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

DENNIS CAROLINA VILLAMIL DIAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
LETICIA, AMAZONAS
2021

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

DENNIS CAROLINA VILLAMIL DIAZ

INFORME TECNICO CIBERSEGURIDAD: RED TEAM & BLUE TEAM

TUTOR:
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
LETICIA, AMAZONAS
2021

RESUMEN

El crecimiento exponencial que ha tenido el Internet en los últimos años ha traído consigo grandes beneficios para la humanidad, a tal punto que podamos realizar múltiples acciones sin salir de casa y prueba de ello ha sido la reciente pandemia.

Sin embargo también ha traído violación de la seguridad de la información y delitos informáticos, ya que Internet se usa para realizar actividades del gobierno, transacciones bancarias, compras en línea, redes sociales, estudiar, trabajar, etc. casi todo lo que tenemos en la vida real se encuentra en internet y muchas de las personas que utilizan este tipo de plataformas no tienen el suficiente conocimiento de como proteger sus datos personales para evitar ser víctimas de ciberdelincuentes.

Por otro lado en las organizaciones el panorama no es diferente si bien es cierto que no existe un sistema de información 100% seguro, las mismas han ido implementando en los últimos años nuevas estrategias de seguridad a raíz de ataques de los ciberdelincuentes que por lo general son causados por personas dentro de las mismas organizaciones o terceros con el fin de obtener beneficios grandes económicos.

Parte de esas estrategias organizacionales consiste en tener el personal capacitado y disponible en el área de seguridad informática que implemente y ejecute mecanismos de ciberseguridad para la identificación de vulnerabilidades; Aplicando técnicas de ataques y contención de ataques fundamentados en metodologías de seguridad de la información, con el objetivo de mitigar los riesgos y buscar mejoras continuas en la seguridad de la información dentro de la organización

TABLA DE CONTENIDO

Pág.

TABLA DE ILUSTRACIONES

GLOSARIO

ANTIVIRUS: Son programas cuyo objetivo es detectar y eliminar virus informáticos con el transcurso del tiempo, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos. Actualmente son capaces de reconocer otros tipos de malware como spyware, gusanos, troyanos, rootkits, pseudovirus etc. (Wikipedia, Que es Antivirus, 2011).

BACKUP: Una copia de seguridad, respaldo, copia de respaldo o copia de reserva (en inglés backup y data backup) en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. (wikipedia, wikipedia Metasploit, 2021).

CIBERSEGURIDAD: es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio. Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos. (CISCO, 2021).

CIS: El Center for Internet Security, CIS es una organización independiente sin fines de lucro cuya misión es desarrollar y desarrollar buenos ejemplos de soluciones de ciberseguridad. El objetivo de los controles del CIS es establecer distintas capas de protección, a todos los niveles, con sistemas proactivos de defensa y sistemas reactivos capaces de dar una respuesta rápida cuando se detecte un problema, así como garantizar que los empleados de la organización están concienciados con la seguridad y realizan su trabajo siguiendo una serie de procesos bien definidos. (Anónimo, CIS ControlsSpanishTranslation, 2021).

COPNIA: El Consejo Profesional Nacional de Ingeniería – COPNIA, creado mediante la Ley 94 de 1937, es la entidad pública que tiene la función de controlar, inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional. (COPNIA, Quienes Somos, 2021).

DELITO INFORMATICO: es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. (informatico, 2021).

ERI: Un Equipo de Respuesta a Incidentes (ERI) provee servicios y da soporte para prevenir, gestionar y responder ante los incidentes de seguridad de la información. (Anónimo, Una guía práctica para crear un equipo de respuesta a incidentes cibernéticos, 2021).

FIREWALL: del término original en inglés firewall, es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. (Wikipedia, Que es un Cortafuegos, 2021).

HARDENING: consiste en el endurecimiento del sistema, con el fin de reducir y evitar las amenazas y los peligros de este. (Anónimo, ¿QUE ES HARDENING DE SISTEMAS OPERATIVOS?, 2020).

KALILINUX: es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux. (wikipedia, Que es Kali Linux, 2020).

METASPLOIT: es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos. (Metasploit, 2021).

METERPRETER: es un programa malicioso de tipo troyano que permite a los ciberdelincuentes controlar de forma remota las computadoras infectadas. (Meskauskas, 2020).

NMAP: es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich1) y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas. (wikipedia, nmap, 2021).

OPENVAS: es una suite de software, que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos. (wikipedia, Que es OpenVAS, 2020).

PENTESTING: es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos. El proceso consiste en identificar el o los sistemas del objetivo. Las pruebas de penetración pueden hacerse sobre una "caja blanca" (donde se ofrece toda la información de fondo y de sistema) o caja negra (donde no se proporciona información, excepto el nombre de la empresa). Una prueba de penetración puede ayudar a determinar si un sistema es vulnerable a los ataques,

si las defensas (si las hay) son suficientes y no fueron vencidas. (wikipedia, Examen de penetración, 2020).
SIEM: es un sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad. De esta forma, permite un análisis de la situación en múltiples ubicaciones desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales. La mayoría de los sistemas SIEM funcionan desplegando múltiples agentes de recopilación que recopilan eventos relacionados con la seguridad. (tecnology, 2020).

VIRTUALBOX: es un software de virtualización para arquitecturas x86/amd64. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual. (wikipedia, virtualbox, 2021).

INTRODUCCIÓN

En el último año a raíz de los aislamientos preventivos, medidas de bioseguridad y distanciamiento social por el virus del covid 19, se dio la necesidad que muchas personas trabajaran desde sus casas. Por tal razón se multiplicaron los empleos en modalidad de teletrabajo, es así como las organizaciones han tenido un desafío en ajustarse a estos nuevos ritmos de trabajo y tener a sus empleados desde casa. Tema que a nivel de seguridad informática es todo un reto porque se deben realizar accesos remotos para acceder a la información y mejorar la protección de los datos a nivel corporativo de ataques informáticos.

Los ciberdelincuentes con el pasar de los años van hallando la manera de cambiar sus técnicas para llevar a cabo sus ataques y cada vez están siendo más implacables. Por tal motivo, es de gran importancia implementar estrategias de ciberseguridad que permitan proteger y mitigar estos ataques dentro y fuera de las organizaciones.

Parte de las estrategias de seguridad dentro de una organización es la creación de los equipos Blue Team y Red Team, estos equipos son un grupo de profesionales que poseen conocimientos en el área de sistemas y seguridad informática que se especializan en identificar fallos de seguridad, hacer pruebas de penetración y poner a prueba los sistemas dentro de las organizaciones con el fin de mejorar procesos y establecer controles que permitan reforzar la seguridad de la información, teniendo en cuenta que el activo más importante de una organización es la información y que no existe un sistema 100% seguro pero si uno que este en constante ajuste y pruebas para mitigar riesgos a nivel de seguridad de la información.

El presente informe es una recopilación de las etapas vistas durante el Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team. Iniciando en la legislación colombiana desde el ámbito de la seguridad informática y código de ética profesional del copnia, seguidamente se presenta un caso de análisis de la empresa the whitehouses y en el cual también se realiza un ataque informático donde se analizan los riesgos y vulnerabilidades del sistema, se encuentran las diferencia de un equipo Blueteam y un equipo de respuesta a incidentes informáticos, y se dan a conocer técnicas de contención de ataques informáticos dentro de las organizaciones con la finalidad de buscar una mejora continua con respecto a la ciberseguridad.

Con todos los puntos anteriores se puede dimensionar los conocimientos adquiridos por parte del estudiante durante el seminario y como este tiene una percepción de la temática a en su vida profesional.

OBJETIVOS

OBJETIVO GENERAL

Presentar informe donde se evidencien las implicaciones legales de quienes comentan delitos informáticos, a su vez analizar las técnicas para la identificación de vulnerabilidades en la empresa the whitehouses y la implementación de estrategias para la contención de ataques informáticos con el fin de mitigar riesgos dentro de la organización.

OBJETIVOS ESPECFICOS

- Identificar las leyes y decretos que se aplican para los delitos informáticos en Colombia.
- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.
- Proponer estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

DESARROLLO DEL INFORME

1. ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

Con las nuevas tecnologías y el crecimiento exponencial de las mismas se han aumentado la cantidad de usuario, así como de delitos informáticos, tema que hoy en día es de crucial importancia porque ahora la mayoría de actividades, transacciones y operaciones ya sea del ámbito laboral o personal se hacen por plataformas virtuales sin embargo difiere el nivel importancia de seguridad de la información que se le da por país.

