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

PIERRE MICHAEL NIÑO FORERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
CURSO: SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ
2020

RESUMEN

El presente informe técnico detalla las actividades realizadas acuerdo los requerimientos realizados por la empresa WHITEHOUSE SECURITY, dónde se emplearon diferentes herramientas tecnológicas de código abierto para lograr identificar las vulnerabilidades de las máquinas suministradas y que fueron objeto de robo de información.

Así mismo, describe las diferentes fases para recrear la intrusión a las máquinas suministradas con el fin de conocer como pudo ser el ataque y la forma de contenerlo.

Finalmente, mostraremos como se puede contener este tipo de ataque, así como las medidas de hardenización para evitar o minimizar futuros ataques que pudieran venir de la red externa y las respectivas recomendaciones para prevenir ataques internos.

CONTENIDO

Pág.
GLOSARIO 5
INTRODUCCIÓN 10
1. OBJETIVOS 11
1.1 OBJETIVO GENERAL 11
1.2 OBJETIVOS ESPECÍFICOS 11
2. HERRAMIENTAS UTILIZADAS PARA RECREAR LA INTRUSIÓN 12
2.1 FASE DE RECOLECCIÓN 12
2.2 FASE DE EXPLOTACIÓN 15
3. MEDIDAS PARA CONTENER EL ATAQUE 18
4. MEDIDAS DE HARDENIZACIÓN 21
5. LINK VIDEO SUSTENTACIÓN 24
6. CONCLUSIONES 24
7. RECOMENDACIONES 25
BIBLIOGRAFÍA 26

TABLA DE FIGURAS

Pág.

Figura No. 1 Resultado uso herramienta nmap 192.168.100.237……13
Figura No. 2 resultados escaneo nessus……14
Figura No. 3 vulnerabilidad y forma de explotarla……15
Figura No. 4 resultados escaneo nmap específico……16
Figura No. 5 inicio del ataque……16
Figura No. 6 éxito de la conexión, llegada al meterpreter……17
Figura No. 7 raíz del sistema de la máquina win7 x64……17
Figura No. 8 ubicación archivo winse20w0.exe……18
Figura No. 9 ejercicio exitoso culminado……18
Figura No. 10 Consultar conexiones activas……19
Figura No. 11 Consultar detalle conexión PID 1260……20
Figura No. 12 Evidencia de sesión cerrada desde CMD máquina win7 x64
En la máquina de win7 x86……20
Figura No. 13 Evidencia dónde no se observan conexiones activas en la máquina win7 x86 ……21
Figura No. 14 Desactivar Permitir conexiones de asistencia remota en este equipo……23
Figura No. 15 Activar, actualizar y posterior instalación de parches de seguridad con Windows update……23
Figura No. 16 Activar, actualizar Windows Defender……24
Figura No. 17 Evidencia máquina atacante ya no inicia sesión en la máquina víctima después de la hardenización……24

GLOSARIO

ACK: es un mensaje que el destino de la comunicación envía al origen de ésta para confirmar la recepción de un mensaje.
ARP: acrónimo de Protocolo de Resolución de Direcciones (del inglés, Address Resolution Protocolo).
Ataque: acción realizada por una tercera parte, distinta del emisor y del receptor de la información protegida, para intentar contrarrestar esta protección.
Autoridad de certificación (CA*): entidad que emite certificados de clave pública que sirven para que los usuarios que confíen en esta autoridad se convenzan de la autenticidad de les claves públicas.
Autoridad de certificación (CA*) raíz: CA que no tiene ninguna otra superior que certifique la autenticidad de su clave pública y que por tanto tiene un certificado firmado por ella misma.
base64-code: es un sistema de numeración posicional que usa 64 como base Bluetooth: es una tecnología para comunicaciones de corto alcance.
Beacons: paquetes “anuncio” sin encriptar. No sirven para la recuperación de claves WEP. **BSSID**: el BSSID (Basic Service Set Identifier) de una red de área local inalámbrica es un nombre de identificación único de todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.
Bugtraq: es una lista de correo electrónico para publicación de vulnerabilidades de software y hardware.
Bug: hace referencia a cualquier fallo en una determinada aplicación.
Captcha: es un acrónimo en inglés para Completely Automated Public Turing test to tell Computers and Humans Apart, que en español se puede traducir como "Prueba de Turing pública y automática para diferenciar máquinas y humanos.
Cifrado: transformación de un texto en claro, mediante un algoritmo que tiene como parámetro una clave, en un texto cifrado no legible para quien no conozca la clave de descifrado.
Clausula: estructura de comandos.
Confidencialidad: protección de la información contra lectura por parte de terceros no autorizados.
Contraseña: palabra “password” o cadena de caracteres secreta, de longitud relativamente corta, usada por una entidad para autenticarse.
Cookie: fichero con información relativa a la combinación computador-navegador-usuario que se almacena de forma local.

Cortafuegos: elemento de prevención que realizará un control de acceso con el objetivo de separar nuestra red de los equipos del exterior (potencialmente hostiles). En inglés, firewall.

Cracker: término designado a programadores que alteran el contenido de un determinado programa, por ejemplo, alterando fechas de expiración de un determinado programa para hacerlo funcionar como si se tratara de una copia legítima.

Descifrado/ Desencriptar: transformación inversa al cifrado para obtener el texto en claro a partir del texto cifrado y la clave de descifrado.

Diffie: El protocolo criptográfico Diffie-Hellman, debido a Whitfield Diffie y Martin Hellman, (Diffie– Hellman Problem->DHP) es un protocolo de establecimiento de claves entre partes que no han tenido.

Dirección MAC: es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de una forma única a una tarjeta o dispositivo de red.

DNS: sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o una red privada, del inglés Domain Name System.

Dumping: extraer una determinada información de alguna tabla de la base de datos.

Exploit: (del inglés to exploit, 'explotar' o 'aprovechar') es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Flag: es una marca que se utiliza en las codificaciones de programas.

Framework: Conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular, que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar.

FTP: el servicio FTP (File Transfer Protocol, Protocolo de Transferencia de Ficheros), es uno de los más antiguos dentro de Internet.

Hacker: gente apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats".

Handler: en Metasploit, un handler es lo que utilizamos para conectar con un destino. Dependiendo del payload, el handler quedará a la escucha esperando una conexión por parte del payload (reverse payload) o iniciará una conexión contra un host en un puerto especificado (caso de un bind payload).

Hardenización: Acciones a nivel de hardware o software para fortalecer las medidas de seguridad de equipos o sistemas informáticos.

