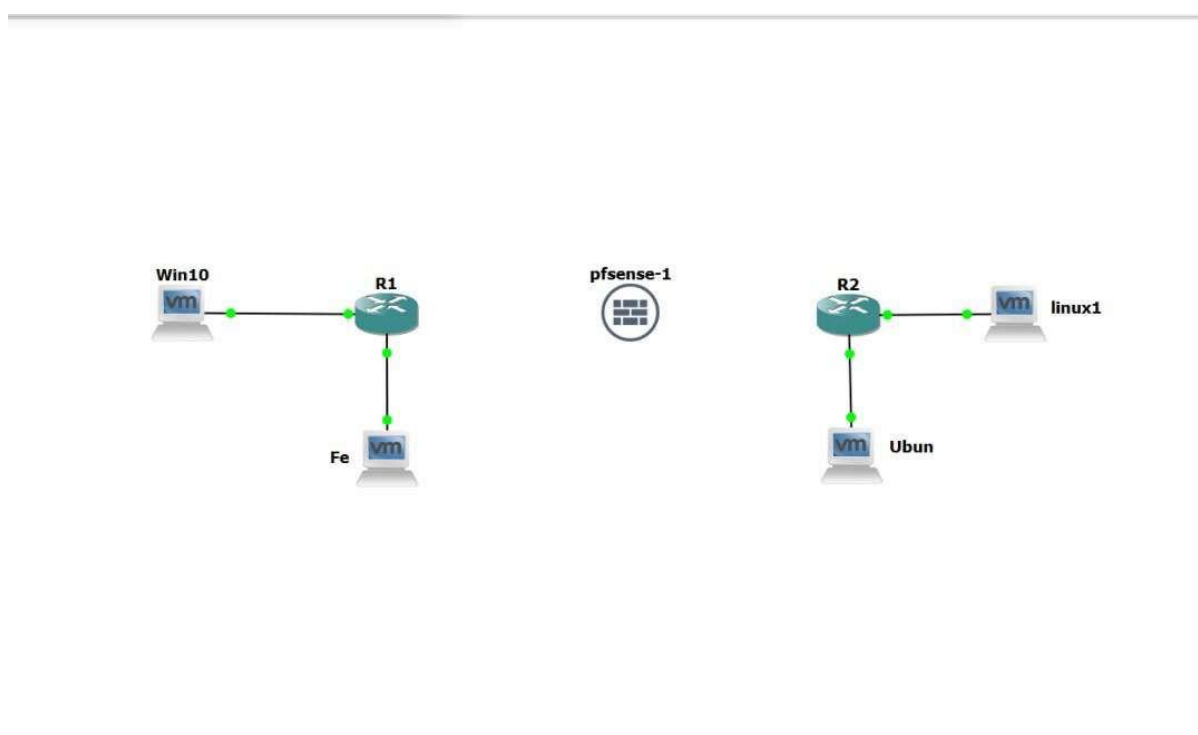


TP : Audit de Sécurité d'un Réseau Local

INTRODUCTION

Objectif : Tester la sécurité d'un réseau interne fictif pour identifier les vulnérabilités et proposer des mesures correctives.

TOPOLOGIE DU TP



Voici le graphique que j'ai pu faire pour avoir un aperçu pour pouvoir continuer le travail