Es por eso que en Colombia desde hace algunos años se viene creando e implementando leyes que ayuden a mitigar y aplicar en las organizaciones para evitar ser víctimas de delitos informáticos, entre la legislación que podemos encontrar en Colombia podemos encontrar:

LEY 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (NACIONAL, 2021)

Ley 1341 de 30 de julio de 2009, sobre principios y conceptos sobre la Sociedad de la Información y la Organización de las Tecnologías de la Información y las Comunicaciones.

Decreto 1162 del 13 de abril de 2010, por el cual se organiza el Sistema Administrativo Nacional de Propiedad Intelectual y se crea la Comisión Intersectorial de Propiedad Intelectual.

Ley Estatutaria 1581 de 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de los datos personales (Diario Oficial nº 48.587 de 18 de octubre de 2012)

Decreto 2364 de 22 de noviembre de 2012, sobre la firma electrónica.

Ley nº 1680 de 20 de noviembre de 2013, por la cual se garantiza a las personas ciegas y con baja visión, el acceso a la información, a las comunicaciones, al conocimiento y a las tecnologías de la información y de las comunicaciones. (Diario Oficial nº 48.980 de 20 de noviembre de 2013).

Ley 1712 de 6 de marzo de 2014, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información Pública Nacional y se dictan otras disposiciones. (Diario Oficial nº 49.084 de 6 de marzo de 2014).

Decreto 2573 de 12 de diciembre de 2014, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. (Publicado en el Diario Oficial 49363 de 12 de diciembre de 2014).

Ley 1915 de 12 de julio de 2018, por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de Derecho de Autor y Derechos Conexos.

Ley 1928 de 24 de julio de 2018, por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.

Ley nº 2015 de 31 de enero de 2020, por medio de la cual se crea la Historia Clínica Electrónica Interoperable (HCEI) y se dictan otras disposiciones.

Decreto nº 1287 de 24 de septiembre de 2020, por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria. (Anónimo, Legislación Informática de Colombia, 2021)

2. ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL

El hecho llevar una vida paralela con el uso del internet nos deja expuestos a delitos informáticos, tema que en Colombia se ha reglamentado y está siendo vigilado por diferentes leyes como la 1273 de 2009, 1581 de 2012 y decreto 1377 de 2013 entre otros.

Es por eso que en esta etapa se estudió un caso aplicado a los profesionales en seguridad informática y en como ejercer esta actividad sin las respectivas autorizaciones tendría repercusiones legales, guiándonos de las respectivas leyes de seguridad informática en Colombia y el código de ética del consejo profesional nacional de ingeniería. También se analizó un caso de delito informático ya cometido en Colombia y el desenlace de los mismos.

De acuerdo a la lectura del anexo 2, escenario 2 se puede encontrar que WhiteHouse Security es una empresa muy importante y con una trayectoria reconocida en al área de seguridad informática, así mismo se menciona en el anexo 3 “Que la información de propiedad de Whitehouse Security Security ha sido desarrollada u obtenido legalmente”. Sin embargo, se encuentran una serie de inconsistencia y contradicciones al contener en su contrato partes no éticas y no legales, por ejemplo:

“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 reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal”. (UNAD, 2021)

Claramente en este párrafo se evidencian una de esas inconsistencias ya que un contrato que no sea revisado y mucho menos modificado por la gerencia habiendo despedido al empleado que lo elaboró puede contener clausulas y condiciones que podrían ir en contra de la misma empresa y de quien sería el contratado, a su vez la empresa advierte leer muy bien el contrato antes de firmar, lo que deja muchas dudas de sus intenciones debido a que se podrían estar incurriendo procesos ilegales pero la empresa de cierto modo tiene conocimiento porque está haciendo una advertencia.

“Entiéndase como ilegal todo aquello que va en contra de la ley” (Española, 2021). Para hacer un análisis de este contrato nos referenciaremos de las leyes 1273 de 2009, 1581 de 2012 y código de ética del copnia y a nivel general de las leyes que desde sus inicios han regido en Colombia para el área de seguridad informática.

Haciendo una revisión minuciosa del acuerdo del anexo 3 que se pide en la actividad (UNAD, 2021) se encuentra que incurre en acciones poco ética desde el momento

en que prohíbe denunciar actos ilegales como se menciona en la “Cláusula Cuarta. Obligaciones de la parte receptora: Ítem 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.” También cuando descarga toda la responsabilidad en dos de sus apartados al profesional a contratar en caso de presentarse algún proceso ilegal o allanamiento, ya se está presentado un caso de falta de ética hacia el profesional.

La ley 1273 de 2009 y demás legislaciones en Colombia para el área de delitos informáticos seguirá en actualización, así como cada vez existen más usuarios en el mundo virtual así mismo quienes quieren atacar y sacar un benéfico económico o personal. Está claro que las leyes cubren gran parte de lo que a esta área compete sin embargo nos falta mucho en comparación a otros países en cuando a la protección de la información y las condenas para quienes pretendan sacar provecho de estos delitos.

Por otro lado el caso Andrómeda (Hernández, 2014) y demás casos de espionaje, que usan medios informáticos para captar información y tener beneficio propio o económico no es el primero que se presenta en Colombia de cierto modo estamos siendo vigilados, pero depende de que se hace con esa información y la intención. La lista de delitos es larga pero así mismo las implicaciones legales para quienes se dedican a este tipo de actividades ilícitas. Por eso como profesionales de la ingeniería hay que profundizar los conocimientos en las leyes que nos rigen, conocer nuestros deberes, derechos, y prohibiciones para así evitarnos tener líos judiciales.

Desde el momento en que se obtiene el título profesional en una universidad acreditada por el ministerio de educación de la república de Colombia y seguidamente la tarjeta profesional en caso de que aplique, se crean unas conductas y procederes claves al momento de desempeñarse laboralmente en cualquier entidad ya sea pública o privada, que determinaran la permanecía y crecimiento profesional de la persona en la misma.

Por tanto como profesionales del área de seguridad informática, está en nuestras manos la orientación que le damos a nuestro conocimiento, sin embargo, al haber firmado el código de ética del COPNIA nos regimos bajo unos principios y normas que hacen que nuestro trabajo no se vea afectado o nuestras acciones estén yendo en contra del mismo o de alguna ley. Permitiendo así enaltecer nuestra labor y dar valor al conocimiento en el área.

3. ETAPA 3 EJECUCIÓN PRUEBAS DE INTRUSIÓN

Con la construcción de esta actividad se realizaron los pasos de iniciación en las fases de un pestesting y las respectivas instalaciones de las herramientas de trabajo como los S.O Windows y Kali. Con la finalidad de Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Las herramientas software que utilizaron para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam, fueron: VirtualBox, Windows 7, Kali Linux, Rejetto, Nmap, y MetaExploit.

De acuerdo a la lectura del anexo 4, escenario 3 se puede encontrar que WhiteHouse Security es una empresa muy importante y con una trayectoria reconocida en al área de seguridad informática, así mismo se menciona en el anexo 4 “se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia.” (UNAD, 2021)

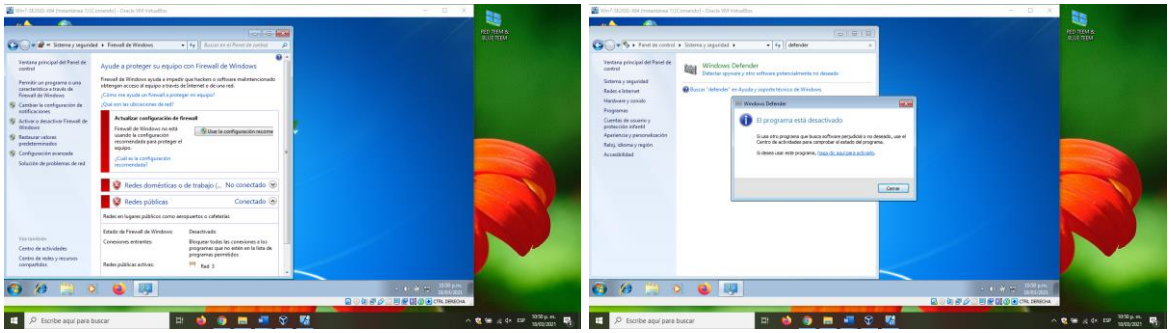
Así mismo el tipo de S.O de los equipos y la aplicación por la cual se está presentado la fuga de información que el rejetto y que exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Por último se realiza un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

EJECUCIÓN DEL ATAQUE

- Fase de recolección de información

Para dar inicio al laboratorio en la maquina víctima de se deben desactivar el firewall, Windows defender y Windows update.

