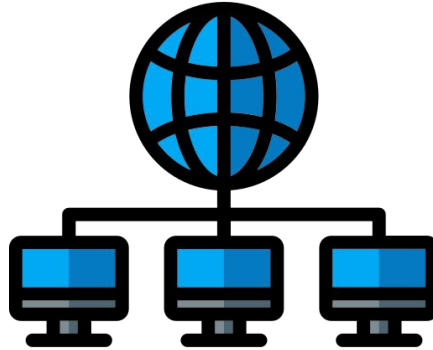


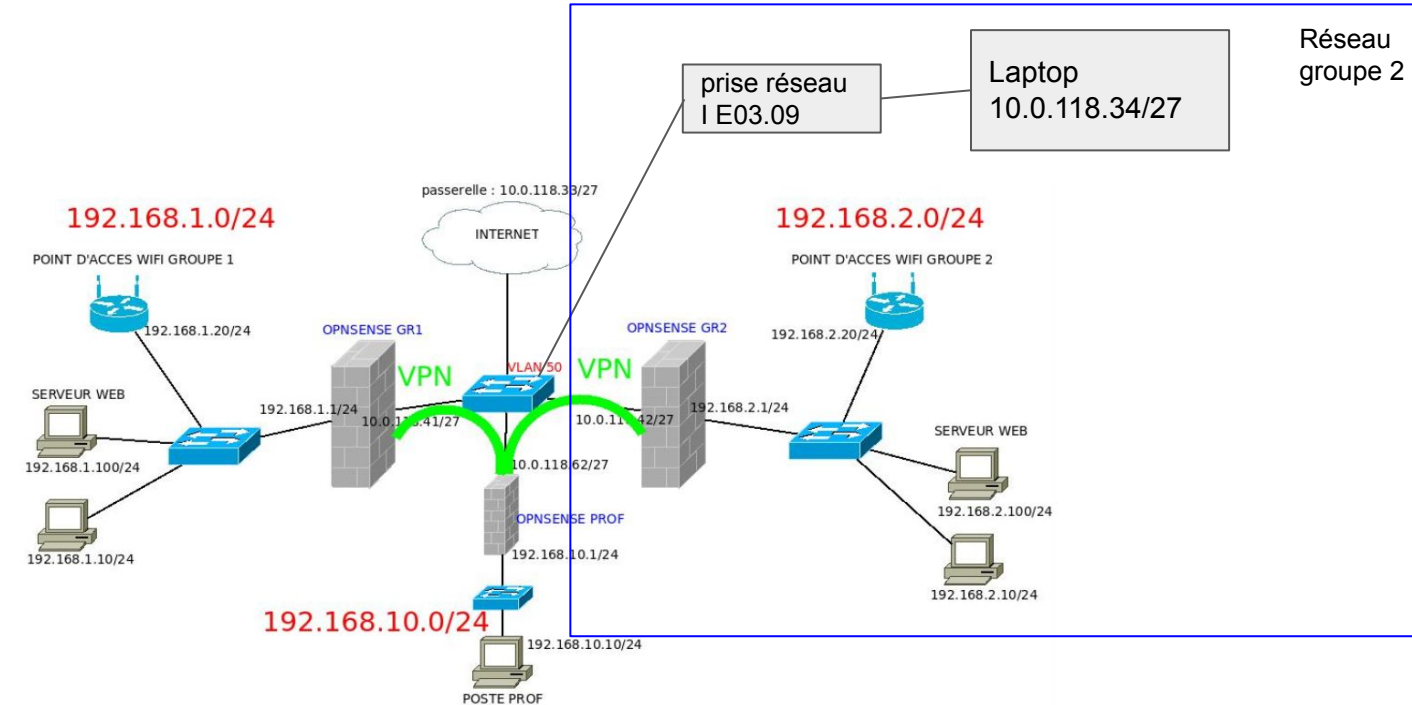
TP Attaque réseaux



BOURDEAU Valentin
BULTEAU François
DURAN Antonin
GAURIER Nicolas
HUMBERT Arthur
TATE Bastien



Configuration du réseau





Serveur web : configuration

Adresse IP :

```
systemctl stop NetworkManager  
killall dhclient  
ip a flush dev eth0
```

```
local@1114-PC12-SNIR:~$ ipcalc 192.168.2.100/24  
Address: 192.168.2.100 11000000.10101000.00000010. 01100100  
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000  
Wildcard: 0.0.0.255 00000000.00000000.00000000. 11111111  
=>  
Network: 192.168.2.0/24 11000000.10101000.00000010. 00000000  
HostMin: 192.168.2.1 11000000.10101000.00000010. 00000001  
HostMax: 192.168.2.254 11000000.10101000.00000010. 11111110  
Broadcast: 192.168.2.255 11000000.10101000.00000010. 11111111  
Hosts/Net: 254 Class C, Private Internet
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP  
group default qlen 1000  
link/ether e4:54:e8:da:c9:26 brd ff:ff:ff:ff:ff:ff  
inet 192.168.2.100/24 brd 192.168.2.255 scope global eth0  
valid_lft forever preferred_lft forever
```


```
root@1114-PC12-SNIR:/local# ip route show  
default via 192.168.2.1 dev eth0  
192.168.2.0/24 dev eth0 proto kernel scope link src 192.168.2.100
```

```
ip a add 192.168.2.100/24 brd  
192.168.2.255  
ip route add default via 192.168.2.1
```




