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

AUTOR

VILOMAR ENRIQUE CASTRO DE AVILA

DIRECTOR DE CURSO

INGENIERO JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS
ESPECIALIZACION EN SEGURIDAD DE LA INFORMACION
BOGOTÁ
2021

Bogotá, 4 de abril de 2021

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

RESUMEN

Gracias a la realización del presente informe, se busca dar a conocer la importancia del rol desempeñado por los equipos de Blue Team & Red Team, para la compañía WhiteHouse Security, logrando soportar la toma de decisiones fundamentadas tanto en los aspectos éticos como legales y técnicos, a los cuales se hace referencia en el presente de manera detallada.

Para dicho informe, se tomó como insumo principal el incidente de seguridad presentado al interior de la organización, con la finalidad de analizar una vulnerabilidad hallada y explotada, lo que permitió el escalamiento de privilegios al sistema comprometido y la identificación de la posible exfiltración de datos de la organización por parte del atacante.

Mediante la implementación de bancos de prueba, se logró evidenciar el vector de ataque empleado para explotar la vulnerabilidad rejetto en su versión 2.3, tomando como insumo las imágenes del servidor suministrada por el equipo de forense y que es objeto de estudio en la auditoria desarrollada.

Por lo anterior, la compañía WhiteHouse Security, vio la necesidad de emplear mediante el apoyo de su equipo de Blue Team, medidas o mecanismos de contención ante futuros eventos que puedan comprometer la continuidad de sus operaciones y así mitigar el grado de exposición ante futuros incidentes que lograsen comprometer la integridad, disponibilidad y confiabilidad de su infraestructura IT.

Como resultado final, se plantean unas recomendaciones éticas, legales y técnicas, mismas que representarán el insumo a considerar por parte de la compañía WhiteHouse Security, en especial por el área de Seguridad Informática, con el único fin de contribuir a robustecer sus procesos internos al igual que la infraestructura IT, en consonancia con el objetivo previsto con la auditoria.

GLOSARIO

- Ataque Informático: Acto o acción mediante el cual se busca comprometer un sistema informático.

- Armitage: Herramienta empleada con el fin de efectuar pruebas de vulnerabilidad a sistemas de información.

- Blue Team: Profesionales en el campo de la ciberseguridad encargados de la identificación, rastreo y modelado de las posibles amenazas que puedan llegar a impactar a una organización.

- Cross Site Scripting (XSS): Tecnica de ataque mediante el cual el atacante inserta códigos en sitios HTML.

- CSIRT: Equipos de respuesta a incidentes informáticos

- Escalación de Privilegios: Procedimiento mediante el cual el atacante de un sistema informático se asigna privilegios de administrador en el sistema previamente comprometido.

- Exfiltración: Es la acción mediante la cual el atacante extrae información del sistema vulnerado para su propio beneficio.

- Exploit: Programa o software mediante el cual se busca explotar una vulnerabilidad hallada en un sistema informático.

- Firewall: Sistema (Software o Hardware) que nos ayuda a prevenir y proteger mediante la configuración de reglas de acceso contra agentes no autorizados.

- Fail2ban: Aplicación escrita en el lenguaje de programación Python la cual se emplea con la finalidad de prevenir las eventuales intrusiones a un sistema.

- IDS: Sistema de detección de intrusos.

- IPS: Sistema de prevención de intrusos.

- Metasploit FrameWork: Herramienta Open Source la cual nos proporciona información de vulnerabilidades de seguridad para su posterior explotación a través de sus diferentes módulos.

- Meterpreter: Es la sesión creada producto de un ataque exitosos a un sistema informático a raíz de una vulnerabilidad previamente hallada.

- Nessus: Software Open Source empleado para realizar escaneos de posibles vulnerabilidades en una infraestructura IT.

- Nmap: Software Open Source para realizar escaneos y enumeración de puertos y servicios de un sistema de información.

- Open Source: Herramientas de fuentes abiertas o uso libre.

- Payload: Es la carga útil o datos transmitidos por un exploit al lanzar un ataque contra un sistema de información.

- Pentesting: Pruebas de penetración realizada a redes o sistemas de información de una organización.

- Pivoting: Capacidad de pasar del sistema in formatico inicialmente comprometido a otro.

- Red Team: Profesionales del campo de la Ciberseguridad, quienes mediante técnicas de seguridad ofensivas contribuyen con el fortalecimiento de la seguridad en una organización.

- Shell: Es el intérprete de ordenes o comandos por medio del cual interactúa un usuario con un sistema de información.

- Snort: Es una herramienta Open Source la cual dentro de su característica más familiar resalta su aplicación como un sistema de prevención de intrusiones (IPS).

- Security Onion 2: Se le conoce como una distribución Open Source de Linux, posee entre sus funcionalidades o características a resaltar el monitoreo de seguridad para redes empresariales, gestión de logs y threat hunting.

- Vulnerabilidad: Debilidad existente en un sistema de información.

- Vector de Ataque: Método que utiliza un atacante en busca de vulnerar un sistema.

- WAF: Firewall para la protección del tráfico web en una organización.

- Whazu: Es una herramienta Open Source dotada de varias funcionalidades con el único fin de contribuir a la contención de posibles ataques informáticos.

INTRODUCCIÓN

Debido al incremento de las nuevas tecnologías emergentes, en especial en lo que concierne a las tecnologías de la información y para nuestro caso, al estudio del sector de la ciberseguridad, surge la necesidad de realizar la presente auditoria, la cual tiene como objetivo principal, estudiar la vulnerabilidad rejetto v 2.3, así podemos generar las recomendaciones y conclusiones, que serán el insumo para suministrar al área de Seguridad Informática de la compañía WhiteHouse Security.

Por lo anterior, partiendo de la necesidad de apoyar con las diferentes vertientes especializadas la resolución de este tipo de incidentes, como lo son los equipos de Blue Team y Red Team, se propone el empleo de técnicas y herramientas para el ataque y contención, contribuyentes con la mitigación de posibles amenazas que busquen entorpecer la continuidad del negocio de una organización.

Como resultado final de la auditoria desarrollada, se dotará a la compañía WhiteHouse Security, de las herramientas y mecanismos vitales para la estructuración, generación y socialización entre sus colaboradores, de las políticas informáticas que contribuyen con el fortalecimiento y disponibilidad tanto de su infraestructura IT como del activo más valioso para una organización, como lo es la información.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Estructurar un informe técnico, argumentando las capacidades técnicas, legales y de gestión, referentes a un equipo Blue Team & Red Team, el cual oriente los procedimientos y mecanismos a implementar por el equipo de expertos de la empresa WhiteHouse Security.

1.2. OBJETIVOS ESPECÍFICOS

- Documentar los diferentes procedimientos legales y técnicos contemplados para cada una de las fases del seminario especializado para equipos estratégicos en ciberseguridad, Red Team & Blue Team.

- Recomendar posibles estrategias y mecanismos a implementar por un equipo de Red Team & Blue Team, con el fin de mitigar el grado de exposición ante un eventual incidente informático.

- Apoyar la apropiación de conocimiento a través de las experiencias contenidas en las conclusiones de este informe, de mecanismos, procedimientos y contramedidas informáticas que apoyen a la compañía WhiteHouse Security en la conservación de la integridad de su infraestructura IT.

- Mitigar el grado de exposición hacia las amenazas informáticas, de las cuales son víctimas las redes en la actualidad, esto garantizando así la continuidad misional del negocio en una organización empresarial.

2. INFORME DE CAPACIDADES LEGALES

2.1. CASO DE ESTUDIO ACTUACIÓN ÉTICA Y LEGAL.

Mediante el presente informe ético y legal, se pretende resaltar en el hecho, mediante el cual la compañía WhiteHouse Security, en su actuar legal no ofrece las garantías mínimas con las que debiese contar para el cumplimiento de sus procesos internos de contratación. Lo anterior fundamentado, en la carencia del recurso humano propio para el desempeño de esta función, lo cual deriva en la asignación de estas responsabilidades a colaboradores (abogado), el cual en aras de su ética profesional y en cumplimiento de sus funciones, dieron a conocer los malos procedimientos operacionales que realizaba la compañía en algunas tareas propias de su Core bussines, esto amparado en lo dispuesto por la ley colombiana, la cual busca identificar la existencia de irregularidades en los procesos que pudiesen ir en contravención con las diferentes legislaciones colombianas, creadas para regular tales conductas.

Adicional a lo antes en mención, se resalta el hecho en el cual, pese a que pueda llegar a ser habitual de que las empresas formulen desafíos para los aspirantes a procesos tan complejos, como lo es para nuestro caso el de la selección de personal para integrar equipos Red Team & Blue Team, mediante los cuales los aspirantes logren explotar todas sus capacidades técnicas para la resolución de estos. Es de conocimiento que, en estos desafíos, el candidato es libre de emplear las herramientas y procedimientos técnicos que considere para lograr enfrentar y resolver tales desafíos.

A raíz de lo antes expuesto, se resalta con preocupación el hecho, en el cual la empresa para este tipo de procesos o desafíos, no delimite un alcance técnico claro para la resolución de esta actividad, lo anterior aumentando el grado de exposición a posibles persistencias o backdoor`s que los candidatos pudiesen crear y ocultar ante los ojos de la compañía y así poder lograr accesos indebidos a la red y usuarios de la misma, pudiendo exfiltrar datos como usuarios o credenciales para fines netamente personales.

Lo antes en mención, se enmarca en el hecho en el cual se ejecutan estos desafíos bajo el segmento de red operacional de la compañía puesto que pese a requerir la implementación de máquinas virtuales como entornos de futuras pruebas, en ninguna instancia se especifica que se apliquen estas condiciones al escenario de desafío actual.

En aras de dar evidencia de las anomalías puestas en conocimiento en el presente informe, a continuación, listamos los apartes del documento en el cual se denotan tales contravenciones, así:

- Este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos.

- La alta gerencia no revisó los contratos con los que se reclutó al nuevo personal, por ende, los contratos fueron entregados sin modificación alguna.

- Ante el evento anterior, la gerencia solicitó tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal.

- Como prueba de admisión al equipo Red Team & Blue Team, se decidió clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión, “característica” de estos equipos.

2.2. **ACUERDO DE CONFIDENCIALIDAD ENTRE LAS PARTES.**

Del acuerdo propuesto por la compañía WhiteHouse Security, se logra evidenciar que este, aduce su enmarcación y alineación con las legislaciones vigentes para el Estado colombiano, en sus apartes correspondientes al generador de este, el uso de procedimientos ilegítimos que al no están reglamentados por el Estado colombiano, atentan y/o vulneran los derechos a la debida reserva de los datos de sus ciudadanos. Lo anterior se manifiesta al momento de que la compañía WhiteHouse Security imparte un ítem exigido a sus aspirantes respecto a la confidencialidad y total reserva para la divulgación de la información ya sea parcial o total, indistintamente de los procesos o mecanismos ilícitos que se pudiesen emplear para el levantamiento de la información, lo que se traduce como conductas tipificadas al margen de la ley colombiana.

Por otra parte, y no menos importante, WhiteHouse Security, mediante la firma de este acuerdo entre las partes, obliga al aspirante del equipo de Red Team & Blue Team a salvaguardar y no divulgar la información en su poder, incluso de ser requerida por organismos del Estado para los fines que este, en ejercicio de sus funciones, lo llegasen a requerir, así esto pudiese interpretarse como un caso de obstaculización de la Ley Nacional Colombiana.

La compañía WhiteHouse Security, bajo la premisa de confidencialidad de la información exigida a los aspirantes de los Equipos Red Team & Blue Team, manifiesta que, pese a que los aspirantes llegasen a detectar malos procedimientos, tales como las interceptaciones de comunicaciones ilegales, intrusiones a sistemas informáticos e incluso exfiltración de datos personales, que bajo ninguna instancia podrán comunicarse a las autoridades, así estas lo llegasen a requerir.

Lo anterior, bajo el entendido de que la información obtenida mediante estos procedimientos atenta contra la entidad, imagen y buen nombre de los ciudadanos

colombianos propietarios de estos datos, quienes podrían verse perjudicados por con el mal uso de estos.

Dentro de las obligaciones que adquieren los receptores de la información con la compañía WhiteHouse Security, se destaca con suma preocupación el hecho de que pese a evidenciarse las actividades ilícitas bajo la dinámica de la operación propiamente dicha, bajo ninguna circunstancia podrán estos, bajo el ejercicios de su deber ciudadano, informar a las autoridades competentes de este tipo de entro de conductas, evitándoles convertirse en cómplices de los delitos cometidos mediante estas malas prácticas dentro del campo de la Ciberseguridad.

Dentro de sus apartes de confidencialidad, WhiteHouse Security, se hace responsable de la información que puede llegar a tener la connotación de ilegal debido a los mecanismos empleados para su obtención y del impacto legal que esta pudiese generar sobre los propietarios, como únicos poseedores o receptores de la información, quienes al momento de llegar a ser requeridos por las autoridades y de tener bajo su custodia, no podrán divulgar el autor material o generador de esta información, que en cuyo caso sería la compañía WhiteHouse Security.

Como punto a resaltar en el presente análisis, se encuentra el hecho de que, al llegar a existir el incumplimiento por parte del acuerdo de confidencialidad, como bien se resaltó anteriormente, la parte que incumpla deberá asumir las consecuencias del incumplimiento u afectación generada a las partes involucradas.

De los mecanismos de resolución de conflictos entre las partes, se puede inferir que al estar expuestos a procesos contemplados por la ley como ilícitos, WhiteHouse Security acude en su interés a la resolución de conflicto por vías no tradicionales, esto pudiendo perjudicar la debida defensa de su contraparte, para este caso el aspirante al equipo de Red Team & Blue Team, quien hace las veces de receptor de la información.

Para finalizar, es de vital importancia anotar que resulta complejo el hecho de que la compañía WitheHouse Security, deje desprotegido jurídicamente al aspirante del equipo de Red Team & Blue Team, quien hace las veces de receptor de la información y que en pleno ejercicio de sus funciones contractuales, maneja información propiedad de la compañía que sabemos puede ser de carácter ilícito, desligándole en su defensa jurídica, de toda relación con la compañía y restándole responsabilidad a esta como propietaria de la información.

Por lo anterior, se relacionan a continuación los puntos del acuerdo en los cuales se exponen las anomalías en mención, así:

- En virtud del presente acuerdo de confidencialidad, la parte receptora, 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.

- 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”.

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

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

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

- La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security.

- La parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

- 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.

3. ARTÍCULOS DE LA LEY 1273 DE 2009 VULNERADOS EN EL ANEXO 3-ACUERDO DE CONFIDENCIALIDAD

En el presente acuerdo se puede evidenciar que se vulneran derechos de los ciudadanos colombianos, contemplados en la Ley 1273 de 2009, en relación con lo antes mencionado y por lo que se procederá a realizar el análisis específico de

acuerdo con los diferentes artículos vulnerados en el presente acuerdo, así:

- “ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO”. Se observa que la compañía WhiteHouse Security, en consecuencia, con los procedimientos arbitrarios estipulados en su acuerdo para la obtención de datos, incurre en técnicas de intrusión y exfiltración de información de sistemas informáticos, objetivo de su operación, sin previa autorización o consentimiento de los propietarios de estos datos.

- “ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS”. Es vulnerado este artículo por parte de la compañía antes mencionada, al momento en que está, en uso de su operación, realiza interceptaciones de información (chuzadas) en aras de obtener datos de los diferentes objetivos priorizados para su operación o continuidad del negocio. Lo anterior puesto en manifiesto en el acuerdo de confidencialidad propuesto por esta.

- “ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES”. Como se manifiesta en el acuerdo de confidencialidad y en relación con este, la compañía WhiteHouse Security al momento de realizar actividades de extracción, recopilación y comercialización de datos de terceros, producto o no de su operación y sin contar con la previa autorizado por parte de los propietarios de estos datos, incurre en una violación del artículo en mención.

- “ARTÍCULO 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS”. Se puede aducir que la compañía WhiteHouse Security, con objeto del ejercicio de la obtención de la información vulnera el artículo citado. Lo anterior se refleja al momento de transferir información, como podrían ser patentes de terceros para fines propiamente lucrativos o estratégicos.

  Cabe resaltar que en este análisis de las conductas consideradas como ilícitas dentro de este acuerdo, solo se asocian en este aparte las tipificadas dentro del marco regulatorio de la Ley 1273 de 2009. Pese a ello, se observan otras conductas consideradas antiéticas e ilícitas las cuales no se cubren en este punto debido a no ser válidos para este estudio.[1]

[1] CONGRESO DE COLOMBIA. Ministerio del Interior y de Justicia. Ley N°1273. 5 de enero de 2009. Bogotá. 2009.

4. INFORME DE CAPACIDADES TÉCNICAS Y DE GESTIÓN

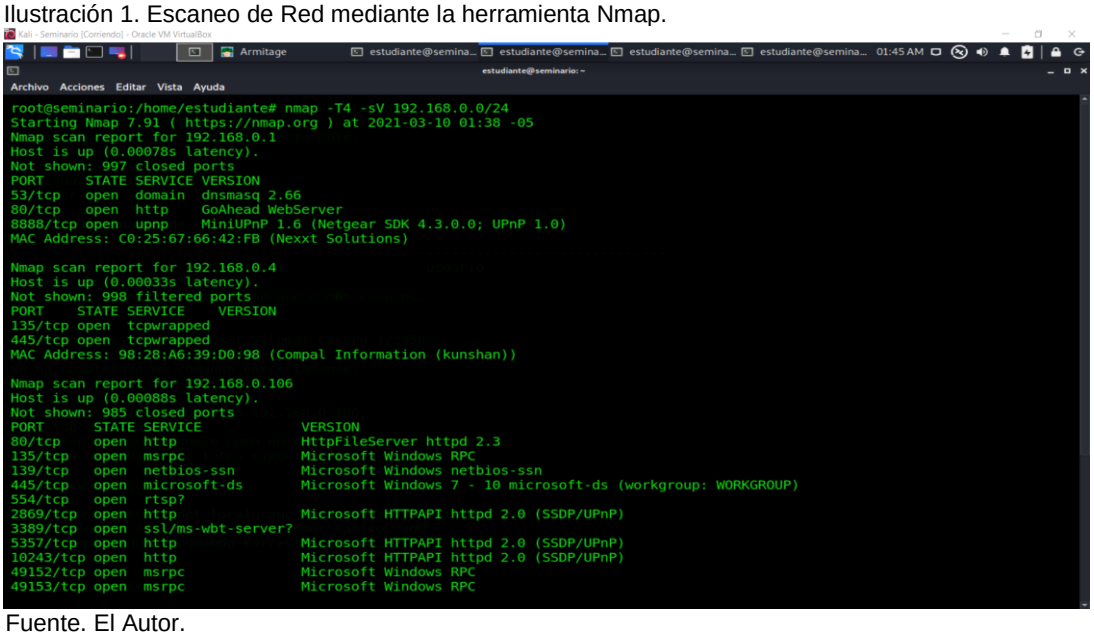
4.1. CASO DE ESTUDIO CAPACIDADES TÉCNICAS Y DE GESTIÓN.

4.1.1. FASE DE ESCANEO Y ENUMERACIÓN. Como una de las fases más relevantes y de suma importancia, es la etapa de recolección de la información o como se le conoce en el idioma inglés, Information Gathering. En esta fase el personal del equipo de Red Team o personal a cargo del Pentesting, hace uso de un pool de herramientas las cuales le permitirán hacer un mapeo o reconocimiento de cada uno de los dispositivos activos que integran la red, al igual de las posibles brechas o vulnerabilidades informáticas que pueden llegar a comprometer a cualquiera de estos dispositivos.

A continuación, procederos a describir cada una de las herramientas empleadas en esta fase, esto con el enfoque de la misión asignada a nuestro equipo de Red Team.

- Nmap. Se empleo esta herramienta con la finalidad de realizar un escaneo al segmento de red de nuestro interés, así como la enumeración tanto de sus puertos como de los servicios que se encuentran configurados para cada uno de estos puertos, como se evidencia en la imagen relacionada a continuación.

Ilustración 1. Escaneo de Red mediante la herramienta Nmap.



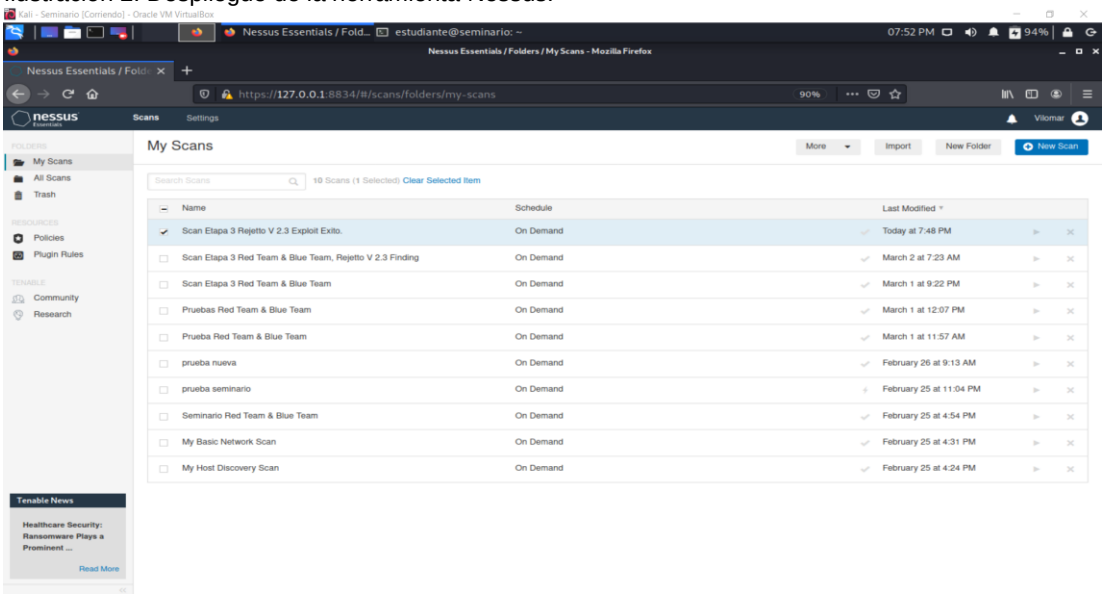
Fuente. El Autor.

Como se evidencia en la imagen anterior, se empleó la herramienta nmap para escanear el segmento de red de nuestro interés, lo anterior mediante el uso de sentencias de comandos, para nuestro caso empleamos el comando nmap -T4 -sV 192.168.0.0/24, en el cual con -T4 se establece un tiempo para

el témplate más alto, -sV con el fin de probar los puertos abiertos y validar los servicios configurados para cada uno de ellos y finalmente asignamos el segmento de red sobre el cual realizaremos el escaneo.

- Nessus. Con el conocimiento previo que adquirimos mediante el empleo de la herramienta anterior, se procede a hacer uso de la herramienta Nessus Essentials, la cual es su versión Open Source, esto con la finalidad de realizar un escaneo a nivel de vulnerabilidades y así identificar la de interés para cada uno de los hosts que integran nuestro segmento de red a auditar. Para lo cual relacionamos la imagen a continuación en la cual se evidencia el uso y correcto despliegue de la herramienta Nessus.

