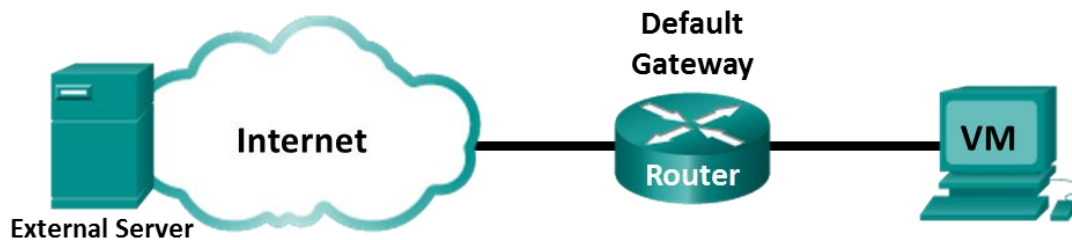


Travaux pratiques – Découvrir Nmap

Topologie



Objectifs

Partie 1 : Découvrir Nmap

Partie 2 : Rechercher des ports ouverts

Contexte/scénario

L'analyse des ports fait généralement partie d'une attaque de reconnaissance. Diverses méthodes d'analyse des ports peuvent être utilisées. Nous allons étudier comment se servir de l'utilitaire de Nmap. Nmap est un utilitaire réseau puissant qui est utilisé pour la découverte du réseau et pour l'audit de sécurité.

Ressources requises

- Poste de travail Kali
- Accès Internet

Instructions

Partie 1 : Découvrir Nmap

Dans cette partie, vous allez utiliser les pages de manuel pour en savoir plus sur Nmap.

La commande **man** [*program* | *utility* | *function*] affiche les pages de manuel associées aux arguments. Les pages de manuel correspondent aux manuels de référence trouvés sur les systèmes d'exploitation Unix et Linux. Ces pages incluent ces sections : Nom, Synopsis, Descriptions, Exemples et Voir aussi.

- a. Lancez le poste de travail Kali.

- b. Ouvrez un terminal.
- c. À l'invite du terminal, saisissez **man nmap**.

```
[analyst@secOps ~]$ man nmap
```

Qu'est-ce que Nmap ?

Nmap est un outil d'exploration réseau et scanneur de ports/sécurité.

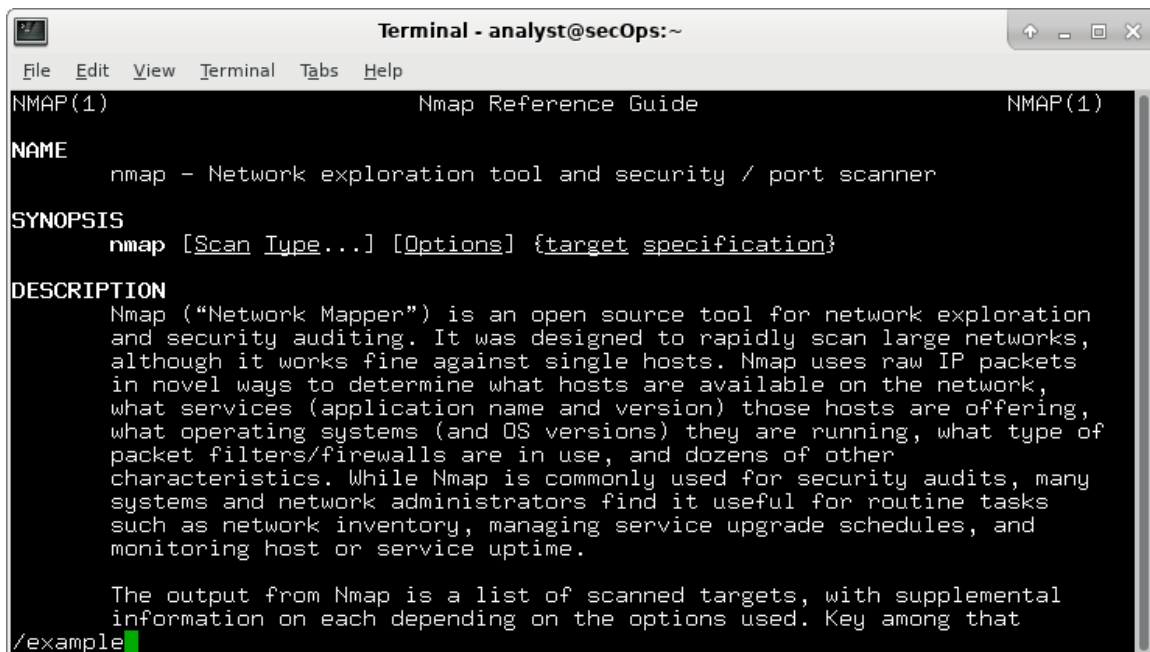
À quoi Nmap sert-il ?

