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

RÓMULO LOMBARDI PEREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PUERTO COLOMBIA ATLÁNTICO
2022

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

RÓMULO LOMBARDI PEREIRA

Tutores:
LUIS FERNANDO ZAMBRANO
JOHN FREDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PUERTO COLOMBIA ATLÁNTICO
2022

CONTENIDO

Pág.

LISTA DE IMÁGENES

Pág.

GLOSARIO

CVE: (Common vulnerabilities and exposures) es una lista de vulnerabilidades conocidas administradas por mitre, por medio de esta lista se pueden clasificar las vulnerabilidades que se descubren de forma diaria hacia los equipos y sistemas vulnerables, por medio de esta lista podemos también clasificar vulnerabilidades para los hallazgos, buscar exploits e incluso otras técnicas de comprobación o explotación, similar a CVE existen otras listas como CWE, BID, IAVA, CAPEC, IAVA

EXPLOITDB: es un servicio en línea que contiene una amplia base de datos de exploits y scripts, entre ellos los de Google hacking (GHDB) que en algún momento fueron creados y mantenidos por Jhonny Long. Por medio de este servicio se pueden buscar exploits para ser ejecutados en equipos objetivo por medio de nombre de vulnerabilidad, tipo de servicio, aplicación, servidor y CVE, este exploit o grupo de exploits que se consigan para el equipo objetivo pueden ser ajustados a la medida según la pericia del pentester e incluso podrían ser importados a metasploit.

METASPLOIT: es una herramienta que por medio de una amplia base de datos nos permite detectar y ejecutar exploits en máquinas objetivos que tengan la vulnerabilidad, es una de las herramientas más utilizadas a nivel general en un pentesting, una de las mayores ventajas de esta herramienta aparte de la posibilidad de utilizar payloads y diferentes métodos para entrar a un sistema vulnerable es que es una herramienta de licenciamiento open, es una herramienta de la marca rapid 7.

NMAP: es una herramienta muy completa orientada a escaneo de puertos y detección de servicios, de hecho, cuenta con scripts complementarios que ayudan a detectar vulnerabilidades.

OPENVAS: es un escáner de vulnerabilidades de licencia open, que permite realizar pruebas de vulnerabilidades a dispositivos de infraestructura.

RED TEAM: el equipo rojo como normalmente es llamada se encarga de hacer simulaciones de ataque en diferentes aspectos para medir redes, aplicaciones y verificar controles, para saber que tan preparados están ante un ataqu en el vida real.

BLUE TEAM: el equipo azul como normalmente es llamado se encarga de mantener y probar constantemente las defensas a nivel interno de su red ante ataques del equipo rojo.

VIRTUALBOX: software utilizado para para manejar versiones de sistemas operativos.

RESUMEN

El presente documento contiene una recopilación de las actividades realizadas durante la prestación de servicios del proyecto TheWhiteHouse Security junto con los resultados obtenidos. Dicho proyecto tuvo como fin realizar una consultoría y auditoria a ciertos activos pertenecientes a la infraestructura en aras de detectar posibles falencias o aspectos de mejora relacionados con el campo de ciberseguridad en la organización. La mencionada consultoría fue realizada respetando la confidencialidad, integridad y disponibilidad de la información sensible compartida por el cliente.

INTRODUCCIÓN

La organización TheWhiteHouse Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial.

La organización requiere una asesoría o consultoría por parte de un equipo experto en ciberseguridad en aras de atender necesidades puntuales de la organización como son la implementación de un banco de trabajo para los postulados permitiéndole demostrar sus capacidades, adicionalmente, ha decidido que es hora de conformar equipos de Red Team y Blue Team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta y dichos equipos serán sometidos a pruebas según una serie de sucesos ocurridos en la organización que se resumen dentro de las labores realizadas.

1 OBJETIVOS

1.1 GENERAL

Elaborar informe técnico con resultado de labores realizadas dentro del periodo de pruebas realizadas en la organización TheWhiteHouse Security.

1.2 ESPECÍFICOS

- Asesorar a la compañía sobre la legislación colombiana ante delitos informáticos.

- Sustentar a la compañía las fases de ejecución de unas pruebas de penetración o pentesting.

- Desplegar un banco de pruebas para la compañía con el fin que los postulados puedan demostrar sus capacidades técnicas.

- Sustentar desde el punto de vista profesional y ético a la compañía los sucesos del “Caso Andrómeda”.

- Realizar un análisis bajo la ley 1273 de 2009 a los modelos de contrato y acuerdo de confidencialidad de la entidad para sus nuevos equipos de Red Team y Blue Team.

- Asesorar al equipo de Red Team en el proceso de ejecución de unas pruebas de penetración en aras de poder comprobar una posible explotación de vulnerabilidades en un equipo de la organización.

- Asesorar al equipo de Blue Team en el proceso de remediación y mitigación ante un incidente de seguridad detectado en la organización.

2 DESARROLLO DEL INFORME

2.1 PRIMER SET DE ACTIVIDADES DENTRO DEL PERIODO DE PRUEBA.

El ciclo de pruebas inicia con una asesoría sobre la ley 1273, el proceso de pentesting y el banco de trabajo para los postulantes al equipo nuevo de red y Blue Team

2.1.1 Pregunta 1.

“Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley”.

2.1.2 Respuesta a la pregunta 1.

Ley 1273 de 2009 esta ley es la principal ley que existe relacionada con delitos informáticos en Colombia, dentro de ella se resumen 12 artículos donde se puede resaltar hurto informático, violación de datos personales, uso de software malicioso y suplantación de sitios web, sin embargo, esta ley bajo la experiencia del autor y conociendo otras leyes a nivel mundial todavía debe ser mejorada y ajustada para incluir otros delitos o actividades maliciosas.

2.1.3 Pregunta 2.

“En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting”.

2.1.4 Respuesta a la pregunta 2.

Las pruebas de penetración / penetration testing o pentest son un set de pruebas que permiten identificar y comprobar (explotar) vulnerabilidades de forma controlada en un activo o infraestructura del cliente, esto ayuda a los clientes a detectar y corregir vulnerabilidades que normalmente no son detectadas y que podrían ser aprovechadas por ciberdelincuentes. A continuación, se resumen las etapas relacionadas dentro del pentest:

- Reconocimiento: en esta etapa se busca identificar si los equipos objeto de las pruebas (locales en las oficinas del cliente o remotos desde VPN, MPLS, entre otros) están activos o identificar en sí que equipos objeto están disponibles. Generalmente en un pentesting pueden pasar dos escenarios: el primero donde

solo se asigne un segmento de red y sobre ello identificar equipos, ejemplo 172.16.0.X/24 y el segundo escenario donde se dé una lista de IP url objeto de pruebas, ejemplo: 192.168.1.100, unad.edu.co. también puede pasar un tercer escenario el cual es que no se logre la conectividad adecuada de forma local o remota por VPN a los segmentos o equipos objeto de las pruebas, por eso es importante verificar las tablas de enrutamiento del equipo del pentester.
Algunas herramientas utilizadas para reconocimiento son:

- Advanced IP scanner
- Comando ping
- Nmap / zenmap

Otro escenario que se puede dar en el reconocimiento es que las pruebas estén orientadas a web y se requiera investigar sobre las IP públicas o url en internet, para ello existen programas como censys, Shodan y Zoomeye con la capacidad de brindarnos información muy relevante al momento de hacer un pentesting o para otras labores más complejas como un ethical hacking / Red Team.

- Identificación de puertos y servicios: posterior a tener identificado los activos objeto de las pruebas se procede a identificar los puertos y servicios que estén asociados a cada uno con el fin de identificar posibles vectores de ataque y/o vulnerabilidades asociadas, para esto principalmente se utilizan dos técnicas:

  - Banner grabbing: por medio de escaneos e identificación del banner de un servicio se puede llegar a conocer versión del servicio, del sistema operativo, vulnerabilidades asociadas entre otros. Herramientas locales y remotas como el caso de Shodan y censys utilizan esta técnica.
  - Escaneo de puertos y servicios: por medio de escáneres o herramientas se identifican los puertos abiertos en los equipos objeto de las pruebas utilizando diferentes técnicas (escaneos ICMP, Escaneos ARP, Escaneos TCP half open, escaneos UDP, entre otros).

  Algunas herramientas utilizadas para identificar puertos y servicios son:

  - ID Serve
  - Recon-ng
  - Nmap / Zenmap (escaneos tipo -sS, -sA, -sT, -sV, entre otros)
  - Nessus

- Open VAS

- Escaneo / identificación de vulnerabilidades: posterior a tener identificados los puertos y servicios inicia el escaneo de vulnerabilidades, en la mayoría de los casos el escáner de vulnerabilidades es capaz de hacer la labor de reconocimiento e identificación de vulnerabilidades de forma simultánea, el escaneo de vulnerabilidades en si como su nombre lo indica permite identificar "Posibles" vulnerabilidades asociadas a los equipos, esto lo hace de diferentes formas:

  - Versiones de servicios: según la versión de servicios el escáner de vulnerabilidades puede determinar según su base de datos de vulnerabilidades que dicho servicio es vulnerable debido a que le faltan actualizaciones o puntualmente es vulnerable a algo que no se remedio por parte del fabricante, ejemplo Apache 2.4, IIS 7.0.

  - Puertos identificados: según el puerto que este activo a un servicio el escáner de vulnerabilidades está en capacidad de determinar que dicho puerto es vulnerable, esto principalmente se debe a que algunos puertos de servicios por defecto no utilizan cifrado en transporte para proteger la información que viaja desde y hacia la aplicación o servicio, ejemplo: Puerto 80 en servidor web.

  - Pruebas automatizadas: dentro del set de pruebas alojados en las bases de datos y plugin de los escáneres de vulnerabilidades esta la posibilidad que dicha herramienta identifique que un puerto o servicio sea débil a cierto ataque, ejemplo: inyección de SQL, XSS, CSRF, SSRF, entre otros

  Dentro de las herramientas utilizadas para escaneo de vulnerabilidades se puede resumir:

  - Nessus

  - Acunetix

  - Burpsuite

  - Netsparker

  - OpenVAS

  - Nexpose

  - Core impact

- OWASP ZAP

- Nikto

Algunas de las herramientas mencionadas anteriormente son de licencia comercial (paga) y otras son de licencia open, en otros casos como el de nikto su base de datos no esta tan actualizada como el caso de un Acunetix. Por lo tanto, es importante antes de hacer un pentesting según el tipo de infraestructura o activos a ser analizados determinar que herramientas se debe utilizar, por ejemplo, para escaneos de activos en red, servidores, entre otros Nessus tiene mayor efectividad que un escáner tipo Burpsuite ya que Burpsuite está orientado únicamente a servidores, aplicaciones y servicios web.

Por último, es importante resaltar que en esta etapa también entran validaciones manuales que puede hacer el pentester en busca de vulnerabilidades, entre más experimentado sea el pentester tendrá una mayor probabilidad de encontrar un hallazgo.

- Explotación de vulnerabilidades: La principal diferencia con la etapa anterior es que en esta etapa se busca comprobar o explotar las vulnerabilidades mientras que en la etapa anterior solo se identifican, pero no se tiene un 100% de certeza que la vulnerabilidad exista, para hacer este proceso el pentester puede hacer varias labores:

    - Explotación manual: Manualmente el pentester sin ayuda de herramientas busca comprobar la vulnerabilidad, ejemplo en una vulnerabilidad de directorio por medio de la técnica dot dot slash (../../../../) manualmente la ejecuta en el navegador, otro ejemplo puede ser un ataque de manipulación de parámetros donde por medio de las herramientas de desarrollador del navegador que use podría manipular el parámetro.