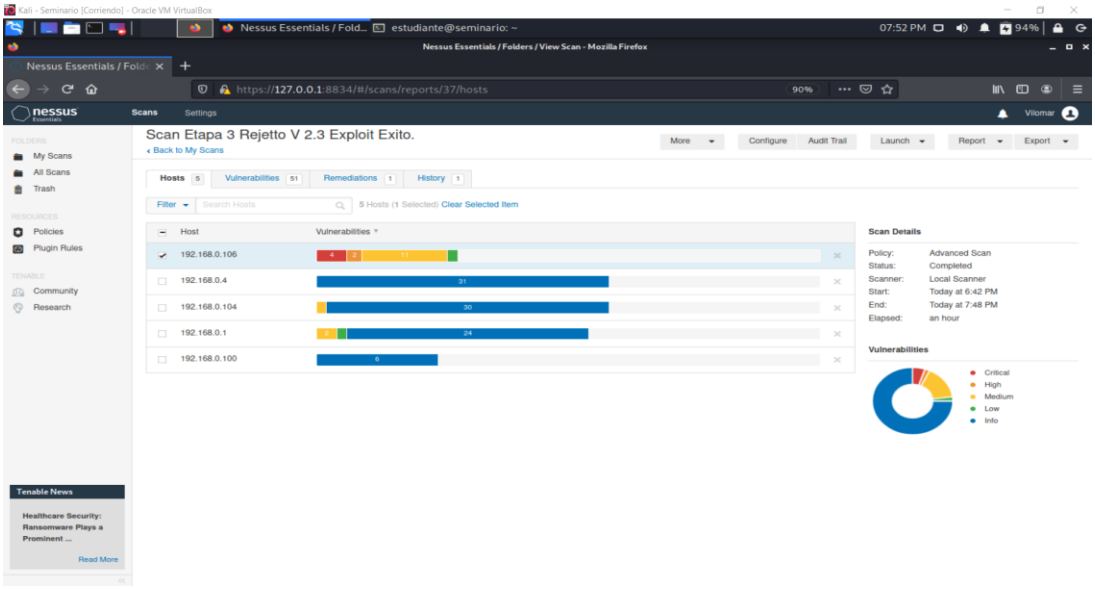
Ilustración 2. Despliegue de la herramienta Nessus.



Fuente. El Autor.

Como se valida en la imagen previa, se configura y lanza el Scan a nuestro segmento de red, esto con la finalidad principal de hallar posibles brechas y vulnerabilidades presentes en los dispositivos que la integran.

Ilustración 3.Resultado Escaneo de Vulnerabilidades con la herramienta Nessus.

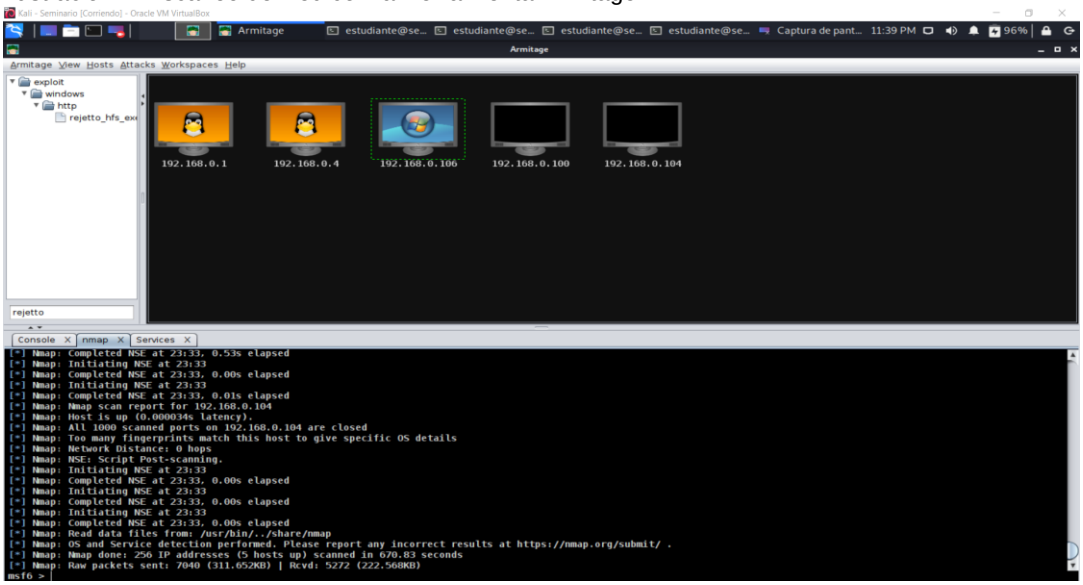


Fuente. El Autor.

De la imagen anterior podemos resaltar como aspecto relevante las diferentes alertas y vulnerabilidades presentes para cada uno de los hosts de la red, sin embargo, reclama relevancia el equipo de cómputo de nuestro interés el cual se identifica mediante la dirección IP **192.168.0.106**, en el cual nos centraremos a lo largo del desarrollo del presente informe.

- Armitage. Es otra herramienta de la cual nos apoyamos como equipo de Red Team, para nuestro caso, la etapa de reconocimiento en su fase para el escaneo de los servicios y puertos del equipo objeto de esta auditoría, como se evidencia en la siguiente imagen.

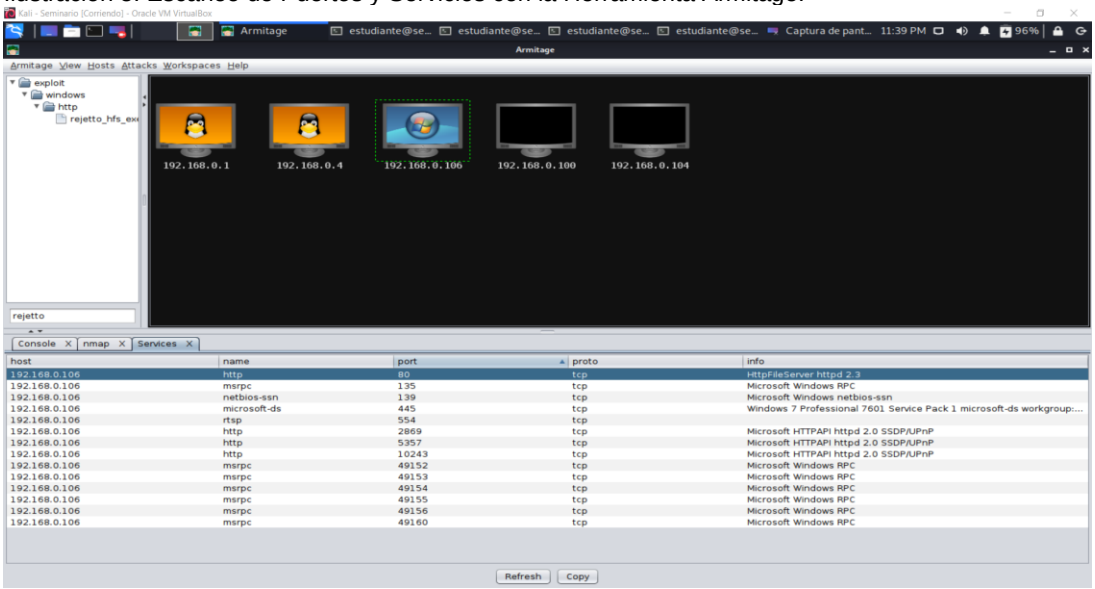
Ilustración 4. Escaneo de Red con la Herramienta Armitage.



Fuente. El Autor.

Del escaneo anterior se puede resaltar el uso de nmap como repositorio de la aplicación Armitage, por lo cual el resultado de este es el mismo que obtenemos a través de la herramienta propia Nmap.

Ilustración 5. Escaneo de Puertos y Servicios con la Herramienta Armitage.



Fuente. El Autor.

Una vez identificado nuestra maquina objetivo y realizados los escaneos antes en mención, procedemos a listar los puertos y servicios que se ejecutan en el equipo, de lo cual se resalta el Puerto 80, en el cual se ejecuta un servicio HttpFileServer httpd 2.3, el cual analizaremos en futuros apartes de este informe.

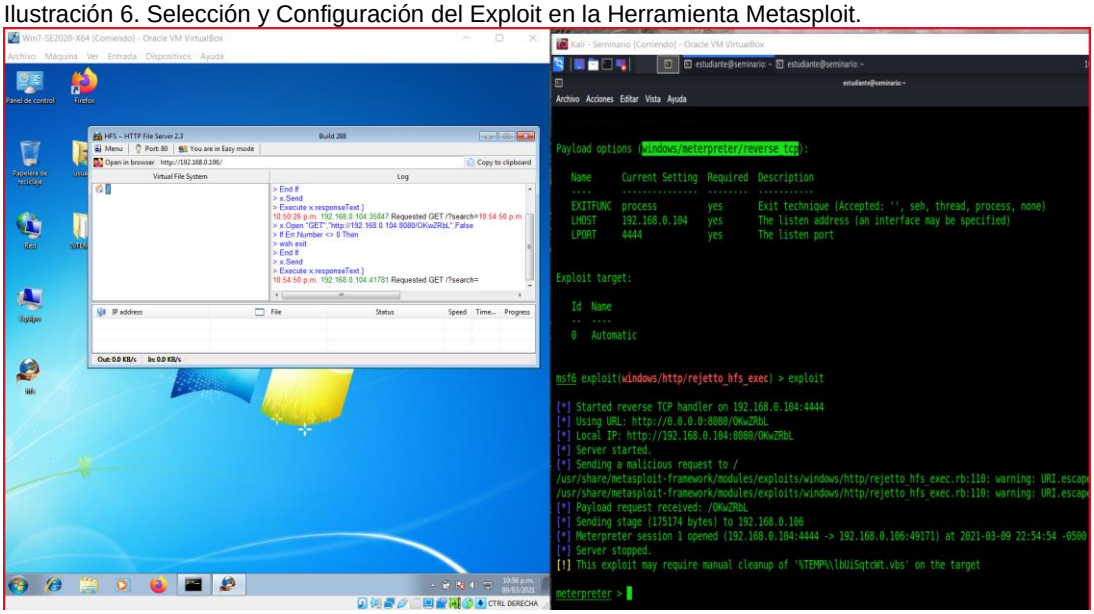
4.1.2. FASE DE EXPLOTACIÓN O HACKING. Entiéndase como la fase en la cual nuestro equipo de Red Team, una vez identificada la vulnerabilidad a explotar y con la previa selección de las herramientas automáticas o manuales, sean estas Open Source o de pago, se realizarán los ataques necesarios con el único objeto de lograr comprometer el sistema de interés. No sin antes enfatizar que el éxito de esta fase depende de los resultados obtenidos en la fase anterior y así poder garantizar el éxito de nuestro vector de ataque.

Como herramientas a empleadas por parte de nuestro equipo de Red Team para el éxito de esta auditoría, se mencionan las siguientes:

- Metasploit. Entiéndase este como un FrameWork, o conjunto de herramientas para realizar ataques informáticos, esto mediante la ejecución de exploits, con el fin de lograr la explotación de un sistema informático objetivo.

  Para nuestro caso una vez conocido nuestro vector de ataque, se procede a seleccionar el exploit apropiado para la explotación de la vulnerabilidad previamente hallada, por lo anterior a continuación se relaciona imagen en la cual se detalla tal procedimiento.

Ilustración 6. Selección y Configuración del Exploit en la Herramienta Metasploit.



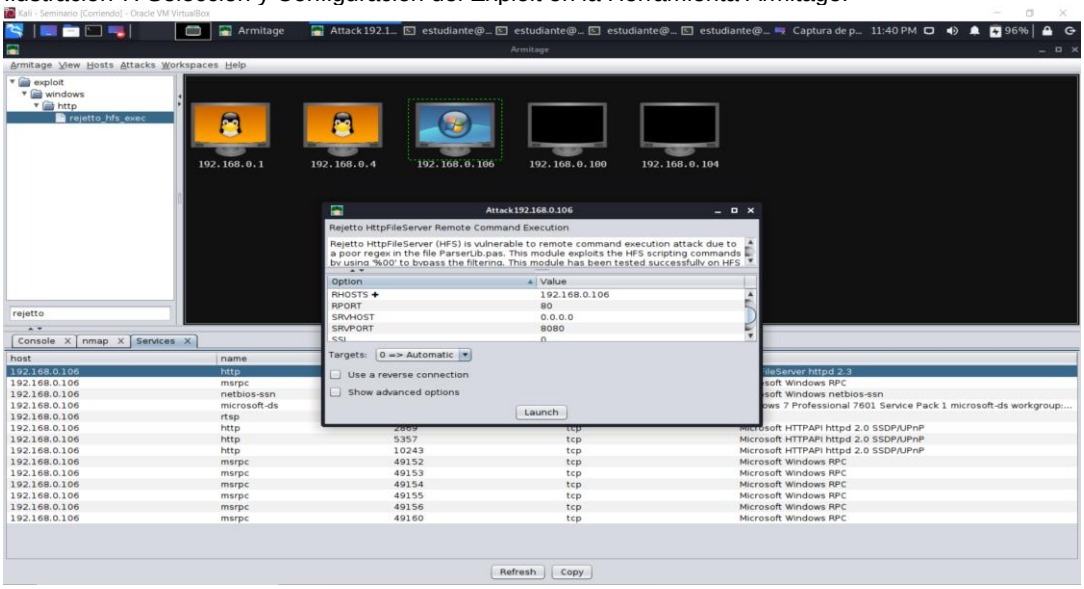
Fuente. El Autor.

En la imagen anterior se procede a efectuar la selección y configuración del exploit correspondiente a la vulnerabilidad hallada para la maquina víctima, el cual es **windows/http/rejetto_hfs_exec,** el cual afecta el servidor HTTP previamente instalado en nuestra maquina comprometida en la PoC, para el éxito de nuestro exploit se deben listar las opciones requeridas a configurar

por este mediante el comando show options y así procedemos a configurar el RHOSTS y la Payload a cargar, en nuestro caso sería **windows/meterpreter/reverse_tcp**. De ser exitoso nuestro exploit, obtendremos como resultado se obtiene un Meterpreter.

- Armitage. Como se mencionó en la fase de reconocimiento de este informe, Armitage cuenta a su vez con la base de datos de Metasploit, contenidos esta herramienta con interfaz gráfica. Esta nos permite lanzar el ataque a nuestro sistema objetivo de manera automática, como se evidencia en la siguiente imagen.

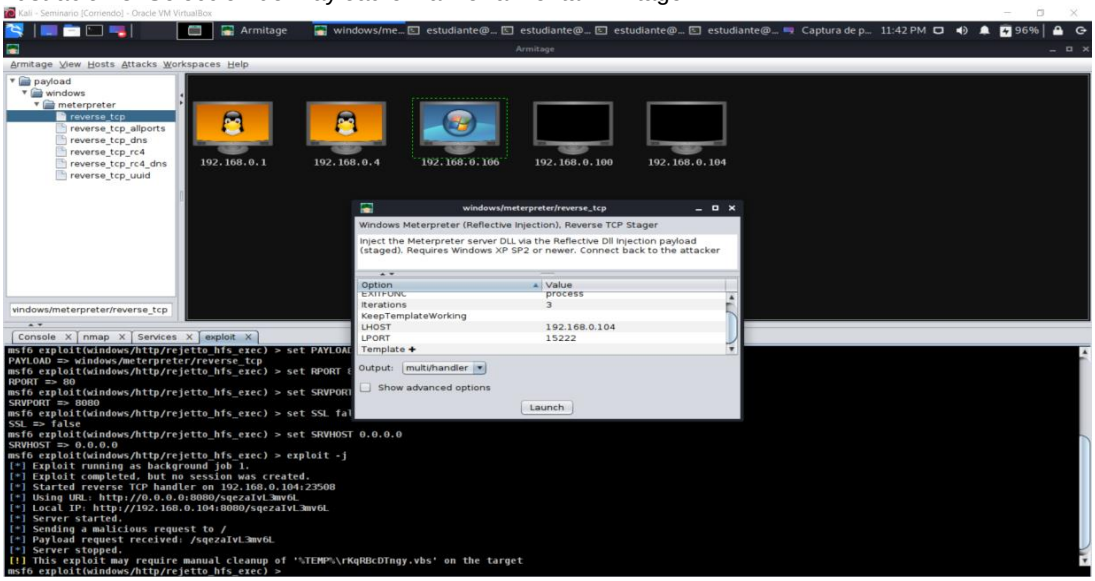
Ilustración 7. Selección y Configuración del Exploit en la Herramienta Armitage.



Fuente. El Autor.

En esta imagen se selecciona el exploit a emplear para nuestro ataque, el cual es rejetto_hfs_exec, visualizado en la columna izquierda de la imagen.

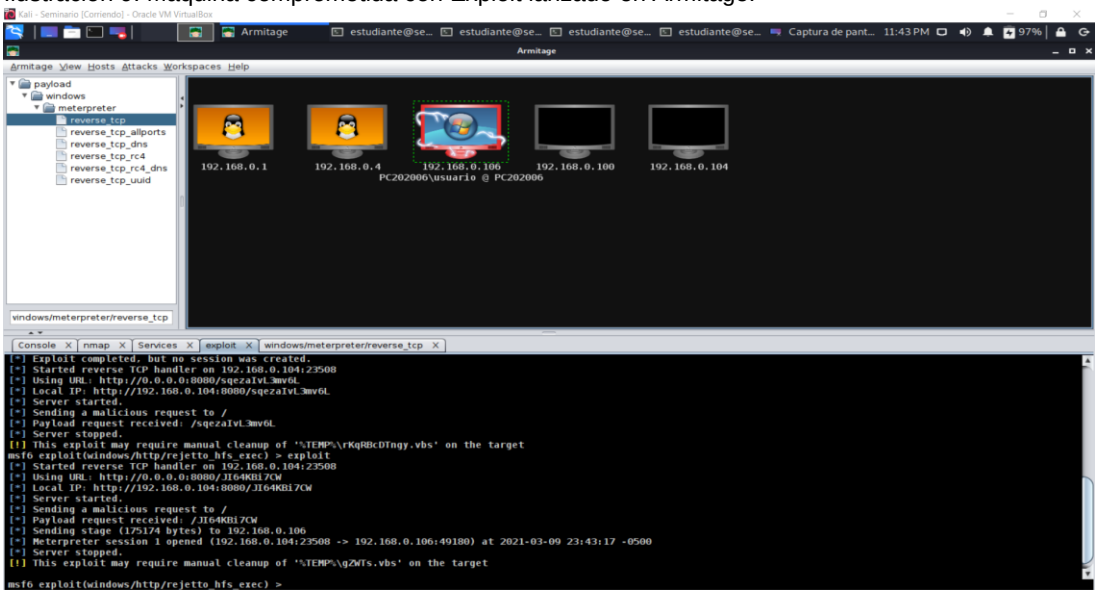
Ilustración 8. Selección del Payload en la Herramienta Armitage.



Fuente. El Autor.

En esta imagen se da a conocer el proceso a realizar para la selección del Payload a lanzar junto al exploit seleccionado, lo cual se evidencia en la columna ubicada a la izquierda de esta imagen.

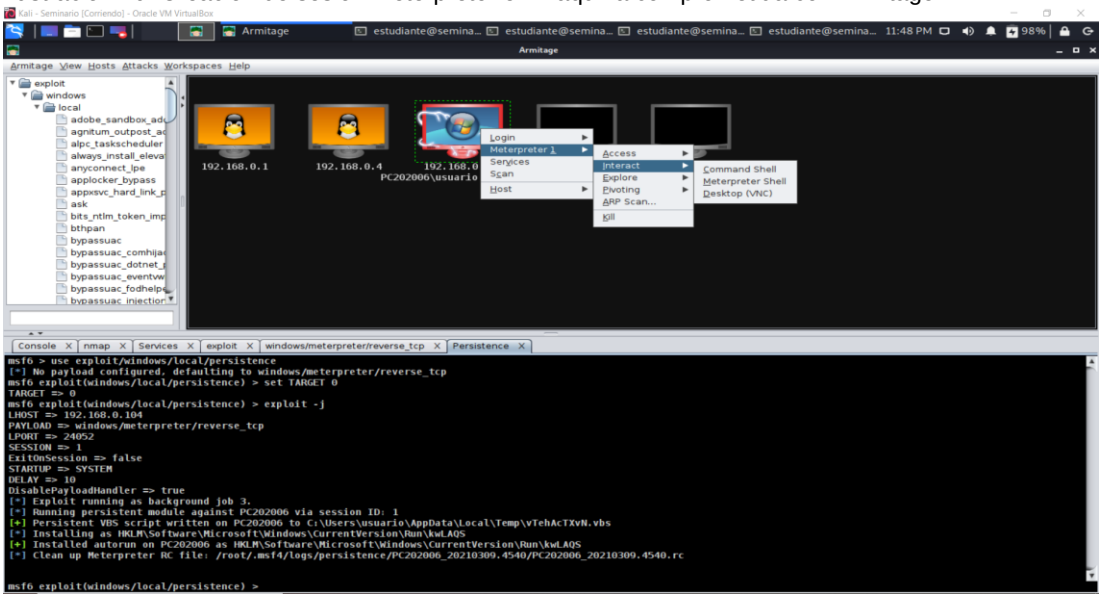
Ilustración 9. Maquina comprometida con Exploit lanzado en Armitage.



Fuente. El Autor.

Como podemos observar en la imagen anterior, al momento de lanzar el exploit mediante el uso de la herramienta Armitage, la maquina objeto de estas pruebas, adquiere un color rojo, lo cual indica que fue comprometida mediante la vulnerabilidad previamente hallada.

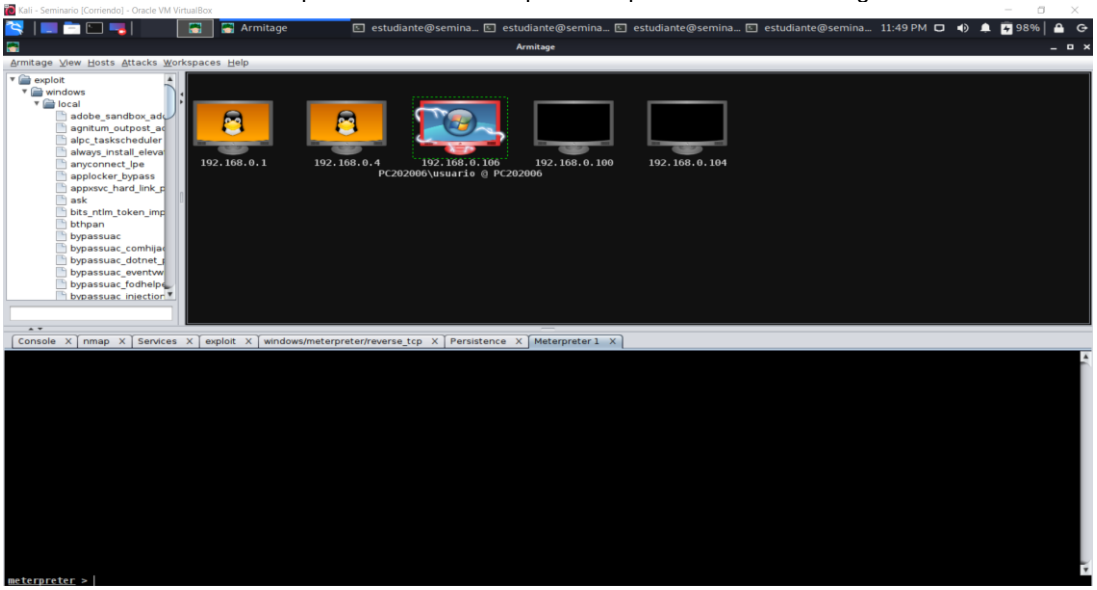
Ilustración 10. Creación de sesión Meterpreter en Maquina comprometida con Armitage.



Fuente. El Autor.

Por último, en la siguiente imagen se da conocer la sesión de meterpreter creada a través de nuestra herramienta Armitage.

Ilustración 11. Sesión Meterpreter creada en Maquina comprometida con Armitage.



Fuente. El Autor.

5. INFORME CON EL ANÁLISIS DEL CASO RED TEAM - ANEXO 4.

Tomando como insumo del presente análisis de Red Team, la información suministrada por el documento Anexo 4 -escenario 3, resaltamos aspectos los cuales nos facilitaron la identificación de la vulnerabilidad asociada al sistema

objetivo, adicional a las implicaciones técnicas generadas por la misma. Por lo anterior se describen los diferentes aspectos relevantes, los cuales fueron apoyo indispensable para la realización de nuestras pruebas, así:

5.1.1. EQUIPOS DE COMPUTO COMPROMETIDOS. En el anexo se especifica la cantidad de equipos de cómputo afectados por la vulnerabilidad, lo cual es solo un equipo, por lo anterior y una vez confrontada esta información con los datos obtenidos en nuestra fase de reconocimiento y enumeración, mediante el escaneo realizado a través de Nmap, Nessus y Armitage, se logró acortar la brecha informática a un solo equipo de cómputo, lo cual corrobora lo informado a través del anexo en cuestión.

