Rapport d'exercice : Scan Nmap du réseau local

1.Introduction

L'objectif de cet exercice est de comprendre la topologie de mon réseau local et d'identifier les appareils et services actifs à l'aide de **Nmap**, un outil de scan réseau. Cela permet de se familiariser avec les concepts de ports TCP/UDP, services réseau et détection de systèmes.

2.Méthodologie

1. **Identification de mon IP et du réseau :**

   ```
   ipconfig
   ```

   - IP de mon PC : `192.168.1.195`
   - Masque de sous-réseau : `255.255.255.0` → réseau `192.168.1.0/24`
   - Passerelle : `192.168.1.254` (routeur Freebox)

---

2. **Scan des appareils actifs sur le réseau :**

   ```
   nmap -sn 192.168.1.195/24

   # Permet de détecter tous les hôtes actifs sur le réseau.
   ```

   Résultat : 7 appareils détectés :

IP	MAC Address	Fabricant / info
192.168.1.68	7E:E9:38:AD:0F:05	Inconnu
192.168.1.80	DC:00:B0:52:FA:46	Freebox SAS
192.168.1.96	1A:BD:F3:68:27:AB	Inconnu (mon téléphone)
192.168.1.148	E8:FD:F8:F9:B3:08	Shanghai High-Flying Electronics Technology
192.168.1.165	48:9E:BD:C4:35:A3	HP (mon imprimante)
192.168.1.254	70:FC:8F:69:F8:C8	Freebox SAS (routeur)
192.168.1.195	-	Mon PC

   Résumé : Tous ces appareils répondent aux pings → actifs sur le réseau.

---

3. **Scan des ports et services pour chaque appareil :**

   ```
   nmap -sV [IP]

   # -sV permet de détecter les ports ouverts et d'identifier les services qui y sont
   # associés.

   # Exemple pour scanner les ports et services de mon ordinateurs :
   # nmpa -sV 192.168.1.195
   ```

3.Résultats

Tableau résumé du scan Nmap de mon : PC, Téléphone et Routeur

Appareil	IP	MAC Address	Port	État	Service	Version/Info / Remarques
PC Windows	192.168.1.195	-	135	open	msrpc	Microsoft Windows RPC
			139	open	netbios-ssn	Microsoft Windows netbios-ssn
			445	open	microsoft-ds?	Partage fichiers Windows ?
			5357	open	http	Microsoft HTTPAPI httpd 2.0 (UPnP/SSDP)
			5500	open	hotline?	Service inconnu par Nmap
Téléphone	192.168.1.96	1A:BD:F3:68:27:AB	49152	open	tcpwrapped	Service non identifié, protégé
			62078	open	tcpwrapped	Service non identifié, protégé
Routeur Freebox	192.168.1.254	70:FC:8F:69:F8:C8	53	open	domain	dnsmasq 2.91
			80	open	http	nginx
			443	open	ssl/http	nginx
			445	open	microsoft-ds	SMB, partage de fichiers
			554	open	rtsp	Freebox rtspd 1.2
			5357	open	http	nginx
			5678	open	upnp	fbxigdd 1.1 (AliceBox PM203 UPnP)
			8090	open	http	nginx
			9091	open	http	nginx

3.2 Observations

- **PC Windows** : plusieurs ports ouverts pour le partage Windows et UPnP.
- **Téléphone** : ports protégés (`tcpwrapped`), probablement pour AirPlay ou gestion à distance.
- **Routeur Freebox** : expose des services web et UPnP, ainsi que SMB et RTSP.

Points de sécurité :

- SMB ouvert sur PC et routeur → risque si mal configuré.
- UPnP sur le routeur → peut exposer des services internes du réseau.
- HTTP/HTTPS sur routeur → interface admin accessible sur le réseau.

4.Conclusion

Cet exercice permet de visualiser les appareils connectés à un réseau domestique et de comprendre comment les services exposés peuvent être identifiés avec Nmap.

- Le scan réseau (`sn`) permet de recenser les hôtes actifs.
- Le scan de version (`sV`) fournit des informations sur les ports ouverts et services.
- Identifier les ports sensibles (SMB, UPnP, HTTP) est essentiel pour la sécurité réseau.

Apprentissage clé : même un réseau domestique contient plusieurs services exposés qu'il est important de connaître pour sécuriser ses appareils.