Traccia:

Vedremo da vicino nmap e i suoi comandi.
Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:

- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

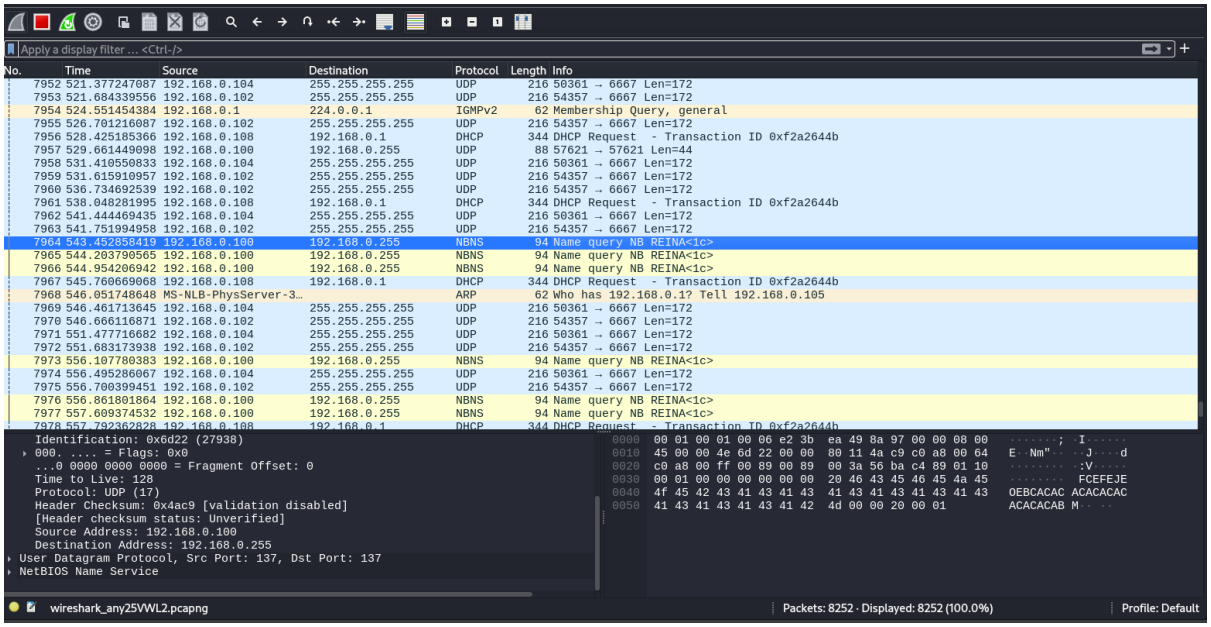
Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente con Wireshark.

La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alla macchine.
E' molto importante in questa fase essere organizzati e strutturati.
Dunque, per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report Excel / altro (tabella su word ad esempio) che riporti in maniera chiara:

- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -p 1-1023 192.168.0.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 16:54 EDT
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 16:54 (0:00:01 remaining)
Nmap scan report for 192.168.0.109 (192.168.0.109)
Host is up (0.0012s latency).
Not shown: 1011 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.108
|      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
|_ssl-date: 2024-04-16T20:55:52+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
```

```
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      35000/udp   mountd
|   100005  1,2,3      51916/tcp   mountd
|   100021  1,3,4      42181/udp   nlockmgr
|   100021  1,3,4      57196/tcp   nlockmgr
|   100024  1          35844/tcp   status
|_  100024  1          42338/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?
513/tcp open  login       OpenBSD or Solaris rlogind
514/tcp open  tcpwrapped
MAC Address: 08:00:27:B1:7C:1D (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:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-04-16T16:55:43-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h19m58s, deviation: 2h18m34s, median: -1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```



SWITCH -A

Con la scansione con lo switch –A fornisce più informazioni sul target.

Rileva le versioni dei servizi in esecuzione sulle porte aperte.

Rileva il sistema operativo e l'hardware del target.