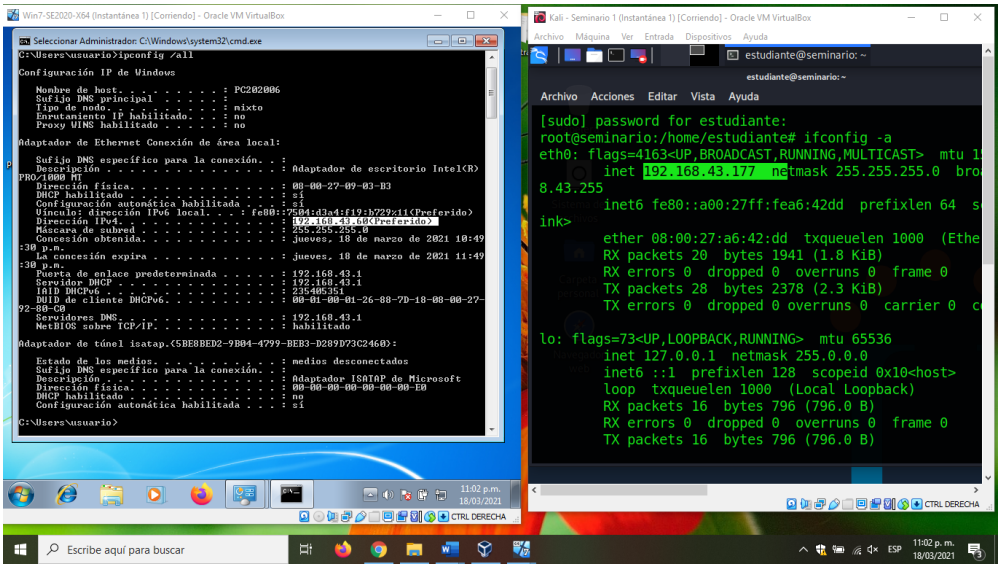
Ilustración 1. Entorno de Trabajo Maquina Victima



Fuente: Carolina Villamil

Verificamos las direcciones IP de la maquina víctima y de la maquina Kali

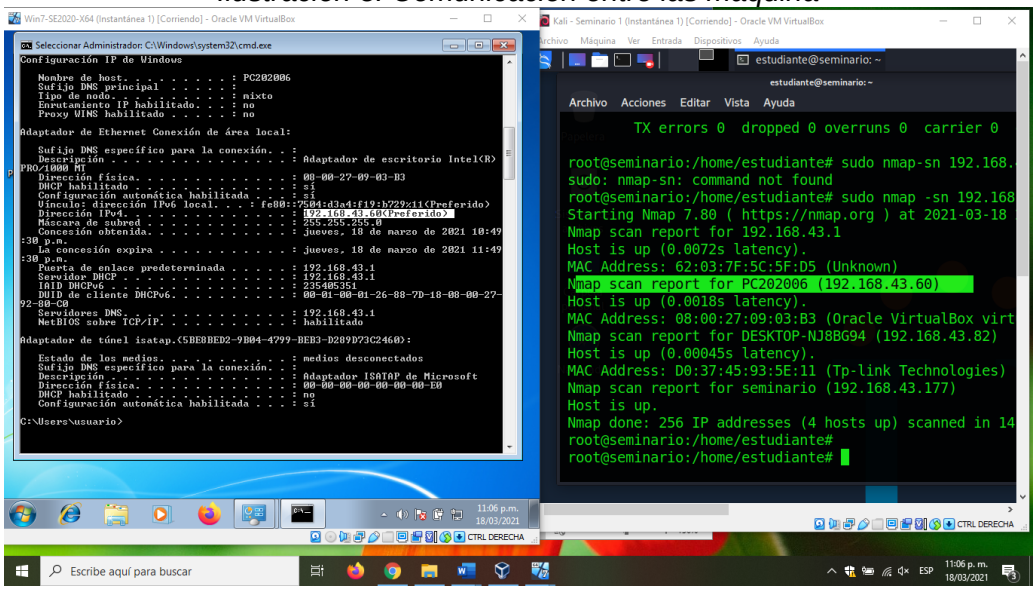
Ilustración 2.: Verificación IP vulnerables



Fuente: Carolina Villamil

Ahora vamos a verificar que exista comunicación entre las maquina con NMAP y el comando: que sirve para escanear toda la red:
Sudo nmap -sn 192.168.43.0/24

Ilustración 3. Comunicación entre las maquina

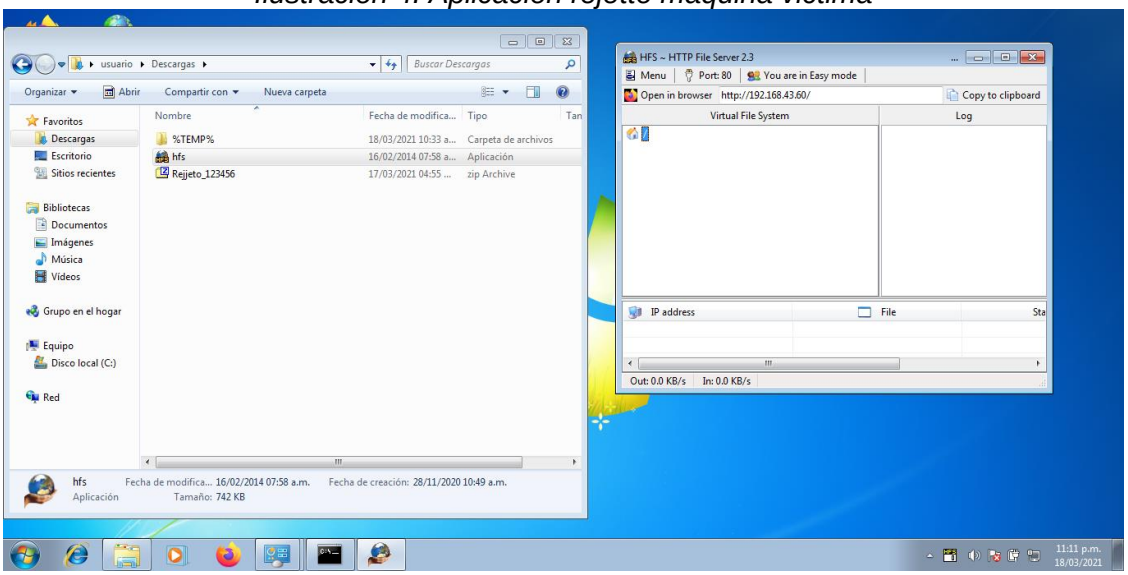


Fuente: Carolina Villamil

- Fase de Búsqueda de vulnerabilidades

Ahora descargamos e instalamos en la maquina victima la aplicación rejetto:

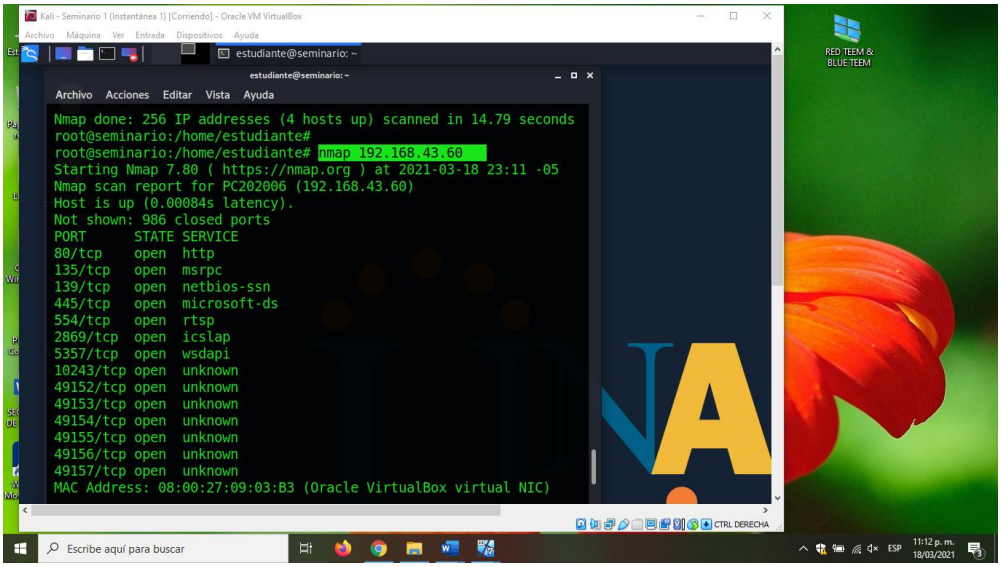
Ilustración 4. Aplicación rejetto maquina victima