    - Explotación con herramientas de forma manual: Por medio de herramientas como en este caso Burpsuite el pentester podría capturar haciendo uso del proxy de interceptación las peticiones enviadas y recibidas, luego podría de forma manual modificar parámetros y entendiendo puntos clave como datos cifrados en base 64 utilizando las herramientas de decoder que brinda la herramienta.

    - Explotación con exploit a la medida: En este caso el pentester podría ejecutar el ataque de dos formas: la primera seria desarrollando su propio exploit desde cero haciendo uso de lenguajes como Python y la segunda seria tomando un exploit publicado en sitios como exploit db y ajustándolo o reprogramándolo a la medida de su necesidad para el ataque, luego de

forma manual o con ayuda de una herramienta podría ejecutar el exploit en la infraestructura objeto de las pruebas para verificar que se logre la explotación.

- Explotación con herramientas de exploit: este punto se refiere al uso de metasploit, esta herramienta contiene una amplia base de datos de exploit´s las cuales pueden ser identificados por sistema operativo, tipo, CVE y demás. Acá el pentester haciendo uso de la herramienta puede comprobar dos cosas: la primera (en la mayoría de casos) que el objetivo realmente sea vulnerable y la segunda que la vulnerabilidad efectivamente es explotable, para ello el pentester manualmente debe configurar los parámetros que utilizara en el exploit como por ejemplo: payloads (medio por el cual el pentester interactúa con el sistema vulnerable, ejemplo consola de comando, webshell, otros), IP origen, puerto origen, IP destino, puerto destino.

- Elaboración de informes: esta etapa final se relaciona con la elaboración del informe técnico, ejecutivo o técnico/ejecutivo donde se plasman los resultados detallados obtenidos durante las pruebas, acá es importante algo que no se mencionó previamente y es que en cada fase se deben documentar los hallazgos obtenidos y los datos que generan las herramientas, en algunos casos piden incluso que se documenten las pruebas que brindaron resultados fallidos o negativos y el paso a paso detallado sobre el proceso de explotación, por lo tanto es importante tener una bitácora y documentar la mayor cantidad de información posible. Una vez se genere ese informe se recomienda ser socializado con el cliente.

- Retest: es una etapa donde se comprueban que las vulnerabilidades identificadas y comprobadas en el pentest inicial hayan sido remediadas por el cliente, normalmente el cliente se encarga de realizar la remediación ya que es la infraestructura de ellos y el pentester (en este caso nosotros) no debería ser juez y parte como ejecutor y como persona que remedie el hallazgo. Según lo identificado puede que las vulnerabilidades sean totalmente resueltas, sean parcialmente resueltas o no resueltas (persistentes). Es importante destacar que no es un ejercicio nuevo completo, para esto se necesitaría ejecutar un segundo pentest o prueba de penetración.

2.1.5 Pregunta 3.

“Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas: Metasploit, Nmap, OpenVas Servicios en línea: ExploitDB CVE”.

2.1.6 Respuesta a la pregunta 3.

Herramientas.

- Metasploit: es una herramienta que por medio de una amplia base de datos nos permite detectar y ejecutar exploits en máquinas objetivos que tengan la vulnerabilidad, es una de las herramientas más utilizadas a nivel general en un pentesting, una de las mayores ventajas de esta herramienta aparte de la posibilidad de utilizar payloads y diferentes métodos para entrar a un sistema vulnerable es que es una herramienta de licenciamiento open, es una herramienta de la marca rapid 7.

- Nmap: es una herramienta muy completa orientada a escaneo de puertos y detección de servicios, de hecho, cuenta con scripts complementarios que ayudan a detectar vulnerabilidades o activos como por ejemplo firewall, WAF. Dentro de las opciones de Nessus se tiene escaneos de tipo TCP, UDP, furtivo, half open, entre otros, por medio de estas técnicas se puede identificar puertos y servicios. También existe un programa con interfaz gráfica llamado zenmap para Linux y Windows, por último, Nmap funciona con licencia open.

- OpenVas: OpenVAS es un escáner de vulnerabilidades de licencia open, que permite realizar pruebas de vulnerabilidades, de hecho, nace de una versión inicial de Nessus por lo tanto compartieron muchas funcionalidades y bases de datos, actualmente OpenVas si bien cumple la función no es tan efectivo como un Nessus, OpenVAS al igual que Nessus podría ser utilizado para pruebas de infraestructura y web.

Servicios en línea:

- ExploitDB: es un servicio en línea que contiene una amplia base de datos de exploits y scripts, entre ellos los de Google hacking (GHDB) que en algún momento fueron creados y mantenidos por Jhonny Long. Por medio de este servicio se pueden buscar exploits para ser ejecutados en equipos objetivo por medio de nombre de vulnerabilidad, tipo de servicio, aplicación, servidor y CVE, este exploit o grupo de exploits que se consigan para el equipo objetivo pueden ser ajustados a la medida según la pericia del pentester e incluso podrían ser importados a metasploit.

- CVE: (Common vulnerabilities and exposures) es una lista de vulnerabilidades conocidas administradas por mitre, por medio de esta lista se pueden clasificar las vulnerabilidades que se descubren de forma diaria hacia los equipos y sistemas vulnerables, por medio de esta lista podemos también clasificar vulnerabilidades para los hallazgos, buscar exploits e incluso otras técnicas de

comprobación o explotación, similar a CVE existen otras listas como CWE, BID, IAVA, CAPEC, IAVA, IAVB.

2.1.7 Pregunta 4.

Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1– Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad.

2.1.8 Respuesta a la pregunta 4.

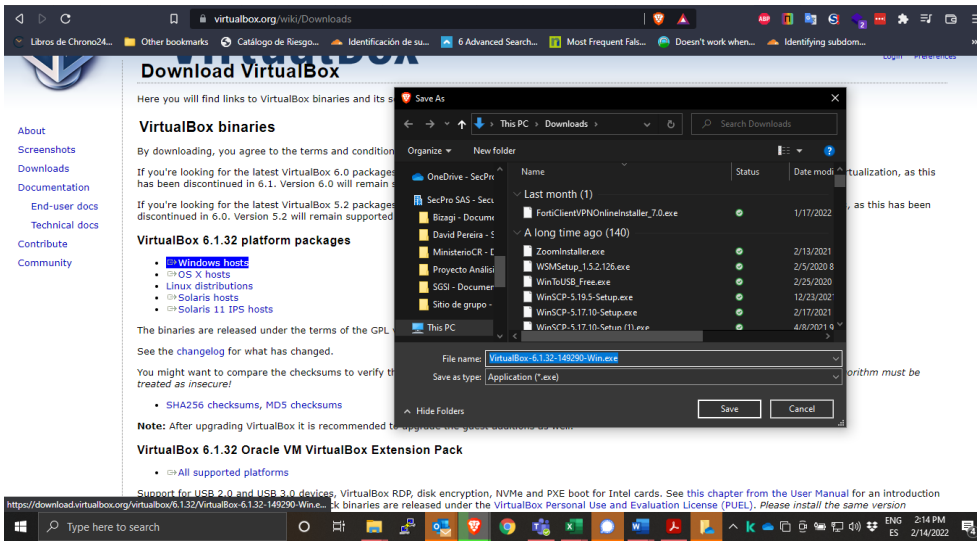
Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

- Paso A: Descargar la herramienta hipervisor “VirtualBox” en su última versión.

<u>Paso A</u>

En la figura 1 se evidencia la descarga de virtual box última versión:

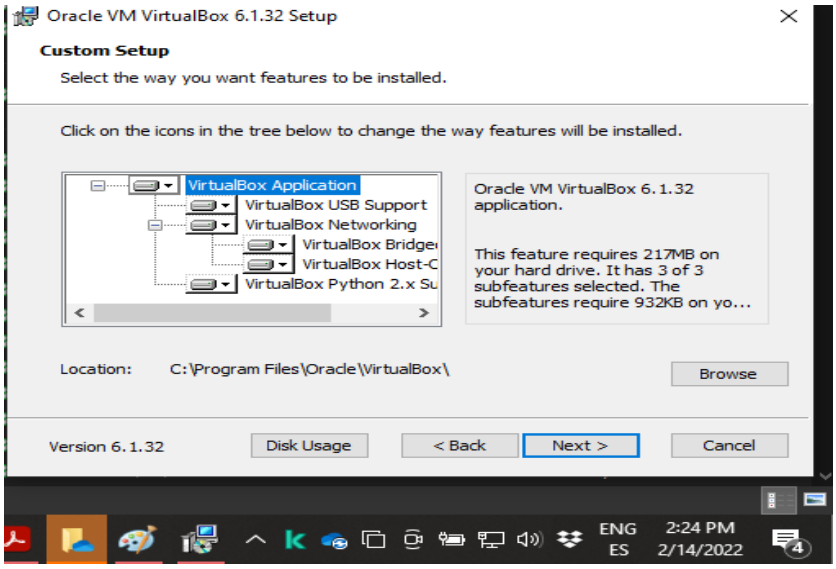
Figura 1. Descarga de virtual box



Fuente: el autor

En la figura 2 se evidencia el proceso de instalación de virtual box

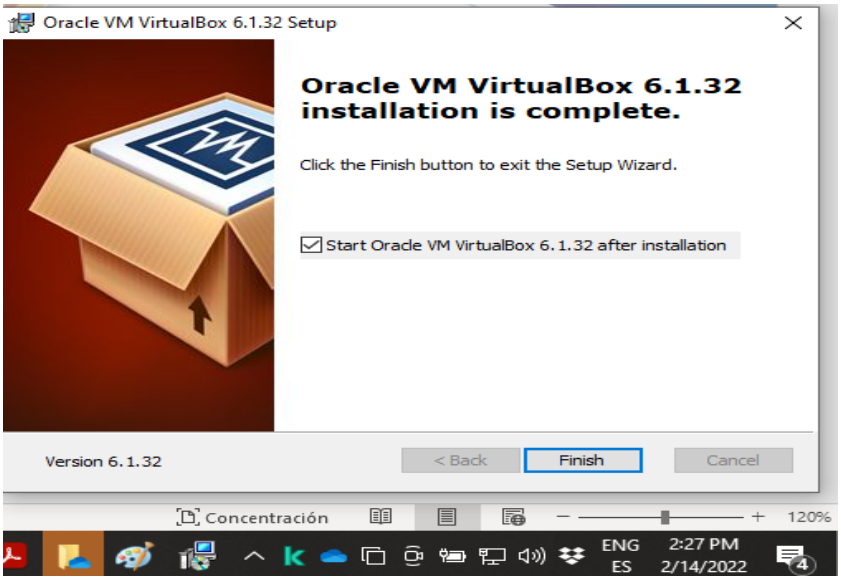
Figura 2. Proceso de instalación de VirtualBox



Fuente: el autor

En la figura 3 se evidencia que el proceso de instalación se completó de manera exitosa

Figura 3. Instalación completada de VirtualBox



Fuente: el autor

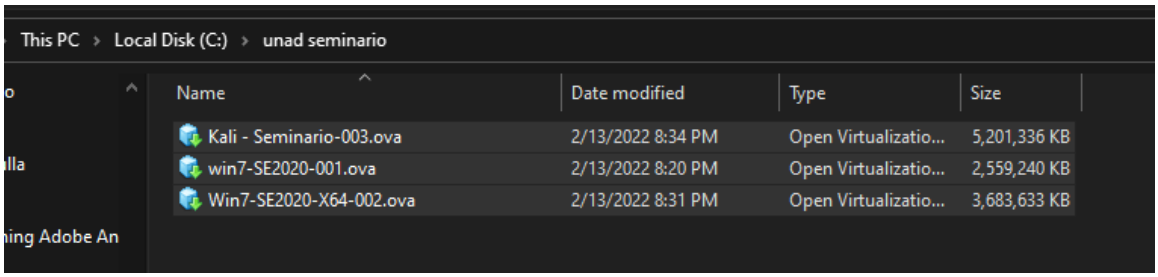
- Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato .OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico.

