

Atelier 3 : Scanner avec nmap

Pour cet atelier, nous allons scanner la VM Metasploitable2 en utilisant **nmap**.

Partie 1 – Configuration

□ Quelle est l'adresse IP de votre VM Kali Linux ? Quelle est l'adresse IP de votre VM Metasploitable2 ?

l'adresse IP de ma machine Metasploitable est : 10.0.2.4

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c1:09:a0
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
```

L'adresse IP de ma machine Kali est : 10.0.2.15

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
      inet6 fe80::a00:27ff:fe86:288e  prefixlen 64  scopeid 0x20<link>
```

□ Quelle version de nmap avez-vous installée dans Kali (réponse sous la forme : x.xx) ?

La version de nmap installée sur ma machine Kali est : la version 7.94

```
(aissatou@kali)-[~]
$ nmap --version
Nmap version 7.94SVN ( https://nmap.org )
```

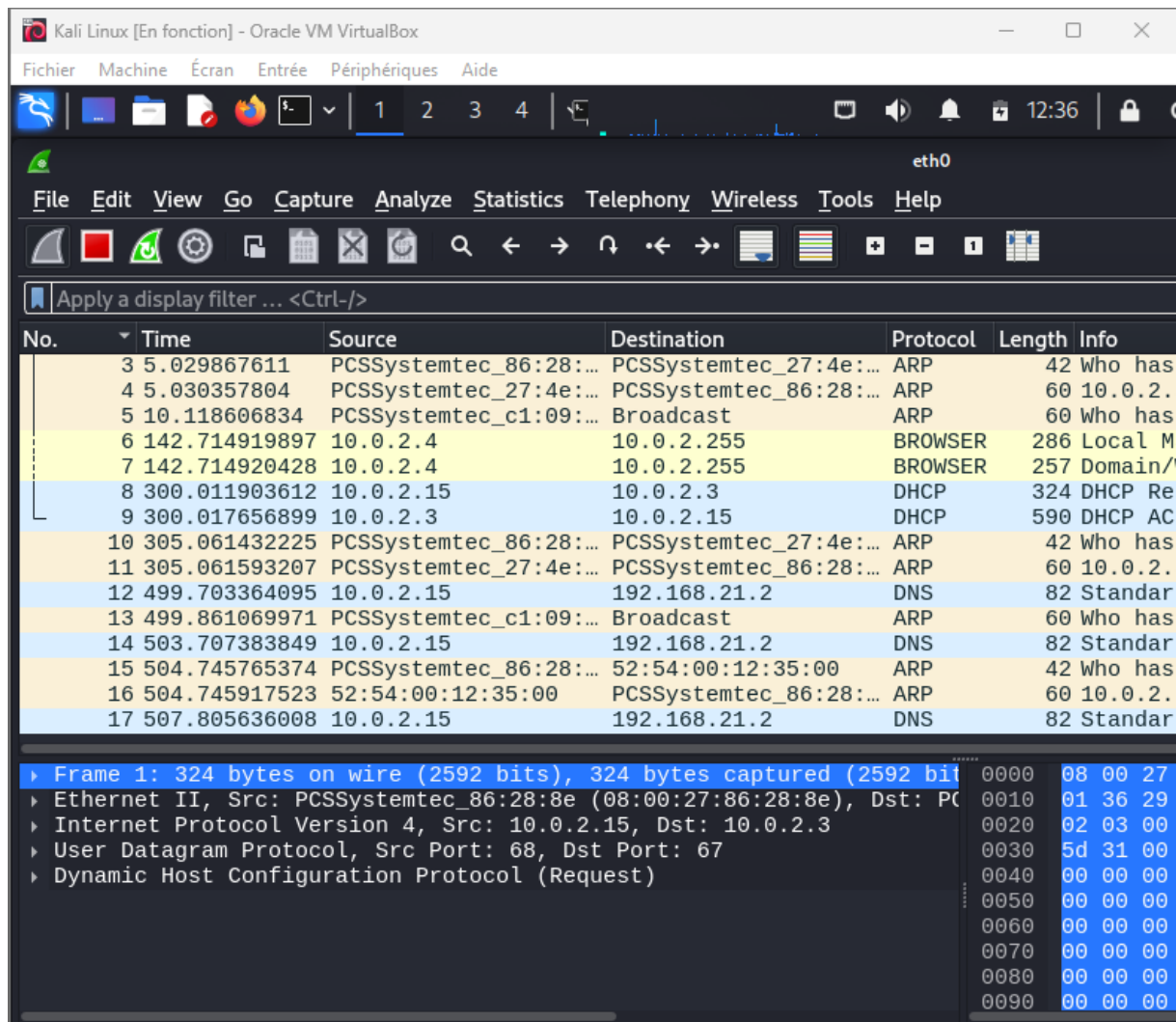
Voici la commande permettant de scanner l'@IP de la machine Kali : `sudo nmap -sn 10.0.2.15`

```
$ sudo nmap -sn 10.0.2.15
[sudo] password for aissatou:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 11:59 GMT
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds

(aissatou@kali)-[~]
```

