

Report esercitazione con Nmap W9D1

In questo esercizio useremo lo strumento Nmap dalla macchina Kali per eseguire delle scansioni sulla macchina Metasploitable2.

Prerequisiti:

Assicurarsi che le due macchine siano entrambe su rete interna e che possano comunicare tra di loro.

- Configurazione IP di Kali:

```
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255  
    inet6 fe80::a00:27ff:fe3e:18bd prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:3e:18:bd txqueuelen 1000 (Ethernet)  
    RX packets 3762 bytes 279118 (272.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 3984 bytes 297146 (290.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Configurazione IP di Metasploitable2:

```
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:ef:f5:ca  
          inet addr:192.168.32.105  Bcast:192.168.32.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:feef:f5ca/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:6058 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:5905 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:444304 (433.8 KB)  TX bytes:379718 (370.8 KB)  
          Base address:0xd020 Memory:f0200000-f0220000
```

Scansione TCP

La scansione TCP tramite Nmap si effettua tramite il comando `sudo nmap -sT <IP target> -p <range di porte>`, è una scansione invasiva perché stabilisce una connessione completa con il target, completando la three-way-handshake (syn, syn-ack, ack).

```
(kali@kali)-[~]  
$ sudo nmap -sT 192.168.32.105 -p 1-1024  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 11:29 EDT  
Nmap scan report for 192.168.32.105  
Host is up (0.0024s 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: 08:00:27:EF:F5:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
```

Scansione SYN

La scansione SYN è meno invasiva rispetto alla TCP in quanto è utilizzata per scoprire quali porte sono aperte sulla macchina target senza completare la three-way-handshake. Il comando per iniziare la scansione è `sudo nmap -sS <IP target> -p <range di porte>`.

```
(kali@kali)-[~]  
$ sudo nmap -sS 192.168.32.105 -p 1-1024  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 11:17 EDT  
Nmap scan report for 192.168.32.105  
Host is up (0.0065s 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: 08:00:27:EF:F5:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
```

Scansione con switch -A

È una delle scansioni più invasive, in quanto invia molte richieste, ma ci permette di recuperare molte informazioni sulla macchina target, come ad esempio la versione del sistema operativo, le porte aperte ed i servizi attivi su di esse.

```
(kali@kali)-[~]
$ nmap -A 192.168.32.105 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 11:33 EDT
Nmap scan report for 192.168.32.105
Host is up (0.0032s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 192.168.32.105
|_   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
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
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-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
8BITMIME, DSN
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
|_   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              38500/udp   mountd
|_   100005  1,2,3              57285/tcp   mountd
|_   100021  1,3,4              45911/tcp   nlockmgr
|_   100021  1,3,4              50463/udp   nlockmgr
|_   100024  1                   49414/tcp   status
|_   100024  1                   52262/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?
514/tcp   open  shell          Netkit rshd
MAC Address: 08:00:27:EF:F5:CA (PCS Systemtechnik/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:
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ clock-skew: mean: 2h00m05s, deviation: 2h49m51s, median: -1s
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ smb-os-discovery:
|_   OS: Unix (Samba 3.0.20-Debian)
|_   Computer name: metasploitable
|_   NetBIOS computer name:
|_   Domain name: localdomain
|_   FQDN: metasploitable.localdomain
|_   System time: 2025-04-25T11:34:56-04:00