Nmap est un outil open source d'exploration réseau et d'audit de sécurité, il a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique.

- d. Lorsque vous êtes sur la page du manuel, vous pouvez utiliser les touches fléchées haut/bas pour faire défiler les pages. Vous pouvez également appuyer sur la barre d'espace pour avancer d'une page à la fois.

Pour rechercher un terme ou une expression spécifique, saisissez une barre oblique (/) ou un point d'interrogation (?) suivi de ce terme ou de cette expression. La barre oblique permet d'effectuer une recherche vers l'avant dans tout le document, tandis que le point d'interrogation effectue une recherche en arrière dans le document. La touche **n** permet d'accéder à la correspondance suivante.

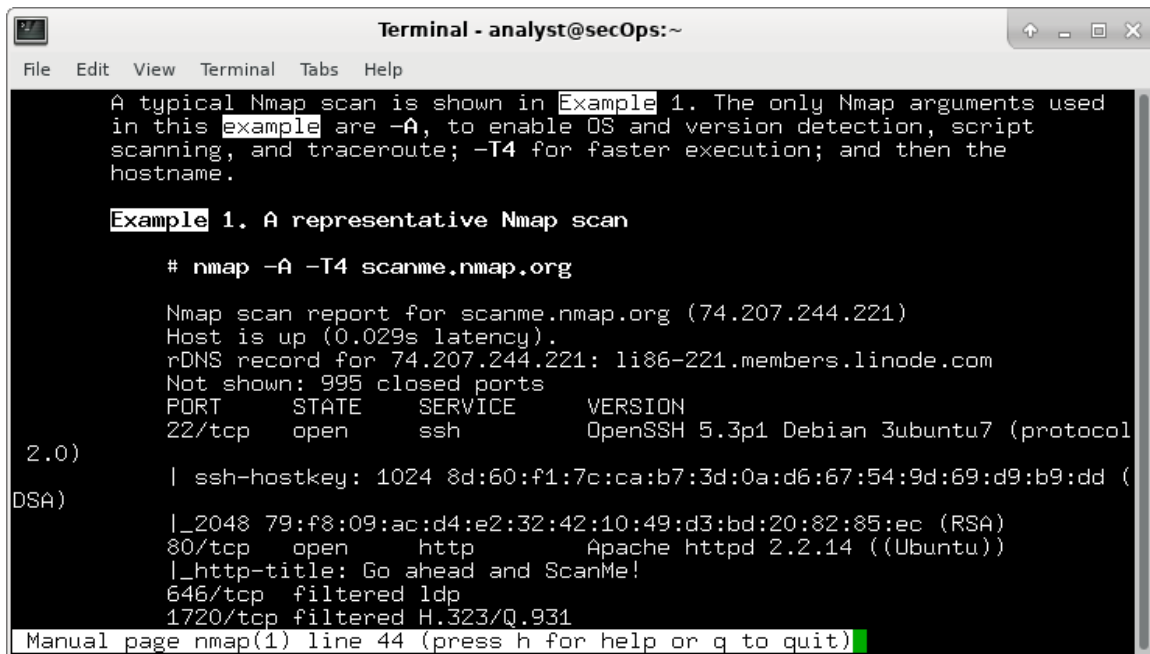
Saisissez **/example** et appuyez sur ENTRÉE. Cette opération permet de rechercher le mot **example** vers l'avant dans les pages du manuel.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
NMAP(1)                                Nmap Reference Guide                                NMAP(1)
NAME
  nmap - Network exploration tool and security / port scanner
SYNOPSIS
  nmap [Scan Type...] [Options] {target specification}
DESCRIPTION
  Nmap ("Network Mapper") is an open source tool for network exploration
  and security auditing. It was designed to rapidly scan large networks,
  although it works fine against single hosts. Nmap uses raw IP packets
  in novel ways to determine what hosts are available on the network,
  what services (application name and version) those hosts are offering,
  what operating systems (and OS versions) they are running, what type of
  packet filters/firewalls are in use, and dozens of other
  characteristics. While Nmap is commonly used for security audits, many
  systems and network administrators find it useful for routine tasks
  such as network inventory, managing service upgrade schedules, and
  monitoring host or service uptime.

