Esercitazione WEEK 11 D1
Scansione dei servizi con Nmap

Ettore Farris - 16/01/2024

Descrizione sintetica

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint
- Syn Scan
- TCP connect (Trovate differenze tra i risultati della scansioni TCP connect e SYN?)
- Version detection

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un report contenente le seguenti info (dove disponibili): -

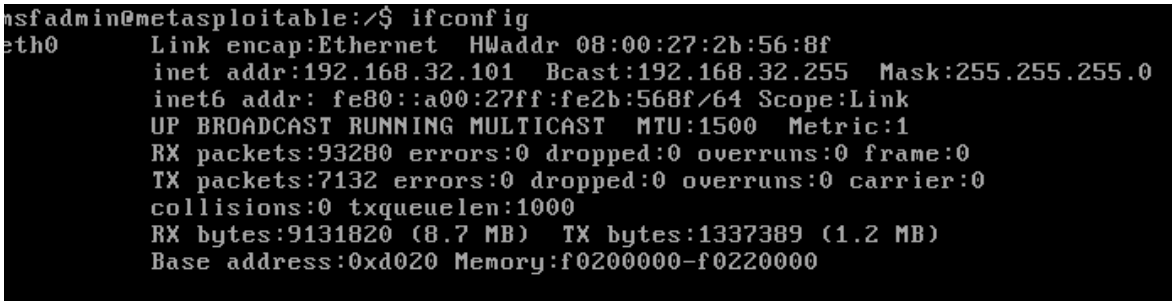
- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

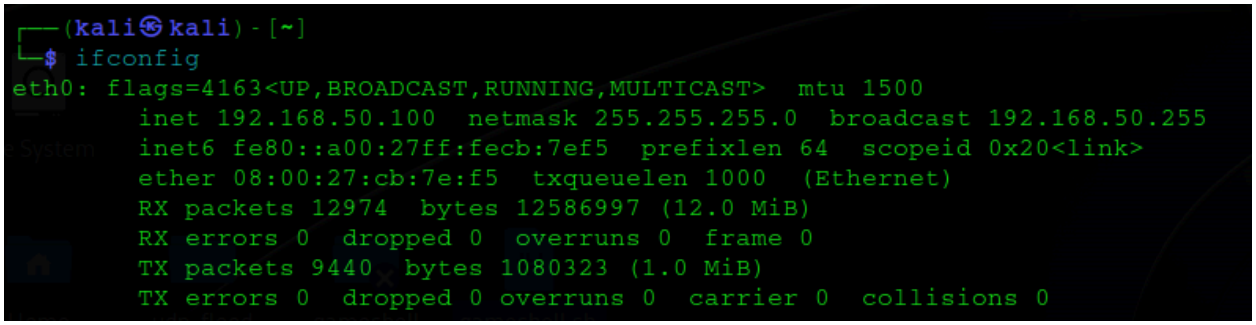
https://www.poftut.com/nmap-output/

nmap -oN report1 IP

1) Scansione con Kali e Metasploitable su reti diverse

Per questa scansione, le macchine Kali Linux e Metasploitable appartengono a reti interne diverse, rispettivamente chiamate *intnet* e *pfsense* e hanno i seguenti indirizzi IP:





