

NMAP

Traccia: Traccia: Tecniche di scansione con Nmap 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.

E la seguente sul target Windows:

- OS fingerprint.

Oggi abbiamo imparato a conoscere il programma NMAP, uno strumento utile per la scansione e mappatura delle reti identificando le porte aperte, i dispositivi connessi, i servizi attivi e le vulnerabilità. E' spesso utilizzato in ambito di sicurezza informatica.

OS Fingerprint

Il primo comando che andremo ad analizzare sarà il comando OS Fingerprint, viene utilizzato su NMAP per identificare il sistema operativo di un dispositivo utilizzando l'indirizzo IP, ne analizza le risposte ricevute dai pacchetti inviati e confronta le informazioni con un database di firme di sistemi operativi conosciuti. Il comando che si utilizza sarà:

`nmap -O [indirizzo IP]`

Qui lo abbiamo utilizzato inviando il comando dalla macchina Kali Linux, indirizzandolo alla macchina Metasploitable2.

```
(root@kali) ~# nmap -O 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:43 EDT
Nmap scan report for 192.168.1.246
Host is up (0.00091s 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: 08:00:27:0F:42:61 (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 1.61 seconds
```

Ciò che ci andrà a mostrare le informazioni rilevate tra cui l'elenco delle porte aperte, e nelle righe finali ci rivelerà quale è il sistema operativo della macchina Metasploitable2 presa in esame, ovvero Linux.

Syn Scan

Il secondo comando che siamo andati ad eseguire è il Syn Scan, ovvero una scansione meno invasiva, basata sul protocollo TCP, ma che non porta a termine il 3-hand-shake, limitandosi ad eseguire solo i primi 2 passaggi (Syn e Syn/Ack) per assicurarsi che la porta sia aperta. Il comando che verrà avviato sarà:

nmap -sS [indirizzo IP]

Questo tipo di scansione è più rapida e meno rilevabile dai firewall e sistemi di rilevamento delle intrusioni.

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:44 EDT
Nmap scan report for 192.168.1.246
Host is up (0.00027s 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: 08:00:27:0F:42:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

TCP Connect

Il terzo comando che andremo ad eseguire sarà il TCP Connect. Funziona in maniera analoga al Syn Scan, ma a differenza di questo, andrà a completare il 3-way-handshake in tutto e per tutto. Consente una analisi più completa delle porte aperte in quanto riesce a completare l'invio dei pacchetti. Il comando utilizzato è:

nmap -sT [indirizzo IP]

Rispetto a Syn Scan, questo metodo di scansione è facilmente rilevabile dal firewall o da sistemi di rilevamento delle intrusioni.

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:46 EDT
Nmap scan report for 192.168.1.246
Host is up (0.0018s 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: 08:00:27:0F:42:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Version Detection

L'ultimo comando che andremo a vedere è Version Detection, questo comando serve ad identificare i servizi in esecuzione sulle porte aperte di un host, inviando richieste specifiche ai servizi e analizzando le risposte ricevute per identificare le porte aperte e le applicazioni e versioni specifiche attive su di esse. Il comando eseguito sarà:

nmap -sV [indirizzo IP]

L'obiettivo di questo comando è quello di identificare le vulnerabilità e mappare la rete in maniera efficiente tramite un report dettagliato.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:03 EDT
Stats: 0:01:57 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 10:05 (0:00:05 remaining)
Stats: 0:02:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 10:05 (0:00:06 remaining)
Stats: 0:02:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 10:05 (0:00:06 remaining)
Nmap scan report for 192.168.1.246
Host is up (0.00072s 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?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry?
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: 08:00:27:0F:42:61 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.34 seconds
```

OS Fingerprint su Windows

Infine siamo andati ad eseguire il comando OS Fingerprint anche sulla macchina reale Windows per testarne l'efficacia.

Recuperando l'indirizzo IP della macchina reale siamo andati ad eseguire nuovamente il comando OS Fingerprint. L'output che ne abbiamo ottenuto è il seguente:

```
(root@kali)-[/home/kali]
# nmap -O 192.168.1.14

Nmap scan report for 192.168.1.14
Host is up (0.00042s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE      SERVICE
43/tcp    filtered  whois
49/tcp    filtered  tacacs
135/tcp   open       msrpc
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
MAC Address: 18:93:41:8B:CF:4F (Unknown)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
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 954.66 seconds
```

Nelle righe finali il report rileverà un sistema operativo Microsoft Windows 10, con aperte le porte 135, 139, 445, con le porte 43 e 49 aperte, ma con restrizioni.