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

LUIS JAIR MENDEZ GUEVARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VILLAVICENCIO
2020

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

LUIS JAIR MÉNDEZ GUEVARA

Proyecto de Grado para optar por el título de
Especialista en Seguridad Informática

Director

JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VILLAVICENCIO
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Villavicencio, Octubre de 2020

Dedicatoria

A Dios, mis padres y mi hermano.

AGRADECIMIENTOS

A mi familia gracias por ayudarme cada día a cruzar con firmeza el camino de la superación, porque con su apoyo y aliento hoy he logrado uno de mis más grandes anhelos. Con amor y agradecimiento infinito.

TABLA DE CONTENIDO

LISTA DE FIGURAS

GLOSARIO

SEGURIDAD INFORMÁTICA: La seguridad informática puede entenderse como una característica de un sistema informático que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Según Thompson, en su publicación “Redes seguras”, de 2011, se puede definir a la seguridad informática como “la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.”[1]

SEGURIDAD DE LA INFORMACIÓN: La seguridad de la información, según ISO 27001, consiste en la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en el tratamiento de los datos dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• Confidencialidad: La confidencialidad, según José Vargas Hernández, nos dicen que los objetos de un sistema “han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades”.[2]

• Integridad: Significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada.

---

1 THOMPSON, Iván. Definición de administración. 2018. Recuperado en: https://www.promonegocios.net/administracion/definicion-administracion.html

2 VARGAS, José. Administración de redes y seguridad informática. Gestiópolis. 2002. Disponible en: https://www.gestiopolis.com/administracion-de-redes-y-seguridad-informatica/

• Disponibilidad: Indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio.

Es así como el portal iso27000.es, en su publicación digital Sistema de Gestión de la Seguridad de la Información (2005), señala que "para garantizar que la seguridad de la información es gestionada correctamente, debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI." [3]

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: Es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. ISO 27001 señala que dicho sistema "ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir."[4]

RED TEAM: Un Red Team se podría definir como una especie de test de intrusión (controlados y sin causar daño real a las infraestructuras TI) gracias al cual se pueden encontrar fallos en la estructura tecnológica de una organización. Pero, en realidad, el equipo rojo, va un poco más allá de vigilar la vulnerabilidad en materia de tecnología: los clientes, consensuando el alcance con el Red Team, pueden definir una serie de ataques a un objetivo y un equipo humano se encarga de realizar sus propios ataques bajo un contrato de alcance concreto y otro de confidencialidad."[5]

3 SGSI. ¿Qué es SGSI? 2009. Recuperado de: https://www.pmg-ssi.com/2015/07/que-es-sgsi/
4 FABRA, Alberto. ¿Cuál es la importancia de las políticas de una empresa? 2017. Recuperado en: https://negocios.uncomo.com/articulo/cual-es-la-importancia-de-las-politicas-de-una-empresa-26555.html
5 González, Oscar. ¿Qué es un redteam? 2019. Recuperado en: https://www.viewnext.com/que-es-un-red-team/

BLUE TEAM: Los Blue Team son equipos multidisciplinares de expertos en ciberseguridad especializados en analizar el comportamiento de los sistemas de una empresa y estudiar cómo se comportan sus usuarios y equipos para poner al descubierto de forma rápida cualquier incidente que pueda haber pasado inadvertido para el resto de sistemas de seguridad."[6]

PENTESTING: es un método para evaluar la seguridad de un sistema informático donde se simula un ataque que podría ocurrir en la vida real como lo son (phishing, Skimming, estafa cibernética, carta nigeriana, malware, smishing, etc.), para después de esta simulación identificar las posibles vulnerabilidades que tiene ese sistema y entregar una posible solución al dueño de dicho sistema.

METASPLOIT: Es una herramienta enfocada a explotar todas las vulnerabilidades encontradas dentro de un sistema informático que se está auditando o atacando, esta herramienta se puede usar tanto de manera legal por auditores en seguridad informática como lo son hackers de sombrero Blanco, y de manera ilegal como lo son los hackers de sobrero Negro.

NMAP: Es una herramienta que me sirve para escanear vulnerabilidades en las redes de los sistemas de información que se están auditando o atacando, al igual que la herramienta anterior se puede utilizar para fines legales como para fines delictivos. Y la esencia fundamental de ella es dejar expuesto los puertos que están abiertos en una red, los dispositivos que están conectados a la red y la estructura que posee dicha red.

6 ItDigitalSecurity. ¿Qué es un Blue Team y cómo trabaja? 2018. Recuperado en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

1. INTRODUCCIÓN

El cambio de modelos de negocio es cada vez más frecuente, dadas las nuevas tecnologías y el crecimiento constante de las compras online. María Cristina Cifuentes, analista estratega del sector inmobiliario y constructor del grupo Bancolombia, en su página web, asegura que “esto ha llevado a repensar la forma en que las tiendas y departamentos comerciales llegan a sus compradores, en especial en países desarrollados como Estados Unidos, donde cada vez son menos personas comprando en el interior de los centros comerciales, y más, comprando desde sus celulares y computadores.”[7]

Esta situación, según la misma fuente, unida al “sinnúmero de posibilidades de compras online, han venido creciendo y remplazando las compras en tiendas físicas, a tal punto que muchas de las cadenas, en especial las tiendas por departamentos, están revaluando su modelo de negocio”.[8] Es así como, “en 2016, el comercio minorista en Internet registró un crecimiento del orden del 13%, alcanzando los USD 312.1 mil millones, siendo el año con el mejor desempeño histórico en EE.UU.”[9]

Lo anterior, permite darnos una idea de la gran importancia de la implementación de un equipo de ciberseguridad en blueteam y redteam, para salvaguardar y proteger los activos informáticos más importantes de la compañía (entre los que se encuentran bases de datos, redes, equipos de cómputo, servidores, impresoras, portales web, etc.) y, que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

---

7 CIIFUENTES, María Cristina. La sostenibilidad de los centros comerciales en Colombia, ante la amenaza del comercio online. 2017. Disponible en: https://www.grupobancolombia.com/wps/portal/empresas/capital-inteligente/actualidad-economica-sectorial/sostenibilidad-de-centros-comerciales-colombia-ante-amenaza-del-comercio-online

8 CIFUENTES, óp. cit.

9 Ibíd.

En otras palabras, tener un equipo de seguridad blue team y red team es un trabajo fundamental para conservar confiables, los sistemas de la misma. La tarea entonces, “comprende la administración de riesgos, definición, creación e implementación de políticas de seguridad, procedimientos, estándares, guías, clasificación de información, organización de la estructura de seguridad de la compañía, y la capacitación de los individuos de la organización, entre otras.”[10]

10 ZUCCARDI y GUTIÉRREZ. Seguridad Informática. Pontificia Universidad Javeriana. 2006. Disponible en: http://pegasus.javeriana.edu.co/~edigital/Docs/Seguridad%20Informatica/Seguridad%20Informatica%20v1.0.pdf

2. OBJETIVOS

2.1. Objetivo General

Socializar los aspectos relevantes de las actividades que se desarrollaron durante el transcurso del seminario especializado “SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM” y plantear recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por RedTeam & BlueTeam.

2.2. Objetivos Específicos

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

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

3. DESARROLLO DEL INFORME

3.1 Leyes en ciberseguridad en Colombia.

La primera parte de esta informe trata sobre la actualidad legislativa en Colombia contra delitos informáticos que no es muy buena que digamos comparada con la de otros países, pero se pueden encontrar unas leyes importantes e interesantes:

Ley 527 del año 1999: esta ley es la primera ley promulgada en delitos informáticos en Colombia que parece más una normatividad que enmarca y promueve el buen uso de los datos, el comercio electrónico y las firmas digitales en Colombia.

Ley 1266 del año 2008: esta ley básicamente trata o contiene la normatividad sobre el habeas data y manejo de los datos personales de una persona por parte de una entidad privada o Pública o una persona natural.

Ley 1273 de 2009: esta ley modifica el código penal para ese año creando un nuevo bien jurídico llamado " la protección de la información y datos" y adiciona básicamente 8 artículos que van del 296A al 296J, y dice que se sanciona todos los delitos informáticos como (phishing, Skimming, estafa cibernética, carta nigeriana, malware, smishing,etc.) que afecten el bien jurídico expuesto anteriormente ya que está violando un derecho primordial de cualquier persona nacida en Colombia que es el derecho a la intimidad.