En las imágenes .OVA existe: Un Windows 7 X86, un Windows 7 X64, un Kali Linux.

Paso B

En la figura 4 se evidencia la descarga de las máquinas virtuales

Figura 4. Descarga de máquinas virtuales

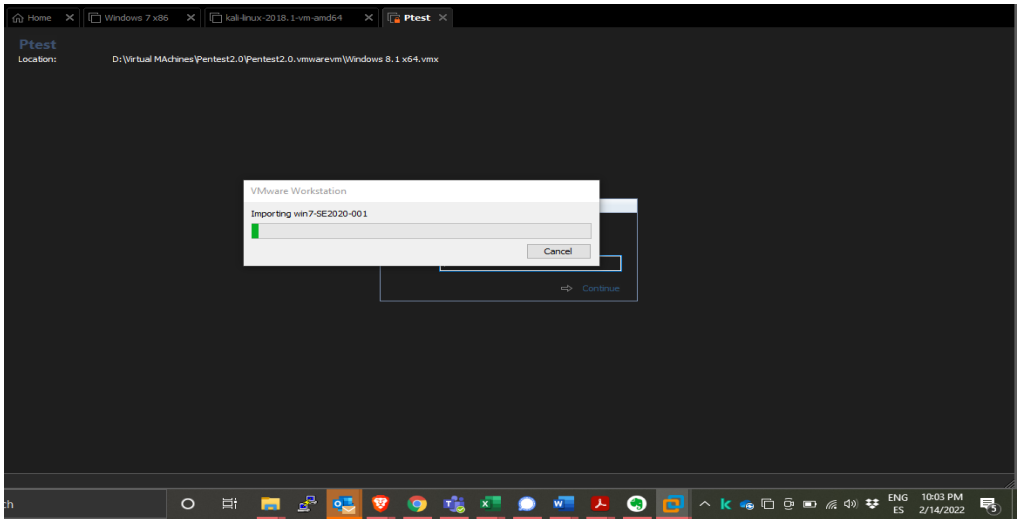


Fuente: el autor

Importación de las máquinas virtuales en Kali Linux

Nota: no se realizó el proceso en VirtualBox ya que mi máquina virtual Kali está en VMware, en la figura 5 se evidencia el proceso de importación en VMware ya instalado previamente.

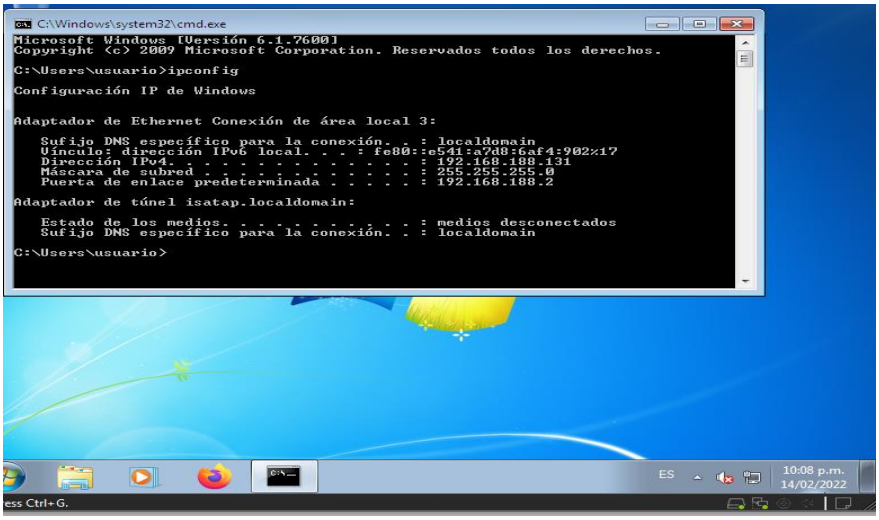
Figura 5. Importación máquina virtual Windows



Fuente: el autor

En la figura 6 se evidencia el encendido y verificación de IP máquina virtual Windows 7Se1.

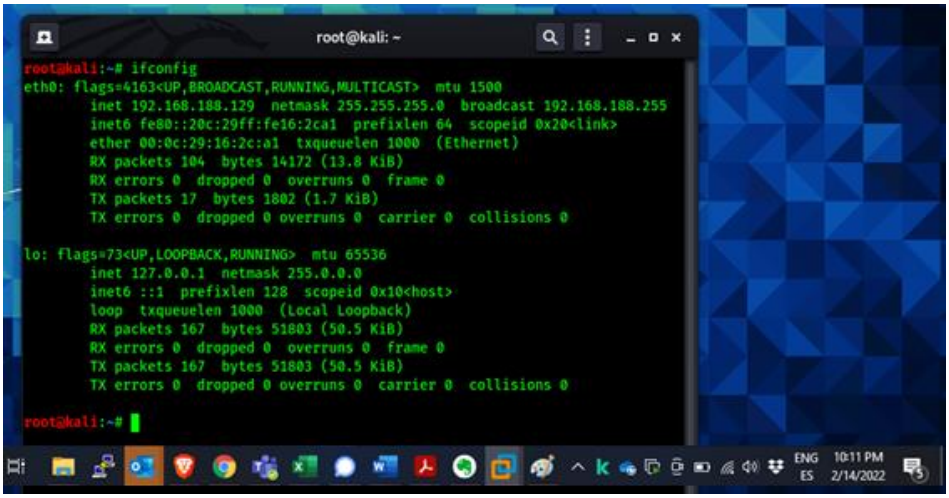
Figura 6. Encendido e IP de máquina Windows



Fuente: el autor

En la figura 7 se evidencia la IP Máquina virtual Kali

Figura 7. Configuración IP máquina Kali Linux



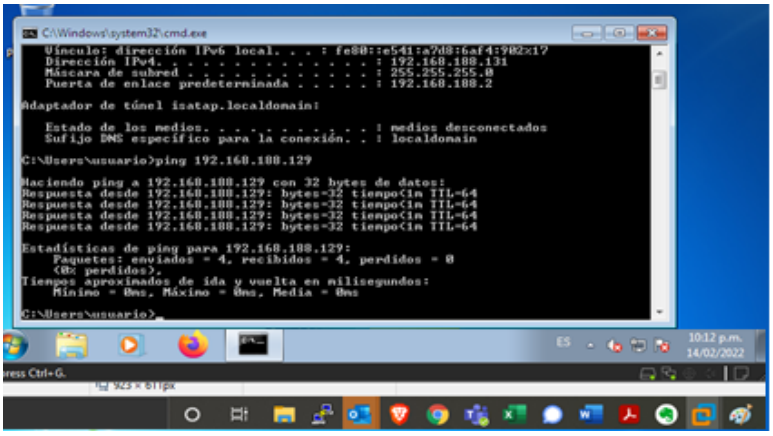
Fuente: el autor

- Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Paso C

En la figura 8 se evidencia la prueba de ping por ICMP desde Windows

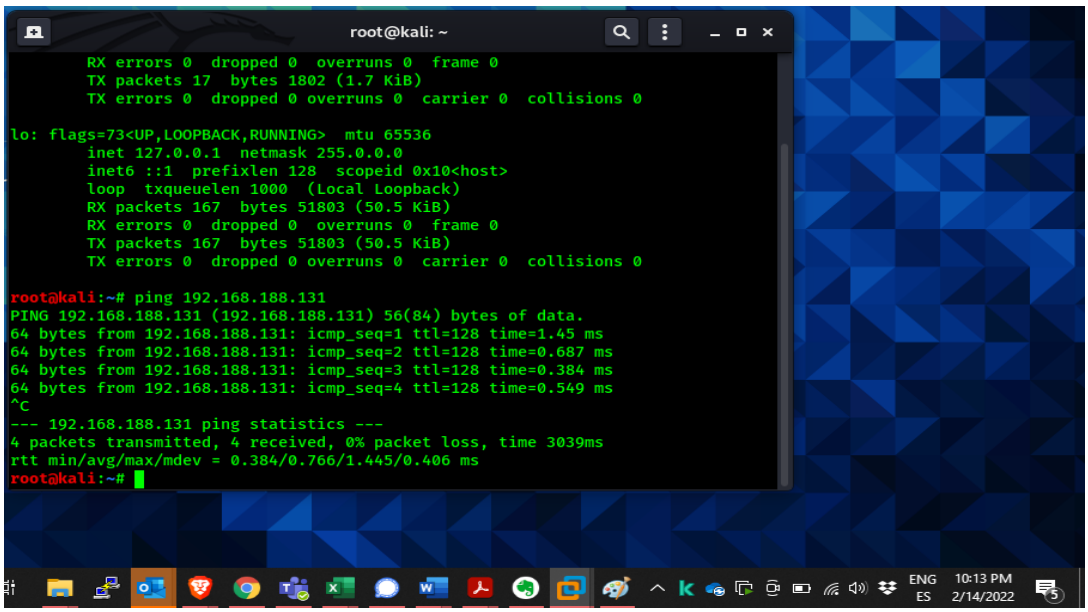
Figura 8. Ping máquina Windows a kali



Fuente: el autor

En la figura 9 se evidencia el mismo proceso, pero en el sentido contrario es decir de la maquina Kali a la Windows

Figura 9. Ping máquina kali a Windows



Fuente: el autor

2.2 SEGUNDO SET DE ACTIVIDADES DENTRO DEL PERIODO DE PRUEBA:

Dentro de este set se realiza el proceso de consultoría referente al modelo de contrato y acuerdo de confidencialidad para los nuevos equipos de red/Blue Team basados en la ley de delitos informáticos 1273 de 2009.

2.2.1 Pregunta 1

"¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad".

2.2.2 Respuesta a la pregunta 1.

Después de analizar la documentación suministrada se evidencian las siguientes anormalidades:

Anexo 3:

- Clausula 1: ítem "se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados."

  Análisis: dentro de esta cláusula hay dos puntos muy preocupantes que dan un síntoma claro de actividades ilegales dentro del proceso de Red Team y Blue Team, el primero es que el contratado no podría divulgar información a las autoridades legales ante algún incidente o suceso que requiera su apoyo como por ejemplo una actividad ilícita o una implicación delictiva. La segunda y más preocupante que se relaciona con procesos ilegales dentro de la empresa contratante no podrán ser divulgados, significa que se harán procesos ilegales e incluso delictivos con el fin de llevar a cabo el objetivo de la empresa o del cliente que le pide a la empresa.

- Clausula 2: ítem 2 Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"

Análisis: Dentro de esta cláusula aún más preocupante se detallan pruebas que violan las leyes y la privacidad de las personas como son las chuzadas (escuchar o interceptar comunicaciones de personas de forma no autorizada), interceptación de información (captura u obtención de información por medio de escucha de tráfico, archivo malicioso instalado en un equipo o dispositivo de forma no autorizada) y por ultimo acceso abusivo a sistema informático donde una persona o grupo malicioso accede sin autorización del titular o dueño de un activo , acceso, otros al sistema de información.

