

SCANSIONE TCP CON NMAP (sT)

- FONTE DELLO SCAN: METASPLOITABLE
- TARGET DELLO SCAN: porte 1-1024 (WELL KNOWN)
- TIPO DI SCAN: TCP

SVOLGIMENTO

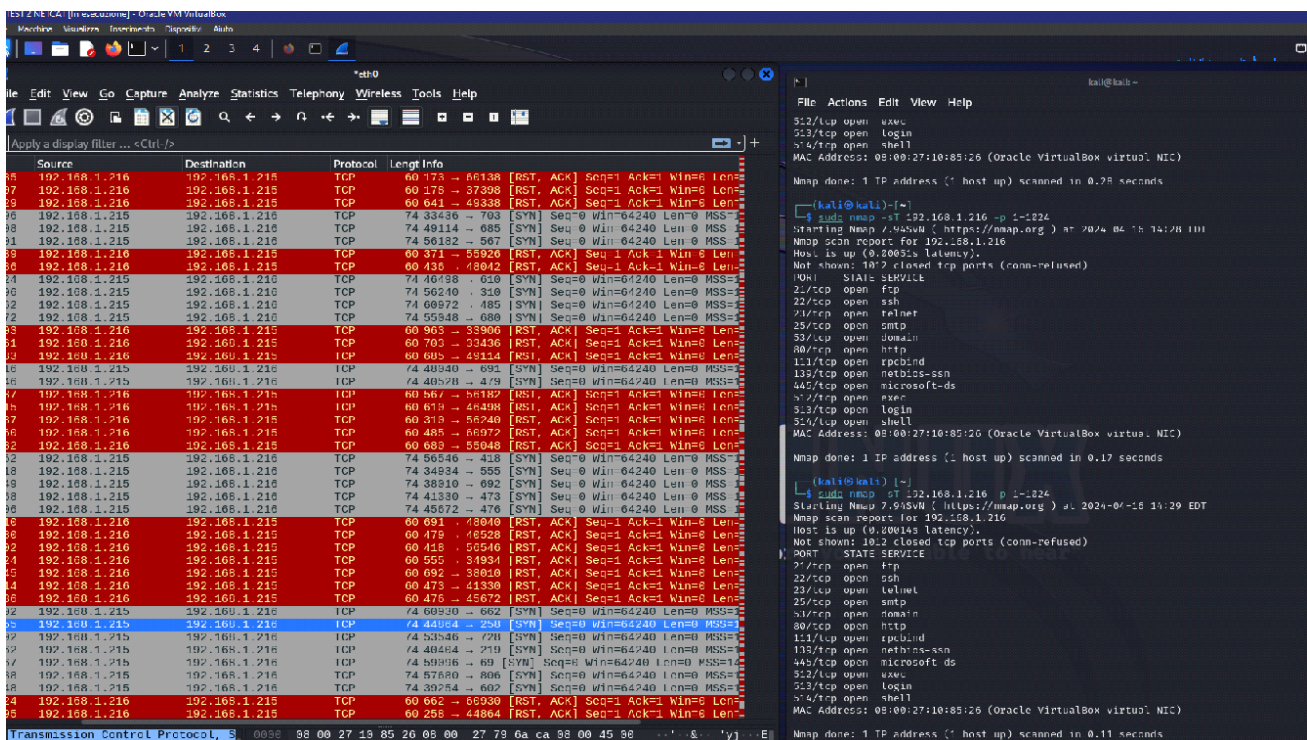
Utilizziamo il comando:

```
sudo nmap -sT 192.168.1.216 -p 1-1024
```

Effettuiamo lo scan delle porte e la rilevazione dell'invio di pacchetti mediante Wireshark.

Possiamo da subito vedere i risultati: per le porte chiuse, con lo scan sT la macchina target ci invierà dei pacchetti con i flag [RST, ACK].

