S5E2

Nmap

Che cosa è Nmap?

Nmap (Network Mapper) è uno strumento open-source estremamente potente e versatile per la scansione della rete e l'identificazione dei dispositivi e dei servizi. Le sue funzionalità principali includono:

- Scansione degli Host: Identifica gli host attivi all'interno di una rete.
- Identificazione dei Servizi: Rileva i servizi in esecuzione su ciascun host, inclusi i numeri di porta e i protocolli.
- Rilevamento dei Sistemi Operativi: Utilizza varie tecniche di fingerprinting per determinare il sistema operativo in esecuzione su un host.
- Scansione delle Vulnerabilità: Può essere utilizzato per identificare potenziali vulnerabilità nei dispositivi e nei servizi rilevati.

Vediamo alcuni dei comandi più comuni che possiamo utilizzare e le situazioni in cui possono essere applicati. Prima di approfondire i comandi, è utile capire la differenza tra pacchetti raw e non raw.

Pacchetti raw

I pacchetti raw sono pacchetti di dati che vengono creati e manipolati a un livello molto basso, direttamente a livello del protocollo di rete. Utilizzando pacchetti raw, Nmap ha il pieno controllo su tutti gli aspetti del pacchetto, inclusi i campi dell'intestazione IP, i campi TCP/UDP, e i dati del payload. Questo permette a Nmap di eseguire scansioni molto precise e personalizzate, come la scansione SYN, FIN, che spesso vengono utilizzate per eludere firewall e sistemi di rilevamento delle intrusioni (IDS).

Pacchetti non raw

I pacchetti non raw sono pacchetti che vengono generati e gestiti attraverso le normali API di sistema, utilizzando le funzioni di rete standard fornite dal sistema operativo. Quando Nmap utilizza pacchetti non raw, si affida al sistema operativo per creare e inviare i pacchetti, come nel caso di una scansione TCP Connect.

Esercizio pratico

Si richiede 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.

Metasploitable

Per raggiungere il nostro obbiettivo possiamo percorrere due strade. Il primo comando che andrò a utilizzare ci darà tutte le informazioni che desideriamo, ma per fare ciò impiegherà più tempo e sarà più ‘rumoroso’.
Il secondo approccio invece sarà l’utilizzare più comandi per raggiungere le informazioni di cui abbiamo bisogno. Questo approccio sarà decisamente più discreto e ogni comando verrà svolto molto più velocemente.

Procedimento numero 1 comando: nmap -A -T4 192.168.1.161

Come si può notare dalle immagini con il primo comando abbiamo già ricevuto tutte le informazioni di cui avevamo bisogno.
Questa pratica è estremamente potente ma anche estremamente ‘rumorosa’, infatti consiglio di utilizzarla in caso l’azienda a cui stiamo facendo il pentesting ci abbia chiesto un pentesting in whitebox, oppure abbia dispositivi poco performanti.

```
┌──(root㉿christian)-[/home/christian/Scrivania]
└─# nmap -A -T4 192.168.1.161
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-29 14:08 CET
Nmap scan report for 192.168.1.161
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.75
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-date: 2024-10-24T17:38:23+00:00; -4d19h31m02s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing ou
tside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DS
N
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      44963/tcp   mountd
|   100005  1,2,3      52457/udp   mountd
|   100021  1,3,4      33114/udp   nlockmgr
|   100021  1,3,4      34241/tcp   nlockmgr
|   100024  1          53377/tcp   status
|_  100024  1          59755/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 21
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, LongColumnFlag, ConnectWithDatabase, SupportsCompression, Supp
ortsTransactions, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: Nb%0_m(|\8A}rGJ}VumA
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing ou
tside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-10-24T17:38:23+00:00; -4d19h31m02s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=10/29%OT=21%CT=1%CU=39299%PV=Y%DS=2%DC=T%G=Y%TM=6720DE
OS:85%P=aarch64-unknown-linux-gnu)SEQ(SP=C9%GCD=1%ISR=CC%TI=Z%CI=Z%II=I%TS=
OS:7)SEQ(SP=C9%GCD=1%ISR=CC%TI=Z%II=I%TS=7)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW
OS:5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%
OS:W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=N%T=40%W=16D0%O=M5B4N
OS:NSNW5%CC=N%Q=)T1(R=Y%DF=N%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=
OS:Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T4(R=N)T5(R=Y%DF=N%T=40%W=0%S=Z%A
OS:=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T6(R=N)T
OS:7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=D228%RUD=G
OS:)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -4d18h31m02s, deviation: 2h00m00s, median: -4d19h31m02s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
```

```
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-10-24T13:38:13-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 199/tcp)
HOP RTT     ADDRESS
1   0.41 ms 192.168.64.1
2   0.83 ms 192.168.1.161

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.36 seconds
```

Procedimento numero 2
Con il secondo procedimento andrò a richiedere comando per comando le informazioni di cui ho bisogno, noteremo che in questo caso riceveremo le informazioni più velocemente ma al contempo saranno meno dettagliate.
Sistema operativo comando: nmap -O 192.168.1.161

```
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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=10/29%OT=21%CT=1%CU=34465%PV=Y%DS=2%DC=I%G=Y%TM=6720E4
OS:7C%P=aarch64-unknown-linux-gnu)SEQ(SP=CB%GCD=1%ISR=CE%TI=Z%CI=Z%II=I%TS=
OS:7)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5=M5
OS:B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A
OS:0)ECN(R=Y%DF=N%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=N%T=40%S=O%A=S
OS:+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=
OS:)T5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=40%W=0%S=A%
OS:A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIP
OS:CK=G%RUCK=99A3%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.31 seconds
```

Nella figura si può notare come le informazioni siano decisamente meno dettagliate. In questo caso abbiamo avuto in risposta il ping e la richiesta delle porte che già erano all'interno del pacchetto base di nmap, in più abbiamo ottenuto anche delle informazioni sul sistema operativo.

Syn Scan comando: nmap -sS 192.168.1.161

```
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 0.26 seconds
```

Nell'immagine si nota come con il comando '-sS' abbiamo richiesto uno Scan delle porte semplicemente con la richiesta SYN, facendo ciò abbiamo uno Scan più veloce e silenzioso.

TCP connect comando: nmap -sT 192.168.1.161

```
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 0.18 seconds
```

Come si nota in figura in questo caso abbiamo utilizzato un comando Scan porte ma con una richiesta completa, SYN, SYN/ACK, ACK. Questo sistema è tecnicamente più lento e più rumoroso.

Version Detection comando: nmap -sV 192.168.1.161

```
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
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 11.81 seconds
```

Con questo comando andiamo a utilizzare il Banner Grabbing.
Il Banner ci permette di visualizzare le versioni dei protocolli attivi.

Windows 7

Anche qui possiamo utilizzare le due strade citate prima per ricevere informazioni sul sistema operativo. Essendo che la macchina virtuale è di nostra proprietà utilizzerò il comando **-A -T4 192.168.1.67** per ricevere più informazioni possibili.

```
Network Distance: 2 hops
Service Info: Host: CHRI-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -20m00s, deviation: 34m38s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: CHRI-PC, NetBIOS user: <unknown>, NetBIOS MAC: ae:2d:05:19:61:bc (unknown)
| smb2-time:
|   date: 2024-10-29T14:24:25
|_  start_date: 2024-10-29T13:17:18
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: chri-PC
|   NetBIOS computer name: CHRI-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-10-29T15:24:25+01:00

TRACEROUTE (using port 256/tcp)
HOP RTT     ADDRESS
1   0.40 ms 192.168.64.1
2   1.01 ms 192.168.1.67

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.84 seconds
```