

Mercredi 18 septembre 2024



Bienvenue!

SÉANCE 02: Initiation au Hacking
Réseau : Explorer et Cibler des services

Sommaire

- **Introduction (très) informelle au réseau**
- **Nmap**
- **3 services réseau**
 - **HTTP**
 - **FTP**
 - **SSH**

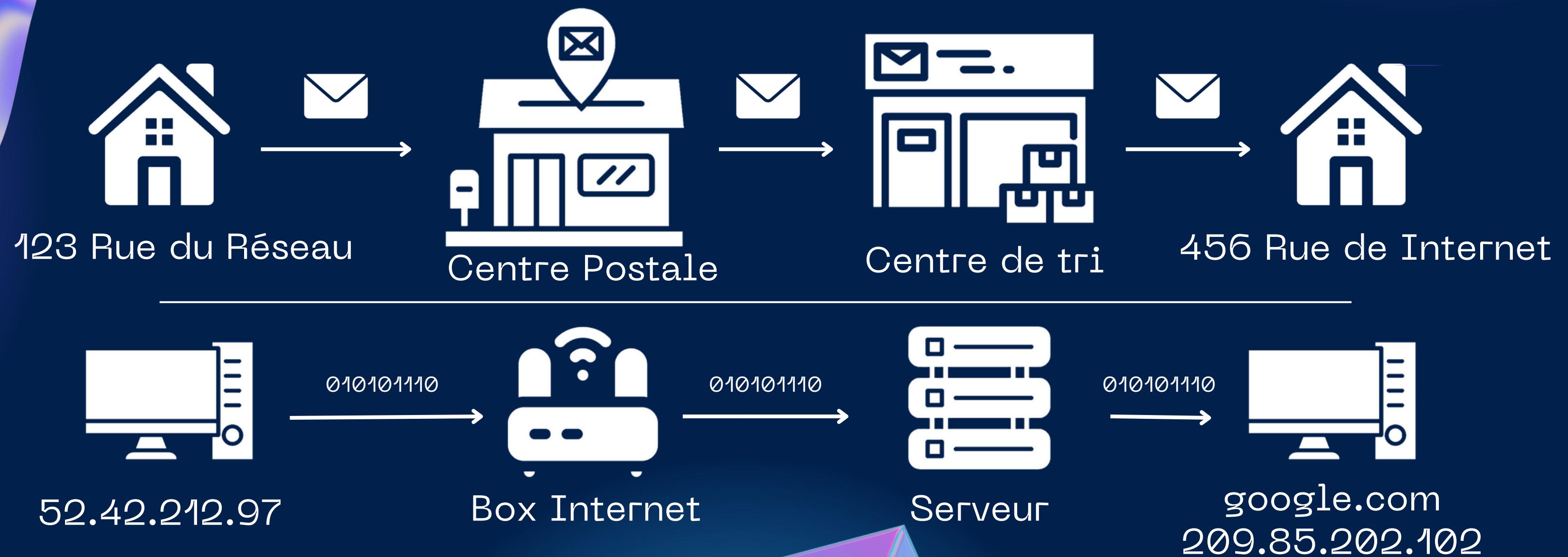
Introduction (très) informelle au réseau



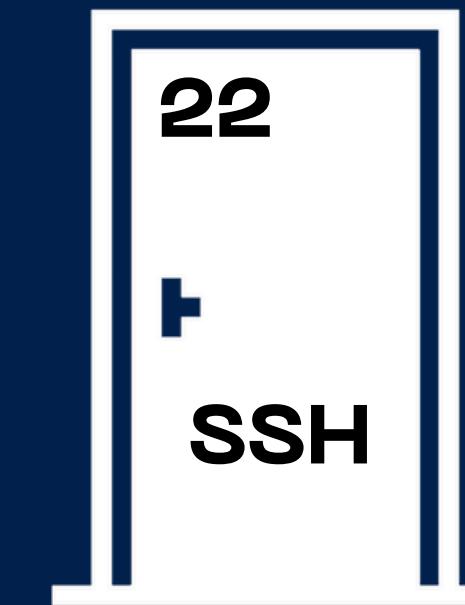
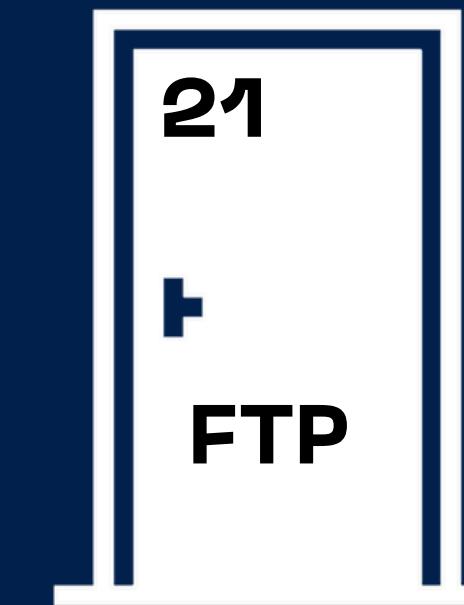
Introduction (très) informelle au réseau