1)MÉTHODOLOGIE

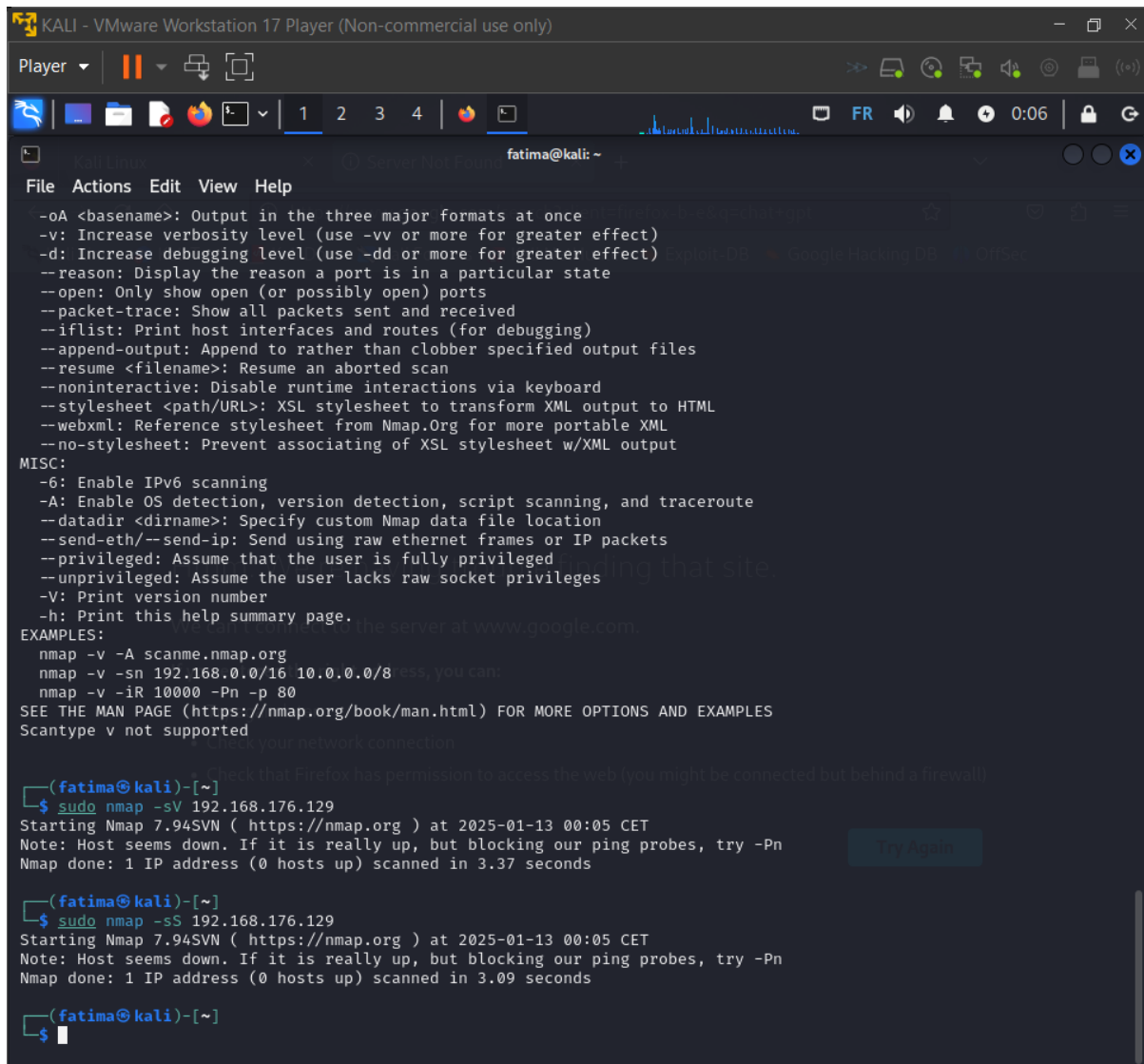
D'abord nous allons installer nos machine virtuelle pour pouvoir faire le travail

- Ensuite je vais mettre tout les machine en mm reseau pour permettre la connectivité entre eux et facilité le travail
- Nous allons utilisé kali comme systeme d'exploitation ,Ubuntu comme server ,Pfsense,win 10 et fedora et linux mint comme des clients

Nmap : Pour la découverte de réseau et le scan des ports.