Fuente: Carolina Villamil

Ahora desde la máquina de Kali escaneamos por puerto que tiene abiertos la maquina víctima con el comando nmap y la ip de la víctima:

Ilustración 5. Escaneo de Puertos

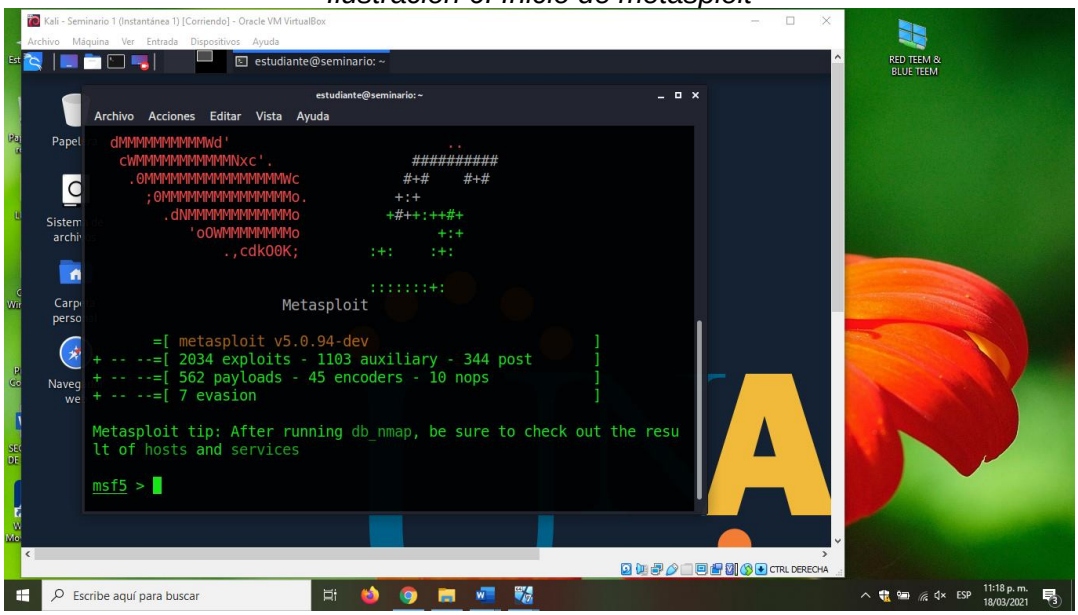


Fuente: Carolina Villamil

- Fase De Explotación

Se inicio metaesploit con el comando msfconsole de maquina Kali

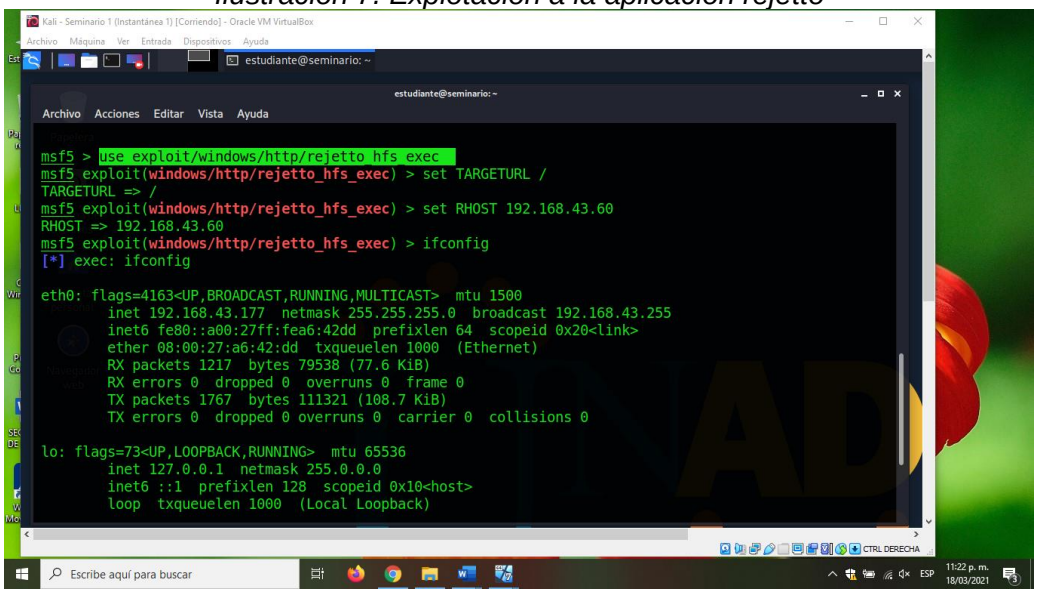
Ilustración 6. Inicio de metasploit



Fuente: Carolina Villamil

Los comandos a usar para realizar el exploit son los siguientes ya identificadas las IP's tanto de atacante como víctima:

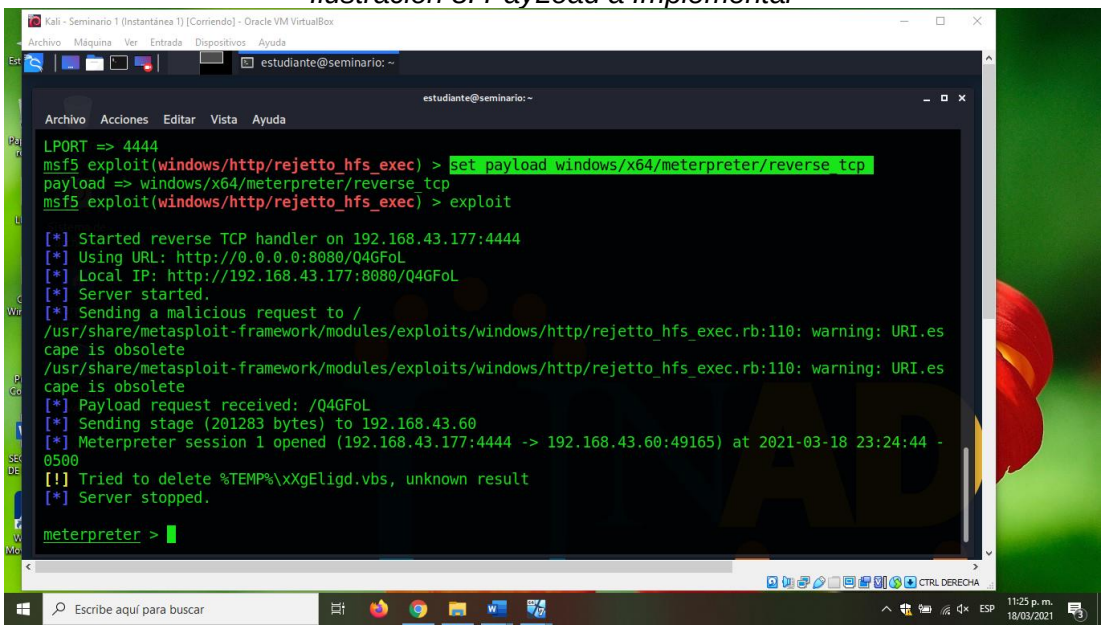
Ilustración 7. Explotación a la aplicación rejetto



Fuente: Carolina Villamil

aquí utilizamos el payload con el comando: set payload windows/x64/meterpreter/reverse_tcp

