security Training* | SANS Courses, Certifications & Research. https://www.sans.org/media/analyst-program/red-blue-purple-teams-combining-security-capabilities-outcome-39190.pdf

Fiscalía General de la Nación. (s.f.). *Cartilla Metodológica de Atención de Delitos Informáticos. Fiscalía General de la Nacion*. https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf

INCIBE. (2021, 25 de mayo). *Información confidencial, secreto profesional. Acuerdos de confidencialidad*. https://www.incibe.es/empresas/blog/informacion-confidencial-secreto-profesional-acuerdos-confidencialidad

Los principales tipos de delitos informáticos y sus características. (s.f.). Universidad Virtual. | UNIR Colombia - Maestrías y Grados virtuales. https://colombia.unir.net/actualidad-unir/tipos-delitos-informaticos/

MINTIC. (2016). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*. https://gobiernodigital.mintic.gov.co/692/articles-150509_G21_Gestion_Incidentes.pdf

Moreno Garcia, M. (2022). *Gestión de incidentes de ciberseguridad*. Ediciones de la U.

NIST. (2012). *NIST 800-61 r2*. https://doi.org/10.6028/NIST.SP.800-61r2

Oakley, J. G. (2019). *Professional Red Teaming*. Apress. https://doi.org/10.1007/978-1-4842-4309-1

Rehberger, J. (2020). *Cybersecurity Attacks – Red Team Strategies*. Packt Publishing.

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Editorial Científica 3Ciencias. https://doi.org/10.17993/ingytec.2018.46

Routin, D., Thoores, S., & Rossier, S. (2022). *Purple Team Strategies: Enhancing Global Security Posture Through Uniting Red and Blue Teams with Adversary Emulation*. Packt Publishing.

Sehgal, K., & Thymianis, N. (2023). *Cybersecurity Blue Team Strategies: Uncover the Secrets of Blue Teams to Combat Cyber Threats in Your Organization*. de Gruyter GmbH, Walter.

Selmanaj, D. (2024). *Adversary Emulation With MITRE ATT&CK: Bridging the Gap Between the Red and Blue Teams*. O'Reilly Media.

Apéndices

Apéndice A

Enlace a video de sustentación del trabajo final del seminario especializado.

https://www.youtube.com/watch?v=XjcBjN-mIGA