CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

ANNYI CATHERINE MAYORGA GALINDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2022

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

ANNYI CATHERINE MAYORGA GALINDO

LUIS FERNANDO ZAMBRANO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

CONTENIDO

Pág.

TABLA DE ILUSTARCIONES

Pág.

GLOSARIO

MAQUINA VIRTUAL: Corresponde a un ambiente virtual, donde facilita la instalación de entornos de prueba sobre los S.O, configurados en el computador, brindando opciones de búsqueda de diferentes vulnerabilidades sobre los servicios montados en los sistemas configurados.

EXPLOIT: Es una fracción de un programa o software, que realiza la explotación de una vulnerabilidad previamente seleccionada, con el fin de visualizar falla y posibles mitigaciones ante la misma.

VULNERABILIDAD: Es un riego o falla alojado en un sistema de información o aplicativo, generando afectaciones de seguridad sobre los datos, posibilitando el acceso a un ciberdelincuente y el control total sobre los mismos.

METASPLOIT: Corresponde a un framework, de uso de código abierto, que facilita la exploración de la vulnerabilidad, brindando toda la información de los sistemas de las maquinas víctimas.

ENTORNO DE PRUEBA: Es un ámbito controlado, para la realización de pruebas de software, sin riegos de afectación sobre servicios ya configurados en otros entornos reales, con el fin de identificar fallas en prevención a los servicios originales.

METERPRETER: Corresponde a un payload, por medio de la interacción de un Shell, donde se visualiza toda la explotación de la víctima.

SISTEMA DE INFORMACION: Es un conjunto de datos, que permite la identificación de los datos por medio del análisis de diferentes plataformas de interacción dentro de una organización.

SISTEMA OPERATIVO: Corresponde a un grupo de programas, que facilita el uso de diferentes aplicativos sobre una computadora.

RESUMEN

En el siguiente documento, se expone el análisis del desarrollo del entorno de pruebas de las actividades anteriormente vistas en el presente seminario dirigido sobre Red Team y Blue Team, donde se proponen diferentes escenarios emitidos por el especialista, ya que a través de su previo conocimiento, se establecen planes de mitigación de riesgos, ante las vulnerabilidades encontradas o que se pueden llegar a presentar en una organización, en este caso WhiteHouse Security, en el laboratorio realizado, se identifican las fallas que se presentan, como sectores de riesgo, tales como en S.O, denegación de servicios, perdida y duplicidad de información, accesos, creación de usuarios con privilegios de administrador, entre otros, brindando control total sobre los servicios utilizados por las organizaciones, generando afectaciones graves ante la seguridad de la información.

PLABRAS CLAVES: Perdida de información, riesgo, vulnerabilidad, sistema operativo, sistemas de información, Red Team y Blue Team.

ABSTRACT

The following document presents the analysis of the development of the testing environment of the activities previously seen in this seminar on Red Team and Blue Team, where different scenarios issued by the specialist are proposed, since through their prior knowledge, establish risk mitigation plans, in the face of vulnerabilities found or that an organization may present, in this case WhiteHouse Security, in the laboratory carried out, the flaws that they present are identified, as risk sectors, such as in OS, denial of services, loss and duplication of information, access, creation of users with administrator privileges, among others, providing full control over the services used by organizations, generating serious effects on information security.

KEY WORDS: Loss of information, risk, vulnerability, operating system, information systems, Red Team and Blue Team.

INTRODUCCIÓN

Por medio de los hallazgos entregados por el equipo rojo y azul, el especialista de seguridad informática, establece el impacto de cada incidente de seguridad de la información sobre los sistemas de la organización, donde a través de la socialización de las herramientas utilizadas en los ambientes de pruebas, se expresa la viabilidad de mitigar el impacto sobre los riesgos de seguridad, ya que se establece los puntos críticos y niveles de criticidad de la vulnerabilidad, para así establecer controles efectivos y planes de trabajo para el resguardo de los datos.

Con la ayuda de variadas fuentes bibliográficas, bases de datos mundiales, se logra mantener una actualización de las vulnerabilidades más conocidas en los S.O, sistemas de información, aplicativos, entre otros, donde a través de estos referentes, se logra certificar y garantizar una mitigación, como también la corrección de vulnerabilidades, evitando riegos potenciales, y protegiendo el activo más importante de una organización que es la información.

1. OBJETIVOS

1.1 OBJETIVOS GENERAL

Analizar los hallazgos emitidos en los laboratorios realizados, estableciendo controles de seguridad, ante las vulnerabilidades encontradas, generando planes de trabajo, para el resguardo y protección de la información, ya que se establece la identificación de vacíos de seguridad en la organización contratante.

1.2 OBJETIVOS ESPECÍFICOS

- Socializar las leyes nacionales y gubernamentales, que rigen el resguardo de la información y datos personales.
- Inspeccionar entes irregulares ante delitos informáticos dentro de la organización.
- Establecer ambientes virtuales, para el estudio de nuevas herramientas de seguridad y prevención de vulnerabilidades en los sistemas.
- Proponer planes de trabajo que genere mitigación de los riegos potenciales en los sistemas de información y aplicativos de la organización.
- Implementar herramientas de seguridad para el resguardo de la seguridad.
- Socializar las pautas de seguridad con empleados y entes regulatorios de las mismas, fortaleciendo conocimientos sobre la protección de los datos, dentro de la organización.

2. DESARROLLO DEL INFORME

De acuerdo con lo estipulado, se procede con la visualización del caso problémico, donde el especialista se ve enfrentado ante la oferta laboral ofrecida por la organización WhiteHouse Security.

2.1. INFORME TECNICO.

A través del análisis del acuerdo de confidencialidad suministrada por la organización, el especialista establece puntos claves con base a su experiencia profesional y ética, resaltando los siguientes ítems donde se presentan irregularidades.

En la Cuarta clausula, correspondiente a las obligaciones del receptor, se identifica el siguiente ítem.

- “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros”.

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

- “Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento”.

En la cláusula octava, correspondiente a las soluciones de discusión.

- “En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security”.

Conforme a los hallazgos dentro del acuerdo de confidencialidad, se identifica irregularidades éticas, profesionales y legales, teniendo en cuenta que no es pertinente no denunciar cualquier acción de espionaje que se establezca sobre un tercero, ya que se estaría violando el debido proceso de la seguridad de la información del mismo, como también se identifica que no es aceptable la prohibición de divulgación de un delito encontrado sobre los procesos cotidianos dentro de la organización contratante, a su vez no es pertinente que proporcionen

responsabilidad absoluta de la información sobre el receptor, ya que el activo es de propiedad de la organización y el receptor solo está ejerciendo su labor de supervisión de los procesos en la misma.

Mediante el acuerdo entregado se evidencia que la organización dentro de sus cláusulas establece quedar exenta ante cualquier responsabilidad, sobre evidencia corrupta alojada dentro de la misma, haciendo responsable al receptor, deber que anteriormente se establecía dentro de sus funciones éticas y profesionales, ya que se encuentra en un rol de auditor de la información, por ende, no pueden ser responsabilidad del mismo, ya que el activo en este caso la información es netamente de propiedad de la organización contratante.

"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"[1].

Se establecen dentro de la ley 1273 los delitos vulnerados en el acuerdo suministrado.

- Clausula Primera

  Artículo 269ª. Donde se constata la falta grave, al realizar alguna inspección o extracción de información de terceros o divulgación de esta, ya que dentro del acuerdo estipula el no reportar ante las autoridades dichos procedimientos ilegales.

- Clausula segunda.

  Articulo 269c. Correspondiente a la interceptación de los datos, donde indica como delito o irregularidad la interceptación de la información almacenada en sistemas informáticos.

- Clausula cuarta.

  Articulo 269f. Correspondiente a la violación de los datos intransferibles de cada persona, ya que dentro del acuerdo se incurre en el delito de extracción de información a terceros, sin ser notificados y sin previo aviso.

  Artículo 269i. El cual corresponde al robo de información a través de herramientas informáticas, donde se manifiesta como delito la manipulación de la información por parte del personal a través de mecanismos de seguridad no autorizados por la entidad.

[1] SIC. LEY 1273 DE 2009. [En línea]. Enero 2019. [Consultado: 19 de febrero de 2022]. Disponible: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Cada uno de estos artículos indica condenas no menores de 48 a 96 meses de pena, por incumplir con procedimientos éticos legales dentro de cada carrera informática o de manipulación de datos o sistemas de información.

Adicional, se establece que por medio del código de ética COPNIA, se suspende la tarjeta profesional, debido a las malas prácticas éticas y profesionales ejecutadas en beneficio propio o de entidades contratantes.

“Como experto enciberseguridad aplicaría a este trabajo en WhiteHouse Security, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio, debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros”.

- Al momento de analizar la situación problémica como competente en la rama de la seguridad de la información expreso que no aplicaría, ya que dentro del código de ética estipulado por COPNIA, rigen puntos importantes, tal como el resguardo y protección de la información, sin importar las presentes auditorías a las que se encuentren asignados.

