

TP n° 2 : Ethical Hacking

HAFDAOUI HAMZA & AMGAROU SALMA

Objectives:

Le but de ce TP est d'explorer des techniques avancées de scan réseau en maîtrisant les scans Nmap, y compris différentes techniques telles que le moteur de scripts NSE, l'automatisation, les techniques d'évasion des pare-feu/IDS et la fragmentation des paquets. Afin de bien comprendre le fonctionnement des processus de scan pour chaque attaque, vous capturerez et analyserez le trafic à l'aide de Wireshark

Plan du TP :

- Partie 1 : Introduction à Nmap
- Partie 2 : Maîtrise de Nmap
- Partie 3 : Identification des systèmes d'exploitation (OS Fingerprinting)
- Partie 4 : Évasion des pare-feu et IDS/IPS

Rapport pour la Partie 1 : Introduction à Nmap

Objectifs

- Découvrir les hôtes actifs sur le réseau.
- Capturer et analyser le trafic réseau généré lors des scans à l'aide de Wireshark.

Étape 1 : Configuration du réseau

1. Commandes utilisées :

- La commande `ip addr show` montre les interfaces réseau actives sur la machine Kali Linux :
- L'adresse IP active de la machine est `192.168.122.210`.
- L'interface active est `eth0`.

1. Observation :

- La machine Kali Linux est connectée au réseau `192.168.122.0/24`.

```
kali@kali: ~  
with nghttp2 1.64.0, with nghttp3 0.8.0, with brotli 1.1.0, with LZ4 1.9.4, with  
Zstandard 1.5.6, with libsmi 0.4.8, with LC_TYPE=C.UTF-8, binary plugins  
supported.  
  
(kali@kali)-[~]  
$ ip addr show  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 52:54:00:1a:de:21 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.122.210/24 brd 192.168.122.255 scope global dynamic noprefixroute eth0  
        valid_lft 3258sec preferred_lft 3258sec  
    inet6 fe80::5054:ff:fe1a:de21/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
2	2.048213316	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
3	4.032304143	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
4	6.017144017	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
5	8.000235544	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
6	10.048264471	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
7	12.032118273	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
8	14.016273018	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =

Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface eth0	0000	01 80 c2 00 00 00 fe 54 00 1a de 21 00
IEEE 802.3 Ethernet	0010	03 00 00 00 00 00 80 00 52 54 00 98 40
Logical-Link Control	0020	00 00 80 00 52 54 00 98 40 e6 80 01 00
Spanning Tree Protocol	0030	02 00 02 00

Étape 2 : Scan ping (-sP) avec Nmap

1. Commandes utilisées :

- `nmap -sP 192.168.122.200-211`
- Objectif : Identifier les hôtes actifs dans la plage IP donnée.

1. Résultat du scan :

- Nmap détecte un seul hôte actif avec l'adresse IP 192.168.122.210.

- 1. Analyse dans Wireshark :
 - Les paquets capturés incluent :
 - STP (Spanning Tree Protocol) : Ce protocole est vu, mais non pertinent pour le scan.
 - ARP (Address Resolution Protocol) : Des requêtes "Who has" (qui correspond à une adresse IP donnée ?) sont envoyées sur le réseau.
- 1. Filtrage Wireshark :
 - Les requêtes ARP montrent que la machine scanne activement pour découvrir les adresses IP actives.

