Esercitazione W11D4

Nmap

Fabio Benevento - 19/01/2024

Traccia

Questo esercizio può essere utile per lo studente per prendere dimestichezza con i vari comandi di nmap. Poiché su Linux è un potente tool di scansione della rete, si richiede di utilizzare i seguenti comandi e trascrivere i vari risultati su un report:
- TCP: # nmap -sS ip address
- output su file: # nmap -sV -oN file.txt ip address
- scansione su porta: # nmap -sS -p 8080 ip address
- scansione tutte le porte: # nmap -sS -p- ip address
- scansione UDP: # nmap -sU -r -v ip address
- scansione sistema operativo: # nmap -O ip address
- scansione versione servizi: # nmap -sV ip address
- scansione common 100 ports: # nmap -F ip address
- scansione tramite ARP: # nmap -PR ip address
- scansione tramite PING: # nmap -sP ip address

Infine, disegnare 3-4 grafici delle scansioni effettuate, esplicitando le varie fasi di syn, syn/ack ecc.

Implementazione

Di seguito è mostrato l'output ottenuto in seguito all'esecuzione del comando indicato.

- TCP: # nmap -sS ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:10 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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
MAC Address: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.92 seconds
```

- output su file: # nmap -sV -oN file.txt ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -oN nmap_metasploit.txt 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:14 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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  unknown
MAC Address: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 186.40 seconds
```

- scansione su porta: # nmap -sS -p 8080 ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 8080 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:17 EST
Nmap scan report for 192.168.50.101
Host is up (0.0040s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

- scansione tutte le porte: # nmap -sS -p- ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p- 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:23 EST
Nmap scan report for 192.168.50.101
Host is up (0.013s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34310/tcp open  unknown
41975/tcp open  unknown
50623/tcp open  unknown
52374/tcp open  unknown
MAC Address: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 32.05 seconds
```

- scansione UDP: # nmap -sU -r -v ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -r -v 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:26 EST
Initiating ARP Ping Scan at 10:26
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 10:26, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:26
Completed Parallel DNS resolution of 1 host. at 10:26, 13.01s elapsed
Initiating UDP Scan at 10:26
Scanning 192.168.50.101 [1000 ports]
Discovered open port 53/udp on 192.168.50.101
Discovered open port 111/udp on 192.168.50.101
Increasing send delay for 192.168.50.101 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.50.101 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.50.101 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.50.101 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.50.101 from 400 to 800 due to max_successful_tryno increase to 8
Discovered open port 137/udp on 192.168.50.101
UDP Scan Timing: About 3.88% done; ETC: 10:40 (0:12:48 remaining)
UDP Scan Timing: About 6.83% done; ETC: 10:41 (0:13:52 remaining)
UDP Scan Timing: About 10.58% done; ETC: 10:43 (0:14:56 remaining)
UDP Scan Timing: About 15.68% done; ETC: 10:43 (0:14:04 remaining)
Discovered open port 2049/udp on 192.168.50.101
UDP Scan Timing: About 22.02% done; ETC: 10:43 (0:13:10 remaining)
UDP Scan Timing: About 28.60% done; ETC: 10:43 (0:12:16 remaining)
UDP Scan Timing: About 34.54% done; ETC: 10:44 (0:11:18 remaining)
UDP Scan Timing: About 39.51% done; ETC: 10:43 (0:10:22 remaining)
UDP Scan Timing: About 44.84% done; ETC: 10:43 (0:09:30 remaining)
UDP Scan Timing: About 50.29% done; ETC: 10:44 (0:08:37 remaining)
UDP Scan Timing: About 55.62% done; ETC: 10:44 (0:07:43 remaining)
UDP Scan Timing: About 61.07% done; ETC: 10:44 (0:06:48 remaining)
UDP Scan Timing: About 66.19% done; ETC: 10:44 (0:05:54 remaining)
UDP Scan Timing: About 71.43% done; ETC: 10:44 (0:05:00 remaining)
UDP Scan Timing: About 76.55% done; ETC: 10:44 (0:04:07 remaining)
UDP Scan Timing: About 81.57% done; ETC: 10:44 (0:03:14 remaining)
UDP Scan Timing: About 86.80% done; ETC: 10:44 (0:02:19 remaining)
UDP Scan Timing: About 91.90% done; ETC: 10:44 (0:01:25 remaining)
UDP Scan Timing: About 97.11% done; ETC: 10:44 (0:00:30 remaining)
Completed UDP Scan at 10:44, 1085.52s elapsed (1000 total ports)
Nmap scan report for 192.168.50.101
Host is up (0.0018s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
944/udp  open|filtered unknown
2049/udp open          nfs
MAC Address: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1098.75 seconds
           Raw packets sent: 1512 (70.291KB) | Rcvd: 1104 (80.554KB)
```

- scansione sistema operativo: # nmap -O ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:32 EST
Nmap scan report for 192.168.50.101
Host is up (0.0017s 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
MAC Address: 08:00:27:10:8A:34 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds
```

- scansione versione servizi: # nmap -sV ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV  192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:44 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s 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
MAC Address: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 66.04 seconds
```

- scansione common 100 ports: # nmap -F ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -F 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 11:13 EST
Nmap scan report for 192.168.50.101
Host is up (0.0018s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
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
8009/tcp open  ajp13
MAC Address: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
```

- scansione tramite ARP: # nmap -PR ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PR 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 11:23 EST
Nmap scan report for 192.168.50.101
Host is up (0.00074s 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
MAC Address: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.88 seconds
```

- scansione tramite PING: # nmap -sP ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 11:27 EST
Nmap scan report for 192.168.50.101
Host is up (0.0019s latency).
MAC Address: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
```

Report finale

Di seguito il report in forma tabellare con le informazioni trovate

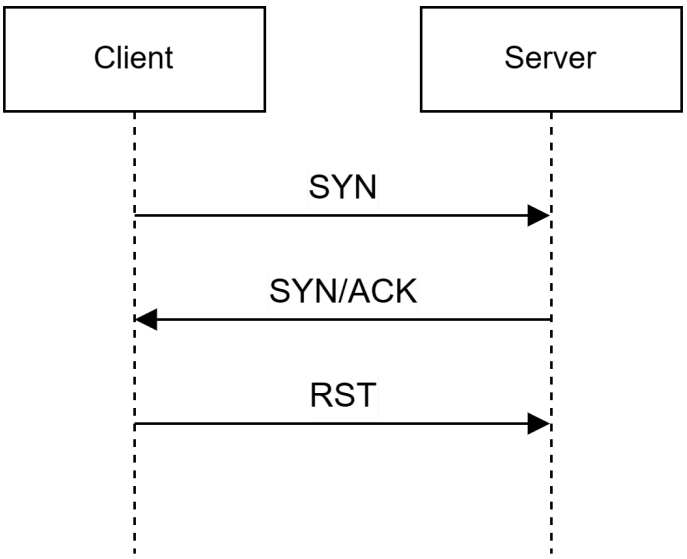
Fonte	Kali Linux - IP: 192.168.50.100	
Target	Metasploitable - IP: 192.168.50.101	
Tipo di scan	Nmap (varie modalità)	
Numero servizi trovati		12
Porta	**Servizio**	**Versione**
21	ftp	vsftpd 2.3.4
22	ssh	OpenSSH 4.7p1
23	telnet	Linux telnetd
25	smtp	Postfix smtpd
53	domain	ISC Bind 9.4.2
69	tftp	
80	http	Apache 2.2.8
111	rpc-bind	2
137	netbios-ns	
138	netbios-dgm	
139	netbios-ssn	Samba 3.x - 4.x
445	microsoft-ds	Samba 3.x - 4.x
512	exec	netkit-rsh rexeccd
513	login	
514	shell	netkit-rsh
944	unknown	
1099	java-rmi	GNU classpath gmiregistry

1524	bindshell	Metasploitable root shell
2049	nfs	2-4
2121	ftp	ProFTP 1.3.1
3306	mysql	5.0.51a
5432	postgresql	8.3.0 - 8.3.7
5900	vnc	protocol 3.3
6000	X11	
6667	irc	UnrealIRCd
8009	ajp13	Apache jserv (prot. 1.3)
8081	http	Apache Tomcat 1.1
8787	msgsvr	
34310	unknown	
41975	unknown	
50623	unknown	
52364	unknown	

Grafici scansioni effettuate

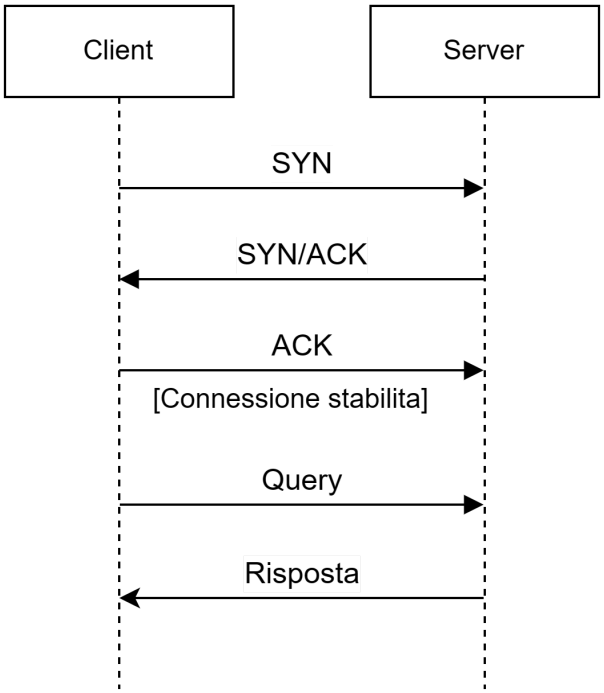
Nmap -sS

Questo comando specifica a Nmap di eseguire una "scansione TCP SYN" o "scansione stealth". Durante questa scansione, il client invia un pacchetto TCP SYN al server. Se la porta è aperta, il server risponde con un pacchetto TCP SYN/ACK. Infine, il client invia un pacchetto TCP RST per terminare la connessione senza completare il three-way handshake.



Nmap -sV

Questo comando viene utilizzato per eseguire la scansione dei servizi, cercando di identificare le versioni dei servizi che operano sulle porte aperte. Durante questa scansione, Nmap utilizza la tecnica di "scansione TCP connect". In questo caso, il client stabilisce effettivamente una connessione completa con il server. Dopo aver stabilito la connessione, Nmap invia alcune richieste al servizio in esecuzione sulla porta per ottenere informazioni sulla versione. Il grafico seguente mostra l'interazione tra client e server in questo tipo di scansione.



Nmap -sA

Questa opzione esegue una scansione di tipo ACK. Invece di inviare un pacchetto SYN come in una scansione normale, il client invia un pacchetto TCP ACK alla porta di destinazione. Se la porta è aperta, non viene inviato alcun pacchetto di risposta. Se la porta è chiusa, viene restituito un pacchetto RST/ACK. Questo tipo di scansione è utile per determinare la presenza di firewall o filtri di rete che potrebbero rispondere in modo diverso a pacchetti ACK.