  Al momento de efectuar los procesos se debe tener en cuenta las leyes estipuladas por el consejo nacional de protección, junto con las fuerzas nacionales policiales, y el entorpecer sus labores judiciales; a su vez dentro del código de ética, se estipula la denuncia de delitos que afecten a la integridad de este, por medio del ocultamiento de información a favor de un tercero o entidad contratante.

Es importante aclarar que en Colombia se rige a través de la ley 1273 de 2009, donde en el caso también de referencia como “OPERACIÓN ANDROMEDA BUGGLY”, donde se habla a cerca de la regulación y medidas de “Investigación halló fallas de seguridad'. No controlaron actividades de personal militar y civil, sobre la información”[2], se establece un precedente ante la organización WhiteHouse Security, como por ejemplo en los siguientes artículos el estado establece un control sobre el cuidado de la información por medio de sus accesos:

- “Artículo 269A: Acceso abusivo a un sistema informático”
- “Artículo 269C: Interceptación de datos informáticos”

Se comprende que por medio de la violación de permisos sobre los sistemas de información de cualquier organización como lo son (ingresos no autorizados,

[2] ELTIEMPO. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [En línea]. Enero 2015. [Consultado: 19 de febrero de 2022]. Disponible: https://www.eltiempo.com/archivo/documento/CMS-15141236

interceptar información, vigilar procesos y acciones de terceros, entre otros), donde se corrobora que, en el acuerdo entregado al especialista, se infringen algunos artículos importantes en el régimen legal y ético de este.

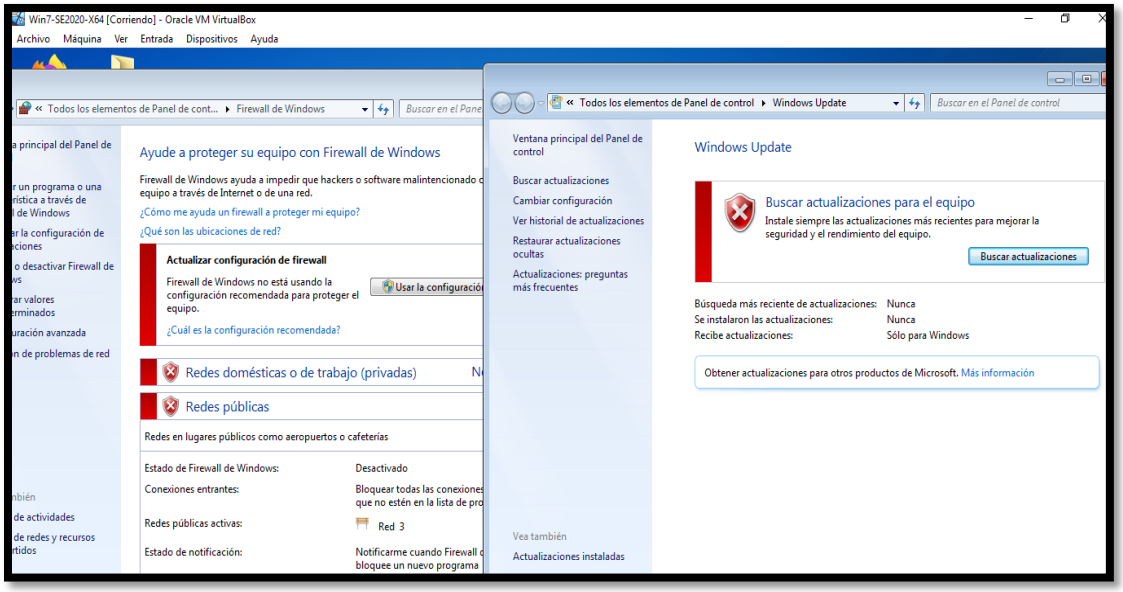
2.1.1. Fase de recolección de datos…

De acuerdo con lo indicado en esta fase, se procede con la recolección de todos los datos que la organización pueda suministrar, junto con toda la información de los sistemas de información y el software utilizado por la misma, una vez se identifique toda la información, se utiliza la herramienta NMAP, ya que, a través de ella, se podrá distinguir que puertos se encuentran abiertos o cerrados dentro de los sistemas entregados, junto con la información alojada en cada uno de estos.

Para establecer la identificación de estas vulnerabilidades, se procede con la desactivación del Firewall de Windows, donde se facilita el análisis a profundidad de todos los servicios de la organización.

- Se procede con la desactivación del Firewall y Update de las máquinas virtuales Win 7 (x86-x64).

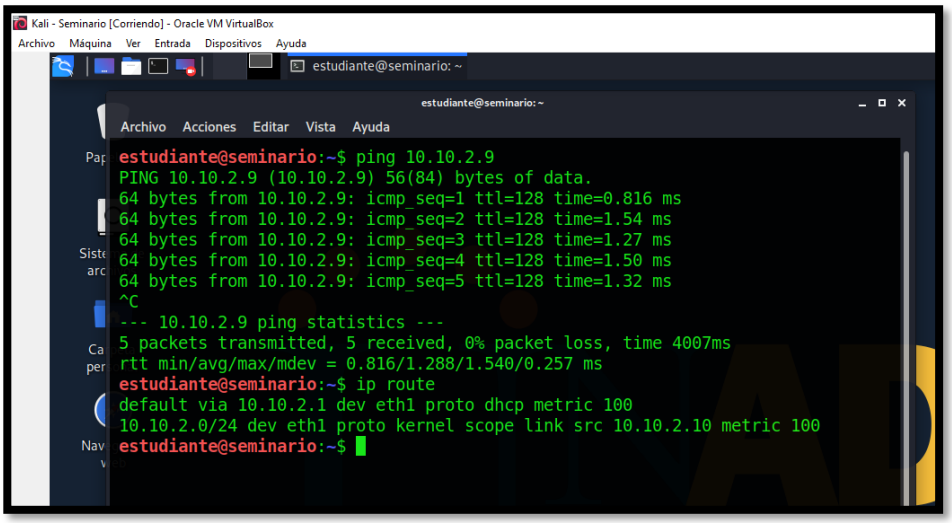
Ilustración 1. Inhabilitar Firewall y Update Win 7 x64.



Fuente: Elaboración propia.

- Reconocimiento del enrutador.

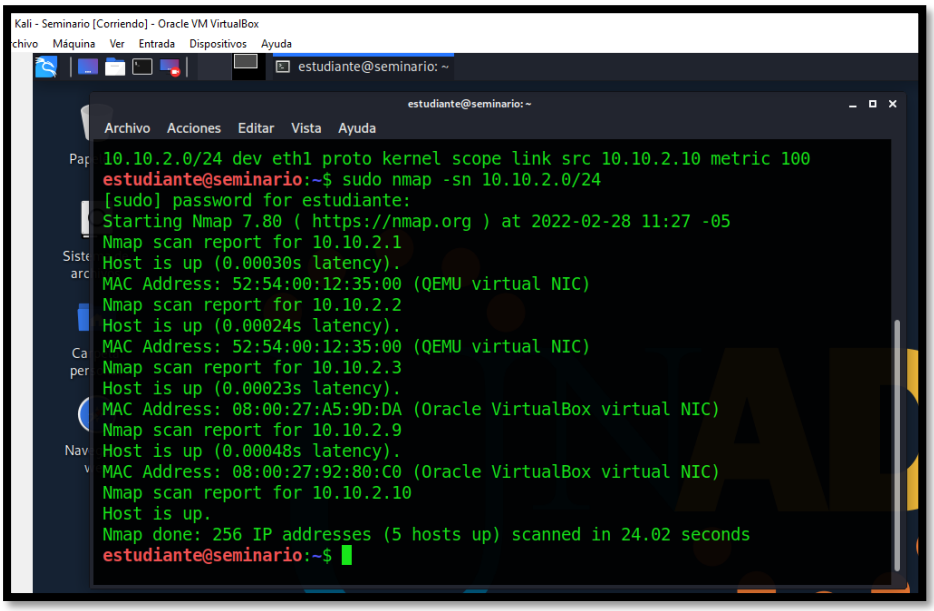
Ilustración 2. Enrutador.



Fuente: Elaboración propia.

- Identificación de los dispositivos que se encuentran conectados a la red 10.10.2.0/24.

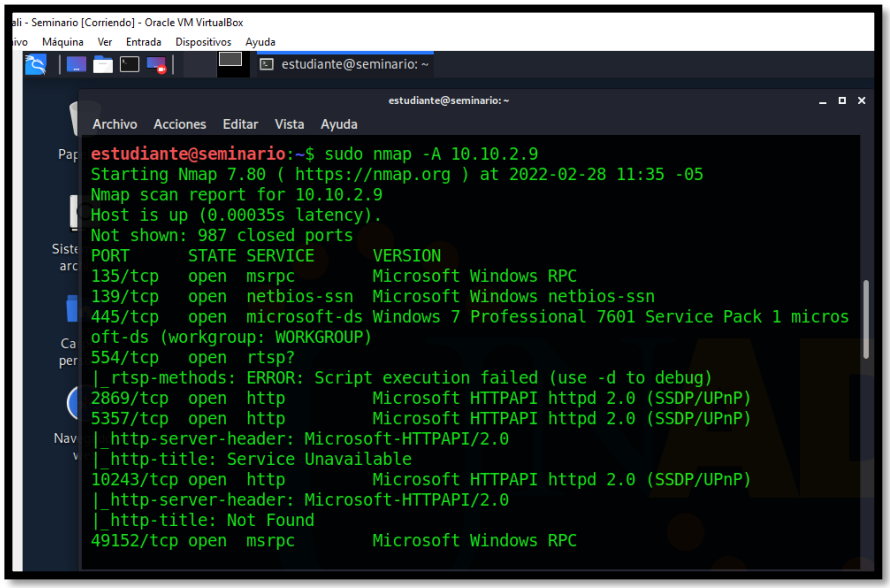
Ilustración 3. Red 10.10.2.0/24.