Serveur web : configuration

Vérification de la présence du serveur web Apache :



• Antonin DURAN
• Nicolas GAURIER

Compte rendu TP technologie Web



Sommaire :

1. Introduction
2. Mise en place d'un Serveur
 - Serveur Apache2
 - Première page HTML/CSS :
 - Ajout de fonctionnalité PHP :
3. Script CGI
 - Script Capture / Suppression d'images :
 - Script Capture
 - Script de Suppression
 - Modification des retours de Script
4. Base de données

Introduction

```
root@1114-PC12-SNIR:/local# ls /var/www/html -la
total 24
drwxrwxrwx 2 root root 4096 déc. 21 15:25
drwxrwxrwx 3 root root 4096 déc. 21 11:20
-rw-r--r-- 1 root root 10988 déc. 21 15:28 index.html
-rwxrwxrwx 1 1190 513 41 déc. 21 15:15 phpinfo.php
```



Session SSH accessible

Consigne : Mot de passe ssh d'une machine LAN : "password" avec accès ssh depuis internet

Création utilisateur "admin"

Définition du mot de passe : "password"

Définition des droits de la session "admin" : uniquement dans son propre dossier

La consigne est respectée.



Session SSH accessible

Création de l'utilisateur "admin" :

```
sudo useradd -m -d /home/admin admin  
sudo passwd admin
```

```
unnamed@DEBIAN-UORLGIV:~$ ssh admin@192.168.2.10  
admin@192.168.2.10's password:  
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-104-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
80 mises à jour peuvent être appliquées immédiatement.  
44 de ces mises à jour sont des mises à jour de sécurité.  
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgrad  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check y  
  
Last login: Wed Mar 23 15:05:06 2022 from 192.168.2.24  
$ ls  
$ ls  
$  
$  
$ ls -la  
total 36  
drwxr-xr-x 4 admin noanyright 4096 mars 23 14:55 .  
drwxr-xr-x 4 root root 4096 mars 23 14:53 ..  
-rw-r--r-- 1 admin noanyright 220 févr. 25 2020 .bash_logout  
-rw-r--r-- 1 admin noanyright 3771 févr. 25 2020 .bashrc  
drwx----- 2 admin noanyright 4096 mars 23 14:55 .cache  
drwxr-xr-x 5 admin noanyright 4096 mars 23 14:55 .config  
-rw-r--r-- 1 admin noanyright 807 févr. 25 2020 .profile  
-rw-r--r-- 1 admin noanyright 0 mars 23 14:55 .sudo_as_admin_successful  
-rw-r--r-- 1 admin noanyright 1600 avril 9 2020 .Xdefaults  
-rw-r--r-- 1 admin noanyright 14 avril 9 2020 .xscreensaver
```

Test de connexion SSH depuis une autre machine



Session SSH accessible

Modification des droits de l'utilisateur :

Création d'un groupe inutile : **noanyright**

```
groupadd noanyright
```

```
usermod -g noanyright -G noanyright
```

```
sudo nano /etc/sudoers
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
#include /etc/sudoers.d
```

```
$ sudo nano
[sudo] Mot de passe de admin :
admin n'apparaît pas dans le fichier sudoers. Cet incident sera signalé.
$
```



Faible de sécurité corrigée

Avant correction :

```
$ su local  
Mot de passe :  
local@1114-PC11-SNIR:/home/admin$ exit
```

```
-rwsr-xr-x 1 root root 71912 20 janv. 21:10 su
```

```
chmod 100 su
```

Après correction :

```
-rwxr-xr-x 1 root root 84344 sept. 5 2019 stty  
---x----- 1 root root 67816 févr. 7 14:33 su
```

```
$ su  
-sh: 13: su: Permission denied
```

dossier /usr/bin



Point d'accès WIFI : Configuration

- en
- conf t
- interface BVI
- ip address 192.168.2.20 255.255.255.0
- no shutdown
- exit x2
- ping 192.168.2.1

Enable Radio:

☒ Enable

☐ Disable

SSID Table

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input checked="" type="radio"/>	Gr2	none	none	open	none		✓



Vérification du réseaux et des ports ouvert

On supprime tous les ports non utilisés.