Host: se refiere a cada una de las computadoras conectadas a una red que proveen o utilizan servicios de ella.
HTTP: es el protocolo utilizado en cada transacción de la World Wide Web, del inglés Hyper Text Transfer Protocol.
HTML: (del inglés Hyper Text Markup Language, lenguaje de marcas de hipertexto) es el lenguaje de programación en el que se escriben las páginas Web.
ICMP: es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP), del inglés Internet Control Message Protocol).
ID: es un código de identificación.
IDS: es un sistema para detectar ataques de intrusos en sistemas informáticos.
IEEEl 802.11: es una codificación de una norma para uso de funcionamiento de una red. Define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos).
Intranet: red de ordenadores privados que utiliza la tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.
IP: se trata de un protocolo no orientado a conexión, usado por el origen y el destino para comunicación de datos a través de una red de paquetes conmutados, del inglés Internet Protocol. Intrusiones: son penetraciones que se hacen en los sistemas sin permisos o derechos.
Interface: dispositivo físico que se emplea normalmente para realizar conexiones, como tarjetas de red por ejemplo.
ISP: Internet Services Provider son servicios proveedores de Internet.
Kernel: se refiere al núcleo de un sistema operativo.
Linux: núcleo libre de sistema operativo basado en Unix.
Log: registro de eventos que se producen durante un rango de tiempo en particular.
Malware: es un tipo de software que tiene como objetivo infiltrase o dañar una computadora sin el consentimiento del propietario.
Memoria RAM: memoria utilizada como memoria de trabajo para el software instalado en un ordenador, del inglés Random-Access Memory.
Mysql: es un sistema de gestión de bases de datos relacional, multihilo y multiusuario.
Parche: cambios que se aplican a un problema para solucionar errores o actualizaciones.
Padding: es una propiedad que crea un espacio por dentro de la caja a la que se aplica, impidiendo, por así decirlo, que se toque su borde.
Payload: se refiere a los efectos destructivos, nocivos o molestos que cualquier virus puede producir cuando ya ha tenido lugar su infección, además de los efectos

secundarios de dicha infección (cambios en la configuración del sistema, reenvío de e-mail, ejecución del virus en el arranque del sistema o de Windows, etc).
Php: (acrónimo recursivo de PHP: Hypertext Preprocessor) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo Web y que puede ser incrustado en HTML.
PID: es una abreviatura de process ID.
Police: se refiere a reglas pre definidas para una determinada aplicación.
Plugins: programa que puede anexarse a otro para aumentar sus funcionalidades (generalmente sin afectar otras funciones ni afectar la aplicación principal). No se trata de un parche ni de una actualización, es un módulo aparte que se incluye opcionalmente en una aplicación.
Proxy: es un programa o dispositivo que realiza una acción en representación de otro. Trama: unidad de envío de datos.
Render: es el proceso de generar un proceso a partir de un modelo, usando una aplicación.
Router: dispositivo usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar.
Root: nombre dado a una cuenta con privilegios de administrador. Script: archivo de órdenes o archivo de procesamiento por lotes, es un programa usualmente simple que por lo regular se almacena en un archivo de texto plano.
Sniffer: es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.
Sql: el lenguaje de consulta estructurado o SQL (por sus siglas en inglés Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas.
SSH1: aplicación y protocolo propio para la transmisión segura de los datos. SSH2: aplicación y protocolo propio para la transmisión segura de los datos, es la versión más actual y trabaja con un modo de cifrado más seguro.
SSL: son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.
SYN: es un tipo de Flag muy usado en el protocolo TCP/IP.
TCP: Protocolo de Control de Transmisión, del inglés Transmisión Control Protocol.
Troyano: en una aplicación que se infiltra en otra para tener accesos no autorizados.
UDP: protocolo del nivel de transporte basado en el intercambio de datagramas, del inglés User Datagram Protocol.
Unix: sistema operativo portable, multitarea y multiusuario.

Url: es una forma de organizar la información en la Web, son las direcciones Web.
Virus: tipo de malware que tiene como objetivo el alterar el normal funcionamiento de una computadora.
VPN: red privada virtual, del inglés Virtual Private Network. Verbose: definir una aplicación que se ejecute con respuesta detallada de las informaciones.
Wi-fi: mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.
Zona desmilitarizada (DMZ): dentro de una red protegida por un cortafuego, zona separada de los servidores públicos por un segundo cortafuegos[1].

[1] Cristiano Días. Hacking ético y seguridad en Red. 2014. Tomado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/34501/7/cdiasTFC0614memoria.pdf

INTRODUCCIÓN

Las actividades detalladas en este informe técnico hacen parte de las estrategias planteadas en los equipos Red Team & Blue Team, acuerdo los requerimientos realizados por la empresa WHITEHOUSE SECURITY quien manifestó haber sido víctima de una intrusión en algunos equipos de computo de su empresa, por lo que nosotros planteamos las estrategias correspondientes para lograr identificar los equipos, la forma y consecuencia de la intrusión por parte de un atacante desconocido.

Teniendo en cuenta las consideraciones y condiciones de la empresa, referentes al tema presupuestal se emplearon herramientas informáticas de código abierto que permiten un alto grado de credibilidad el los procesos de detección de la intrusión y de la misma forma controlar o contener la amenaza.

Finalmente, se pretende entregar las recomendaciones y conclusiones respectivas con el ánimo de mejorar los sistemas de protección de los equipos y en general de la red de la empresa.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Aplicar las estrategias contempladas en los equipos Red Team & Blue Team para realizar la identificación de la intrusión y la contención en la empresa WHITEHOUSE SECURITY empleando herramientas de código abierto.

1.2 OBJETIVOS ESPECÍFICOS

Llevar a cabo la recreación del ataque que pudieron recibir las máquinas que suministró la empresa, mediante la utilización de herramientas informáticas especializadas en intrusión y explotación de vulnerabilidades.

Realizar la contención de la máquina atacante mediante herramientas o configuraciones en las máquinas suministradas win7 x64 x86.

Realizar las respectivas conclusiones y recomendaciones con el fin de fortalecer los equipos empleados para las operaciones de la empresa.

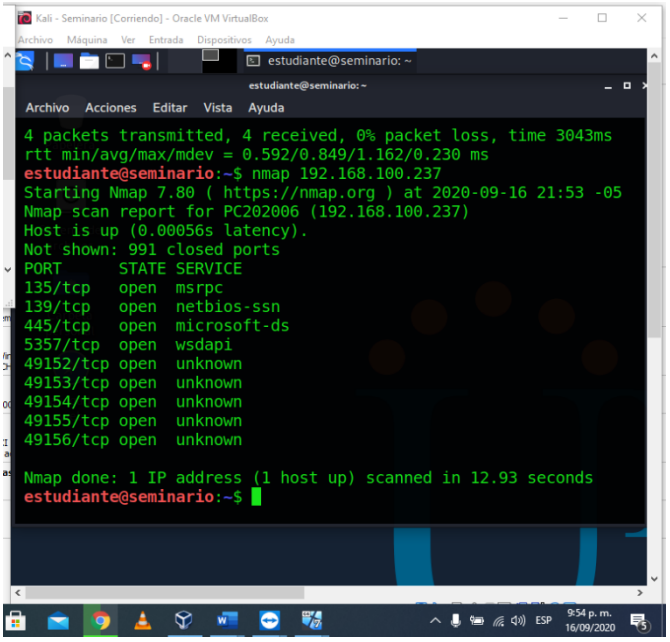
2. HERRAMIENTAS UTILIZADAS PARA RECREAR LA INTRUSIÓN

En esta fase se utilizaron las herramientas nmap, Nessus y metaspliot de la siguiente manera:

2.1 FASE DE RECOLECCIÓN

Se Inició la recolección de la información útil de la máquina win7 x64 haciendo uso de la herramienta nmap, mediante el comando: nmap y la ip de la máquina asignada así, nmap 192.168.100.237, como se aprecia en la figura No. 1.