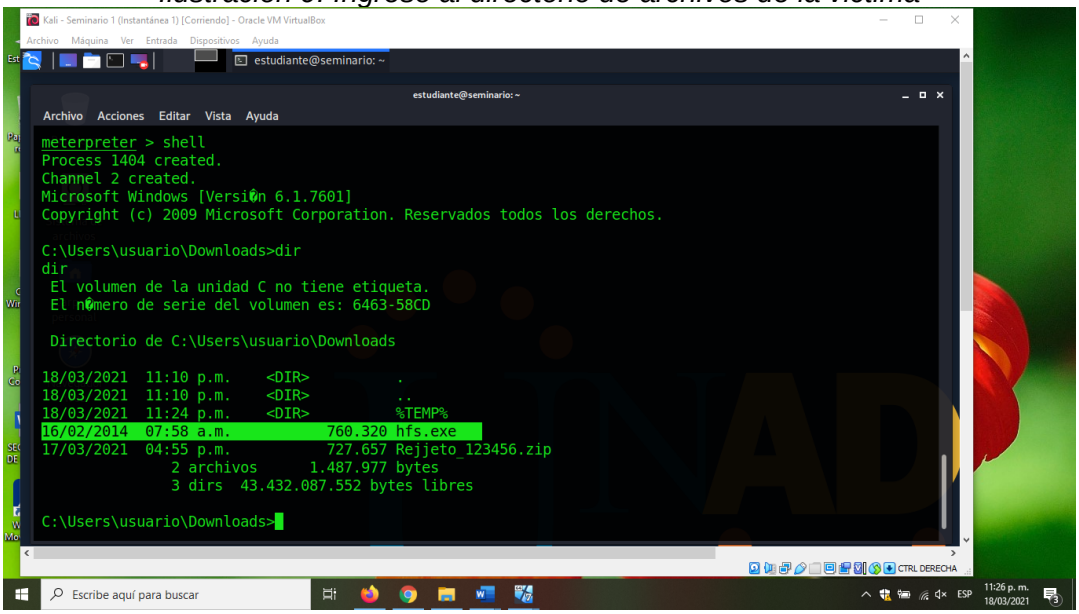
Ilustración 8. PayLoad a Implementar



Fuente: Carolina Villamil

Entramos a la zona de descargas en el equipo victima:

Ilustración 9. Ingreso al directorio de archivos de la victima

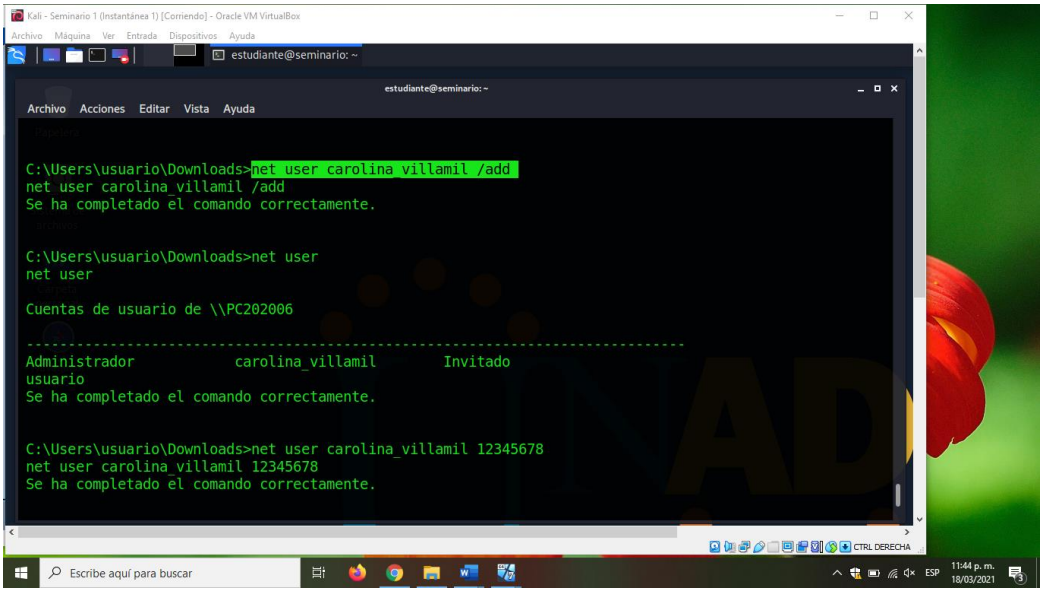


Fuente: Carolina Villamil

- Fase Post-explotación.

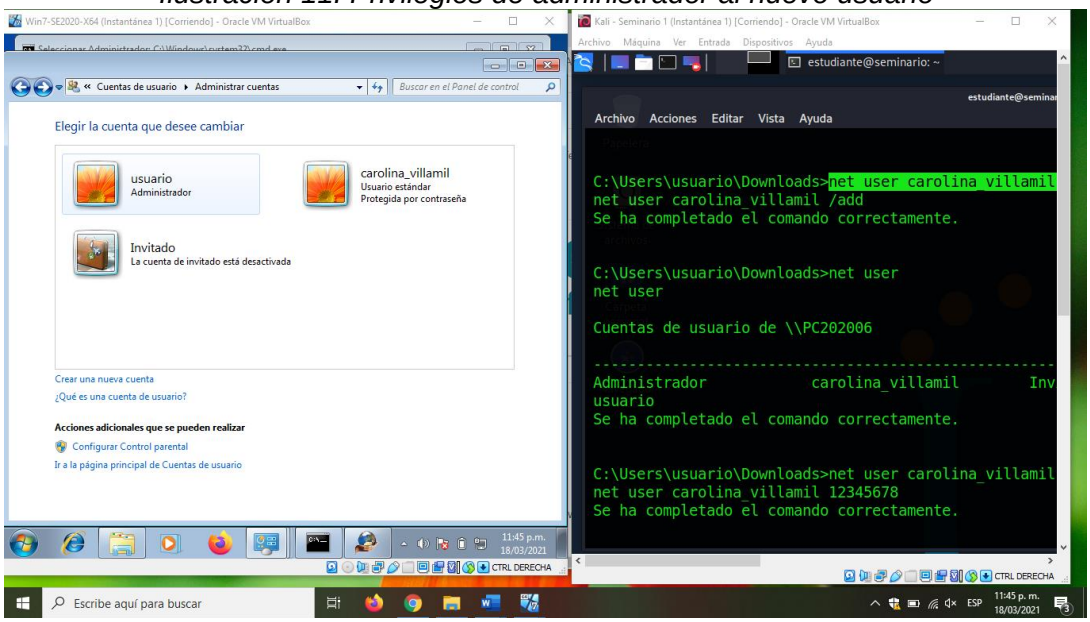
Ahora vamos a crear una cuenta de en el equipo victima inicialmente usuario estándar: net user carolina_villamil /add

Ilustración 10. Creación de Usuario Windows Victima



Fuente: Carolina Villamil

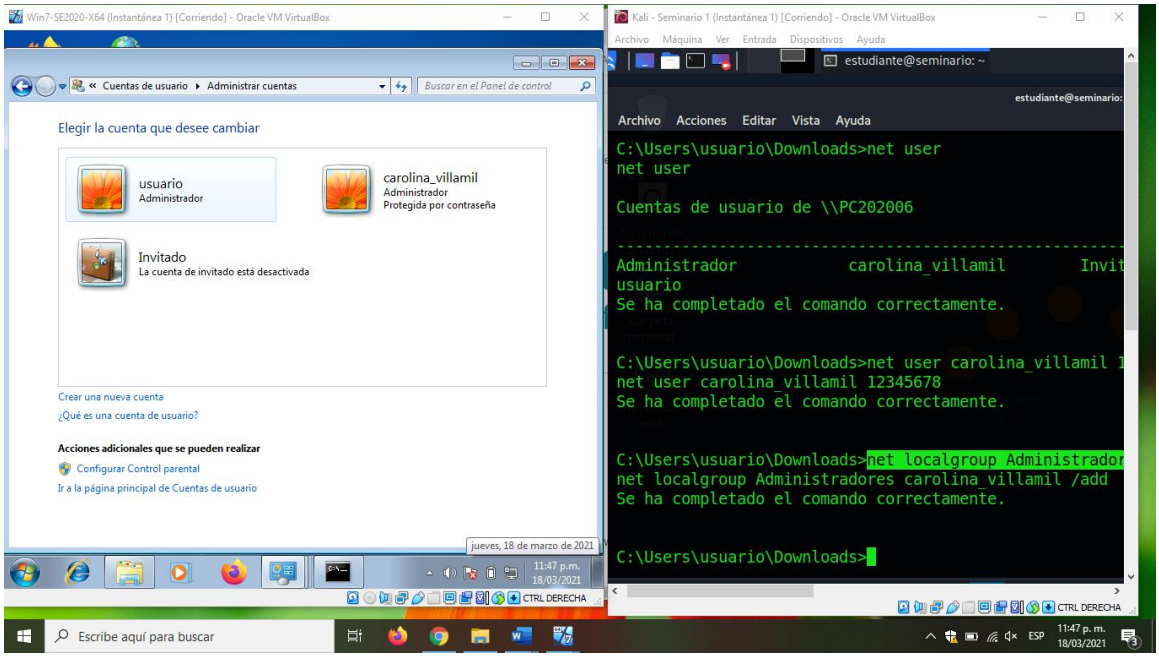
Ilustración 11. Privilegios de administrador al nuevo usuario