Le porte aperte invece mostreranno un



SCANSIONE SYN CON NMAP

FONTE DELLO SCAN: METASPLOITABLE

TARGET DELLO SCAN: Porte 1-1024

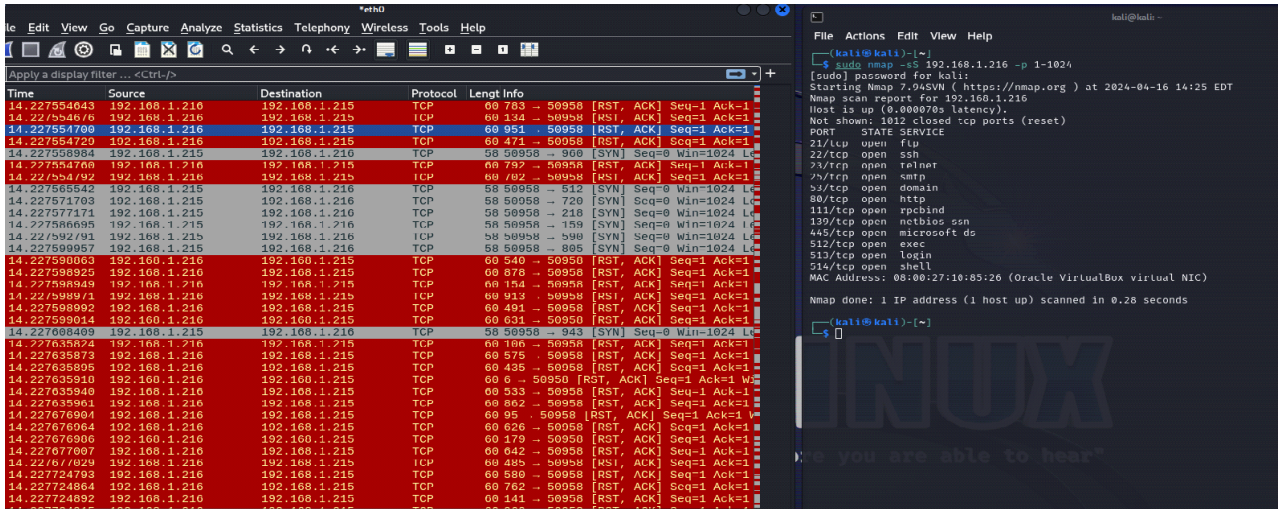
TIPO DI SCAN: SYN

SVOLGIMENTO

Utilizziamo il comando:

sudo nmap -sS 192.168.1.216 -p 1-1024

Avviamo la scansione con Wireshark. I pacchetti vengono catturati e mostrano le caratteristiche dello scan con il SYN.



-sS sono richieste dove il TCP handshake non viene concluso, ma viene inviato solamente il pacchetto SYN.

-I pacchetti con un [RST,ACK] segnalano che la porta è chiusa, e non ci sono servizi attivi.

- le porte aperte vengono segnalate con un pacchetto [SYN, ACK]. Tuttavia, poiché nella scansione SYN l'obiettivo è non portare a termine il 3way handshake, viene immesso un RST, ACK in modo da interromperlo.

