

Report Esercizio di Scansione Nmap

Introduzione

In questo esercizio andiamo ad utilizzare i vari comandi per effettuare una scansione con NMAP gli indirizzi IP di 3 macchine utilizzate in bridge in modo da utilizzare la stessa rete. Utilizziamo la macchina Kali Linux per utilizzare lo strumento NMAP. Nmap (Network Mapper) è lo strumento open source standard per l'esplorazione di rete e l'audit di sicurezza. Serve a scoprire quali dispositivi sono connessi a una rete e quali servizi stanno offrendo.

Nmap (Network Mapper) è universalmente riconosciuto come lo strumento open source di riferimento per l'esplorazione e l'analisi di sicurezza delle reti. Il suo scopo principale è identificare i dispositivi collegati a una rete e i servizi da essi esposti.

1. Dettagli del Report

Comando OS fingerprint Windows XP

Questo comando viene utilizzato per verificare la versione del sistema operativo riferito all'IP della macchina Windows XP:

```
(kali@kali)~$ nmap -O 192.168.1.155
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-06 10:39 -0500
Nmap scan report for 192.168.1.155
Host is up (0.0023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1 (95%), Microsoft Windows 2000 SP4 or Windows XP SP1a (95%), Microsoft Windows Server 2003 SP1 or SP2 or Windows XP SP1 (95%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows XP SP3 (92%), Microsoft Windows 2000 Server SP3 or SP4 (92%)
No exact OS matches for host (test conditions non-ideal).
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 11.82 seconds

(kali@kali)~$
```

Comando OS fingerprint Metasploitable

Stesso discorso per quanto riguarda il comando applicato all'indirizzo IP della macchina Metasploitable:

```
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: 08:00:27:32:78:F3 (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
```

Comando Syn Scan Metasploitable

Il seguente comando invece viene eseguito per verificare lo stato delle porte relative la macchina oggetto di analisi tramite la scansione hand-open, che invia pacchetti SYN attendendo in risposta pacchetti SYN/ACK, differente dal 3-way-handshake:

```
└─$ nmap -sS 192.168.1.96
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-06 11:17 -0500
Nmap scan report for 192.168.1.96
Host is up (0.00042s 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: 08:00:27:32:78:F3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.43 seconds

(kali㉿kali)-[~]
└─$
```

Comando TCP Connect Scan Metasploitable

Il seguente comando serve per effettuare una scansione tramite pacchetti TCP, quindi utilizzando il processo 3-way-handshake:

```

└─$ nmap -sT 192.168.1.96
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-06 11:20 -0500
Nmap scan report for 192.168.1.96
Host is up (0.0055s 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
MAC Address: 08:00:27:32:78:F3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds

(kali㉿kali)-[~]
└─$

```

Differenze comandi: Syn Scan e TCP Connect Scan

La differenza sta tutta nel Three-Way Handshake del protocollo TCP e nei permessi che si hanno quando si lancia l'attacco sulla macchina da cui lanci l'attacco. Per quanto riguarda il comando Syn Scan, Nmap invia un pacchetto SYN (come se volesse iniziare una connessione) se la porta è aperta, il bersaglio risponde SYN/ACK. A questo punto, invece di completare la connessione con un ACK, Nmap invia immediatamente un RST (Reset) per interrompere la comunicazione.

I vantaggi della Scansione Nmap includono una maggiore velocità, poiché richiede un minor scambio di pacchetti quindi il dispositivo attaccante è reso meno individuabile, essendo più difficile che venga rilevata nei log delle applicazioni del bersaglio, anche se i firewall moderni siano comunque in grado di intercettarla. Uno svantaggio è che questo comando richiede privilegi di sistema poiché Nmap deve creare pacchetti "grezzi" (raw sockets), bypassando il normale funzionamento del sistema operativo.

TCP Connect Scan è la scansione di "ripiego" che Nmap usa quando non sei root. Nmap chiede al sistema operativo locale di stabilire una connessione completa con il

bersaglio; Dunque invia pacchetti SYN, riceve pacchetti SYN/ACK e completa la connessione inviando pacchetti ACK.

Ovviamente la scansione risulta più “rumorosa” perchè viene rilevata come connessione effettiva dai log di sistema, completando il ciclo di connessione TCP. Ovviamente dovendo completare la connessione risulta anche più lenta per una questione numerica di pacchetti.

Comando Version Detection Metasploitable

Questo comando esegue, oltre ad effettuare la scansione, una richiesta di versioni dei servizi in riferimento alle porte presenti:

```
L$ nmap -sV 192.168.1.96
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-06 12:04 -0500
Nmap scan report for 192.168.1.96
Host is up (0.0013s 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 rshexecd
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: 08:00:27:32:78:F3 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
ux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.43 seconds
```