Figura No. 1 Resultado uso herramienta nmap 192.168.100.237

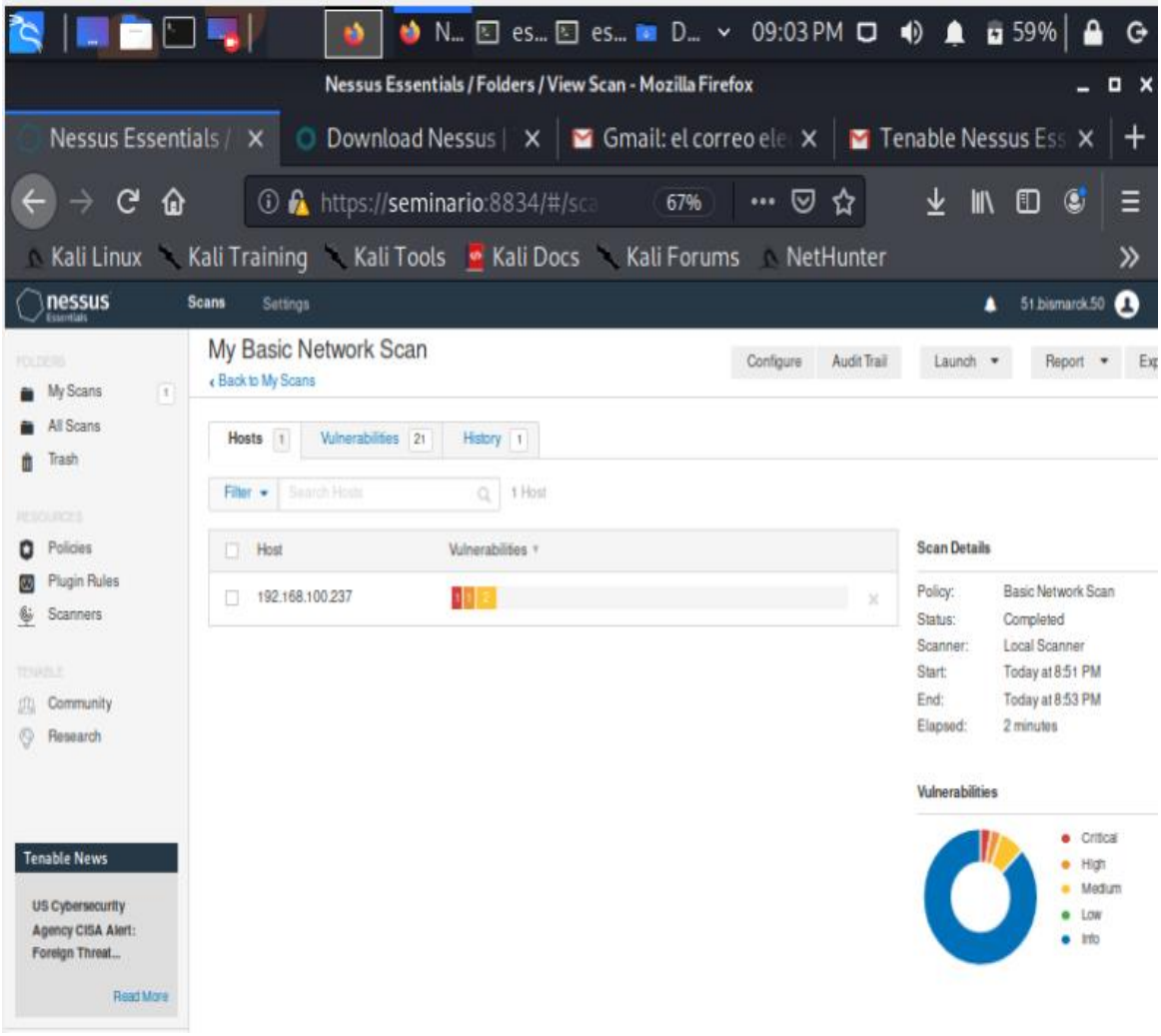


Fuente: Pierre Niño.

Del procedimiento anterior se puede observar que el puerto 445 para las conexiones TCP se encuentra abierto y adicional lo emplea el sistema operativo para conexiones remotas.

Para ampliar la información, se empleó la herramienta nessus, los resultados del escaneo se reflejan acuerdo su nivel de vulnerabilidad como se aprecia en la figura No. 2.

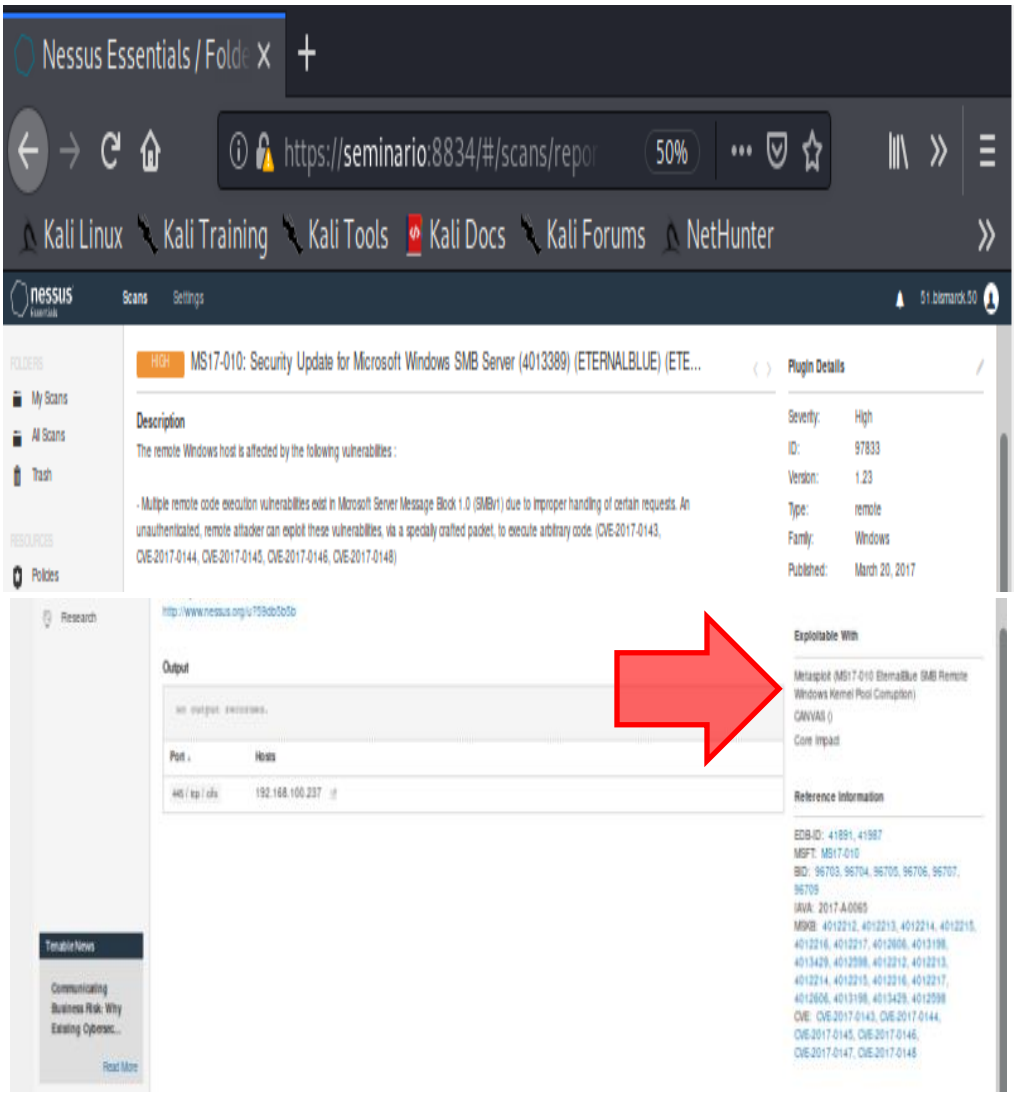
Figura No. 2 resultados escaneo nessus.



Fuente: Pierre Niño.