Fuente: Elaboración propia.

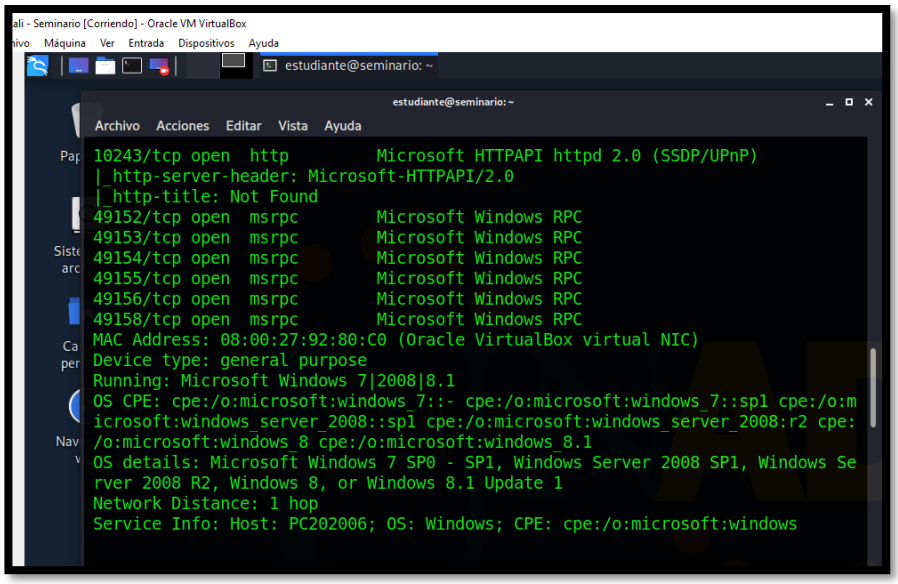
- Reconocimiento de puertos abiertos y servicios alojados en los mismos Win 7 x86 identificada con la IP: 10.10.2.11.

Ilustración 4. Puertos abiertos y servicios Win x64.



Fuente: Elaboración propia.

Ilustración 5. Puertos abiertos y servicios Win x64.

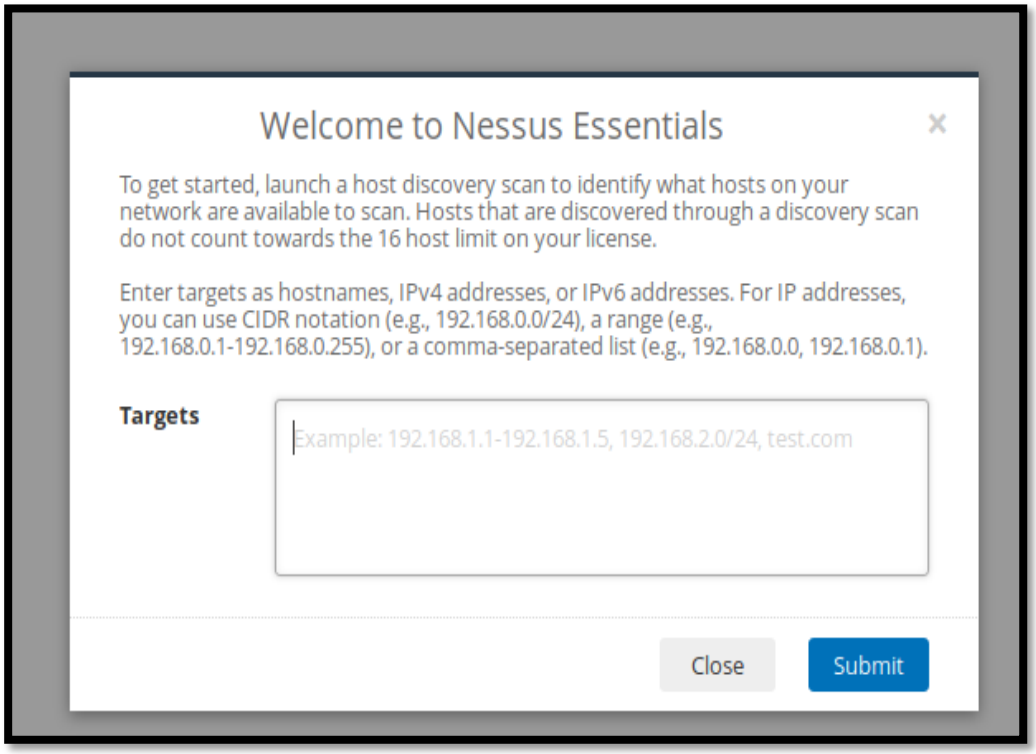


Fuente: Elaboración propia.

2.1.2. Fase de estudio de vulnerabilidades…

De acuerdo con lo indicado en esta fase, se procede con la validación de todos los riesgos encontrados, donde a su vez se generan el plan de trabajo, para proceder con la explotación de las vulnerabilidades, utilizando herramientas como NESSUS y NMAP, donde cada una de ellas emiten la facilidad de distinguir las particularidades de las vulnerabilidades encontradas.

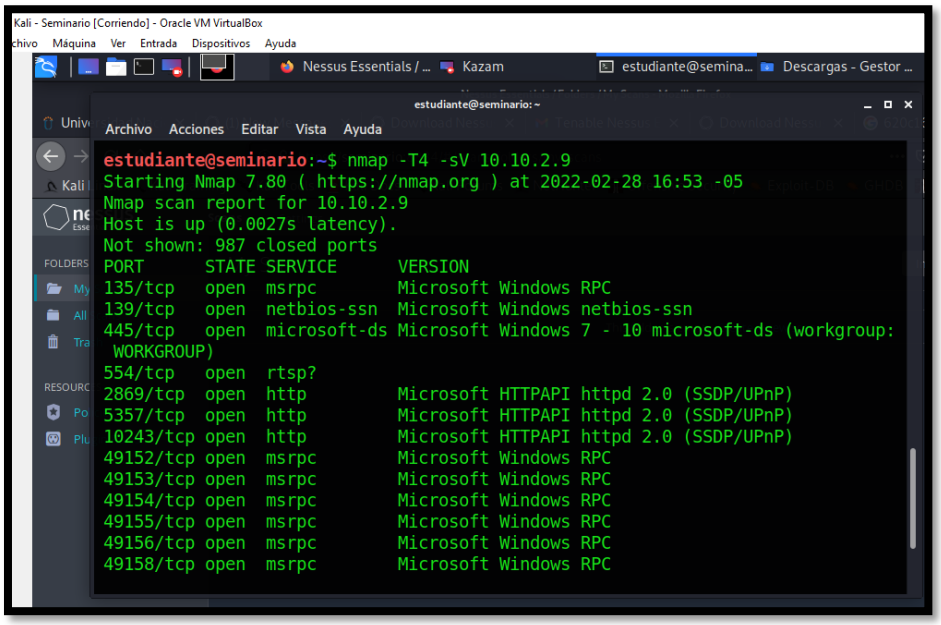
Ilustración 6. Entorno NESSUS.



Fuente: Elaboración propia.

- Una vez instalada la herramienta, se procede con la identificación nuevamente de los puertos abiertos, junto con los servicios empleados por los mismos, para que así la herramienta trabaje en la búsqueda de las vulnerabilidades alojadas en los equipos intervenidos (Win 7 x64 10.10.2.9/24).

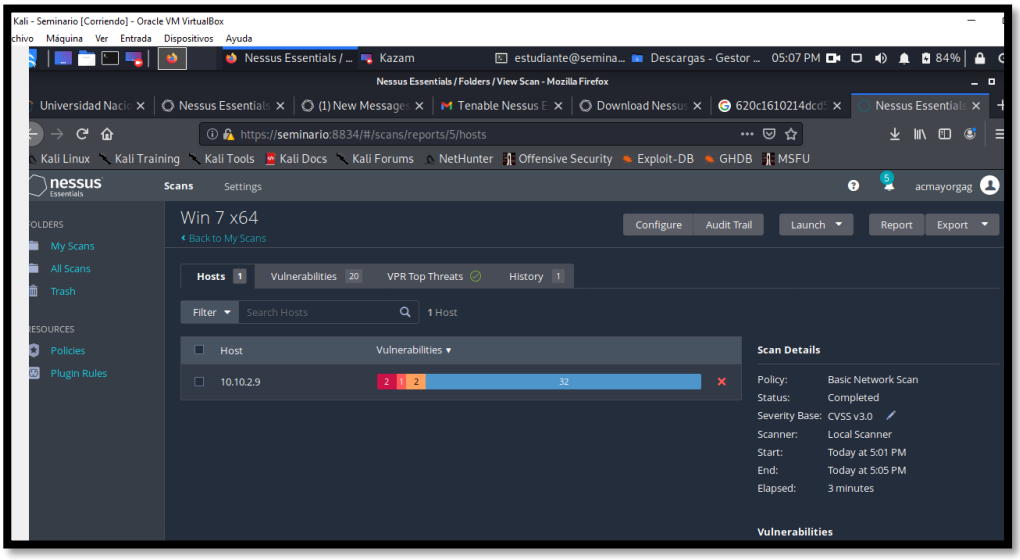
Ilustración 7. Nuevo análisis de puertos.



