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

JOSE HERNEY JIMENEZ PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

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

JOSE HERNEY JIMENEZ PEREZ

Informe Técnico
ESPECIALISTA EN SEGURIDAD INFORMATICA

JOHN FREDDY QUINTERO
Director de curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Activo de información. Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Amenaza. Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

Antivirus. Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware

Confidencialidad. Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

Denegación de servicio. Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él.

Disponibilidad. Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

Fuga de información. La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

Incidente de seguridad. Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Integridad. La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

Política de seguridad. Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos.

Ransomware. El ciberdelincuente, toma control del equipo infectado y secuestra la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

SGSI. Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001.

Suplantación de identidad. Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling).

Troyano. Se trata de un tipo de malware o software malicioso que se caracteriza por carecer de capacidad de autorreplicación. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación.

Vulnerabilidad. Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota.

RESUMEN

La implementación de equipos de respuesta Red team y Blue team buscan mejorar la seguridad de los sistemas de las compañías y entidades, simulando ataques y verificando la contención o prevención que tiene establecida. Esto permite identificar las vulnerabilidades, amenazas y fallas de seguridad. Todo esto se presenta en el marco normativo del estado colombiano frente a la seguridad de la información. Se recomiendan las herramientas utilizadas por los equipos Red team y Blue team para el desarrollo de estrategias de seguridad que brinden una utilidad importante tanto en la simulación de ataque como en defensa.

INTRODUCCIÓN

Como resultado a lo experimentado con la entidad WhiteHouse Security realizamos este informe que busca plasmar lo aprendido sobre equipos de respuesta Blue Team y Red Team. Revisaremos el marco legal colombiano con lo respectivo a delitos informáticos y el código de ética para el análisis del acuerdo de confidencialidad sugerido por WhiteHouse Security.

Se aplica el procedimiento de Red Team para la simulación de un ataque en un ambiente de prueba para entender el uso de exploit con la aplicación de HFS en un sistema Windows 7. Posteriormente se analiza la contención que debería aplicar el Blue Team como respuesta a un ataque ejecutado.

Conocer herramientas tanto de RT & BT que ayuden a cumplir el propósito de cada equipo, mejorando así la seguridad en los sistemas de información de la compañía.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Construir un informe técnico en el cual se presenten los aspectos más relevantes del desarrollo de las actividades del Seminario Especializado que permitan fortalecer las los conocimientos de los equipos de seguridad Red Team & Blue Team como estrategia a la seguridad de la información.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar las leyes y códigos que apliquen a los delitos informáticos y a al ejercicio de la profesión relacionada con la seguridad de la información.

- Comprender como el desarrollo y aplicación de las pruebas de intrusión en unsistema informático puede ayudar a resolver el incidente de seguridad en WhiteHouse Security, al permitir identificar los fallos y vulnerabilidades existentes a nivel de sistema operativo en los equipos atacados.

- Analizar el ataque informático, desde la perspectiva de Blue Team y Read Team, ocurrido en WhiteHouse Security y establecer las acciones iniciales y medidas de hardenización que se deben implementar en la infraestructura tecnológica de la organización para lograr la contención exitosa del ataque y evitar que se vuelva a repetir.

- Sustentar mediante un video el desarrollo de las actividades realizadas en el Seminario Especializado Equipos Estratégicos en Ciberseguridad Red Team & Blue Team.

2 MARCO LEGAL SOBRE DELITOS INFORMATICOS EN COLOMBIA

En Colombia se ha venido trabajando por parte del gobierno nacional en fortalecer la legislación frente a los crecientes delitos informáticos. Como futuros especialistas en seguridad de la información es importante conocer la normatividad existente en el campo de la ciberseguridad. Las siguientes son las leyes más importantes hoy en Colombia frente a este tema:

2.1 LEY 1273 DE 2009 “DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS”

Mediante esta ley se modificó el código penal y se creó un bien jurídico tutelado con el fin de preservar los sistemas que utilicen las tecnologías de la información y las comunicaciones[1].

Con la ley 1273 de 2009 se busca tipificar los delitos informáticos de la siguiente manera:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva.
- Artículo 269I: Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos.

Estas tipificaciones o mejor, quienes incurran en estos delitos podrán tener una pena de prisión de entre 36 y 96 meses y multas de entre 100 y 1000 smlmv.

Resumiendo, los artículos encontramos que quien acceda a un sistema del sector privado o público sin autorización alguna, así no genere ninguna afectación ni

[1] MINTIC. Ley 1273 5 Ene 2009. Disponible en https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

perdida para el dueño del sistema puede tener una incidencia penal. Así mismo aquel que obstaculice o impida el funcionamiento de un sistema informático, como puede ser una denegación de servicio “DDoS”, una saturación de canal, etc. El hecho de interceptar datos sin la debida autorización también trae consecuencias penales, esta puede ser inclusive en la red pública de internet sin necesidad de estar en la red interna del dueño del sistema informático. Todo aquel que borre, dañe o altere datos de un sistema incurre en el delito del articulo 269D. En cuanto al software malicioso, no solo tiene pena quien lo introduzca en un sistema, sino todo aquel que lo produzca lo trafique, adquiera, venda o envíe. El articulo 269F proteja los datos personales, la persona que intercambie, divulgue o modifique las bases de datos de personas también tiene pena de prisión.
El suplantar sitios web también se encuentra como delito en esta ley; cualquiera que diseñe programe o envíe enlaces de páginas de suplantación.

El hurto por medios informáticos es de los delitos más cometidos en Colombia junto con la transferencia no consentida de activos. Estos se observan por ejemplo cuando el atacante roba datos de credenciales bancarias y transfiere dinero de las cuentas de la víctima a otra cuenta bancaria que puede ser propia o de un tercero.

Según la ley 1273 existen circunstancias agravantes que pueden aumentar la pena desde la mitad hasta las tres cuartas partes:

1. Si la falta se comente en entidades estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Si el delito es cometido por un servidor público en ejercicio de sus funciones
3. Si hay aprovechamiento de confianza por parte del dueño del sistema, como puede ser el caso de un empleado con su empleador.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Si obtiene provecho para si o para un tercero.
6. Si se comete el delito con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Si utiliza como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, como por ejemplo un administrador de Firewall o de la seguridad informática de una empresa, además de una inhabilitación del ejercicio de la profesión relacionada.

2.2 LEY 1581 DE 2012. PROTECCION DE DATOS PERSONALES.

Mediante esta ley que tiene por objeto desarrollar el derecho que tienen las personas de conocer, actualizar y rectificar la información personal que existan en las bases de datos. Esta ley es aplicable a entidades tanto publicas como privadas que traten bases de datos con información personal. En ella encontramos unos principios rectores para el tratamiento de datos personales[2]:

- Principio de legalidad.
- Principio de finalidad.
- Principio de libertad. El tratamiento de los datos personales solo puede darse con el consentimiento previo y expreso del titular. No podrán ser obtenidos sin previa autorización.[3]
- Principio de veracidad o calidad.
- Principio de transparencia.
- Principio de acceso y circulación restringida. Los datos personales no podrán estar disponibles en internet ni en ningún otro medio de comunicación masiva.
- Principio de Seguridad. La información personal deberá se manejada con medidas técnicas, humanas y administrativas que sean necesarias para dar seguridad a los registros evitando cualquier adulteración, perdida, consulta indebida uso o acceso no autorizado.
- Principio de Confidencialidad. Las personas que intervengan en el tratamiento de los datos personales están obligadas a garantizar la reserva de la información.