5.1.2. APLICACIÓN INSTALADA EN LA MAQUINA OBJETIVO. El anexo nos pone en conocimiento de una aplicación instalada en la maquina a auditar, la cual es rejetto v.2.3.

Por lo anterior en nuestra fase de recolección de información, se estudió la funcionalidad de la aplicación en cuestión, esto en aras de conocer su operación y así delimitar nuestro futuro vector de ataque, en nuestra fase de explotación.

5.1.3. SISTEMA OPERATIVO BAJO EL CUAL SE ALOJA LA APLICACIÓN. Gracias a la información contenida en el anexo 4, se conoce que la aplicación a analizar funciona bajo un sistema operativo de Windows y con una arquitectura X64, esto facilitándonos la selección de nuestro exploit, ya que conocemos el sistema operativo bajo el cual se ejecuta el servicio.

5.1.4. ASPECTOS RELEVANTES ASOCIADOS A ESTA APLICACIÓN. Se nos informa en el anexo 4, que la aplicación rejetto v. 2.3, tiene asociado un exploit, quien podría generar una Shell y como producto final llegar a lograr establecer con éxito una sesión de meterpreter.

5.1.5. ESCALAMIENTO DE PRIVILEGIOS. Por ultimo y no menos importante, se nos informa al respecto de una posible escalación de privilegios mediante el exploit asociado a esta aplicación, lo cual llevaría a la creación de un usuario administrador del sistema.

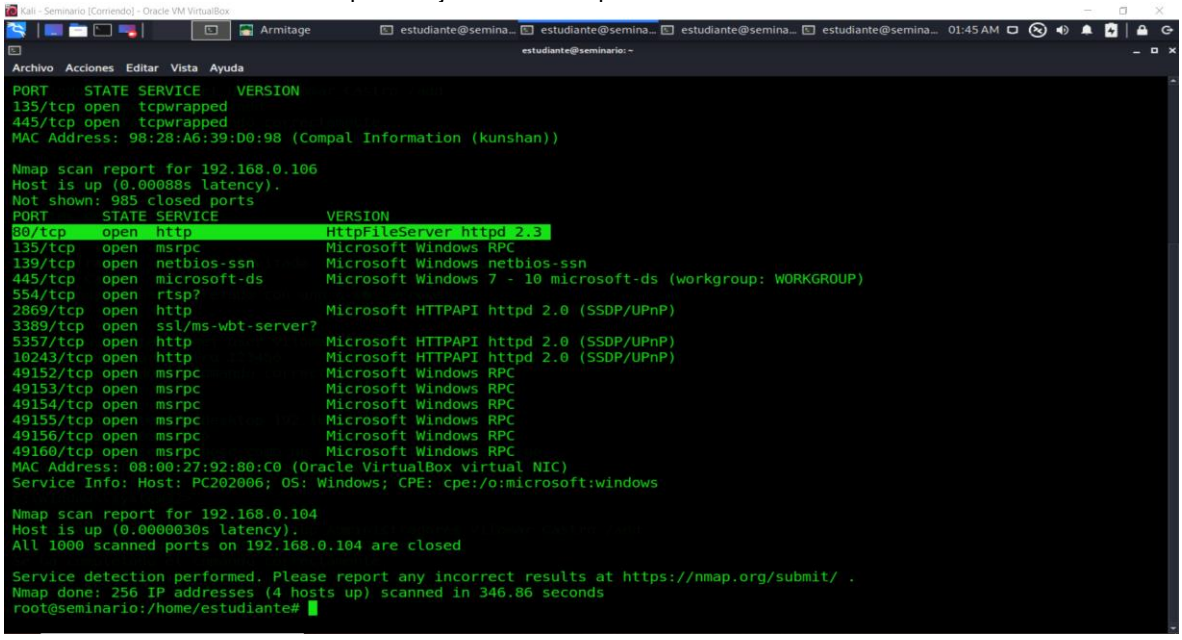
5.1.6. COPIA DEL SISTEMA PARA EL EQUIPO RED TEAM. Mediante el suministro de la imagen del servidor, la cual contiene la vulnerabilidad a explotar, podemos adentrarnos en la realización de las diferentes fases del Pentesting, esto bajo un ambiente controlado y finalmente poder generar el informe con los resultados de la prueba de concepto PoC realizada para la alta gerencia.

6. INFORME DE HERRAMIENTAS EMPLEADAS PARA IDENTIFICAR FALLOS POR PARTE DEL EQUIPO RED TEAM.

Para lograr identificar los fallos de seguridad presentes en la maquina objetivo de este análisis, se utilizaron las herramientas relacionadas a continuación:

6.1.1. Nmap. Empleada durante el desarrollo de la fase de recolección de la información.

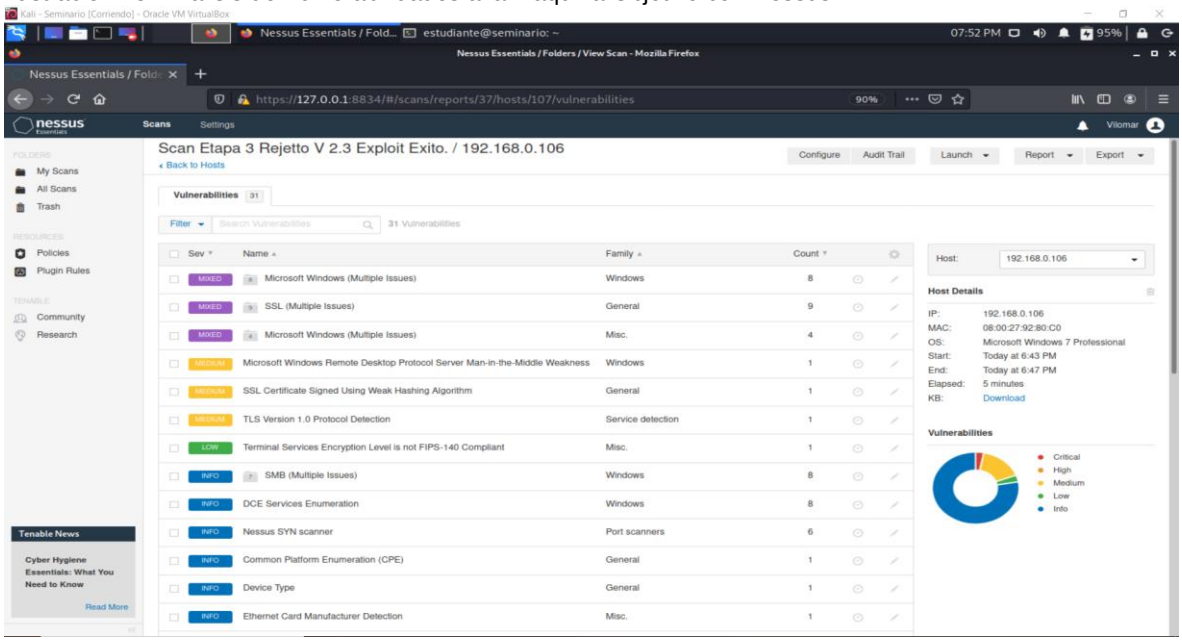
Ilustración 12. Análisis de la Maquina Objetivo con Nmap.



Fuente. El Autor.

6.1.2. Nessus. Al igual que la herramienta anterior, Nessus lo utilizamos en la fase de recolección de información y análisis de vulnerabilidades.

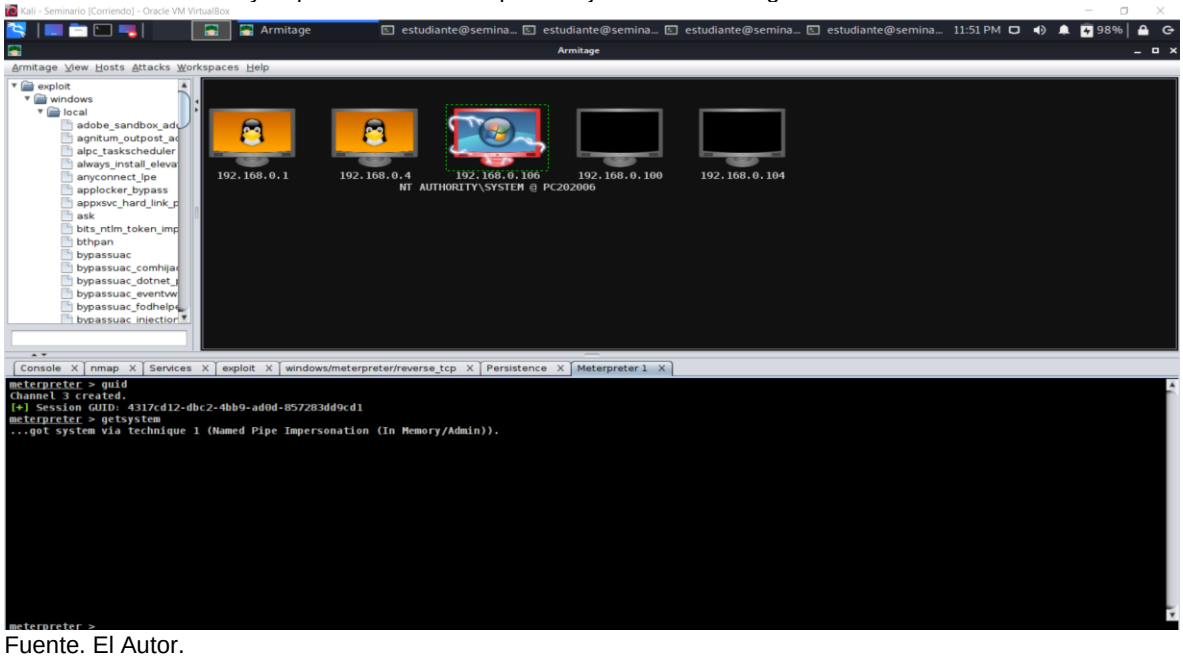
Ilustración 13. Análisis de Vulnerabilidades a la Maquina Objetivo con Nessus.



Fuente. El Autor.

6.1.3. Armitage. A diferencia de las anteriores, esta herramienta la empleamos tanto en la fase de análisis y recolección de información, como a su vez en la fase de explotación.

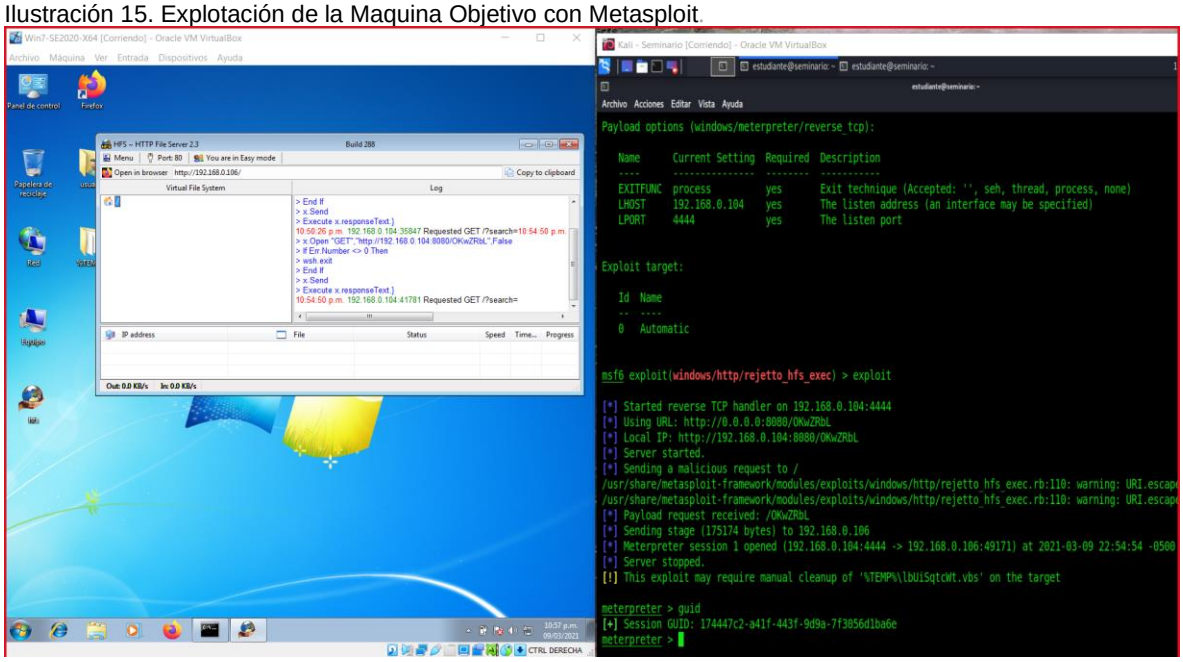
Ilustración 14. Análisis y Explotación de la Maquina Objetivo con Armitage.



Fuente. El Autor.

6.1.4. Metasploit. Con este FrameWork, se logra explotar la vulnerabilidad identificada en la fase anterior mediante el uso de un vector de ataque previamente definido.

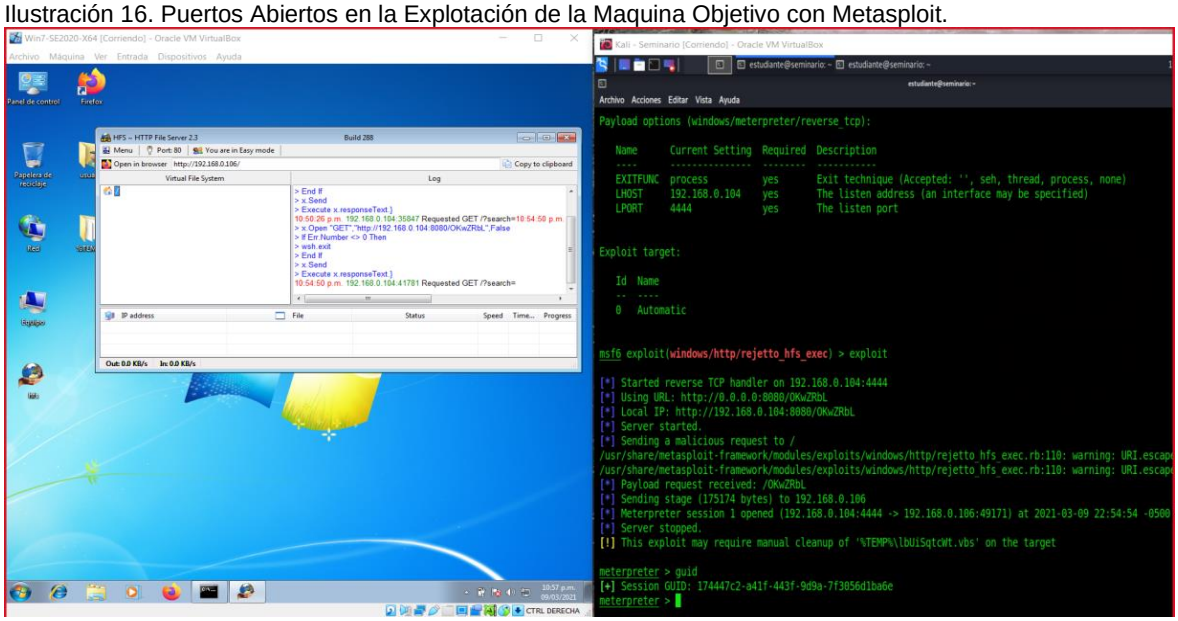
Ilustración 15. Explotación de la Maquina Objetivo con Metasploit.



Fuente. El Autor.

6.1.5. PUERTO ABIERTO POR LA APLICACIÓN REJETTO V 2.3. Debido a los resultados obtenidos en nuestra fase de análisis y reconocimiento, se pudo conocer que el servicio de la aplicación rejetto v 2.3, se ejecuta a través del puerto **80**. Sin embargo, como resultado de nuestra fase de explotación se pudo comprobar que al momento de establecer nuestra sesión de meterpreter, se establece la conexión entre la maquina atacante identificada con dirección IP **192.168.0.104**, puerto **4444** y la maquina objetivo con una dirección IP **192.168.0.106** a través del puerto **49171**, como se evidencia en la siguiente grafica.

Ilustración 16. Puertos Abiertos en la Explotación de la Maquina Objetivo con Metasploit.



Fuente. El Autor.

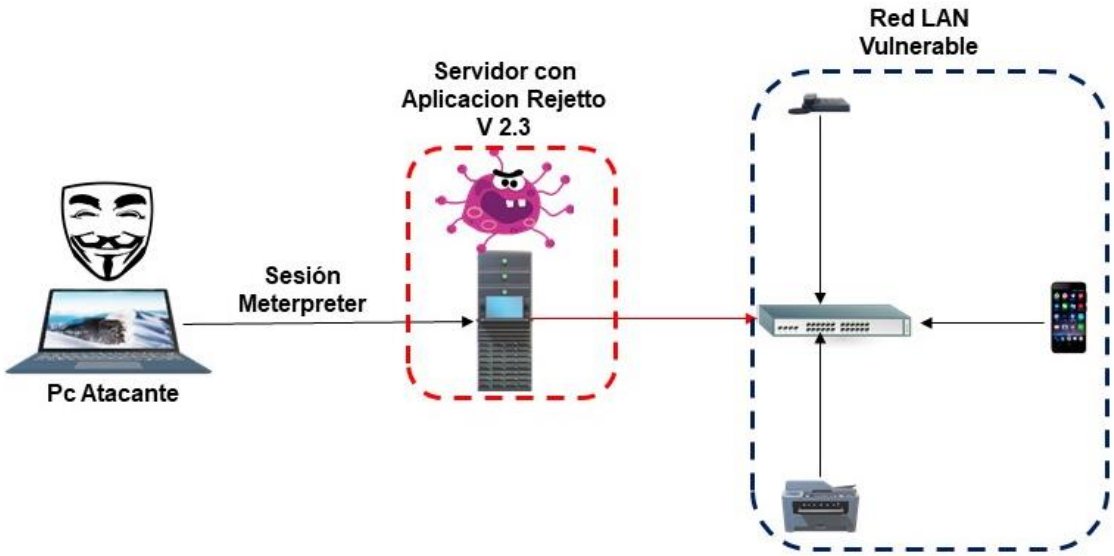
7. INFORME DE AFECTACIÓN DEL ATAQUE A LA MAQUINA WINDOWS 7.

Mediante la realización de este ataque dirigido a la máquina con sistema operativo Windows X64, la cual cuenta con el servicio y la aplicación rejetto en su versión 2.3, previamente configurado en el puerto 80, es posible establecer una sesión de meterpreter para posteriormente escalar privilegios como administrador, logrando así la exfiltración de datos en el sistema comprometido.

Lo anterior debido a que la aplicación del servidor de archivos HTTP, específicamente en la versión objeto de esta prueba, alberga una vulnerabilidad que puede ser explotada mediante el exploit **windows/http/rejetto_hfs_exec,** contenido dentro del repositorio de Metasploit, permitiendo así establecer una sesión meterpreter anónima, comprometiendo los principios esenciales de la integridad, disponibilidad y confidencialidad de los datos almacenados en este servidor.

Por lo anterior a continuación se relaciona una imagen, en esta se hace una breve descripción del ataque generado a través del exploit antes en mención.

Ilustración 17. Descripción del Ataque a través de la Vulnerabilidad en la aplicación Rejetto V 2.3.



Fuente. El Autor.

8. INFORME EXPLOTACIÓN DE VULNERABILIDADES EN LA MAQUINA DE WINDOWS 7 X64**.**

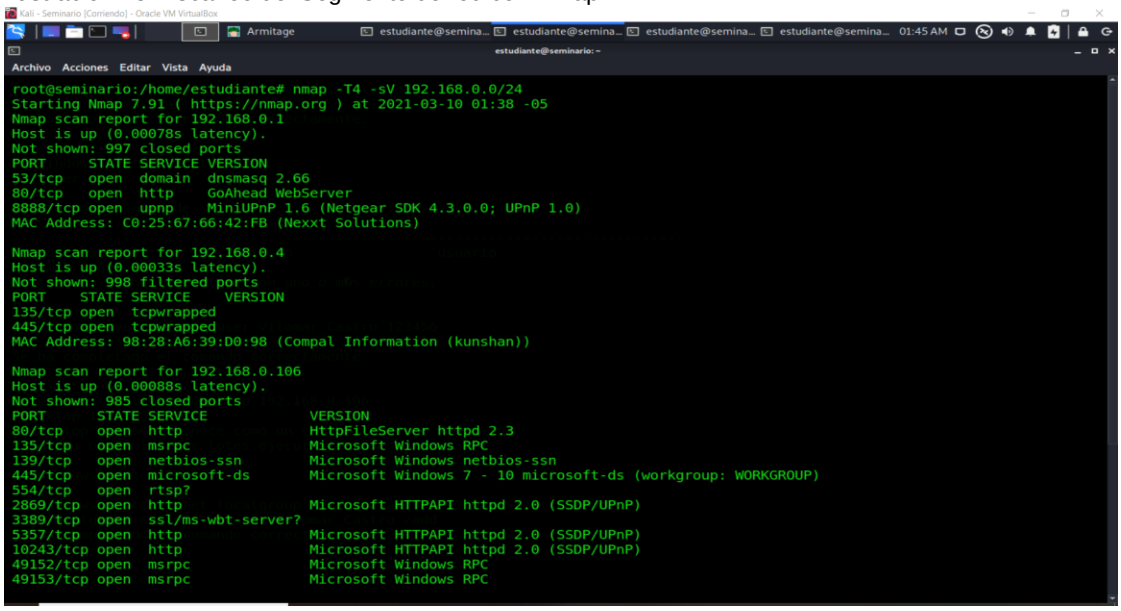
A continuación, se describen las diferentes fases empleadas, esto con el fin de lograr la explotación exitosa de la vulnerabilidad objeto de este informe, y que va alineada con la aplicación rejetto v 2.3.

Como complemento a la descripción antes en mención, se incluyen imágenes que evidencian cada uno de los pasos realizados para lograr la explotación de la vulnerabilidad.

8.1.1. FASE DE RECOLECCIÓN DE LA INFORMACIÓN. Para la realización de esta fase de forma exitosa empleamos herramientas descritas en los apartes mencionados anteriormente en este informe, sin embargo, nos enfocaremos en los procedimientos realizados con cada una de estas herramientas en esta fase, así:

- Nmap. Se realiza un escaneo del segmento de red contemplado en el alcance de esta prueba de concepto, como se evidencia en la siguiente imagen.

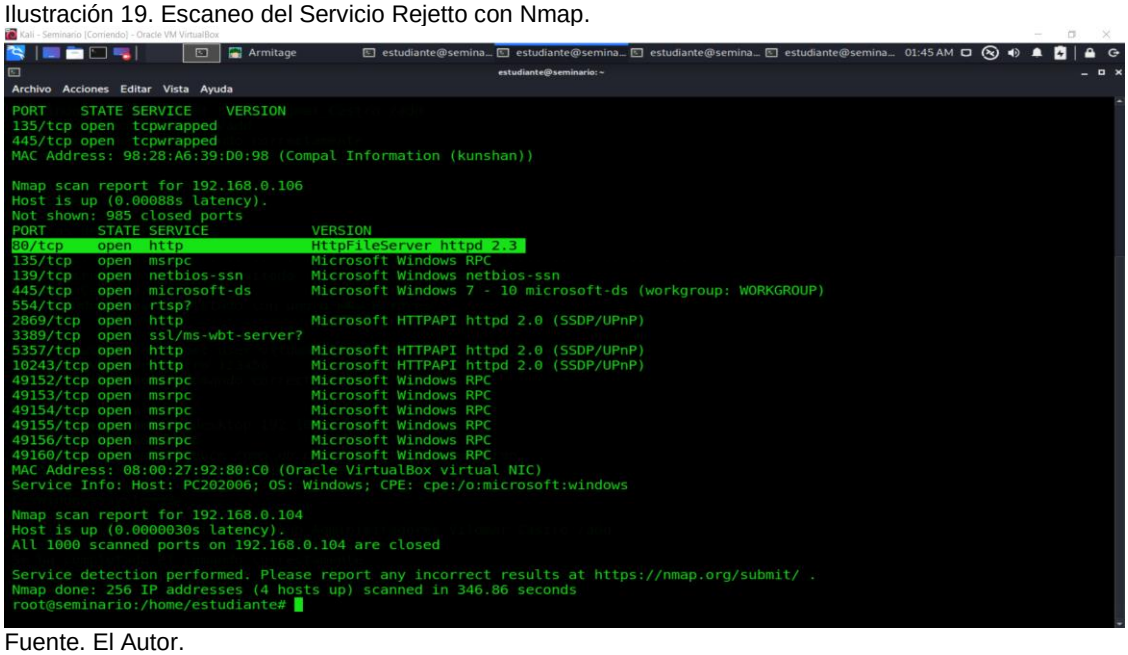
Ilustración 18. Escaneo del Segmento de red con Nmap.