  The output from Nmap is a list of scanned targets, with supplemental
  information on each depending on the options used. Key among that
/example
```

- e. Dans le premier exemple, trois correspondances s'affichent. Pour accéder à la correspondance suivante, appuyez sur **n**.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (
DSA)
|_ 2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open  http     Apache httpd 2.2.14 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
646/tcp   filtered ldap
1720/tcp  filtered H.323/Q.931
Manual page nmap(1) line 44 (press h for help or q to quit)
```

Regardez l'exemple 1.

Quelle est la commande **nmap** utilisée ?

La commande nmap utilisée est la suivante : **nmap -A -T4 scanme.nmap.org playground**

Utilisez la fonction de recherche pour répondre aux questions suivantes.

À quoi sert le commutateur **-A** ?

"-A" est un commutateur ou une option qui active une analyse plus complète. Cela inclut la détection du système d'exploitation, l'analyse des versions des services, la détection des scripts de sécurité et d'autres informations supplémentaires.

À quoi sert le commutateur **-T4** ?

"-T4" est un autre commutateur qui définit le niveau d'agressivité du balayage. Dans ce cas, il s'agit d'un niveau d'agressivité **"4"**, ce qui signifie un rythme de balayage assez rapide.

- f. Faites défiler la page pour en savoir plus sur nmap. Saisissez « **q** » lorsque vous avez terminé.

Partie 2 : Analyse des ports ouverts

Dans cette partie, vous allez utiliser les commutateurs issus de l'exemple des pages de manuel Nmap pour analyser votre hôte local, votre réseau local et un serveur distant à scanme.nmap.org.

Étape 1: Analysez votre hôte local.

- Si nécessaire, ouvrez un terminal sur la machine virtuelle. À l'invite, saisissez **nmap -A -T4 localhost**. Selon votre réseau local et vos périphériques, l'analyse peut durer de quelques secondes à quelques minutes.

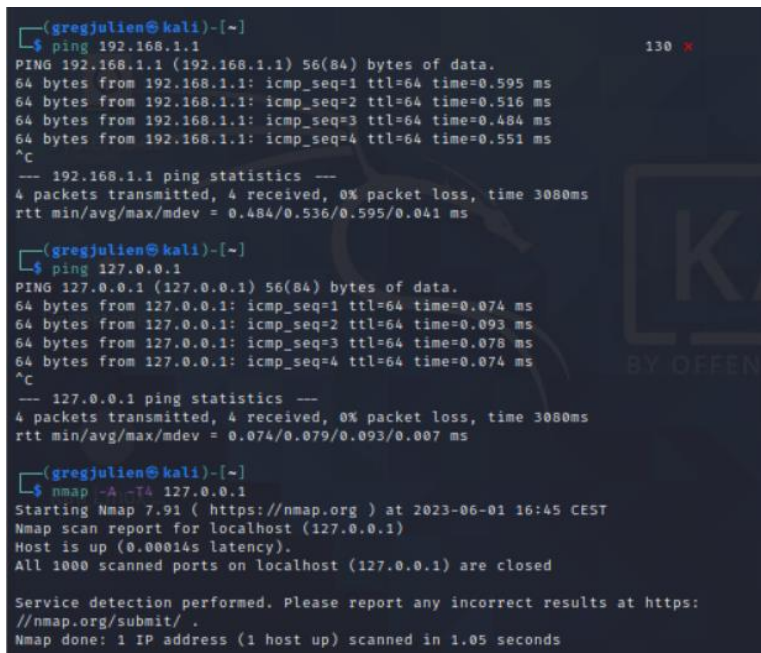
```
[kali@root ~]$ nmap -A -T4 localhost

Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 17:20 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000056s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
21/tcp open  ftp vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r-- 1 0 0 0 Apr 19 15:23 ftp_test
<some output omitted>
```

- Vérifiez les résultats et répondez aux questions suivantes.

Quels sont les ports et les services ouverts ?

En réalisant la commande **nmap -A -T4 localhost** sur ma kali, voici le résultat :



```
(gregjulien@kali)~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.595 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.516 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.484 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.551 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.484/0.536/0.595/0.041 ms

(gregjulien@kali)~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data:
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.093 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.078 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.074 ms
^C
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.074/0.079/0.093/0.007 ms

(gregjulien@kali)~$ nmap -A -T4 127.0.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-01 16:45 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
All 1000 scanned ports on localhost (127.0.0.1) are closed
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
```

Le message est donc différent de celui du TP.