Con esta ley se busca un mayor control sobre las bases de datos que contienen información personal en especial la información sensible. Para ser tratada, almacenada y/o transmitida la información debe ser autorizada por el titular. Esta autorización debe obtenida por un medio que pueda ser consultada posteriormente y en ella debe especificarse la finalidad de la información suministrada por el titular.

---

[2] SECRETARIA SENADO. Ley estatutaria 1581 de 2012. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[3] SIC. Protección de Datos Personales. Disponible en: https://www.sic.gov.co/preguntas-frecuentes-pdp#:~:text=La%20Ley%201581%20de%202012%20proh%C3%ADbe%20la%20transferencia%20de%20datos,e%20inequ%C3%ADvoca%20para%20la%20transferencia.

3 ETAPAS DEL PENTESTING

El pentesting consiste en realizar pruebas de penetración sobre un sistema informático utilizando diversas herramientas y diversas técnicas con el fin de encontrar vulnerabilidades, fallas en la configuración o desactualizaciones. Esta práctica es legal siempre y cuando se tenga el consentimiento pleno del dueño del sistema y de las limitantes que este estipule. La intención al realizar un pentesting es mejorar la seguridad del mismo sistema verificando el estado de seguridad y encontrando las falencias y oportunidades de mejora.

Existen varias metodologías o estándares para realizar un pestenting, algunas con procedimientos más específicos que otros, sin embargo, se destacan unas etapas comunes o principales como son las siguientes:

3.1 PLANIFICACION

Es la coordinación inicial donde se establecen los lineamientos y el alcance. Definir el tipo de pentesting y definir las limitaciones. También se acuerda el periodo de duración y el objetivo de la evaluación.

3.2 DETECCION

Es la etapa donde se recolecta la mayor información posible del sistema. Se puede realizar un escaneo de red interna y/o publica, servidores, sistemas operativos, aplicaciones, equipos de usuario final y herramientas de seguridad. El objetivo es encontrar los puntos débiles y analizar los posibles escenarios de explotación.

Herramientas utilizadas: Nmap, Nessus, Openvas.

3.3 EXPLOTACION

Una vez identificados los puntos vulnerables llega el momento de hacer la penetración al sistema. Por medio de diversas herramientas se busca explotar esas vulnerabilidades encontradas. Después de estar dentro del sistema se busca mantener los accesos y hacer movimientos laterales para poder acceder a los diversos recursos del sistema.

Herramientas utilizadas: Metasploit

3.4 REPORTE

Finalizada la penetración se eliminan los cambios que se hallan realizado sobre la red o los equipos del sistema (backdoors, puertos abiertos, accesos). Se elaboran los reportes correspondientes al pentesting realizado, generalmente se entrega uno técnico y un ejecutivo; estos se diferencian por el lenguaje que se maneja en cada uno y pueda ser entendible para los diferentes grupos de la compañía o entidad. En los reportes se consignan las recomendaciones y conjunto de medidas que ayuden a remediar las vulnerabilidades encontradas.

4 HERRAMIENTAS DE CIBERSEGURIDAD

Conocer herramientas que nos ayuden a la hora de hacer una prueba de penetración es fundamental para la elaboración de un adecuado trabajo. Unas de las herramientas mas conocidas en el ámbito de la ciberseguridad son la siguientes:

4.1 METASPLOIT

Metasploit framework[4] es una herramienta multiplataforma (Unix/Linux, Mac OS y Windows) que nos ayuda a investigar vulnerabilidades de seguridad. Lo interesante es que es de código abierto y gratuita, esto le permite contar con más de 900 exploits para Windows, Linux y Mac OS. También cuenta con módulos o payloads para explotar estas vulnerabilidades.

Esta herramienta es muy útil para efectuar auditorias o pentesting sobre un sistema.

4.2 NMAP

Nmap también es una herramienta gratuita y de código abierto. Ésta es especifica para el descubrimiento de redes como parte de una auditoria de seguridad. Útil para el inventario de red, Ha sido usada para escanear redes de cientos de miles de máquinas.[5] Nmap utiliza docenas de técnicas avanzadas de mapeo de red incluso con filtros IP, firewalls y routers de por medio. Escanea puerto tanto UDP como TCP, detecta el tipo de sistema operativo e inclusive la versión utilizada.

4.3 OPENVAS

Openvas[6] en una herramienta de código abierto y gratuita utilizada para realizar análisis de uno o varios hosts. Mediante un escáner de vulnerabilidades se verifican los puertos abiertos y posibles vulnerabilidades. Lo interesante es que genera un reporte con las alertas al finalizar el escaneo. Tiene su versión por comandos (CLI) o por interfaz web. Puede utilizarse desde Metasploit. Openvas viene por defecto en las distribuciones de Kali Linux.

---

[4] METASPLOIT. Metasploit. Disponible en https://www.metasploit.com/

[5] NMAP ORG. Introducción. Disponible en https://nmap.org/

[6] OPENVAS. Openvas. Disponible en: https://www.openvas.org/

4.4 EXPLOITDB

Es una de las bases de datos de exploits gratuitos mas populares. Es un proyecto de Offensive Security que busca plasmar en una base de datos los exploit públicos y de software vulnerable para su investigación y que sea útil para pruebas de penetración. Esta base crece conforme va pasando el tiempo, sin embargo, esta permite filtrar por tipo de plataforma, etiquetas vulnerabilidades, etc.

Cabe mencionar que existen otras bases de datos de exploits como los son Rapid7, CXSecurity, Vulnerability Lab, Google Hacking Database, entre otras.

4.5 CVE

Por sus siglas en ingles Common Vulnerabilities and Exposures. es una lista de identificadores comunes para vulnerabilidades de ciberseguridad conocidas. Mediante CVE se estandariza la descripción y la identificación de una vulnerabilidad lo que lo hace útil para su divulgación en los equipos de ciberseguridad para su análisis y remediación. Es una herramienta gratuita y de uso público. Suele mostrar un acceso directo a la información de la vulnerabilidad y donde puede conseguirse mas detalles.

5 ANALISIS ANEXO 2 Y 3 (TIPO LEGAL)

Se solicita por parte de la compañía WhiteHouse Security, como parte de un proceso de selección de personal, la revisión de un acuerdo de confidencialidad que aparentemente tiene problemas de legalidad. Se menciona la importancia que el candidato debe poder trabajar bajo presión y dar respuesta en corto tiempo.

Para el análisis del acuerdo (Anexo 3) se resaltan las siguientes irregularidades que se solicita sean revisadas:

1. En el apartado número 2, se observa un espacio en blanco el cual encerramos en un cuadro (En contratos y en documentos como acuerdos no pueden existir este tipo de espacios vacíos. Se podría añadir información sin consentimiento del aspirante).

2. En la cláusula primera se menciona que la parte receptora se obliga a no divulgar directa ni indirectamente información confidencial sobre “procesos ilegales”. Es un deber general de los profesionales denunciar delitos contravenciones y faltas, aportando toda la información y pruebas que sea posible. Así mismo se deben hacer respetar las disposiciones legales y reglamentarias, como denunciar sus transgresiones.

