Université de Technologie d'Haïti

UNITECH

Facultés des sciences, de génie et d'architecture

TD N3-Test de Sécurité Metasploit

Nom et prénom : Shamaya LOUIS

Niveau : 4em année

Date : 23/02/2026

Contents

1.Description des résultats de la tâche

Dans le domaine de la cybersécurité, les tests d'intrusion permettent d'identifier les vulnérabilités présentes dans un système informatique afin d'améliorer sa protection.

Ce travail dirigé a pour objectif de mettre en place un environnement de laboratoire comprenant une machine attaquante sous Kali Linux et une machine vulnérable Metasploitable 2.

À l'aide d'outils spécialisés tels que Nmap et Metasploit Framework, nous avons simulé plusieurs scénarios d'analyse et d'exploitation de vulnérabilités réseau.

1.1 L'objectif de ce td consiste à mettre en place et exploiter un environnement Metasploit dans Kali Linux pour simuler un test d'intrusion réel.

- Installer et configurer un système Kali Linux avec Metasploit Framework.
- Lancer et manipuler le terminal Metasploit (msfconsole).
- Scanner un réseau pour identifier les services vulnérables à l'aide de Nmap.
- Explorer une première interaction avec une machine vulnérable (Metasploitable).
- Valider la connectivité réseau entre l'attaquant (Kali) et la cible (Metasploitable).

Matériaux utiliser

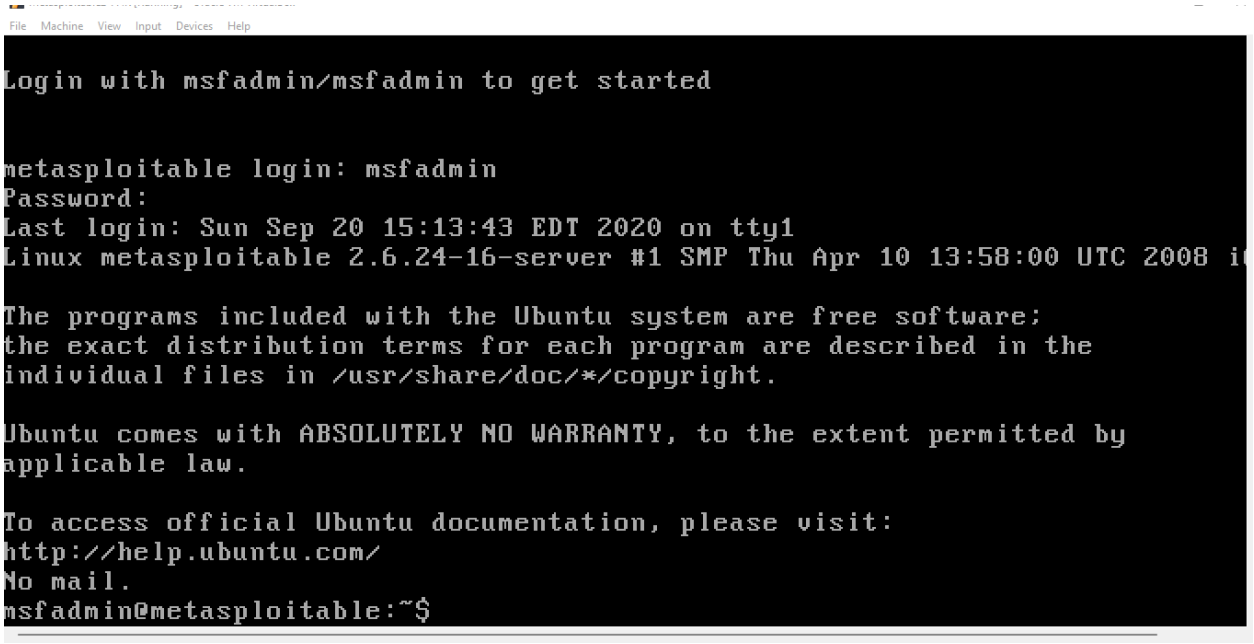
Logiciel de virtualisation, Kali linux, Metasploit Framework (inclus par defaut dans kali linux) et une machine cible

2.Résultats de l'exécution des commandes

Déroulement du TD

La machine virtuelle Metasploitable a été importée dans VirtualBox via le fichier OVA fourni puis après le démarrage on utilise les identifiants ci-dessous :

- **Login :** msfadmin
- **Password :** msfadmin

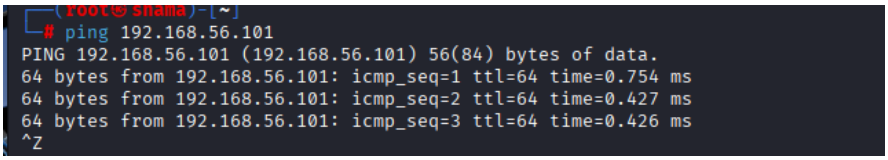


On optient l'adresse IP avec la commande : ip a

2.1 Scan de vulnérabilités

nous avons identifier les services réseau ouverts sur la machine virtuelle à l'aide du scanner de sécurité Nmap.