Fuente. El Autor.

De este escaneo con la aplicación Nmap, destacamos la información relacionada con la máquina que contiene el servicio rejetto v 2.3, como se observa en la imagen a continuación.

Ilustración 19. Escaneo del Servicio Rejetto con Nmap.



Fuente. El Autor.

- Armitage. De igual forma se considera la realización del escaneo de la maquina objetivo de estas pruebas con esta herramienta, esto con el fin de descartar falsos positivos en los que podemos incurrir al momento de decidir

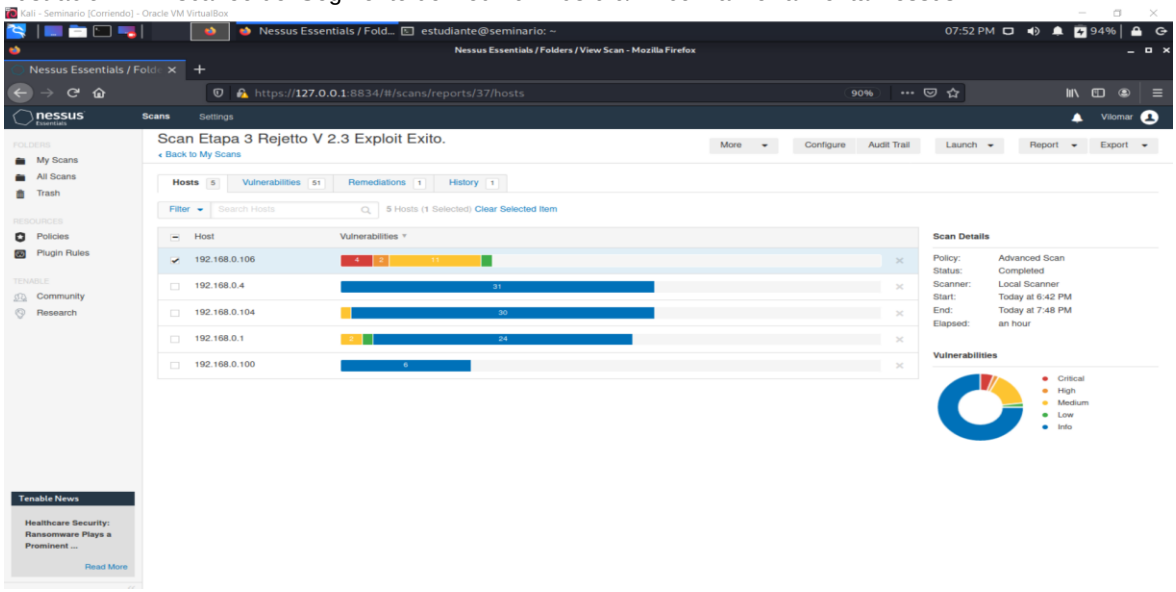
emplear solo una única herramienta, de lo anterior podemos evidenciar la similitud en los resultados del escaneo realizado con las dos herramientas en la siguiente imagen.

Ilustración 20. Escaneo de la Maquina Objetivo con la Herramienta Armitage.

Fuente. El Autor.

8.1.2. ANÁLISIS DE VULNERABILIDADES. Para llevar a cabo esta fase, decidimos emplear la herramienta Nessus Essentials, en su versión Open Source. Con esta pretendemos realizar un análisis de vulnerabilidades al segmento de red de nuestro interés, el cual tiene como direccionamiento IP **192.168.0.0/24,** de lo anterior obtendríamos como producto el resultado descrito en la imagen a continuación, en esta se evidencian las diferentes vulnerabilidades clasificadas en orden de criticidad para cada una de las máquinas de la red.

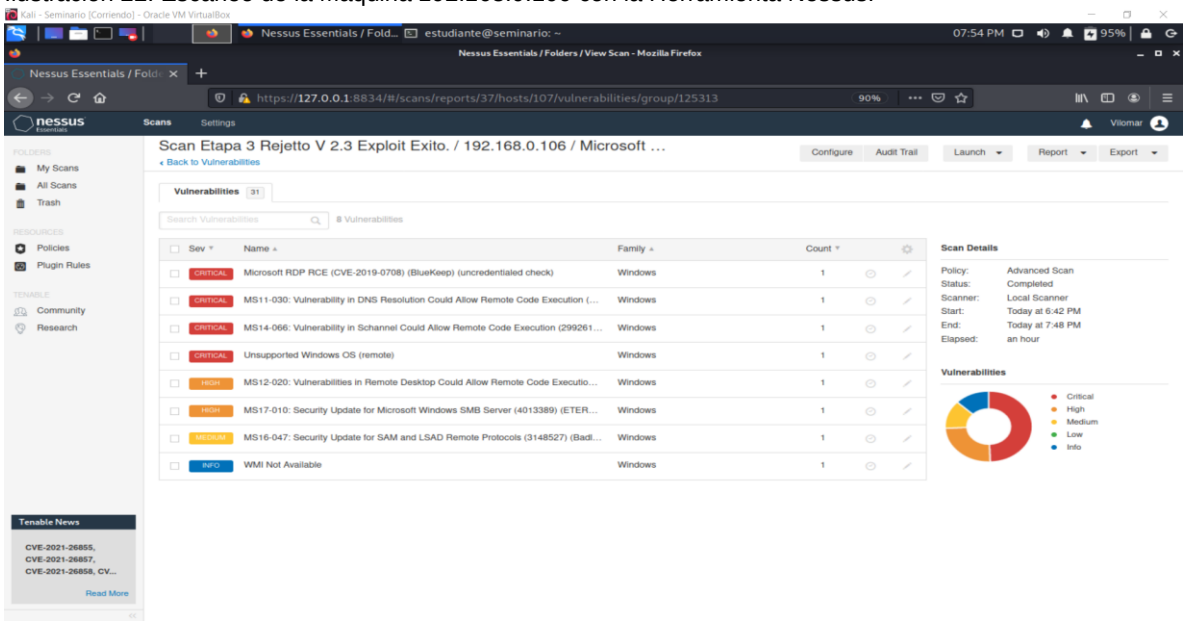
Ilustración 21. Escaneo del Segmento de Red 192.168.0.0/24 con la Herramienta Nessus.



Fuente. El Autor.

Siguiendo la línea de tiempo del paso anterior, centramos nuestro enfoque en analizar las vulnerabilidades arrojadas para la máquina de nuestro interés, la cual tiene como direccionamiento IP **192.168.0.106**, como lo muestra la imagen a continuación.

Ilustración 22. Escaneo de la Maquina 192.168.0.106 con la Herramienta Nessus.



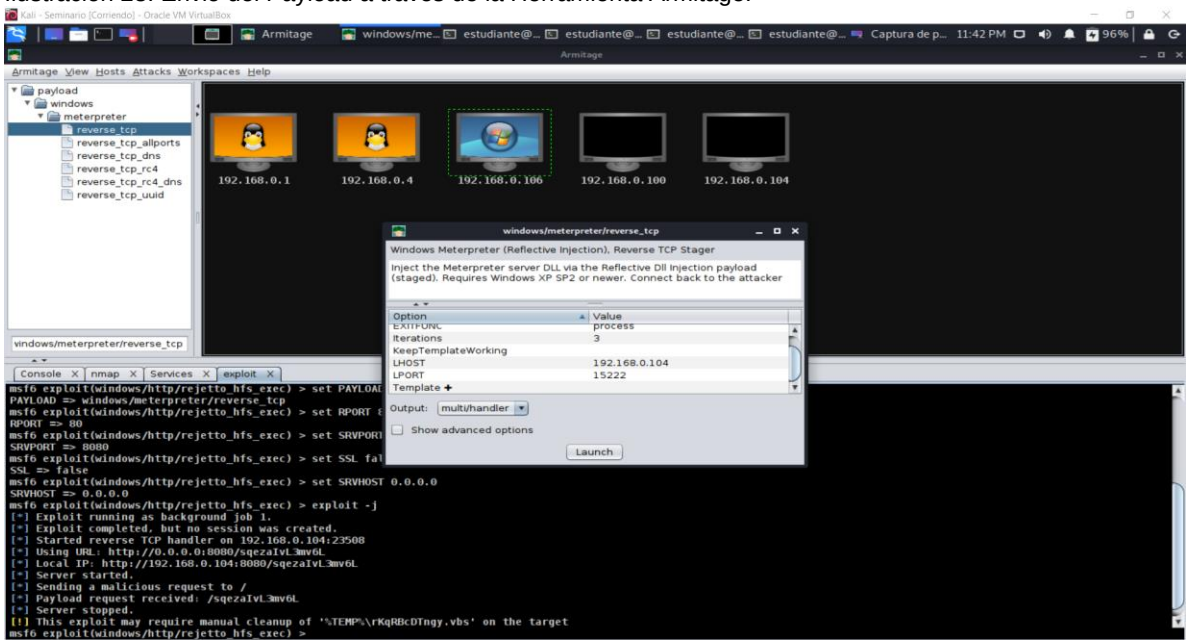
Fuente. El Autor.

8.1.3. FASE DE EXPLOTACIÓN Y ESCALACIÓN DE PRIVILEGIOS. Para la ejecución de la fase de explotación y escalación de privilegios seleccionamos 2 herramientas descritas en los apartes de las fases anteriores de este informe, como lo son Metasploit-Framework y Armitage.

A continuación, realizaremos una descripción del paso a paso efectuado para lograr explotar con éxito la vulnerabilidad asociada a la aplicación rejetto, está en su versión 2.3.

8.1.3.1. EXPLOTACIÓN CON LA HERRAMIENTA ARMITAGE. Aprovechando las funciones automatizadas con las que cuenta la herramienta, iniciaremos con la selección de la Payload **windows/meterpreter/reverse_tcp**, la cual será enviada antes de configurar y enviar nuestro exploit, como se relaciona en la imagen a continuación.

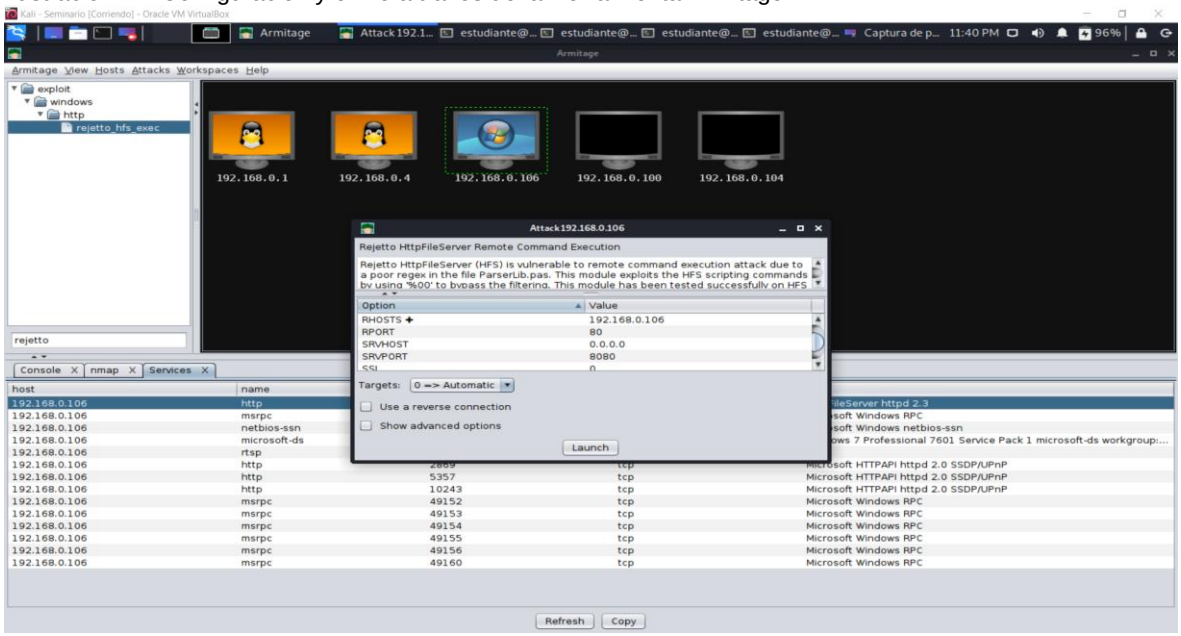
Ilustración 23. Envió del Payload a través de la Herramienta Armitage.



Fuente. El Autor.

El paso siguiente es configurar los parámetros requeridos por el exploit **rejetto_hfs_exec**, como lo son el **RHOSTS 192.168.0.106**, como se observa en la imagen a continuación.

Ilustración 24. Configuración y envió a través de la Herramienta Armitage.



Fuente. El Autor.

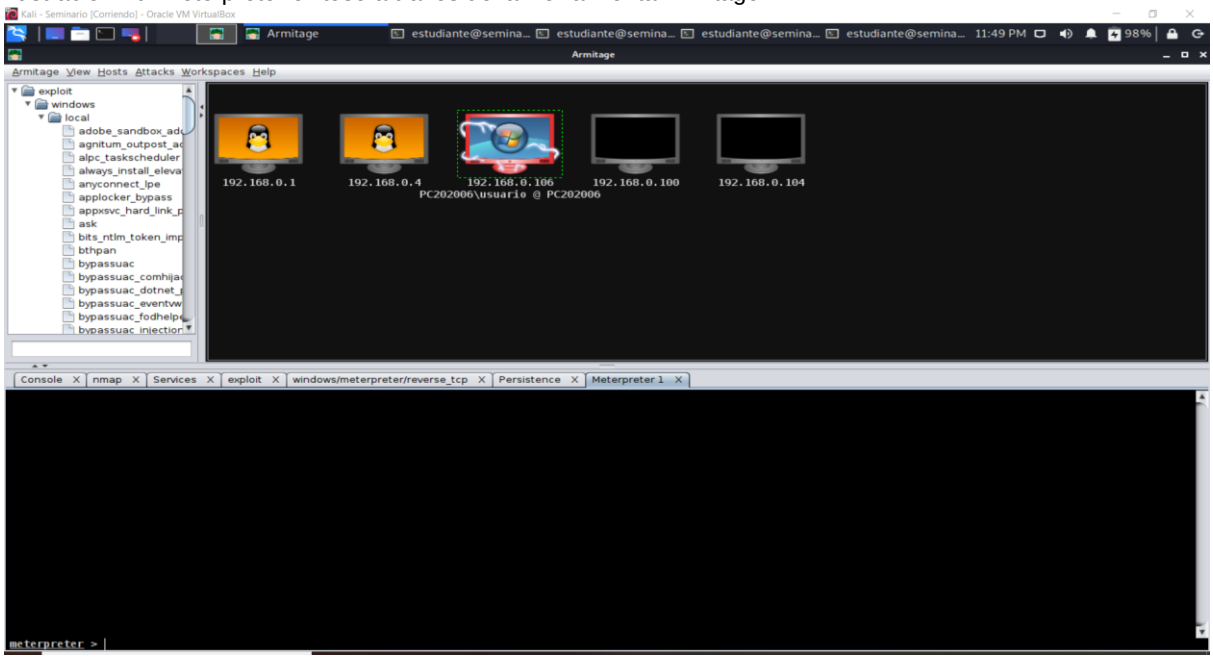
Al lanzar el exploit validaremos que, una vez ejecutado de manera exitosa, se establecerá la sesión de meterpreter como se evidencia en la siguiente imagen.

Ilustración 25. Sesión de Meterpreter establecida a través de la Herramienta Armitage.

Fuente. El Autor.

Como paso final se creará nuestra sesión de meterpreter, como se observa en la siguiente imagen.

Ilustración 26. Meterpreter exitoso a través de la Herramienta Armitage.



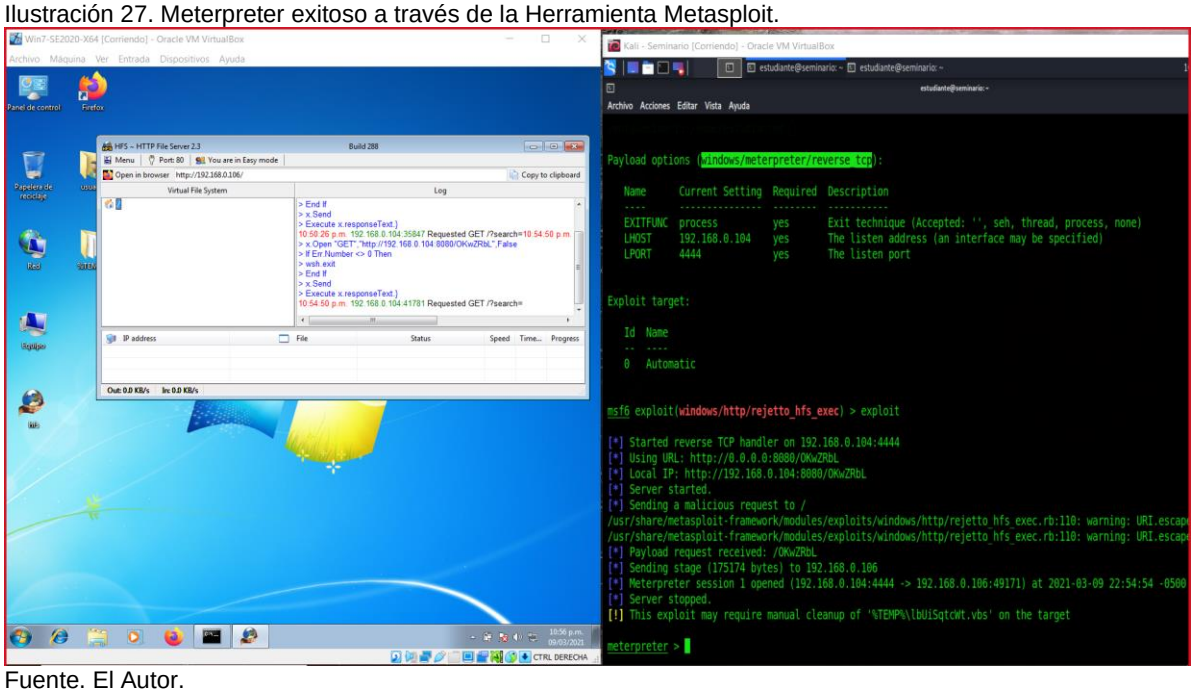
Fuente. El Autor.

8.1.3.2. EXPLOTACIÓN CON LA HERRAMIENTA METASPLOIT. Como herramienta principal para la ejecución de nuestro ejercicio de Red Team, realizaremos la explotación y escalación de privilegios mediante el uso de esta herramienta.

Inicialmente, procederemos a realizar la búsqueda de nuestro exploit dentro de la herramienta, lo anterior mediante el comando **search hfs**. Ubicado nuestro exploit lo seleccionamos con el comando **use + # id** del exploit, para nuestro caso es el exploit **windows/http/rejetto_hfs_exec**.

Una vez ubicados en nuestro exploit procederemos a listar las diferentes opciones requeridas para su correcta configuración, en nuestro caso **RHOSTS 192.168.0.106** y la **Payload windows/meterptreter/reverse_tcp**. Por último, lanzamos nuestro ataque mediante el comando **exploit** o en su defecto **run**.

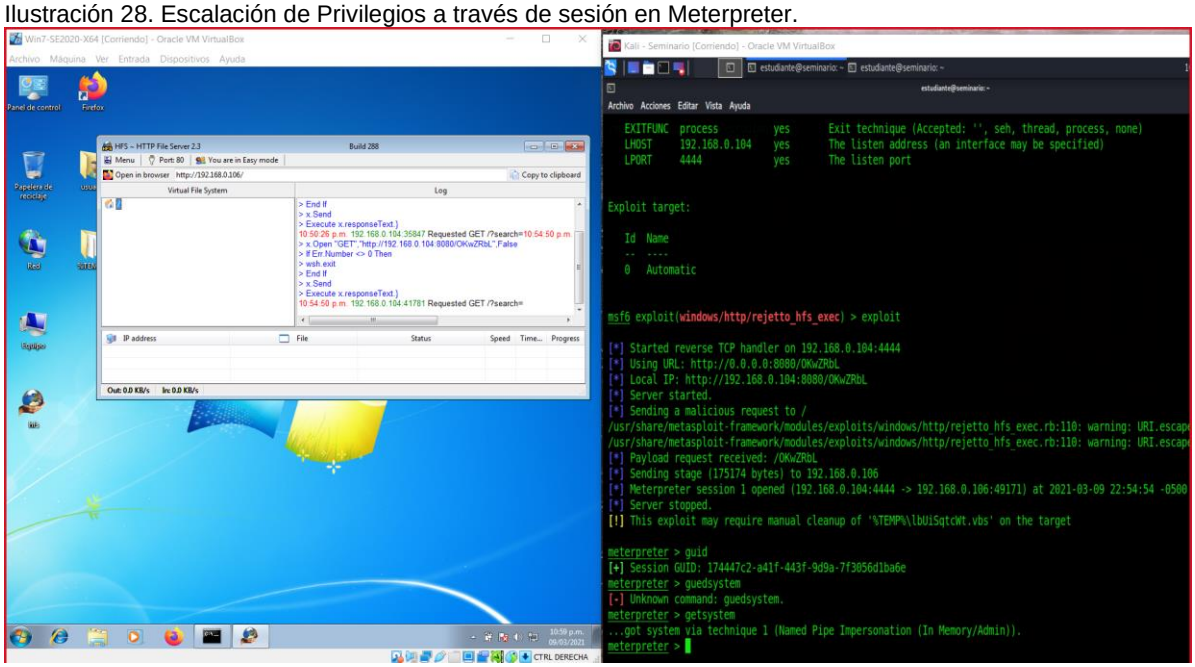
Ilustración 27. Meterpreter exitoso a través de la Herramienta Metasploit.



Fuente. El Autor.

una vez obtenida nuestro meterpreter, se procede a utilizar el comando **guid**, esto con el fin de verificar la identificación de nuestra sesión y así mediante el comando **getsystem** escalar privilegios dentro del sistema.