Fuente: Elaboración propia.

- Diagnóstico de la herramienta NESSUS.

Ilustración 8. Diagnostico herramienta NESSUS.

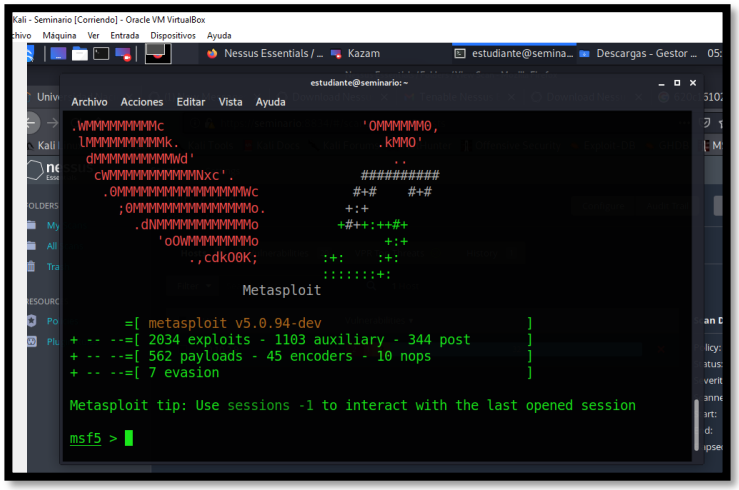


Fuente: Elaboración propia.

2.1.3. Fase de explotación de vulnerabilidades…

- De acuerdo con lo indicado en esta fase, se procede con la explotación de las vulnerabilidades encontradas, a través de la configuración del exploit requerido de la siguiente manera.

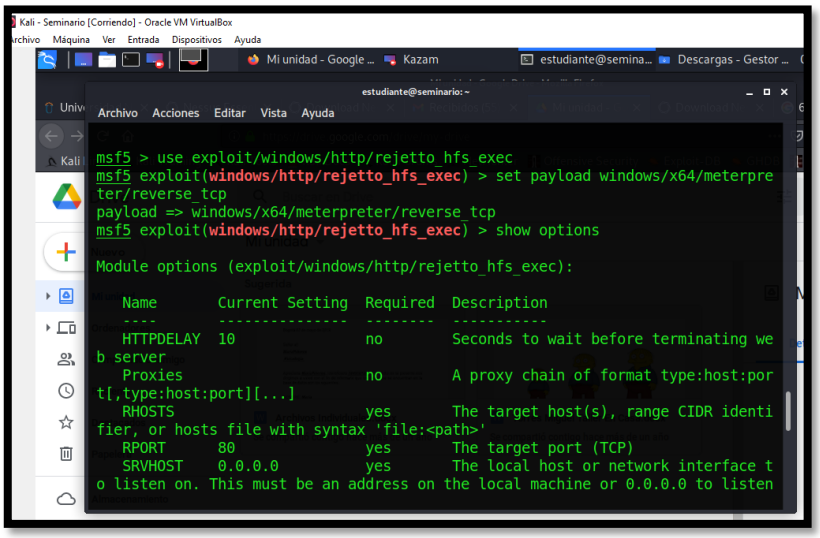
Ilustración 9. Consola MSFCONSOLE.



Fuente: Elaboración propia.

- Se procede con la configuración del exploit Rejetto 2.3, junto con el siguiente payload, sobre la IP: 10.10.2.9/24, estableciendo como RHOST.

Ilustración 10. Rejetto 2.3.



Fuente: Elaboración propia.

Ilustración 11. RHOST 10.10.2.9.

Fuente: Elaboración propia.

2.2. ASPECTOS Y ESTRATEGIAS RED TEAM Y BLUE TEAM

2.2.1. Aspectos de seguridad Red Team…

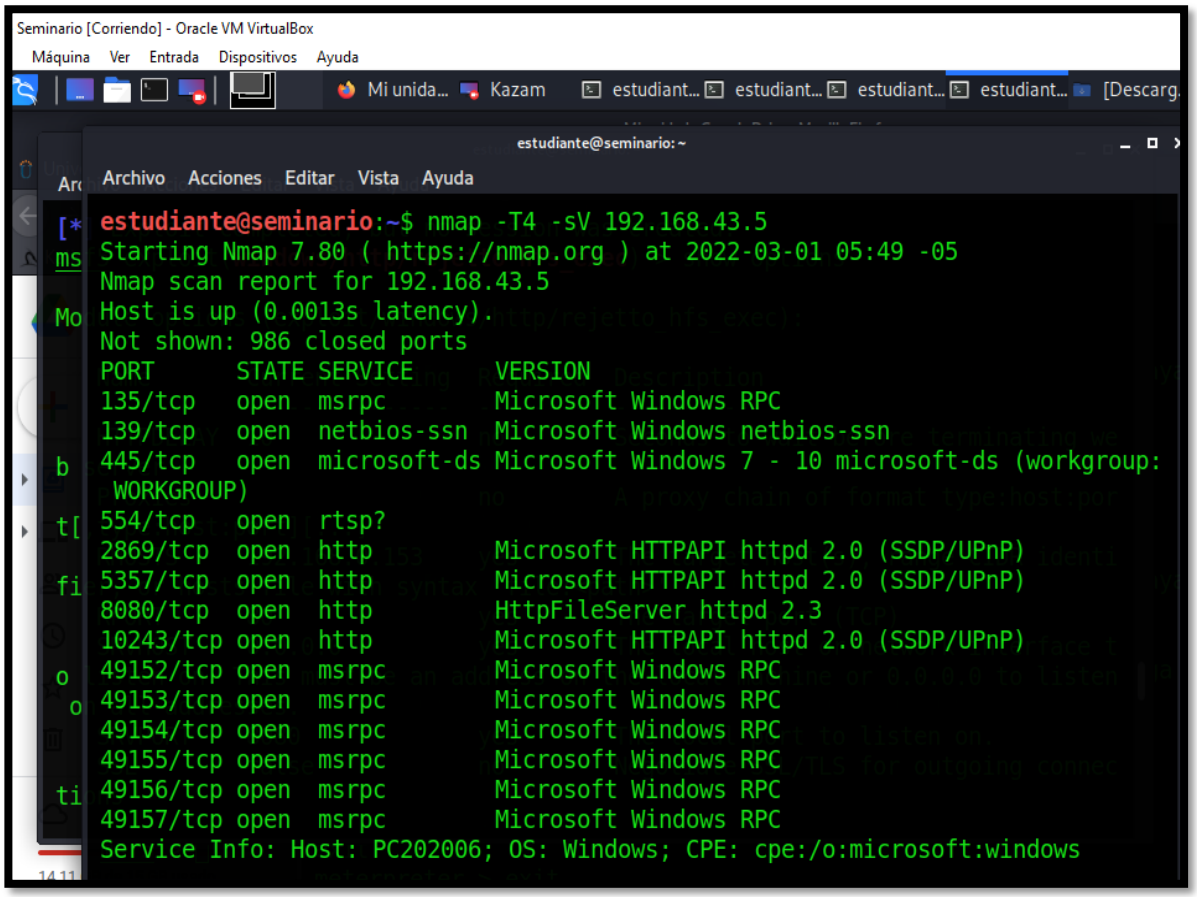
Con el fin de reconocer los aspectos de seguridad empleados por el equipo rojo, por medio de las pruebas ejecutadas, sobre el resguardo y filtración de la información en los sistemas de información y aplicativos de la organización, es importante establecer que los datos son el activo más importante, y que por tal motivo, se evidencio que por parte del reporte emitido por el equipo rojo, es la instalación de un aplicativo con el nombre de Rejetto, sobre la máquina de Windows 7 x64bits, indican que dicho aplicativo contiene un exploit de vulneración de información, el cual provoca Shell inverso, junto con visualización de sesiones de Meterpreter.

De acuerdo con los hallazgos se establece la validación sobre la creación de usuarios con roles de administrador dentro del sistema, donde por medio de la explotación de la información, se identifican los vacíos de seguridad que presentan los servicios de la organización.

A través de la clasificación de la información con base a la experiencia obtenida, el equipo expresa algunas de las herramientas utilizadas para la comprobación de la veracidad de la información suministrada, entre ellas está, sistema operativo Windows 7 x64 bits, motores de búsqueda como Google, aplicativo Rejetto, y NMAP.

