CheatSheet - NMAP

Host Discovery

- Scan en couche 2 (ARP)

```
nmap -PR -sn 192.168.56.0/24
```

- Scan en couche 3 (ICMP)

```
nmap -PE -sn 192.168.56.0/24 # ICMP Echo (Test de connectivité)
nmap -PP -sn 192.168.56.0/24 # ICMP Timestamps (Synchronisation d'horloge des routeurs)
nmap -PM -sn 192.168.56.0/24 # ICMP Mask Query (Découverte du masque du subnet local)
```

- Scan en couche 4 (TCP/UDP)

```
nmap -PS80,443 -sn 192.168.56.0/24 # Simple TCP SYN (Sur les ports 80 (défaut) et 443)
nmap -PA80 -sn 192.168.56.0/24 # Simple TCP ACK (Sur le port 80 (défaut))
nmap -PU -sn 192.168.56.0/24 # Simple UDP Datagram (Expecting ICMP Reponse)
```

Port Scanning

- Récupération des ports ouverts

```
nmap -p- 192.168.56.95 # Simple TCP scan (All ports)
nmap -F 192.168.56.95 # Scan rapide (limité aux ports bien connus
nmap -p- -r 192.168.56.95 # Simple TCP scan (scan des ports dans l'ordre)
nmap -p80 192.168.56.95 # Simple TCP scan (port spécifique)
```

- Récupération des versions des services

```
nmap -p- -sV 192.168.56.95 # Simple TCP scan avec recherche de bannières
```

Vulnerability Scanning

- Scan de vulnérabilité

```
nmap -sV -p21 -script vuln 192.168.56.95 # Scan de vulnérabilité sur le port 21
```