```
(kali@kali)-[~]
$ nmap -sP 192.168.122.200-211
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-26 11:32 EST
Nmap scan report for kali (192.168.122.210)
Host is up.
Nmap done: 12 IP addresses (1 host up) scanned in 1.67 seconds
```

Étape 3 : Observations des protocoles capturés

- 1. DNS (Domain Name System) :
 - Le scan Nmap effectue également une résolution DNS pour identifier les noms associés aux adresses IP scannées.
- 1. ARP (Address Resolution Protocol) :
 - Le scan utilise ARP pour vérifier quels dispositifs répondent sur les adresses IP scannées.
- 1. ICMP (Internet Control Message Protocol) :
 - Le trafic ICMP est visible lorsque Nmap envoie des pings aux hôtes de la plage IP.

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
44	58.352264925	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.203? Te
45	58.352265773	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.204? Te
46	58.352266613	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.205? Te
47	58.352267609	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.206? Te
48	58.352268533	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.207? Te
49	58.352269318	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.208? Te
50	58.352270257	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.209? Te
51	58.352271090	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.211? Te
52	58.552565277	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.200? Te
53	58.786953216	192.168.122.210	192.168.122.1	DNS	88	Standard query 0xf168 PTR 2
54	58.787136894	192.168.122.1	192.168.122.210	DNS	106	Standard query response 0xf
55	60.033928377	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root = 32768/0/52:54:
56	62.017900089	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root = 32768/0/52:54:
57	63.910761852	52:54:00:1a:de:21	52:54:00:98:40:e6	ARP	42	Who has 192.168.122.1? Tell
58	63.910847850	52:54:00:98:40:e6	52:54:00:1a:de:21	ARP	42	192.168.122.1 is at 52:54:0
59	64.000981047	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root = 32768/0/52:54:
60	64.257171641	52:54:00:98:40:e6	52:54:00:1a:de:21	ARP	42	Who has 192.168.122.210? Te
61	64.257192434	52:54:00:1a:de:21	52:54:00:98:40:e6	ARP	42	192.168.122.210 is at 52:54
62	66.048991276	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root = 32768/0/52:54:
63	68.033277138	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root = 32768/0/52:54:
64	70.018259250	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root = 32768/0/52:54:

Frame 1: 52 bytes on wire (416 bits), 52 bytes capture

IEEE 802.3 Ethernet

Logical-Link Control

Spanning Tree Protocol

0000 01 80 c2 00 00 00 fe 54 00 1a de 21 00 26

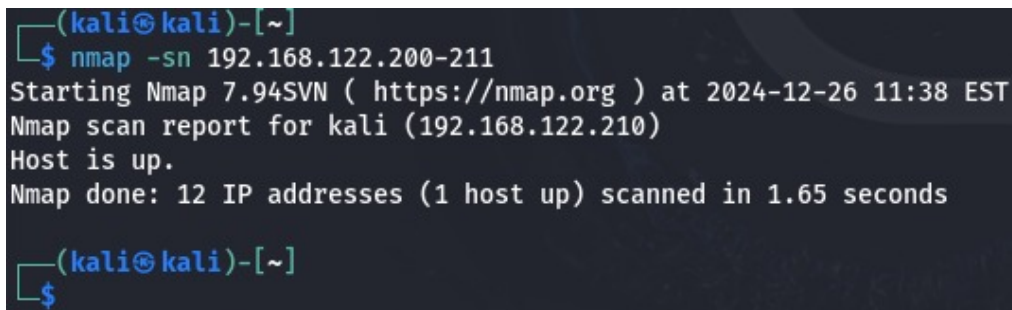
0010 03 00 00 00 00 00 80 00 52 54 00 98 40 e6

0020 00 00 80 00 52 54 00 98 40 e6 80 01 00 00

0030 02 00 02 00

Résumé des observations

- **Machine scannée :**
- Kali Linux avec l'adresse IP 192.168.122.210.
- **Hôte détecté :**
- Le scan ping détecte uniquement la machine active (elle-même) sur cette plage IP.
- **Protocoles analysés :**
- **ARP :** Utilisé pour découvrir les hôtes actifs.
- **ICMP :** Envoyé comme ping aux adresses IP.
- **DNS :** Résolution des noms d'hôte.



```
(kali㉿kali)-[~]  
$ nmap -sn 192.168.122.200-211  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-26 11:38 EST  
Nmap scan report for kali (192.168.122.210)  
Host is up.  
Nmap done: 12 IP addresses (1 host up) scanned in 1.65 seconds  
  
