Esercizio nmap/Wireshark

Traccia:

Nell'esercizio di oggi pomeriggio 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:

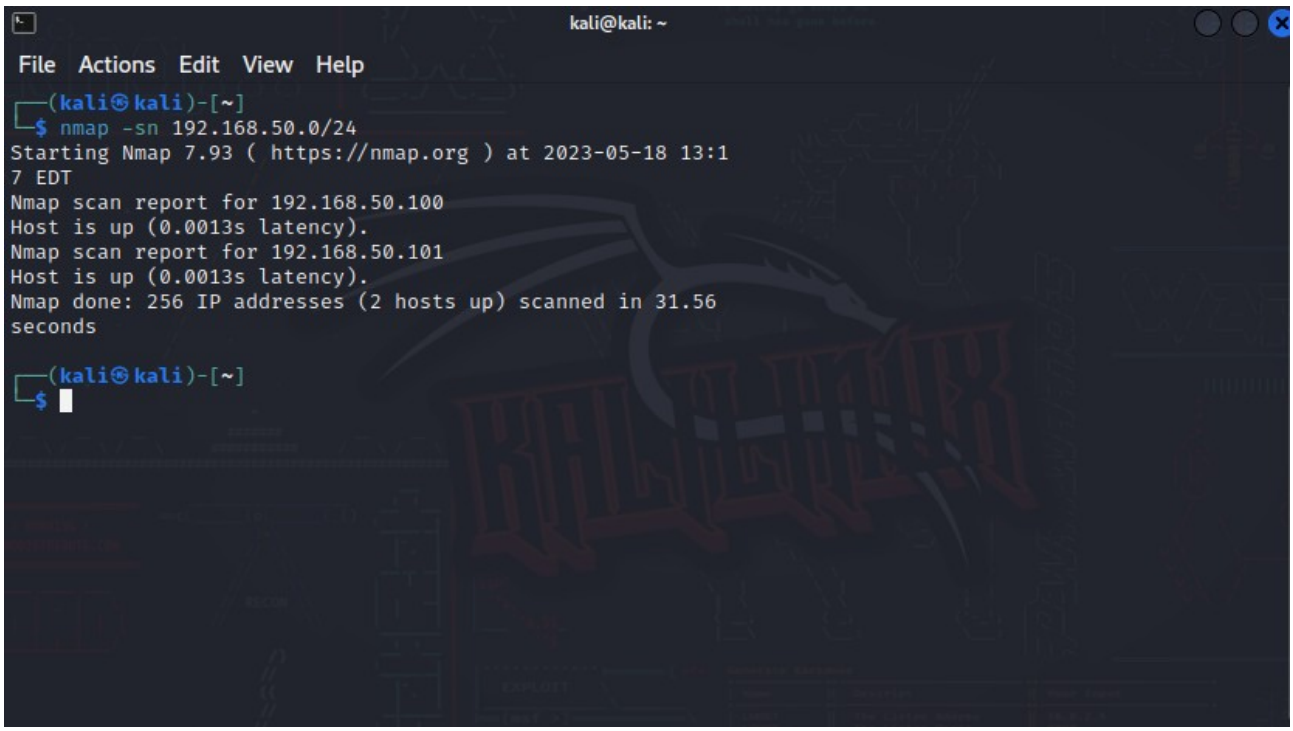
- Host discovery (sulla propria rete LAN)
- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente (Kali) 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)

