

Présentation Module M37

Réseau et Sécurité

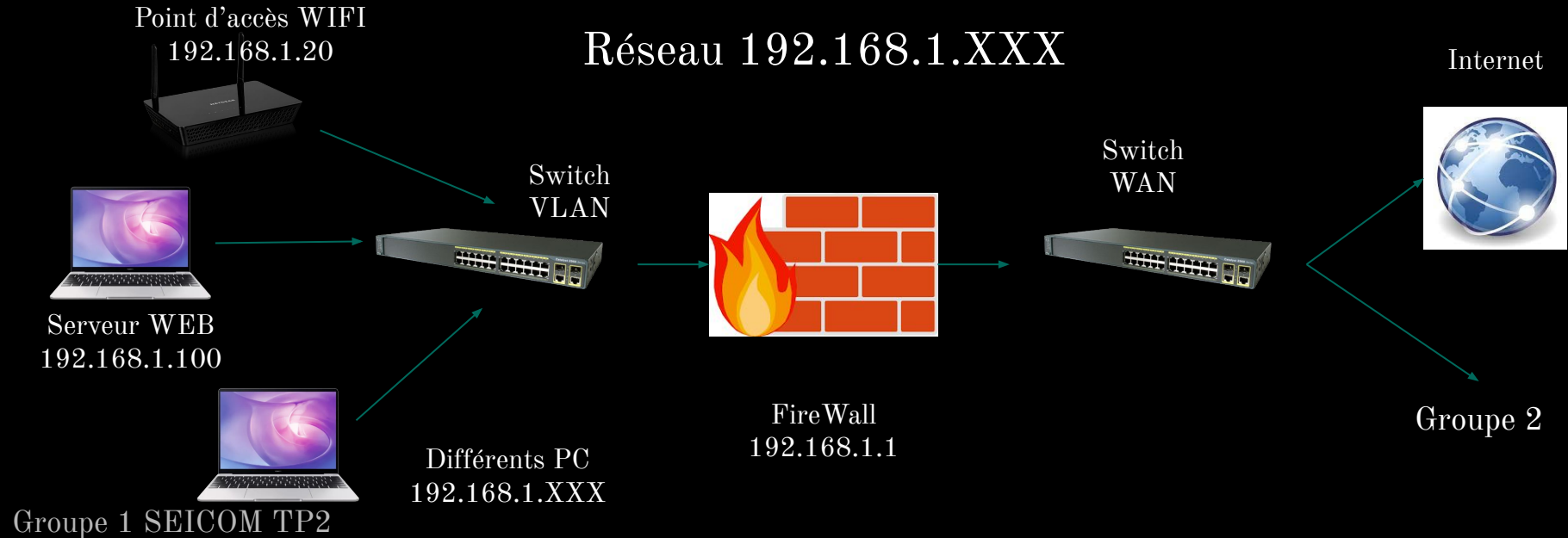


LETHIEC Gwendal
LE PELTIER Baptiste
RIVERA Jennifer
PASOS Daniela
LAURENT Simon
DOMENEC Mathis

Sommaire

- I. Description du Réseau à Réaliser
- II. Configuration des PC
- III. Configuration du routeur WIFI
- IV. Mise en place du FireWall (OpenSense)
- V. Attaques Mises en Place
- VI. Défenses Tentées

Description du Réseau à Réaliser



Configuration des PC

Changement des Adresses IP de chaque PC
=> 192.168.1.XXX



```
ifconfig  
ip address flush  
  
ip address add  
  
ifconfig  
  
ping 192.168.1.XXX
```

192.168.1.	11	Mathis
	12	Daniela/Jennifer
	13	Baptiste
	100	Serveur Web
	21	Lenovo B50-30
	1	Opensense

Groupe 1 SEICOM

Groupe 1 SEICOM

Express Security Set-Up

Express Set-Up

SSID Configuration

Host Name:

1. SSID

PaysdelaLoire.education

☒ Broadcast SSID in Beacon

MAC Address:

2. VLAN

Configuration

3. Security

IP Address:

IP Subnet Mask

Default Gateway

SNMP Community

Radio0-802.11

Role in Radio

Optimize Radio

Aironet Express

SSID Table

Delete

Hostname AP

Home: Summary Status

Association

Clients: 0

Infrastructure clients: 0

Network Identity

IP Address

192.168.1.20

MAC Address

0019.5587.bd48

Network Interfaces

Interface	MAC Address	Transmission Rate
FastEthernet	0019.5587.bd48	100Mb/s
Radio0-802.11G	0019.559e.6130	54.0Mb/s