Fuente: Carolina Villamil

Ahora con el comando net localgroup Administradores carolina_villamil /add agregamos el usuario como administrador

Ilustración 12. Visualización de usuarios administradores



Fuente: Carolina Villamil

- Fase de Informe

En esta etapa se logra identificar que gran parte de que el ataque fuera exitoso es que la maquina victima tuviera desactivado su firewall, Windows defender, Windows update y antivirus si lo tuviera. Lo cual deja en evidencia el papel que juegan las personas que usan estas aplicaciones en una organización.

Así mismo es posible encontrar las vulnerabilidades por medio del uso de herramientas como NMAP o metaexploit desde la maquina atacante (Kali), reconociendo puertos abiertos e información del equipo víctima. Finalmente, después de realizar toda la actividad y el ataque se presenta un informe con las respectivas capturas de pantalla del ataque y evidencia de ello es la creación de un usuario administrador llamado carolina_villamil

Es claro que dentro de la organización hay un equipo que está siendo vulnerable a un ataque en este caso con la aplicación rejetto, así como se puedo efectuar este ataque en las maquinas se puede realizar en otro equipo dentro de la organización. Lo cual deja muy vulnerable y expuesto el estado actual de seguridad informática con la que encuentra la empresa the whitehouse.

4. ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

Cuando se presenta un ataque en tiempo real es porque generalmente el equipo o la maquina víctima se encuentra conecta en red ya sea vía cableada o wifi, aunque también pueden existir otros tipos de ataque como el de ingeniería social. Sin embargo el ataque se puede presentar desde la misma red interna o desde internet y las acciones que realizaría serían las siguientes:

a) Hacer un escaneo de la red para saber que puertos están abiertos y de qué manera está siendo vulnerado el equipo
b) Desconectar el equipo de la red
c) Revisar y activar el firewall
d) Revisar y activar el antivirus
e) Desinstalar cualquier programa desconocido
f) Cambiar las contraseñas de usuario a una más segura
g) Activar las licencias de los softwares que no las tengan
h) Instalar o contratar alguna herramienta que me permita contrarrestar cualquier ataque como por ejemplo Fortinet

Cabe aclarar que no existe un sistema 100% seguro, pero si una serie de técnicas y métodos que pueden ayudar a mitigar a ser víctimas, todo depende del tipo de información que se maneje en la empresa y el ejercicio constante de auditoria y capacitación con usuarios de la misma.

Análisis del ataque

El Red Team de la empresa The WhiteHouse realiza un proceso de emulación de escenarios de amenazas a los que se puede enfrentar una organización, analizando la seguridad desde el punto de vista de los atacantes.

En el ataque que hizo el equipo Red Team, se encontró que se realizó por medio de una máquina virtual (VirtualBox), así mismo que el S.O víctima tenía la licencia del Windows caducada y el firewall y el antivirus desactivados. A su vez el usuario de la maquina víctima instalo un programa para transferencia de archivos (Rejetto) por el cual se dio el ataque.

Hardenización es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuanto más funciones desempeña. (wikipedia, Endurecimiento (informática), 2020). De acuerdo a esta definición y de lo que se encontró en el ejercicio, se procedió a realizar la desinstalación del programa rejetto, activación del firewall, de Windows defender y del antivirus. Sin embargo no se activó la licencia del S.O Windows, debido a la caducidad del mismo.

Parte de este ataque inicio porque el usuario del equipo victima desactivo las opciones de seguridad e instalo un programa que puso en vulnerabilidad su sistema, por ello una de las primeras medidas que se deben tomar es capacitación de usuario con el fin de reducir los riesgos y aumentar la seguridad son:

- No abrir archivos desconocidos.
- No descargar desde paginas no oficiales
- Tener contraseñas robustas.
- Tener cuidado con los correos electrónicos.
- Tener nuestros sistemas operativos actualizados.
- Tener un programa antivirus activado.

Ahora bien las medidas de Hardening contra las amenazas pueden ser:

- Usuarios: Mediante cursos de concienciación en la seguridad informática.
- Programas malintencionados: No descargando ningún programa de fuentes desconocidas o no oficiales.
- Exploits: Manteniendo nuestros sistemas operativos actualizados.
- Intrusos: Estableciendo permisos y niveles de acceso.
- Fuerza mayor: Mediante el uso de backups. (Fortinet, 2021)

DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

Antes de encontrar la diferencia entre estos dos equipos, se debe mencionar que blueTeam que es el equipo de seguridad que tiene la posibilidad de defenderse de forma controlada y constructiva de ataques. El principal objetivo del Blue Team es realizar evaluaciones de las distintas amenazas que puedan afectar a las organizaciones, monitorizar (red, sistemas, etc.) y recomendar planes de actuación para mitigar los riesgos. Además, en casos de incidentes, realizan las tareas de respuesta, incluyendo análisis de forense de las máquinas afectadas, trazabilidad de los vectores de ataque, propuesta de soluciones y establecimiento de medidas de detección para futuros casos. (Revista, 2020)

Por otro lado el equipo de respuesta a incidentes informáticos se define como un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas. (wikipedia, Equipo de Respuesta ante Emergencias Informáticas, 2014)

Ahora bien, después de revisadas y analizadas las funciones de cada no se puede determinar que no exista una diferencia cuando el objetivo es el mismo proteger y mitigar ataques de seguridad dentro de una organización, los dos están conformados por un equipo de profesionales del área de la seguridad informática, sistemas o redes. Y sus funciones no difieren porque analizan la red, los sistemas y software usados dentro de la organización. A su vez los dos equipos presentan al final un informe del estado actual de la organización en cuando a taques se refiere y presentan una serie de medidas para mitigar los mismo, por tanto podemos determinar que Blue y CERT cumplen las mismas funciones.

HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS

Partamos del punto que para contener un ataque ya debemos contar con unas herramientas, es decir ya tengo mi escudo ante ataques informáticos y como lo mencionábamos en el primer punto es clave tener nuestros S.O y software activos y actualizados. Ahora bien en el mercado se encuentran una lista de software que nos pueden brindar un todo en uno en contención de ataque informáticos como por ejemplo:

Cisco FireSight, solución de Contención Rápida de Amenazas Cisco: Cisco FireSIGHT escanea la actividad de la red con sensores cuya inteligencia es actualizada constantemente con las últimas alertas. Estos sensores buscan en los sistemas corporativos código malicioso o prohibido por las políticas de seguridad. También monitorizan las conexiones de usuarios y dispositivos para detectar si se conectan a dominios peligrosos, como podrían ser los de una botnet. (Cisco FireSight, solución de Contención Rápida de Amenazas Cisco, 2021)

Cortafuegos**:** Es importante combinar las cualidades de un cortafuegos efectivo y bien configurado, con un sistema antivirus dotado de detección heurística que monitorice todo cuanto sucede en tu equipo. De ese modo, será capaz de detectar patrones de comportamiento sospechoso y podrá comunicarse con el cortafuegos para bloquear y aislar esas probables amenazas incluso antes de que se activen y se conviertan en un serio problema de seguridad. (Wikipedia, Que es un Cortafuegos, 2021)

Access Rights Manager**:** puedes administrar y auditar los permisos de acceso en toda su infraestructura tecnológica como la perfecta herramienta de seguridad. Las herramientas de seguridad informática tienen excepcionales formas de tratarse cuando hablamos de ataques, sean internos o externos. (Anónimo, Access Rights Manager como tu herramienta de seguridad informática predilecta, s.f.)