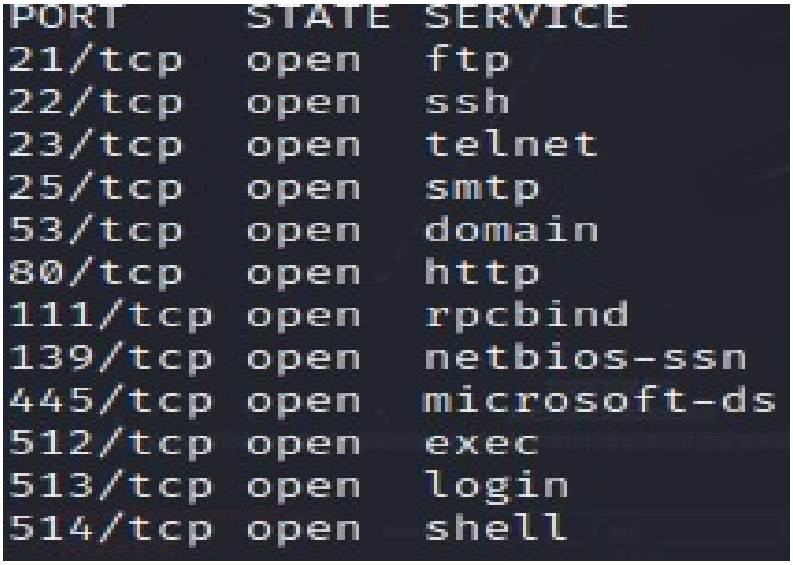
-Host discovery rete Lan

Una volta settate le machine (linux/metasploit) con rispettivi ip:192.168.50.100/182.168.50.101, possiamo avviare nmap e inserendo il commando (nmap -sn 192.168.50./24), difatti una volta avviato tale commando nmap riconosce i 2 host.



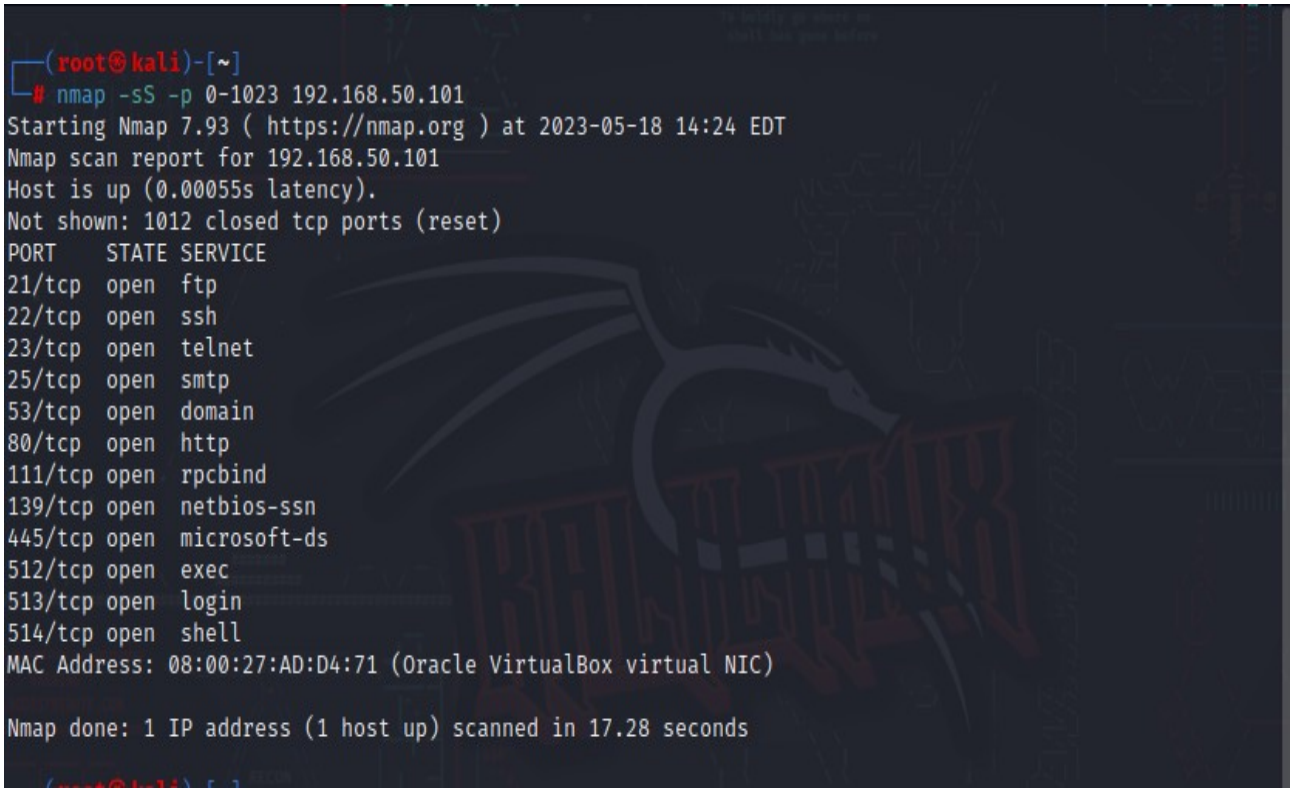
Scansione TCP sulle porte well-know

Una volta effettuato il seguente commando su nmap -sT -p 0-1023 192.168.50.101 appaiono dei risultati riguardanti porte well-know.