- Clausula 3: ítem 3 No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

  Análisis: En esta cláusula también piden hacer varias cosas ilegales, la primera que avalen el espionaje y robo de información a terceros y la segunda que no puedan denunciar ante las autoridades legales sobre estos delitos, lastimosamente en esta empresa buscan de alguna manera cubrirse y culpar directamente a los empleados que hagan el delito, también si el caso dado una persona ética encuentra una actividad delictiva no lo pueda decir ante las autoridades competentes.

- Clausula 4: ítem 4 Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

  Análisis: Al igual que la cláusula anterior buscan que no se denuncie los actos delictivos que se estarían haciendo durante las actividades de “Red Team”.

- Clausula 4: ítem 7 Responder por el mal uso que le den sus representantes a la información confidencial.

  Análisis: Acá de una forma directa buscan culpar a la persona que firme el acuerdo sobre el mal uso que hagan los superiores o representantes de la empresa sobre la información “confidencial” obtenida de manera maliciosa

- Clausula 3: ítem 8 Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

  Análisis: En esta cláusula de forma directa la empresa está implicando al empleado que firme el acuerdo toda la responsabilidad de las acciones que puedan imputar contra la empresa y sus directivos por tener información confidencial obtenida de manera maliciosa o delictiva, esta cláusula que parece más una imputación no es ética ni legal.

- Clausula 8: 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.

  Análisis: Nuevamente la empresa de forma no ética e ilegal quieren evadir toda responsabilidad sobre los delitos que allí se cometen y buscan implicar al empleado sea directamente culpable o no sea culpable sino parte del equipo de Red Team.

2.2.3 Pregunta 2.

"Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 - Acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273".

2.2.4 Respuesta a la pregunta 2.

Dentro de los procesos ilegales o anormales de las cláusulas previamente descritas en el punto 2 se encuentran que vulneran las siguientes leyes colombianas:

- Clausula 1: "se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados."

  Análisis: en esta cláusula se vulneran los siguientes artículos de la ley 1273 de 2009

  - Articulo 269 F (Violación de datos personales) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 H (Circunstancias de agravación punitiva) es el aumento de pena de cualquier artículo de la ley si se comete el delito sobre sistemas estatales u oficiales, si se comete aprovechando la confianza depositada por el poseedor de la información, revelando la información en un perjuicio de otro, obtención de provecho para sí mismo o un tercero.

  Adicionalmente en esta cláusula se vulneran los siguientes artículos de la ley 1581 de 2012.

  - Principio de libertad

- Principio de confidencialidad

- Principio de transparencia

- Clausula 2: ítem 2 Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"

  Análisis: en esta cláusula se vulneran los siguientes artículos de la ley 1273 de 2009

  - Articulo 269 A (acceso abusivo a un sistema informático), da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 B (Obstaculización ilegítima de sistema informático o red de telecomunicación) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 C (Interceptación de datos informáticos) da para una pena de máximo 72 meses.

  - Articulo 269 E (Uso de software malicioso) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 F (Violación de datos personales) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 H (Circunstancias de agravación punitiva) es el aumento de pena de cualquier artículo de la ley si se comete el delito sobre sistemas estatales u oficiales, si se comete aprovechando la confianza depositada por el poseedor de la información, revelando la información en un perjuicio de otro, obtención de provecho para sí mismo o un tercero.

  - Articulo 269 J (Transferencia no consentida de activos) da para una pena de máximo 120 meses y multa de 1500 salarios mínimos legales mensuales vigentes.

Adicionalmente en esta cláusula se vulneran los siguientes artículos de la ley 1581 de 2012.

- Principio de libertad

- Principio de confidencialidad

- Principio de transparencia

- Clausula 3: ítem 3 No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

  Análisis: en esta cláusula se vulneran los siguientes artículos de la ley 1273 de 2009

  - Articulo 269 B (Obstaculización ilegítima de sistema informático o red de telecomunicación) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 C (Interceptación de datos informáticos) da para una pena de máximo 72 meses.

  - Articulo 269 F (Violación de datos personales) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 H (Circunstancias de agravación punitiva) es el aumento de pena de cualquier artículo de la ley si se comete el delito sobre sistemas estatales u oficiales, si se comete aprovechando la confianza depositada por el poseedor de la información, revelando la información en un perjuicio de otro, obtención de provecho para sí mismo o un tercero.
  - Articulo 269 J (Transferencia no consentida de activos) da para una pena de máximo 120 meses y multa de 1500 salarios mínimos legales mensuales vigentes.

- Clausula 4: ítem 4 Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

  Análisis: en esta cláusula se vulneran los siguientes artículos de la ley 1273 de 2009

  - Articulo 269 B (Obstaculización ilegítima de sistema informático o red de telecomunicación) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 C (Interceptación de datos informáticos) da para una pena de máximo 72 meses.

- Articulo 269 F (Violación de datos personales) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.
- Articulo 269 H (Circunstancias de agravación punitiva) es el aumento de pena de cualquier artículo de la ley si se comete el delito sobre sistemas estatales u oficiales, si se comete aprovechando la confianza depositada por el poseedor de la información, revelando la información en un perjuicio de otro, obtención de provecho para sí mismo o un tercero.

- Articulo 269 J (Transferencia no consentida de activos) da para una pena de máximo 120 meses y multa de 1500 salarios mínimos legales mensuales vigentes

Adicionalmente en esta cláusula se vulneran los siguientes artículos de la ley 1581 de 2012.

- Principio de libertad

- Principio de confidencialidad

- Principio de transparencia

- Clausula 4: ítem 7 <u>Responder por el mal uso que le den sus representantes a la información confidencial.</u>

  Análisis: en esta cláusula se vulneran los siguientes artículos de la ley 1273 de 2009.
  - Articulo 269 F (Violación de datos personales) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 H (Circunstancias de agravación punitiva) es el aumento de pena de cualquier artículo de la ley si se comete el delito sobre sistemas estatales u oficiales, si se comete aprovechando la confianza depositada por el poseedor de la información, revelando la información en un perjuicio de otro, obtención de provecho para sí mismo o un tercero.

  Adicionalmente en esta cláusula se vulneran los siguientes artículos de la ley 1581 de 2012.

  - Principio de libertad

  - Principio de confidencialidad

  - Principio de transparencia

- Clausula 3: ítem 8 Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

  Análisis: en esta cláusula se vulneran los siguientes artículos de la ley 1273 de 2009.

  - Articulo 269 F (Violación de datos personales) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 H (Circunstancias de agravación punitiva) es el aumento de pena de cualquier artículo de la ley si se comete el delito sobre sistemas estatales u oficiales, si se comete aprovechando la confianza depositada por el poseedor de la información, revelando la información en un perjuicio de otro, obtención de provecho para sí mismo o un tercero.

Adicionalmente en esta cláusula se vulneran los siguientes artículos de la ley 1581 de 2012.

- Principio de libertad

- Principio de confidencialidad

- Principio de transparencia

- Clausula 8: <u>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</u>.

  Análisis: en esta cláusula se vulneran los siguientes artículos de la ley 1273 de 2009.

  - Articulo 269 F (Violación de datos personales) da para una pena de máximo 96 meses y 1000 salarios mínimos legales mensuales vigentes.

  - Articulo 269 H (Circunstancias de agravación punitiva) es el aumento de pena de cualquier artículo de la ley si se comete el delito sobre sistemas estatales u oficiales, si se comete aprovechando la confianza depositada por el poseedor de la información, revelando la información en un perjuicio de otro, obtención de provecho para sí mismo o un tercero.

  Adicionalmente en esta cláusula se vulneran los siguientes artículos de la ley 1581 de 2012

- Principio de libertad

- Principio de confidencialidad

2.2.5 Pregunta 3.

"¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿usted como experto en ciberseguridad aplicaría a este trabajo en TheWhiteHouse, 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".

2.2.6 Respuesta a la pregunta 3.

Como consultores expertos en ciberseguridad y como ciudadanos de bien formado **no** se tomaría el trabajo de la empresa TheWhiteHouse por $15.000.000 ni por XXXXX millones de pesos. Bajo las enseñanzas de ética brindadas por familiares, instructores, colegas docentes y demás no es ético acceder a ese trabajo, además hay otros motivos dentro de los cuales se resume: es ilegal y puede dar cárcel, podría afectar la vida de muchas personas víctimas de los actos delictivos que allí piden, se podría generar dinero ilícito para los terceros e incluso recibir pagos de esos dineros, el consultor podría ser víctima de amenazas, entre otros.

Por último, de manera profesional el consejo profesional nacional de ingeniería COPNIA[1] sobre los cuales se rigen todos los ingenieros del país tiene un código de ética sobre el cual se rige el comportamiento profesional del ingeniero, dentro de ese código se puede rescatar lo siguiente:

- Resalta la importancia de la ley 842 de 2003 emitida por el congreso de la República de Colombia relacionada con el título VI, código de ética profesional y los artículos relacionados con el código de ética profesional dentro de los cuales se destacan

    - Cumplir con los requerimientos de COPNIA.

    - Custodia de los bienes, valores, documentos e información que tenga acceso, evitando el uso indebido (esto es una violación directa con las cláusulas de TheWhiteHouse)

[1] (COPNIA, 2015)

- Denunciar los delitos, contravenciones y faltas contra el código de ética, aportando toda la información y pruebas que se tuviera en su poder (esto es una violación directa con las cláusulas de TheWhiteHouse)

- Permitir, tolerar o facilitar el ejercicio ilegal de la profesión (esto es una violación directa con las cláusulas de TheWhiteHouse)

- Causar intencionalmente daño o perdida de bienes, equipos, herramientas, documentos que por razón del ejercicio se tuviera en su poder.

- Rechazar toda clase de recomendaciones en trabajos que impliquen daños evitables al entorno humano.

- Ofrecer o aceptar trabajos en contra de las disposiciones legales, vigentes o aceptar tareas que excedan la incumbencia que otorga su título (esto es una violación directa con las cláusulas de TheWhiteHouse)

2.2.7 Pregunta 4.

"Deberá buscar la noticia del caso "OPERACIÓN ANDRÓMEDA BUGGLY" en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar".

2.2.8 Respuesta a la pregunta 4.

La operación Andrómeda Buggly fue una operación ejecutada por las fuerzas armadas de Colombia en el periodo de 2012 a 2014 en aras de poder reclutar personal y conocimientos sobre técnicas avanzadas de hacking, esto lo hicieron por medio de un sitio donde recibían a todos los geeks o expertos en ciberseguridad de la época que quisieran estar allí, era una especie de hackaton o safe place para este grupo de personas. Según los medios oficiales y las fuerzas armadas de Colombia no se realizó ningún tipo de investigación maliciosa ni se incumplió ninguna ley o norma principalmente la 1273 de 2009, solo accedieron confirmar que si hubo actividades de inteligencia. dentro de los implicados se resalta principalmente el Sr Andrés Sepúlveda donde entre las supuestas actividades que hizo tuvo acceso a información confidencial por parte de las fuerzas armadas por medio de errores de procedimiento.