Sur le message du TP, nous avons le port 21 sur lequel le service ftp écoute.

Pour chacun des ports ouverts, notez le logiciel qui fournit les services.

D'après les résultats de la commande Nmap du message du TP, le logiciel qui fournit le service sur le port 21 est "vsftpd" (Very Secure FTP Daemon) dans sa version 2.0.8 ou ultérieure.

Étape 2: Analysez votre réseau

AVERTISSEMENT : avant d'utiliser Nmap sur un réseau, demandez l'autorisation des propriétaires du réseau.

- a. À l'invite de commande du terminal, saisissez **ip address** pour déterminer l'adresse IP et le masque de sous-réseau de cet hôte. Dans cet exemple, l'adresse IP de cette machine virtuelle est 10.0.2.15 et le masque de sous-réseau est 255.255.255.0.

```
[kali@root] ~]$ ip address
```

<output omitted>

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
```

```
link/ether 08:00:27:ed:af:2c brd ff:ff:ff:ff:ff:ff
```

```
inet 10.0.2.15/24 brd 10.0.2.255 étendue dynamique globale enp0s3
```

```
valid_lft 85777sec preferred_lft 85777sec
```

```
inet6 fe80::a00:27ff:feed:af2c/64 lien de portée
```

```
valid_lft forever preferred_lft forever
```

Enregistrez l'adresse IP et le masque de sous-réseau de votre machine virtuelle.

```
(gregjulien@kali)-[~]
$ ip address
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
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether 00:50:56:b1:61:16 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.5/24 brd 192.168.1.255 scope global noprefixroute eth0
valid_lft forever preferred_lft forever
```

À quel réseau votre machine virtuelle appartient-elle ?

Ma machine appartient au réseau 192.168.1.0.

- b. Pour localiser les autres hôtes sur ce réseau local, saisissez **nmap -A -T4 network address/prefix**. Le dernier octet de l'adresse IP doit être remplacé par un zéro. Par exemple, l'adresse IP 10.0.2.15, où .15

correspond au dernier octet. Par conséquent, l'adresse réseau est 10.0.2.0. /24 est le préfixe. Il s'agit du raccourci pour le masque de sous-réseau 255.255.255.0. Si le masque de réseau votre machine virtuelle est différent, recherchez votre préfixe dans le «tableau de conversion CIDR» sur Internet. Par exemple, 255.255.0.0 correspond à /16. L'adresse réseau 10.0.2.0/24 est utilisée dans cet exemple

Remarque : cette opération peut prendre un certain temps, surtout si plusieurs périphériques sont connectés au réseau. Dans l'environnement de test, l'analyse a pris environ 4 minutes.

```
[kali@root $ nmap -A -T4 10.0.2.0/24
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 17:13 EDT
```

```
<output omitted>
```

```
Nmap scan report for 10.0.2.15
```

```
Host is up (0.00019s latency).
```

```
Not shown: 997 closed ports
```

```
PORT STATE SERVICE VERSION
```

```
21/tcp open ftp vsftpd 2.0.8 or later
```

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
|_rw-r--r-- 1 0 0 0 26 mars 2018 ftp_test
```

```
| ftp-syst:
```

```
| STAT:
```

```
| FTP server status:
```

```
| Connected to 10.0.2.15
```

```
| Logged in as ftp
```

```
| TYPE: ASCII
```

```
| No session bandwidth limit
```

```
| Session timeout in seconds is 300
```

```
| Control connection is plain text
```

```
| Data connections will be plain text
```

```
| At session startup, client count was 1
```

```
| vsFTPD 3.0.3 - secure, fast, stable
```

```
|_End of status
```

```
22/tcp open ssh OpenSSH 8.2 (protocol 2.0)
```

```
23/tcp open telnet Openwall GNU/*/Linux telnetd
```

```
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Post-scan script results:
```

```
| clock-skew:
| 0s:
| 10.0.2.4
| 10.0.2.3
|_ 10.0.2.2

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .

Nmap done: 256 IP addresses (4 hosts up) scanned in 346.89 seconds
```

Comment d'hôtes sont activés ?

Il y a 4 hôtes qui sont activés d'après l'exemple.

Dans vos résultats Nmap, répertoriez les adresses IP des hôtes qui se trouvent sur le même réseau local que votre machine virtuelle. Répertoriez certains des services qui sont disponibles sur les ordinateurs hôtes détectés.

Étape 3: Analysez un serveur distant.

- Ouvrez un navigateur web et accédez à l'adresse **scanme.nmap.org**. Veuillez lire le message posté.

Quel est l'objectif de ce site ?

L'objectif principal de "scanme.nmap.org" est de servir de cible d'analyse pour les utilisateurs de Nmap, afin qu'ils puissent expérimenter et se familiariser avec les fonctionnalités de l'outil. Les utilisateurs peuvent effectuer des balayages de ports, des détections de services, des détections de systèmes d'exploitation et d'autres types d'analyses sur ce domaine sans violer les politiques de sécurité ou les lois en vigueur.

- À l'invite du terminal, saisissez **nmap -A -T4 scanme.nmap.org**.

```
[kali@root $ nmap -A -T4 scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 16:46 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.040s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
```

```
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp filtered smtp
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
4444/tcp filtered krb524
9929/tcp open nping-echo Nping echo
31337/tcp open tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 23.96 seconds

c. Vérifiez les résultats et répondez aux questions suivantes.

Quels sont les ports et les services ouverts ?

Les ports et services ouverts sont :

- 22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
- 25/tcp filtered smtp
- 80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
- 135/tcp filtered msrpc
- 139/tcp filtered netbios-ssn
- 445/tcp filtered microsoft-ds
- 593/tcp filtered http-rpc-epmap
- 4444/tcp filtered krb524
- 9929/tcp open nping-echo Nping echo
- 31337/tcp open tcpwrapped

Quels sont les ports et les services filtrés ?

Les ports et les services filtrés sont :

- 25/tcp filtered smtp
- 135/tcp filtered msrpc
- 139/tcp filtered netbios-ssn
- 445/tcp filtered microsoft-ds
- 593/tcp filtered http-rpc-epmap
- 4444/tcp filtered krb524

Quelle est l'adresse IP du serveur ?

L'adresse IP du serveur est : 45.33.32.156

Quel est le système d'exploitation ?

Son OS est Linux.

Question de réflexion

Nmap est un outil puissant pour l'exploration et la gestion du réseau. Comment Nmap peut-il contribuer à la sécurité du réseau ? Comment Nmap peut-il être utilisé par un hacker comme outil néfaste ?

Voici comment Nmap peut contribuer à la sécurité du réseau :

- Détection des ports ouverts : Nmap peut être utilisé pour analyser un réseau et détecter les ports ouverts sur les machines cibles. Cela permet aux administrateurs système de découvrir les services en cours d'exécution et de s'assurer que seuls les ports nécessaires sont accessibles, réduisant ainsi la surface d'attaque potentielle.
- Détection des vulnérabilités : Nmap peut effectuer des analyses de vulnérabilité en recherchant les versions des services et des systèmes d'exploitation. En comparant ces informations avec des bases de données de vulnérabilités, les administrateurs peuvent identifier les failles potentielles et prendre des mesures correctives pour les résoudre.
- Audit de sécurité : Nmap peut être utilisé pour effectuer des audits de sécurité en analysant la configuration des pare-feu, la présence de services non autorisés ou non sécurisés, et en identifiant les faiblesses potentielles du réseau.
- Surveillance du réseau : Nmap peut être utilisé pour surveiller le réseau et détecter les modifications non autorisées, telles que l'ouverture de nouveaux ports ou l'installation de nouveaux services.

Cependant, en tant qu'outil puissant, Nmap peut également être utilisé par des individus malveillants ou des hackers comme un outil néfaste. Voici quelques exemples :

- Balayage de ports et d'hôtes : Les hackers peuvent utiliser Nmap pour effectuer des balayages de ports et d'hôtes afin d'identifier des machines vulnérables ou des services mal configurés pour lancer des attaques ultérieures.
- Enumération des services : Nmap permet de découvrir les services et les versions utilisées sur les machines cibles, ce qui peut aider les hackers à identifier des vulnérabilités spécifiques et à exploiter des failles connues.
- Attaques par déni de service : Nmap peut être utilisé pour effectuer des scans de manière intensive, ce qui peut entraîner une surcharge des ressources du réseau ou des serveurs cibles, provoquant ainsi une interruption de service.
- Fingerprinting : Nmap peut être utilisé pour collecter des informations sur les systèmes cibles, telles que les versions des services et les systèmes d'exploitation. Ces informations peuvent être utilisées pour cibler des attaques spécifiques ou pour des activités de reconnaissance approfondie.