SSID	VLAN	Encryption	Authentication	Key Management	Secure Start	Broadcast SSID
PaysdelaLoire.education	none	wep mandatory	open	none		✓

Création d'un faux AP

HackezNous



HackezMoi



PaysdelaLoire.education



—

MDP : logia
WEP : 4C6F676961

Mise en Place du FireWall

1) Reset du FireWall
=> Mode Usine

2) Entrée des adresses IPv4
LAN : 192.168.1.1
WAN : 10.0.118.41

```
LAN (re1)      -> v4: 192.168.1.1/24  
WAN (re0)      -> v4: 10.0.118.41/27
```

3) Configuration LAN et WAN

VPN: IPsec: Tunnel Settings

General information

- ☒ Disabled ☐ Disable this phase1 entry
- ☒ Connection method: default
- ☒ Key Exchange version: V2
- ☒ Internet Protocol: IPv4
- ☒ Interface: WAN
- ☒ Remote gateway: 10.0.115.11
- ☒ Dynamic gateway: ☒ Allow any remote gateway to connect
- ☒ Description: VPN Gr1

Advanced Options

- ☒ Install policy
- ☒ Disable Rekey
- ☒ Disable Reauth
- ☒ Tunnel isolation
- ☒ NAT Traversal: Enable
- ☒ Disable MOBIKE
- ☒ Dead Peer Detection

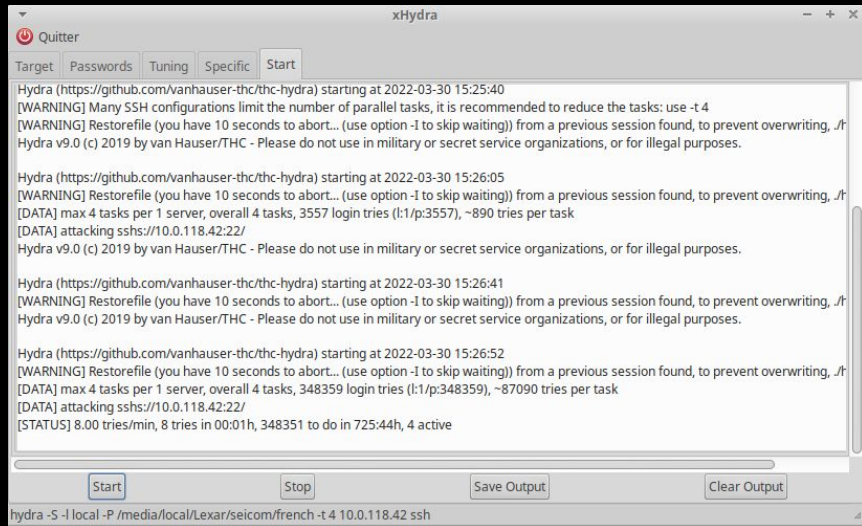
Phase 1 proposal (Authentication)

- ☒ Authentication method: Mutual PSK
- ☒ My identifier: My IP address
- ☒ Peer identifier: Peer IP address
- ☒ Pre-Shared Key: toto

Phase 1 proposal (Algorithms)

- ☒ Encryption algorithm: AES
128
- ☒ Hash algorithm: SHA256
- ☒ DH key group: 14 (2048 bits)
- ☒ Lifetime: 28800

Attaques Mises en Place



Hydra

Recherches MDP point
d'accès groupe2

Tentatives de BrutForce

mz

```
local@111X-PCXX-SNIR:~$ sudo mz -h  
[sudo] Mot de passe de local :
```

Défenses Tentées

```
local@111X-PCXX-SNIR:~$ sudo nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 10.0.119.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-30 15:56 CEST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Initiating Ping Scan at 15:56
Scanning 32 hosts [8 ports/host]
Completed Ping Scan at 15:56, 26.08s elapsed (32 total hosts)
Nmap scan report for 10.0.119.64 [host down]
Nmap scan report for 10.0.119.65 [host down]
Nmap scan report for 10.0.119.66 [host down]
Nmap scan report for 10.0.119.67 [host down]
```

Nmap

```
local@111X-PCXX-SNIR:~$ sudo dsniff -c -i eth0
dsniff: listening on eth0
```

dsniff

Merci de nous avoir écoutés

Des Questions ?

—