Elementos importantes de esta ley que se encuentran estipulados como delitos informáticos en Colombia y sus sanciones:

1) Artículo 269A, Acceso abusivo a cualquier sistema informático: el que sin autorización acceda o permanezca en cualquier sistema informático (celulares, equipos de cómputo, red de datos, servidores, etc.) con seguridad o no, se expone a una pena de 48 a 96 meses de prisión y una multa de 100 a 1000 salarios mínimos legales vigentes.

2) Articulo 269B, Obstaculización no autorizada de cualquier Sistema Informático: el que obstaculice el funcionamiento de cualquier sistema informático (celulares, equipos

de cómputo, red de datos, servidores, etc.) de manera ilegitima se expone a una pena de48 a 96 meses de prisión y una multa de 100 a 1000 salarios mínimos legales vigentes.

3) Articulo 269C, Interceptación de datos informáticos: el que acceda a información confidencial o sensible dentro de un sistema informático de cualquier persona natural o jurídica sin autorización se expone a una pena entre 32 a 72 meses de prisión.

4) Articulo 269D, Daño Informático: el que sin estar facultado o por omisión dañe, suprima, modifique datos informáticos o sistemas informáticos se expone a una pena de 48 a 96 meses de prisión y una multa de 100 a 1000 salarios mínimos legales vigentes.

5) Articulo 269E, Uso de Software Malicioso: personas que creen, distribuyan, usen o implanten software malicioso que tenga efectos dañinos en cualquier sistema informático se expone a una pena de 48 a 96 meses de prisión y una multa de 100 a 1000 salarios mínimos legales vigentes.

6) Articulo 269F, Violación de los datos personales: cualquier persona natural o jurídica que (obtenga, compile, sustraiga o los utilice para beneficio propio o de terceros) datos personales o sensibles para una persona sin estar facultado se expone a una pena de 48 a 96 meses de prisión y una multa de 100 a 1000 salarios mínimos legales vigentes.

7) Articulo 269G, Suplantación de los sitios web: cualquier persona natural o jurídica que cree, suplante y utilice un sitio web falso para capturar datos personales y sensibles de una persona ilegítimamente se expone a una pena de 48 a 96 meses de prisión y una multa de 100 a 1000 salarios mínimos legales vigentes.

3.2 Actuación Ética y Legal.

En esta segunda parte y teniendo en cuenta las leyes también, expongo como debe actuar de manera ética y legal un experto en ciberseguridad siguiendo al pie de la letra el “Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares” COPNIA, en los siguientes puntos más relevantes:

Artículo 31 “Deberes generales de los profesionales” en los numerales e, f, g, donde dice muy clarita mente que yo como ingeniero y profesional ético y moral, que soy debo permitir, informar, suministrar y colaborar con cualquier autoridad competente (policía, fiscalía, procuraduría, etc.), si lo requiere para adelantar sus investigaciones.

Artículo 32 “Prohibiciones generales a los profesionales” en el numeral c, j, que yo como ingeniero no debo aceptar de ningún tipo comisiones de dinero (sueldo, y contrato vitalicio) por hacer cosas ilícitas prestando mis servicios profesionales.

Artículo 34 “Prohibiciones especiales a los profesionales respecto de la sociedad” en él dice que no debo aceptar trabajos que vayan en contra de las disposiciones legales de la ley colombiana.

Artículo 35 “Deberes de los profesionales para con la dignidad de sus profesiones” numerales b, c, el cual dice que debo respetar y hacer respetar mi profesión cumpliendo a cabalidad todas las disposiciones legales y denunciar en caso de ser necesario.

Artículo 40 “Prohibiciones a los profesionales respecto de sus clientes y el público en general” en el numeral a, no debo prestar mis servicios profesionales a un cliente, si lo que voy hacer no cumple con todas las disposiciones legales que están implementadas en Colombia.

3.3 Ejecución pruebas de intrusión (RED TEAM)

La tercera etapa se llevó acabo de manera practica a través de un laboratorio controlado con la herramienta VirtualBox el cual constaba de 3 máquinas virtuales con las siguientes características:

1. **Windows 7 de 64 bits**

4 gigas de RAM

Disco duro de 50 gigabyte

Intel pro/1000 MT desktop (Nat)

Memoria de video de 18 megas

2. **Windows 7 de 32 bits**

4 gigas de RAM

Disco duro de 50 gigabyte

Intel pro/1000 MT desktop (Adaptador Puente, Remote NIDS compatible divice)

128 megas de video.

3. **Kali Linux de 64 bits**

2 gigas de RAM

Disco duro de 50 gigabyte

Intel pro/1000 MT desktop (NAT)

16 megas de video

Las primeras dos maquinas eran una copia exacta de dos máquinas que presentaron un problema de seguridad en junio de 2020 en una empresa llamada “Whitehouse Security” una empresa planteada en la situación problema del seminario, la tercera maquina fue nuestra herramienta para hacer las pruebas y los análisis necesarios a esta situación.

La practica se desarrollo en las siguientes etapas:

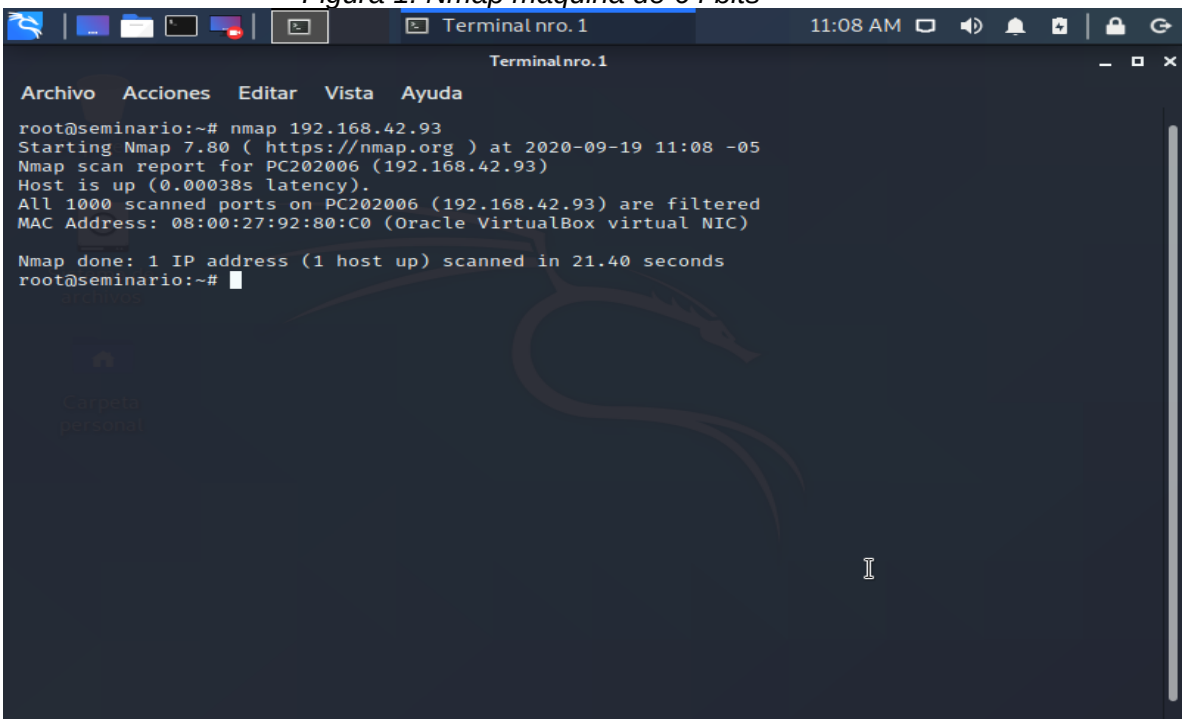
Fase de Reconocimiento:

Primero leí la información suministrada en el “Anexo 4 - Escenario 3 ” e identifique los datos más relevantes del caso, primero que las máquinas que estábamos sospechando trabajaban con un Windows 7 de 64 y 32 bits respectivamente, segundo que compartían información a través de un una conexión SMB para compartir el uso de impresoras y archivos en red, tercero no estaban actualizados sus sistemas Operativos para el día que ocurrió la perdida de la información que fue 10 de junio de 2020 y por el contrario tenían su última actualización el día 05 de febrero de 2017, y por ultimo y no menos importante la compañía WHITEHOUSE SECURITY en su informe decían que estaban preocupados de que la falla estuviera relacionada con el fallo CVE-2017-0144 ya que los equipos no contaban con la actualización MS17-010.