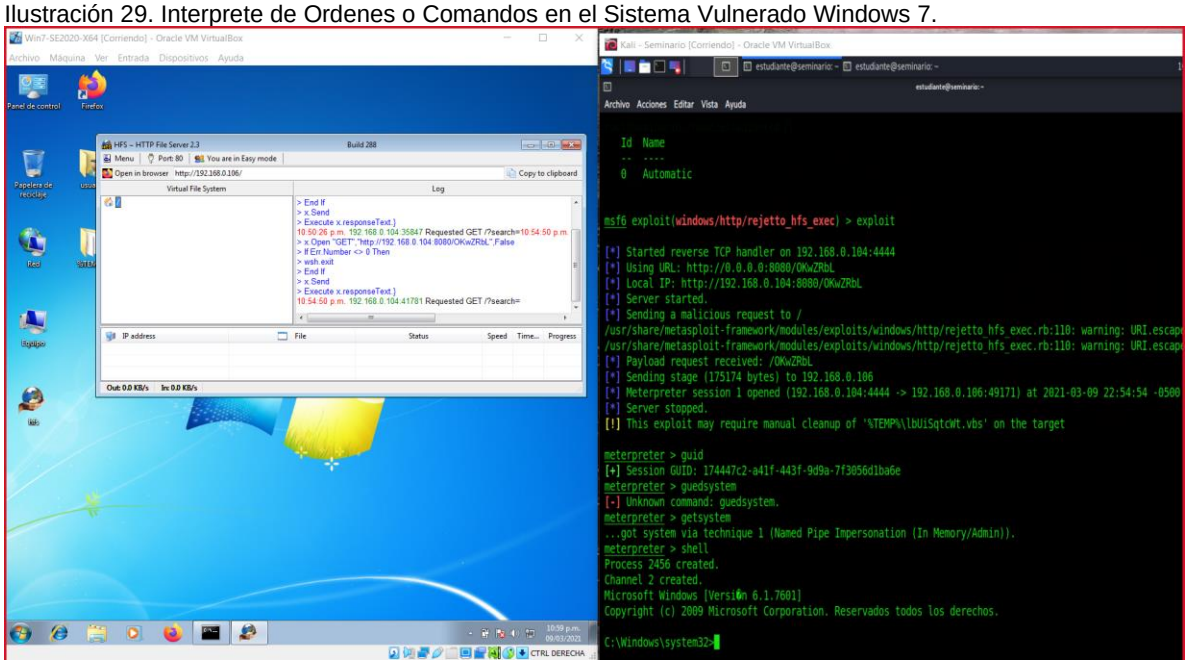
Ilustración 28. Escalación de Privilegios a través de sesión en Meterpreter.



Fuente. El Autor.

por último, mediante el comando **shell**, ejecutamos nuestro interprete de ordenes dentro de nuestro sistema Windows 7 X64 vulnerado, como se muestra en la siguiente imagen.

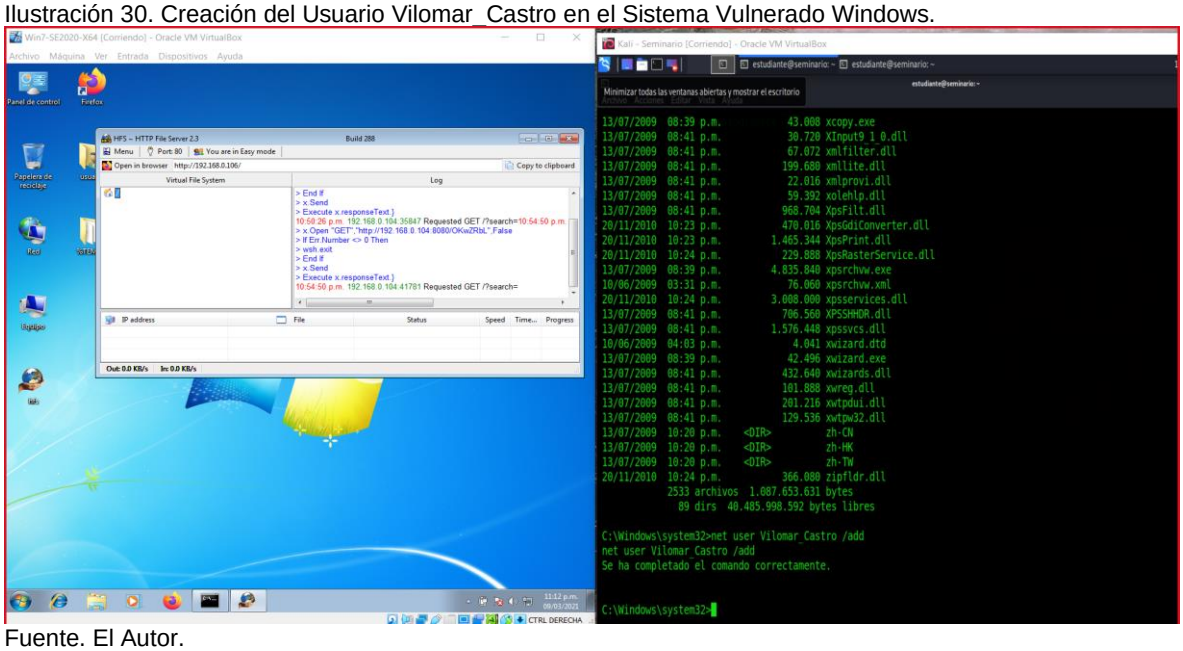
Ilustración 29. Interprete de Ordenes o Comandos en el Sistema Vulnerado Windows 7.



Fuente. El Autor.

8.1.3.3. CREACIÓN DE USUARIO COMO ADMINISTRADOR. Se crea el usuario **Vilomar_Castro** mediante el comando **net user Vilomar_Castro /add.**

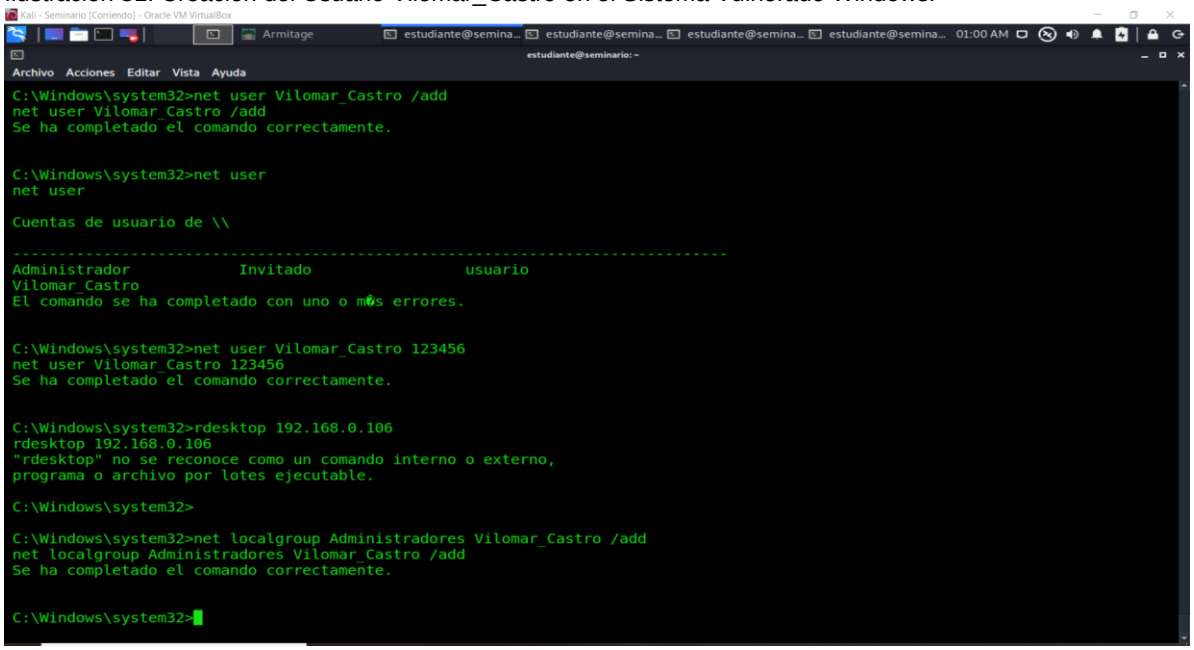
Ilustración 30. Creación del Usuario Vilomar_Castro en el Sistema Vulnerado Windows.



Fuente. El Autor.

Se le asigna una contraseña para el inicio de sesión al usuario **Vilomar_Castro**, esta es **123456**. De igual forma se agrega al usuario **Vilomar_Castro** al grupo de Administradores, esto mediante el comando **net localgroup Administradores Vilomar_Castro /add**, lo anterior para efectos de garantizar el éxito de nuestra PoC.

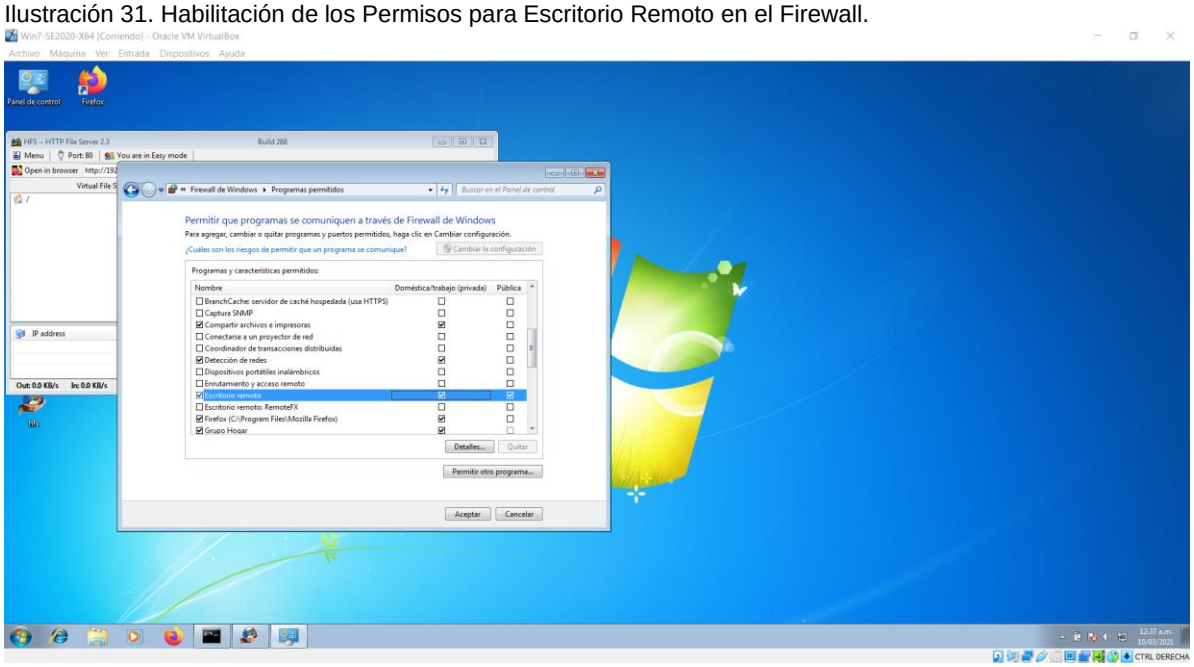
Ilustración 31. Creación del Usuario Vilomar_Castro en el Sistema Vulnerado Windows.



Fuente. El Autor.

Una vez creado e incluido en el grupo de administradores nuestro usuario **Vilomar_Castro**, procedemos a habilitar en la maquina Windows 7 X64, específicamente en el Firewall de Windows permisos para escritorio remoto.

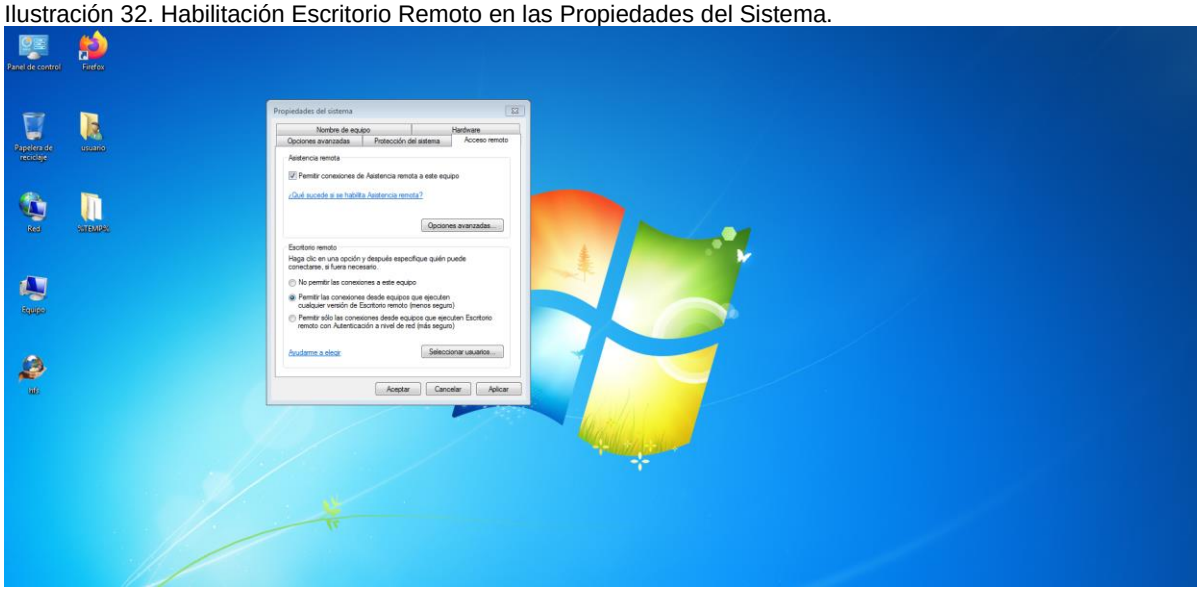
Ilustración 31. Habilitación de los Permisos para Escritorio Remoto en el Firewall.



Fuente. El Autor.

Se habilitan las conexiones remotas a la maquina comprometida desde las propiedades del sistema.

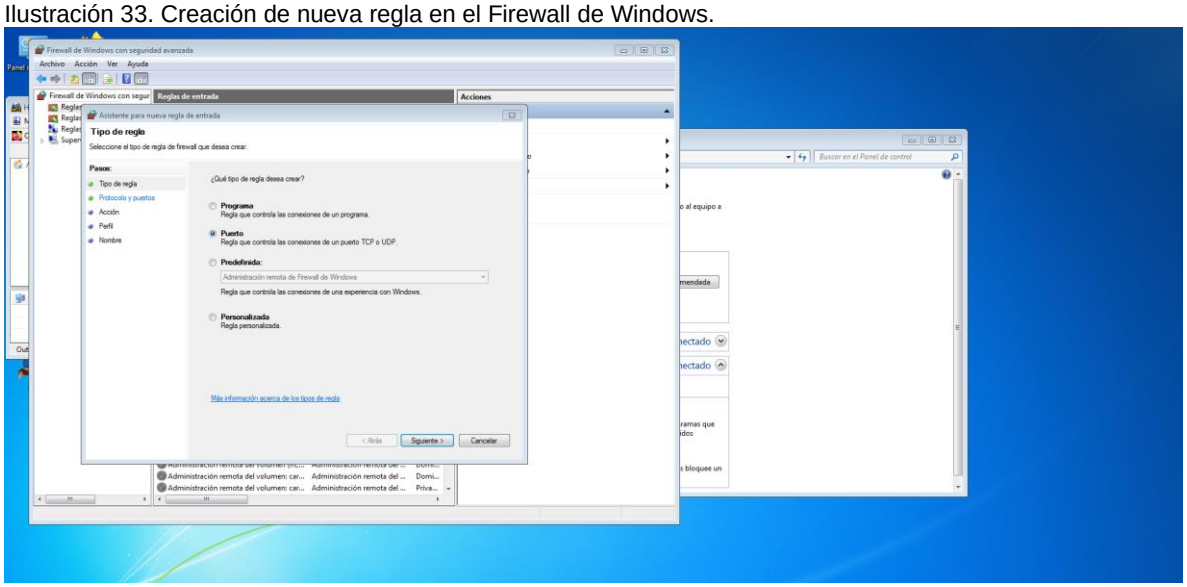
Ilustración 32. Habilitación Escritorio Remoto en las Propiedades del Sistema.



Fuente. El Autor.

En las opciones avanzadas del Firewall de Windows, se configura una nueva regla de entrada, esta con el fin de habilitar un nuevo puerto para la conexión remota a la maquina vulnerada.

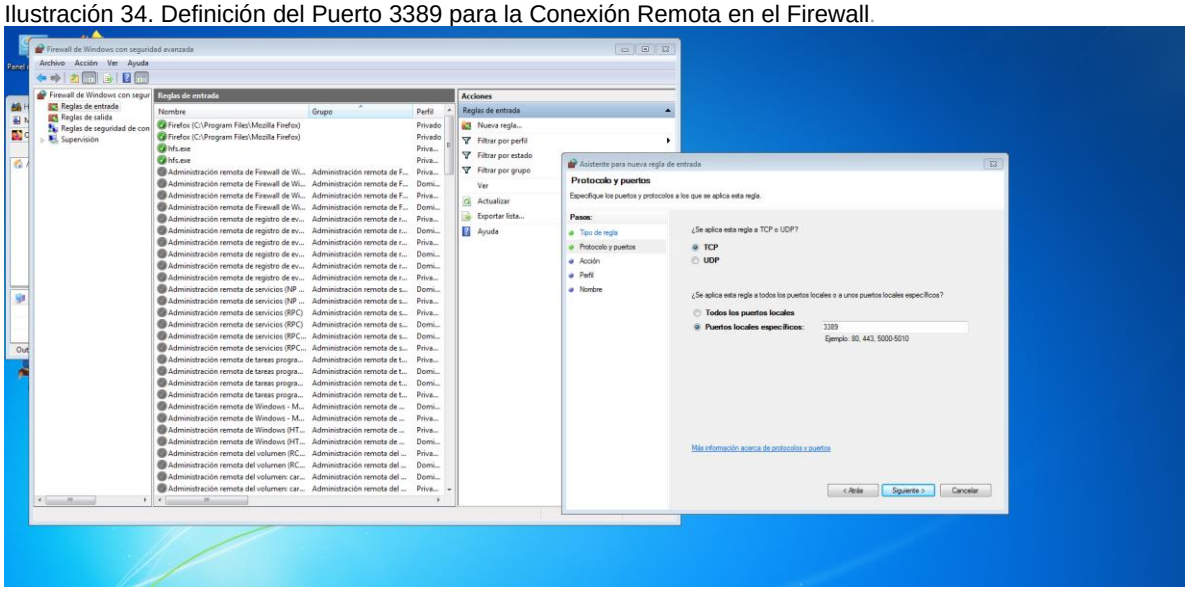
Ilustración 33. Creación de nueva regla en el Firewall de Windows.



Fuente. El Autor.

Se define el puerto **3389** para la conexión remota hacia la maquina objeto de nuestro análisis.

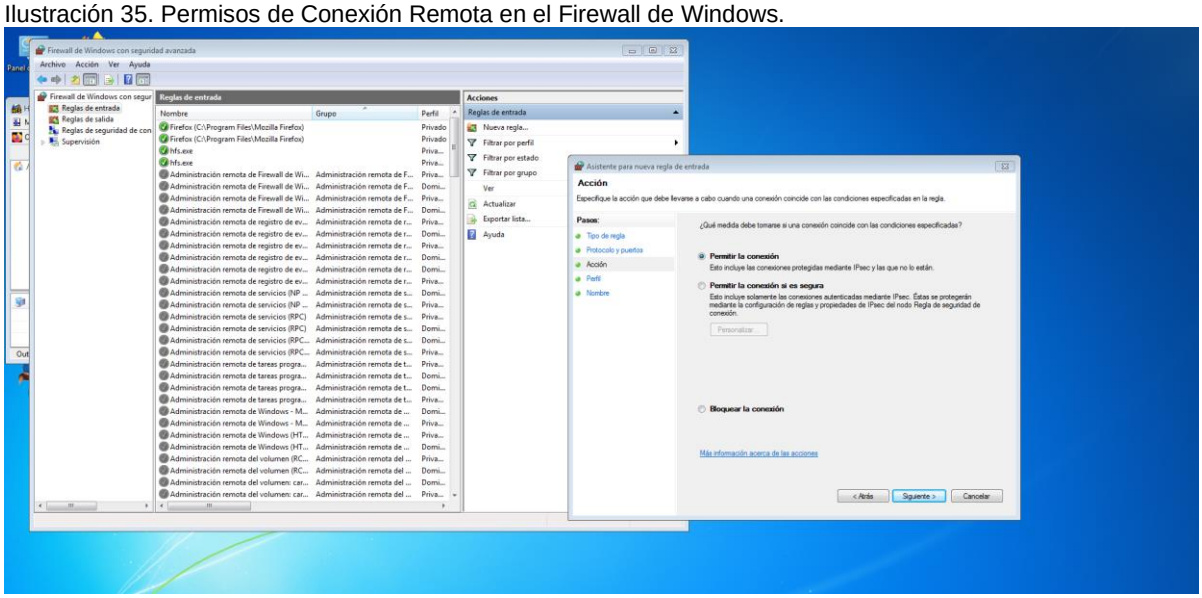
Ilustración 34. Definición del Puerto 3389 para la Conexión Remota en el Firewall.



Fuente. El Autor.

Permitimos la conexión de escritorio remoto a nuestra maquina Windows 7 X64.

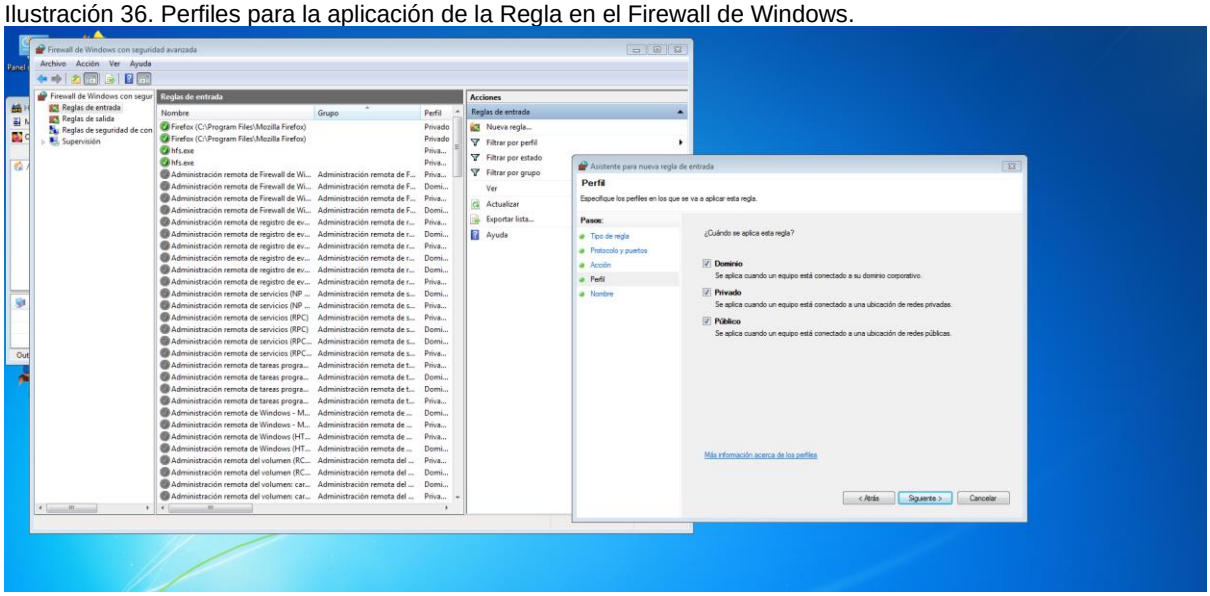
Ilustración 35. Permisos de Conexión Remota en el Firewall de Windows.



Fuente. El Autor.

Seleccionamos los diferentes perfiles a los cuales se aplicaría la regla a crear.