A) KALI

Elle va nous permet faire le scanne de réseau et le scan des ports



```
KALI - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
fatima@kali: ~
File Actions Edit View Help
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype v not supported
(fatima@kali)-[~]
$ sudo nmap -sV 192.168.176.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:05 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.37 seconds
(fatima@kali)-[~]
$ sudo nmap -sS 192.168.176.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:05 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
(fatima@kali)-[~]
$
```

On utilise nmap sS La commande nmap -sS est utilisée pour effectuer un "SYN scan" (scan SYN), également appelé "scan furtif" ou "half-open scan". Ce type de scan est populaire en raison de sa rapidité et de sa capacité à éviter la détection par certaines configurations de pare-feu ou de systèmes de détection d'intrusion (IDS).

```
KALI - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
fatima@kali: ~
File Actions Edit View Help
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype v not supported

(fatima@kali)-[~]
$ sudo nmap -sV 192.168.176.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:05 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.37 seconds

(fatima@kali)-[~]
$ sudo nmap -sS 192.168.176.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:05 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds

(fatima@kali)-[~]
$ sudo nmap -sS 192.168.112.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:07 CET
Nmap scan report for 192.168.112.131
Host is up (0.00010s latency).
All 1000 scanned ports on 192.168.112.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:5C:CA:A4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

(fatima@kali)-[~]
$ sudo nmap -sV 192.168.112.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:08 CET
Nmap scan report for 192.168.112.131
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.112.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:5C:CA:A4 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds

(fatima@kali)-[~]
$
```

a commande `nmap -sV` est utilisée pour effectuer un scan de **détection de version des services** sur les ports ouverts d'un hôte cible. Ce scan permet à Nmap de déterminer quel logiciel (et sa version) est en cours d'exécution sur un port spécifique.

Voici le fonctionnement de `nmap -sV` :

```
KALI - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
fatima@kali: ~
File Actions Edit View Help
$ sudo nmap -sS 192.168.176.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:05 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds

(fatima@kali)-[~]
$ sudo nmap -sS 192.168.112.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:07 CET
Nmap scan report for 192.168.112.131
Host is up (0.00010s latency).
All 1000 scanned ports on 192.168.112.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:5C:CA:A4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

(fatima@kali)-[~]
$ sudo nmap -sV 192.168.112.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:08 CET
Nmap scan report for 192.168.112.131
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.112.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:5C:CA:A4 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds

(fatima@kali)-[~]
$ sudo nmap -O 192.168.112.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:09 CET
Nmap scan report for 192.168.112.131
Host is up (0.00079s latency).
All 1000 scanned ports on 192.168.112.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:5C:CA:A4 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.78 seconds

(fatima@kali)-[~]
$
```

La commande `nmap -O` est utilisée pour activer la détection du **système d'exploitation** (OS detection) d'un hôte cible. Lorsque vous utilisez l'option `-O`, Nmap tente d'identifier le système d'exploitation qui tourne sur la machine cible en analysant les réponses aux paquets envoyés pendant le scan.

```
KALI - VMware Workstation 17 Player (Non-commercial use only)
Player
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:5C:CA:A4 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

(fatima@kali)-[~]
$ sudo nmap -sV 192.168.112.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:08 CET
Nmap scan report for 192.168.112.131
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.112.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:5C:CA:A4 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds

(fatima@kali)-[~]
$ sudo nmap -sS 192.168.112.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:09 CET
Nmap scan report for 192.168.112.131
Host is up (0.00079s latency).
All 1000 scanned ports on 192.168.112.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:5C:CA:A4 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.78 seconds

(fatima@kali)-[~]
$ sudo nmap -sT 192.168.112.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 00:10 CET
Nmap scan report for 192.168.112.131
Host is up (0.00092s latency).
All 1000 scanned ports on 192.168.112.131 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
MAC Address: 00:0C:29:5C:CA:A4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds

(fatima@kali)-[~]
$
```

La commande `nmap -sT` est utilisée pour effectuer un **scan de connexion complète** (ou "TCP connect scan"). Contrairement au scan **SYN** (`-sS`), qui n'achève pas la connexion TCP, le scan `-sT` tente d'établir une connexion complète avec chaque port ouvert sur la cible.

On a utiliser sa pour chaque machine client client pour verifier le reseau et les porsts ouverts avec Kali vu qu'il a deja nmap dedans

Nmap est un outil puissant pour l'exploration et l'analyse de réseaux. Il est essentiel pour les administrateurs réseau, les experts en sécurité et les tests de pénétration afin de surveiller, sécuriser et analyser les réseaux.

NB: J'ai pas pu utiliser NESSUS et wirshark parce que j'avais des probleme avec machine