

Les différents tests de reconnaissance effectués avec leur résultats

Tous les résultats se trouvent dans le dossier *resultats*

1. NMAP

Scan SYN discret

```
sudo nmap -sS -Pn --reason -oN nmap_tcp_syn.txt 10.0.10.2
```

Scan UDP discret des 20 ports les plus courants

```
sudo nmap -sU -Pn --top-ports 20 --reason -oN nmap_udp_top20.txt 10.0.10.2
```

Scan des versions des services et de l'OS

```
sudo nmap -sV -O -Pn -oN nmap_version_os.txt 10.0.10.2
```

Scan de tout les ports SYN discret

```
nmap -p- -sS -Pn -oN nmap_tcp_all_ports.txt 10.0.10.2
```

Scan à l'aide d'un script NSE + versions des services

```
sudo nmap -sC -sV -Pn -oN nmap_scripts.txt 10.0.10.2
```

Scan global

```
sudo nmap -A -oN nmap_all.txt 10.0.10.2
```