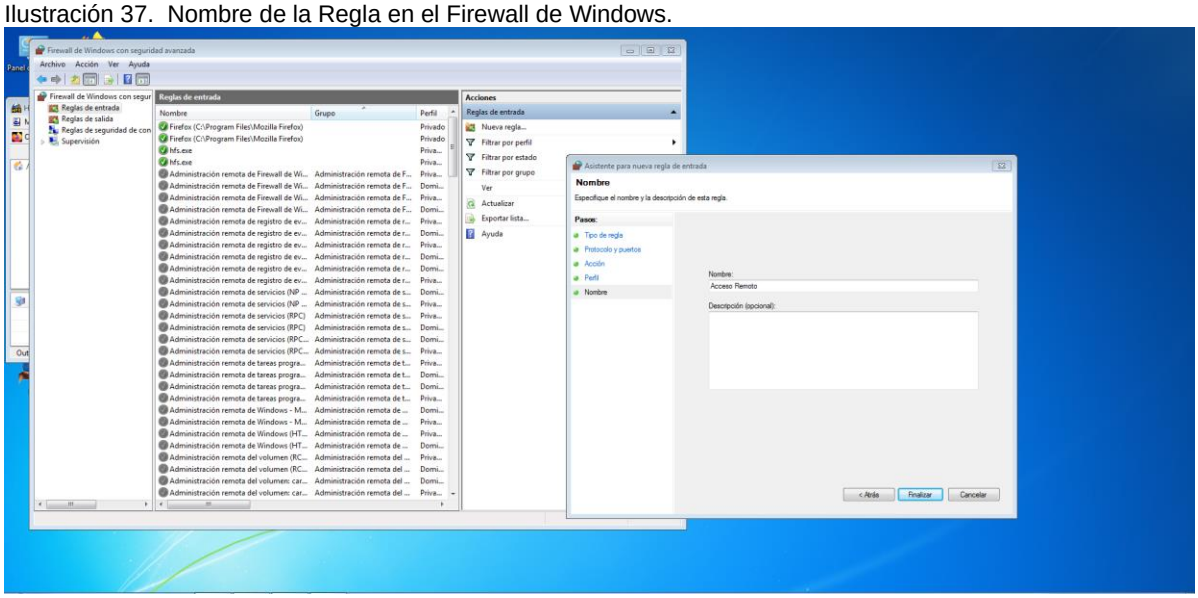
Ilustración 36. Perfiles para la aplicación de la Regla en el Firewall de Windows.



Fuente. El Autor.

Por último, le asignamos un nombre y si es de preferencia una descripción para la regla a crear.

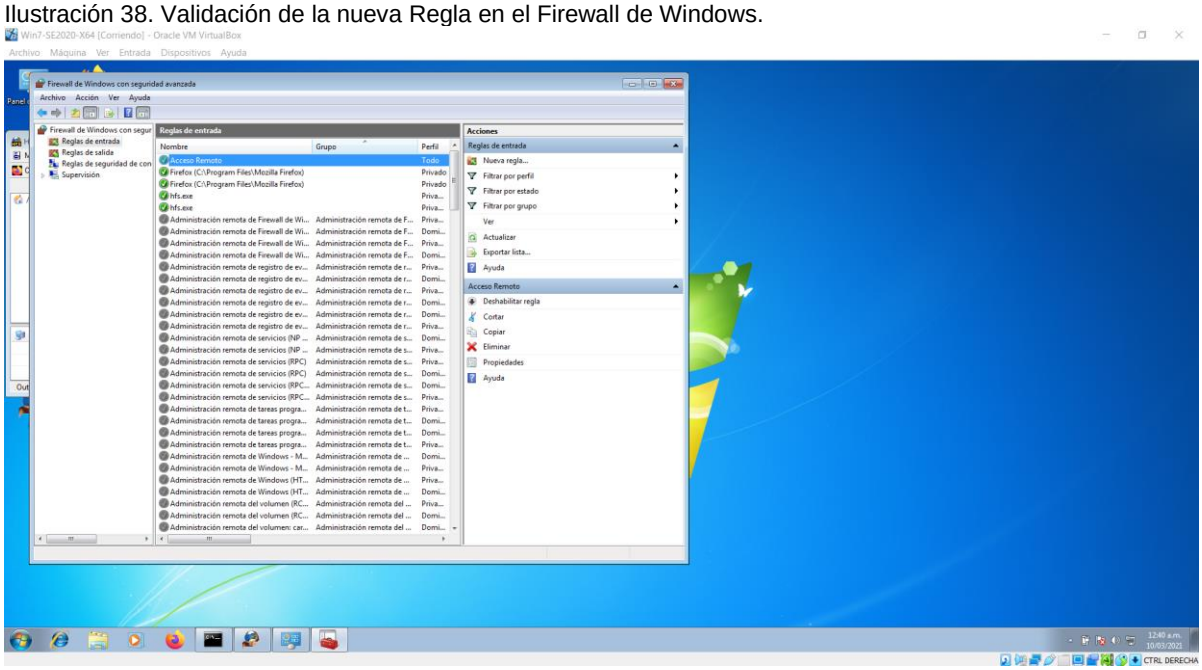
Ilustración 37. Nombre de la Regla en el Firewall de Windows.



Fuente. El Autor.

Realizados los pasos descritos con anterioridad, validamos el estado de nuestra nueva regla.

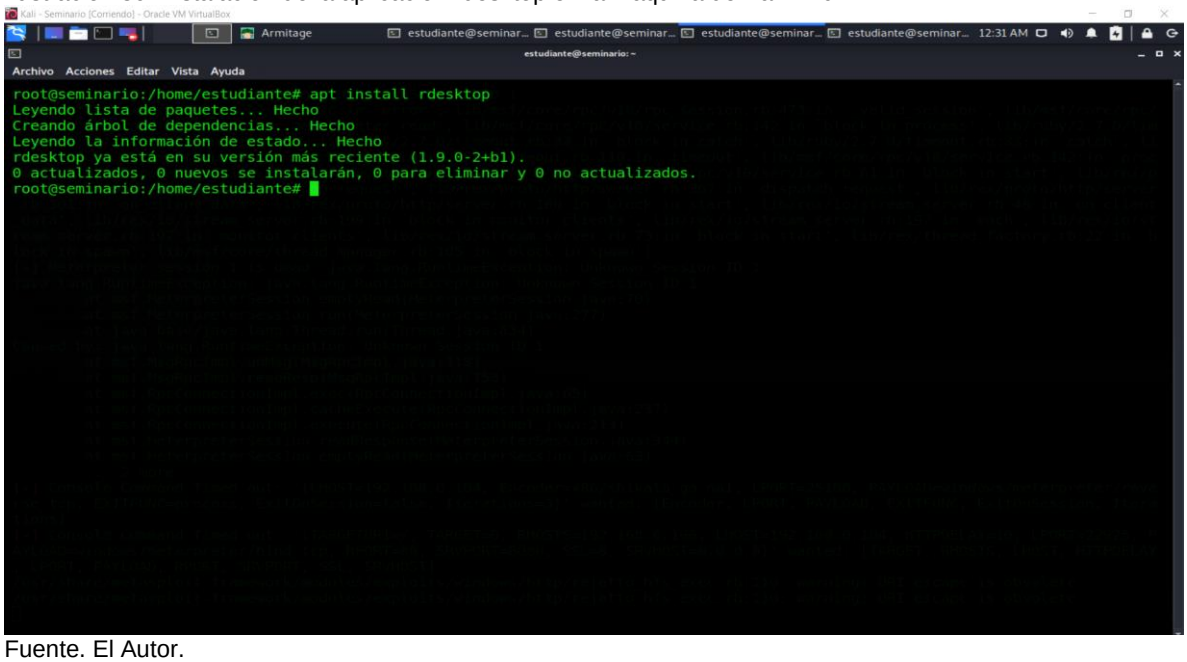
Ilustración 38. Validación de la nueva Regla en el Firewall de Windows.



Fuente. El Autor.

Instalamos la aplicación de **rdesktop** en la máquina de Kali Linux atacante, esto lo hacemos mediante la terminal.

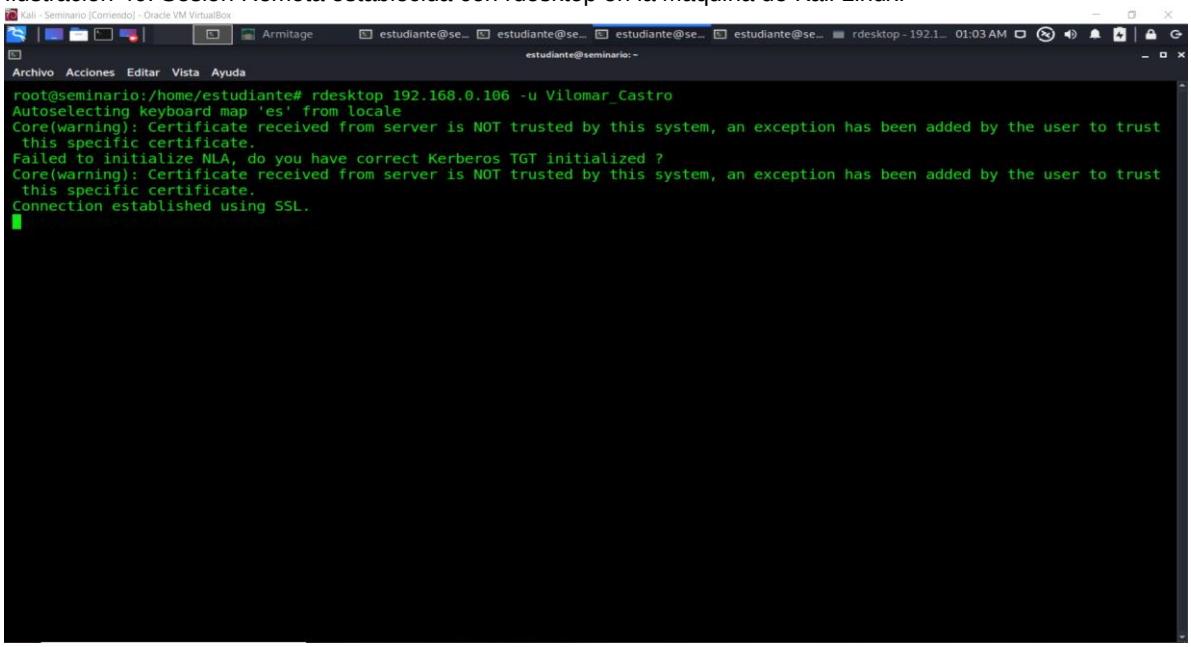
Ilustración 39. Instalación de la aplicación rdesktop en la Maquina de Kali Linux.



Fuente. El Autor.

Se establece la conexión remota con la maquina vulnerada de Windows 7 X64, para esto se emplea la aplicación **redesktop** con el siguiente comando **rdesktop 192.168.0.106 -u Vilomar_Castro.**

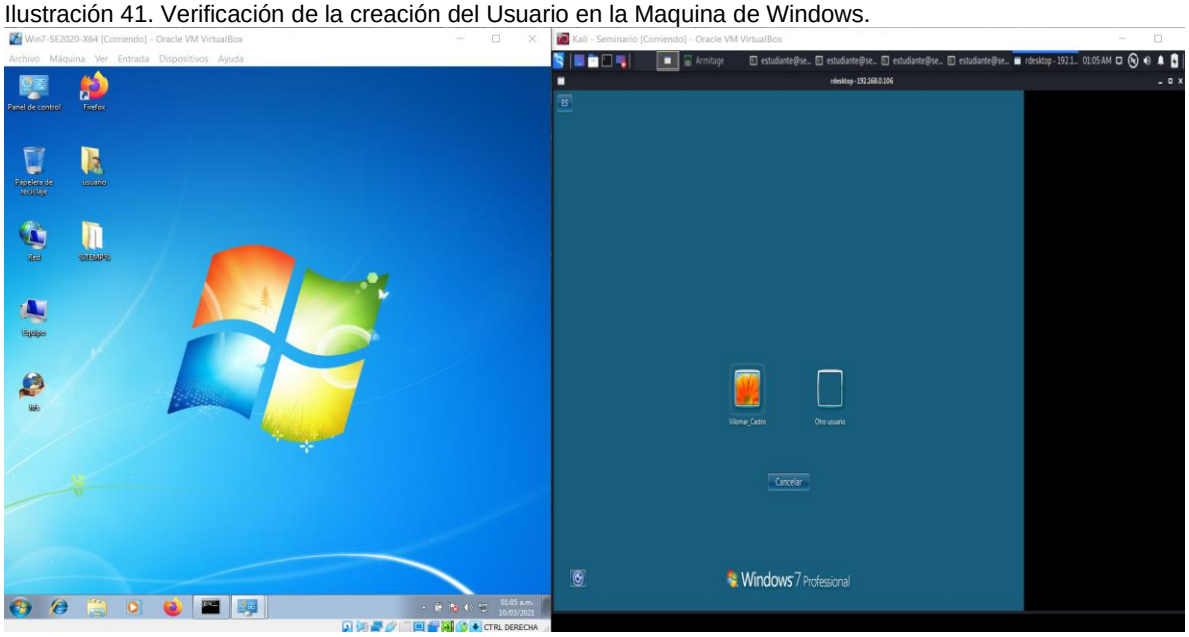
Ilustración 40. Sesión Remota establecida con rdesktop en la Maquina de Kali Linux.



Fuente. El Autor.

En esta instancia procedemos a verificar la creación de nuestro usuario en la maquina vulnerada.

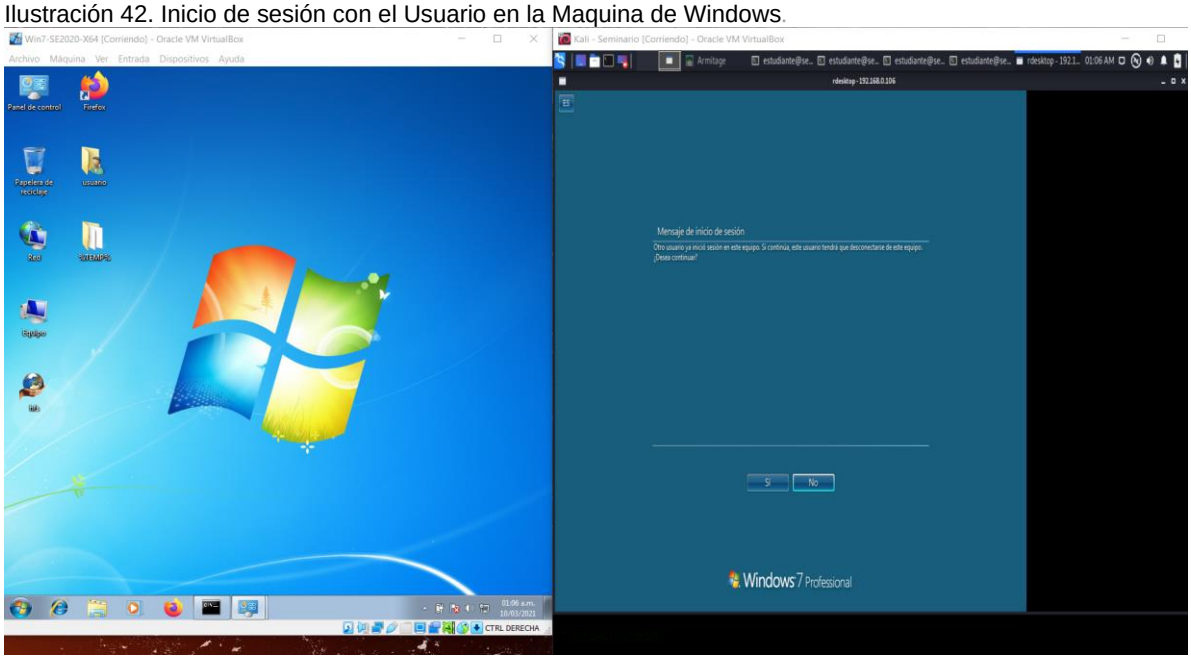
Ilustración 41. Verificación de la creación del Usuario en la Maquina de Windows.



Fuente. El Autor.

Procedemos a iniciar sesión en la maquina con el usuario **Vilomar_Castro**, creado para nuestra PoC.

Ilustración 42. Inicio de sesión con el Usuario en la Maquina de Windows.



Fuente. El Autor.

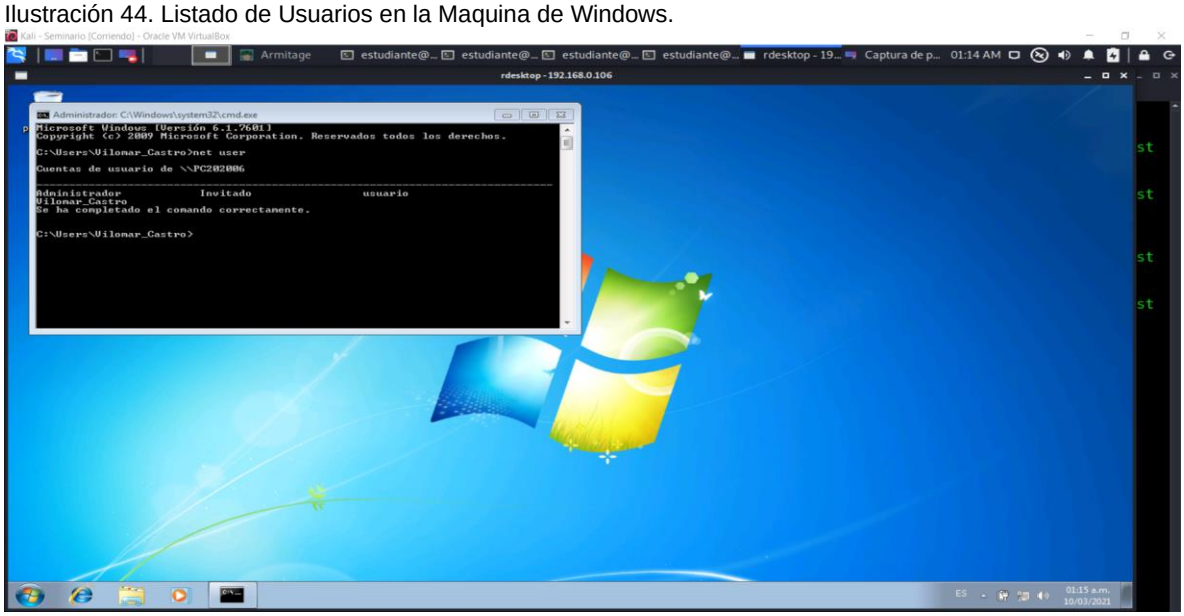
Se inicia exitosamente la sesión con el usuario **Vilomar_Castro** en la maquina vulnerada de Windows 7 X64.

Ilustración 43. Sesión con el Usuario Vilomar_Castro en la Maquina de Windows.

Fuente. El Autor.

En la maquina objeto de nuestro análisis, en una terminal mediante el comando **net user**, se listan los usuarios del sistema, en lo cual evidenciamos que nuestro usuario **Vilomar_Castro** se encuentra en el grupo de administradores.

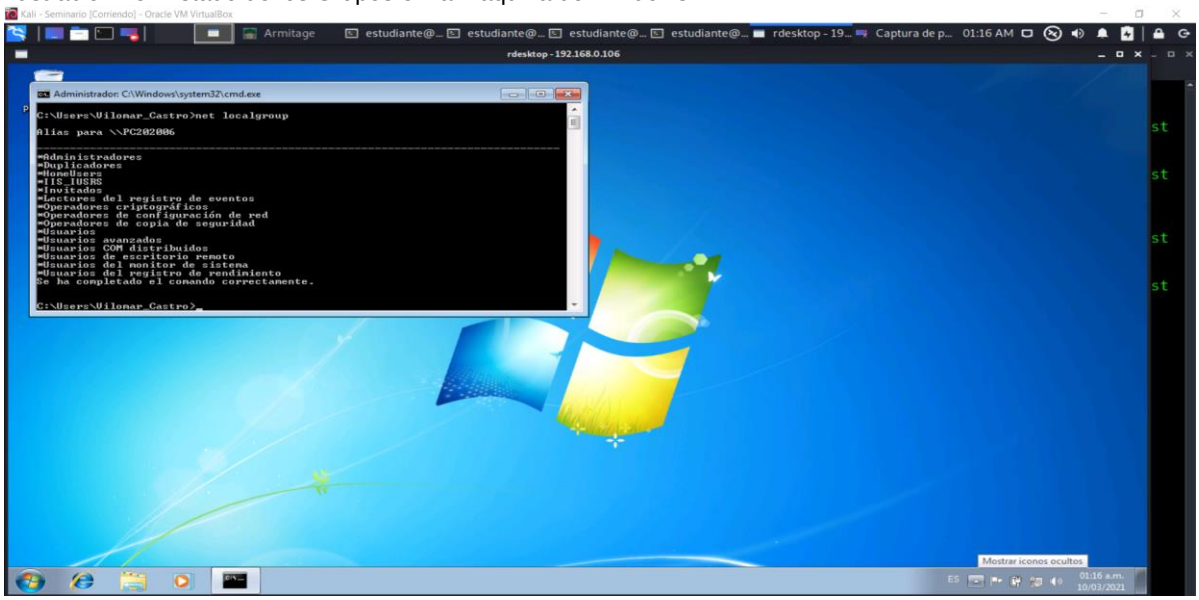
Ilustración 44. Listado de Usuarios en la Maquina de Windows.



Fuente. El Autor.

Para efectos de verificación, listamos mediante el comando **net local group**, los grupos del sistema.

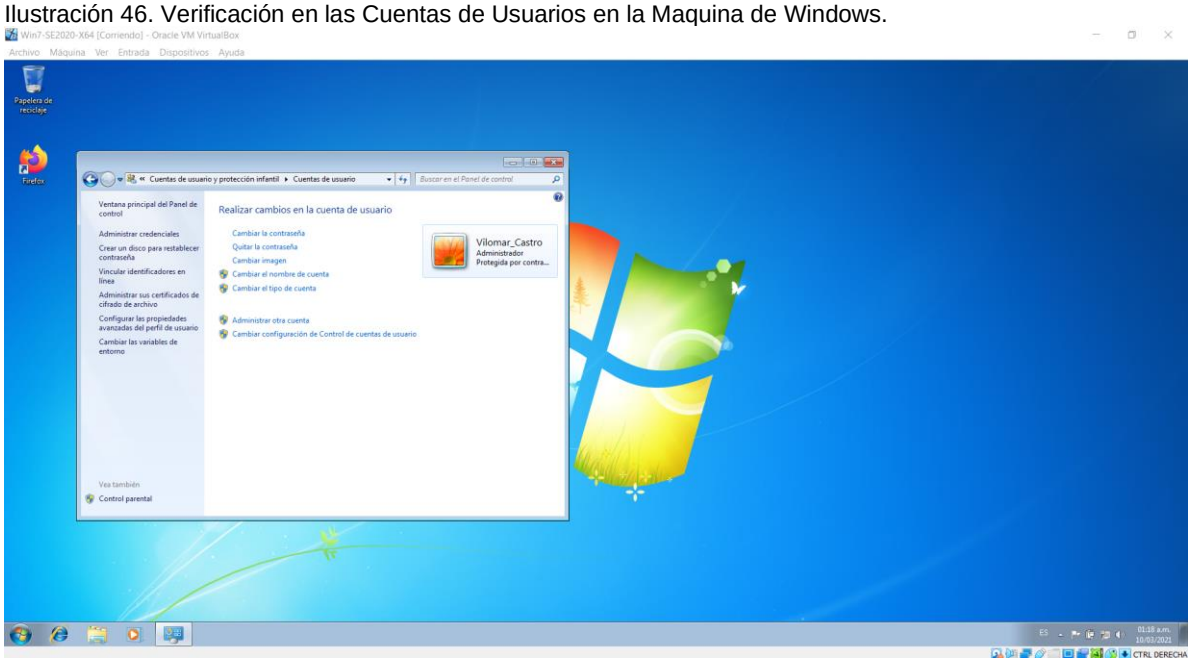
Ilustración 45. Listado de los Grupos en la Maquina de Windows.



Fuente. El Autor.

Verificamos en las cuentas de usuarios la creación y los privilegios de nuestro usuario **Vilomar_Castro**.

Ilustración 46. Verificación en las Cuentas de Usuarios en la Maquina de Windows.



Fuente. El Autor.

8.2. **ANÁLISIS DE ACCIONES NECESARIAS PARA LA CONTENCIÓN DE UN ATAQUE EN TIEMPO REAL.**

Mediante el presente análisis situacional, se pretende dar a conocer las diferentes acciones o mecanismos de contención empleados al momento de ser víctimas de un ataque en tiempo real, lo anterior con el único fin de mitigar el grado de exposición y comprometimiento del sistema informático objeto de los cibercriminales. Por lo anterior se proceden a mencionar a continuación las diferentes acciones para tener en cuenta al momento de ser víctimas de un ataque en tiempo real.