- Se establece que por medio del uso de NMAP, se ejecuta el escaneo de puertos y servicios de la maquina victima Windows 7 x64, emitiendo la siguiente información.

Ilustración 12. Nuevo escaneo de puertos.



Fuente: Elaboración propia.

Donde se evidencia la apertura del puerto 8080/tcp, indicando que por a través de ese puerto, se puede establecer riesgo de vulnerabilidad, al no encontrarse bloqueado por el firewall.

- Se identifica por medio del motor de búsqueda Google, la información que puede llegar a establecer graves afectaciones provocadas por la herramienta de Rejetto dentro del sistema víctima, como se indica a continuación en la búsqueda sobre la amenaza, suministrando los siguientes datos.

Ilustración 13. Búsqueda Exploit DB.

Fuente: Elaboración propia.

- Una vez identificada la vulnerabilidad, se procede a obtener más información sobre la misma.

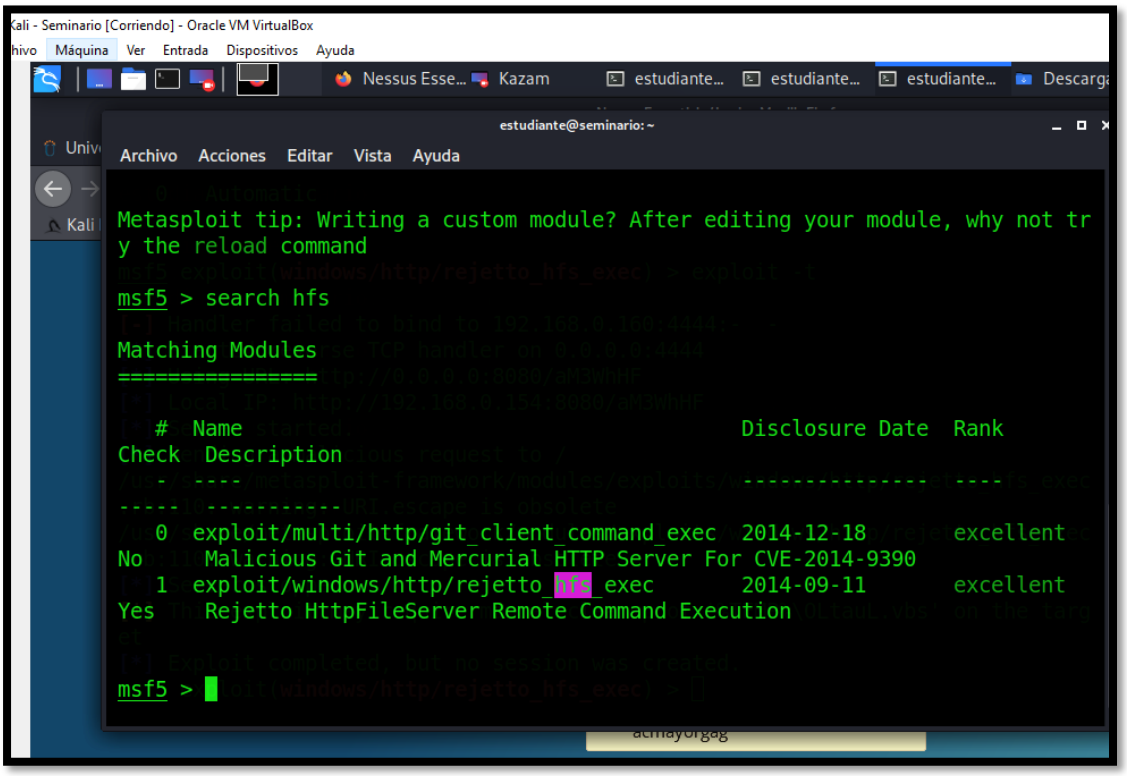
Ilustración 14. Información adicional vulnerabilidad.

Fuente: Elaboración propia.

- Con los datos recolectados, se identifica la mayor información, para identificar el ataque y proceder con la explotación de la vulnerabilidad encontrada.

- Por medio de la utilización de la consola de Metasploit, se procede a enlistar los exploit's, haciendo uso del comando search hfs.

Ilustración 15. exploit para la explotación de la vulnerabilidad.



Fuente: Elaboración propia.

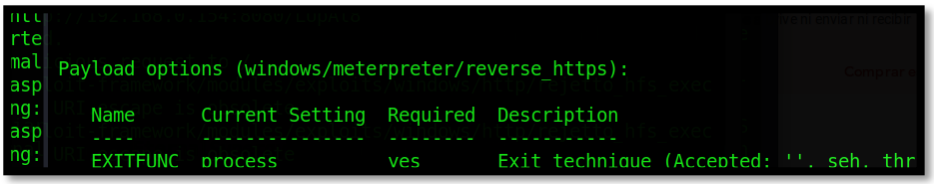
- Toda vez se identifique la vulnerabilidad y se establezca la visualización del exploit, se socializan las herramientas que se emplearían para avanzar en la identificación de la anomalía de seguridad y posteriormente establecer la explotación de esta, sobre la maquina víctima.

    - S.O. Windows 7
    - Visualización de Shell reverse.
    - Sesión de Meterpreter
    - BD exploit
    - NMAP
    - METASPLOIT

Se selecciona el exploit requerido, pero es de aclarar que no todas las veces toma por defecto el payload adecuado, ya que muchas veces en el cargue de la selección,

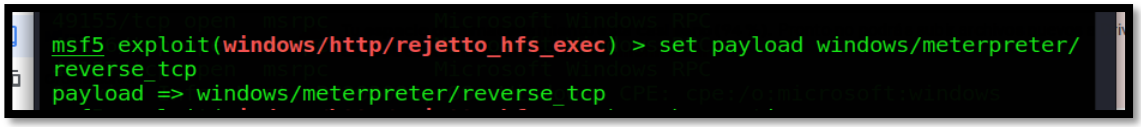
la carga con otra configuración, una diferente como HTTPS, por tal motivo es necesario realizar la modificación pertinente en el payload de la siguiente manera.

Ilustración 16. Payload sin modificar.



Fuente: Elaboración propia.

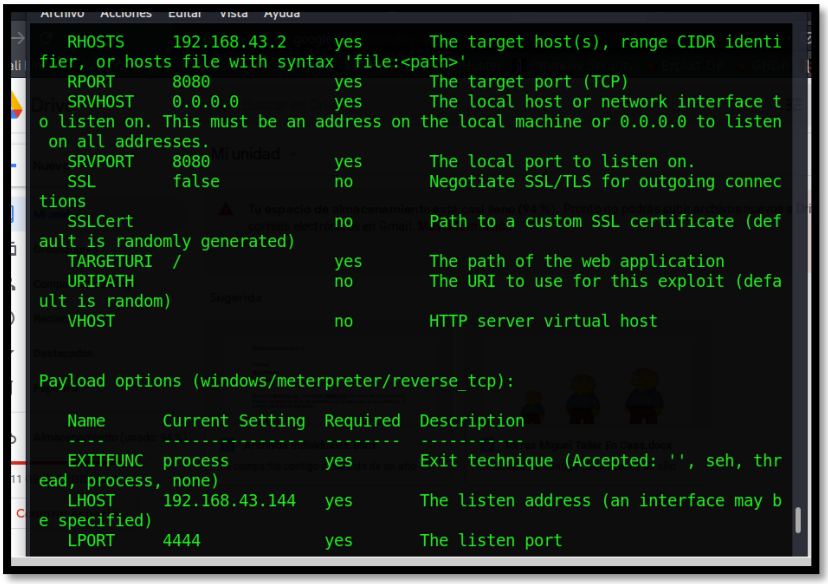
Ilustración 17. Payload modificado.



Fuente: Elaboración propia.

- Como ya se tiene la selección del payload necesario para proceder con el ataque, se deben realizar las modificaciones de las IP, de las máquinas de las victimas como la del atacante.

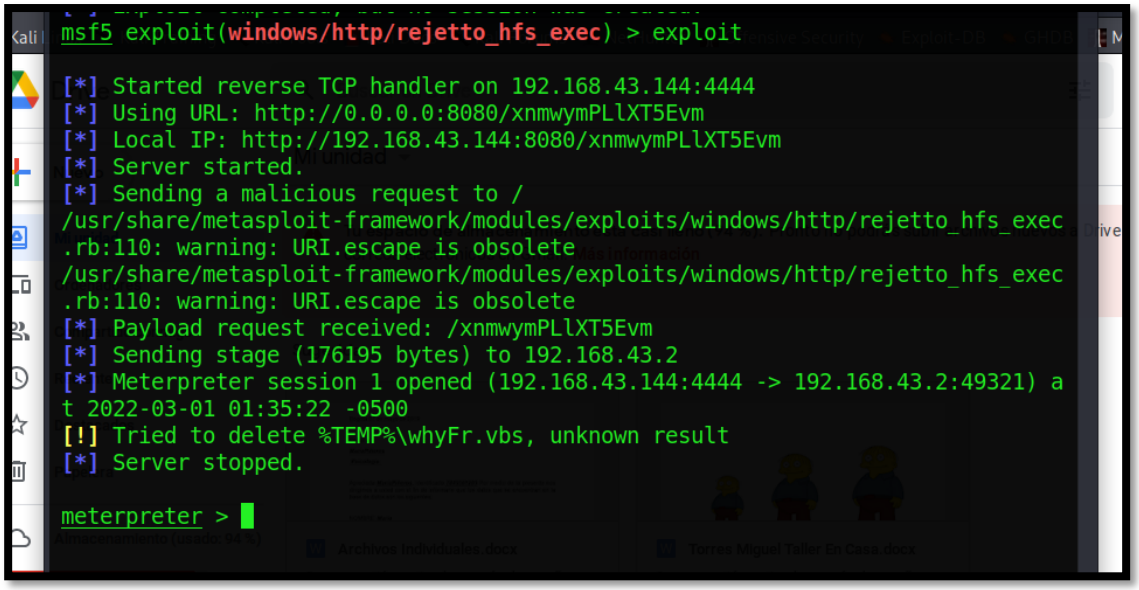
Ilustración 18. Modificación de datos.