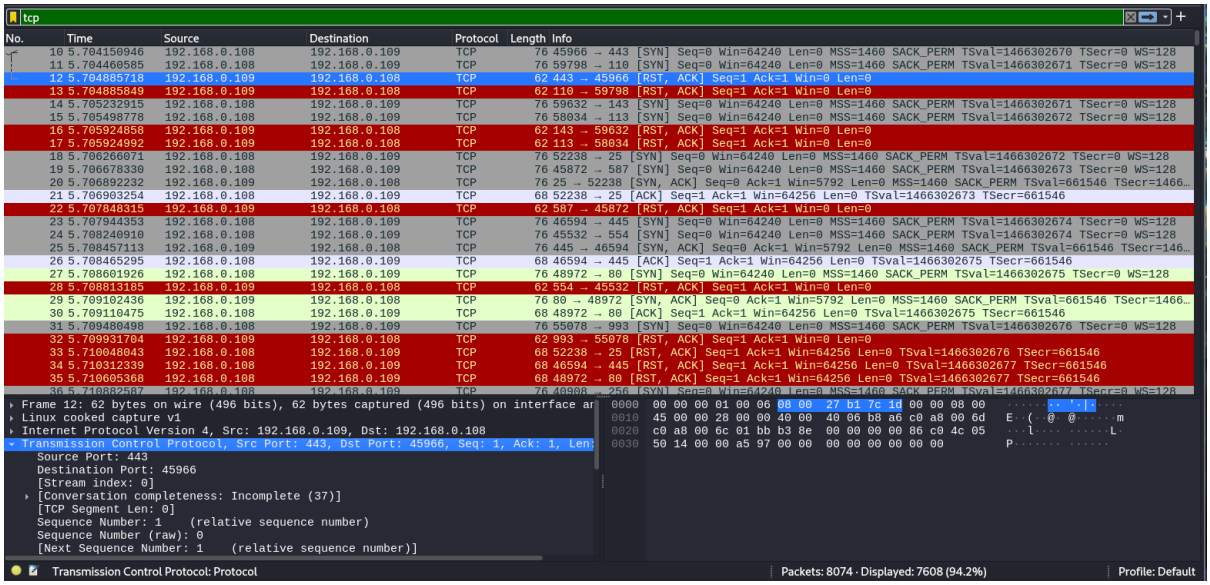
Esegue degli script di Nmap Scripting Engine per avere informazioni su vulnerabilità potenzialmente note.

Esegue il tracciamento dei pacchetti verso il target per determinarne il percorso.

Comando:

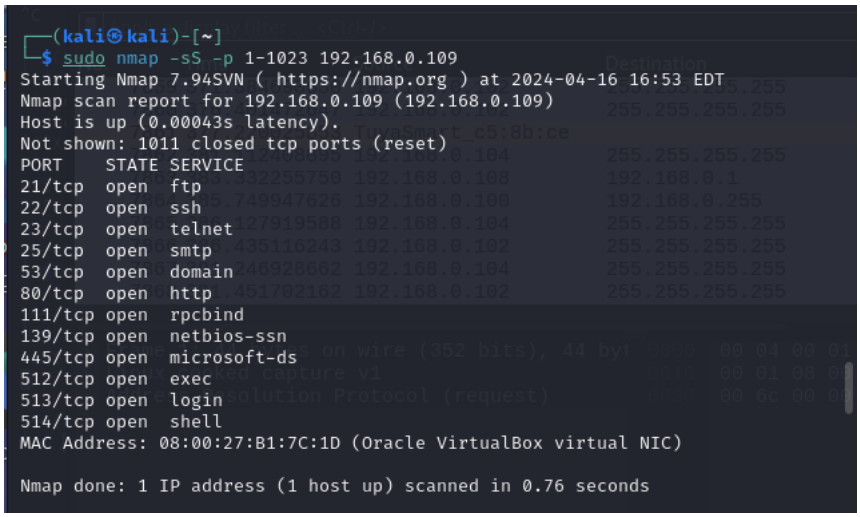
sudo nmap –A –p 1-1023 [Indirizzo IP]