Fase de Escaneo:

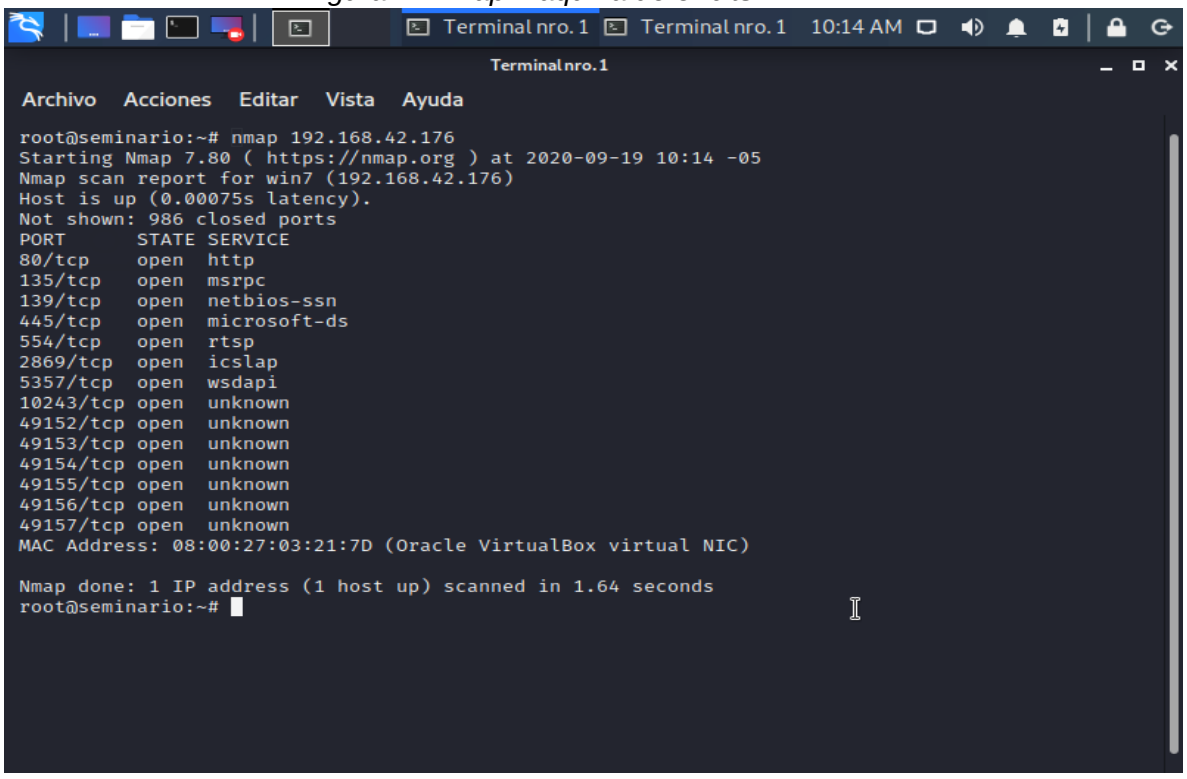
Segundo procedí a hacer un escaneo de vulnerabilidades a través de la herramienta nmap la cual es una herramienta que me sirve para escanear vulnerabilidades en las redes de los sistemas de información que se están auditando o atacando y su esencia fundamental es dejar expuesto los puertos que están abiertos de los dispositivos que están conectados a la red, se lo aplique a las dos máquinas para confirmar mis sospechas de la primera fase, y encontré que la maquina con nombre Win7-SE2020-X64 y S.O de 64bits tenía todos los puertos cerrados al hacer el escaneo, por ende no me arrojo ninguna vulnerabilidad(Observar Figura 1), en cuanto a la segunda maquina con nombre win7-SE2020 y S.O encontré 14 puertos abiertos (como se puede ver en la Figura 2 y 3) confirmando mi sospechas ya que entre esos puertos se encontraba el puerto 445 el cual es el puerto encargado del protocolo smb y el servicio Microsoft-ds que es el que permite el uso compartido de impresoras y datos en red.