Se puede observar que nessus detecto en el host 192.168.100.237 21 vulnerabilidades de las cuales 4 son críticas y están relacionadas con el acceso remoto de windows como se aprecia en la figura No. 3, así mismo nos muestra el código de la vulnerabilidad MS17-010, adicionalmente muestra otros datos de interés como la forma de explotarlos y la descripción de la vulnerabilidad como tal.

Figura No. 3 vulnerabilidad y forma de explotarla.

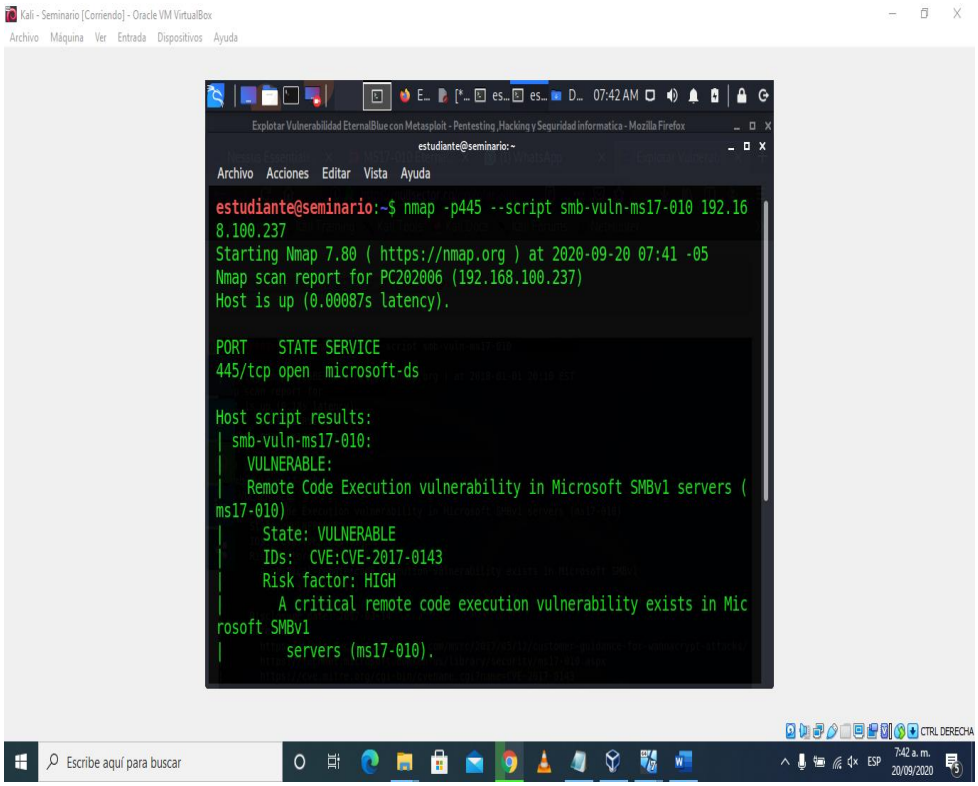


Fuente: Pierre Niño.

Para complementar la recolección y conociendo la vulnerabilidad CVE-2017-0144, hacemos uso de un comando más específico de nmap, que nos indicara si la máquina de win7 x64 es vulnerable o no.

Para realizar esto se empleó el comando: nmap --script smb-vuln -ms17-010 -v como se aprecia en la figura No. 4, allí nos muestra que el puerto 445 está abierto y se puede establecer una comunicación tcp, adicionalmente nos informa que sí es vulnerable.

Figura No. 4 resultados escaneo nmap específico.

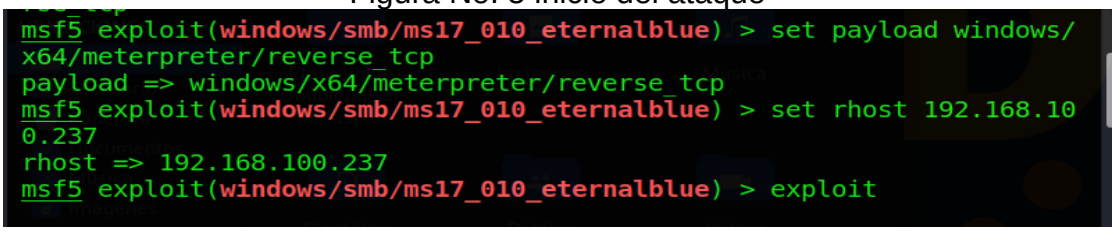


Fuente: Pierre Niño.

2.2 FASE DE EXPLOTACIÓN

En esta fase, se empleó la herramienta metasploit, mediante el framework para la máquina de win7 x64, exploit/Windows/smb//ms17_010_eternalblue, como se observa en la figura No. 5.

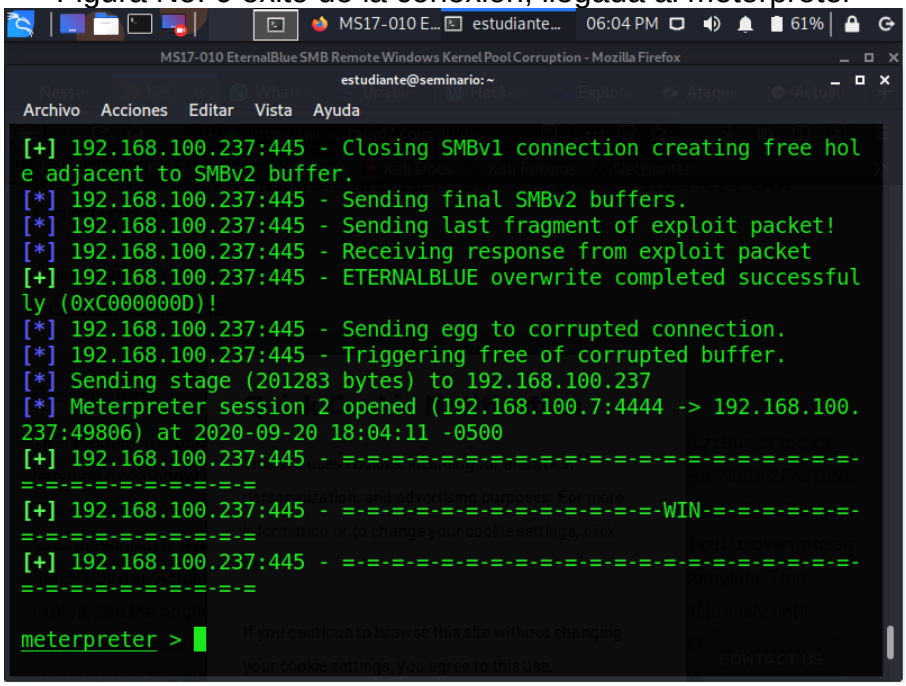
Figura No. 5 inicio del ataque



Fuente: Pierre Niño

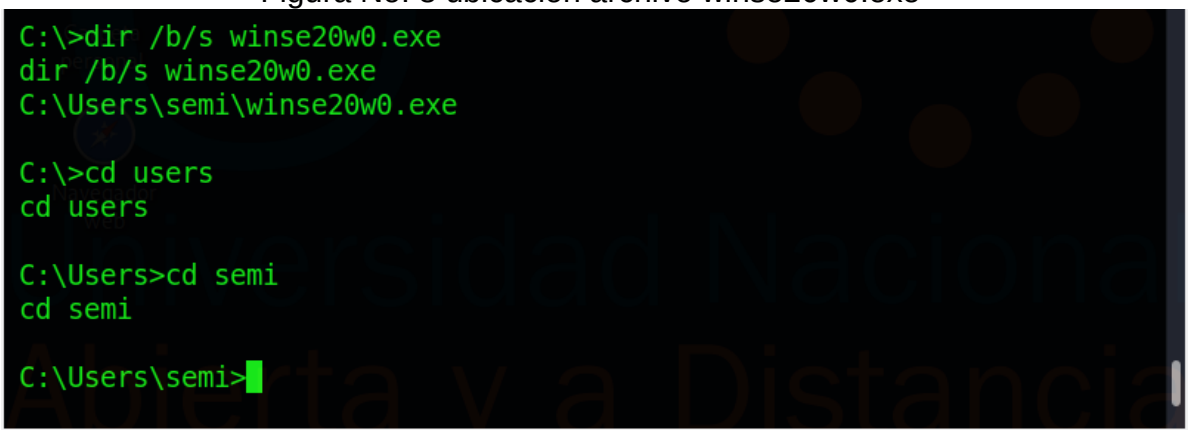
En la siguiente figura No. 6, se muestra el resultado del lanzamiento del exploit, en este caso se logró iniciar la sesión en la máquina win7 x64 desde la máquina atacante.