Avec la commande ping <ip_cible>, on verrifier la communication



Nmap <ip_cible> : plusieurs ports ouverts détectés (FTP, SSH, HTTP, etc.)

```
┌──(root㉿shama)-[~]
└─# nmap 192.168.56.101
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-23 21:37 +0100
Nmap scan report for 192.168.56.101
Host is up (0.00026s 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
```

Nmap -sv -o <ip_cible> : identifier les versions de services et du système d'exploitation.

```
┌──(root㉿shama)-[~]
└─# nmap -sv -o 192.168.56.101
Nmap 7.98 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given por
ts
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
```

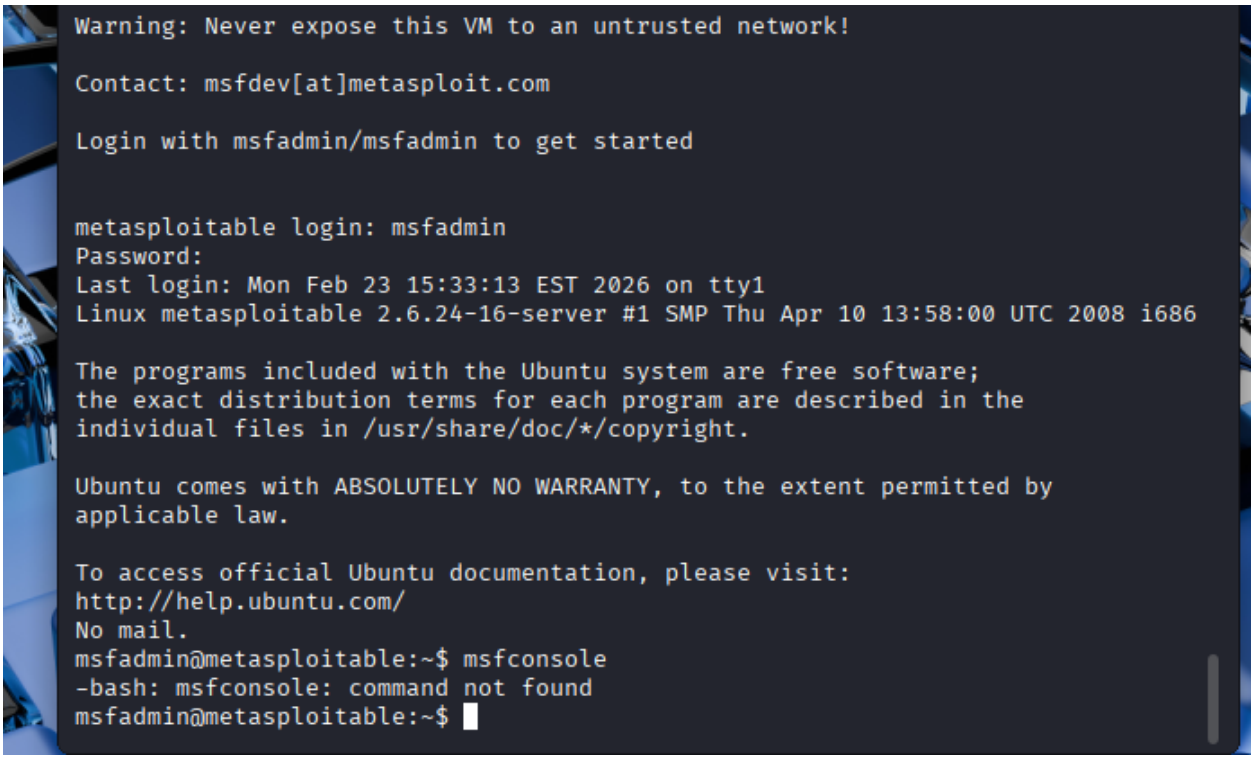
telnet <ip_cible> : Connexion au service Telnet

```
┌──(root㉿shama)-[~]
└─# telnet 192.168.56.101
Trying 192.168.56.101 ...
Connected to 192.168.56.101.
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:
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Mon Feb 23 15:33:13 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:~$
```

Exploits FTP – Metasploitable 2 via Metasploit

Msfconsole



Conclusion

Ce travail a permis d'acquérir une connaissance approfondit dans les étapes d'un test d'intrusion, notamment la reconnaissance, scanner un réseau, identifier et exploiter les vulnérabilités et aussi permet d'accéder à un système. Avec l'utilisation de kali linux et quelque outil intégrer comme nmap et metasploit nous avons pu réaliser quelques tests pour démontrer et comprendre les vulnérabilités.