- Monitoreo y Active Directory: para conocer los cambios realizados, quién los ha realizado y en qué momento

- Análisis de permisos de usuario: ayuda a proteger contra amenazas a la seguridad interna a través del estudio de los privilegios de acceso de usuarios a diferentes destinos.
- Monitoreo de Microsoft Exchange: rastrea cambios en bandejas de entrada, carpetas, calendarios y carpetas públicas.
- Aprovisionamiento y administración de usuarios: configura nuevas cuentas de usuario y permite administrarlas a través de plantillas definidas.
- Auditorías para uso compartido de archivos Windows.
- Monitoreo y administración del acceso de SharePoint.

5. ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM.

De acuerdo a la información revisada, analizada y puesta en practica durante el seminario, se puede determinar que son varios los aspectos que aportan al desarrollo de estrategias dentro de estos equipos:

- Inicialmente el aspecto de establecer roles y actividades claras que se desempeñaran en cada equipo dentro de la organización, con la estrategia de que cada equipo se integre de profesionales idóneos para realizar los respectivos ataques ya sea un equipo red team o blue team.

- A su vez los equipos siempre deben definir los aspectos que se tomaran en cuenta para la estrategia del ataque o defensa en la empresa, ya sea por el tamaño de la empresa, naturaleza, infraestructura tecnológica, perfiles de usuario u otros relevantes para que se lleve a cabo de manera controlada dependiendo del equipo que se integre.

- Una estrategia a tener en cuenta es establecer periodos de análisis y efectividad de las políticas y medidas de seguridad de la empresa, para asegurar que los potenciales riesgos y las amenazas están siendo revisados, identificados y mitigados.

- El aspecto de definir previamente mediante un contrato de confidencialidad el objetivo y funciones que cada equipo desempeñara en la empresa, con su respectivo alcance y si las partes (Empresa y equipo blue team o red team) están de acuerdo con las cláusulas y demás contenido del documento proceder a su firma.

- Los ataques deben representar una amenaza constante si quien los realiza es un equipo red team o contención/vigilancia si es un equipo blue team, los ataques que se realizan siempre de manera controlada y con el consentimiento de la gerencia de la empresa. Estos ataques se deben realizar hasta conseguir el objetivo final: manipular, filtrar, robar información, denegación del servicio o fraude. Además se usan también técnicas de ingeniería social, Por ejemplo: phishing, malware y ransomware.

- Finalmente un aspecto que aporta en gran medida a estas estrategias, es el levantamiento de información también conocida como la fase de reconocimiento, porque es allí donde se recopila toda la información sobre el sistema que se va a atacar o defender, lo ideal es identificar todos los aspectos relevantes, debido a que entre más información se tenga más fácil se podrán ejecutar los pasos para el ataque o contención de amenazas cibernéticas.

6. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN

Partamos del hecho que no existe un sistema o organización 100% seguro o exento de ataques informáticos, dada la naturaleza de los sistemas y el constante avance de las tecnologías así mismo aumentan la agilidad de los ciberdelincuentes que se adaptan a estos cambios y generalmente logran perpetrar ataques cibernéticos.

Sin embargo una empresa puede mitigar ser victima de ataque informáticos si aplica unas estrategias y/o técnicas de seguridad como pueden ser:

- Crear las políticas de seguridad de la información.
- Constante vigilancia de los sistemas.
- Establecer privilegios de usuario.
- Realizar auditorías de sistemas y es aquí donde entran los equipos red team y blue team que definen las técnicas defensivas y ofensivas de ataques informáticos.
- Uso de software como Firewall y Antivirus.
- Actualización de los sistemas operativos y software usados por la empresa.
- Finalmente realizar jordanas de socialización y capacitación al personal de la empresa con respecto a delitos informáticos, ataques informáticos y cómo actuar ante ellos.

7. CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.

Parte de la información recibida y aprendida durante el seminario, se podría concluir que el objetivo final de un equipo de ciberseguridad ya sea red team o blue team es hacer un seguimiento a la seguridad de una empresa y efectividad de sus políticas de seguridad. Por medio de ataques a sus sistemas y unas etapas del ataque que permitan identificar las fallas, para posteriormente mediante un informe técnico conocer el estado real de seguridad, solucionar esos fallos de seguridad y fortalecer los sistemas de la empresa.

A su considero que el conocimiento nace a raíz de las investigaciones y experiencia, por ello es un buen ejercicio leer y documentarse de legislación, noticias y métodos que se han usado en empresas o sectores victimas de ataques informáticos. Para así tener una guía de como proceder o lograr identificar las etapas de un determinado ataque y tomas las respectivas medidas de defensa.

Finalmente en internet se encuentran una gama de aplicaciones y herramientas tanto de pago como libres, que permiten que el ejercicio del personal de ciberseguridad sea mas completo ya que con esas herramientas se utilizan comandos y secuencias para llevar acabos los ataques o respectivos informes de trasteo de vulnerabilidades.

CONCLUSIONES

- La legislación en Colombia para el área de delitos informáticos seguirá en constante actualización debido a los avances tecnológicos que se van dando cada día, así como cada vez existen más usuarios en el mundo virtual a si mismo quienes quieren atacar y sacar un benéfico económico o personal. Está claro que las leyes cubren gran parte de lo que a esta área compete sin embargo nos falta mucho en comparación a otros países en cuando a la protección de la información y las condenas para quienes pretendan sacar provecho de estos delitos. Así mismo los profesionales en el área de sistemas o seguridad informática tienen el libre albedrio de elegir como usar su conocimiento, pero teniendo plenamente identificadas y siendo conscientes de las implicaciones legales en caso de querer tener beneficio propio a costa de cometer delitos informáticos.

- En una organización se puede mitigar el riesgo de ser víctima de un ataque informático usando una serie de estrategias de contención como mantener nuestros sistemas actualizados o haciendo uso de software de contención de ataques informáticos. Sin embargo deben existir dentro de las organizaciones profesionales en la seguridad informática que conformen un equipo Blueteam, redTeam o equipo de respuesta a incidentes informáticos. Para que sean quienes se encarguen de vigilar, monitorear y contrarrestar posibles ataque y robos de información dentro de las organizaciones. A su vez este equipo debe estar en constante actualización y capacitación tanto a los usuarios de la empresa como a los softwares que allí sean usados.

- Actualmente en el mercado podemos encontrar herramientas de contención de ataques informáticos “hardware o software”. Que permiten a las organizaciones estar un poco más protegidas de ciberdelincuentes, recordemos que no existe un sistema 100% seguro pero que si pueden tomar medidas y aprender de los errores o ataques para que no se vuelvan a repetir. Este mundo de la seguridad informática está en constante aprendizaje.

RECOMENDACIONES

Es primordial que los profesionales que conformen el equipo de seguridad informática tengan muy claro su rol dentro de la organización, para ello se deben establecer metas, objetivos y protocolos de seguridad en la organización. También estar en constante revisión de las modificaciones de la legislación colombiana en el área de delitos informáticos. A su vez tener en cuenta que no solo es proteger los sistemas informáticos sino también el talento humano dentro de la organización y esto se logra con capacitaciones y retroalimentación de los sucesos que se presenten o tomando ejemplo de noticias y reportes de ataques informáticos en otras entidades para tomar las respectivas medidas de seguridad.

En este sentido es indispensable adoptar tácticas, técnicas y procedimientos para mitigar los ataques de los ciberdelincuentes que buscan atacar a las organizaciones vulnerables para obtener beneficos económicos y sobre todo en esta época de pandemia y de transición. Si bien es cierto no existe un sistema completamente seguro si se pueden implementar técnicas para minimizar el riesgo de ser víctimas de estos delincuentes.

Se recomienda diseñar e implementar una estrategia de ciberseguridad con el fin de prevenir amenazas y proteger los activos de las organizaciones, como ya se mencionó existen herramientas tipo software y técnicas desde un enfoque metodológicos que ayuden a los a los usuarios para complementar el esquema de seguridad y mantener la seguridad dentro de la organización.