Figura No. 6 éxito de la conexión, llegada al meterpreter


MS17-010 E...
estudiante...
06:04 PM
61%
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Mozilla Firefox
estudiante@seminario: ~
Archivo Acciones Editar Vista Ayuda
[+] 192.168.100.237:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.100.237:445 - Sending final SMBv2 buffers.
[*] 192.168.100.237:445 - Sending last fragment of exploit packet!
[*] 192.168.100.237:445 - Receiving response from exploit packet
[+] 192.168.100.237:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.100.237:445 - Sending egg to corrupted connection.
[*] 192.168.100.237:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.100.237
[*] Meterpreter session 2 opened (192.168.100.7:4444 -> 192.168.100.237:49806) at 2020-09-20 18:04:11 -0500
[+] 192.168.100.237:445 - =-=-=-=

Para demostrar la intrusión a esta máquina vamos copiar y ejecutar el archivo winse20w0.exe, el cual lo situamos en la ruta C:\User\semi, como se muestra en la figura No. 8.

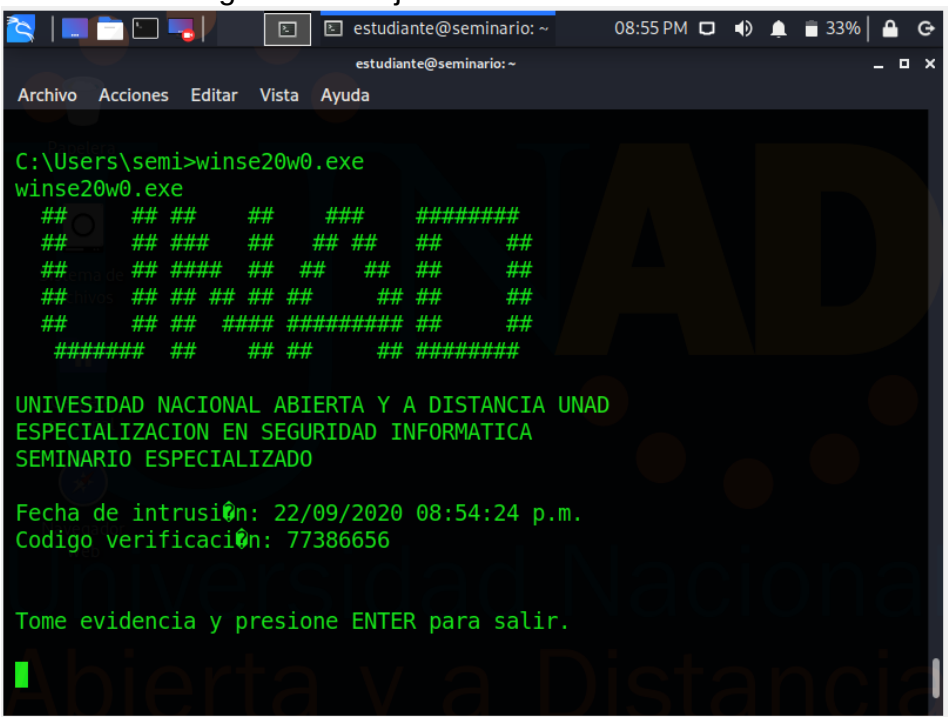
Figura No. 8 ubicación archivo winse20w0.exe



Fuente: Pierre Niño.

En la figura No. 9 se muestra el archivo winse20w0.exe ejecutado, esto es a manera de mostrar lo vulnerable que se encuentra la máquina.

Figura No. 9 ejercicio exitoso culminado



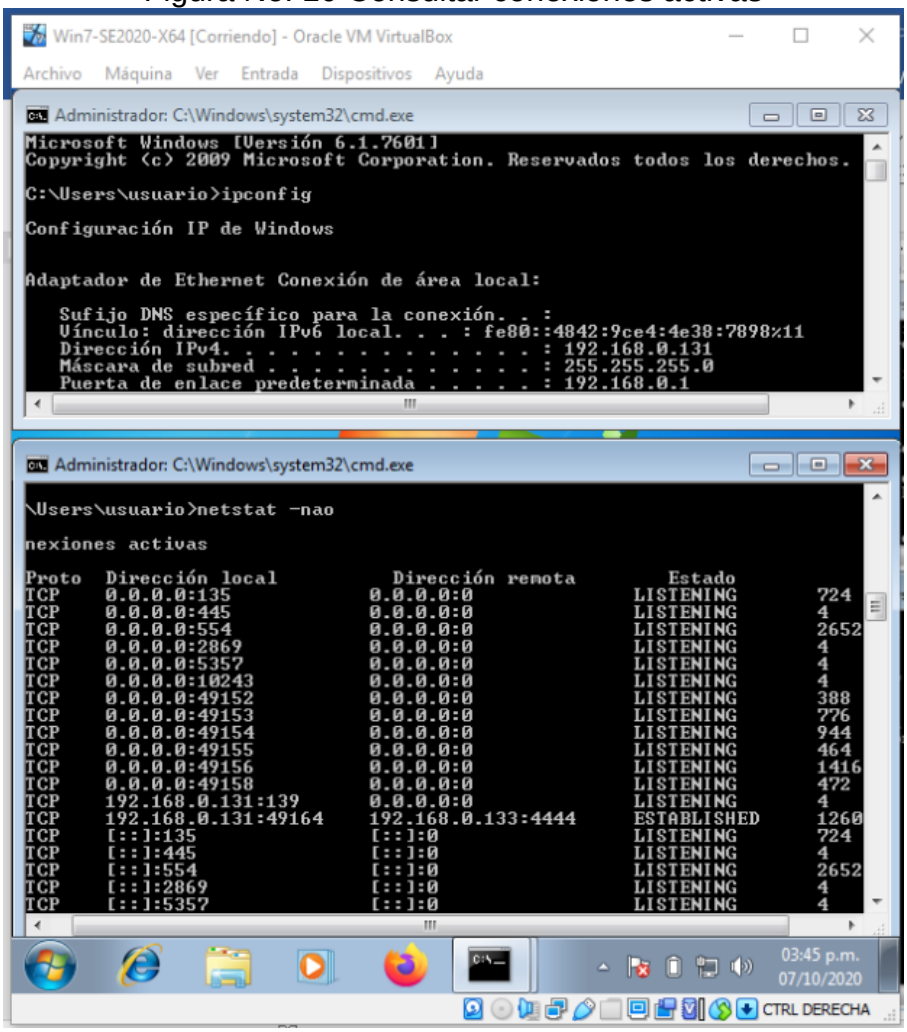
Fuente: Pierre Niño.