Partie 2 - Découverte des hôtes

Quelles sont les méthodes utilisées par nmap pour effectuer la découverte des hôtes lorsqu'il est exécuté en tant qu'utilisateur root (c'est-à-dire via `sudo`) ?



les methodes utilisees par nmap pour effectuer la decouverte des hotes sont :

1. Scan ARP : Nmap peut envoyer des requêtes ARP sur le réseau local pour découvrir les hôtes actifs. Cela fonctionne en interrogeant les adresses MAC pour trouver les périphériques actifs.
2. Scan ICMP Echo : Nmap peut envoyer des requêtes ICMP Echo (ping) aux adresses IP pour déterminer si un hôte est actif. Cela fonctionne en écoutant les réponses ICMP des hôtes.
3. Scan TCP SYN : Nmap peut également effectuer un scan TCP SYN en envoyant des paquets SYN aux ports bien connus des hôtes pour déterminer s'ils sont ouverts. Cela peut aider à identifier les hôtes actifs et les services en cours d'exécution.
4. Scan TCP ACK : Nmap peut envoyer des paquets TCP ACK pour détecter les pare-feu et les filtres réseau. Cela peut aider à comprendre la topologie du réseau et à identifier les hôtes actifs.

Dans notre cas, la methode utilisee par Nmap est ARP.

Ensuite, ciblez l'adresse IP **8.8.8.8**, qui correspond au serveur DNS public de Google (une fonction connue sous le nom de « IP Anycast »). Comme précédemment, faites simplement un scan de découverte d'hôte avec nmap sans scan de port.

Livrables :

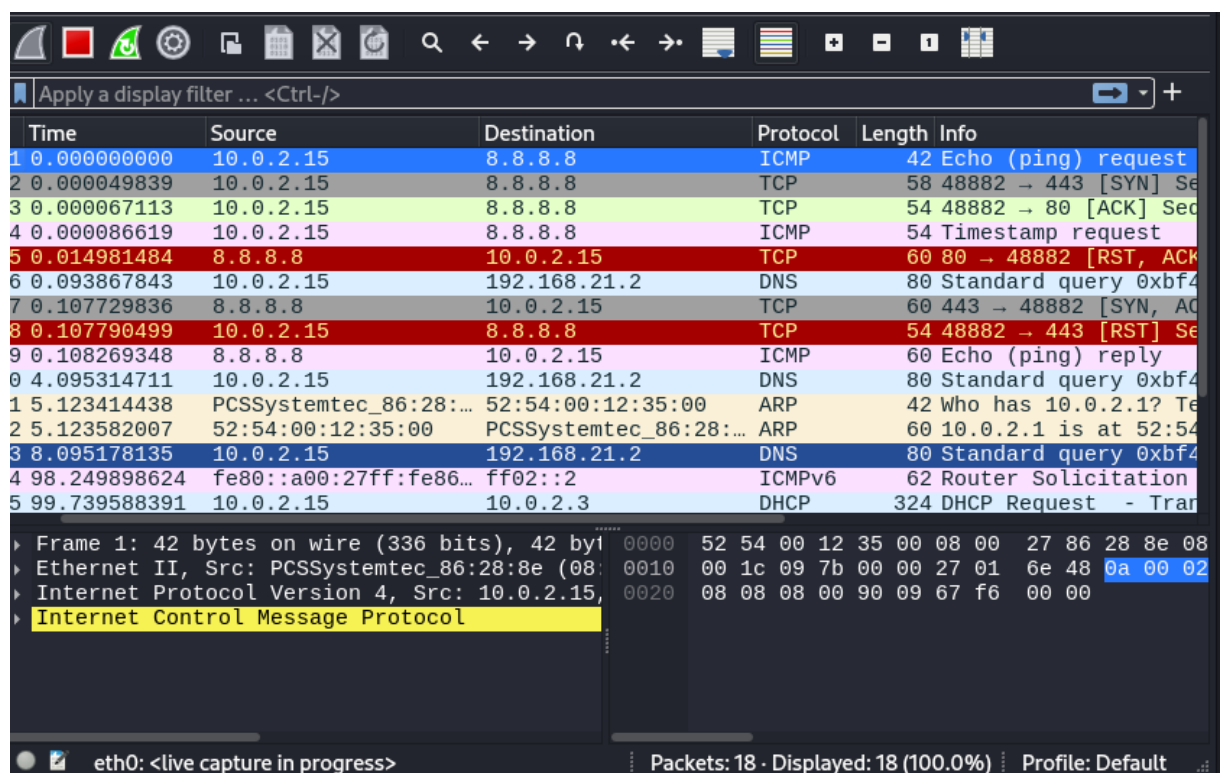
- Quelle commande avez-vous saisie pour exécuter le scan en tant qu'utilisateur root ?