3. En la cláusula segunda habla explícitamente de datos secretos como “datos de chuzadas e interceptación de información”. Lo que da a entender una clara violación a la ley por interceptación de datos informáticos y violación de datos personales.

4. En la cláusula tercera aclara que la el origen de la información confidencial puede ver con creaciones del intelecto por lo que el aspirante debe ser precavido ya que puede existir una posible violación a los derechos de propiedad intelectual y derechos de autor.

5. Clausula cuarta habla de adicionar obligaciones según la necesidad que el titular de la información manifieste. De tener muy en cuenta que las adiciones de obligaciones deben ser concertadas y no generadas de forma unilateral.

6. La cláusula cuarta numeral tres y cuatro de forma explícita solicita no denunciar ante las autoridades actividades sospechosas de “espionaje” o cualquier “información confidencial e ilegal” que conozca. Esto va en contra del código de ética y del deber de los profesionales para con la dignidad de la profesión, donde se indica que se deben respetar las disposiciones legales, así como denunciar sus transgresiones.

7. Clausula cuarta numerales siete, ocho y nueve hacen a la parte receptora responsable ante las autoridades en algún caso de allanamiento. En el código de ética, en el artículo 39 indica que es deber de los profesionales para con los clientes mantener en secreto todo trabajo que se realice para éste, salvo “obligación legal” de revelarla.

8. En la cláusula octava solicita “dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security”. Esto va en contra del código de ética. Es deber de los profesionales denunciar delitos y faltas tanto del código como de las disposiciones legales vigentes.):

5.1 ANALISIS SEGUN LEY 1273 DE 2009

Después de revisar y analizar el acuerdo de confidencialidad nos damos cuenta que se puede estar violando la ley 1273 de 2009 en los artículos[7]:

“Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.” En la cláusula segunda del acuerdo menciona “accesos abusivos a sistemas informáticos” lo que puede llevar al aspirante a incurrir de manera indirecta con la violación al artículo 269A.

“Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema

[7] SECRETARIA SENADO. LEY 1273 DE 2009. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

informático que los transporte.” Según el acuerdo en la cláusula segunda define como parte de la información confidencial que manejará el aspirante menciona de manera explícita “datos de chuzadas, interceptación de información” lo que claramente induce en la violación al artículo 269C.

“Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.” El acuerdo no es claro con el tipo de información que se puede llegar a manejar, ya que menciona que puede provenir de cualquier fuente (Clausula 3ra) y adicionalmente que puede ser ilegal (Clausula 4ta. Num 9), lo que podría tratarse de datos personales. El artículo es claro que cualquier persona que manipule de alguna forma ese tipo de información tendrá pena de prisión.

Se pueden aplicar estos agravantes de la ley 1273 de acuerdo a la lectura del acuerdo:

“Sobre redes o sistemas informáticos o de comunicaciones **estatales** u **oficiales** o del sector financiero, nacionales o extranjeros.” La compañía The WhiteHouse Security, según el anexo 2, asesora gobiernos, por lo que la información que trata muy probablemente es gubernamental o de tipo político. Los agravantes aumentan de la mitad a las tres cuartas partes de la pena.

“Con fines terroristas o generando riesgo para la seguridad o defensa nacional.” El manejo de información confidencial del estado conlleva mucha responsabilidad para cualquier profesional de la seguridad de la información, si se administra de forma incorrecta puede ponerse en riesgo la seguridad nacional.

“Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.” El acuerdo establece que el receptor es el responsable de la administración de la información y al ser ilegal en caso de aceptar el acuerdo podríamos exponernos a este agravante y afectar el ejercicio de nuestra profesión.

5.2 ANALISIS DE LA PROPUESTA (CODIGO DE ETICA)

Son varias las irregularidades observadas en el documento. Mencionamos a continuación los artículos del código de ética para el ejercicio de la ingeniería en general y sus profesiones afines[8]:

“ARTÍCULO 31. f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.” La compañía Whitehouse Security no puede quedar exenta de responsabilidad en caso de incurrir en un delito. Es un deber del profesional denunciar cualquier falta que observe y que viole las leyes colombianas.

“ARTÍCULO 33. f) Ejercer la profesión sin supeditar sus conceptos o sus criterios profesionales a actividades partidistas.” Conforme a este articulo no se podría firmar el acuerdo tal como está. Se debe imponer los conocimientos profesionales y de las leyes colombianas del aspirante a la hora de observar transgresiones a la ley.

“ARTÍCULO 34. g) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación.” Este acuerdo va en contra de la ley, puesto que solicita mantener en secreto información que puede ser ilegal. No es posible aceptar este acuerdo de forma ética.

“ARTÍCULO 35. b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.” Es un deber denunciar cualquier delito que se observe en el ejercicio de la profesión.

“ARTÍCULO 39. a) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo.” El acuerdo de confidencialidad puede mantenerse, siempre y cuando no vaya en contra de las disposiciones legales del estado, ni atente contra la seguridad nacional.

[8] COPNIA. Código de Ética. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

“FALTAS GRAVÍSIMAS. e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares.” Los delitos en los que pueda incurrir el aspirante debido a información que atente en contra del estado se considera falta gravísima que puede ocasionarle la cancelación de la matricula profesional.

Validando estos artículos se evidencia que hay procesos poco confiables según se muestra en el acuerdo de confidencialidad. Por lo tanto, sin importar la cifra considerable de salario y las prestaciones que pueda representar confirmo que no firmaría el documento, puesto que va en contra de las disposiciones éticas y legales. El firmarlo conlleva un riesgo alto que puede materializarse en la perdida de la matricula profesional, pasando por una pena pecuniaria o hasta la privación de la libertad.

6 ANALISIS RED TEAM

Obtenida la información inicial suministrada por la empresa WhiteHouse Security procedemos de forma metódica a analizar los fallos de seguridad.

6.1 HERRAMIENTAS UTILIZADAS

Es importante conocer las herramientas de reconocimiento en cualquier proceso de pentesting o de análisis de vulnerabilidades.

6.2 NMAP

Nmap es una herramienta gratuita y de código abierto utilizada para el mapeo de red. Funciona utilizando paquetes IP sin procesar que se envían a través de la red. Con Nmap se puede realizar un inventario de dispositivos conectados, identificar los puertos abiertos que pueden ser explotados. También es posible identificar las reglas de firewall aplicadas a la red.

Nmap, que se ejecuta por línea de comandos, también tiene una versión GUI llamada Zenmap que fue creada por los mismos desarrolladores. Zenmap es utilizada principalmente por principiantes ya que es más sencilla de usar.

Por línea de comando es posible escanear un sistema por nombre o por IP:

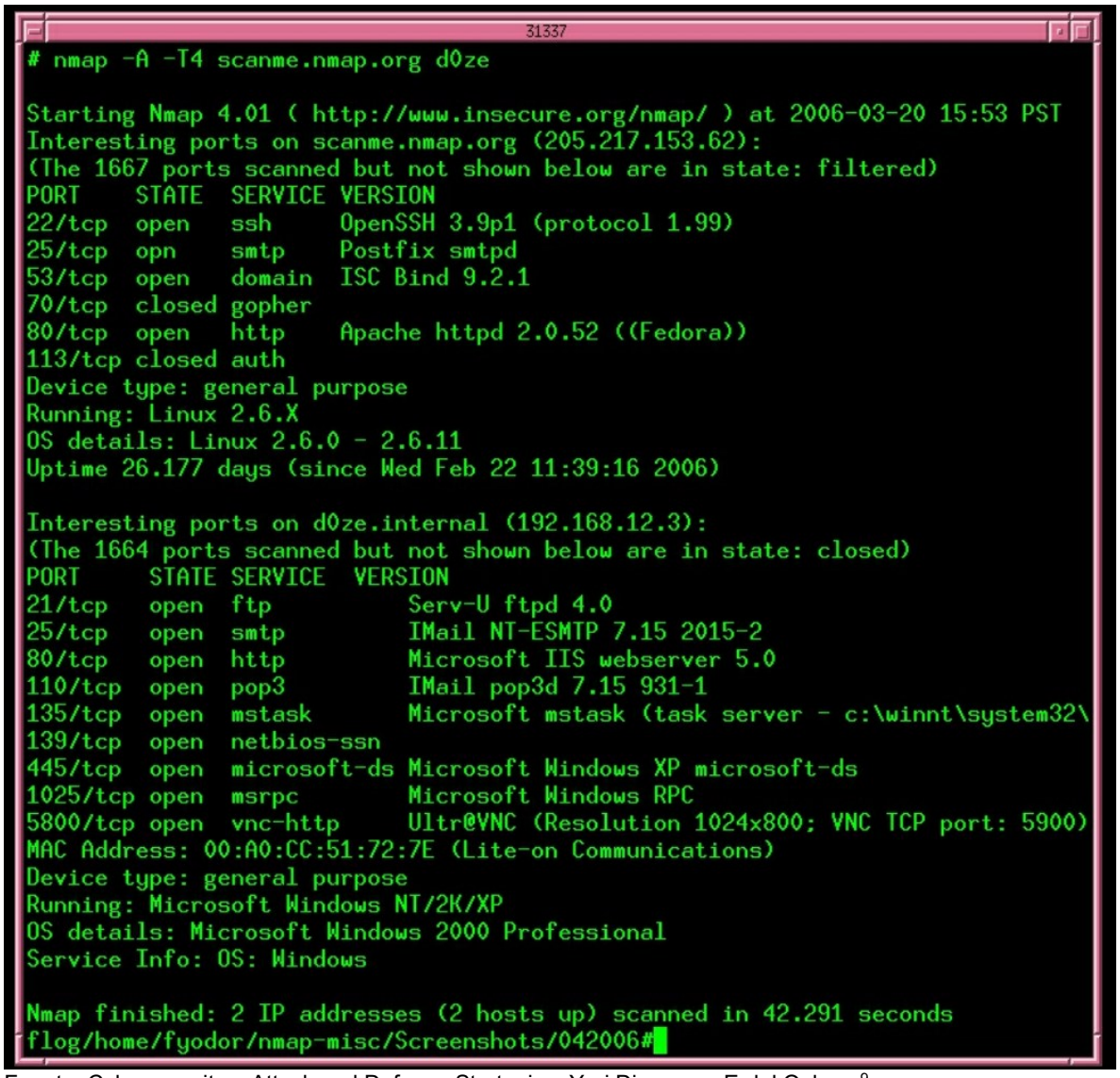
#nmap www.bancatuya.com

#nmap 255.250.123.189

Estos comandos son utilizados generalmente en combinación de otros como TCP SYN, Scan and Connect, UDP Scan, y FIN Scan.

El siguiente es un ejemplo de un escaneo a dos IP. Una publica y una privada. Se observan según los resultados del escaneo los puertos que están abiertos y cerrados, así como los servicios que está corriendo.

Figura 1. Ejemplo NMAP



Fuente: Cybersecurity – Attack and Defense Strategies. Yuri Diogenes, Erdal Ozkaya[9]

6.3 METASPLOIT

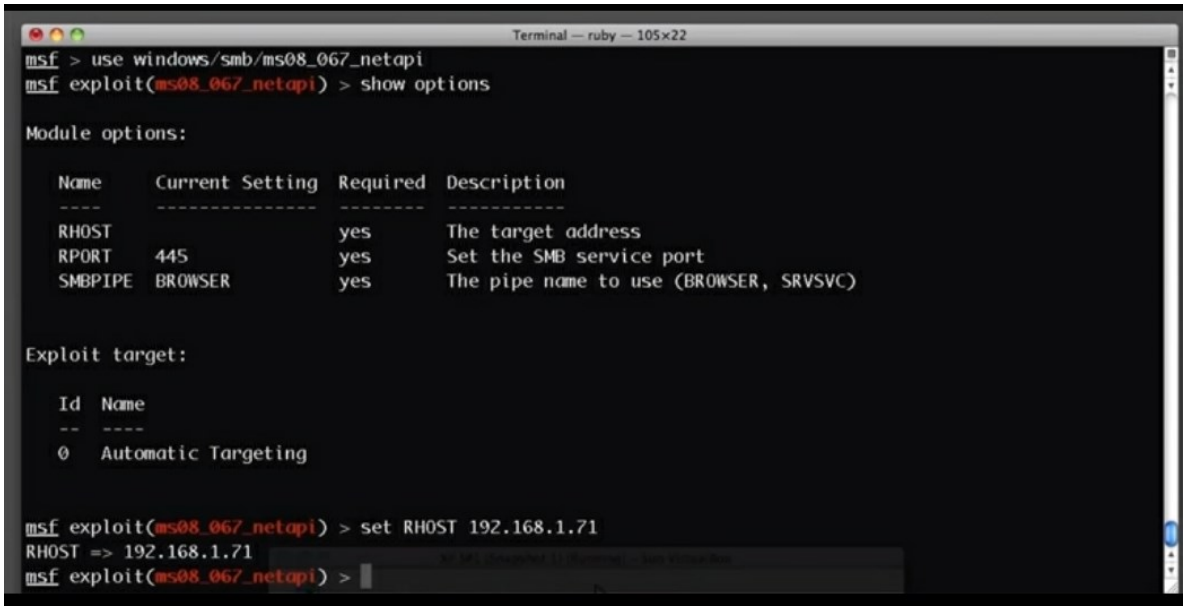
Es un framework orientado al hacking, basado en Linux. Ha sido utilizado innumerables veces por hackers. Esto debido a que cuenta con numerosas herramientas para realizar diferentes tipos de ataques. La herramienta recibió la atención de los profesionales de seguridad y hoy en día se utiliza para enseñar hacking ético. Metasploit también se utiliza para pruebas de penetración que los

[9] YURI DIOGENES, ERDAL OZKAYA. Cybersecurity - Attack and Defense Strategies.

hackers suelen utilizar para realizar ataques. Por medio de una línea de comandos pueden lanzarse exploits en función del objetivo.

El siguiente es un ejemplo de la interfaz de Metasploit apuntando a la ip 192.168.1.71:

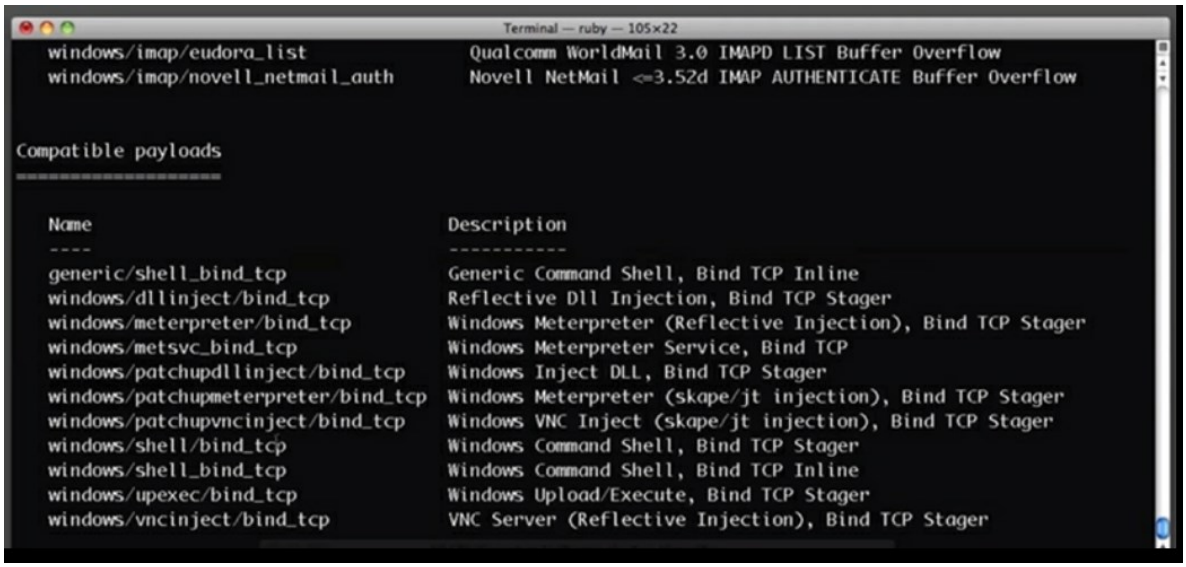
Figura 2. Interfaz Metasploit



Fuente: Cybersecurity – Attack and Defense Strategies. Yuri Diogenes, Erdal Ozkaya

Observamos los diferentes payloads compatibles que pueden desplegarse en el target:

Figura 3. Ejemplo Payloads Metasploit



Fuente: Cybersecurity – Attack and Defense Strategies. Yuri Diogenes, Erdal Ozkaya

6.4 METERPRETER

Meterpreter es quizá la herramienta más poderosa de Metasploit. Con esta herramienta es posible obtener una gran cantidad de información sobre un objetivo comprometido. Con algunos comandos se puede manipular características del sistema. Es una especie de interprete que permite interactuar con el host o servidor comprometido en procesos ya de post-explotación[10].

Los comandos o utilidades que sobresalen son[11]:

KEYSCAN. Es posible capturar lo que el usuario digita en la máquina. Así se podrían obtener credenciales, correos, etc.

ROUTE. Con este comando es posible modificar la tabla de enrutamiento del host.

DOWNLOAD. Con este comando se descargan los ficheros o archivos desde la maquina remota.

---

[10] THE HACKER WAY. Conceptos Basicos de Meterpreter – MetaSploit Framework. Disponible en: https://thehackerway.com/2011/04/26/conceptos-basicos-de-meterpreter-metasploit-framework/#:~:text=COMANDOS%20DE%20METERPRETER%20EN%20SISTEMAS%20WINDOWS

[11] OFFENSIVE-SECURITY. Meterpreter basic commands. Disponible en: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

CD. Permite moverse entre directorios.

LS. Permite listar los archivos del directorio actual.

PS. Muestra la lista de procesos que se encuentran corriendo en el objetivo.

SEARCH. Busca la locación de un archivo especifico en todo el sistema o en una carpeta especifica.

WEBCAM_SNAP. Guarda una foto con la cámara web de la computadora comprometida. Esta imagen la guarda en JPEG en el directorio actual.

SCREENGRAB. Toma un PrintScreen del equipo victima y lo guarda directamente en un directorio del Kali Linux.

6.5 DATOS SUMINISTRADOS O INFORMACION INICIAL

La información suministrada por el usuario quien nos solicita un análisis de fallos de seguridad es muy valiosa a la hora de buscar el origen de la brecha o el fallo. En este caso nos indican posibles causas de la fuga de información que debemos tener en cuenta.

WINDOWS 7 X64. Esta versión de Micosoft fue lanzada en 2009. El soporte general sobre este sistema operativo finalizó en enero de 2015 y el soporte extendido finalizó en 2020.

En el análisis de vulnerabilidades entra mucho en juego los sistemas operativos que se usan en el sistema. Por ejemplo, si las actualizaciones de seguridad como en el caso de Windows 7, como el soporte del fabricante finalizan, es muy probable que ese sistema operativo se convierta en vulnerable y con el paso del tiempo sea más fácil explotar vulnerabilidades, existiendo mayor cantidad de exploits.

HFS REJETTO V.2.3. La versión actual de HFS (Http File Server) es la 2.3m, lanzada en 2018. La versión de la aplicación instalada en el Windows de nuestro caso es de una fecha anterior al año 2014. Buscamos en las bases de CVE con el nombre Rejetto y encontramos 3 aplicables a diferentes versiones de la aplicación.

Hace parte de la investigación determinar desde cuando está instalada la aplicación, e indagar cómo se instaló y si fue con consentimiento del usuario, confirmar el motivo. Obteniendo estas respuestas se podría determinar que la aplicación exista en más equipos dentro de la red de la organización.

Por medio de un sistema de control de aplicaciones, o de un antivirus avanzado se podría escanear si hay más equipos corriendo esta aplicación vulnerable. Esto es importante si se desea minimizar el riesgo de que exista más filtraciones de información.

ESCALAMIENTO DE PRIVILEGIOS. Con sospechas de escalamiento de privilegios el riesgo que se corre por parte de la compañía es alto. Por medio de esta técnica se pueden realizar movimientos laterales llegando incluso a tomar gestión de administradores de red, bases de datos, sistemas de seguridad, control de CCTV, administradores de servidores, etc. Este sin duda es uno de los escenarios más indeseables para cualquier compañía que se preocupe por la seguridad de sus datos.