Figura 1: Nmap maquina de 64 bits



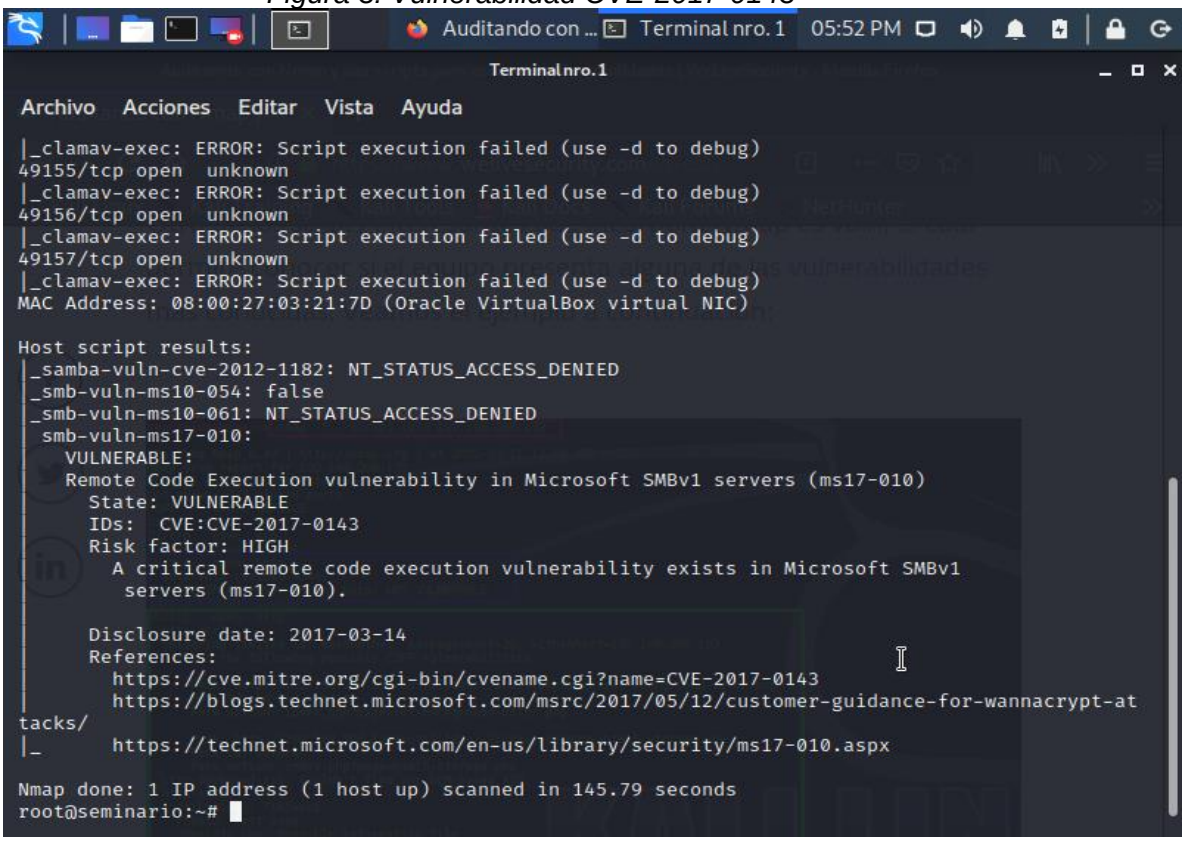
Fuente: Autor

Figura 2: Nmap maquina de 32bits



Fuente: Autor

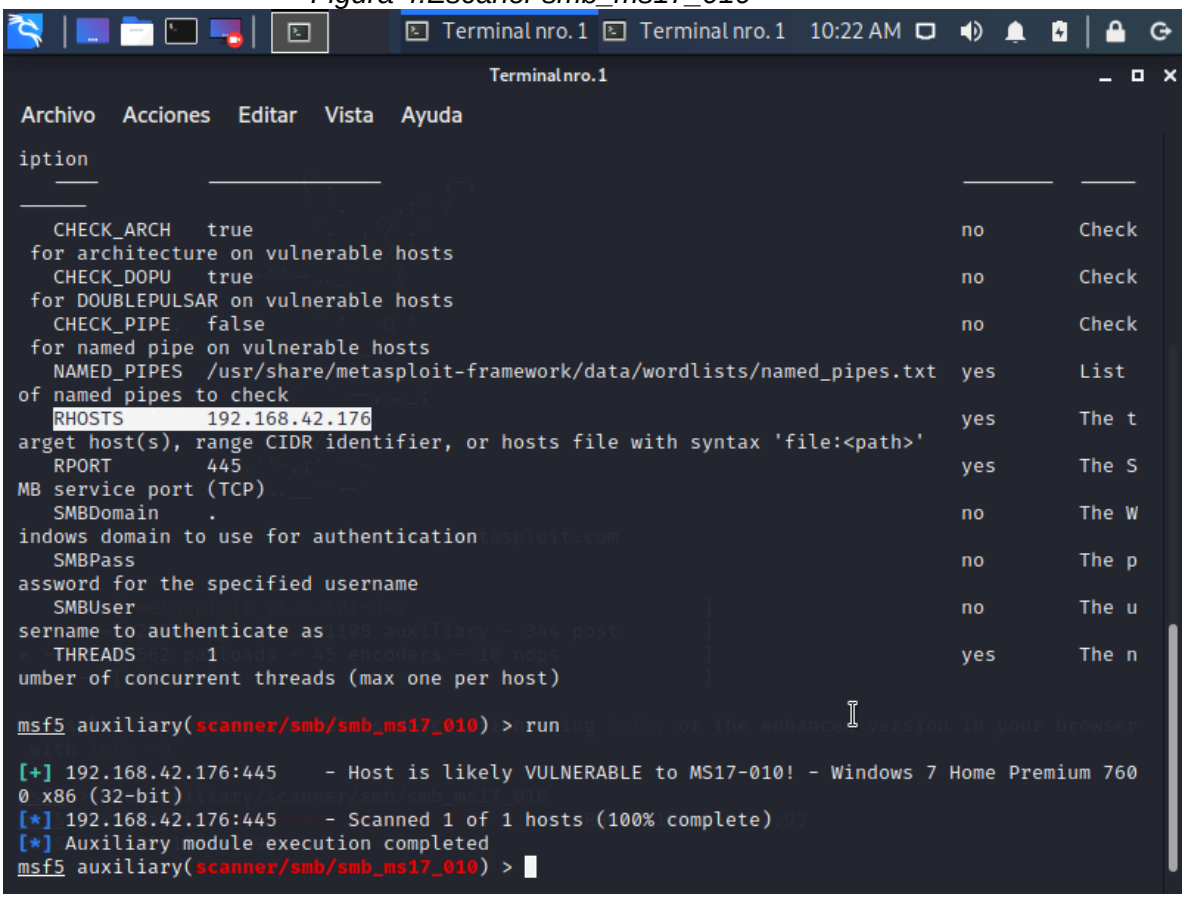
Figura 3: Vulnerabilidad CVE-2017-0143



Fuente: Autor

Seguido a esto decidí escanear la máquina que tenía el S.O de 32bits con un escáner específico que está dentro de la herramienta metasploit la cual es una herramienta enfocada a explotar todas las vulnerabilidades encontradas dentro de un sistema informático que se está auditando o atacando, pero dentro de sus funcionalidades también hay algunos escáneres de vulnerabilidades específicos como lo es smb_ms17_010 que dio como resultado al terminar el análisis que efectivamente la maquina era vulnerable(observar Figura 4).