la commande utilisée pour exécuter le scan en tant que user est : **sudo nmap -sn 8.8.8.8**

```
(aissatou@kali)-[~]
$ sudo nmap -sn 8.8.8.8
[sudo] password for aissatou:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 12:45 GMT
Nmap scan report for 8.8.8.8
Host is up (0.11s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

(aissatou@kali)-[~]
$
```

- Quelles méthodes nmap utilise-t-il pour effectuer la découverte des hôtes lorsqu'il est exécuté en tant qu'utilisateur root ?



The image shows a Wireshark network capture of traffic from 10.0.2.15 to 8.8.8.8. The packet list table is as follows:

Time	Source	Destination	Protocol	Length	Info
1 0.000000000	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request
2 0.000049839	10.0.2.15	8.8.8.8	TCP	58	48882 → 443 [SYN] Seq
3 0.000067113	10.0.2.15	8.8.8.8	TCP	54	48882 → 80 [ACK] Seq
4 0.000086619	10.0.2.15	8.8.8.8	ICMP	54	Timestamp request
5 0.014981484	8.8.8.8	10.0.2.15	TCP	60	80 → 48882 [RST, ACK
6 0.093867843	10.0.2.15	192.168.21.2	DNS	80	Standard query 0xbf4
7 0.107729836	8.8.8.8	10.0.2.15	TCP	60	443 → 48882 [SYN, AC
8 0.107790499	10.0.2.15	8.8.8.8	TCP	54	48882 → 443 [RST] Se
9 0.108269348	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply
0 4.095314711	10.0.2.15	192.168.21.2	DNS	80	Standard query 0xbf4
1 5.123414438	PCSSystemtec_86:28:...	52:54:00:12:35:00	ARP	42	Who has 10.0.2.1? Te
2 5.123582007	52:54:00:12:35:00	PCSSystemtec_86:28:...	ARP	60	10.0.2.1 is at 52:54
3 8.095178135	10.0.2.15	192.168.21.2	DNS	80	Standard query 0xbf4
4 98.249898624	fe80::a00:27ff:fe86...	ff02::2	ICMPv6	62	Router Solicitation
5 99.739588391	10.0.2.15	10.0.2.3	DHCP	324	DHCP Request - Tran

The packet details pane for the first packet (Frame 1) shows:

- Ethernet II, Src: PCSSystemtec_86:28:8e (08:00:00:08:00:10), Dst: 08:00:00:08:00:08
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
- Internet Control Message Protocol

The status bar at the bottom indicates: eth0: <live capture in progress> | Packets: 18 · Displayed: 18 (100.0%) | Profile: Default

Les methodes utilisees sont :scan ICMP, scan TCP et scan ARP

- Quel est le nom de l'hôte qui répond à la requête DNS inverse envoyée par nmap pour **8.8.8.8.in-addr.arpa** ? Vous pouvez obtenir cette information à partir de la trace Wireshark que vous venez d'obtenir.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.21.2	DNS	80	Standard query 0x69c6 PTR 8.8.8.8.in-addr.arpa
2	4.276393639	10.0.2.15	192.168.21.2	DNS	80	Standard query 0x69c7 PTR 8.8.8.8.in-addr.arpa
3	8.287040392	10.0.2.15	192.168.21.2	DNS	80	Standard query 0x69c8 PTR 8.8.8.8.in-addr.arpa

Le nom de l'hôte est : 10.0.2.15

- Dans un court paragraphe, expliquez quelles réponses sont reçues suite à la découverte de l'hôte par nmap. Formulez votre réponse dans le format suivant : nmap a envoyé <message de demande>, et quelques paquets plus tard, l'hôte cible a envoyé <message de réponse>.

nmap a envoyé une requête demandant de faire un scan de l'hôte spécifié, et quelques paquets plus tard, l'hôte cible a envoyé l'ensemble des informations en rapport avec lui à savoir le temps pris pour faire le scan, spécification de la source c'est-à-dire de l'hôte, de la destination, le protocole utilisé par nmap la taille, et la méthode nmap.