Como consultores se podría hacer un informe extenso sobre el caso en mención, pero no es el objeto del informe; ahora bien, las implicaciones legales y los puntos de vista del equipo consultor son:

- El equipo considera que hubo actividades maliciosas y delictivas dentro de esas instalaciones por algunos integrantes del grupo.

- El equipo desconoce que integrantes lo hicieron y si fue de forma no intencionada o intencionada.

- Hubo clara violación de la ley 1273 de 2009 para el equipo en todos los artículos.

- El equipo cree que no todos los implicados fueron capturados ni se comprobara el grado de culpabilidad de los implicados.

- Lastimosamente el equipo considera que también personal de las fuerzas armadas estuvieron implicados dentro de los actos que infringen la ley 1273 de 2009.

- Es posible que no todos los implicados tengan su imputación de cargos y reciban la pena que debe darse bajo la ley colombiana.

2.3 TERCER SET DE ACTIVIDADES DENTRO DEL PERIODO DE PRUEBA

2.3.1 Pregunta 1.

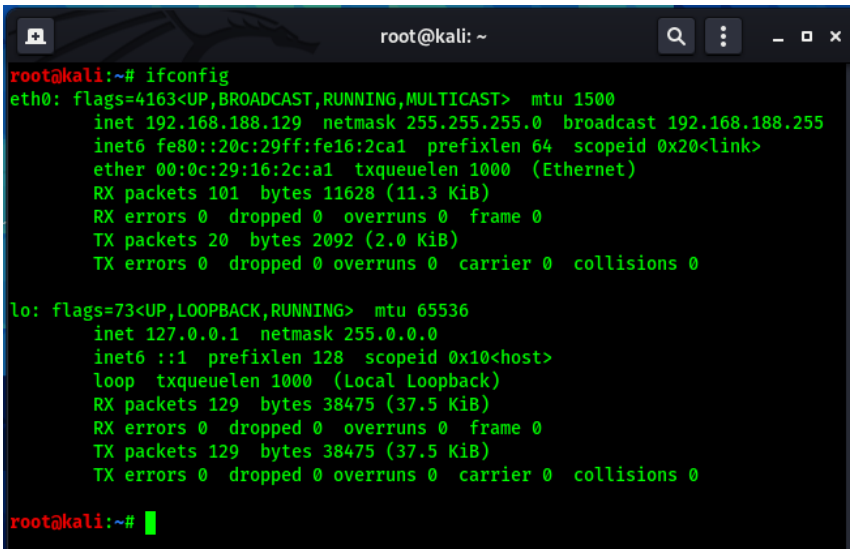
“Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Red Team. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting”.

2.3.2 Respuesta a la pregunta 1.

Reconocimiento

En la figura 10 se evidencia la ejecución del comando ifconfig para detectar el segmento de red del equipo Kali y tomar esa referencia como punto de partida

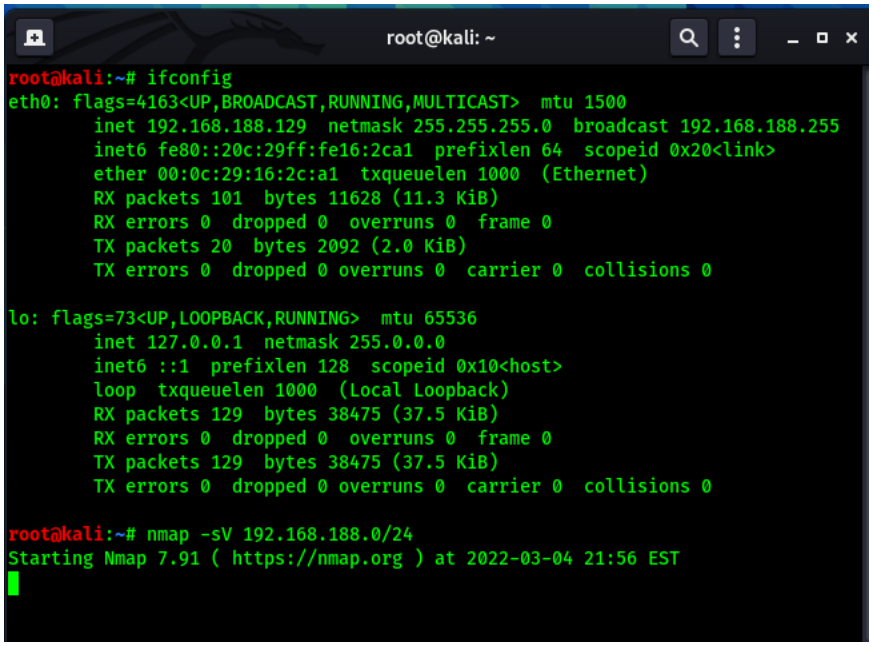
Figura 10. Identificación de segmento de red a ser analizado



Fuente: el autor

Posteriormente como se aprecia en la figura 11 se inician escaneos de redes con el comando Nmap -sV

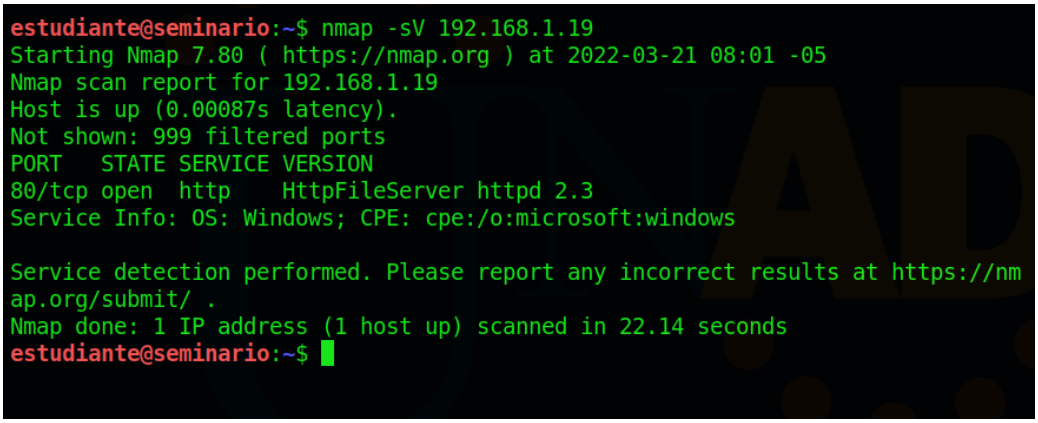
Figura 11. Ejecución de comando Nmap -sV



Fuente: el autor

Posteriormente como se evidencia en la siguiente figura se logra identificar el equipo Windows 7 con el/los puertos abiertos

Figura 12. Resultado de reconocimiento y enumeración de puertos TCP en equipo Windows

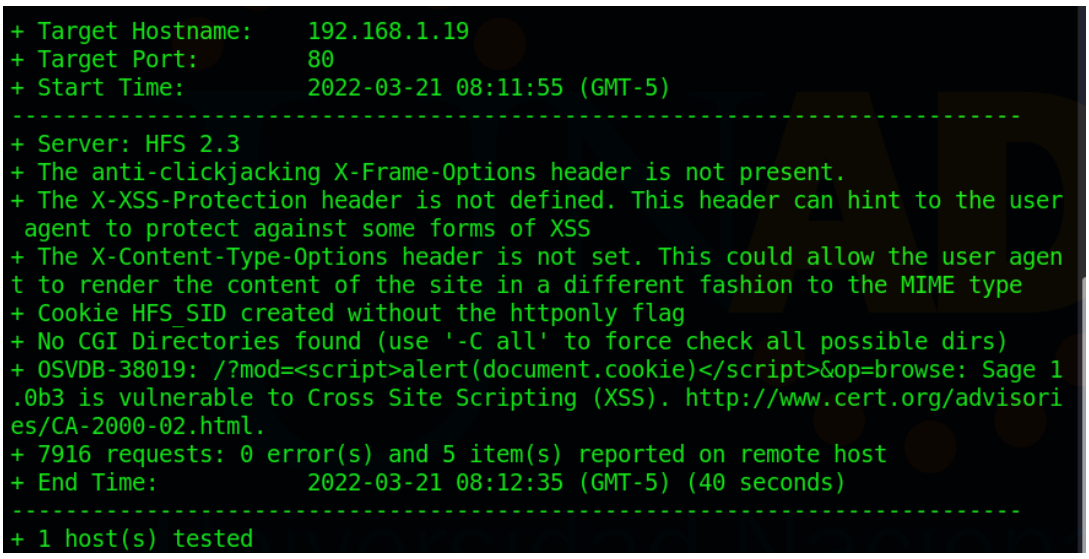


Fuente: el autor

Escaneo de vulnerabilidades

Se inicia el proceso de escaneo de vulnerabilidades para identificar posibles vulnerabilidades en el equipo Windows como se evidencia en la figura 13.

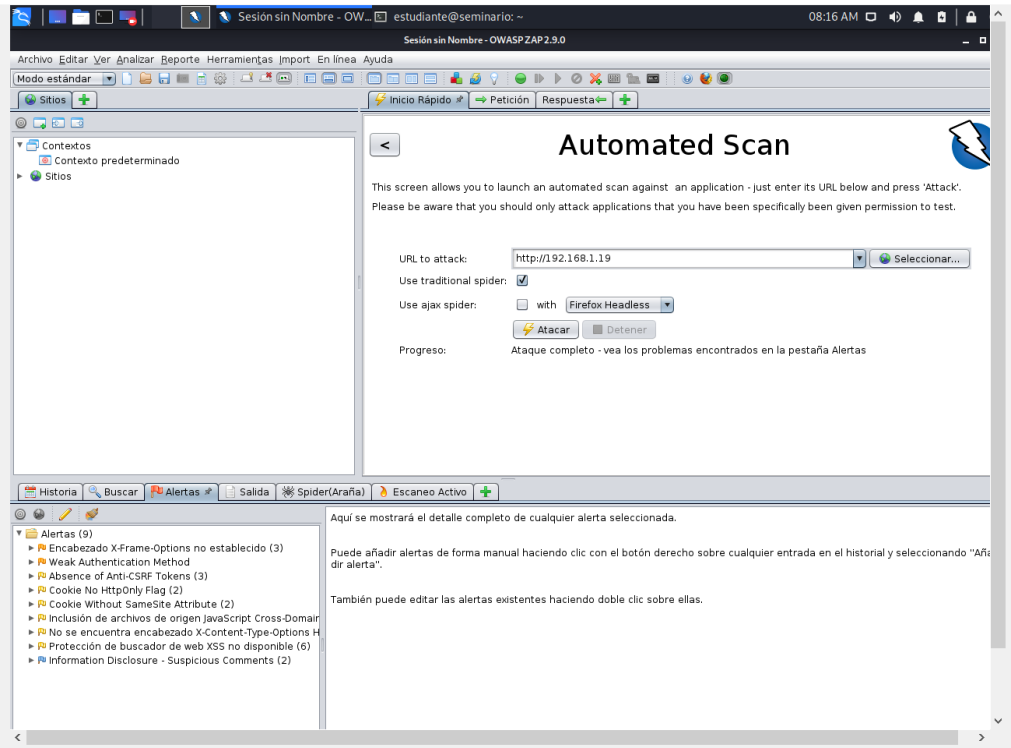
Figura 13. Escaneo de vulnerabilidades con nikto



Fuente: el autor

Se continua con otras herramientas el escaneo como se evidencia en la figura 14.