3. MEDIDAS PARA CONTENER EL ATAQUE

En la máquina de win7 x64

Se listaron todas las conexiones activas en la máquina con la herramienta netstat, con el comando “netstat -nao”, como se observa en la figura No. 10, dónde se detalla la dirección local de la máquina win7 x64 IP 192.168.0.131 con el puerto de conexión TCP 49164 y la dirección de la máquina atacante IP 192.168.0.133 con el puerto 4444 con el PID (Identificación del Proceso) No. 1260.

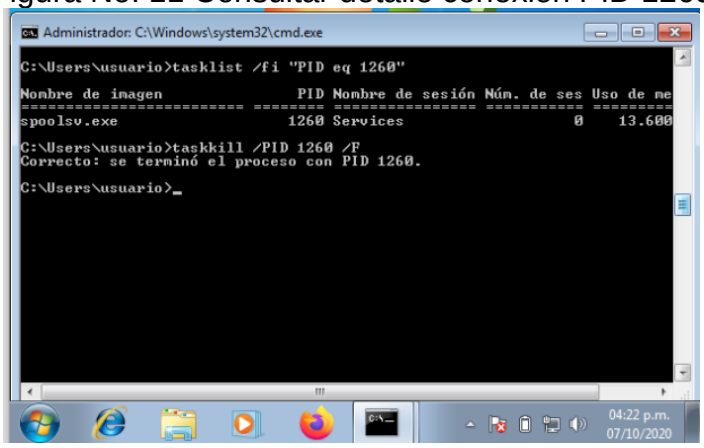
Figura No. 10 Consultar conexiones activas



Fuente: Pierre Niño

Luego se empleó el comando tasklist para mostrar los procesos activos, con el parámetro /fi, para que filtre la salida y colocamos PID (identificador de proceso). Con el fin de ver los detalles del mismo, de esta manera: tasklist /fi “PID eq 1260”, de la misma forma con el comando: taskkill /PID 1260 /F matamos ese proceso, en otras palabras, terminamos el proceso que nos inició la máquina atacante, como se muestra en la figura No. 11.

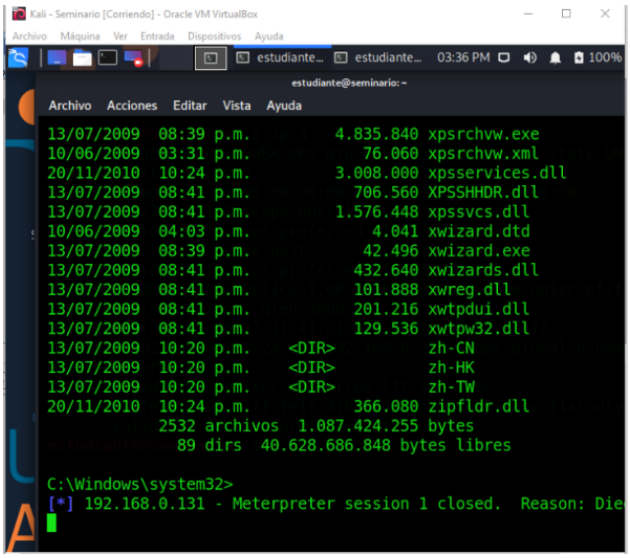
Figura No. 11 Consultar detalle conexión PID 1260



Fuente: Pierre Niño

En la figura No. 12 se observa que en la máquina atacante se cierra la sesión de la máquina víctima con IP No. 192.168.0.131, lo cual quiere decir que el atacante ya no puede realizar ninguna petición nuevamente hasta volver a iniciar el ataque, cabe destacar que iniciamos nuevamente el ataque y no se abrió la sesión.

Figura No. 12 Evidencia de sesión cerrada desde CMD máquina win7 x64
En la máquina de win7 x86

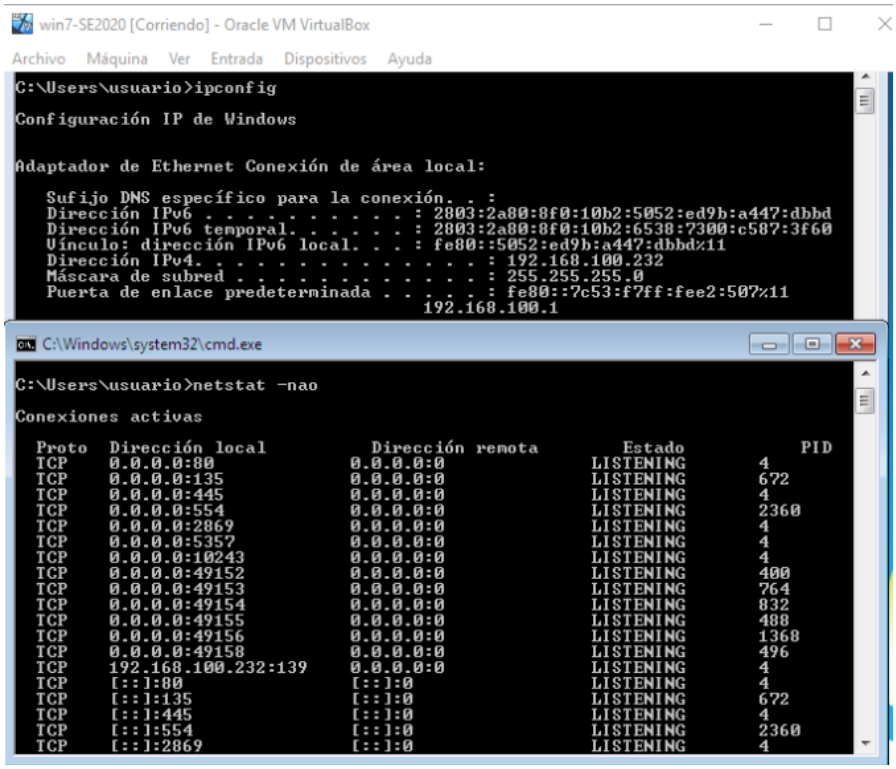


Fuente: Pierre Niño

En esta máquina se realizó el mismo procedimiento para saber si hay procesos abiertos, sin encontrar procesos activos, como se muestra en la figura No. 13.

Esto lo que indica es que el atacante no logro acceder a esta máquina, lo que permite pensar que la única máquina comprometida sería la máquina win7 x64 y se deduce que en ésta fue dónde el atacante logró sustraer la información de la empresa.

Figura No. 13 Evidencia dónde no se observan conexiones activas en la máquina win7 x86



Fuente: Pierre Niño.

Las actividades realizadas obedecen a los criterios contemplados en la “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información”[2], lo que garantiza actividades estructuradas.