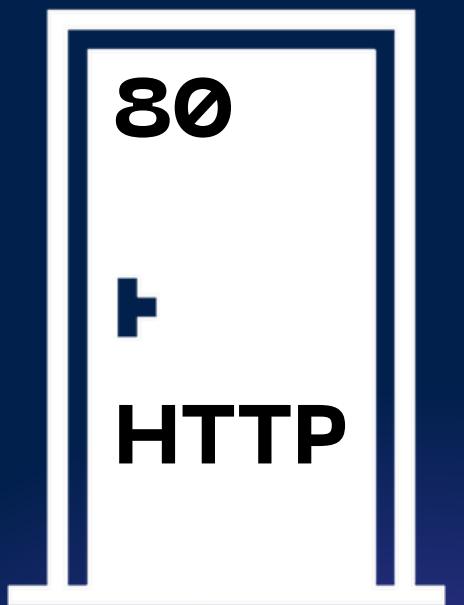
Introduction (très) informelle au réseau



Introduction (très) informelle au réseau



Ports



Nmap

Scanner de ports

Flag	Description
-sV	Tente de déterminer la version des services en cours d'exécution
-p <x> ou -p-	Recherche de port pour le port <x> ou recherche de tous les ports
-v	Retourne plus de détails
...	...

nmap <IP>

HTTP



Port 80

```
gobuster -u <IP>:<Port> -w <wordlist> dir
```

FTP (File Transfer Protocol)

Port 21



```
ftp <IP>
```

Se connecter en tant que Anonymous

SSH (Secure Shell)

Port 22



```
ssh <username>@<IP> -p <port>
```

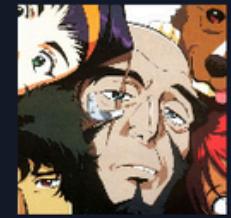
```
hydra -L <username> -p <wordlist> <IP> ssh
```

Bruteforce le nom d'utilisateur

```
hydra -l <username> -P <wordlist> <IP> ssh
```

Bruteforce le mot de passe

La room <https://tryhackme.com/r/room/cowboyhacker>



Bounty Hacker

You talked a big game about being the most elite hacker in the solar system. Prove it and claim your right to the status of Elite Bounty Hacker!

Easy 0 min

HTTP



Port 80

gobuster -u <IP>:<Port> -w <wordlist> dir

FTP (File Transfer Protocol)

Port 21

ftp <IP> Se connecter en tant que Anonymous

SSH (Secure Shell)

Port 22

ssh <username>@<IP> -p <port>

hydra -L <username> -p <wordlist> <IP> ssh Bruteforce le nom d'utilisateur

hydra -l <username> -P <wordlist> <IP> ssh Bruteforce le mot de passe



Nmap

Scanner de ports

Flag	Description
-sV	Tente de déterminer la version des services en cours d'exécution
-p <x> ou -p-	Recherche de port pour le port <x> ou recherche de tous les ports
-V	Retourne plus de détails
...	...

nmap <IP>

La room <https://tryhackme.com/r/room/cowboyhacker>



Bounty Hacker

You talked a big game about being the most elite hacker in the solar system. Prove it and claim your right to the status of Elite Bounty Hacker!

Easy 0 min

Liste des commandes administratives disponibles pour l'utilisateur.

sudo -l

Site qui recense des commandes pour obtenir des privilèges plus élevés.

<https://gtfobins.github.io/>

Merci et à la semaine prochaine !



La séance sur notre Github:
<https://github.com/CyberMines-Nancy/SEANCES>



@cyber.mines