Figura 14. Escaneo de vulnerabilidades con ZAP



Fuente: el autor

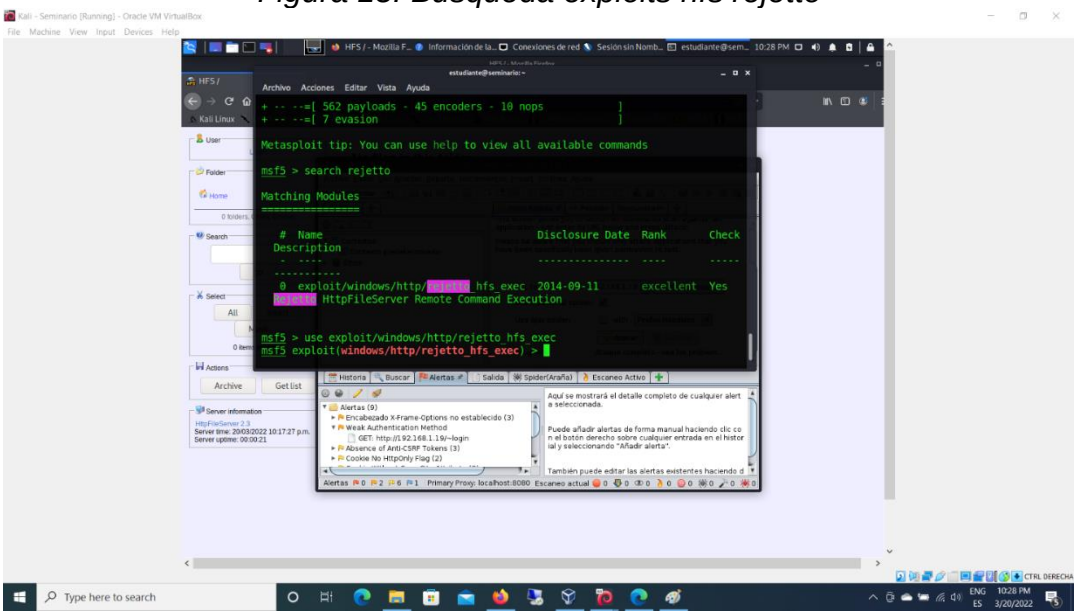
Se realiza también búsquedas manuales en clear web sobre posibles vulnerabilidades asociadas a los puertos y servicios descubiertos, dentro de esas búsquedas se identifican posibles vulnerabilidades relacionadas con el servicio HFS que podrían conllevar a una consola remota.

Explotación

Partiendo de la premisa anterior y haciendo uso de la herramienta metasploit se identifican posibles exploits que serán utilizados como se evidencia en las figuras 15 a la 19

En la figura 15. Se puede identificar la búsqueda del exploit.

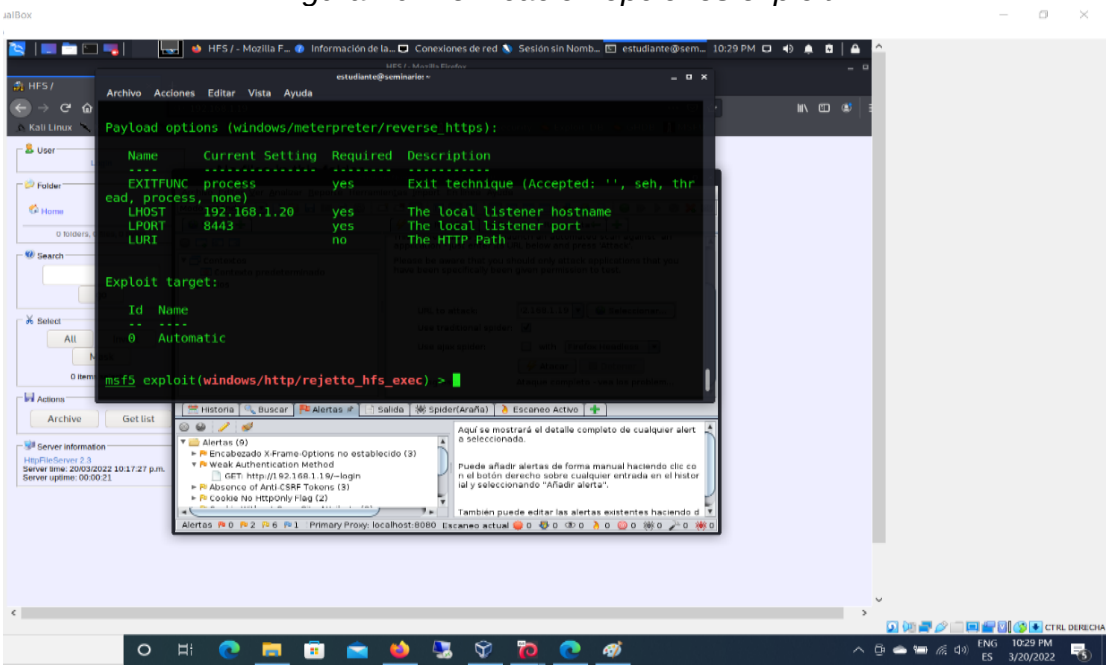
Figura 15. Búsqueda exploits hfs rejetto



Fuente: el autor

En la figura 16 se puede identificar las opciones que brinda el exploit.

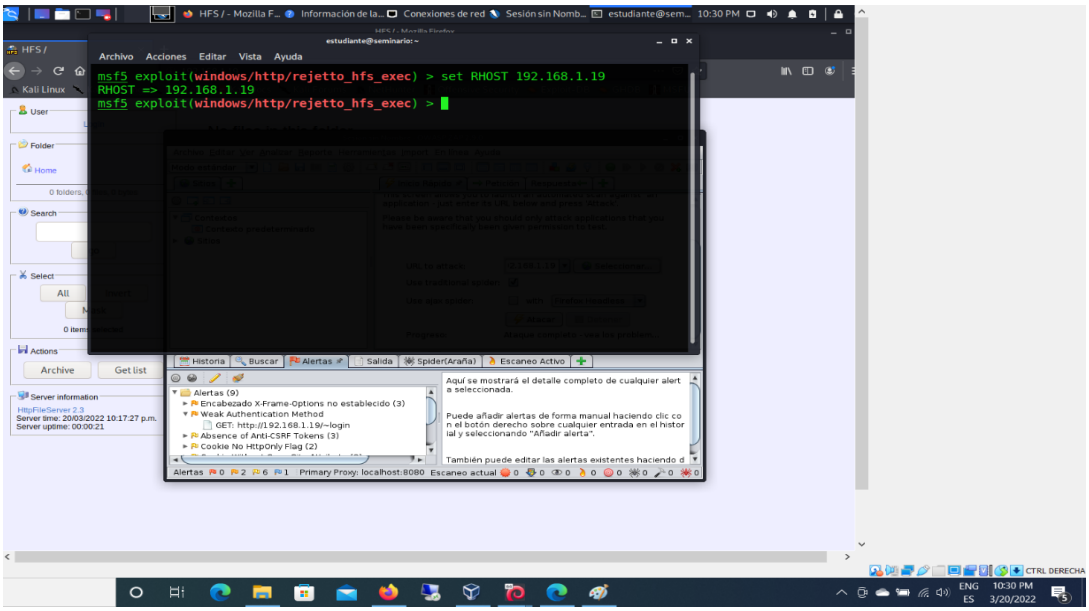
Figura 16. Verificación opciones exploit



Fuente: el autor

En la figura 17 se puede identificar la configuración del host remoto

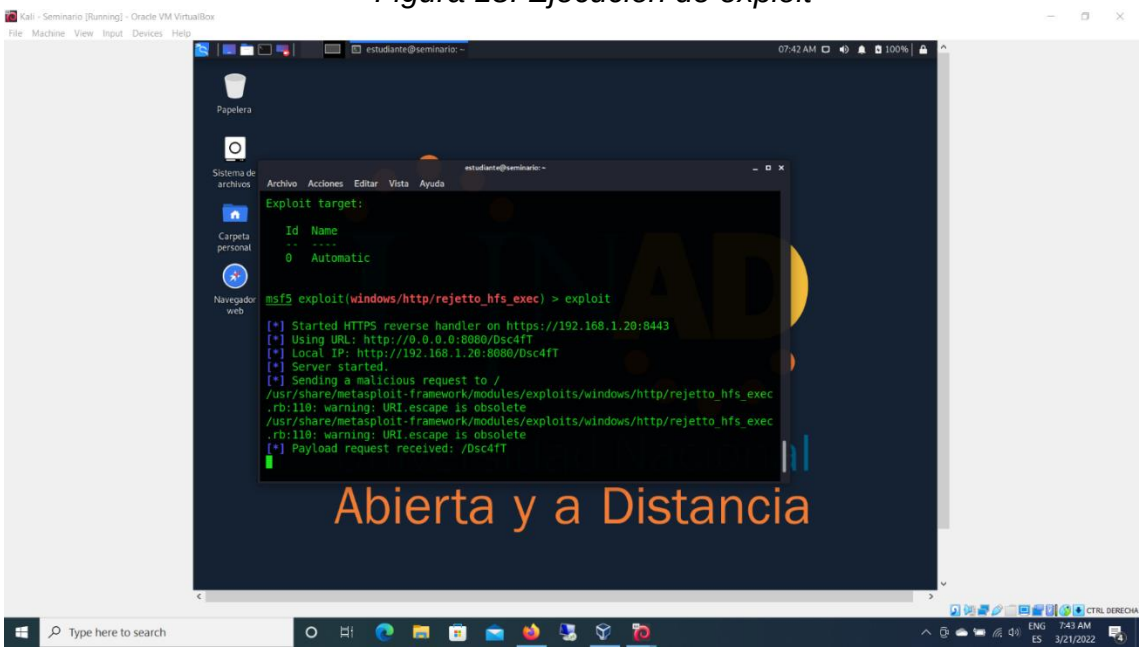
Figura 17.Cconfiguración RHOST



Fuente: el autor

En la figura 18 se puede identificar la ejecución del exploit

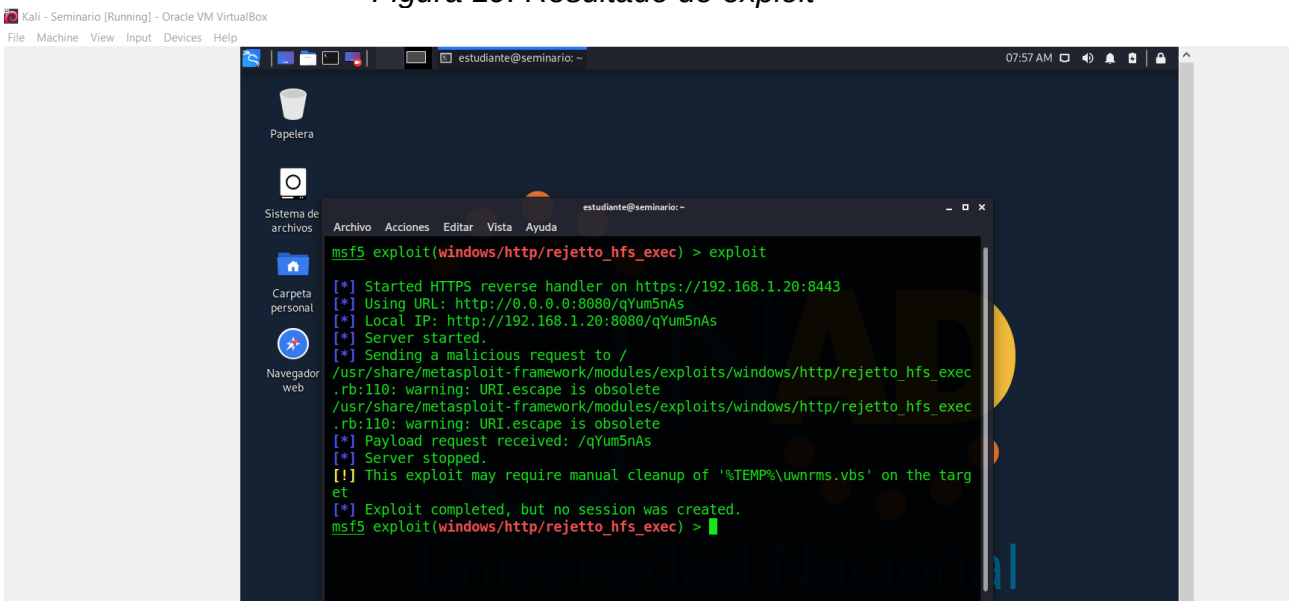
Figura 18. Ejecución de exploit



Fuente: el autor

En la figura 19 se puede identificar el resultado del exploit

Figura 19. Resultado de exploit



Fuente: el autor

Como se evidencia en la figura 19 se logró ejecutar el exploit en este caso sin que generara la sesión remota por meterpreter, sin embargo, se comprueba que el sistema es vulnerable y puede o pudo ser víctima de esta vulnerabilidad.

Disclaimers**:**

- Se realizaron intentos de explotación a vulnerabilidades críticas que pueden generar un Shell reverso al pentester, en este caso tuve dificultades ya que según la investigación realizada el exploit de eternal blue en algunos sitios comentan que funciona al 100% en sistemas de 64 bits, en otros sitios indican que funcionan en 32 y 64 bits pero no con la versión home premium, sin embargo dentro de las labores que realice y las investigaciones no logre encontrar a tiempo la forma de generar el Shell reverso.

- Teniendo en cuenta las indicaciones de los instructores, se cambia escenario de laboratorio debido que en la primera versión del trabajo se tuvo fallas para utilizar la máquina virtual x64 y se tuvo problemas para acceder al recurso rejjeto.zip debido a que en los archivos se adjuntó un RAT dark comet y el antimalware lo detecto como archivo malicioso

2.3.3 Pregunta 2.

“A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 7 X64”.

2.3.4 Respuesta a la pregunta 2

- Al indicar que el servidor posiblemente tiene un Shell reverso significa que podría ser una vulnerabilidad cuyo exploit maneje un payload que genere consola de comandos tcp con meterpreter u otros.

- Luego se indica que es una sesión de meterpreter, lo que confirma la anterior premisa.

- Otro factor bajo mi experiencia es que existen numerosas vulnerabilidades con Shell reverso que pueden ser aprovechadas por puerto SMB.

- También existen vulnerabilidades de tipo HTTP donde se puede hacer inyecciones o manipulaciones para tener un webshell o consola de comando.

2.3.5 Pregunta 3.

“¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la máquina Windows 7? ¿Qué puerto abre la aplicación específica en el anexo?”

2.3.6 Respuesta a la pregunta 3.

Las herramientas utilizadas para los diferentes procesos fueron:

- Reconocimiento y enumeración:
  - Nmap
  - Nikto
  - Nessus
- Explotación:
  - Metasploit

    Los puertos identificados que fueron utilizados para los intentos de explotación fueron HTTP 80

2.3.7 Pregunta 4.

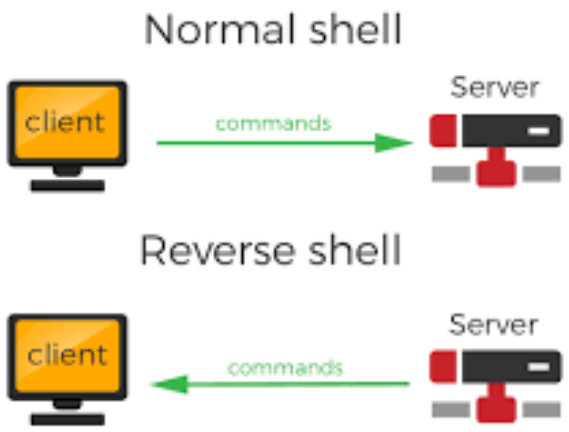
“Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque”.

2.3.8 Respuesta a la pregunta 4

El ataque ejecutado donde se explota una vulnerabilidad que permite generar un Shell o consola reversa, brinda al Penetration Tester (en este caso) un acceso a consola de comandos del equipo afectado con permisos administrativos (usuario NT AUTHORITY SYSTEM). Con este acceso el pentester puede ejecutar cualquier comando y tiene control total sobre la maquina sin que el usuario final lo note, por este motivo es que este ataque es tan crítico y de alto impacto.

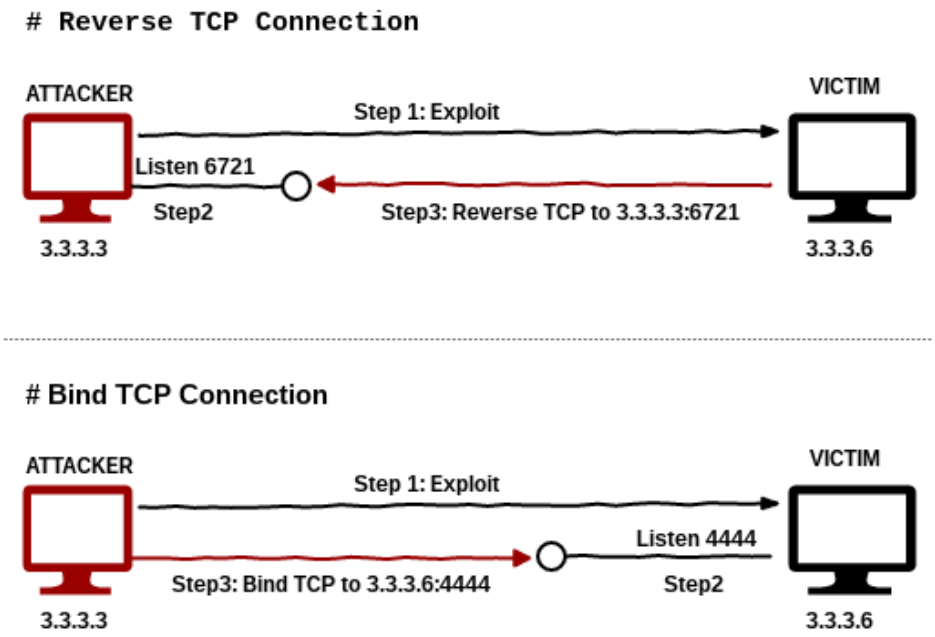
A continuación, se relacionan unos gráficos explicando el ataque como se evidencia en la figura 20 y 21 y se presenta la diferencia entre un Shell normal y reverso:

Figura 20. Shell reverso



Fuente: https://rioasmara.com/2022/01/16/core-impact-agent-install-with-reverse-shell/

Figura 21. Conexión reversa TCP



Fuente: https://underc0de.org/foro/hacking/t36409/

2.3.9 Pregunta 5.

“Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7”.

2.3.10 Respuesta a la pregunta 5.

La serie de pasos realizados fueron:

Laboratorio

- Escaneo / enumeración de servicios del segmento de red utilizando el comando Nmap -sS 192.168.1.0/24.
- Identificación de IP del equipo Windows 192.168.1.19 con puertos y servicios abiertos en TCP.
- Escaneo / enumeración de posibles url del equipo con herramienta nikto y ZAP.
- Investigación en clear web para identificar posibles vulnerabilidades del servicio HFS por puerto 80.

- Búsqueda de exploits con la herramienta metasploit para el servicio HFS del sistema operativo Windows 7.

- Análisis de la información recabada con las herramientas de escaneo de vulnerabilidades.

- Uso de exploit exploit/windows/http/rejetto_hfs_exec.

- Investigación en clear web para identificar posibles opciones o alternativas en aras de poder completar la explotación trayendo el shell reverso.

- Se intento realizar la explotación sin forma de obtener el Shell reverso.

Nota: las evidencias de los pasos anteriormente realizados se detallan en el punto 1 del set de actividades 3

2.4 CUARTO SET DE ACTIVIDADES DENTRO DEL PERIODO DE PRUEBA.

En este set de pruebas se realiza la Consultoría al equipo de Blue Team.

2.4.1 Pregunta 1.

"¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos".

2.4.2 Respuesta a la pregunta 1.

- Programas y procesos en ejecución: los programas y procesos en ejecución ayudan a identificar como su nombre indica que procesos y programas tienen el mayor consumo de recursos de RAM, disco y procesador de la estación, servidor o activo afectado, esto puede ayudar a identificar de una forma relativamente rápida si un proceso o programa está consumiendo de forma elevada recursos y con esto se podría hacer un process kill para recuperar recursos del activo.

- Conexiones /trafico de red: por medio de un sniffer, línea de comandos para ver conexiones establecidas, tablas de enrutamiento o función de monitoreo de red sea por medio del firewall, switch y otros se podría evidenciar el tráfico entrante y saliente hacia el activo afectado, esto nos permite en un periodo corto o mediano identificar conexiones entrantes o salientes que puedan ser de un origen o hacia un destino malicioso, identificar el puerto utilizado y protocolo en aras de poder hacer un reglado o restricción evitando que dicho tráfico siga pasando hacia el activo, esto último es más fácil de realizar si la red donde está

el activo o grupo de activos afectados están bajo la protección de un firewall o WAF (web Application firewall).

- Logs / eventos / registros: se puede revisar los logs, eventos o registros del activo afectado desde varias formas, la primera y principal es desde el mismo activo siempre y cuando se tengan dichos registros configurados en el sistema operativo, aplicación o servicio. Por defecto los sistemas operativos manejan ciertos registros que podrían dar una guía al momento de un ataque o incidente. otra opción para verificar eventos de un equipo afectado puede ser un IDS/IPS como Wazuh o similares capaz de recopilar y agrupar eventos de activos por medio de agentes instalados en cada activo a ser monitoreado, usando consultas y filtros se puede sacar los datos necesarios para identificar los posibles sucesos de un ataque. La última opción es un correlacionador de eventos o SIEM donde permite agrupar más fuentes de datos que solo un sistema operativo, por ejemplo, un SIEM está en condición de integrarse por medio de agentes a activos, IDS/IPS, servicios de monitoreo, servicios de protección, EDR, otros. Con esto un SIEM está en capacidad de no solo detectar las anomalías desde una fuente de origen, por medio de consultas y filtros puede trazar eventos desde varias fuentes de origen permitiendo hacer una trazabilidad mayor ante el hecho ocurrido, ejemplo: detección de paquetes legítimos desde el firewall, donde en la aplicación web hacen llamados a recursos muy grandes que consumen recursos de la aplicación, por lo tanto, genera una denegación de servicio.

- Nota: tener en cuenta que para el IDS/IPS y SIEM los activos o sistemas a ser monitoreados deben tener los registros de eventos o logs habilitados y con la mayor verbosidad posible para que dichos eventos sean capturados, de lo contrario las tecnologías no registraran los eventos suficientes y no será útil al momento de investigar o analizar un posible ataque.

2.4.3 Pregunta 2.

“¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team qué medidas de hardenización propondría para que el ataque no se repita?”

2.4.4 Respuesta a la pregunta 2.

inicialmente proponemos lo siguiente:

- Tener las actualizaciones de sistema habilitadas, verificar que esté funcionando dicho modulo y tener los sistemas / componentes actualizados en la última versión disponible (en algunos casos existen excepciones cuando hay sistemas legacy).

- Si no se puede tener el sistema 100% actualizado por casos como legacy o uso de software desactualizado sin soporte del fabricante, mantener el sistema con las últimas versiones y actualizaciones que estuvieron disponibles.

- Aplicar según la línea base o stig o benchmark controles relacionados con: cifrado, controles de red, auditoria y registro de eventos.

2.4.5 Pregunta 3.

"¿Describa con sus palabras las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos?"

2.4.6 Respuesta a la pregunta 3.

- Equipo Blue Team: el equipo Blue Team es el equipo encargado o equipo orientado a la defensa de una compañía u organización, este equipo está integrado por expertos en ciberseguridad con skills defensivos como análisis de malware, análisis de tráfico, detección de eventos maliciosos, auditoria, entre otros.

- El equipo de respuesta a incidentes como su nombre lo indica esta encargada de responder ante incidentes o amenazas que pongan en riesgo la ciberseguridad de la empresa, es un equipo multidisciplinario compuesto por expertos en ciberseguridad con skills defensivos como ingeniería / análisis forense, análisis de malware y otros.

- Como tal la diferencia es que el equipo de respuesta a incidentes únicamente está orientado a los incidentes de ciberseguridad, sin embargo, en un equipo Blue Team se puede derivar un equipo de respuesta a incidentes puesto que el Blue Team no solo tiene que ver con la detección o defensa de la compañía, sino responder y mitigar eventos maliciosos ante un incidente de ciberseguridad.

2.4.7 Pregunta 4.

"¿Si dentro de un equipo Blue Team le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?"

2.4.8 Respuesta a la pregunta 4.

Dentro de un equipo Blue Team se podrían utilizar los lineamientos de CIS para dos cosas:

- Implementación de los CIS controls: Los controles CIS son un grupo de acciones priorizadas que forman un conjunto de mejores prácticas de defensa para la mitigación de los ataques más comunes contra redes y sistemas. Son desarrollados por una comunidad de expertos en tecnologías de la información y las comunicaciones que aplican su experiencia en el desarrollo de estas prácticas de seguridad que son aceptadas globalmente.

- Los controles CIS comprenden un conjunto de 18 practicas (CIS controls 8) y 20 prácticas (CIS controls 7.1) o recomendaciones de defensa de la seguridad tecnológica que a su vez están conformados por subcontroles, los subcontroles se orientan hacia controles básicos, controles fundamentales y controles organizacionales. Una empresa que este implementando los controles por primera vez debe aplicar solo los fundamentales.

- Uso de CIS Benchmarks: los Benchmarks se complementan con los CIS controls ya que cada control de línea base este cruzado con un CIS controls, por ejemplo, en la línea base un control de cifrado este cruzado con el control fundamental número 3 del CIS controls. Los Benchmarks nos ayudan a definir líneas base de seguridad para los equipos, aplicaciones y servicios, estos se pueden obtener de forma gratuita desde https://downloads.cisecurity.org/#/, dentro de los Benchmarks podemos rescatar líneas base para sistemas operativos Windows, Linux, debian, Mac OSX, Android, iOS, entre otros. aplicaciones como apache, nginx, otros. Proveedores de nube como AWS, Azure y Google cloud platform. Motores de bases de datos como Oracle, postgre y SQL Server. Haciendo uso de herramientas como Nessus se puede ejecutar de forma rápida una verificación de línea base en un activo en aras de comprobar el estado de implementación del benchmark en el equipo objeto de las pruebas.

2.4.9 Pregunta 5.

“Explique y redacte las funciones y características principales de lo que es un SIEM”.

2.4.10 Respuesta a la pregunta 5.

Dentro de las funciones y opciones principales de un SIEM podemos resumir:

- Monitoreo Correlación de eventos: permite agrupar eventos desde varios orígenes de datos en aras de poder detectar de forma más rápida y detallada eventos maliciosos que pudieran ocurrir contra un activo.

- Creación de casos de uso, alertas personalizadas: por medio de filtros especiales o condicionales se pueden generar alertas o desencadenar

accionadores (triggers) que permitan reportar a un individuo o equipo sobre un evento malicioso para que puedan tomar acciones en una forma rápida.

- Monitoreo en tiempo real por medio de consultas, gráficos o estadísticas configurables donde permite al Blue Team tener una vista mejorada sobre el estado general de los equipos pertenecientes a la compañía.

2.4.11 Pregunta 6.

"Defina por lo menos 3 herramientas de contención de ataques informáticos hardware o software, recuerde que las herramientas de contención son diferentes a las herramientas de detección".

2.4.12 Respuesta a la pregunta 6.

- IDS/IPS: son herramientas que permiten prevenir o detectar posibles intrusos en un equipo o red objeto del ataque por medio de recolección de eventos y reglas realizadas a la medida por medio de los especialistas o reglas por defecto configuradas por el proveedor de seguridad, esto permite en tiempo real brindar la información necesaria al equipo de incidentes en aras de poder detener la amenaza.

- EDR: Un sistema EDR se caracteriza por poder agrupar varias tecnologías y elementos de detección como, por ejemplo, la inteligencia artificial y el Big Data, que permiten mejorar de forma programada y autónoma la detección y prevención de amenazas complejas, así como su posterior eliminación o mitigación. Aunque comparte cometidos con el antivirus tradicional, también conocido como EPP (EndPoint Protección Platform), como son la detección, identificación y la prevención de los efectos de malware, exploits, y en algunos casos, ransomware, esta herramienta además puede detectar amenazas avanzadas, como ingeniería social (phishing), APT, zero day, entre otros.

- Firewall/ WAF: son herramientas de monitoreo de tráfico donde permiten al Blueteam poder detener posibles ataques con tráfico malicioso por medio de reglados configurados manualmente por el equipo o por medio de set de reglas conocidos ampliamente como lo son shallalist, mod Security y otros. Adicional a detener el posible evento maliciosos permite evidenciar y almacenar dichos eventos asociados que se pueden integrar con otros sistemas como IDS/IPS, SIEM y otros.

- Por último, se brinda la ruta de acceso al video de sustentación del presente informe: Video seminario

3 CONCLUSIONES

Al ejecutar los sets de actividades del proyecto trazado para TheWhiteHouse security se concluye:

- Se logra realizar el banco de trabajo para que los aspirantes a cargos de red y Blue Team logren demostrar sus conocimientos a nivel practico.

- Por medio de la consultoría se logra identificar en los modelos de contrato y acuerdos de confidencialidad cláusulas que no estaban alineadas con la ley 1273 de 2009 y de no subsanarse hubieran llevado a castigos severos a nivel legal para la organización.

- Se realizaron labores de auditoria por medio de pruebas de penetración donde se logró comprobar una vulnerabilidad critica que aprovechaba un fallo del HFS para generar una Shell o consola de comando remota

- Se realizaron labores de consultoría para el equipo de Blue Team en aras de orientarlos al momento de resolver un incidente teniendo en cuenta posibles puntos de partida y algunas líneas base como CIS

4 RECOMENDACIONES

Teniendo en cuenta los hallazgos y resultados de las labores realizadas durante el proyecto se recomienda lo siguiente:

- Contar con un área o consultor que pueda brindar asesoría legal a la empresa relacionada con las normativas nacionales e internaciones de ciberseguridad en aras de proteger la empresa ante cualquier incumplimiento y garantizar a los clientes que los actos realizados durante los servicios prestados junto con su información estarán resguardados dentro del marco legal vigente según su ubicación.

- Realizar investigaciones de estados legales para los futuros aplicantes a puestos de trabajo, ejemplo: antecedentes de la policía nacional, antecedentes de procuraduría, fiscalía, entre otros.

- Tener las actualizaciones de sistema habilitadas, verificar que esté funcionando dicho modulo y tener los sistemas / componentes actualizados en la última versión disponible (en algunos casos existen excepciones cuando hay sistemas legacy)

- Si no se puede tener el sistema 100% actualizado por casos como legacy o uso de software desactualizado sin soporte del fabricante, mantener el sistema con las últimas versiones y actualizaciones que estuvieron disponibles

- Aplicar según la línea base o stig o benchmark controles relacionados con: cifrado, controles de red, auditoria y registro de eventos.

- Habilitar logs de sistema.

- Mantener al equipo de trabajo actualizado ante certificaciones, técnicas, herramientas y demás. Esto ayuda a mejorar las capacidades técnicas de los equipos.

BIBLIOGRAFÍA

Congreso de Colombia. Ley 1928 del 24 de julio de 2018. Colombia. [En línea]. Colombia. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

Congreso de Colombia. Ley 1273 del 5 de enero de 2009. Colombia. [En línea]. Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

Congreso de Colombia. Ley 1581 del 17 de octubre de 2012. Colombia. [En línea]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

Copnia. Código de Ética. 2015. Colombia. [En línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

PEÑARREDONDA, José Luis. Buggly, la comunidad en la que el Ejército camufló a sus hackers. [En línea]. Colombia. Febrero 5 de 2014. Disponible en: https://www.enter.co/empresas/seguridad/asi-es-la-presunta-fachada-de-la-central-de-hackeo-del-ejercito/

PEÑARREDONDA José Luis. Detrás de Buggly: la historia de la fachada Andrómeda. [En línea]. Colombia. Diciembre 9 de 2015. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Fuerzas Militares. El informe que sacudió el caso de la fachada Andrómeda. [En línea]. Colombia. Enero 24 de 2015. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution. [En línea]. Disponible en: https://www.infosecmatter.com/nessus-plugin-library/?id=53514.

MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution – Metasploit. [En línea]. Disponible en: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/smb/ms17_010_psexec

Attacker KB. MS17-010 CVE-2011-0657. [En línea]. Julio 30 de 2020. Disponible en: https://attackerkb.com/topics/vztYSKY5LX/cve-2011-0657/vuln-details

Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553). [En línea]. Abril 13 de 2011. Disponible en: https://www.rapid7.com/db/vulnerabilities/WINDOWS-HOTFIX-MS11-030/

MS11-030: Rejetto HttpFileServer Remote Command Execution – Metasploit. [En línea]. Disponible en: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/http/rejetto_hfs_exec

OWASP Equipo de respuesta a incidentes. [En línea]. Disponible en: https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf

CIS Benchmarks. Operating Systems. [En línea]. Disponible en: https://downloads.cisecurity.org/#/

CIS, The 18 CIS Critical Security Controls. [En línea]. Disponible en: (https://www.cisecurity.org/controls/cis-controls-list)

Security Information and Event Management (SIEM). [En línea]. USA. Disponible en: https://logrhythm.com/solutions/security/siem/

Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa. [En línea]. Abril 27 de 2021. España. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa

8 Use ModSecurity Web Application Firewall to Mitigate OWASP's Top 10 Web Application Vulnerabilities. [En línea]. Agosto 15 de 2021. Disponible en: https://eds-s-ebscohost-com.bibliotecavirtual.unad.edu.co/eds/detail/detail?vid=0&sid=100c1589-d175-451f-8cb3-0b13eb77e85c%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZSZzY29wZT1zaXRl

RIASCOS GÓMEZ Libardo Orlando. Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009. [En línea]. Julio 12 de 2012. Colombia. Disponible en: https://vlex.com.co/vid/delitos-datos-personales-habeas-737885729