Link del video: https://youtu.be/jBQsHhvskS0

REFERENCIAS

Anónimo. (28 de mayo de 2020). ¿QUE ES HARDENING DE SISTEMAS OPERATIVOS? Obtenido de https://www.ciset.es/publicaciones/blog/746-hardening

Anónimo. (03 de abril de 2021). CIS ControlsSpanishTranslation. Obtenido de https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

Anónimo. (03 de ABRIL de 2021). Legislación Informática de Colombia. Obtenido de http://www.informatica-juridica.com/legislacion/colombia/

Anónimo. (06 de abril de 2021). the blue team. Obtenido de Argentina, Mkit: https://mkit.com/es/services/blue-team-operations

Anónimo. (10 de marzo de 2021). Una guía práctica para crear un equipo de respuesta a incidentes cibernéticos. Obtenido de https://www.infocyte.com/es/blog/2019/09/04/a-practical-guide-to-building-a-cyber-incident-response-team/

Anónimo. (s.f.). Access Rights Manager como tu herramienta de seguridad informática predilecta. Recuperado el 27 de marzo de 2021, de e-dea.co: https://www.e-dea.co/blog/access-rights-manager-como-herramienta-de-seguridad-informatica

Carmona, A. (17 de febrero de 2021). Adoptar las mejores prácticas del CIS (Center for Internet Security) en tiempos de COVID-19. Obtenido de https://kippeo.com/adoptar-las-mejores-practicas-del-cis-center-for-internet-security-en-tiempos-de-covid-19/

CISCO. (03 de Abril de 2021). ¿Qué es la ciberseguridad? Obtenido de https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html
Cisco FireSight, solución de Contención Rápida de Amenazas Cisco. (27 de MARZO de 2021). Obtenido de https://datacom.global/cisco-seguridad-deteccion-de-amenazas-en-las-organizaciones/

COPNIA. (03 de Abril de 2021). Quienes Somos. Obtenido de https://www.copnia.gov.co/nuestra-entidad/quienes-somos#:~:text=El%20Consejo%20Profesional%20Nacional%20de,general%2C%20en%20el%20territorio%20nacional.

COPNIA. (s.f.). COPNIA - CODIGO DE ETICA - EN LINEA. Obtenido de https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

Cornejo, A. (03 de octubre de 2018). El cortafuegos es una valiosa herramienta de seguridad. Obtenido de https://pco.com.mx/cortafuegos-una-herramienta-contra-ataques-ciberneticos/

ELIASIB, G. (2 de abril de 2019). hackingprofessional. Obtenido de Fases de un pentesting: https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/
Española, R. A. (03 de 04 de 2021). ¿Que es Ilegal? Obtenido de https://dle.rae.es/ilegal

FORTINET. (06 de junio de 2017). HOW TO CLOSE SECURITY GAPS TO STOP RANSOMWARE AND OTHER THREATS. Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/white-papers/eBook-How-to-Close-Security-Gaps-to-Stop-Ransomware-and-Other-Threats.pdf

Fortinet. (27 de marzo de 2021). Proteger contra las amenazas avanzadas actuales. Obtenido de https://www.fortinet.com/lat/solutions/enterprise-midsize-business/protect-advanced-threats

Fuertes, D. (28 de Noviembre de 2019). Controles del CIS: novedades de la versión 7.1. Obtenido de https://blog.isecauditors.com/2019/11/novedades-version-7-1-controles-cis.html

Hernández, N. Q. (17 de MAYO de 2014). De Andrómeda a los 'hackers'. Obtenido de EL ESPECTADOR: https://www.elespectador.com/noticias/investigacion/de-andromeda-a-los-hackers/

informatico, D. (17 de Marzo de 2021). wikipedia. Obtenido de https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

itdigitalsecurity.es. (30 de mayo de 2018). ¿Qué es un Blue Team y cómo trabaja? Obtenido de https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

Lara, Á. S. (6 de diciembre de 2018). securitytwins.com. Obtenido de VNC más Meterpreter en máquina vulnerada: https://securitytwins.com/2018/12/06/vnc-mas-meterpreter-en-maquina-vulnerada/

manageengine. (27 de marzo de 2021). ¿Qué son y cómo implementar los Controles de Seguridad Crítica CIS? Obtenido de https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Meeting, V. O. (03 de abril de 2021). CESICAT. Obtenido de https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf
Meskauskas, T. (26 de febrero de 2020). ¿Cómo eliminar Meterpreter? Obtenido de https://www.pcrisk.es/guias-de-desinfeccion/9601-meterpreter-

trojan#:~:text=Meterpreter%20es%20un%20programa%20malicioso,escribir%20nada%20en%20el%20disco.

Metasploit. (02 de abril de 2021). Wikipedia. Obtenido de Metasploit: https://es.wikipedia.org/wiki/Metasploit

mkit.com. (27 de marzo de 2021). The blue team. Obtenido de https://mkit.com/es/services/blue-team-operations

NACIONAL, P. (03 de ABRIL de 2021). Normatividad sobre delitos informáticos. Obtenido de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Rejetto | Remote Command Execution (Metasploit). (10 de enero de 2018). Obtenido de https://www.youtube.com/watch?v=JIjF4yVyqhQ

Revista, U. (07 de enero de 2020). Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? Obtenido de https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

School, E. B. (febrero de 2018). ESIC Business & Marketing School. Obtenido de Red team: qué es, estrategias y ejemplo de un caso real: https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque

tecnology, t. (10 de MARZO de 2020). Soluciones SIEM permiten detectar amenazas de seguridad en tu empresa. Obtenido de https://www.tuyu.es/soluciones-siem/

TIC´S, M. d. (s.f.). Ley 1581 de 2013. Obtenido de https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

TICS, M. d. (s.f.). Ley 1273 de 2009. Obtenido de https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

UNAD. (2021). UNAD. Obtenido de Seminario Especializado: Equipos Estratégicos en Red Team & Blue Team: https://campus125.unad.edu.co/ecbti88/mod/forum/post.php?reply=54068#mformforum

viewnext.com. (9 de enero de 2020). QUE ES SIEM. Obtenido de https://www.viewnext.com/que-es-un-siem/

Wikipedia. (2021 de ENERO de 13). Que es Nmap. Obtenido de https://es.wikipedia.org/wiki/Nmap

Wikipedia. (30 de diciembre de 2011). Que es Antivirus. Obtenido de https://es.wikipedia.org/wiki/Antivirus

Wikipedia. (15 de marzo de 2014). Equipo de Respuesta ante Emergencias Informáticas. Obtenido de https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas

Wikipedia. (26 de diciembre de 2017). Que es Windows 7. Obtenido de https://es.wikipedia.org/wiki/Windows_7

Wikipedia. (12 de julio de 2020). Endurecimiento (informática). Obtenido de https://es.wikipedia.org/wiki/Endurecimiento_(inform%C3%A1tica)#cite_note-col-1

Wikipedia. (23 de agosto de 2020). Examen de penetración. Obtenido de https://es.wikipedia.org/wiki/Examen_de_penetraci%C3%B3n

WIKIPEDIA. (1 de ABRIL de 2020). HTTP File Server. Obtenido de https://en.wikipedia.org/wiki/HTTP_File_Server

Wikipedia. (12 de agosto de 2020). Que es Kali Linux. Obtenido de https://es.wikipedia.org/wiki/Kali_Linux

Wikipedia. (17 de marzo de 2020). Que es Apenas. Obtenido de https://es.wikipedia.org/wiki/OpenVAS

wikipedia. (12 de agosto de 2020). wikipedia kali linux. Obtenido de kali linux: https://es.wikipedia.org/wiki/Kali_Linux

wikipedia. (24 de marzo de 2021). Obtenido de nmap: https://es.wikipedia.org/wiki/Nmap

wikipedia. (27 de febrero de 2021). Gestión de información y eventos de seguridad. Obtenido de https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_informaci%C3%B3n_y_eventos_de_seguridad#cite_note-margaret-1

WIKIPEDIA. (27 de FEBRERO de 2021). Gestión de información y eventos de seguridad. Obtenido de https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_informaci%C3%B3n_y_eventos_de_seguridad

Wikipedia. (17 de febrero de 2021). Que es un Cortafuegos. Obtenido de https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)

wikipedia. (19 de marzo de 2021). virtualbox. Obtenido de https://es.wikipedia.org/wiki/VirtualBox

wikipedia. (2021 de marzo de 2021). wikipedia Metasploit. Obtenido de https://es.wikipedia.org/wiki/Metasploit

WIKIPEDIA. (s.f.). WIKIPEDIA. Obtenido de Oracle VM VirtualBox : https://es.wikipedia.org/wiki/VirtualBox