

Progetto settimanale nmap sS

Nmap è un port scanner che oggi utilizzeremo per vedere e scansionare le eventuali vulnerabilità. Il primo metodo che andremo a usare è sS:

sS è un metodo di scan poco invasivo e che sta per Syn Scan, una volta ricevuto un pacchetto syn/ack della macchina target, non conclude il 3 way handshake.

Con il comando -p andiamo a scansionare in dettaglio le porte. La scansione la iniziamo a fare con: `nmap -sS 192.168.50.101 -p 1-1024`, dopo che viene lanciato il comando ci viene mostrato un report della scansione fatta sull'indirizzo ip che abbiamo impostato. Sotto troviamo PORT, STATE e SERVICE:

PORT ci fa vedere le porte e il rispettivo numero.

STATE ci mostra se le porte sono aperte.

SERVICE ci mostra i servizi.

I servizi che troviamo sono:

Ftp: Sta per file transfer protocol, si usa per trasferire file su internet.

Ssh: Sta per Sicure Shell ci fa stabilire una sessione remota cifrata tramite interfaccia a riga di comando con un altro host.

Telnet: Sta per Terminal Network ed è un protocollo utilizzato per fornire all'utente sessioni di login remoto.

Smtp: E' l'acronimo di Simple Mail Transfer Protocol, si tratta di un protocollo per trasferire le email verso i server di posta elettronica.

Domain : Dominio.

HTTP: Sta per hypertext transfer protocol.

La scansione che abbiamo fatto ci ha mostrato diversi valori che poi andremo a vedere con le catture di Wireshark.

Wireshark è uno strumento di analisi della rete potente e allo stesso tempo versatile: consente di tenere sott'occhio tutto ciò che accade nella propria rete e prendere le adeguate contromisure nel caso in cui qualcosa non vada per il verso giusto, ci permette di filtrare i pacchetti dati in tempo reale, ottenendo la visualizzazione delle sole informazioni che interessano oppure di eseguire una "scrematura" a posteriori.

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.50.101 -p 1-1024
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 14:11 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 1012 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
MAC Address: 16:FE:53:6E:26:5A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

Progetto settimanale nmap sS

Questa è una scansione con Wireshark che evidenzia quello che abbiamo fatto con Nmap usando il metodo sSc.

In questo caso possiamo vedere come inizia un processo tre way hand shake, ma vediamo che l'unico pacchetto inviato è [Syn], qui non si è concluso il tre wayhandshake.

37	14.239165215	192.168.50.100	192.168.50.101	TCP	58 63175 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=
38	14.239168465	192.168.50.100	192.168.50.101	TCP	58 63175 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=
39	14.239170798	192.168.50.100	192.168.50.101	TCP	58 63175 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=
40	14.239173923	192.168.50.100	192.168.50.101	TCP	58 63175 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=
41	14.239189548	192.168.50.100	192.168.50.101	TCP	58 63175 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=
42	14.239196381	192.168.50.100	192.168.50.101	TCP	58 63175 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=
43	14.239201465	192.168.50.100	192.168.50.101	TCP	58 63175 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=
44	14.239213631	192.168.50.100	192.168.50.101	TCP	58 63175 → 810 [SYN] Seq=0 Win=1024 Len=0 MSS=
45	14.239222006	192.168.50.100	192.168.50.101	TCP	58 63175 → 90 [SYN] Seq=0 Win=1024 Len=0 MSS=
46	14.252927756	192.168.50.101	192.168.50.100	TCP	58 25 → 63175 [SYN, ACK] Seq=0 Ack=1 Win=5840
47	14.253384506	192.168.50.100	192.168.50.101	TCP	54 63175 → 25 [RST] Seq=1 Win=0 Len=0
48	14.254110173	192.168.50.101	192.168.50.100	TCP	54 256 → 63175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	14.254110923	192.168.50.101	192.168.50.100	TCP	58 80 → 63175 [SYN, ACK] Seq=0 Ack=1 Win=5840
50	14.254110965	192.168.50.101	192.168.50.100	TCP	54 143 → 63175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
51	14.254111006	192.168.50.101	192.168.50.100	TCP	58 23 → 63175 [SYN, ACK] Seq=0 Ack=1 Win=5840
52	14.254111048	192.168.50.101	192.168.50.100	TCP	58 53 → 63175 [SYN, ACK] Seq=0 Ack=1 Win=5840
53	14.254111090	192.168.50.101	192.168.50.100	TCP	54 554 → 63175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
54	14.254190798	192.168.50.100	192.168.50.101	TCP	54 63175 → 80 [RST] Seq=1 Win=0 Len=0
55	14.254218673	192.168.50.100	192.168.50.101	TCP	54 63175 → 23 [RST] Seq=1 Win=0 Len=0
56	14.254221298	192.168.50.100	192.168.50.101	TCP	54 63175 → 53 [RST] Seq=1 Win=0 Len=0
57	14.254755798	192.168.50.101	192.168.50.100	TCP	54 443 → 63175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	14.254755923	192.168.50.101	192.168.50.100	TCP	54 199 → 63175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Ma ci da conferma che la porta è aperta e questo c'è lo dice Syn/Ack (a riga 46), ma la macchina del target ci risponde con RST e RST/ACK e ci dice che la porta è chiusa.