[2] 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/articles-5482_G21_Gestion_Incidentes.pdf

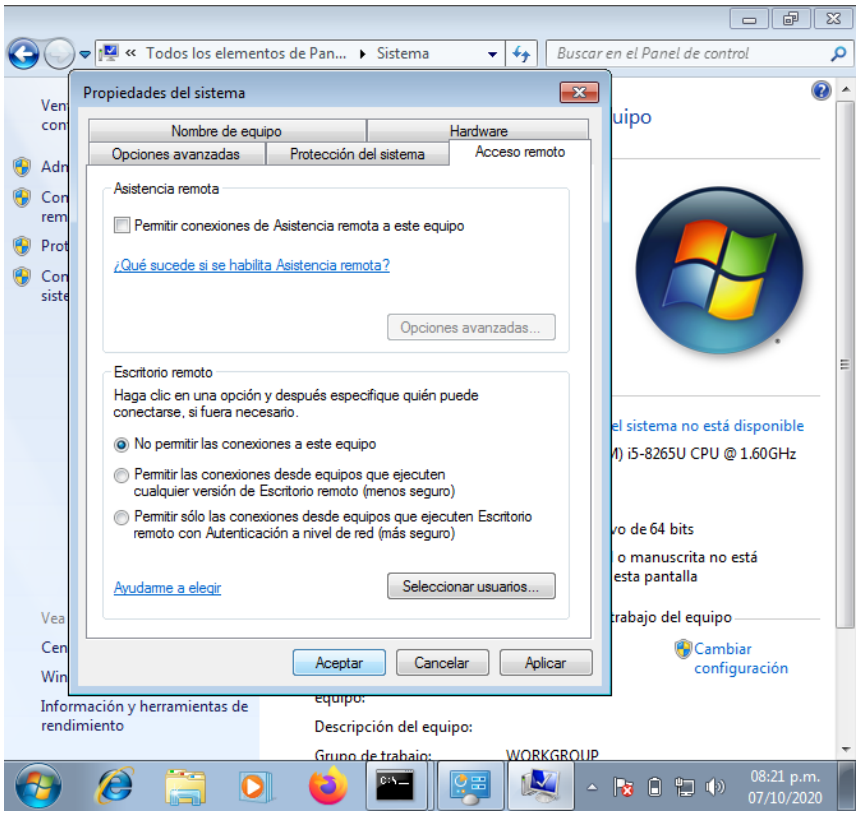
4. MEDIDAS DE HARDENIZACIÓN

Para hardenizar las máquinas Windows 7 X64 y X86 se procedió básicamente a verificar y activar todos los sistemas de seguridad que poseen los sistemas operativos como el firewall, Windows defender y acto seguido se realizan las actualizaciones necesarias con los parches de seguridad liberados por Microsoft, inicialmente dejamos el mismo puerto el “4444” pero nos mostró pantalla azul, lo que indica que la medida tomada de matar el proceso en el punto anterior con el “taskkill /PID 1260 /F” podría haber bloqueado ese puerto, sugiriendo una buena medida tomada, porque el atacante no puede volver a utilizar ese puerto.

Posteriormente se procedió a realizar las verificaciones y activaciones de los sistemas de seguridad de los sistemas operativos, más importante aún la desactivación del de la opción de permitir conexiones de asistencia remota en los equipos, como se muestra en la figura No. 14 desactivar “Permitir conexiones de asistencia remota en este equipo” ya que esta opción se encontraba activa, en la figura No. 15, se evidencia la activación y posterior actualización del sistema con el Windows update, para instalar todos los parches de seguridad faltantes, para el caso de estas máquinas se encontraron 117 actualizaciones, lo que quiere decir que estas máquinas estaban totalmente vulnerables, posteriormente activamos y actualizamos Windows Defender como se observa en la figura No. 16.

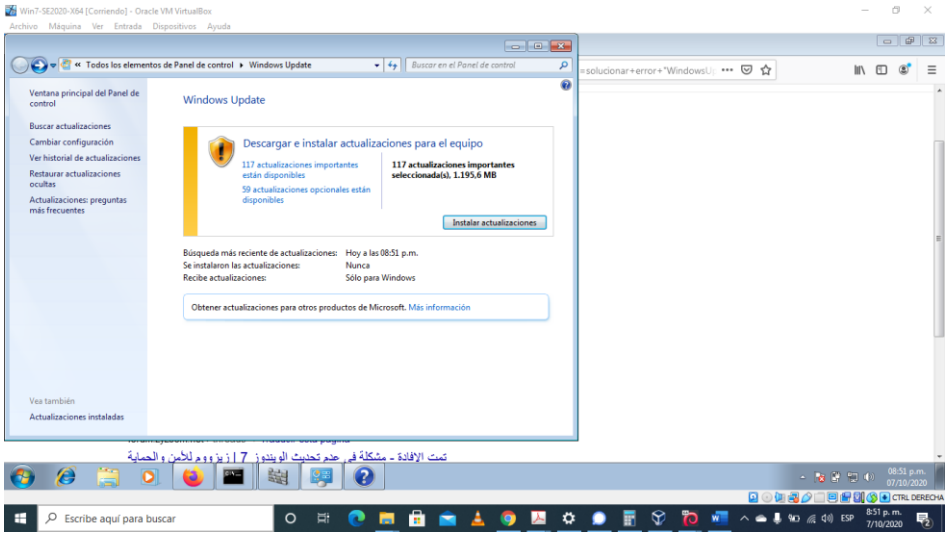
Finalmente, para la hardenización inicial y acorde a las observaciones dadas por WHITEHOUSE SECURITY dónde expresan claramente que no existe presupuesto para implementar herramientas adicionales de pago, se observa en la figura No. 17 que la amenaza fue neutralizada y contenida, se evidencia que la máquina atacante ya no puede iniciar una sesión en las máquinas víctima.

Figura No. 14 Desactivar Permitir conexiones de asistencia remota en este equipo



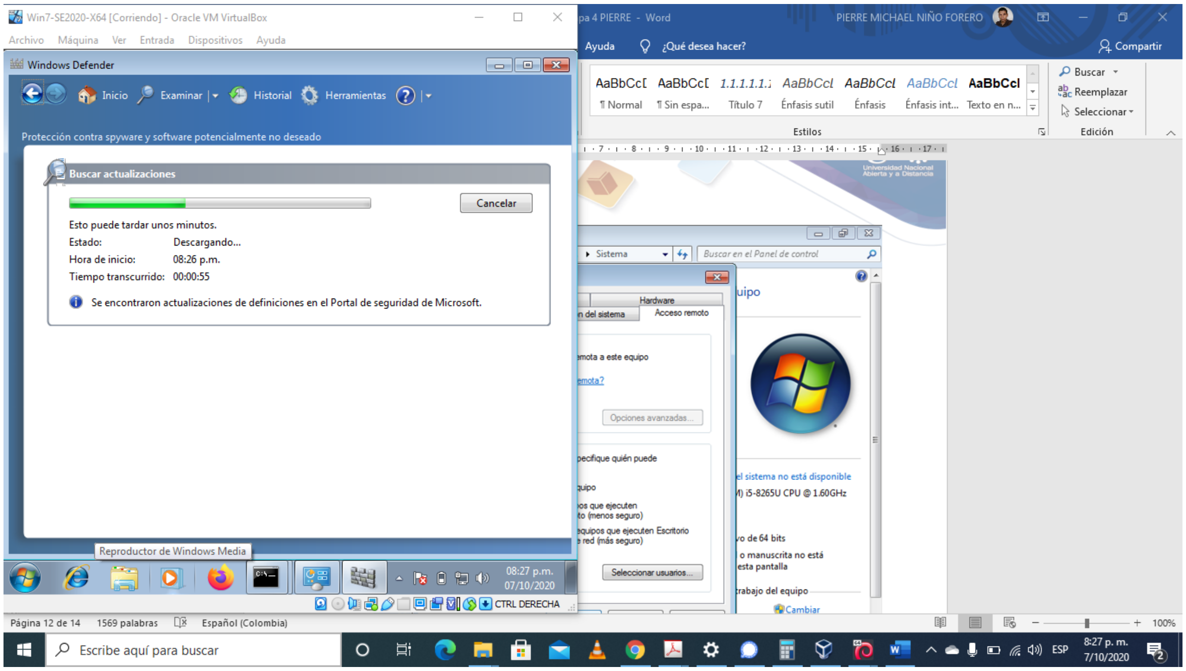
Fuente: Pierre Niño.