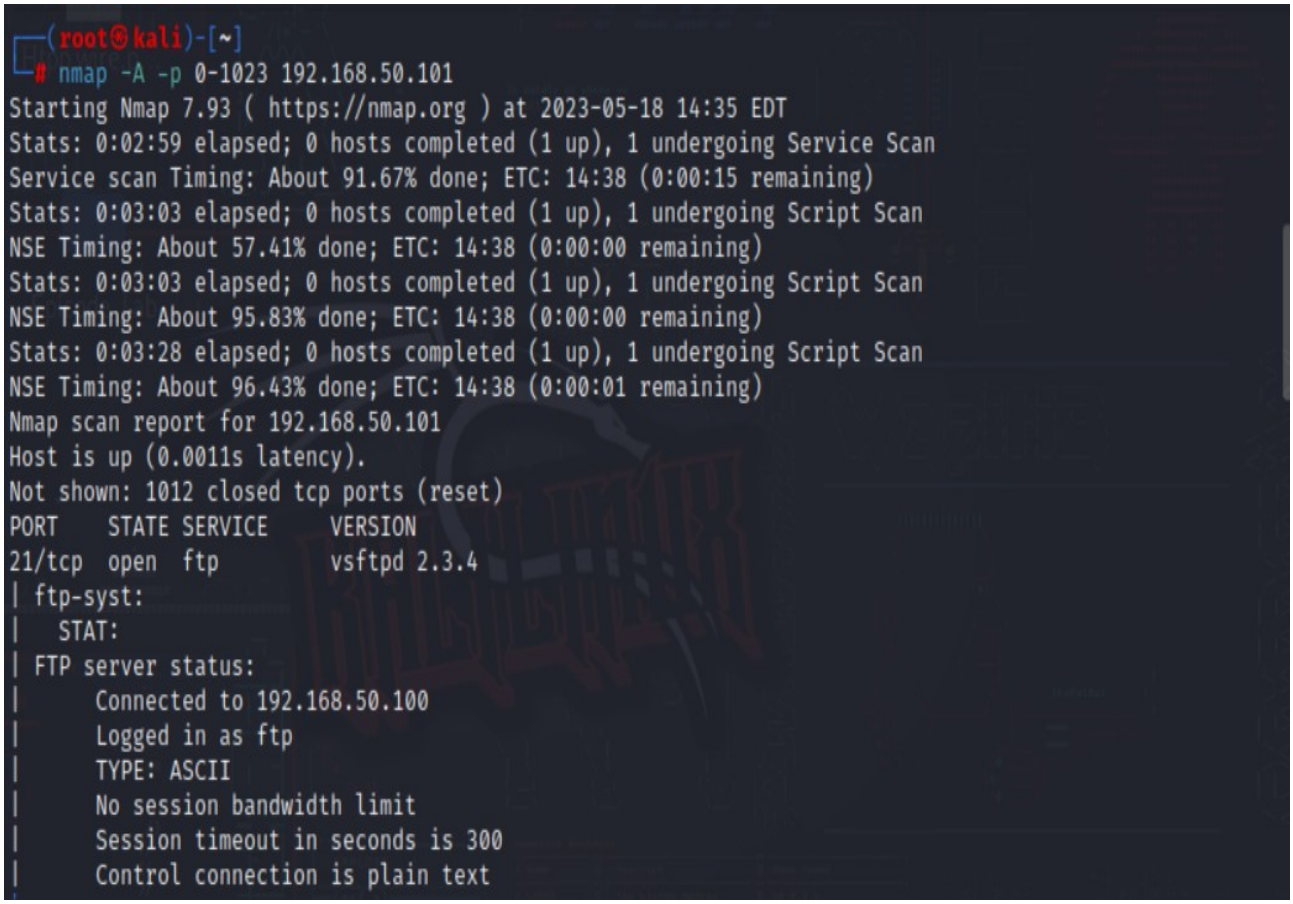
-Scansione SYN sulle porte well-know

Come nel precedente scansione effettuiamo il seguente commando su nmap (nmap -sS -p 0-1023 192.168.50.101) sulle porte well-know SYN