Fuente: Elaboración propia.

Toda vez se procede con la modificación de los datos necesarios, se conduce a ejecutar el ataque, por medio del comando “exploit”, donde se visualiza la vulnerabilidad y posteriormente permite el acceso total a la maquina víctima.

Ilustración 19. Ataque vulnerabilidad.



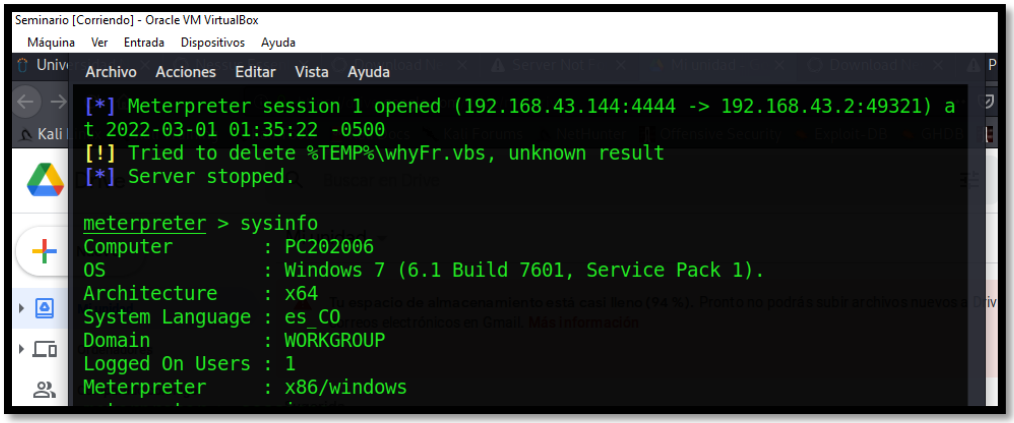
Fuente: Elaboración propia.

De acuerdo con lo evidenciado en la ilustración anterior, se identifica el acceso al Meterpreter, donde se procede con la indagación del sistema en busca de recolección de la mayor información que sea posible.

Dentro de la información hallada se logró acceder a:

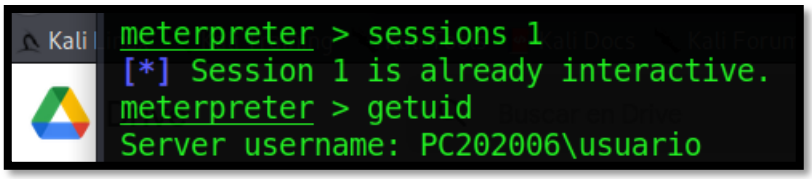
- Información del sistema.
- Nombres de usuarios
- Información de tarjetas de red, (Entre otros.)

Ilustración 20. Información del sistema.



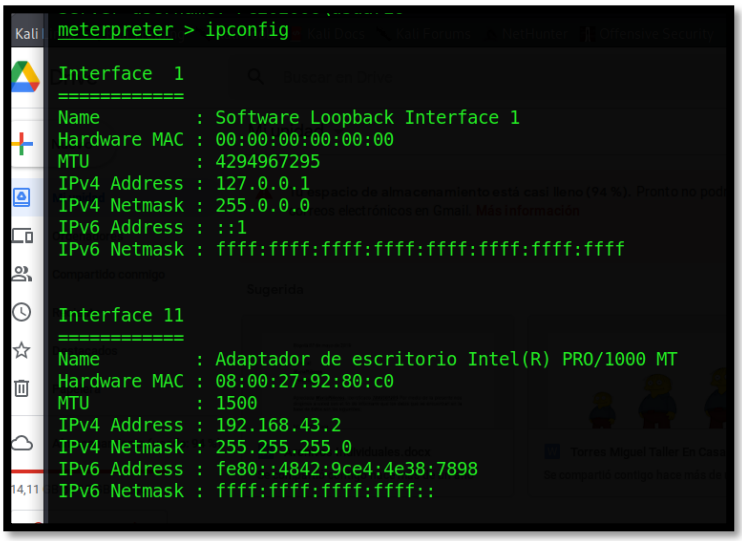
Fuente: Elaboración propia.

Ilustración 21. Username.



Fuente: Elaboración propia.

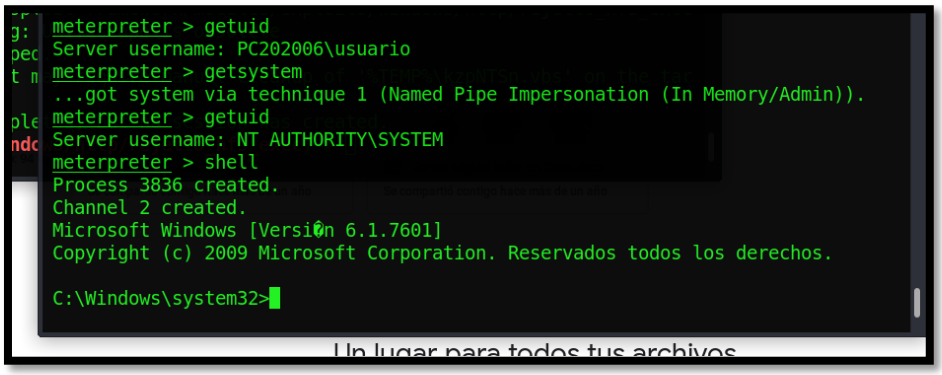
Ilustración 22. Tarjeta de red.



Fuente: Elaboración propia.

Una vez se tenga conocimiento total sobre la maquina víctima, se realizan pruebas de creación de usuarios, junto con la asignación de privilegios de administrador sobre el usuario creado, pero posteriormente se debe realizar el ingreso ejecutando el comando “Shell” en el sistema para generar modificaciones requeridas.

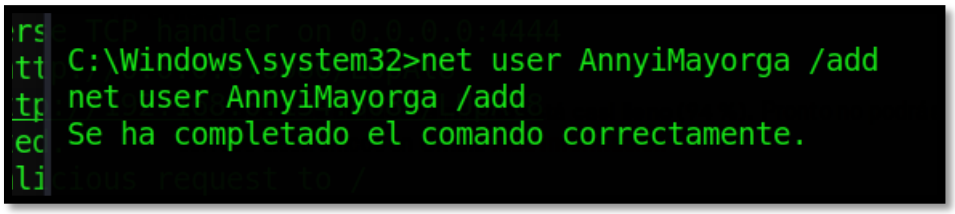
Ilustración 23. Ingreso al Shell.



Fuente: Elaboración propia.

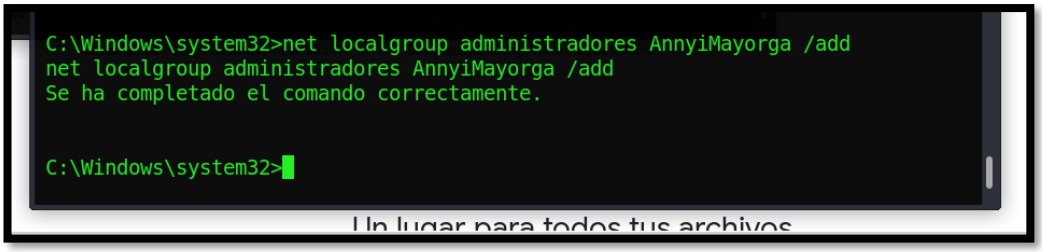
En este caso se realiza la creación del usuario AnnyiMayorga correspondiente a uno de los especialistas, estableciendo privilegios de administrador sobre el mismo, de la siguiente manera.

Ilustración 24. Creación de usuario.



Fuente: Elaboración propia.

Ilustración 25. Rol de administrador sobre el usuario.



Fuente: Elaboración propia.

Ilustración 26. Interfaz gráfica cuentas de usuario.

Fuente: Elaboración propia.

De acuerdo con los hallazgos encontrados por los especialistas, se logra demostrar ante la organización, las fallas de seguridad a las que están expuestos los sistemas y aplicativos de la misma, donde se exponen las vulnerabilidades y riesgos potenciales ante la perdida y manipulación de información a lo que se encuentran expuestos.