Figura No. 15 Activar, actualizar y posterior instalación de parches de seguridad con Windows update



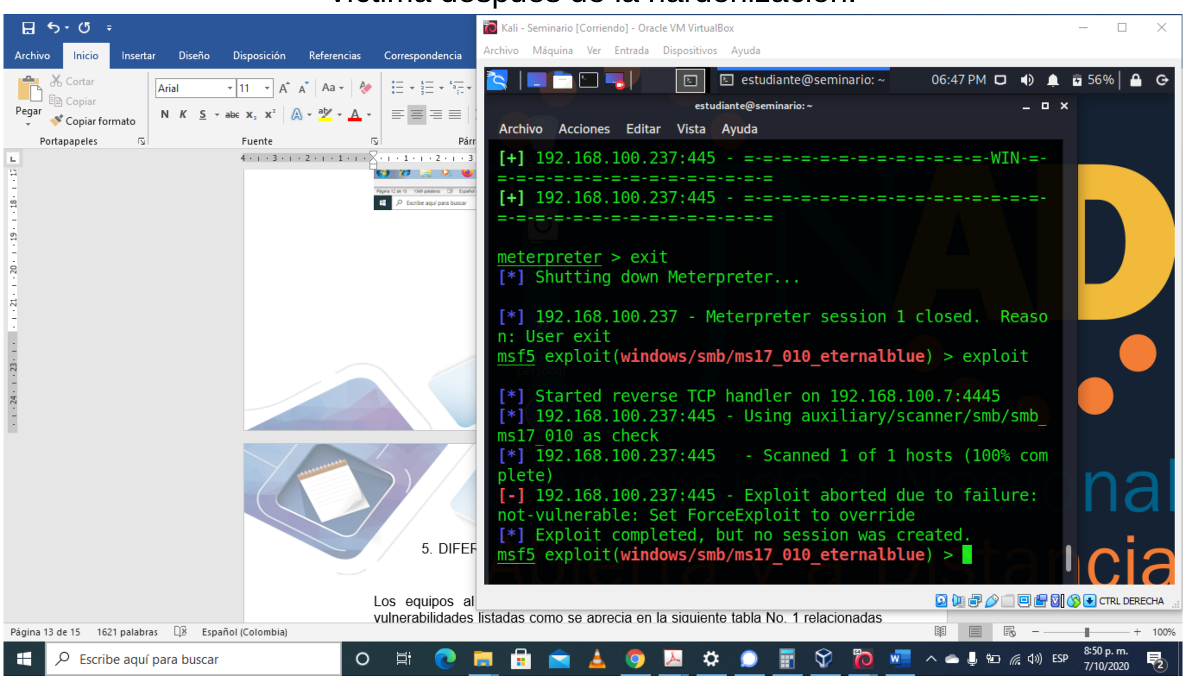
Fuente: Pierre Niño.

Figura No. 16 Activar, actualizar Windows Defender



Fuente: Pierre Niño

Figura No. 17 Evidencia máquina atacante ya no inicia sesión en la máquina víctima después de la hardenización.



Fuente: Pierre Niño.

5. LINK VIDEO SUSTENTACIÓN

https://youtu.be/h5O7Nz85AmI

6. CONCLUSIONES

Acuerdo las diferentes pruebas realizadas en la fase de intrusión se puede establecer que la máquina vulnerada fue la win7 x64, confirmando las sospechas de la empresa WHITEHOUSE SECURITY, dado que el atacante aprovecho el SMBv1 que se encontraba activo para compartir impresoras y otros archivos dentro de la red y que esta máquina tiene un sistema operativo antiguo, desactualizado y con los sistemas de seguridad nativos desactivados como el Windows Update, Windows Defender y Firewall al momento de las pruebas.

La máquina win7 x86 pudo ser vulnerada, pero es probable que el atacante no tuviera la experticia necesaria ya que utilizó el mismo payload para la máquina win7 x64 generando los pantallazos azules en la misma, esto ocurre porque esta máquina tiene una arquitectura diferente.

Es determinante la activación y actualización de los diferentes sistemas de seguridad nativos del sistema operativo, estos brindan protección que contribuye notablemente ante un ataque de este tipo.

Las medidas implementadas de contención ante el ataque en la máquina win7 x64 dieron resultados, ya que se logró cerrar la conexión y bloquear el puerto que el atacante estaba utilizando en su máquina, ocasionando que el atacante se viera forzado a cambiar su puerto al momento de realizar otro ataque.

7. RECOMENDACIONES

Fortalecer las políticas de seguridad informática como mecanismo fundamental para crear una cultura de se seguridad en la organización y minimizar los riesgos de ataques informáticos.

Mantener activas y actualizadas las medidas de seguridad nativas de los sistemas operativos de las máquinas win7 x64 y win7 x86 como el Windows Update, Windows Defender y Firewall.

En lo posible mantener desactivada la opción de “Permitir conexiones de asistencia remota en este equipo”, o por lo menos en los momentos que los equipos no se estén utilizando.

Conectar estos equipos a una intranet y realizar las actualizaciones localmente, en definitiva, no se recomienda que estén conectados a internet.

Restringir el acceso a estas máquinas mediante el bloqueo de los puertos USB u otros periféricos de entrada/salida de datos.

Instalar antivirus licenciado, con el fin de contar con actualizaciones pertinentes y confiables.

Intentar migrar la aplicación utilizada por la empresa a unos sistemas operativos actuales y licenciados, con el fin de contar con las actualizaciones, dado que Microsoft ya no libera parches de seguridad para sistemas operativos Windows 7.

Ver la posibilidad de incluir en los planes de inversión de la empresa sistemas adicionales de seguridad perimetral como firewall, sistemas de detección y prevención de Intrusos como IDS, IPS entre otros.

Denunciar ante las autoridades el caso, preferiblemente ante la Fiscalía General de la Nación en su página en internet.

BIBLIOGRAFÍA

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/articles-5482_G21_Gestion_Incidentes.pdf

SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran. (2020) SOFECOM, Servicios integrales en IT. Recuperado de: https://sofecom.com/que-es-un-siem/

Windows: Eliminar conexiones activas tcp. (2015). SYSADMIT. https://www.sysadmit.com/2015/01/windows-eliminar-conexiones-activas-tcp.html#:%7E:text=Otra%20forma%20de%20eliminar%20las,utilizando%20la%20utilidad%20gratuita%20wKillcx.&text=Tal%20y%20como%20vemos%20en,netstat%20para%20eliminar%20la%20conexi%C3%B3n

Datacom.global. (2016). Recuperado de: https://datacom.global/cisco-seguridad-deteccion-de-amenazas-en-las-organizaciones/

Esystemsas.com. (2020). Recuperado de: https://esystemsas.com/seguridad-informatica/

Blog.smartekh.com. (2017) Recuperado de: https://blog.smartekh.com/sandbox-porque-paraque

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

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26) Recuperado de: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

Cve.mitre.org (2020). Common Vulnerabilities and Exposures. Recuperado de https://cve.mitre.org/

Munjal, Meenaakshi N. (2013). "ETHICAL HACKING: AN IMPACT ON SOCIETY." 7.1. Páginas 922-931. Web.

Phases Of Hacking. (2018) Ethical Hacking. Greycampus.com. Web.

Radziwill, Nicole et al. (2018) "The Ethics Of Hacking: Should It Be Taught?." Arxiv.org. N.p., 2005. Web.

Summarizing. (2018). The Five Phases Of Penetration Testing - Cybrary." Cybrary. N.p., 2015. Web.