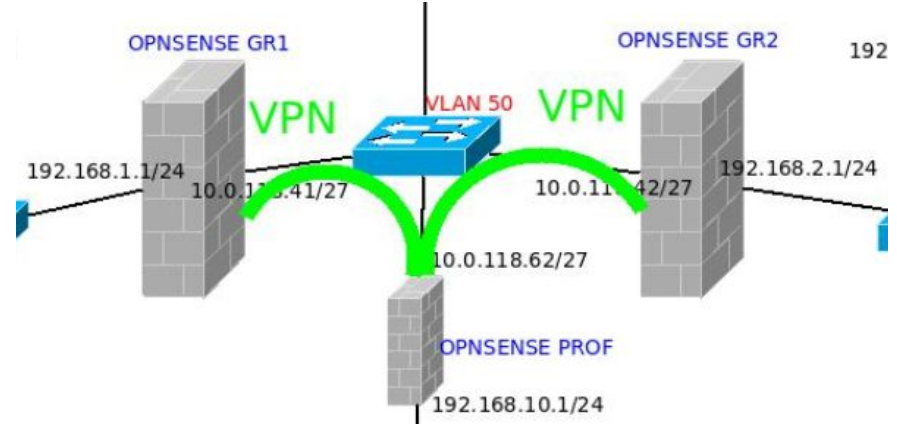
Sur le serveur 192.168.2.100 on ferme le port ssh et on laisse le port http ouvert pour donner accès à la page web.



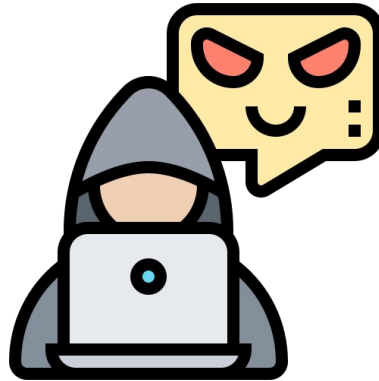
Mise en place du FireWall

On a mit en place le FireWall entre les réseaux 10.0.118.42/27 et 192.168.2.1/24

On a mit en place une liaison vpn entre les FireWall.



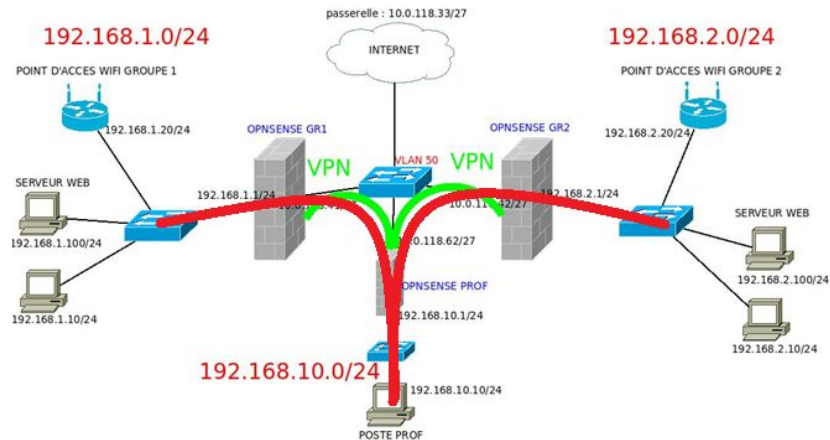
Attaque de réseaux ennemie





Brute force pour trouver le mpd : 'toto'

Connexion au Pc





Etude des ports

```
local@SNIR-LAT-09:~$ nmap 192.168.1.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-23 15:10 CET
Nmap scan report for 192.168.1.1
Host is up (0.0015s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.1.10
Host is up (0.0012s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind

Nmap scan report for 192.168.1.27
Host is up (0.031s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind

Nmap scan report for 192.168.1.100
Host is up (0.00089s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
```

nmap 192.168.1.1-255



Connexion ssh aux différentes machines

Brute force pour trouver le mdp ssh

sur les ip .10 et .100 aucune résultat viable

sur le .27 succès avec le mdp : 'local'



Connecter à un pc du réseaux en ssh

On essaye d'atteindre les autres machines du réseaux avec une attaque brute force sur les ports ssh des autres pc.

```
sudo hydra -l local -p 10-million-combos -t 4 192.168.1.100 ssh
```




Accès sur l'ordinateur 192.168.1.27

```
local@lpt01:~/Bureau/COUCOUC$ ls
10-million-combos.txt  10-million-combos.zip  eheh  hydra.restore  perdu.jpg
local@lpt01:~/Bureau/COUCOUC$ █
```

Conclusion

Utilisation des application :

- Hydra
- Nmap
- AirCrack (etc..)
- Wifit (analyse des réseau wifi)