TRACEROUTE
HOP RTT      ADDRESS
1   3.22 ms  192.168.32.105

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 99.69 seconds
```

Tabella riassuntiva delle scansioni

Tipo scansione	IP sorgente	IP target	Risultati scansione
TCP	192.168.32.100	192.168.32.105	12 porte aperte
SYN	192.168.32.100	192.168.32.105	12 porte aperte
Switch -A	192.168.32.100	192.168.32.105	12 porte aperte, servizi e versioni associati alle porte, info sul sistema operativo, traceroute

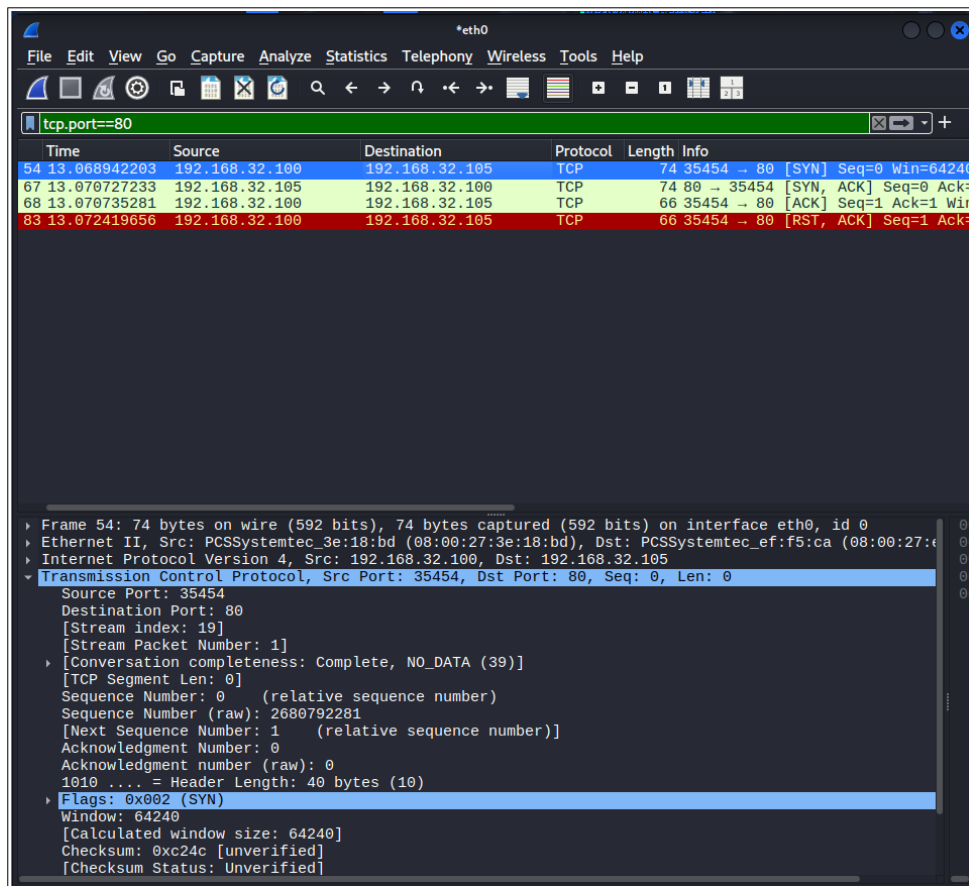
Facoltativo

Evidenziare le differenze tra scansione TCP e SYN tramite cattura di Wireshark.

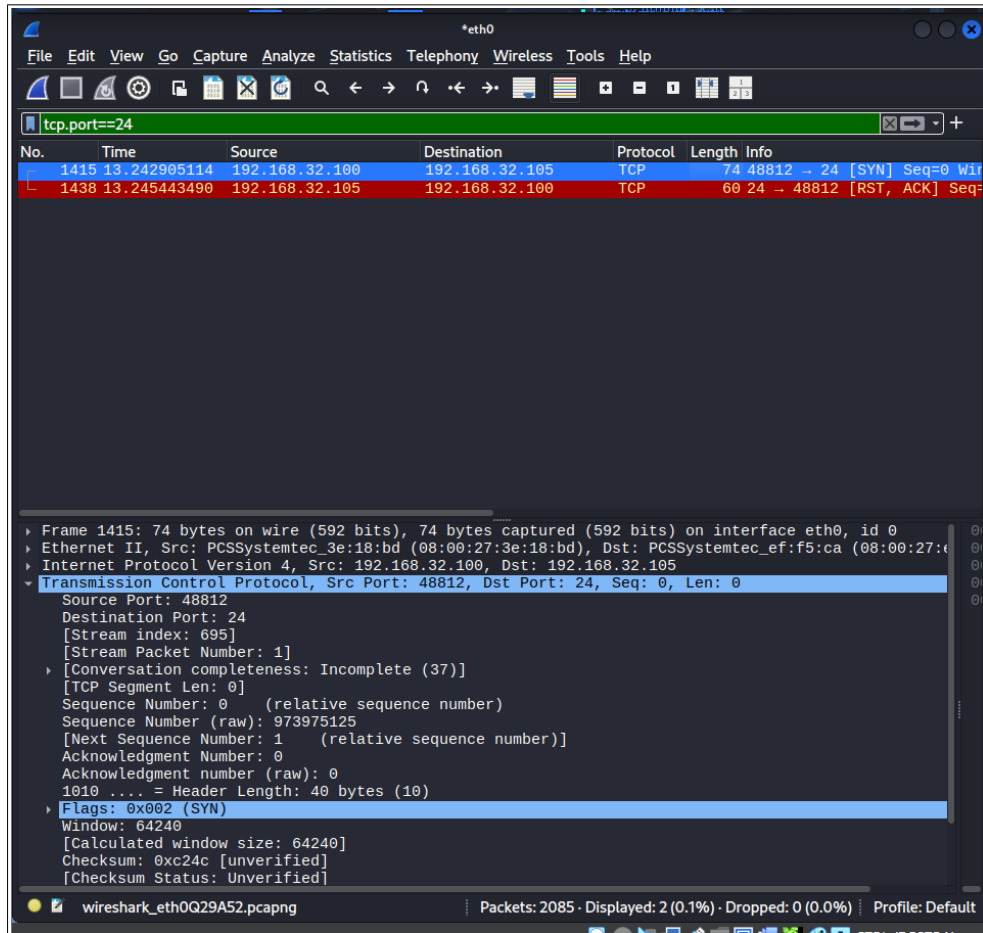
Scansione TCP

Tramite la cattura con Wireshark dei pacchetti possiamo notare come la connessione restituisca la sequenza della three-way-handshake [SYN, SYN-ACK, ACK], nelle porte che risultano aperte. Se la porta è chiusa restituisce la dicitura [RST, ACK].

Di seguito viene mostrata la scansione sulla porta 80 (servizio HTTP) e come si presenta la cattura in caso Nmap trovi una porta aperta.

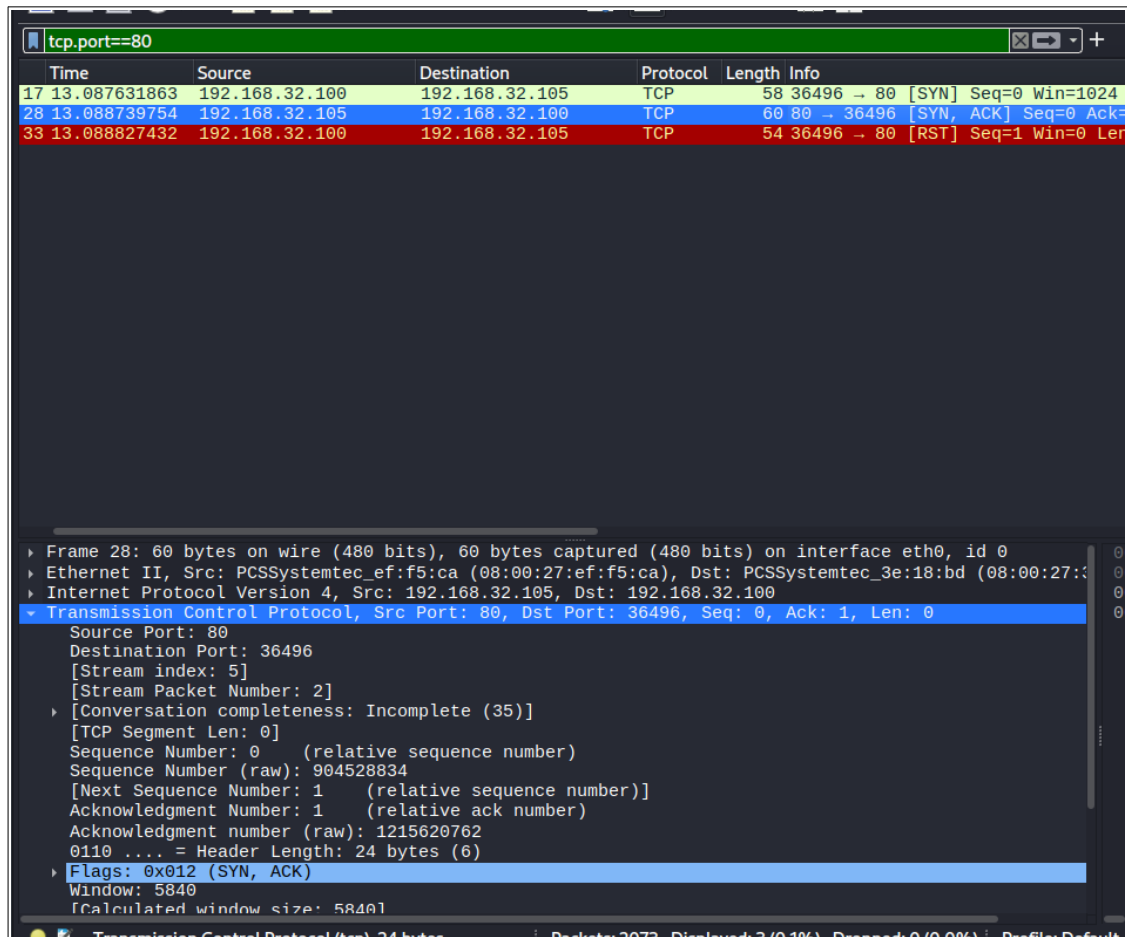


Qui sotto viene mostrata la scansione sulla porta 24 e che sappiamo essere chiusa, infatti non viene completata la three-way-handshake e subito dopo il tag [SYN], viene inviato il segnale [RST, ACK].



Scansione SYN

Mediante la cattura con Wireshark possiamo notare come, una volta trovata una porta aperta, non venga completata la three-way-handshake, in quanto subito dopo aver ricevuto il flag [SYN, ACK] la connessione viene interrotta e viene emesso il messaggio [RST].



Quando la scansione di Nmap trova una porta chiusa, come per TCP, invia il flag [RST,ACK]