167	1.291518972	192.168.1.216	192.168.1.215	TCP	60 993 → 53720 [RST, ACK] Seq=1
168	1.291518994	192.168.1.216	192.168.1.215	TCP	74 23 → 49918 [SYN, ACK] Seq=0
169	1.291519015	192.168.1.216	192.168.1.215	TCP	74 21 → 59988 [SYN, ACK] Seq=0
170	1.291519037	192.168.1.216	192.168.1.215	TCP	74 80 → 49830 [SYN, ACK] Seq=0
171	1.291519059	192.168.1.216	192.168.1.215	TCP	60 199 → 48002 [RST, ACK] Seq=1
172	1.291519081	192.168.1.216	192.168.1.215	TCP	60 110 → 51964 [RST, ACK] Seq=1
173	1.291519103	192.168.1.216	192.168.1.215	TCP	60 587 → 57448 [RST, ACK] Seq=1
174	1.291537242	192.168.1.215	192.168.1.216	TCP	66 39692 → 111 [ACK] Seq=1 Ack=
175	1.291563035	192.168.1.215	192.168.1.216	TCP	66 49918 → 23 [ACK] Seq=1 Ack=1
176	1.291571436	192.168.1.215	192.168.1.216	TCP	66 59988 → 21 [ACK] Seq=1 Ack=1
177	1.291577058	192.168.1.215	192.168.1.216	TCP	66 49830 → 80 [ACK] Seq=1 Ack=1
178	1.291587818	192.168.1.216	192.168.1.215	TCP	60 113 → 42186 [RST, ACK] Seq=1
179	1.291587843	192.168.1.216	192.168.1.215	TCP	74 53 → 35922 [SYN, ACK] Seq=0
180	1.291592421	192.168.1.215	192.168.1.216	TCP	66 35922 → 53 [ACK] Seq=1 Ack=1
181	1.291646227	192.168.1.215	192.168.1.216	TCP	66 39692 → 111 [RST, ACK] Seq=1
182	1.291697794	192.168.1.215	192.168.1.216	TCP	66 49918 → 23 [RST, ACK] Seq=1
183	1.291737983	192.168.1.215	192.168.1.216	TCP	66 59988 → 21 [RST, ACK] Seq=1
184	1.291778682	192.168.1.215	192.168.1.216	TCP	66 49830 → 80 [RST, ACK] Seq=1
185	1.291828992	192.168.1.215	192.168.1.216	TCP	66 35922 → 53 [RST, ACK] Seq=1

SCANSIONE CON SWITCH -A CON NMAP

- FONTE DELLO SCAN: METASPLOITABLE
- TARGET DELLO SCAN: porte 1-1024

- TIPO DI SCAN: TCP -A

SVOLGIMENTO

Effettuiamo lo scan con Nmap usando il comando:

sudo nmap -A 192.168.1.216 -p 1-1024

Lasciamo che Wireshark colga i pacchetti scansionati.

A differenza degli scan precedenti, il processo di scansione impiega maggiore tempo, portando con sé però numerose altre informazioni riguardanti le porte e il sistema scansionato.

Lo switch -A fornisce una visione molto più approfondita dello scan con Nmap.

- Viene fornito lo stato del server FTP.
- Viene fornito il nome del sistema operativo e della macchina analizzata (Unix - Metasploitable)
- Viene fornito il nome del dominio

```

$ sudo nmap -A 192.168.1.216 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 14:43 EDT
Nmap scan report for 192.168.1.216
Host is up (0.00021s latency).
Not shown: 1012 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 192.168.1.215
|_  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
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_RC4_128_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
|_ssl-date: 2024-04-16T18:43:59+00:00; +1s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=The
re is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_  program version    port/proto  service
|_  100003  2,3,4            2049/tcp   nfs
|_  100003  2,3,4            2049/udp   nfs
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
MAC Address: 08:00:27:10:85:26 (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
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
  _clock-skew: mean: 1h20m01s, deviation: 2h18m34s, median: 0s
  smb-os-discovery:
    OS: Unix (Samba 3.0.20-Debian)
    Computer name: metasploitable
    NetBIOS computer name:
    Domain name: localdomain
    FQDN: metasploitable.localdomain
    System time: 2024-04-16T14:43:51-04:00
  _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
HOP RTT      ADDRESS
1    0.21 ms  192.168.1.216

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 22.23 seconds

```

DIFFERENZE TRA TCP E SYN

La differenza tra scan TCP (-sT) e SYN (-sS) che possiamo verificare da queste analisi sta nel modo in cui la macchina si comporta a seconda della scansione.

Nel primo caso, i pacchetti effettuano il ciclo completo del 3way handshake, creando un rumore maggiore all'interno del network.

Per quanto riguarda il SYN scan, quando si rileva una porta aperta il ciclo viene interrotto volontariamente.