Figura 4:Escáner smb_ms17_010

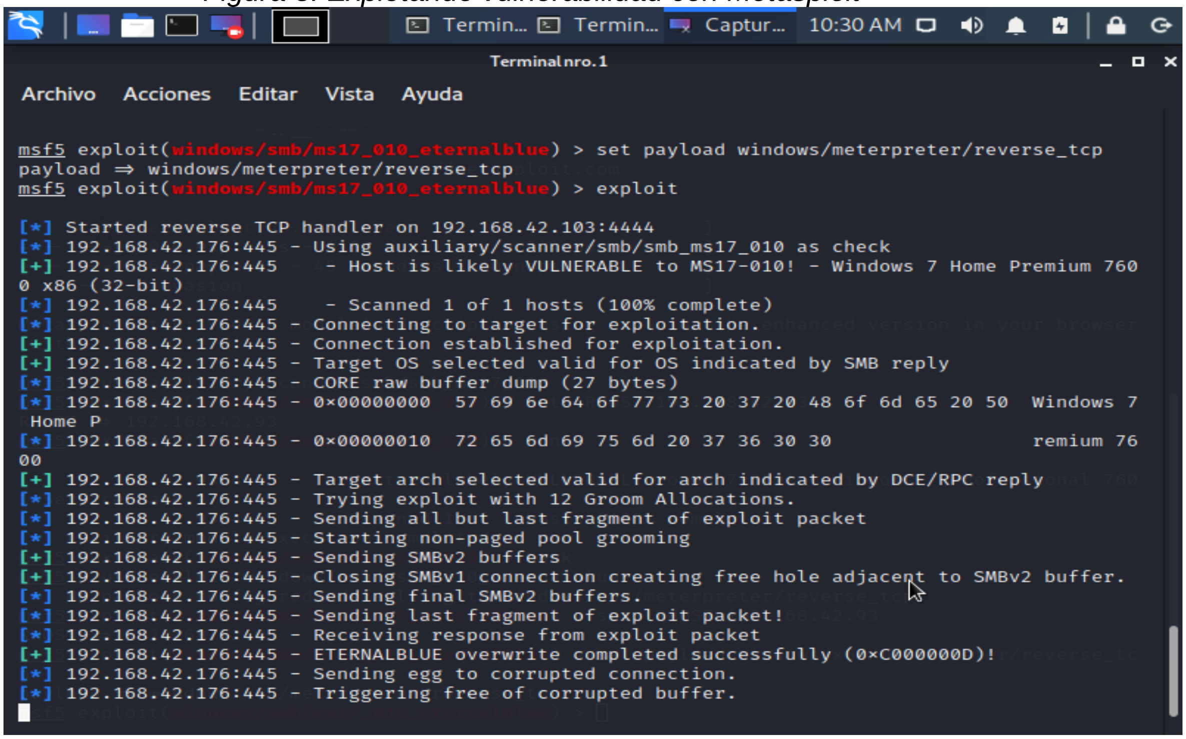


Fuente: Autor

Fase Obtener Acceso y Mantener Acceso

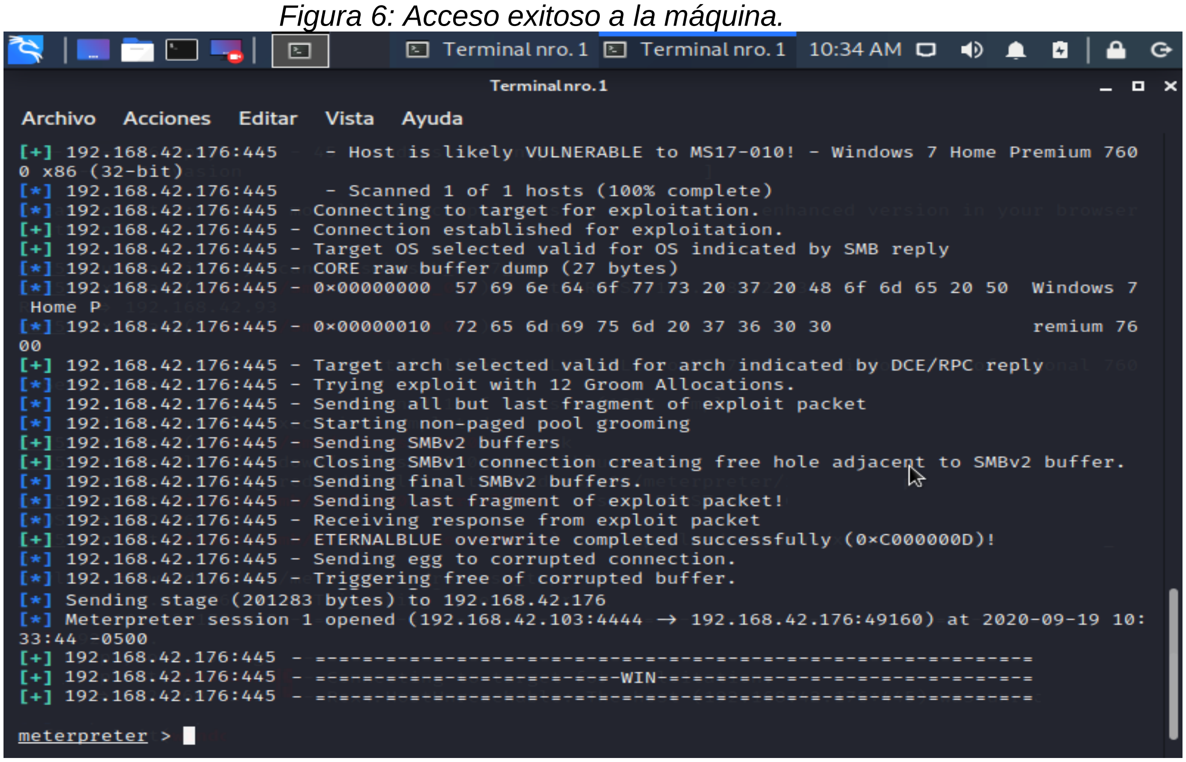
Tercero Procedí a explotar las vulnerabilidades encontradas en la fase de escaneo y lo hice con la herramienta metasploit, que como ya lo había dicho anteriormente esta herramienta está enfocada a explotar todas las vulnerabilidades encontradas dentro de un sistema informático que se está auditando o atacando, esta explotación se hizo mediante uno de sus exploit llamados “ms17_010_eternalblue” el cual permite específicamente obtener acceso a la maquina por medio del puerto 445 y el protocolo smb (observar figura 5,6 y 7).

Figura 5: Explotando vulnerabilidad con Metasploit



Fuente: Autor

Figura 6: Acceso exitoso a la máquina.



Fuente: Autor

Figura 7: Iniciando cmd en la maquina objetivo

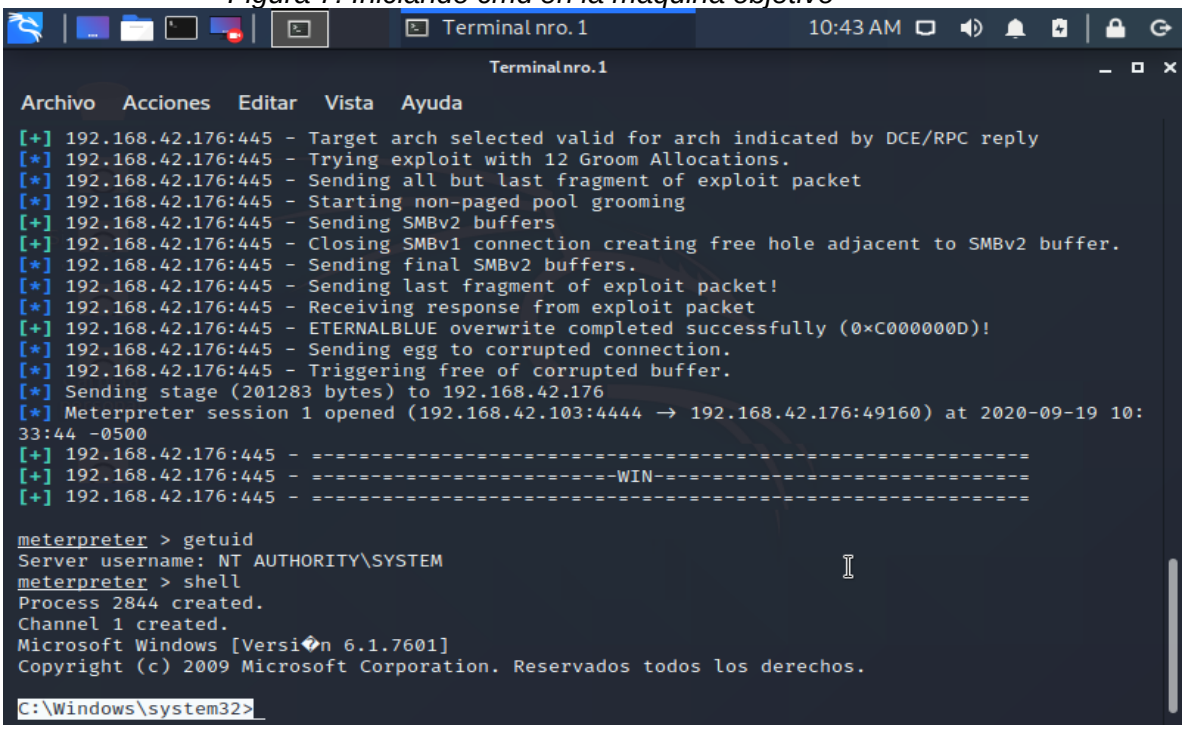
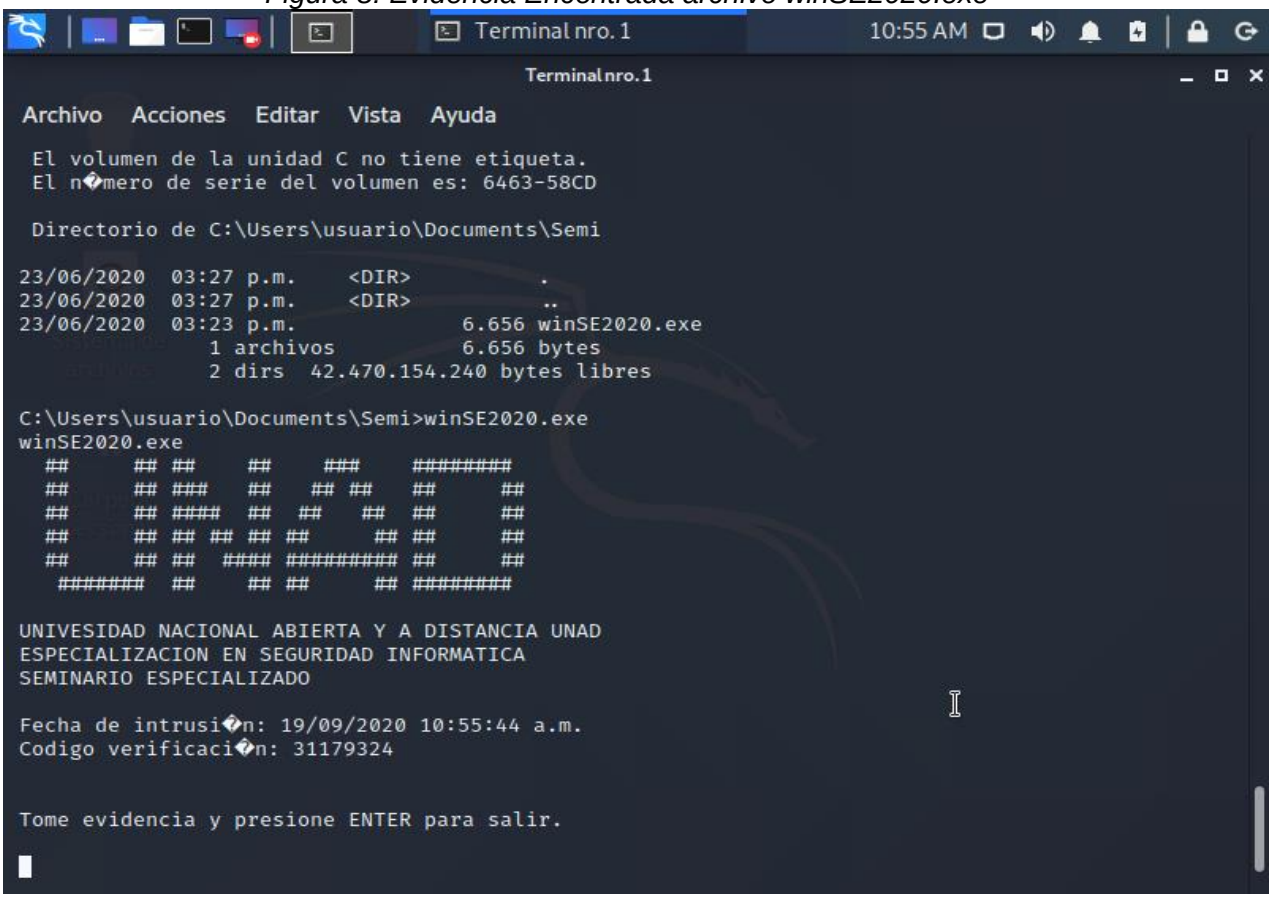