8.2.1. IDENTIFICACIÓN DEL VECTOR DE ATAQUE EMPLEADO POR LOS CIBERDELINCUENTES. Como una acción inicial a realizar al momento de ser víctimas de un ataque informático en tiempo real, se considera la identificación del vector de ataque (exploit) empleado por el o los atacantes, esto con el fin de identificar la clase de vulnerabilidad existente en el sistema la cual es motivo del presente ataque.

8.2.2. IDENTIFICACIÓN DEL HOST COMPROMETIDO EN EL PRESENTE ATAQUE. Se procede a la identificación de el o los hosts comprometidos durante el presente ataque informático, lo anterior con el fin de aislar los equipos comprometidos de la red y así poder mitigar el grado de exposición al cual se pueden ver expuestos el resto de los dispositivos que conforman la infraestructura de la compañía.

Mediante el aislamiento de los equipos comprometidos en un ataque en tiempo real, se pueden prevenir técnicas como el pivoting que el atacante puede realizar en aras de saltar del sistema informático inicialmente comprometido al resto de los dispositivos de la red, razón por la cual cobra mucha importancia la identificación y aislamiento de los sistemas comprometidos, así evitar la técnica antes mencionada.

8.2.3. ANÁLISIS DE VULNERABILIDADES EN EL HOST COMPROMETIDO EN EL ATAQUE. Una vez identificado el dispositivo comprometido en el ataque y posterior a su aislamiento del resto de la infraestructura de red, se procede a realizar un análisis de vulnerabilidades existentes en este host, así como el nivel de impacto y facilidades que generan al atacante las vulnerabilidades halladas.

Como resultado del procedimiento anterior, validaremos si para las vulnerabilidades halladas se documentan en los repositorios oficiales exploit´s para su explotación o si por el contrario son vulnerabilidades de día Zero, de las cuales se resalta que a estas últimas se les define como vulnerabilidades de las cuales no se tiene conocimiento alguno de su existencia, modos de explotación o impacto en un sistema informático por ser de único conocimiento del agente que perpetua el ciberataque, razón por la cual no se podría subsanar con prontitud.

8.2.4. EXPLOTACIÓN DE LAS VULNERABILIDADES HALLADAS EN UN AMBIENTE CONTROLADO. Una vez identificadas las vulnerabilidades existentes en el sistema informático comprometido por el atacante, se procede a realizar su explotación en un ambiente controlado, para esto se emplean bancos de trabajo en entornos simulados en los cuales, mediante la recreación de los sistemas comprometidos a nivel de Hardware y Software, se recrean los posibles ataques mediante la utilización de herramientas como Metasploit, Armitage, Cross Site Scripting (XSS), entre otros.

Como resultado del procedimiento anterior, podemos determinar el impacto y grado de exposición causado por la explotación de la vulnerabilidad encontrada y si mediante esta sería posible la escalación de privilegios en el sistema y así poder realizar la exfiltración de información en el sistema comprometido.

8.2.5. REMEDIAR LAS VULNERABILIDADES EXISTENTES EN EL SISTEMA COMPROMETIDO. Apoyados en los resultados de las pruebas descritas en el aparte anterior, procedemos a implementar medidas para subsanar las vulnerabilidades previamente identificadas y halladas en el sistema comprometido. Como medidas a implementar a continuación describimos las siguientes.

- Actualizaciones de Seguridad. Se deben implementar en los sistemas operativos comprometidos, las ultimas actualizaciones de seguridad liberadas por el fabricante y así contar con los diferentes parches de seguridad actualizados a las ultimas vulnerabilidades conocidas.

- Actualizaciones de Antivirus. Es vital contar con las bases de datos de los antivirus actualizadas a la fecha y así contar con las ultimas protecciones a los virus y malware de los que se tiene conocimiento a la fecha.

- Actualizaciones del Firmware para los IDS, IPS, Firewall y WAF que integran la Infraestructura de Red. Los dispositivos mencionados en este aparte deben de contar con las ultimas actualizaciones de Firmware liberadas por el fabricante para el modelo de nuestro interés, estas contarían así con las ultimas políticas de contención para las amenazas registradas en sus bases de datos.

- Parchear las vulnerabilidades previamente halladas. Se deben implementar los diferentes parches de seguridad en el sistema informático comprometido en el ataque, estos se deben aplicar tanto a nivel del sistema operativo anfitrión como a las aplicaciones, servicios y puertos en los cuales se aloja la vulnerabilidad explotada.

- Creación de Reglas en los dispositivos de seguridad perimetral. Por ultimo y no por eso menos importante, se crean reglas en los diferentes equipos de seguridad perimetral con los que cuenta nuestra infraestructura de red, como lo son los IDS, IPS, Firewall, WAF. Para estas reglas debemos hacer énfasis en los servicios y puertos comprometidos en el presente ataque, evitando así las posibles conexiones de agentes sospechosos a la red, los cuales pueden pretender la intrusión a la infraestructura de red para así lograr la exfiltración de datos y creación de puertas traseras (Back Door´s) garantizando el acceso para futuros ataques.

9. ASPECTOS QUE APORTAN AL DESARROLLO DE ESTRATEGIAS DE RED TEAM & BLUE TEAM.

Como aspectos relevantes para el desarrollo de estrategias de Red Team & Blue Team en una organización, podemos resaltar los siguientes:

- Elaboración por parte de la compañía de las políticas de seguridad de la información para la organización.
- Estructuración del manual de procedimiento para el manejo de incidentes informáticos.
- Contar con un manual de procedimientos de recuperación ante un incidente.
- Definir políticas para el uso de la infraestructura IT de la organización.
- Establecer procedimientos para la creación de puntos de restauración.
- Manejo de procedimientos para conexiones remotas seguras a través de VPN.
- Configurar políticas en los dispositivos de seguridad perimetral, como los Firewall, WAF, IDS, IPS.
- Contar con procedimientos y herramientas para el análisis de incidentes en tiempo real.
- Promover campañas de sensibilización a los colaboradores de la compañía para el correcto uso de la infraestructura IT.
- Definir y socializar en la compañía el directorio de contactos del área responsable para el manejo de incidentes informáticos.

10. ESTRATEGIAS QUE PERMITEN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN.

Tomando como antecedente el ataque realizado a través de la vulnerabilidad rejetto en su versión 2.3, estudiado en la etapa 3 del ejercicio de Red Team y como miembros activos del equipo de Blue Team, con la finalidad de mitigar el grado de exposición que tendríamos en un futuro al interior de la compañia, implementaremos medidas de hardenización con el fin de fortalecer los dispositivos de cómputo, red y seguridad perimetral que conforman la infraestructura de red de la compañía.

Por lo anterior a continuación se plantean una seria de políticas estrategicas de seguridad para el correcto uso de los sistemas informáticos de la organización WhiteHouse Security, mediante las cuales se incentive el uso adecuado de los dispositivos de cómputo y de red que conforman la infraestructura IT de la compañía, así:

10.1.1. POLÍTICA PARA EL USO CORRECTO DE LOS EQUIPOS DE COMPUTO. En esta se especifica a los usuarios de la compañía del uso correcto de los equipos de cómputo pertenecientes a la empresa WhiteHouse Security, por lo anterior los usuarios deben garantizar que el uso de los equipos de cómputo es solo para fines de las actividades por causa o acción de las funciones propias del cargo, de lo anterior se denota que en estos equipos no se permite el almacenamiento de información o instalación de aplicaciones no requeridas para el desempeño de sus funciones.

10.1.2. POLÍTICA PARA EL USO ADECUADO DEL CORREO. Mediante la expedición y socialización de esta política, se da a conocer a los empleados de la compañía el correcto uso del correo electrónico corporativo, esto manifestado en la no utilización de este para el envío o recepción de mensajería con motivos ajenos a las funciones desempeñadas por su cargo en la empresa, sin importar el tipo de comunicaciones enviadas o recibidas a través de este. Adicional a lo antes expuesto, se prohíbe emplear el correo electrónico corporativo para realiza el registro en servicios web no propios de actividades corporativas.

10.1.3. POLÍTICA DE INSTALACIÓN DE SOFTWARE NO AUTORIZADO. Mediante la implementación de esta política, se pretende limitar la instalación y uso de Software o aplicativos ajenos a los autorizados por la organización, lo anterior debido a que estos pueden llegar a proceder de fuentes no confiables, con lo cual se pueden generar software mal intencionado alojado en la aplicación instalada de procedencia aparentemente legitima.

Como complemento a lo anterior, se aclara que no está autorizado el uso de software pirata para la realización de las actividades de la compañía, por lo que de llegar a requerir el usuario de un software específico que no exista en la empresa, este requerimiento debe de ser escalado al área respectiva para su adquisición.

10.1.4. POLÍTICA DE USO DEL ANTIVIRUS Y FIREWALL. El usuario de los dispositivos de cómputo de la compañía, en ninguna circunstancia se podrá desinstalar o en su defecto deshabilitar el antivirus y firewall instalado en el Pc, por lo anterior se dispondrá de una contraseña de administración de este la cual estará en custodia del personal IT responsable de la administración de esta.

Entendiendo, la naturaleza de las actividades del personal que requieran la deshabilitación del antivirus y firewall instalados en su Pc, estas deberán hacer la solicitud formal en la cual justifican tal acción y así obtener el soporte por parte del

área encargada.

10.1.5. POLÍTICA PARA USO DE DISPOSITIVOS DE ALMACENAMIENTO CD-DVD-USB. Los usuarios que llegasen a requerir para el cumplimiento de su función, el uso de dispositivos de almacenamientos externos deberá realizar un análisis completo mediante el antivirus corporativo instalado en su Pc, esto con el fin de prevenir la infección del sistema con posibles virus u malware informático a través de estos dispositivos. No obstante, es de aclarar que los dispositivos externos autorizados para su utilización en las actividades de la compañía son los suministrados para el desempeño de sus funciones, previa revisión del área de IT responsable.

10.1.6. POLÍTICA PARA EL USO DE ACCESO REMOTO A DISPOSITIVOS. Se enfatiza a los usuarios de la infraestructura IT de la compañía, y en el caso de requerir para el cumplimiento de sus funciones el acceso remoto a los equipos tanto de cómputo como de red, el empleo de conexión a través de la VPN suministrada por la compañía para este tipo de requerimientos, por lo anterior no se encuentra autorizado el uso de aplicativos u herramientas para este tipo de conexiones, ajenas a la suministrada por WhiteHouse Security.

Por lo anterior, en aras de que el colaborador requiera este tipo de conexión, deberá solicitar al administrador IT a través de correo corporativo, las credenciales requeridas para garantizar la conexión.

10.1.7. POLÍTICA PARA EL MANEJO DE CREDENCIALES DE ACCESO. La finalidad de la presente política es dar a conocer a los usuarios de los diferentes dispositivos que componen la infraestructura IT de la organización, que está totalmente prohibido el préstamo o suministro de sus credenciales de acceso a personal ajeno a su destinatario. De igual forma se resalta que el colaborador no debe suministrar sus credenciales para facilitar así el acceso a áreas donde se restringe el acceso o se clasifica su acceso al mismo.

Dado lo anterior, se recuerda a los colaboradores, el cambio periódico de las credenciales de acceso a su Pc y aplicativos a los cuales aplique la presente política, al igual que garantizar el almacenamiento seguro de sus credenciales, esto con el fin de mitigar el grado de exposición a ataques de ingeniería social a los cuales se puedan ver expuestos.

10.1.8. POLÍTICA DE BACKUPS DE LA INFORMACIÓN. Se aclara a todos los usuarios, la necesidad de realizar copias de respaldo periódicas de la información almacenada en los dispositivos asignados, estos pueden ser Pc y Smartphone, almacenando estas en un lugar seguro el cual garantice la integridad de la información de respaldo, en caso de que el usuario llegara a requerir un punto de restauración confiable.

10.1.9. POLÍTICA PARA EL MANTENIMIENTO DE LOS EQUIPOS DE COMPUTO. Se agendará según cronograma, previamente establecido por el área de IT de WhiteHouse Security, los mantenimientos preventivos periódicos a los equipos de cómputo de la compañía, en estos se validará el estado actual del equipo a nivel de Hardware como de las aplicaciones o Software instalado en el mismo.

10.1.10. POLÍTICA PARA LAS AUDITORIAS A LOS SISTEMAS INFORMÁTICOS. La compañía WhiteHouse Security, se apoyará por equipos externos de Red Team & Blue Team, para la realización de auditorías especializadas a los sistemas informáticos e infraestructura de red, propiedad de la compañía, con lo cual se pretende mitigar el grado de exposición a posibles vectores de ataque a los cuales se puede encontrar expuesta.

Para las auditorías a los sistemas informáticos, como pueden ser servicios Cloud o aplicativos virtualizados a través de infraestructura de terceros, la compañía solicitara a estos los respectivos informes en los cuales se detalle el estado actual de la operación de los sistemas como de los mecanismos implementados para mitigar su exposición a las amenazas informáticas actuales.

10.1.11. POLÍTICAS PARA EL USO DE SOFTWARE DE TRANSFERENCIA DE ARCHIVOS. Tomando como base la vulnerabilidad hallada en la aplicación rejetto v 2.3, se prohíbe el uso de servidores para transferencia de archivos, lo anterior sin previa validación por parte del área de IT de la compañía, como única finalidad la de evitar las posibles conexiones, exfiltración de información y puertas traseras que este tipo de aplicaciones puede generar y así el llegar a comprometer la integridad de los sistemas informáticos e infraestructura de la compañía WhiteHouse Security.

10.1.12. POLÍTICA PARA LA CREACIÓN DE REGLAS EN LOS DISPOSITIVOS INFORMÁTICOS DE SEGURIDAD PERIMETRAL. El equipo Blue Team de la compañía WhiteHouse Security, dada la necesidad técnica se ve en la obligación de crear reglas y políticas estrictas en particular para los servicios a través de conexiones HTTP, para cada uno de los dispositivos de seguridad perimetral, como lo son FIREWALL, WAF, IDS, IPS. Mediante estas políticas se realizara un control y filtrado de tráfico a través de servicios y puertos, estos tomando como antecedente el ataque al cual se vio expuesta mediante la aplicación rejetto v 2.3, para lo cual se realiza un estricto control al flujo de datos generado a través del puerto 80, 8080, 4444 y 49171, puertos en los cuales gracias al análisis previo del equipo de Red Team para nuestro caso se encuentra alojado y se estableció la sesión de Meterpreter del servicio HttpFile Server httpd 2.3, el cual es la aplicación rejetto v 2.3.

11. ANÁLISIS SOBRE LAS DIFERENCIAS ENTRE UN EQUIPO DE BLUE TEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS.

Los equipos de Blue Team se encuentran conformados por profesionales en el campo de la ciberseguridad, los cuales apoyados en herramientas tecnológicas de inteligencia artificial y algoritmos de perfilamientos complejos lo cual le permita con una mayor velocidad de análisis la identificación, rastreo y modelado de las posibles amenazas que puedan llegar a impactar a una organización, para así lograr establecer medidas o estrategias que contribuyan con la mitigación de estas amenazas para la operación de la compañía. Por lo anterior se puede concluir que los equipos de Blue Team, mediante un análisis en el comportamiento o hábitos de los usuarios de los sistemas de una empresa, pueden llegar a determinar las medidas de contención frente a nuevas o existentes o nuevas amenazas que puedan llegar a atentar contra la infraestructura tecnológica de una empresa.

Por otra parte, a diferencia de los equipos Blue Team, los equipos de respuesta a incidentes informáticos (CSIRT), tienen como finalidad la de actuar frente a la existencia de incidentes informáticos que comprometan la infraestructura de una organización, por lo anterior los CSIRT, actúan frente a un evento, entiéndase este como vulnerabilidad, comprometimiento e intrusión a un sistema informático, ante lo cual se encargaran de implementar las medidas técnicas correctivas que permitan la recuperación ante el incidente y así lograr garantizar la continuidad del negocio con la menor afectación posible.

Por lo anterior, la misión de los equipos CSIRT en una compañía, cobra una gran importancia no solo mediante su función reactiva frente a un incidente informático, sino a su vez en su actuar proactivo ante la prevención de posibles vectores de ataques, esto apoyándose en el intercambio de información de incidentes con otros equipos.

12. ANÁLISIS SOBRE LA PERTINENCIA DE TRABAJAR CON CIS COMO PROPUESTA DE ASEGURAMIENTO POR PARTE DE UN EQUIPO BLUE TEAM.

Las ventajas resultantes de articular el trabajo de un equipo de Blue Team con CIS (Center For Internet Security), se fundamentan en la capacidad de contar con políticas y mecanismos estructurados por un equipo multisectorial de orden Internacional, el cual mediante la implementación de controles y políticas actualizadas nos suministra las herramientas necesarias para afrontar los desafíos en materia de riesgos Cibernéticos de la actualidad, presentes en Internet.

Como miembros de un Equipo de Blue Team, dentro del cual apoyamos nuestros procedimientos con CIS, obtenemos múltiples beneficios entre los cuales soporte con herramientas de ciberseguridad, estas con el fin de mitigar las posibles amenazas e incidentes informáticos a los cuales nos podemos ver expuestos en el día a día.

Como prestación adicional, el hecho de saber que CIS soporta su operación de monitoreo de incidencias de manera continua y como resultado posterior socializa mediante informes la existencia de las nuevas vulnerabilidades y amenazas que surgen cada día en Internet, lo cual nos brinda un aprendizaje adelantado de las medidas a implementar para contrarrestar el grado de exposición a estas vulnerabilidades.

Por último, al interactuar CIS con diferentes sectores de la economía y al ser una organización sin ánimo de lucro, nos facilita como equipo Blue Team el contar con herramienta orientadas hacia cada sector en el cual se fundamente la operación de la compañía a la cual soportemos.

13. ANÁLISIS DE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM.

El sistema o software SIEM es aquel que facilita a la organización el análisis de la información de los sistemas junto con el análisis de eventos presentes en el mismo, esto es posible mediante una gestión unificada de información, la cual mediante la utilización de un correlacionador de eventos le facilita al personal del área de IT, identificar las amenazas reales de los falsos positivos que se puedan presentar en la infraestructura IT de la compañía.

Lo anterior es posible gracias a la capacidad de gestión y procesamiento ágil de los datos procesados a través del software SIEM, brindándole al área encargada de la compañía, información veraz respecto al análisis de vulnerabilidades y gestión de estas.

En su estructura un software SIEM esta soportado por la gestión de eventos de seguridad (SEM) y la gestión de información de seguridad (SIM). SEM se encarga de la monitorización y correlación en tiempo real de los eventos, mientras que SIM utiliza la información generada por SEM para almacenarla y generara reportes de auditoria basados en estos datos.

Como parte de las funciones principales que compone a un sistema SIEM, podemos resaltar las siguientes:

13.1.1. FACILITA LA VISUALIZACIÓN DE POSIBLES AMENAZAS. Gracias a la implementación del SIEM, las compañías tienen un informe en tiempo real de las diferentes amenazas a las cuales se encuentra expuesta su infraestructura TI, por lo cual pueden implementar las contramedidas requeridas para su mitigación.

13.1.2. CLASIFICACIÓN DE AMENAZAS REALES DE FALSOS POSITIVOS. Gracias a esta función del SIEM, el personal administrador del sistema puede clasificar las amenazas reales de los falsos positivos, esto permitiendo así una mejor

gestión del recurso tecnológico y humano de la compañía, evitando el desgaste del personal para la atención de eventos de menor impacto.

13.1.3. DOCUMENTACIÓN DE EVENTOS DE SEGURIDAD. Facilita la documentación de los eventos de seguridad que fueron atendidos por los responsables del sistema, lo cual traduce en la capacidad de generar informes veraces de auditorías que reflejen la trazabilidad de cada evento gestionado por los responsables del área encargada de la compañía.

13.1.4. CUMPLIMIENTO DE LAS REGULACIONES. Gracias a la estructura de la información generada, enmarca los informes generados dentro de los estándares definidos por la industria, lo cual facilita su análisis y entendimiento.

13.1.5. EVALUACIÓN DE VULNERABILIDADES. Otorga la capacidad de evaluar las vulnerabilidades reales del sistema y el grado de exposición a la misma, lo cual nos otorga una mejor gestión de los incidentes en orden de prioridades según su impacto a la infraestructura IT de la compañía.

13.1.6. MONITOREO. Permite el monitoreo en tiempo real de los sistemas, lo cual se traduce en la reducción de los tiempos de respuesta ante la posibilidad de un incidente que impacte la continuidad del negocio de la compañía.

13.1.7. ANÁLISIS Y CORRELACIÓN DE LOGS EN TIEMPO REAL. Como otra de las funcionalidades del sistema SIEM, encontramos la de analizar y correlacionar los datos ingresados al sistema con el fin de validar el estado actual del mismo frente a posibles riesgos informáticos que atenten contra la estabilidad de la infraestructura IT de la organización.

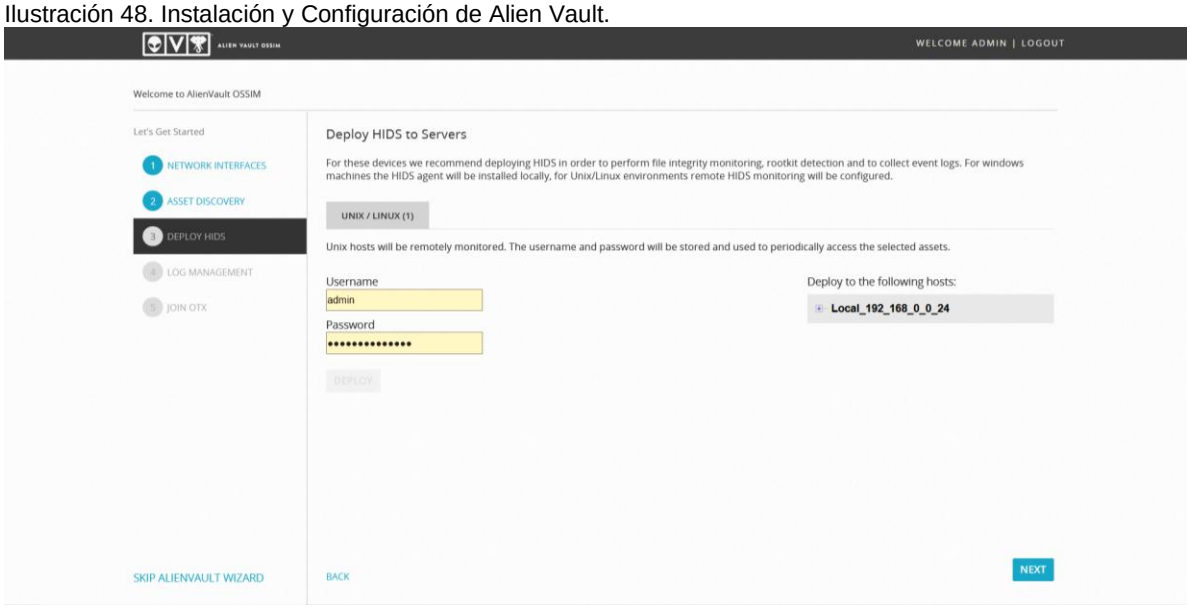
13.1.8. INFORMACIÓN DE APOYO PARA ANÁLISIS FORENSE. Gracias a la gestión y manejo de la información que se realiza a través del sistema SIEM, se facilita el soporte para la labor de un análisis forense de determinado incidente informático.

13.1.9. DETECCIÓN DE VIOLACIONES. Los SIEM facilitan la detección de posibles violaciones o intrusiones de seguridad a las infraestructuras IT de una organización, lo cual se traduce en una mejor capacidad de gestión del riesgo dentro del marco de las políticas de seguridad implementadas por la compañía.

13.1.10. AUTOMATIZACIÓN DE TAREAS. Como parte de sus facilidades, los SIEM cuentan dentro de sus capacidades con la automatización de tareas, esto se traduce en una optimización para la asignación del recurso humano en la gestión de un incidente de seguridad.

En la siguiente imagen, para fines ilustrativos procedimos a instalar bajo un entorno de virtual un software empleado para SIEM como lo es Alien Vault.