Progetto settimanale nmap sT

sT é il metodo di scansione più invasivo, per controllare se una porta è aperta o meno, nmap sT va a completare tutti i passaggi del 3 ways handshake stabilendo di fatto un canale a differenza di sS che chiude la connessione prima.

La scansione sul terminale riporta gli stessi elementi che abbiamo riscontrato sulla scansione precedente , come : ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, microsoft-ds, exec, login, e Shell.

Ma la differenza la potremmo vedere solo sulla scansione fatta da Wireshark dove ci verrà mostrato esattamente cos'è andato a fatto durante la scansione.

```
(root@kali)~[/home/kali]
# nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 14:29 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0023s latency).
Not shown: 1012 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
MAC Address: 16:FE:53:6E:26:5A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

sT

Con la cattura di Wireshark possiamo vedere come i pacchetti Syn, Syn/Ack e Ack vengono inviati completando il tre way handshake, stabilendo il canale, che poi viene interrotto da Rst, Ack, chiudendo la porta.

25	10.115041130	192.168.50.100	192.168.50.101	TCP	74 56036 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=
26	10.115079630	192.168.50.100	192.168.50.101	TCP	74 41622 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
27	10.115096713	192.168.50.100	192.168.50.101	TCP	74 40988 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=
28	10.115104047	192.168.50.100	192.168.50.101	TCP	74 46574 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=
29	10.115110797	192.168.50.100	192.168.50.101	TCP	74 35304 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=
30	10.117387255	192.168.50.101	192.168.50.100	TCP	74 21 → 33946 [SYN, ACK] Seq=0 Ack=1 Win=5792
31	10.117987713	192.168.50.100	192.168.50.101	TCP	66 33946 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0
32	10.118287505	192.168.50.100	192.168.50.101	TCP	66 33946 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
33	10.118469130	192.168.50.100	192.168.50.101	TCP	74 43872 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=
34	10.118547213	192.168.50.100	192.168.50.101	TCP	74 38004 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=
35	10.118845630	192.168.50.101	192.168.50.100	TCP	54 143 → 35172 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	10.118846172	192.168.50.101	192.168.50.100	TCP	54 110 → 60806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	10.118846422	192.168.50.101	192.168.50.100	TCP	54 135 → 46452 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	10.118846672	192.168.50.101	192.168.50.100	TCP	74 139 → 39532 [SYN, ACK] Seq=0 Ack=1 Win=5792
39	10.118846713	192.168.50.101	192.168.50.100	TCP	54 256 → 36078 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	10.118846797	192.168.50.101	192.168.50.100	TCP	74 53 → 34062 [SYN, ACK] Seq=0 Ack=1 Win=5792
41	10.118846922	192.168.50.101	192.168.50.100	TCP	74 23 → 46310 [SYN, ACK] Seq=0 Ack=1 Win=5792
42	10.118896547	192.168.50.100	192.168.50.101	TCP	66 39532 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0
43	10.118931838	192.168.50.100	192.168.50.101	TCP	66 34062 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0
44	10.118939463	192.168.50.100	192.168.50.101	TCP	66 46310 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0
45	10.118982505	192.168.50.101	192.168.50.100	TCP	54 993 → 56036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
46	10.118982620	192.168.50.101	192.168.50.100	TCP	74 80 → 41622 [SYN, ACK] Seq=0 Ack=1 Win=5792

-A