Terminal nro. 1
10:43 AM
Terminal nro. 1
Archivo Acciones Editar Vista Ayuda
[+] 192.168.42.176:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.42.176:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.42.176:445 - Sending all but last fragment of exploit packet
[*] 192.168.42.176:445 - Starting non-paged pool grooming
[+] 192.168.42.176:445 - Sending SMBv2 buffers
[+] 192.168.42.176:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.42.176:445 - Sending final SMBv2 buffers.
[*] 192.168.42.176:445 - Sending last fragment of exploit packet!
[*] 192.168.42.176:445 - Receiving response from exploit packet
[+] 192.168.42.176:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.42.176:445 - Sending egg to corrupted connection.
[*] 192.168.42.176:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.42.176
[*] Meterpreter session 1 opened (192.168.42.103:4444 → 192.168.42.176:49160) at 2020-09-19 10:33:44 -0500
[+] 192.168.42.176:445 - =-=-=-=

Figura 8: Evidencia Encontrada archivo winSE2020.exe



Fuente: Autor

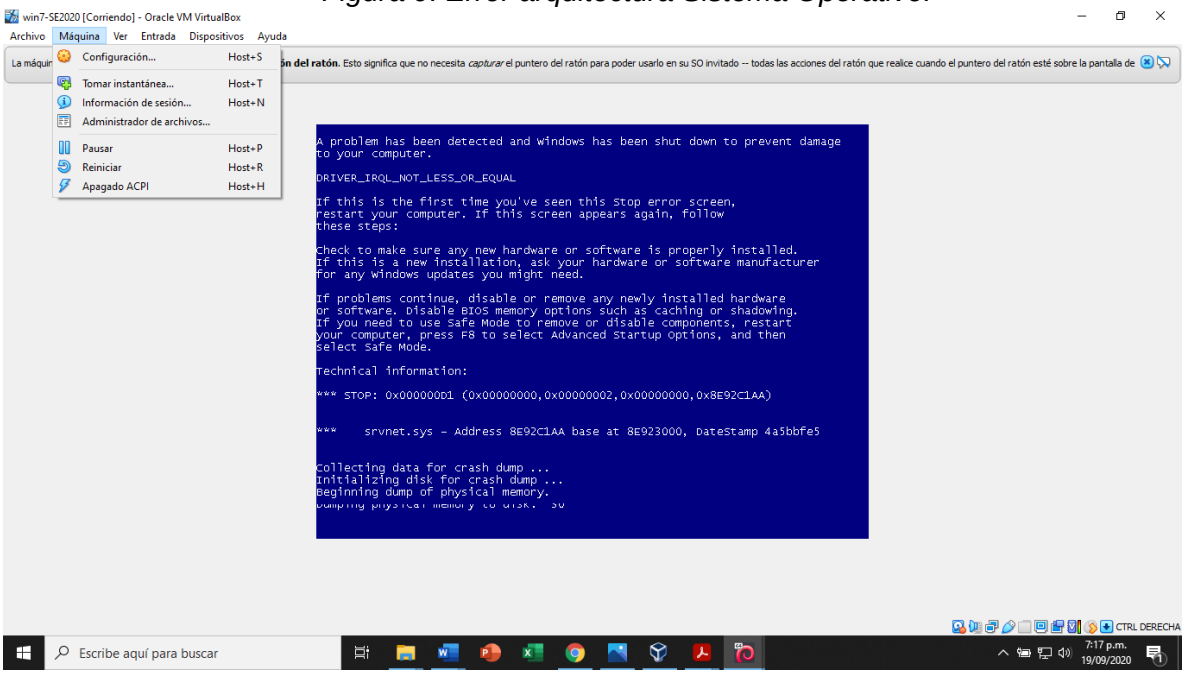
Fase de evidencias encontradas durante el ejercicio.

Bueno en la máquina de 64 bits de nombre “Win7-SE2020-X64”, tal cual con todas las configuraciones que tenía sin cambiarle alguna, se pudo observar que la maquina tenía todos sus puertos cerrados, es mas no recibía los pings que mandaban las demás máquinas, tenía el firewall activado el cual protegía a la máquina, sin embargo si a esa máquina le abren el puerto 445 se puede entrar en ella sin ser detectado ya que no cuenta con la actualización MS17-010 y en consecuencia se vuelve vulnerable al fallo “smb-vuln-ms17-010”.

En cuanto a otra maquina la de 32 bits y de nombre “win7-SE2020” si estaba totalmente desprotegida contra el fallo “smb-vuln-ms17-010” encontré que tenía 14 puertos abiertos, pero uno de ellos era totalmente vulnerable al fallo, el puerto 445 ya que esta máquina tampoco contaba con la actualización MS17-010, también puede constatar que la maquina se reiniciaba y mostraba pantallazos azules algunas veces cuando era atacada en la vulnerabilidad mencionada anteriormente debido a la arquitectura del sistema operativo(Observar Figura 9).

Por otra parte, el ataque que fue víctima el equipo consiste en entrar de manera abusiva sin ser detectado al equipo a través del puerto 445, el exploit lo que hace es insertar o instalar una blackdoor dentro el puerto aprovechando que este está abierto para compartir impresoras y datos, la intrusión permite de forma remota sacar o leer cualquier información que tenga el equipo.

Figura 9: Error arquitectura Sistema Operativo.



Fuente: Autor

3.4 Contención de Ataques Informáticos (BLUE TEAM).

Esta etapa es muy importante por que muchas veces nosotros como expertos en ciberseguridad en una compañía no sabemos como actuar en el momento de una crisis y que acciones tomar para protegerme de un determinado ataque, es por eso que en esta parte del informe se divide en dos “Acciones Necesarias Para Contener Un Ataque En Tiempo Real” y “Acciones De Hardenización A Implementar Para Evitar Que Sucedan Ataques De Seguridad Informática (de acuerdo a la situación planteada dentro del seminario)”.

Acciones Necesarias Para Contener Un Ataque En Tiempo Real:

Las acciones que se deben tomar son las siguientes:

1) Establecer prioridades basadas en la evaluación e impacto dentro de la organización.

Si estamos conteniendo un ataque informático, debemos evitar que se propague y detenerlo rápidamente para evitar mayores daños. Por cierto, la cantidad de servicios que presta el sistema informático inevitablemente debe reducirse, bloquearse o separarse, lo que tiene un gran impacto en el flujo de trabajo de cada empresa y sus departamentos. Aunque la decisión es muy difícil, debe tomarse de acuerdo al riesgo dentro de la organización. Por esta razón, es importante priorizar sus procesos de negocio para así minimizar el impacto dentro de la misma.

2) Establecer un personal idóneo y capacitado para el momento de la crisis.

En tiempos de crisis, el tiempo es dinero en los ciberataques. Por lo tanto, permitir que empleados sin experiencia o subordinados débiles trabajen juntos puede generar desacuerdos internos sobre quién tomará la iniciativa cuando pueda surgir un problema. expansión y deterioro de la situación. Para evitar este escenario, es importante tener un plan, fortalecer el liderazgo y realizar ensayos anuales.

3) Tomar acciones correctivas optimas

Las reparaciones rápidas y breves pueden resultar tentadoras. Sin embargo, debemos tener en cuenta que la tecnología adicional agrega complejidad y la complejidad es enemiga de la seguridad. Es muy importante evaluar toda la organización (procesos, políticas, servicios), así como las tecnologías necesarias para proteger la red y los datos.

4) Contratar un equipo de seguridad externo.