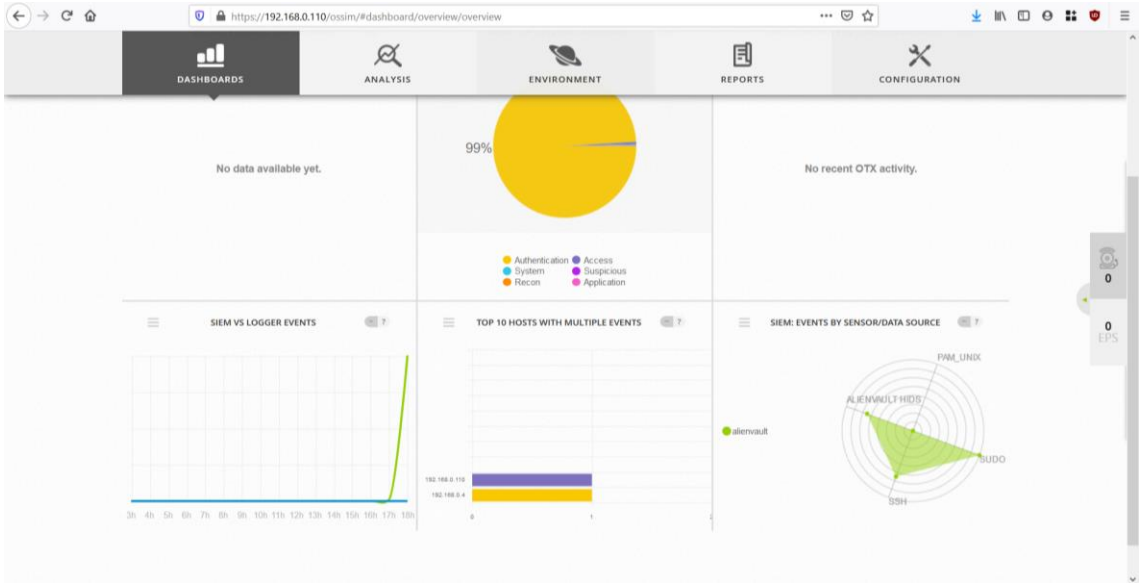
Ilustración 48. Instalación y Configuración de Alien Vault.



Fuente. El Autor.

Posterior a la configuración inicial e ingreso con las credenciales de acceso establecidas, de ingresa al entorno de presentación en el cual se obtiene datos primarios basados en el segmento de red en el cual nos encontramos, lo cual se evidencia en la siguiente imagen.

Ilustración 49. Dashboards OSSIM Alien Vault.



Fuente. El Autor.

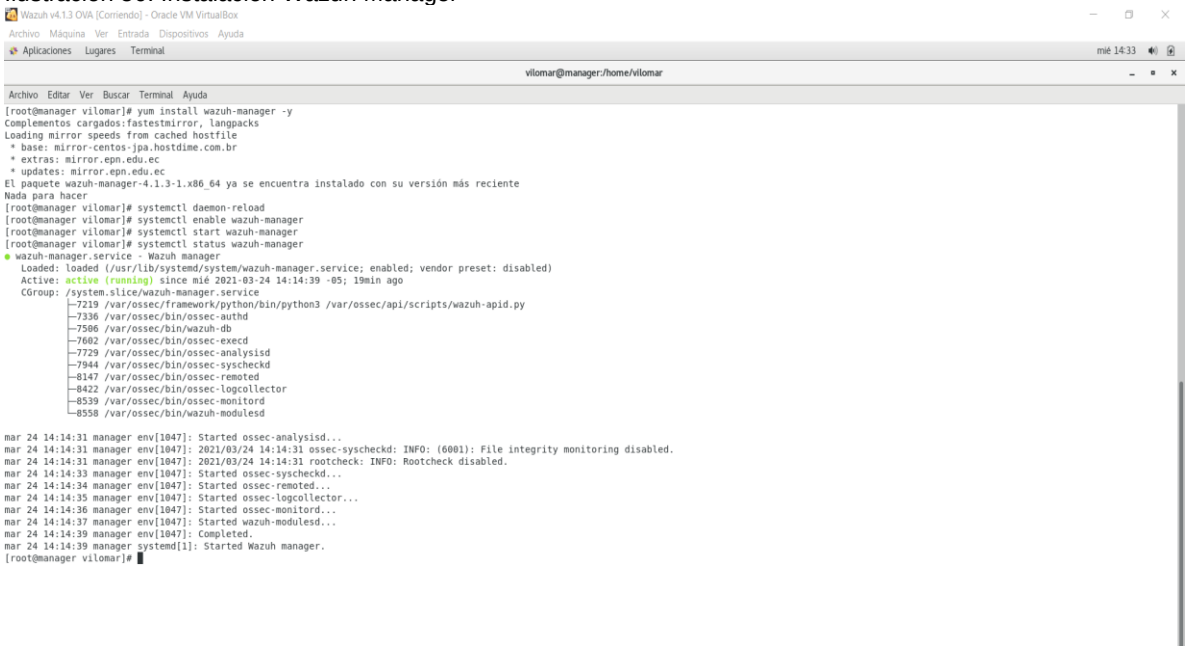
14. INFORME DE HERRAMIENTAS PARA LA CONTENCIÓN DE ATAQUES INFORMÁTICOS.

En el presente apartado, procederemos a describir una selección de herramientas las cuales nos son de apoyo para la contención de ataques informáticos hacia la infraestructura IT de una compañía.

14.1.1. WAZUH. Es una herramienta Open Source dotada de varias funcionalidades con el único fin de contribuir a la contención de posibles ataques informáticos.

Para su correcta instalación, wazuh consta de un instalador para servidor en Linux (Manager) y en el otro extremo se encontraría la versión del cliente, la cual para nuestro caso se instaló en nuestra maquina Windows 7 X64 Cabe resaltar que la aplicación cliente (Agent) requiere de registrarse al servidor para así obtener la llave de registro para su funcionalidad, como se evidencia en la siguiente imagen.

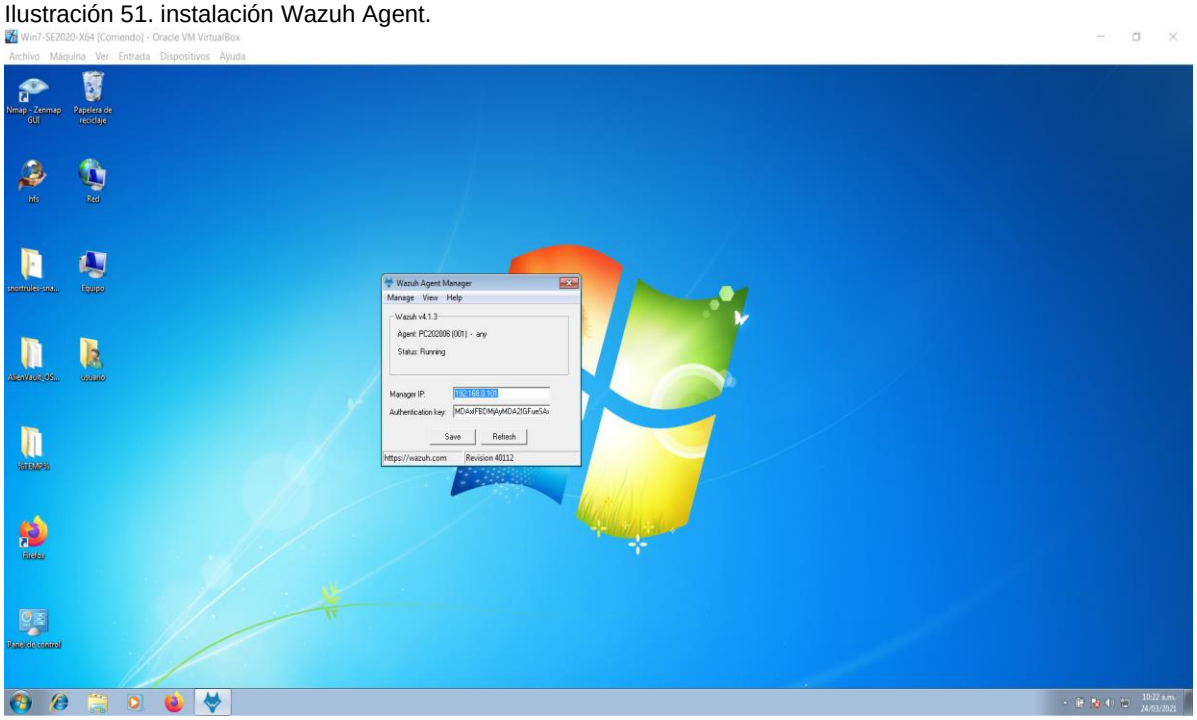
Ilustración 50. Instalación Wazuh Manager



Fuente. El Autor.

Para fines demostrativos, se instaló la aplicación de Wazuh Agent, el cual sería nuestro cliente alojado en nuestro entorno virtual de Windows 7 X64, para lo cual se relaciona la siguiente imagen.

Ilustración 51. instalación Wazuh Agent.

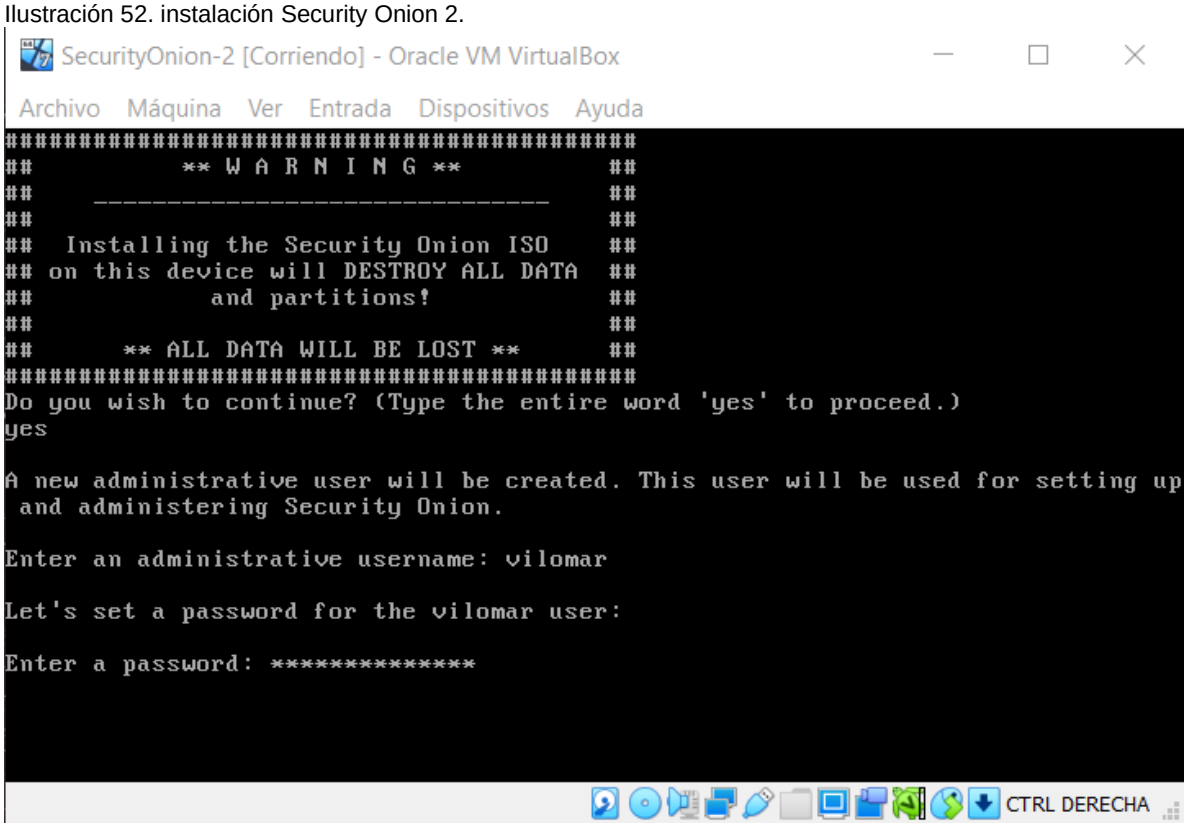


Fuente. El Autor.

14.1.2. SECURITY ONION 2. Se le conoce como una distribución Open Source de Linux, posee entre sus funcionalidades o características a resaltar el monitoreo de seguridad para redes empresariales, gestión de logs y threat hunting, esto fortaleciendo como una herramienta con múltiples bondades para la contención de los posibles ataques informáticos a los cuales se encuentran expuestas las organizaciones.

Por lo anterior y para efectos ilustrativos se relaciona imagen donde se evidencia el entorno inicial para la instalación de la herramienta.

Ilustración 52. instalación Security Onion 2.



Fuente. El Autor.

14.1.3. SNORT. Es una herramienta Open Source la cual dentro de su característica más familiar resalta su aplicación como un sistema de prevención de intrusiones (IPS).

Como mecanismos principales para su operación, este emplea un conjunto de reglas las cuales le permiten detectar conexiones maliciosas a la red y así generar las alertas ante posibles eventos informáticos maliciosos.

14.1.4. Fail2ban. Esta se denota como una aplicación escrita en el lenguaje de programación Python la cual se emplea con la finalidad de prevenir las eventuales intrusiones a un sistema.

El modo de operación de esta herramienta se basa en el bloqueo para la posterior penalización a aquellas conexiones externas, cuyo único fin es ingresa a una infraestructura de red mediante ataques de fuerza bruta, esto en apoyo a las reglas configuradas en dispositivos de seguridad perimetral, como lo es un firewall.

CONCLUSIONES

Mediante la realización de esta actividad se lograron conocer las legislaciones vigentes para Colombia en lo referente a las conductas tipificadas como delitos informáticos, al igual que las directrices impartidas por el estado colombiano en temas de protección de datos personales.

Además, introducir al lector en lo referente al tema de la ciberseguridad, en especial en lo que respecta a las buenas prácticas de Red Team & Blue Team, dentro de las cuales se hace énfasis en el Pentester como disciplina fundamental para garantizar la integridad, confiabilidad y disponibilidad de la información de un organismo o entidad contratante de estos servicios profesionales.

Se logró inducir al lector a adentrarse en el innovador, pero al igual desafiante mundo del Red Team & Blue Team como carrera profesional dentro del campo de la seguridad de la información al tiempo que fue posible analizar el actuar ilegal en los procesos de la compañía WhiteHouse Security, evidenciado mediante el acuerdo de confidencialidad propuesto por esta última para los futuros integrantes de los equipos Red Team & Blue Team, específicamente en las cláusulas que aducen a la ilegalidad para el cumplimiento del desempeño de las funciones de estos aspirantes al cargo.

Gracias al conocimiento previo de la Ley 1273 de 2009, se lograron identificar todos los matices que se pueden encontrar en compañías de esta envergadura, líderes en el mercado de la ciberseguridad. De allí, que basándose en el código de ética que regula el actuar profesional como futuros expertos en ciberseguridad, sea posible discernir entre una propuesta laboral honesta y sobre todo que opere bajo el marco legal colombiano para esta profesión y otra en la que se ponga en tela de juicio la moral, ética y los valores tanto personales como profesionales, característicos de los profesionales en seguridad de la información.

Aunado a ello, con esta auditoria fue posible evidenciar diferentes tipos de vulnerabilidades a las cuales se encuentran expuestas las organizaciones, en el día a día de su operación, indistintamente de la naturaleza o el sector bajo el cual se desarrolle la misma.

Se puso en conocimiento, por medio de la aplicación de una prueba de concepto, liderada por el equipo de Red Team, la presencia de una vulnerabilidad, misma que se asocia a una aplicación que en apariencia no genera ningún grado de exposición y permite el comprometimiento de equipos de la red interna de una organización, posibilitando que el atacante logre la exfiltración del activo más valioso de la compañía, su información.

En este orden, el ejercicio de investigación permitió informar a la alta gerencia de la compañía, el grado de exposición al cual se encuentra expuesta, sea esta por omisión de las diferentes políticas implementadas o por falta de socialización de estas, con el fin de fomentar una cultura receptiva hacia la ciberseguridad en todos sus niveles y en busca finalmente de la mejora continua para cada uno de sus procesos. Es así, como dar a conocer la importancia del rol desempeñado por los equipos Blue Team, ayuda a garantizar la integridad en las operaciones de la infraestructura IT en las organizaciones, indistintamente del sector bajo el cual se desarrolle la misma.

De otro lado, fue posible identificar y socializar las diferentes medidas de contención generadas de manera articulada entre el personal de TI y los equipos Blue Team, para así poder, con su implementación, mitigar el grado de exposición al cual se encuentran sometidas día a día las infraestructuras informáticas de las empresas.

Como plus final de este informe, es clave resaltar la socialización de los diferentes organismos y herramientas de ciberseguridad, esto con el objetivo de apoyar y soportar de manera articulada los mecanismos de contención a implementar en las organizaciones, en pro de reducir la superficie de exposición a los incidentes informáticos de la actualidad.

RECOMENDACIONES

- Asignación por parte de la compañía WhiteHouse Security del recurso humano calificado, para la estructuración y generación de los contratos y acuerdos laborales para el personal a integrar los equipos de Red Team & Blue Team.

- Estructurar los acuerdos de confidencialidad para el personal que integrara los equipos de Red Team & Blue Team, en base al marco regulatorio colombiano e internacional, esto alineado con la naturaleza de las funciones a desempeñar por parte del futuro colaborador.

- Consignar como clausula a resaltar en el acuerdo de confidencialidad, los actuares y procedimientos realizados para el cumplimiento de las funciones asignadas para los colaboradores, estarán alineadas con la leyes y decretos veedores de la protección de datos personales e integridad de los sistemas de información e infraestructuras IT.

- Restringir la instalación y el uso de software libre y pirata en los dispositivos de computo y red de la organización, esto con el fin de evitar posibles brechas informáticas que llegasen a comprometer la infraestructura IT de WhiteHouse Security.

- Restringir el uso de dispositivos de almacenamiento externos no suministrados por la compañía para el cumplimiento de las funciones de sus colaboradores, esto con la finalidad de evitar posibles infecciones a través de malware o virus informáticos al interior de la organización.

- Realizar manteniemientos preventivos y correctivos periódicos de los equipos de computo y dispositivos de red que integrar la infraestructura IT de la organización.

- Concientizar a los colaboradores de WhiteHouse Security, acerca de la importancia de realizar copias de seguridad periódicas de su información, almacenando estas en un lugar seguro para su posterior acceso en caso de requerir un punto de restauración.

- Implementar las actualizaciones a las últimas versiones de firmware y parches de seguridad de los dispositivos de seguridad perimetral, liberadas por los fabricantes de las marcas que integren la infraestructura IT de WhiteHouse Security.

- Aplicar de manera periódica las ultimas actualizaciones de seguridad liberadas para los diferentes sistemas operativos instalados en los equipos de cómputo de WhiteHouse Security.

- Configurar reglas para el filtrado de contenido Web en los WAF, esto en aras de contralar y filtrar el tráfico hacia y desde la internet de los colaboradores de la compañía.

- Establecer políticas de seguridad, en dispositivos de seguridad perimetral como Firewall, IDS y IPS, las cuales contribuyan al fortalecimiento de la infraestructura IT, propiedad de la compañía WhiteHouse Security.

- Configurar políticas estrictas para el filtrado de servicios y puertos para conexiones a través del puerto 80 y trafico mediante el protocolo HTTP.

- No almacenar contraseñas o credenciales de acceso a los diferentes dispositivos de uso corporativos (Pc, Smartphone, locaciones), en lugares visibles y vulnerables ante un ataque mediante ingeniería social.

- No compartir el uso de las credenciales de acceso a dependencias con personal no autorizado para el ingreso y uso de estas.

- Realizar un correcto uso del correo corporativo, esto se traduce en no generar, recibir o reenviar información (archivos adjuntos), a través de este al interior de la organización.

- No emplear el correo corporativo para el registro en portales, aplicaciones o páginas web, las cuales no sean para uso exclusivo de las funciones estipuladas ´para el cargo del colaborador.

- El colaborador tendrá la obligación de reportar cualquier comportamiento sospechoso generado a través de su equipo de cómputo.

- Realizar por parte del área de Seguridad informática de WhiteHouse Security, revisiones periódicas del log de eventos de los dispositivos que conforman la infraestructura IT, esto en aras de identificar y evaluar cualquier situación que altere el buen performance de los sistemas.

- Programar auditorias a los sistemas de información de la compañía WhiteHouse Security, mediante el uso de técnicas de Red Team & Blue Team.

- Solicitar a los proveedores de servicios de aplicativos tercerizados (Cloud), los informes de las auditorias en las cuales se evidencia el estado e integridad de los servicios contratados.

- Consultar de manera periódica la existencia de nuevas vulnerabilidades informáticas en los repositorios internacionales creados para tal fin, esto con el fin de implementar las contramedidas que contribuyan con la mitigación ante posibles eventos informáticos.

- Estructurar, generar y socializar con los colaboradores de WhiteHouse Security, las políticas de seguridad de información de estricto cumplimiento para el suso y buen desempeño de la infraestructura IT de la organización.

- Generar conciencia en los usuarios de los sistemas de información de la compañía, de la importancia de hacer un correcto uso de los dispositivos e infraestructura destinada por la empresa para el cumplimiento de sus funciones.

- Realizar campañas periódicas de socialización respecto a la importancia del cumplimiento de cada una de las políticas de seguridad de la información generadas por la compañía.

BIBLIOGRAFÍA

CONGRESO DE COLOMBIA. Ministerio del Interior y de Justicia. Ley N°1273. 5 de enero de 2009. Bogotá. 2009.

CONCEJO PROFESIONAL NACIONAL DE INGENIERÍA. Código de Ética para el Ejercicio de la Ingeniería en General y sus Profesiones Afines y Auxiliares.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI. Anexo 2 – Escenario 2.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI. Anexo 3 – Acuerdo.

ASTUDILLO, Karina. Escaneo. Karina ASTUDILLO. *Hacking Ético.* Tercera Edición. Bogotá: Ra-Ma, 2019, Pag 82-91. ISBN: 978-958-792-094-9.

ASTUDILLO, Karina. Escalamiento de Privilegios. Karina ASTUDILLO. *Hacking Ético.* Tercera Edición. Bogotá: Ra-Ma, 2019, Pag 261-266. ISBN: 978-958-792-094-9.

ASTUDILLO, Karina. Metasploit Framework. Karina ASTUDILLO. *Hacking Ético.* Tercera Edición. Bogotá: Ra-Ma, 2019, Pag 121-149. ISBN: 978-958-792-094-9.

ASTUDILLO, Karina. Armitage. Karina ASTUDILLO. *Hacking Ético.* Tercera Edición. Bogotá: Ra-Ma, 2019, Pag 162-170. ISBN: 978-958-792-094-9.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI. Anexo 4 – Escenario 3.

Recuperado en: http://www.fastandeasyhacking.com// (consulta: 3 de marzo de 2021).

SANS, Kurtis Holland. Incident Response Phases. Incident Handling Annual Testing and Training. Pag 6-11.

LegalSEC SUMMIT, CHAMPION, Shayne. Incident Response With Modest Resources. Pag 5-36.

NIST, CHICONSKY, Paul. Computer Security Incident Handling Guide. Pag 21-49. NIST.SP.800-61r2.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI. Anexo 5 – Escenario 4

Recuperado en: https://documentation.wazuh.com/current/index.html// (consulta: 13 de marzo de 2021).

Recuperado en: https://www.snort.org/documents// (consulta: 13 de marzo de 2021).

Recuperado en: https://securityonionsolutions.com/software///// (consulta: 13 de marzo de 2021).

Recuperado en: https://www.cisecurity.org/cybersecurity-threats// (consulta: 13 de marzo de 2021).

Recuperado en: https://www.helpsystems.com/es/blog/que-es-un-siem// (consulta: 14 de marzo de 2021).

Recuperado en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes// (consulta: 14 de marzo de 2021).

ANEXOS.

A continuación, en el siguiente botón podrá consultar el video de la sustentación: