

W11D4 - Pratica

Giacomo di Giacinto



W11D4 - Pratica PDF

Esercizio

Scansione dei servizi

Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

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
scansione completa: #	nmap -sV 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

Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

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

1)sudo nmap -sS 192.168.1.246

Scansione TCP

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sS 192.168.1.246  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:11 CET  
Nmap scan report for 192.168.1.246  
Host is up (0.0015s 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:CE:D2:42 (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

2)sudo nmap -sV 192.168.1.246

Scansione completa

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:21 CET
Nmap scan report for 192.168.1.246
Host is up (0.00095s 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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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:CE:D2:42 (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 15.74 seconds
```

3)sudo nmap -sV -oN file.txt 192.168.1.246

Output su file

```
(kali@kali)-[~]
$ nmap -sV -oN file.txt 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:26 CET
Nmap scan report for 192.168.1.246
Host is up (0.0028s latency).
Not shown: 977 closed tcp ports (conn-refused)
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  tcpwrapped
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.64 seconds
```



file.txt

4) sudo nmap -sS 192.168.1.246 -p 8080

scansione su porta

```
(kali㉿kali)-[~]  
$ sudo nmap -sS 192.168.1.246 -p 8080  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:33 CET  
Nmap scan report for 192.168.1.246  
Host is up (0.0014s latency).  
  
PORT      STATE SERVICE  
8080/tcp  closed http-proxy  
MAC Address: 08:00:27:CE:D2:42 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

5) sudo nmap -sS -p- 192.168.1.246

scansione su tutte le porte

```
(kali㉿kali)-[~]  
$ sudo nmap -sS -p- 192.168.1.246  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:46 CET  
Nmap scan report for 192.168.1.246  
Host is up (0.0010s 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      |
| 35549/tcp | open  | unknown      |
| 37785/tcp | open  | unknown      |
| 50717/tcp | open  | unknown      |
| 56181/tcp | open  | unknown      |

  
MAC Address: 08:00:27:CE:D2:42 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 19.87 seconds
```

6) sudo nmap -sU -r -v 192.168.1.246

scansione UDP

```
(kali㉿kali)-[~]  
$ sudo nmap -sU -r -v 192.168.1.246  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:42 CET  
Initiating ARP Ping Scan at 19:42  
Scanning 192.168.1.246 [1 port]  
Completed ARP Ping Scan at 19:42, 0.04s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 19:42  
Completed Parallel DNS resolution of 1 host. at 19:42, 0.00s elapsed  
Initiating UDP Scan at 19:42  
Scanning 192.168.1.246 [1000 ports]  
Discovered open port 111/udp on 192.168.1.246  
Discovered open port 53/udp on 192.168.1.246  
Increasing send delay for 192.168.1.246 from 0 to 50 due to max_successful_try  
no increase to 4  
Increasing send delay for 192.168.1.246 from 50 to 100 due to max_successful_t  
ryno increase to 5  
Increasing send delay for 192.168.1.246 from 100 to 200 due to max_successful_  
tryno increase to 6  
Increasing send delay for 192.168.1.246 from 200 to 400 due to 11 out of 12 dr  
opped probes since last increase.  
Discovered open port 137/udp on 192.168.1.246  
UDP Scan Timing: About 4.55% done; ETC: 19:54 (0:10:50 remaining)  
Increasing send delay for 192.168.1.246 from 400 to 800 due to 11 out of 17 dr  
opped probes since last increase.
```


7) sudo nmap -O 192.168.1.246

scansione sistema operativo

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:51 CET
Nmap scan report for 192.168.1.246
Host is up (0.0023s 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:CE:D2:42 (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 2.48 seconds
```

8) sudo nmap -sV 192.18.1.246

scansione versione servizi

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:53 CET
Nmap scan report for 192.168.1.246
Host is up (0.0017s 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  tcpwrapped
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:CE:D2:42 (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 12.04 seconds
```


9) sudo nmap -F 192.168.1.246

scansione common 100 ports

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -F 192.168.1.246
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:57 CET
Nmap scan report for 192.168.1.246
Host is up (0.0010s 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:CE:D2:42 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

10)sudo nmap -F 192.168.1.246

scansione tramite ARP

```
(kali㉿kali)-[~]  
$ sudo nmap -PR 192.168.1.246  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 20:02 CET  
Nmap scan report for 192.168.1.246  
Host is up (0.00099s 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:CE:D2:42 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

9 e10) scansione con e senza ping

scansione con ping

nmap -sP 192.168.1.246

scansione senza ping

nmap -PN 192.168.1.246

```
(kali㉿kali)-[~]  
$ nmap -sP 192.168.1.246  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 20:31 CET  
Nmap scan report for 192.168.1.246  
Host is up (0.0032s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
```

```
(kali㉿kali)-[~]  
$ nmap -PN 192.168.1.246  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 20:32 CET  
Nmap scan report for 192.168.1.246  
Host is up (0.021s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
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 0.28 seconds
```

IP TARGET	OS	TIPO SCANSIONE	COMAN DO	PORTE APERTE	PORTE CHIUSE	MAC ADDRESS
192,168,1,246	METASPLOITABLE	TCP	nmap -sS	23	977	08:00:27:CE:D2:42
192,168,1,246	METASPLOITABLE	scansione completa	nmap -sV	23	977	08:00:27:CE:D2:42
192,168,1,246	METASPLOITABLE	output su file	nmap -sV -oN file.txt	23	977	08:00:27:CE:D2:42
192,168,1,246	METASPLOITABLE	scansione su pora	nmap -sS ip -p 8080	23	977	08:00:27:CE:D2:42
192,168,1,246	METASPLOITABLE	scansione tutte le porte	nmap -sS -p-	30	65505	08:00:27:CE:D2:42
192,168,1,246	METASPLOITABLE	scansione udp	nmap -sU -r -v	3		08:00:27:CE:D2:42
192,168,1,246	METASPLOITABLE	scansione sistema operativo	nmap -O	-	-	08:00:27:CE:D2:42
192,168,1,246	METASPLOITABLE	scansione versione servizi	nmap -sV	23	977	08:00:27:CE:D2:42
192,168,1,246	METASPLOITABLE	scansione common 100 ports	nmap -F	18	82	08:00:27:CE:D2:42
192,168,1,246	METASPLOITABLE	scansione ARP	nmap -PR	23	977	08:00:27:CE:D2:42