Los grupos internos a menudo creen que pueden hacer frente a todo tipo de ataques y crisis por sí mismos, pero a veces los esfuerzos por resolver el problema conducen a otros aún mayores. Por este motivo, es recomendable contratar un equipo de seguridad externo que proporcione una imagen más amplia y holística.

5) Resolver y darle un trámite correcto a los problemas que encontremos.

Como nunca se sabe dónde investigar, es importante seguir las mejores prácticas desde el principio. En tiempos de crisis, confíe en un equipo externo para proteger la integridad de la evidencia. Si esta investigación conduce a una acción legal, es muy importante haber hecho las cosas bien.

6) Enfocarnos en los resultados encontrados durante la investigación.

El primer impulso podría ser crear una lista de verificación basada en nuestra experiencia previa con el ataque. Sin embargo, no existen dos ciberataques similares. Usar esta lista de verificación no sería el método más eficaz. En su lugar, debemos reemplazar la lista de verificación mediante las etapas de Observar - Dirigir - Decidir - Actuar. Este método permite tomar decisiones más informadas, porque más información proviene de diferentes fuentes, porque los intrusos cambian y observan constantemente La idea es ser más rápido que nuestros oponentes.

7) Evaluar el proceso que se ejecutó con los resultados arrojados.

Una vez resueltos los ataques, se deben investigar sus causas y durante el proceso de recuperación, se debe evaluar qué funcionó y qué no funcionó. Este paso es muy importante porque la misma situación puede suceder más adelante si no realiza los cambios apropiados.

8) Denunciar el incidente

Se debe Denunciar del incidente ocurrido a la autoridad competente en Colombia, en este caso es la policía nacional de Colombia y la fiscalía general de la nación.

Acciones De Hardenización A Implementar Para Evitar Que Sucedan Ataques De Seguridad Informática (de acuerdo a la situación planteada dentro del seminario):

Bueno como el problema del ataque sucedió a nivel del sistema operativo o por una falla en los sistemas operativos yo decidí utilizar una hardenización para dichos sistemas:

1) Tener un control dentro de WhiteHouse Security sobre los equipos de cómputo quien los manipula y establecer roles y responsabilidades sobre cada máquina mediante un registro.

2) Actualizar el firmware (BIOS) no solo de las maquinas implicadas dentro del ataque a la empresa si no absolutamente todas.

3) Establecer usuarios y contraseñas seguras en cada máquina de la organización por que como observamos ninguno de los equipos de computo implicados durante el ataque tenían implementado esto y se podía acceder a ellos sin ninguna restricción.

4) Deshabilitar el inicio de sistema para cualquier dispositivo que no sea el disco principal y en el caso de los servidores deshabilitar las lecturas de los dispositivos ópticos como lo son memorias usb o similares.

5) Instalar los sistemas operativos de forma segura en todos los equipos de la organización especialmente en las maquinas implicadas ya que se pudo observar que estas máquinas ni si quiera contaban con dos particiones dentro su instalación, las cuales se usan una para el sistema en si y otra para la información importante de la misma, además de procurar instalar componentes y programas estrictamente necesarios.

6) Administrar de manera correcta todos los servicios de cada maquina dentro de la organización ya que una de las maquinas se encontró falta de administración en dichos servicios.

7) Actualizar todos los equipos de WhiteHouse Security con actualización MS17-010 para que no se nos vuelva a presentar el mismo ataque.

8) Probar periódicamente las actualizaciones que hay disponibles para el sistema operativo windows7, en un servidor controlado para mirar como funcionarían en producción y así mirar si vale la pena actualizarlas o no.

9) Intentar migrar la aplicación que es fundamental para la organización para que corra en un sistema más actual como Windows 10 y así poder tener mejores actualizaciones y más seguridad.

10) Instalar en todas las máquinas de la organización programas de seguridad como antivirus, programas antispyware además de configurar de manera adecuada el firewall de cada una de ellas.

11) Asignación correcta de derechos de usuario en cada maquina tratando de limitar al mínimo estos mismos, para de esta manera poder mitigar los riesgos.

12) Configurar las opciones de seguridad generales como el uso compartido de datos y recursos dentro de la red, además de configurar las opciones de seguridad en red.

13) Restricciones en la instalación de software en los equipos de cómputo de la compañía.

14) Activación de auditorías del sistema para poder tener un registro de los intentos de ataques que se van presentando dentro de la organización.

15) Configuración de los servicios del sistema en cada una de las maquinas teniendo en cuenta los servicios necesarios para cada una de ellas.

16) Configuración de todos los protocolos de red , se recomienda siempre utilizar sistemas de traducción de direcciones NAT para gestionar la red de la organización.

17) Deshabilitar todos los protocolos de red innecesarios en cada una de las máquinas.

18) Configurar todas las opciones de seguridad de los programas que tengan acceso a internet dentro de la organización.

19) Configurar también todos los accesos a carpetas y archivos de cada una de las maquinas ya que como lo pudimos evidenciar en el ataque no había ninguna restricción para acceder a cualquier carpeta o archivo de los equipos.

20) Cifrar los archivos, carpetas y unidades más importante para la organización considerando guardar las llaves de descifrado en un almacenamiento externo a la organización.

21) Y por último hacer un respaldo periódico de toda la información de la organización y administrarlos vía red.

4. CONCLUSIONES

Se Socializo los aspectos relevantes de las actividades que se desarrollaron durante el transcurso del seminario especializado “SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM” planteando recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por RedTeam & BlueTeam..

Se Demostró vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Se Formulo estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

5. CONCLUSIONES QUE PERMITEN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE ENFOQUE DE LA CIBERSEGURIDAD.

Como conclusiones finales en este seminario “Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team”:

Se mejoró la estrategia de ciberseguridad de una organización por todos los medios posibles.

Se demostró también que el uso de una combinación del equipo red team y equipo blue team puede crear mejoras radicales en la postura de seguridad de la organización, ya que la retroalimentación del equipo red team puede informar la estrategia defensiva del equipo blue team.

Se identifico que el aprendizaje en tiempo real y la mejora de procesos por parte del equipo blue team pueden permitir que la organización se someta a varias iteraciones de mejoras defensivas dentro de ella misma.

Se analizo que, si bien los equipos red team y los equipos blue team pueden beneficiar de forma independiente a una organización, el potencial de sinergia entre ellos puede mejorar drásticamente el impacto de una evaluación de seguridad.

6. RECOMENDACIONES.

Bueno como recomendación principal el equipo red team y blue team debe operar como un equipo purpure team que es simplemente adherirse a las mejores prácticas para crear un entorno que sea un baluarte contra los ataques cibernéticos. Como se mencionó anteriormente en las conclusiones, la comunicación entre equipos es el elemento más crítico en esto, pero aquí hay algunas otras recomendaciones de aprovechar al máximo los ejercicios de la red team y del blue team:

Tener un plan de acción.

Las etapas de planificación de los ejercicios de simulación son tan importantes como los propios ejercicios. Hay un sinfín de escenarios y metodologías para usar cuando se intenta explotar un sistema, por lo que es vital limitar su alcance. El equipo red team deben tener objetivos establecidos y metas medibles que proporcionarán datos útiles para que los analice el equipo blue team. Los equipos blue team deben usar estos datos para crear sus propios objetivos y metas para la remediación.

Siempre hacer un seguimiento.

Si bien es tentador simplemente pasar a la siguiente tarea, es fundamental hacer un seguimiento después de cada ejercicio. Las retrospectivas son una excelente manera para que los equipos aprendan unos de otros y pueden arrojar más información sobre la corrección y la prevención de debilidades. Además, las correcciones en sí también deben verificarse, por lo que el seguimiento de los esfuerzos de reevaluación es crucial.

Pensar como un atacante.

Los actores de amenazas no siguen un conjunto de reglas cuando ingresan a un sistema. Los miembros del red team pueden permanecer dentro del alcance del ejercicio y al mismo tiempo tener la libertad de ser igualmente creativos. Sin embargo, recordemos pensar y actuar como un atacante ya que los equipos azules solo pueden prevenir un ataque si pueden comprender cómo se hizo.

Nunca dejar de aprender.