Procediamo quindi con le scansioni

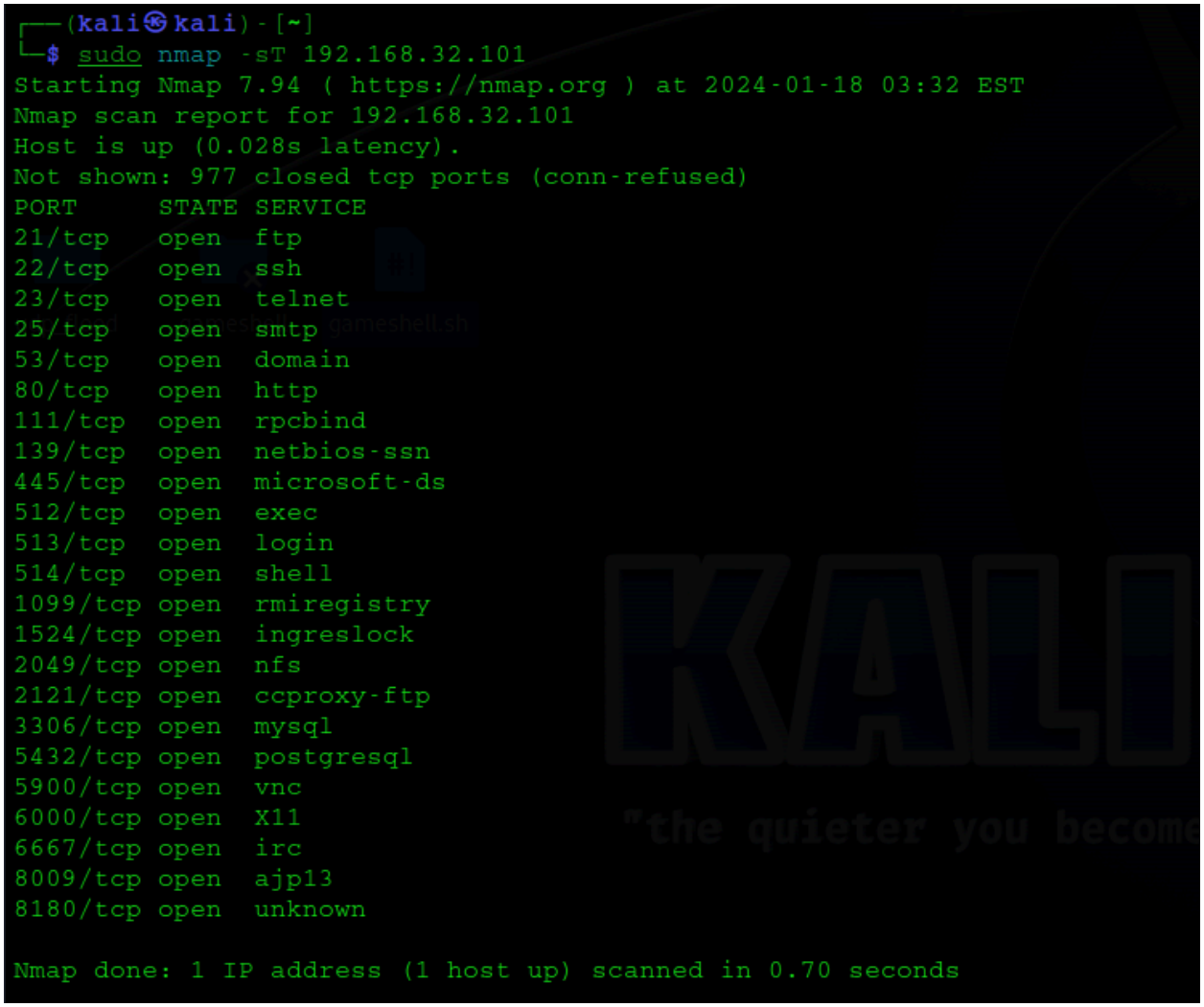
- OS fingerprint

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 03:30 EST
Nmap scan report for 192.168.32.101
Host is up (0.0090s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
```

- SYN scan

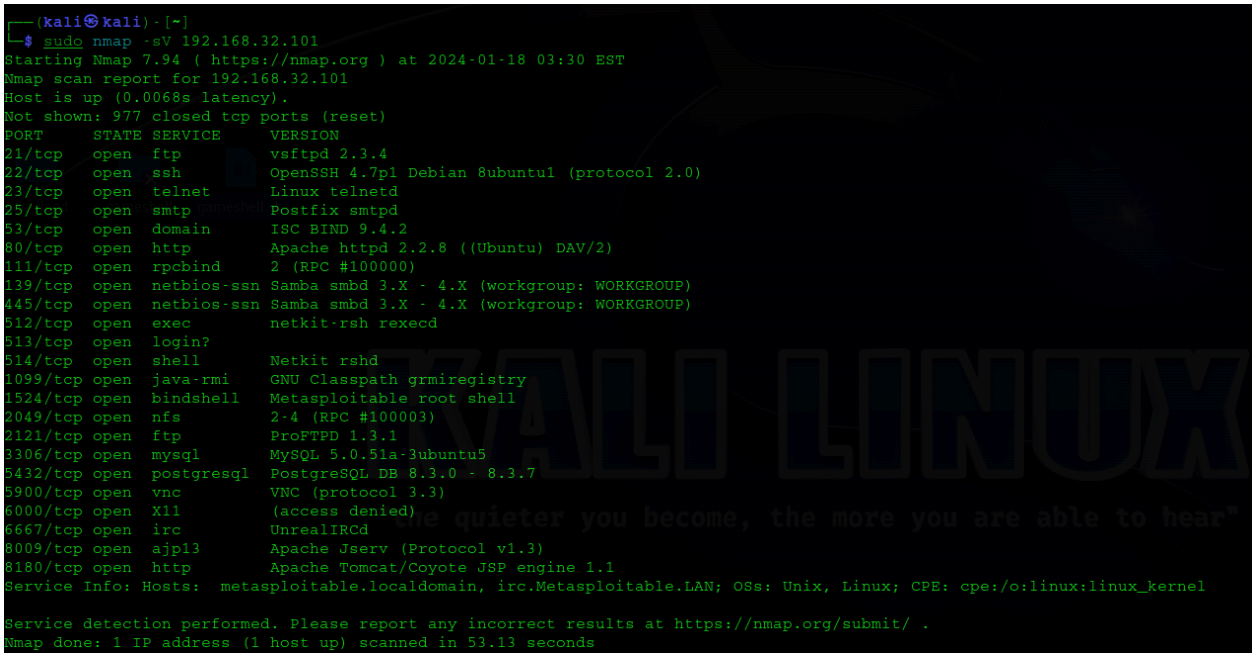
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.32.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 03:30 EST
Nmap scan report for 192.168.32.101
Host is up (0.018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

- TCP scan



Differenze tra TCP e SYN scan: nessuna differenza sostanziale delle informazioni ricevute. Gli unici dati che cambiano sono la latenza e in tempo di esecuzione, inferiore per la SYN scan.

- sV scan



- Esportazione di report

Per l'esportazione del report ho preferito usare una scansione -sV per version detection in quanto fornisce anche informazioni di massima sul sistema operativo usato. Il comando è:

sudo nmap -sV -oN report1.txt -v 192.168.32.101

- l flag -*sv* indica il tipo di scansione

- il flag -*nO <nome file>* è quello dell'output

- il flag -*v* (che sta per *verbose*) rende l'output più leggibile

Verifichiamo la presenza del file e leggiamo l'output:

```
┌──(kali㉿kali)-[~]
└─$ cat report1.txt
# Nmap 7.94 scan initiated Thu Jan 18 04:54:32 2024 as: nmap -sV -oN report1.txt -v 192.168.32.101
Nmap scan report for 192.168.32.101
Host is up (0.024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jan 18 04:55:25 2024 -- 1 IP address (1 host up) scanned in 53.15 seconds
```

2) Scansione con Kali e Metasploitable sulla stessa rete

Modifichiamo le impostazioni di rete e mettiamo entrambe le macchine sulla stessa rete interna dalle impostazioni di VirtualBox (nome rete: *intnet*).

Modifichiamo l'IP di Metasploitable in modo che appartenga allo stesso dominio di Kali, 192.168.50.0 modificando il file */etc/network/interfaces.*

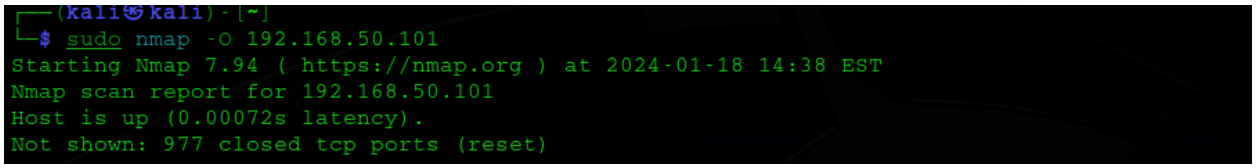
```
  GNU nano 2.0.7         File: /etc/network/interfaces                Modif

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static

address 192.168.50.101
netmask 255.255.255.0
network 192.168.50.100
broadcast 192.168.50.255
gateway 192.168.50.1
```

- *Confronto tra le stesse scansioni con host su reti diverse*

Si può notare come una stessa scan impieghi decisamente meno tempo tra host sulla stessa rete che tra gli stessi, ma su reti diverse.

Prendiamo per esempio la scan di *OS fingerprinting*:

Stessa rete: latenza di 0.00072s

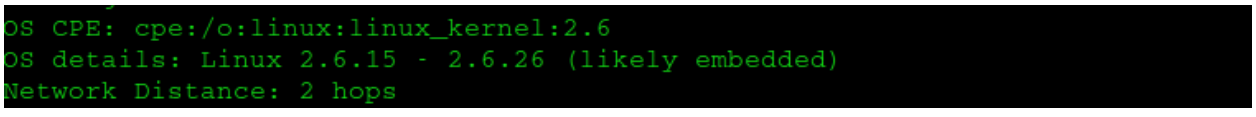


Reti diverse: latenza di 0.009s

Un'altra cosa che salta all'occhio dai risultati della scan è il numero di *hop,* uno nel caso della stessa rete, due in quello di reti diverse. Questo è dovuto al fatto che, se i dispositivi non appartengono alla stessa rete, il traffico passerà per il default gateway "alla ricerca" dell'host su un'altra rete.

Stessa rete: 1 hop

Reti diverse: 2 hops



- *Esportazione del report*

Come nell'esempio precedente, esportiamo un report col comando

"sudo nmap -sV -oN report2.txt -v 192.168.50.101"

cambiando ovviamente il nome del file e l'indirizzo IP di Metasploitable, che in questo caso è 192.168.50.101.