(kali㉿kali)-[~]  
$
```

Étape 4 : Scan Nmap avec -sn sur une plage d'IP

1. **Commandes utilisées :**
 - `nmap -sn 192.168.122.200-211`
 - Objectif : Effectuer un scan sans port pour détecter les hôtes actifs.
1. **Résultat :**
 - Nmap identifie qu'un seul hôte est actif sur cette plage : 192.168.122.210.
1. **Analyse Wireshark :**
 - **Protocole ARP :**
 - De nombreuses requêtes ARP "Who has" ont été envoyées dans la plage IP spécifiée.
 - Chaque requête ARP cherche à savoir quelle machine possède une adresse IP spécifique.
 - Les réponses ARP montrent que seule l'adresse 192.168.122.210 a répondu.
 - **Protocole ICMPv6 :**
 - On observe des paquets "Router Solicitation" (ICMPv6) envoyés à une adresse de diffusion spécifique (ff02::2). Ces paquets sont utilisés par IPv6 pour découvrir des routeurs.
1. **Interprétation :**
 - Nmap utilise principalement ARP pour détecter les hôtes actifs, mais ICMPv6 peut apparaître en fonction de la configuration réseau.

Le scan sans port (-sn) permet uniquement d'identifier les hôtes répondant aux requêtes ARP ou ICMP.

170	226.052164249	fe:54:00:1a:de:21	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/52:54:00:98:4
171	227.875985159	fe80::5054:ff:fe1a:...	ff02::2	ICMPv6	62	Router Solicitation
172	228.036051795	fe:54:00:1a:de:21	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/52:54:00:98:4
173	230.021259618	fe:54:00:1a:de:21	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/52:54:00:98:4
174	232.004135547	fe:54:00:1a:de:21	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/52:54:00:98:4
175	234.052257422	fe:54:00:1a:de:21	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/52:54:00:98:4
176	236.036361751	fe:54:00:1a:de:21	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/52:54:00:98:4
177	238.020272182	fe:54:00:1a:de:21	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/52:54:00:98:4
178	240.004465402	fe:54:00:1a:de:21	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/52:54:00:98:4
179	242.052484252	fe:54:00:1a:de:21	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/52:54:00:98:4

Observation des paquets STP (Spanning Tree Protocol)

- Le protocole STP (Spanning Tree Protocol) est visible dans les captures réseau.
- Utilité :**
- STP est utilisé pour prévenir les boucles réseau dans les environnements commutés.
- Pertinence pour le scan :**
- Les paquets STP ne sont pas générés par Nmap mais sont capturés parce qu'ils sont présents sur le réseau.

No.	Time	Source	Destination	Protocol	Length	Info
30	57.151095011	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.201? Tell 192
31	57.151111659	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.202? Tell 192
32	57.151112894	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.203? Tell 192
33	57.151114176	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.204? Tell 192
34	57.151115462	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.205? Tell 192
35	57.151116412	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.206? Tell 192
36	57.151118081	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.207? Tell 192
37	57.151119097	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.208? Tell 192
38	57.151120051	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.209? Tell 192
39	57.151121007	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.211? Tell 192
40	57.351396821	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.200? Tell 192
42	58.352250282	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.201? Tell 192
43	58.352263934	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.202? Tell 192
44	58.352264925	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.203? Tell 192
45	58.352265773	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.204? Tell 192
46	58.352266613	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.205? Tell 192
47	58.352267609	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.206? Tell 192
48	58.352268533	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.207? Tell 192
49	58.352269318	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.208? Tell 192
50	58.352270257	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.209? Tell 192
51	58.352271090	52:54:00:1a:de:21	Broadcast	ARP	42	Who has 192.168.122.211? Tell 192

Frame 30: 42 bytes on wire (336 bits), 42 bytes captured on interface 0		0000 ff ff ff ff ff ff 52 54 00 1a de 21 08 06 00 01	
Ethernet II, Src: 52:54:00:1a:de:21 (52:54:00:1a:de:21), Dst: 01:00:00:00:00:00		0010 08 00 06 04 00 01 52 54 00 1a de 21 c0 a8 7a d2	
Address Resolution Protocol (request)		0020 00 00 00 00 00 00 c0 a8 7a c9	

Résumé des captures ARP

- Requêtes ARP :**
 - Les requêtes sont visibles dans Wireshark, identifiées par le champ "Who has".
 - Exemple : Who has 192.168.122.201? Tell 192.168.122.210.
- Résultats des réponses ARP :**
 - Les machines ne répondent pas, sauf pour l'adresse IP active détectée.

Résumé Global des Résultats

- Commandes utilisées :**
- nmap -sP et nmap -sn ont été exécutés pour détecter les hôtes sur des plages IP spécifiques.
- Protocoles observés :**
- ARP :** Requis pour découvrir les hôtes sur le réseau local.

- **ICMPv6** : Visible dans le trafic réseau en raison de la configuration réseau.
- **STP** : Capturé mais sans rapport direct avec le scan.
- **Analyse des résultats dans Wireshark** :
- Les paquets ARP montrent une communication réseau réussie entre le scanner et les hôtes.

Rapport pour la Partie 2:

Test 1 : Découverte des Hôtes sur le Réseau

Objectif

- Effectuer un scan pour découvrir les hôtes actifs sur le réseau en utilisant un **scan ping** avec Nmap.

Capturer et analyser le trafic réseau généré pendant le scan avec Wireshark.

Commandes Exécutées

1. Nmap Scan :

- `nmap -sn 192.168.122.210`
- Objectif : Identifier si l'hôte avec l'adresse IP 192.168.122.210 est actif.

The screenshot displays two windows. The top window is Wireshark, showing a list of captured packets. The bottom window is a terminal showing the execution of an Nmap scan.

No.	Time	Source	Destination	Protocol	Length	Info
342	535.998125356	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
343	538.046085434	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
344	540.030300720	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
345	540.887634753	192.168.122.210	192.168.122.1	DNS	88	Standard quer
346	540.887854305	192.168.122.1	192.168.122.210	DNS	106	Standard quer
347	542.014032702	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
348	543.999070218	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
349	545.958907798	52:54:00:1a:de:21	52:54:00:98:40:e6	ARP	42	Who has 192.1
350	545.959197517	52:54:00:98:40:e6	52:54:00:1a:de:21	ARP	42	192.168.122.1
351	546.046099784	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =
352	548.029945110	fe:54:00:1a:de:21	Spanning-tree-(for-...	STP	52	Conf. Root =

The terminal window shows the following output:

```

wireshark_eth0LIHEZ2.pcapng
Packets: 369 · Displayed: 369 (100.0%) Profile: Default
$ nmap -sn 192.168.122.210
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-26 11:45 EST
Nmap scan report for kali (192.168.122.210)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
(kali@kali)-[~]
$

```

Résultats Nmap

- **Sortie :**
- Un seul hôte est détecté : 192.168.122.210.
- Le scan confirme que cet hôte est actif sur le réseau.

Analyse Wireshark

1. **Protocoles Capturés :**
 - **ARP :**
 - Plusieurs requêtes ARP "Who has" ont été envoyées pour résoudre les adresses IP en adresses MAC.
 - Exemple :
who has 192.168.122.210? Tell 192.168.122.1
 - **STP (Spanning Tree Protocol) :**
 - Capturé, mais non pertinent pour le test (protocole réseau de gestion des boucles dans les réseaux commutés).
 - **DNS :**
 - Le scan Nmap inclut des requêtes DNS pour résoudre les noms d'hôte associés aux adresses IP.
1. **Paquets ARP :**
 - Les réponses ARP confirment que l'adresse IP cible 192.168.122.210 est associée à une machine active sur le réseau.
1. **Capture ICMP (non visible dans cette capture mais possible) :**
 - Si configuré, le scan ping pourrait inclure des requêtes ICMP "Echo Request".

Interprétation

1. **Protocole Principal Utilisé :**
 - Pour la détection des hôtes, Nmap utilise principalement **ARP** dans les réseaux locaux.
 - Les paquets ARP montrent que le scanner Nmap interroge directement les adresses IP dans le sous-réseau.
1. **Hôte Actif Détecté :**
 - L'adresse IP 192.168.122.210 a répondu aux requêtes, confirmant qu'un hôte est actif à cette adresse.
1. **Analyse DNS :**
 - Les résolutions DNS sont visibles, ce qui montre que Nmap tente de résoudre les noms associés aux IP scannées.

Test 2 : Scan TCP SYN

Objectif

1. Effectuer un scan TCP SYN sur une machine cible pour détecter les ports ouverts et fermés.
2. Analyser le trafic réseau généré à l'aide de Wireshark.

Étapes Réalisées

Configuration de l'environnement

1. **Commande utilisée pour ouvrir les ports avec netcat :**

```
nc -l -p 21 & nc -l -p 53 & nc -l -p 110 & nc -l -p 25
```

```
[1] + done      wireshark
(kali@kali)-[~]
$ nc -l -p 21 & nc -l -p 53 & nc -l -p 110 & nc -l -p 25
[1] 6314
[2] 6315
[3] 6316
```

- Cette commande configure la machine cible pour écouter sur les ports suivants : 21, 53, 110, et 25.
- Ces ports simulent des services réseau comme FTP (21), DNS (53), POP3 (110), et SMTP (25).