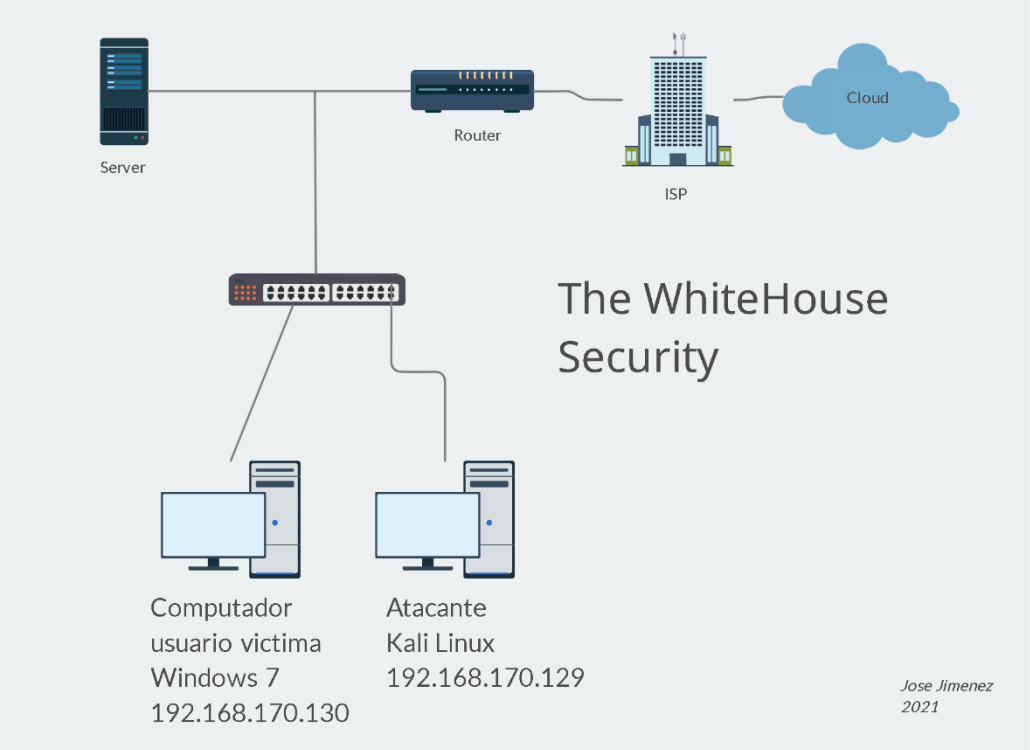
De acuerdo a la infraestructura de la compañía, lo primero es bloquear cualquier permiso o acceso que tenga habilitada la cuenta sospechosa. Además de rastrear posibles logs de autenticación como búsqueda de rastros que permitan detectar el origen del ataque.

Si es necesario realiza un análisis forense que ayude a determinar el origen del fallo de seguridad.

6.6 FUNCIONAMIENTO DEL ATAQUE

Obtenemos la topología de red de la empresa WhiteHouse Security. En ella encontramos el segmento lan 192.168.170.0/24. Se determina que el ataque proviene de la misma red interna. El usuario que tiene el equipo comprometido con la fuga de información tiene por IP 192.168.170.130.

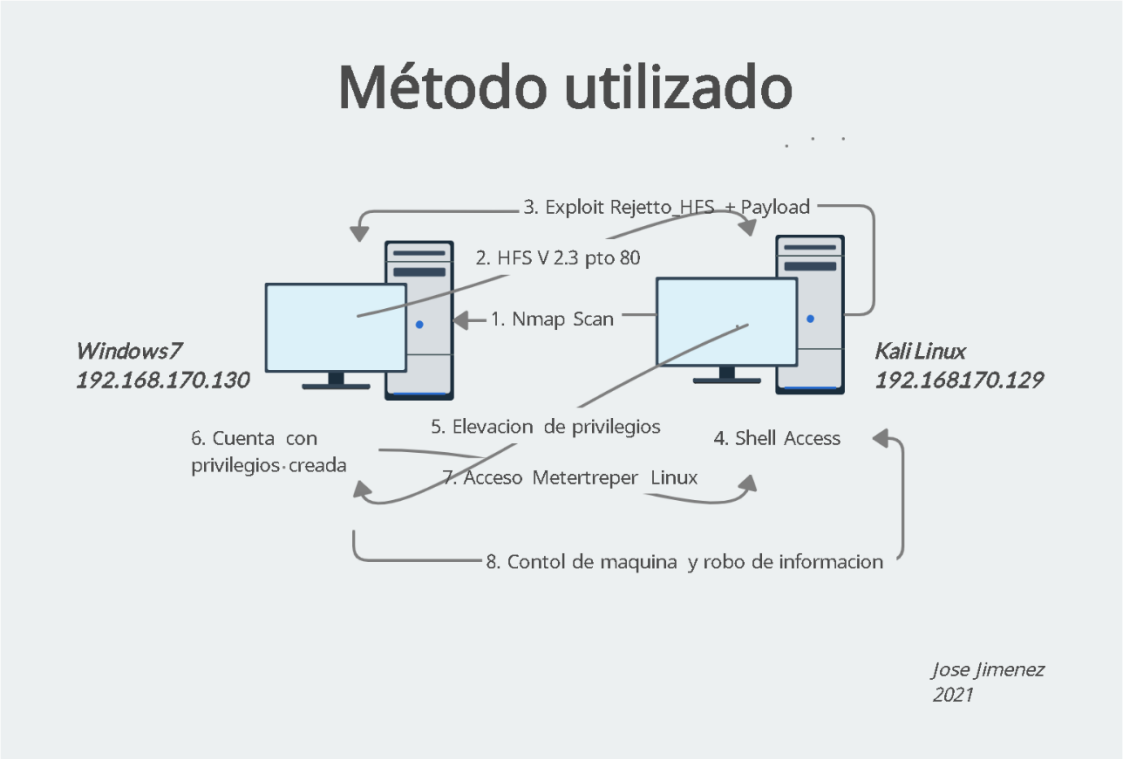
Figura 4. Topologia red WhiteHouse Security



Fuente: Propia

El método que se utilizó fue una explotación de una vulnerabilidad conocida sobre la aplicación portable HFS en su versión 3.2. Mediante un Kali Linux dentro de la red con IP del mismo segmento (192.168.170.129). Se realizó un escaneo de red obteniendo por medio de un Nmap la visualización del puerto 80 activo en un host. Se obtuvo un Shell de acceso después de explotada la vulnerabilidad tomando así el control de la maquina remotamente, luego de crear un usuario con privilegios que le permitía copiar archivos alojados en el computador del usuario. En el punto 3.5 de este documento se muestra de manera detallada el proceso de explotación y escalamiento de privilegios.

Figura 5. Método utilizado.



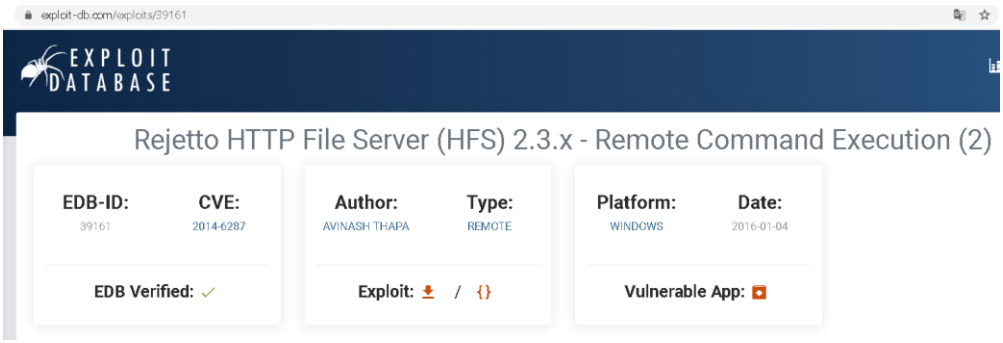
Fuente: Propia

6.7 DEMOSTRACION DE LA EXPLOTACION DE LA VULNERABILIDAD

Realizamos paso a paso la demostración del ataque realizado al interior de las instalaciones de WhiteHouse Security.

