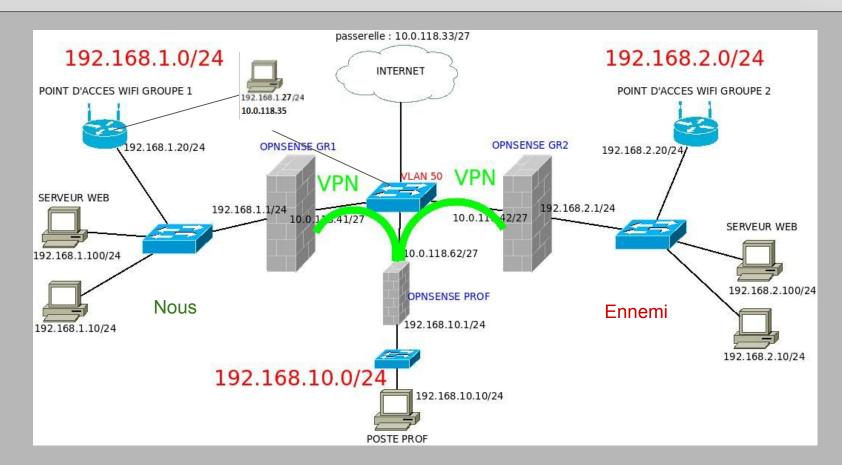


Architecture réseau





Partie défense : Serveur web



Ajout d'une adresse IP : 192.168.1.100/24

Mise en service en service du serveur web

Vérification de l'installation d'Apache

Serveur web OPÉRATIONNEL

Modification de la page HTML

Partie défense : Point d'accès wifi



Configuration de l'AP :

Attribution de l'adresse IP : 192.168.1.20

Point d'accès OPÉRATIONNEL

Ajout d'un SSID public : iPhone de Mathieu

Ajout d'une clé WPA : azerty12

SSID Table											
Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID				
•	iPhone de Mathieu	none	ciphers aes-ccm tkip	open	wpa		✓				

Partie défense : Pc utilisateur



Ajout d'une adresse IP : 192.168.1.10/24

Ajout d'une route par défaut

Changement du mot de passe

Partie defense : Firewall



▼ Inspec

+ / D 0

+ / D 0

+ / 0 0

première correspondance

dernière correspondance

root@OPNsense.localdomain

Sélectionnez une catégorie

Automatically generated rules

Reset du pare-feu

Configuration des adresses IP :

- LAN: 192.168.1.1/24
- WAN: 10.0.118.41/27

Configuration du pare feu :

- DHCP désactivé
- IPV6 : tout refusé
- Nom du serveur = IP de la passerelle

EOPO

Rapports

A Interfaces

A Pare-feu

Alias

Categories

Groupes

NAT

Règles

Pare-feu: Règles: WAN

IPv4+6 TCF

mark Active/Inactive Schedule (click to view/edit)

Alias (cliquer pour visualiser/éditer)

not explicitly passed is blocked by default.

Changement de nom : Firewall -> Aliases

Firewall OPÉRATIONNEI

Changement du mot de passe

VPN mit en place entre les deux Firewall



Destination

192.168.1.10/24

LAN adresse

LAN adresse

contract rejeter

reieter (désactivé)

22 (SSH)

22 (SSH)

80 (HTTP)

WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is

tracer (désactivé

Partie défense : Consignes



- -> Une clé WPA2 « azerty12 »
- -> Un poste passerelle" (sans changement de mot de passe) avec carte wlan0 sur wifi LAN et carte eth0 sur VLAN50
- -> le nombre maximum de 2 règles bloquantes sur le FireWall sera autorisé
- -> la règle (deny any any) est interdite sur le FireWall
- -> le filtrage par adresse MAC est interdit car trop contraignant
- -> Wifi avec SSID visible

SSID Table											
Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID				
•	iPhone de Mathieu	none	ciphers aes-ccm tkip	open	wpa		✓				

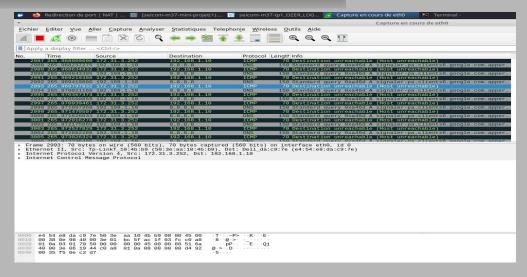
Partie attaque : Analyse



nmap sur le réseau 192.168.2.0

```
^C
local@111X-PCXX-SNIR:~$ nmap 192.168.2.0
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-23 16:34 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 3.03 seconds
local@111X-PCXX-SNIR:~$ [
```

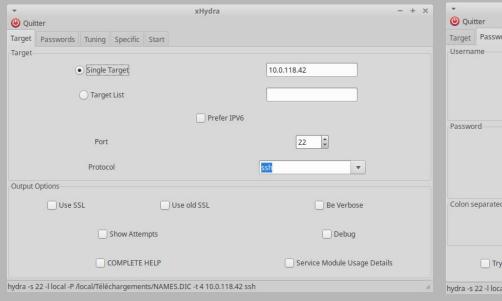
capture de trafic wireshark

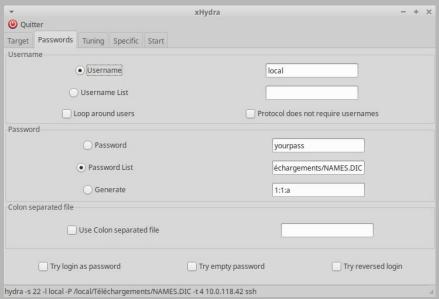


Partie attaque : Attaque du Firewall



Tentative de crack de mdp du ssh :





Partie attaque : Attaque du point d'accès wifi

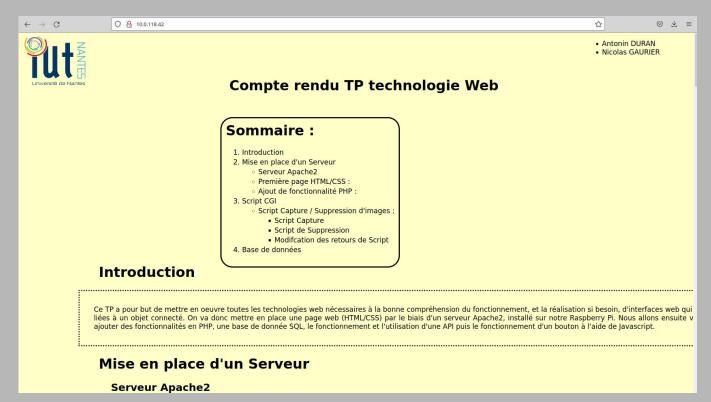


Non tenté car manque de temps

Partie attaque : Attaque du Serveur web



Redirection de notre requête http vers le serveur web:



Conclusion



Sécurité :

Changement des mots de passe des stations

Mise en place d'un VPN

Ajout de règles de filtrage (http, ssh) et redirection

-> bilan mitigé

Gestion de la communication :

La répartition pour la préparation du réseau à été facile à faire, 3 équipes de 2 pour chaque partie. On a pu discuter quand on avait un problème et ne pas non plus s'éparpiller.

Pour la partie attaque, nous nous sommes éparpillés et ne nous sommes pas concertés avant donc nous avons fait par moment la même chose donc nous avons perdu du temps.