Promover una cultura de aprendizaje y anime en los equipos red team y blue team manteniéndonos actualizados con las últimas herramientas y trucos para evitar ser tomados por sorpresa. Los hackers siempre están evolucionando, y los verdaderos equipos purpure team evolucionan junto con ellos.

7. BIBLIOGRAFÍA

Aguilera, P. (2011). Redes seguras (Seguridad informática). Madrid, España: Editex.

AERTIC. (2018). Estudio sobre seguridad informática para conocer el estado actual de las empresas y programar nuevas actuaciones. Disponible en: http://www.aertic.es/2014/11/estudio-sobre-seguridad-informatica-para-conocer-el-estado-actual-de-las-empresas-y-programar-nuevas-actuaciones/.

CIIFUENTES, María Cristina. (2017). La sostenibilidad de los centros comerciales en Colombia, ante la amenaza del comercio online. Disponible en: https://www.grupobancolombia.com/wps/portal/empresas/capital-inteligente/actualidad-economica-sectorial/sostenibilidad-de-centros-comerciales-colombia-ante-amenaza-del-comercio-online

FABRA, Alberto. (2017) ¿Cuál es la importancia de las políticas de una empresa? Recuperado en: https://negocios.uncomo.com/articulo/cual-es-la-importancia-de-las-politicas-de-una-empresa-26555.html

CORPORACIÓN COLOMBIA DIGITAL. (2018) ¿Cómo está Latinoamérica en temas de seguridad informática? Disponible en: http://colombiadigital.net/actualidad/noticias/item/8250-como-esta-latinoamerica-en-temas-de-seguridad-informatica.html.

DEFINICIÓN.DE. (Sin fecha de publicación). Antivirus. Recuperado de: https://definicion.de/antivirus/

DEFINICIÓNABC.COM. (Sin fecha de publicación). Sistemas operativos. Recuperado de: https://www.definicionabc.com/general/sistema.php

DE BENITO. (2014). Del total de empresas las colombianas, 98% son víctimas de ataques informáticos. Diario La República. Disponible en: http://www.larepublica.co/alta-gerencia/del-total-de-empresas-las-colombianas-98-son-v%C3%ADctimas-de-ataques-inform%C3%A1ticos_121871.

GAUDÍ. (Sin fecha de publicación). Seguridad Informática Situación Actual y buenas prácticas. Articulo49.pdf. Disponible en: http://www.asersa.com/asersa/Articulos/Articulo49.pdf.

INTERNET YA. (2018). Tendencias en seguridad informática para el 2018. Disponible en:
http://www.internetya.co/tendencias-en-seguridad-informatica-para-el-2018/

REVISTA DIGITAL “IONOS”. (2016). ¿En qué consiste una zona de seguridad desmilitarizada DMZ? Recuperado en:
https://www.ionos.es/digitalguide/servidores/seguridad/en-que-consiste-una-zona-desmilitarizada-dmz/

JULIÁ. (Sin fecha de publicación). Tendencias: las amenazas más comunes a la seguridad informática. GADAENETWEB. Disponible en:
http://www.gadae.com/blog/amenazas-seguridad-informatica/.

MATALOBOS, Juan Manuel. (2009). Análisis De Riesgos De Seguridad De La Información. Universidad Politécnica de Madrid. Disponible en:
oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf.

MINISTERIO TIC. (Sin fecha de publicación). Sistemas de Gestión de la Seguridad de la Información (SGSI). Disponible en: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html.

PACHECO, Federico. (2010) La importancia de un SGI. Tomado de:
https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

RODRÍGUEZ, Giselle. (2009) Ventajas competitivas a través de la gestión de recursos humanos. Gestiópolis. Recuperado en: https://www.gestiopolis.com/ventaja-competitiva-a-traves-de-la-gestion-de-recursos-humanos/

PRITESHGUPTA.COM. (Sin fecha de publicación). El portal de ISO 27001 en español. Disponible en: http://www.iso27000.es/sgsi.html.

SALCEDO. R. J. (2014). Plan De Implementación Del Sgsi Basado En La Norma Iso 27001:2013. Universidad Oberta Catalunya. Disponible en:
openaccess.uoc.edu/webapps/o2/.../4/rsalcedobTFC1214memoria.pdf

SGSI. ¿Qué es SGSI? (2009). Recuperado de: https://www.pmg-ssi.com/2015/07/que-es-sgsi/

THOMPSON, Iván. (2018) Definición de administración. Recuperado en:
https://www.promonegocios.net/administracion/definicion-administracion.html

TRASOBARES, Alejandro. (2006). Los sistemas de información: evolución y desarrollo. DIALNET. Unirioja, España.
Disponible en: https://dialnet.unirioja.es/descarga/articulo/793097.pdf

VARGAS, José. (2002). Administración de redes y seguridad informática. Gestiópolis. Disponible en: https://www.gestiopolis.com/administracion-de-redes-y-seguridad-informatica/

ZUCCARDI y GUTIÉRREZ. (2006). Seguridad Informática. Pontificia Universidad Javeriana. Disponible en: http://pegasus.javeriana.edu.co/~edigital/Docs/Seguridad%20Informatica/Seguridad%20Informatica%20v1.0.pdf

A. Reyes Plata. (2014) Ethical Hacking. Recuperado en: http://www.seguridad.unam.mx/descarga.dsc?arch=2776.

CARMONA. (2004). Seguridad en el sistema operativo GNU/LINEX. Disponible en: gitaca.unex.es/agila/archivos/seguridad_linex.pdf

CSERVICES. (Sin fecha de publicación). «Servicios_ Ethical Hacking,» csservices.com.ar. Disponible en: http://www.cservices.com.ar/servicios/etHacking_1.htm.

Enter.co. (2015). El Hacking Ético y su importancia para las empresas. Disponible en: http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

Menendez Méndez (2009). Ethical Hacking: Test de intrusión principales metodologías. Monografías.com. Disponible en: www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias2.shtml.

Prezi. (2018). evaluación de variables criticas de seguridad en sistemas operativos. Disponible en: https://prezi.com/napchlmgbk8e/evaluacion-de-variables-

Seguridadx. (2014). ¿Qué es Ethical Hacking? Disponible en: http://www.seguridadx.com/que-es-ethical-hacking/

UDEM. (2018). Ethical Hacking. Recuperado de: cdigital.udem.edu.co/TESIS/CD-ROM28692008/13.Capitulo7.pdf

Muehlberghuber, M., Gürkaynak, F. K., Korak, T., Dunst, P., & Hutter, M. (2013). Red team vs. blue team hardware Trojan analysis: detection of a hardware Trojan on an actual ASIC. In Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy (pp. 1-8).

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. In 2011 IEEE 29th international conference on computer design (ICCD) (pp. 285-288). IEEE.

Mejia, R. (2016). Red team versus blue team: how to run an effective simulation. CSO Online-Security and Risk.

Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity??? Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing Ltd.

Mirkovic, J., Reiher, P., Papadopoulos, C., Hussain, A., Shepard, M., Berg, M., & Jung, R. (2008). Testing a collaborative DDoS defense in a red team/blue team exercise. IEEE Transactions on Computers, 57(8), 1098-1112.

Zhang, X., Xiao, K., Tehranipoor, M., Rajendran, J., & Karri, R. (2013). A study on the effectiveness of Trojan detection techniques using a red team blue team approach. In 2013 IEEE 31st VLSI Test Symposium (VTS) (pp. 1-3). IEEE.

Waksman, A., Rajendran, J., Suozzo, M., & Sethumadhavan, S. (2014). A red team/blue team assessment of functional analysis methods for malicious circuit identification. In 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC) (pp. 1-4). IEEE.

Fontenot, G. (2005). Seeing Red: creating a red-team capability for the blue force. Military Review, 85(5), 4.

Holm, H. (2012). Baltic cyber shield: research from a red team versus blue team exercise. PenTest magazine, 9, 80-86.

Grayman, W. M., Ostfeld, A., & Salomons, E. (2005). Red team-blue team exercise for locating monitors in distribution systems. In Impacts of Global Climate Change (pp. 1-11).

Bresch, C., Michelet, A., Amato, L., Meyer, T., & Hely, D. (2017). A red team blue team approach towards a secure processor design with hardware shadow stack. In 2017 IEEE 2nd International Verification and Security Workshop (IVSW) (pp. 57-62). IEEE.