```

root@kali: /home/kali
File Azioni Modifica Visualizza Aiuto

Network Distance: 1 hop
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
  _smb2-time: Protocol negotiation failed (SMB2)
  _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)
  _clock-skew: mean: 1h59m58s, deviation: 2h49m42s, median: -1s
  smb-os-discovery:
    OS: Unix (Samba 3.0.20-Debian)
    Computer name: metasploitable
    NetBIOS computer name:
    Domain name: localdomain
    FQDN: metasploitable.localdomain
  _System time: 2022-07-22T08:34:52-04:00

TRACEROUTE
HOP RTT ADDRESS
1 3.55 ms 192.168.50.101

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 97.27 seconds

```

Con questa cattura possiamo vedere request e response, come si vede alla seconda/terza riga c'è la request alla ottava riga c'è la response. Anche se la macchina del target cerca di bloccare e chiudere la porta, rimane comunque aperta e l'invio dei pacchetti c'è lo stesso.

File Modifica Visualizza Vaj Cattura Analisi Statistiche Telefonia Wireless Strumenti Aiuto

Applica un filtro di visualizzazione ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3039	59.149922736	192.168.50.100	192.168.50.101	SMB	141	Tree Connect AndX Request, Path: \\192.168.50.101\
3040	59.149942695	192.168.50.100	192.168.50.101	FTP	72	Request: QUIT
3041	59.149945820	192.168.50.100	192.168.50.101	FTP	80	Request: PASS IEUser@
3042	59.150711736	192.168.50.101	192.168.50.100	TCP	66	21 → 33914 [ACK] Seq=59 Ack=17 Win=5888 Len=0 TSva
3043	59.170622195	192.168.50.101	192.168.50.100	SMB	116	Tree Connect AndX Response
3044	59.170643612	192.168.50.100	192.168.50.101	TCP	66	47096 → 445 [ACK] Seq=458 Ack=612 Win=64128 Len=0
3045	59.186840320	192.168.50.101	192.168.50.100	TCP	66	21 → 33920 [ACK] Seq=93 Ack=37 Win=5888 Len=0 TSva
3046	59.187307320	192.168.50.101	192.168.50.100	FTP	80	Response: 221 Goodbye.
3047	59.187322820	192.168.50.100	192.168.50.101	TCP	66	33914 → 21 [ACK] Seq=17 Ack=73 Win=64256 Len=0 TSv
3048	59.187670903	192.168.50.101	192.168.50.100	TCP	66	21 → 33914 [FIN, ACK] Seq=73 Ack=17 Win=5888 Len=0
3049	59.199880445	192.168.50.101	192.168.50.100	HTTP	71	HTTP/1.1 200 OK (text/html)
3050	59.199897612	192.168.50.100	192.168.50.101	TCP	66	41528 → 80 [ACK] Seq=215 Ack=1119 Win=64128 Len=0
3051	59.200177945	192.168.50.100	192.168.50.101	TCP	66	33914 → 21 [RST, ACK] Seq=17 Ack=74 Win=64256 Len=0
3052	59.200260737	192.168.50.100	192.168.50.101	TCP	74	37964 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
3053	59.200308028	192.168.50.100	192.168.50.101	SMB	215	Session Setup AndX Request, NTLMSSP_NEGOTIATE
3054	59.200795612	192.168.50.101	192.168.50.100	TCP	74	25 → 37964 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
3055	59.200818820	192.168.50.100	192.168.50.101	TCP	66	37964 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
3056	59.205638320	192.168.50.101	192.168.50.100	SMB	405	Session Setup AndX Response, NTLMSSP_CHALLENGE, Er
3057	59.205654195	192.168.50.100	192.168.50.101	TCP	66	47102 → 445 [ACK] Seq=203 Ack=471 Win=64128 Len=0
3058	59.247806070	192.168.50.101	192.168.50.100	TCP	66	80 → 41528 [FIN, ACK] Seq=1119 Ack=215 Win=6912 Le
3059	59.250204653	192.168.50.100	192.168.50.101	TCP	66	41528 → 80 [FIN, ACK] Seq=215 Ack=1120 Win=64128 L
3060	59.250322337	192.168.50.100	192.168.50.101	TCP	74	41532 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA

Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: 16:fe:53:6e:26:5a (16:fe:53:6e:26:5a)
 Sender IP address: 192.168.50.101
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