Se realiza un escaneo de IP y luego de detectar las activas se realiza un escaneo Nmap con el objetivo de verificar los servicios activos y protocolos en estado de escucha. Encontramos el puerto 80 usando la opción “-A” con Nmap para que se esfuerce en identificar el sistema operativo, los servicios y versiones del destino.
Con el comando aplicado logramos identificar la aplicación HFS 2.3, ademas del sistema operativo Windows. Buscamos informacion de la aplicación y encontramos que es un desarrollo que permite enviar y recibir archivos, no necesita instalacion (Portable) y utiliza la comunicación web para ello. Buscamos vulnerabilidad de la version vista en el equipo windows y encontramos exploit existentes del tipo Remote().

Figura 6. Explit Database. Vulnerabilidad HFS.



Fuente exploit-db.com

Mediante el Metasploit tambien se puede buscar vulnerabilidades de aplicaciónes por nombre.

Ingresamos a la consola de Metasploit y ponemos la carga útil “reverse_tcp”. Este es un Shell inverso. De esta manera hacemos que el host victima inicie la conexión con el atacante.

Ejecutamos el comando exploit para explotar la vulnerabilidad encontrada. Observamos que inicia automáticamente la herramienta Metertreper que nos indica que ya se tiene acceso al equipo víctima. Podemos confirmarlo ejecutando comandos como sysinfo que nos trae información del sistema.

Por medio de un Ipconfig confirmamos que es la Ip del host victima (192.168.170.130).

Por medio del comando getuid obtenemos la “identidad del usuario” o validamos ls privilegios que tenemos. Adicionalmente con el comando hashdump podremos obtener los hashes en NTLM de las cuentas de usuario creadas en el equipo víctima. Con esta información se podría hackear las credenciales de acceso mediante una herramienta como John the Ripper.

Mediante el comando Shell y gracias al payload cargado podemos tener control sobre la maquina como si ingresáramos al cmd directamente al equipo Windows.

Ya estando en este punto es posible crear cuentas de usuario y agregarlos al grupo de administradores locales.

Si entráramos a la maquina victima podríamos comprobar que el usuario se crea y tiene privilegios de administrador.

Por último, teniendo ya privilegios sobre la maquina víctima del exploit es posible movernos desde el cmd a las diferentes locaciones del PC y extraer la información que deseemos. Esto mediante el comando “download” de metertreper. Como ejemplo creamos un archivo de nombre “base_datos.txt” en el escritorio de la víctima y posteriormente lo descargamos desde el Kali Linux.

El tiempo de descarga dependerá del tamaño del archivo y la latencia de la red. Confirmamos que el archivo base_datos.txt se encuentra ya en nuestra maquina Kali Linux en la carpeta “estudiante”.

7 ANALISIS BLUE TEAM (CONTENCION)

El primer paso de la contención es el aislamiento de los equipos comprometidos. Si el ataque se desplegó con un malware o un virus es posible que infecte o haya infectado a más equipos dentro de la misma red. Este aislamiento va desde la desactivación del puerto del switch de comunicaciones por parte del departamento de TI, o en su defecto la desconexión física y de la red Wifi en caso de que cuente con ese tipo de conexión.

El segundo paso es hacer un copiado del equipo o equipos comprometidos teniendo especial cuidado con la memoria volátil, ya que en esta se puede obtener información por medio de herramientas tecnológicas forenses, como por ejemplo la ejecución de una aplicación en segundo plano, entre otros procesos que ayudan a entender el método del ataque.

Al mismo tiempo que se revisan los equipos, se puede indagar al usuario si ha recibido información sospechosa, como puede ser un correo electrónico, si ha usado USB en el equipo de origen desconocido, o ha instalado aplicaciones ajenas a las usadas en su cargo.

Por parte del SOC se debe analizar logs de las herramientas de monitoreo, como puede ser el Firewall, IPS/IDS, logs en los equipos de comunicaciones, routers, switch, sistema de autenticación de usuarios, cambios en directorio activo, entre otros.

En el ejercicio realizado nos muestra un caso de ataque de tipo exploit por el uso de una aplicación de versión explotable como lo es HFS (Http File Server) en su version 2.3 de Rejetto[12]. Luego del ataque se realiza un escalado de privilegios sobre un equipo dentro de la red de WhiteHouse Security.

Aunque el Blue team y el CSIRT (Equipo de Respuesta a Incidentes de Seguridad) tienen como objetivo la defensa de la entidad frente a los ataques o riesgos informáticos relacionados con la seguridad de la información, tienen diferencias en su función.

El Blue Team se encarga del monitoreo constante de los sistemas informáticos dedicados a la seguridad. Ejecuta mejoras de configuración, actualiza y previene

[12] Rejetto. Disponible en https://www.rejetto.com/hfs/

vectores de ataque que puedan existir al interior o desde el exterior de la organización.

CSIRT. El CSIRT está orientado a la respuesta luego de que el incidente de seguridad ocurre. Su objetivo es minimizar el impacto que pueda tener en la organización. Va de la mano con el equipo de continuidad de negocio. El equipo de respuesta a incidentes coordina cualquier evento que se presente que ponga en riesgo los sistemas de información. Es el equipo responsable de los informes y toda actividad relacionada con incidentes de seguridad dentro de la organización.

CIS. El CIS es el Centro para la Seguridad de Internet[13], con oficina en New York. Su objetivo es promover y desarrollar soluciones de mejores prácticas para la defensa cibernética. Esta organización busca que el ciberespacio sea un lugar seguro y confiable. Como parte de un equipo de Bllue team recibiríamos información importante y actualizada de nuevas amenazas en internet, así como recibir consejos de buenas prácticas en lo relacionado con ciberseguridad, lo que podría aportar en la creación de políticas sobre la seguridad que pueden ser útiles para la organización.

SIEM. El SIEM es un acrónimo que traducido del inglés significa Gestión de información y eventos de seguridad. Es un software que permite detectar fallos y amenazas de seguridad útiles para hacer frente a los riesgos informáticos.

Su característica principal es la de correlacionar eventos proporcionados por los diversos sistemas que puedan existir en una organización. Por ejemplo, se puede configurar que el Firewall de la organización y los switch de comunicaciones envíen logs hacia el SIEM. Si existe un evento que involucre los dos sistemas el SIEM es capaz de relacionarlos y aportar información que lo identifique como un incidente de seguridad o no.

Este sistema es especialmente útil cuando se tiene una gran cantidad de información que analizar a la hora de toparse con un evento que ponga en riesgo la seguridad de la información, ya que centraliza la información. Este crea alertas sobre la misma información que recibe reconociendo patrones de ataque.