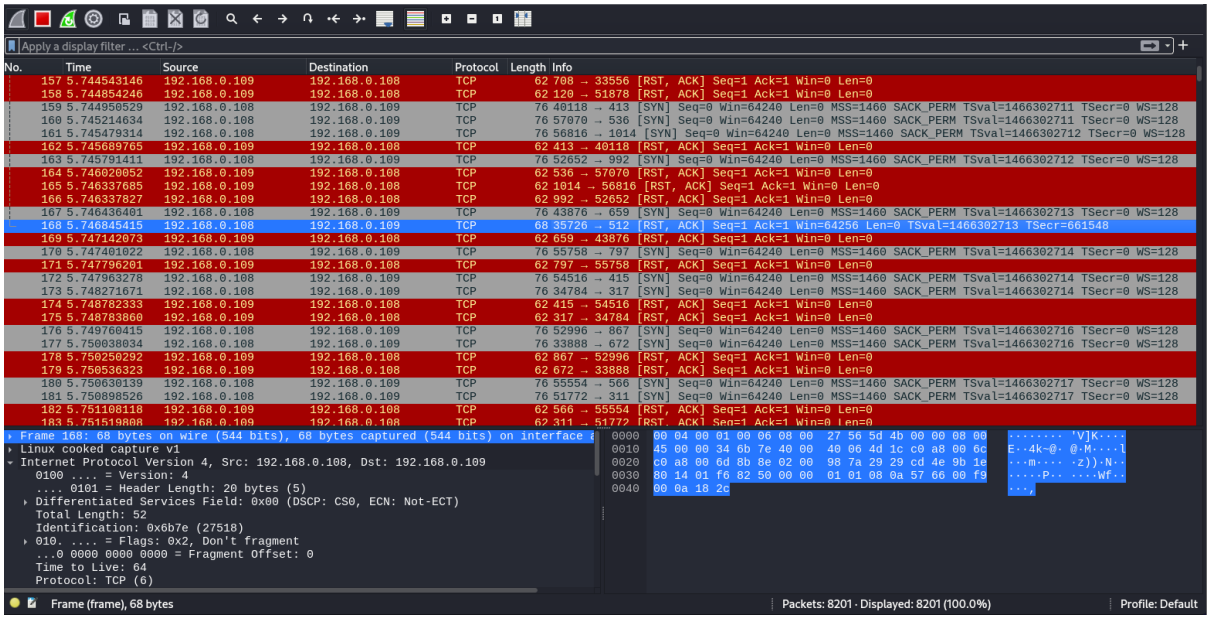
```
└─$ sudo nmap -sT -p 1-1023 192.168.0.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 16:51 EDT
Nmap scan report for 192.168.0.109 (192.168.0.109)
Host is up (0.0026s latency).
Not shown: 1011 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  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:B1:7C:1D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```



TCP

Con la scansione TCP si posso identificare le porte aperte su un Host di rete.
Mappa le reti per determinare quali servizi sono in esecuzione su quali porte
Identifica potenziali punti di ingresso vulnerabili su una rete o un sistema.
Crea un elenco delle risorse di rete, server e dispositivi e i servizi che offrono.
Rileva la versione dei servizi in esecuzione.
Identifica il sistema operativo e l'hardware.
Comando:
sudo nmap –sT –p 1-1023 [indirizzo ip]





SYN

Con la scansione SYN si possono identificare rapidamente le porte aperte su un host di rete senza completare l'handshake TCP. E' una scansione più difficile da rilevare dai sistemi di rilevamento intrusioni o firewall.

La scansione SYN è più veloce rispetto ad altre scansioni perchè non stabilisce una connessione completa.

Non completando l'handshake TCP è meno probabile che venga registrata nei log dei server.

Fornisce risultati affidabili sullo stato delle porte.

Se riceve un pacchetto SYN/ACK significa che la porta è aperta.

Se riceve un pacchetto RST (reset) la porta è chiusa.

Se non riceve risposta la porta potrebbe essere protetta da un firewall.

Comando:

sudo nmap –sS –p 1-1023 [indirizzo ip]

Scansione della domotica collegata:

```
8358 1169.5717532… TuyaSmart_c5:8b:ce                                ARP      62 Who has 192.168.0.1? Tell 192.168.0.104
8359 1171.0154964… 192.168.0.108          192.168.0.1                DHCP    344 DHCP Request  - Transaction ID 0xf2a2644b
8360 1172.6429885… 192.168.0.104          255.255.255.255            UDP     216 50361 → 6667 Len=172
8361 1172.8478024… 192.168.0.102          255.255.255.255            UDP     216 54357 → 6667 Len=172
8362 1177.7503155… 192.168.0.100          192.168.0.255              UDP      88 57621 → 57621 Len=44
8363 1177.8645892… 192.168.0.102          255.255.255.255            UDP     216 54357 → 6667 Len=172
8364 1182.8816822… 192.168.0.102          255.255.255.255            UDP     216 54357 → 6667 Len=172
8365 1187.4280943… 192.168.0.108          192.168.0.1                DHCP    344 DHCP Request  - Transaction ID 0xf2a2644b
8366 1187.6937041… 192.168.0.104          255.255.255.255            UDP     216 50361 → 6667 Len=172
8367 1188.0003714… 192.168.0.102          255.255.255.255            UDP     216 54357 → 6667 Len=172
8368 1191.5065237… AmazonTechno_e6:db:80                             ARP      62 Who has 192.168.0.100? Tell 192.168.0.101
```

Rilevamento nome utente dell'hardware:

```
8221 944.650790502 TpLinkTechno_f4:ce:…                    ARP      62 Who has 192.168.0.100? Tell 192.168.0.1
8222 944.847830292 192.168.0.100          192.168.0.255    NBNS     94 Name query NB REINA<1c>
8223 945.599561923 192.168.0.100          192.168.0.255    NBNS     94 Name query NB REINA<1c>
8224 946.350073772 192.168.0.100          192.168.0.255    NBNS     94 Name query NB REINA<1c>
```

Scansione macchina virtuale:

```
8171 867.129048573 192.168.0.104          255.255.255.255  UDP     216 50361 → 6667 Len=172
8172 867.435719949 192.168.0.102          255.255.255.255  UDP     216 54357 → 6667 Len=172
8173 867.824286906 192.168.0.109          192.168.0.255    BROWSER 288 Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Se…
8174 867.824729860 192.168.0.109          192.168.0.255    BROWSER 259 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
```

Scansione hardware e router:

```
8344 1147.3542410… MS-NLB-PhysServer-32_04:80:c3:e3:65               ARP      62 Who has 192.168.0.1? Tell 192.168.0.105
8345 1147.3938058… PCSSystemtec_56:5d:4b                             ARP      44 Who has 192.168.0.1? Tell 192.168.0.108
8346 1147.3959964… TpLinkTechno_f4:ce:10                             ARP      62 192.168.0.1 is at 74:da:88:f4:ce:10
```