2.2.2. Aspectos de seguridad Blue Team…

La organización, requiere de sus expertos de Blue Team, establecer planes de trabajo y seguridad, ante el eminente ataque cibernético en tiempo real, sobre los sistemas de información alojados en el S.O Windows 7 x64 de la organización, se es necesario establecer medidas de mitigación sobre el equipo que anteriormente se evidencio que está siendo afectado, de acuerdo con la información compilada, se pretende que los expertos empleen técnicas que minimicen el impacto del ataque, y así prever posibles cambios, modificaciones en la información que se pueden llegar a presentar en la organización.

Es importante establecer, que la organización no cuenta con fluidez económica para invertir en herramientas licenciadas, por tal motivo los expertos deben establecer un pool de herramientas de seguridad de código abierto, como por ejemplo la utilización de herramienta NMAP, ya que se evidencia el ataque en tiempo real, se requiere la visualización de los puertos abiertos, junto con sus servicios, a los que se encuentran expuestos, con el fin de rastrear accesos vulnerados.

Como proceso de mitigación ante el ataque, los expertos proceden de la siguiente manera:

- Bloqueo de puertos, para evitar el acceso por intermedio de ellos.
- Cambio de credenciales del usuario afectado, como también se realiza limpieza de los usuarios no autorizados o no identificados en la organización estableciendo la eliminación de estos.
- Limpieza de contraseñas guardadas en los motores de búsqueda.
- Establecer políticas de seguridad, sobre el uso de sistemas de información.
- Validación de activación del firewall y actualizaciones del sistema.
- Bloqueo de puertos innecesarios.
- Control de políticas de directorio activo, donde se restrinja la instalación de aplicativos no autorizados por la organización.
- Cambio de credenciales cada 30 días, sobre los accesos de los usuarios de red.

Dentro del análisis emitido, es posible adicionar herramientas de posible utilización ante este equipo azul, como medida de mitigación.

OSSEC: "OSSEC es una plataforma de monitorización y detección de intrusos de código abierto"[3]. En esta herramienta se logra establecer el análisis sobre los hallazgos, para identificar la transparencia de los datos que emiten alertas, mediante esta herramienta se establece la detección de ataques cibernéticos, que se ejecuten al S.O.

SNORT: "Es el sistema de prevención de intrusiones (IPS) de código abierto más importante del mundo. Snort IPS, usa una serie de reglas que ayudan a definir la actividad de red maliciosa y usa esas reglas para encontrar paquetes que coincidan con ellos y generar alertas para los usuarios"[4]. Con la ayuda de esta herramienta se logra establecer los registros y validación de paquetes en tiempo real, donde se

[3] UNINFORMATICO. OSSEC: El mundo del IDS (Intrusion Detection System) y del HIDS (Host IDS). [En línea]. Noviembre 2020. [Consultado: 15 de marzo de 2022]. Disponible en: https://www.elladodelmal.com/2020/11/ossec-el-mundo-del-ids-intrusion.html

[4] SNORT. ¡Snort 3 está disponible! [En línea]. Enero 2022. [Consultado: 14 de marzo de 2022]. Disponible en: https://www.snort.org/

logra determinar afectaciones por ataques DDos, como también establece una supervisión sobre el tráfico generado en la red, en busca de alguna afectación por un ataque cibernético.

OPENWIPS: "Es un IPS (Intrusion Prevention System) inalámbrico de código abierto"[5]. Corresponde a una herramienta utilizada para la identificación de ataques por medio de las redes inalámbricas, por medio del control de sensores que facilitan la detección de riegos, ya que brinda establecer un análisis de las características establecidas en la interfaz de seguridad, a las que se encuentran expuestas.

Teniendo en cuenta estas herramientas como medida de mitigación de código abierto, que facilitan la implementación de nuevas medidas en beneficio de la organización contratante. Es posible establecer estrategias para los equipos rojos y azules, en beneficio de las organizaciones.

Como desarrollo en el ámbito de seguridad se establecen dichas estrategas de red team y blue team, es de saber que estos equipos deben establecer un apoyo sincrónico entre ambos, ya que deben establecer juntos estrategias de seguridad ante la mitigación de riegos sobre la organización contratante, donde se tiene claro que por medio del equipo rojo se identifican todas las vulnerabilidades en las pruebas sobre los sistemas de información y aplicativos, los cuales deben ser notificados y entregados documentalmente al equipo azul, los cuales deben generar planes de trabajo, donde se debe indagar sobre la vulnerabilidad, realizar la documentación pertinente, por medio de ellos se logra, recolectar información y así establecer estrategias y posibles mejoras ante futuros ataques.

2.3. RECOMENDACIONES ESTRATEGICAS DE SEGURIDAD ANTE UNA ORGANIZACIÓN.

Si bien es cierto que, en nuestros días, las organizaciones no se ajustan a únicamente con el guarda de seguridad, sino que han involucrado la informatización de punta, la cual posibilita poseer dominio de lo que acontece en el área de la organización, "Sin más preámbulos, paso a ofrecerles 31 consejos de ciberseguridad concebidos para ayudar a las empresas a protegerse"[6].

[5] SEGURIDAD. INSTALANDO UN SISTEMA DE DETECCIÓN DE INTRUSOS INALÁMBRICO (WIDS) EN RASPBIAN – I. [En línea]. SEVILLA. RODRIGUEZ. J. Luis. Abril 2014. [Consultado: 14 de marzo de 2022]. Disponible en: https://revista.seguridad.unam.mx/print/2207

[6] GLOBALSING. Consejos de Ciberseguridad para empresas. [En línea]. ZAMBRANO. Eduardo. Noviembre 2016. [Consultado: 20 de marzo de 2022]. Disponible en: https://www.globalsign.com/es/blog/cybersecurity-tips-for-business

Mas que nada, sin rodeos se exponen treinta y una recomendaciones en seguridad de la información proyectados, con la finalidad de contribuir a las organizaciones en la protección.

- Tener precaución al momento de hacer público situaciones de alguien más o a manera personal.

Se debe tener mucha precaución al momento de expresar comentarios en internet, ya que pueden ocasionar dificultades y conllevar a ocasionar posibles robos, además situaciones con abogados y demás.

- Hay que precisar que información recolecta su organización y garantizar su resguardo.

Para la protección de la información en el ciberespacio es necesario llevar a cabo una revisión a cerca de que información general y así reconocer cuales conllevan a ser de predominio común, por lo que no requieren estar vigilados, además verificar aquellos que contienen un grado de interés de mediana envergadura, los cuales al momento de un posible ataque novan a generar gran efecto en la compañía y que en su momento deben estar resguardados con alguna prevención de protección y seguidamente que información es particular y la más relevante para la organización, siendo que esta última ocasionaría grandes consecuencias negativas a la organización y es por ello que obedecerá estar resguardada de manera pertinente de los empleados a un alto grado de resguardo, estipulando que personas pueden ingresar y como lo deben realizar.

- Emplee variados procedimientos de confirmación.

Tales como algo que lo identifica o que comprende o conserva, además de las contraseñas, entre otras.

- Acondicione el reglamento HTTPs en su ciber página.

Este reglamento cuantifica la información referida desde el explorador de internet hasta la computadora central; la constancia es que estos permiten verificar la veracidad al encender el conjunto de iconos que forman parte de la interfaz de un programa de software la cual coge un color verde la cual señala de manera sobresaliente la designación de su organización.

- Haga uso de palabras claves consistentes y evita hacer uso de ellas de nuevo, tal como: ¡45cABC6&94@))! No realizar ¡01234 o Marcos2!,.

En la actualidad esta forma de cifrados es muy propicios para los hackers, los cuales utilizan la información para venderla a terceros, es por ello que se recomienda hacerle la tarea al hacker más complicada al efectuar una contraseña larga que

involucre lo que usted tenga a bien, si se le olvida tenga al alcance una estrategia o cuaderno para evitar olvidarla o perderla, pero esto es de manera segura que debe de permanecer.

- Actualice de manera periódica el programa informático.

Al actualizarlo le está colocando una barrera a los hackers para seles dificulte ingresar a su computadora y si puedes colocar el más actual mucho mejor.

- Reproduzca toda la información por seguridad.

Estas se deben realizar de manera periódica y ubicarlas en espacios variados para evitar el robo.

- Acondicionar una puerta de enlace de perímetro de seguridad con la finalidad de resguardar el enlace al ciberespacio.

Este está en la capacidad de verificar la información que ingresa como también la que sale, estipula que entradas están permitidas y cuales no lo están, siendo estos obstaculizados.

- Motivar al equipo administrativo de la organización para dirigir una educación de ciberseguridad.

Teniendo en cuenta los cambios que se van dando el sector administrativo debe de ser el número uno en estar a la vanguardia y replicarlos en todas las áreas contando con su aprobación.

- Este seguro que la base de tecnología de la información, se encuentra resguardada frente a posibles atentados cibernéticos.

Favorece la aparición de ciberseguros, pero debe de cerciorarse de que estos también protejan el tiempo muerto de la organización.

- Este actualizado frente a las reglamentaciones que día a día se proyecta en beneficio de las organizaciones y de la humanidad.

Es de gran importancia estar al pendiente de las reglamentaciones vigentes y así evitar posibles penalidades.