Partie 3 – Scan des ports TCP

Livrables :

- Quels sont les ports et services spécifiques que nmap trouve ouverts ?

```

21/tcp    open    ftp
22/tcp    open    ssh
23/tcp    open    telnet
25/tcp    open    smtp
53/tcp    open    domain
80/tcp    open    http
111/tcp   open    rpcbind
139/tcp   open    netbios-ssn
445/tcp   open    microsoft-ds
512/tcp   open    exec
513/tcp   open    login
514/tcp   open    shell
1524/tcp  open    ingreslock
2049/tcp  open    nfs
2121/tcp  open    ccproxy-ftp
3306/tcp  open    mysql
3632/tcp  open    distccd
5432/tcp  open    postgres
5900/tcp  open    vnc
6000/tcp  open    X11
6667/tcp  open    irc
8009/tcp  open    ajp13

Nmap done: 1 IP address (1 host up) scanned in 13.120 seconds
msfadmin@metasploitable:~$ _

```

- Combien de ports sont ouverts selon nmap ?

22 ports sont ouverts.

- Combien de ports sont fermés selon nmap ?

Aucun port n'est fermé sur cette liste.

Partie 4 – Scan des ports UDP

□ Quelle commande avez-vous entrée pour faire un scan plus rapide des ports UDP et pour activer également le scan des services et des versions ?

En ajoutant l'argument « -sV » a la commande " sudo nmap -sU @IP" cela nous permettra d'activer le scan de service et de version

```
msfadmin@metasploitable:~$ sudo nmap -sU -sV 10.0.2.4
Starting Nmap 4.53 ( http://insecure.org ) at 2024-04-28 10:38 EDT
Interesting ports on 10.0.2.4:
Not shown: 1480 closed ports
PORT      STATE      SERVICE      VERSION
53/udp    open       domain       ISC BIND (Fake version: 9.4.2)
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open       rpcbind      2 (rpc #100000)
137/udp   open       netbios-ns   Microsoft Windows XP netbios-ssn
138/udp   open|filtered netbios-dgm
864/udp   open|filtered unknown
2049/udp  open       nfs          2-4 (rpc #100003)
Service Info: Host: METASPLOITABLE; OS: Windows

Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.831 seconds
msfadmin@metasploitable:~$
```

□ Quels sont les 4 ports UDP que nmap a trouvé comme étant ouverts (pas ouverts|filtrés, juste ouverts) et quels sont les services qui fonctionnent sur ces ports ? Donnez votre réponse dans l'ordre numérique croissant.

Les 4 ports ouverts sont : le port 53, le port 111, le port 137 et le port 2049.

Les services qui fonctionnent sur ces ports sont :

- 53 → domain
- 111 → rpcbind
- 137 → netbios-dgm
- 2049 → nfs

Partie 5 – Détection du système d'exploitation (OS)

Livrables :

□ Quel est le type de périphérique de la VM Metasploitable2 selon nmap ?

Le type de peripherique est : general purpose.

□ Quelle est la chaîne CPE (Common Platform Enumeration) de la VM Metasploitable2 ?

□ Quelle est la chaîne OS Details fournie par nmap pour la VM Metasploitable2, montrant la gamme de versions de noyau qu'il pense que l'hôte exécute ?

La chaine OS Details a fournie des details sur le système d'exploitation de la VM.

□ Vérifiez la VM Metasploitable2 – Quelle version de noyau exécute-t-elle réellement ? (Fournissez votre réponse sous la forme x.x.x-x-tag)

la version de noyau executee est la version 2.6.X

```
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgres
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20 (Ubuntu 7.04, x86, SMP)
Uptime: 0.165 days (since Sun Apr 28 06:52:33 2024)
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at http://insecu
rg/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.580 seconds
msfadmin@metasploitable:~$ _
```

Partie 6 – Scan des versions et des services

Livrables :

□ Quelle version d'OpenSSH est utilisée ?

La version d'OpenSSH utilisee est : la version 4.7p1

```
msfadmin@metasploitable:~$ sudo nmap -p 22 --script ssh-versions -sV 10.0.2.4
Starting Nmap 4.53 ( http://insecure.org ) at 2024-04-28 11:17 EDT
SCRIPT ENGINE: No such category, file or directory: 'ssh-versions'
SCRIPT ENGINE: Aborting script scan.
Interesting ports on 10.0.2.4:
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Service Info: OS: Linux

Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.120 seconds
msfadmin@metasploitable:~$ _
```

□ Quelle version du serveur DNS BIND est en cours d'exécution ?

On tape la commande `sudo nmap -p 'numport' -- script 'nomservice-versions' -sV @IP`

```
PORT      STATE SERVICE VERSION
53/tcp    open  domain
```

Ici aucune version n'est spécifiée.

Partie 7 - Analyse complète

□ Quel est le groupe de travail NetBIOS du serveur Samba sur la VM de Metasploitable2 ?

```
_ 100021 1,3,4 59207/tcp ntlockmgr
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rshcd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
MAC Address: 08:00:27:C1:09:A0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 25m35s, deviation: 2h18m34s, median: -54m25s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2024-04-28T11:49:58-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

□ Quelle est la clé hôte RSA SSH de 2048 bits qui identifie cette cible ?

```
22/tcp open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA) ←
```