HERRAMEINTAS DE CONTENCION

[13] CIS. Disponible en https://www.cisecurity.org/

1. ANTIVIRUS. Una de las herramientas principales de contención son los antivirus. Esta herramienta es útil no solo para los equipos de cómputo que utilizan los usuarios, sino que también es eficaz en servidores y dispositivos móviles. Es posible que, si la maquina está infectada con malware, un simple escaneo sea suficiente para eliminarlo. Existen Antivirus que se administran de forma centralizada lo que permite realizar ajustes finos sobre aplicaciones instaladas en los usuarios. Por ejemplo, que todo archivo con extensión ".exe" sea borrada inmediatamente de la carpeta "descargas". Esta sería una buena práctica de seguridad, y al tener centralizada la administración es mucho más fácil que configurar manualmente antivirus en X cantidad de dispositivos.
2. IPS. El IPS es un gran aliado en la seguridad perimetral como contención a alguna actividad sospechosa. Mediante este dispositivo se puede bloquear la comunicación que se realiza de manera externa hacia el interior de la red. Si se conoce la dirección IP desde la que se está realizando un ataque, es posible bloquearla totalmente desde el IPS. Como buena práctica es posible tener una referenciación geográfica de acuerdo al direccionamiento público, y de esta manera se puede prevenir comunicaciones de países que sabemos no deberían tener conexión con nuestra entidad (ejemplo, China, Rusia, Irak, etc)
3. WAF. El Waf (Web Application Firewall) es una herramienta poderosa de contención en ambientes web. Si nuestra compañía tiene publicados servicios web a los usuarios, es imperativo implementar una solución de Waf que prevenga ataques como XXS, alteración de parámetros, desbordamiento de buffer, manipulación de campos hidden, envenenamiento de cookies, entre muchos otros. Al igual que con el IPS, es posible bloquear direccionamiento IP publico sospechoso. Y en caso de un ataque, rechazar completamente el origen de conexión del atacante.

8 RECOMENDACIONES

1. Reforzar políticas de seguridad de la información desde la alta dirección dentro de la compañía que permitan recursos para la implementación de sistemas avanzados que permitan la detección temprana de ataques cibernéticos.
2. Organizar planes de capacitación recurrentes a todos los colaboradores sobre Ciberseguridad y como desde su cargo pueden apoyar los objetivos en seguridad de la información.
3. Crear o reforzar el proceso de identificación de vulnerabilidades sobre todos los sistemas o aplicaciones de la entidad. Realizar escaneos periódicos que permitan identificarlas y que mediante un plan de remediación se responsabilice al propietario del equipo o de la aplicación con un tiempo prudente para solucionarla.
4. Implementar un sistema de control de aplicaciones o MDM sobre los dispositivos suministrados por la entidad que logre identificar las versiones instaladas y operativas.

9 LINK VIDEO SUSTENTACION

https://youtu.be/KRkz-hfvrWc

10 CONCLUSIONES

Como futuros especialistas en seguridad informática debemos estar al tanto de la legislación colombiana frente a los delitos informáticos y la protección de datos personales. La ciberseguridad se está incrementando en todos los sectores y así mismo las regulaciones o normas que emite el gobierno al manejo de la información en red.

Las etapas del pentesting pueden variar de acuerdo a nuestros objetivos o los del propietario del sistema a auditar. Al realizar el proceso de pentesting de una forma ordenada nos generará unos mejores resultados, dándonos mayor efectividad y disminución en el tiempo de ejecución.

Las herramientas de pentesting se actualizan periódicamente y hay que estar al tanto de las mejoras o de nuevas herramientas que nos lleven a la vanguardia de la ciberseguridad. Así mismo debemos estar atentos a las nuevas vulnerabilidades que salen sobre el software o aplicaciones que protejamos.

Con el ejercicio del estudio del acuerdo de confidencialidad de Whitehouse Security pudimos apreciar la importancia de conocer las leyes colombianas en cuanto a la protección de datos personales. Estas leyes están por encima del cumplimento de cualquier contrato laboral y se debe ser cuidadoso con lo que se nos solicita en las empresas para el manejo de información confidencial. Debemos indagar el propósito y la fuente de la información. Podemos realizar las preguntas: ¿La información que voy a administrar son datos personales? ¿La obtención de la información se realiza de manera legal? ¿La información es de algún gobierno? ¿Qué objetivo o que destino tiene la información?

La información inicial para afrontar un caso de análisis de fallos de seguridad es fundamental para la resolución del mismo. El proceso de pentesting por parte de un equipo Red Team aporta en gran medida a la seguridad de los sistemas de información de una compañía. Estos equipos tienen las herramientas necesarias para encontrar cualquier brecha que ponga en riesgo la seguridad de la información.

Como especialistas en seguridad de la información debemos estar actualizados tanto en herramientas tecnológicas como en metodologías que nos ayuden a ser eficientes en nuestra labor tanto en defensa como en procesos de pentesting.

Mantener todos los equipos, tanto finales como intermedios, actualizados y con sus respectivos parches de seguridad a sus sistemas operativos, es fundamental a la hora de proteger la información valiosa de las compañías.

Un sistema de analítica de la red en tiempo real previene la fuga de información, o exfiltraciones. Detectar puertos abiertos en equipos finales donde no deberían existir evita que los riesgos se materialicen como sucedió en este caso de fuga de información, que puede afectar tanto económica, como de forma reputacional la organización.

El Blue team es una parte muy importante a la hora de evitar y contener un ataque de seguridad informática. Desarrolla planes y ejecuta cambios y actualización de seguridad sobre los sistemas o hardware de seguridad.

El equipo de respuesta a incidentes está orientado a la coordinación de todos los elementos que intervienen a la hora de mitigar o minimizar el impacto en el momento de un incidente de seguridad.

Con el incremento de los delitos informáticos y el aumento de cibercriminales, debemos estar atentos tanto si pertenecemos a un Blue team o un Red team, y aportar con nuestro conocimiento adquirido a la mitigación tanto de un incidente de seguridad ya realizado como en la prevención, pensando siempre no hay tregua con los hackers que en cualquier momento puede verse expuesta la información que estamos resguardando.

11 BIBLIOGRAFIA

MINTIC. Ley 1273 5 Ene 2009. [En línea]. [30 de marzo 2021]. Disponible en https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

SECRETARIA SENADO. Ley estatutaria 1581 de 2012. [En línea]. [30 de marzo 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

SIC. Protección de Datos Personales. [En línea]. [30 de marzo 2021]. Disponible en: https://www.sic.gov.co/preguntas-frecuentes-pdp#:~:text=La%20Ley%201581%20de%202012%20proh%C3%ADbe%20la%20transferencia%20de%20datos,e%20inequ%C3%ADvoca%20para%20la%20transferencia.

METASPLOIT. Metasploit. [En línea]. [30 de marzo 2021]. Disponible en https://www.metasploit.com/

NMAP ORG. Introducción. [En línea]. [30 de marzo 2021]. Disponible en https://nmap.org/

OPENVAS. Openvas. [En línea]. [30 de marzo 2021]. Disponible en: https://www.openvas.org/

SECRETARIA SENADO. LEY 1273 DE 2009. [En línea]. [30 de marzo 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COPNIA. Código de Ética. [En línea]. [30 de marzo 2021]. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

YURI DIOGENES, ERDAL OZKAYA. Cybersecurity - Attack and Defense Strategies.

THE HACKER WAY. Conceptos Basicos de Meterpreter – MetaSploit Framework. [En línea]. [30 de marzo 2021]. Disponible en: https://thehackerway.com/2011/04/26/conceptos-basicos-de-meterpreter-metasploit-framework/#:~:text=COMANDOS%20DE%20METERPRETER%20EN%20SISTEMAS%20WINDOWS

OFFENSIVE-SECURITY. Meterpreter basic commands. [En línea]. [30 de marzo 2021]. Disponible en: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

Rejetto. [En línea]. [30 de marzo 2021]. Disponible en https://www.rejetto.com/hfs/

CIS. [En línea]. [30 de marzo 2021]. Disponible en https://www.cisecurity.org/