- Permanezca indagando a cerca de la novedad en informatización y examinar modernos abastecedores.

Es de gran importancia que este actualizado frente a lo que día a día está saliendo al mercado en este tema, así mismo este en la mejor disposición para modernizar el programa informático, colocándolo a la vanguardia y protegiéndolo de posibles ataques ciberespaciales.

"Data Protection and Privacy Legislation Worldwide"[7], Colombia hace parte del71% de los países que cuentan con una legislación de privacidad y protección de datos, le sigue en un 9% países con proyecto de ley, así, mismos países sin legislación en un 15% y por último países sin datos en un 5%.

Así, mismo desde el año 2001, Colombia hace parte del reglamento firmante de mecanismos mundiales con relación a las normas de convenio digital.

2.4. CONCLUSIONES EN LA CONSTRUCCION DEL ENFOQUE EN CIBERSEGURIDAD

Al transcurrir de los días y más aún desde el momento en que se dio la presencia del COVID 19 en el mundo, la humanidad se ha visto avocada a una serie de cambios extremos y en esos se incluye la ciberseguridad debido al empleo masivo de la tecnología y que no se estaba preparado para que surgieran ataques que fracturaran y perjudicaran a las organizaciones y también a la humanidad.

Es por ello por lo que en la actualidad ha tomada mucha más fuerza la ciberseguridad y se presentan algunas posibles conclusiones.

- Instruirse teniendo como base los desaciertos ocurridos anteriormente.
- Sea consciente que todo no está totalmente protegido, que puede existir una desprotección y hay que estar en disposición para mitigarla.
- Inicie un proceso de gestión de velocidad de transferencia de la información, teniendo en cuenta el origen y al llegar al lugar o persona indicados.
- Extrae el mayor beneficio a los servidores remotos, en lugar de sus propios sistemas internos.
- Este atento a la nueva normatividad que regulan su campo.
- No se quede con lo que tiene, siempre hay que buscar la innovación en el sector tecnológico y a su vez en los que suministran estas nuevas tecnologías.

[7] UNCTAD. Data Protection and Privacy Legislation Worldwide. [En línea]. Diciembre 2021. [Consultado: 20 de marzo 2022]. Disponible en: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

CONCLUSIONES

Se concluye este documento estableciendo la importancia de establecer los referentes bibliográficos en la socialización de los delitos informáticos, que estipula la ley colombiana, donde se pretende garantizar el uso debido de los sistemas de información y redes utilizadas por las mismas, generando una concientización sobre las políticas de seguridad en los empleados de la organización.

Se deben establecer medidas de seguridad, sobre los protocolos de red y configuración de software de los sistemas, donde se alojan los sistemas de información y aplicativos, estableciendo controles de contingencia ante posibles ataques.

Comprender las medidas de seguridad, establecidas en la explotación de las vulnerabilidades alojadas en los sistemas de la organización, y así los especialistas generan protocolos sobre los hallazgos presentados.

RECOMENDACIONES

Dentro de este informe técnico, se pretende concientizar a los usuarios y administradores de las plataformas de la organización WhiteHouse Security, generando la utilización de buenas prácticas, sobre las políticas de seguridad y resguardo de la información, llevando un control sobre los riegos potenciales a los que puede estar expuesto, debido a las brechas de seguridad que se identificaron en los sistemas de información y aplicativos de la organización, generando recomendaciones generales.

Es por ello que en la actualidad, el triunfo de la propuesta que implique protección informática, no precisamente transitar por estudio a cerca de valor, excelencia y coherencia o grado de inclusividad, pero al igual surge el asunto esencial de contemplar la seguridad informática, en la cual, la información usualmente, la documentación delicada de los usuarios permanezca salvaguardada y que esta evite ser frágil a atentados, con el propósito que no se realicen mediante los mecanismos de protección con que cuenta la organización en su momento, los cuales se encuentran enlazados con él, proveedor.

Donde se debe tener en cuenta la necesidad de establecer medidas estratégicas de seguridad en cualquier organización, así mismo, se debe garantizar controles de evaluación, por tal motivo, se recomienda la implementación de controles CIS, los cuales brindan la ayuda, indicando el paso a paso, sobre la regulación de ataques informáticos y adicional, tener conocimiento a cerca de otros riegos de seguridad.

De acuerdo con lo consultado y analizado anteriormente, se pueden establecer la consolidación de otras recomendaciones como:

- Configuración de control de aplicaciones y navegador, desde la seguridad de Windows.
- Actualización de antivirus.
- Evitar trasladar información de la empresa o personal en dispositivos USB.
- Utilizar servicio de proxy, como control de acceso y navegación.
- Encriptación de la información, junto con la activación de claves de seguridad para su apertura y visualización.
- Corroborar el dominio de las cuentas de correo a la hora de realizar descargas de adjuntos de estas.

- Cierre de sesiones de usuarios en navegadores en equipos temporales o bloqueo de sesiones de usuarios de red en lugares de trabajo al ausentarse.

- Generar siempre copias de seguridad de la información en la nube.

- Desinstalar complementos en los navegadores que no conozca o no sean de su utilidad.

- Activación del corta fuegos en los equipos de cómputo.

ENLACE DE SUSTENTACION: https://youtu.be/oagkAeZfetw

BIBLIOGRAFÍA

ALLSOPP. Will. Advanced Penetration Testing: Hacking the World's Most Secure Networks. March 2017. 288 pág.

COPNIA. Código de ética. [En línea]. 2015. [Consultado: 19 de febrero de 2022]. Disponible: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etic

CYBERSECURITY. USA. [En línea]. Mayo de 2020. [Consultado: 19 de marzo de 2022]. Disponible en: https://ciberseguridad.com/normativa/eeuu/#:~:text=Estados%20Unidos%20no%20ha%20adoptado,las%20empresas%20de%20infraestructura%20cr%C3%ADtica.

ELTIEMPO. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [En línea]. Enero 2015. [Consultado: 19 de febrero de 2022]. Disponible: https://www.eltiempo.com/archivo/documento/CMS-15141236

GLOBALSING. Consejos de Ciberseguridad para empresas. [En línea]. ZAMBRANO. Eduardo. Noviembre 2016. [Consultado: 20 de marzo de 2022]. Disponible en: https://www.globalsign.com/es/blog/cybersecurity-tips-for-business

HOSTINGERTUTORIALES. Como Generar SSH Keys (Llaves SSH) en PuTTY. [En línea]. B. Gustavo. Noviembre 2021. [Consultado: 15 de marzo de 2022]. Disponible en: https://www.hostinger.co/tutoriales/llaves-ss

INCIBE. Copias de seguridad. [En línea]. Marzo 2020. [Consultado: 19 de marzo de 2022]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

J. WHITE. Alan. CLARK. Ben. Blue Team Field Manual (BTFM). Createspace Independent Publishing Platform, United States. January 2017.

REYDESS. Fundamentos de Metasploit Framework para la Explotación. [En línea]. Septiembre 2018. [Consultado: 6 de marzo de 2022]. Disponible en: Fundamentos de Metasploit Framework para la Explotación | Alonso Caballero / ReYDeS

SIC. LEY 1273 DE 2009. [En línea]. Enero 2019. [Consultado: 19 de febrero de 2022]. Disponible: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

SNORT. ¡Snort 3 está disponible! [En línea]. Enero 2022. [Consultado: 14 de marzo de 2022]. Disponible en: https://www.snort.org/

SEGURIDAD. INSTALANDO UN SISTEMA DE DETECCIÓN DE INTRUSOS INALÁMBRICO (WIDS) EN RASPBIAN – I. [En línea]. SEVILLA. RODRIGUEZ. J.X Luis. Jose. Abril 2014. [Consultado: 14 de marzo de 2022]. Disponible en: https://revista.seguridad.unam.mx/print/2207

THEHACKERWAY. Conceptos Básicos de Meterpreter – MetaSploit Framework. [En línea]. Abril 2011. [Consultado: 5 de marzo de 2022]. Disponible en: Conceptos Basicos de Meterpreter – MetaSploit Framework – Seguridad en Sistemas y Técnicas de Hacking. TheHackerWay (THW)

TINOCO LINARES, Ana, et al. Análisis y clasificación de los ataques y sus exploits: Framework Metasploit como caso de estudio. 2020.

UNINFORMATICO. OSSEC: El mundo del IDS (Intrusion Detection System) y del HIDS (Host IDS). [En línea]. Noviembre 2020. [Consultado: 15 de marzo de 2022]. Disponible en: Un informático en el lado del mal: OSSEC: El mundo del IDS (Intrusion Detection System) y del HIDS (Host IDS)

UNCTAD. Data Protection and Privacy Legislation Worldwide. [En línea]. Diciembre 2021. [Consultado: 20 de marzo 2022]. Disponible en: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

UNINFORMATICO. OSSEC: El mundo del IDS (Intrusion Detection System) y del HIDS (Host IDS). [En línea]. Noviembre 2020. [Consultado: 15 de marzo de 2022]. Disponible en: https://www.elladodelmal.com/2020/11/ossec-el-mundo-del-ids-intrusion.html