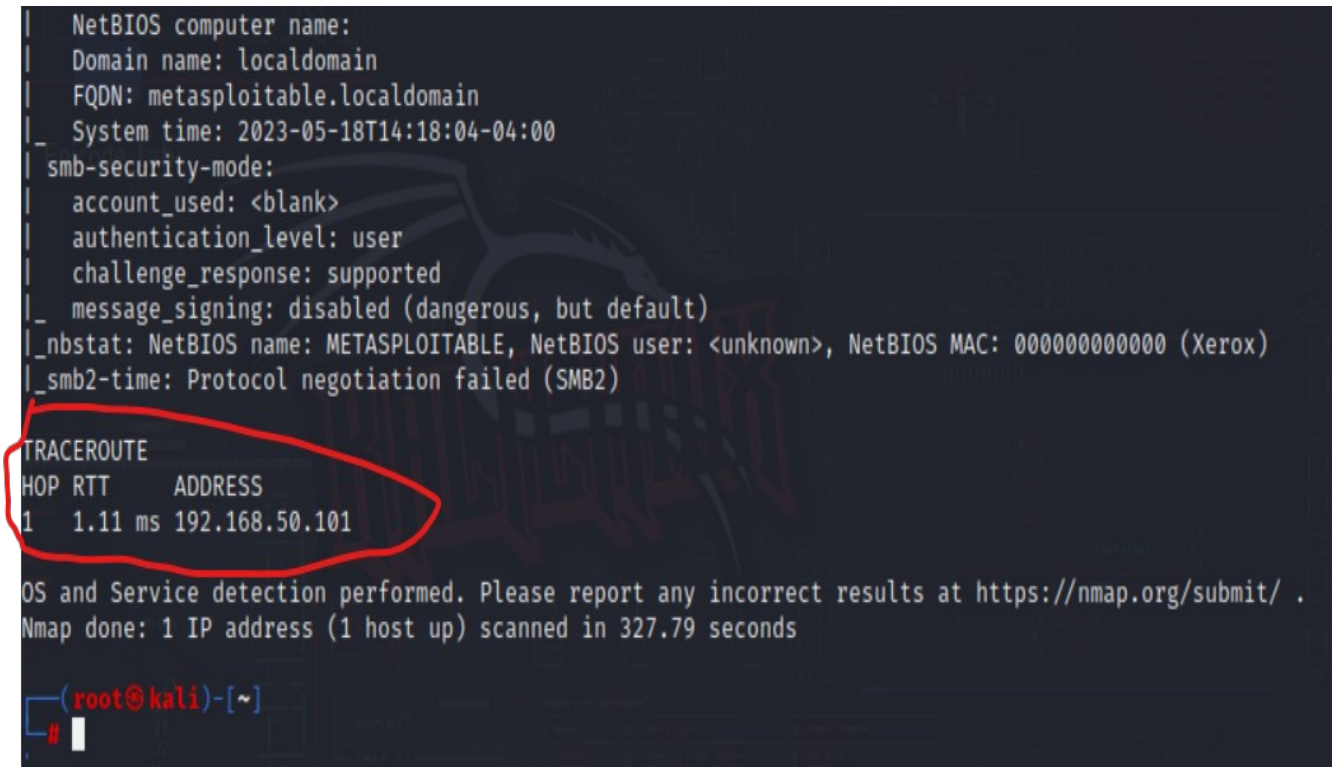
-Scansione con switch <<-A>> sulle porte well-know

Con il commando (nmap -A -p 0-1023 192.168.50.101)



```
|      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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp  open  telnet?
25/tcp  open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
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
```

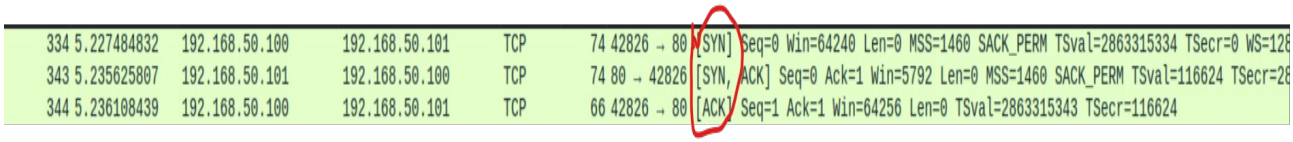
```
|   100005  1,2,3      52666/udp   mountd
|   100005  1,2,3      56607/tcp   mountd
|   100021  1,3,4      55251/tcp   nlockmgr
|   100021  1,3,4      60041/udp   nlockmgr
|   100024  1          33578/udp   status
|_  100024  1          39630/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 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?
514/tcp open  shell?
MAC Address: 08:00:27:AD:D4:71 (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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h39m56s, deviation: 2h49m43s, median: -20m04s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
```



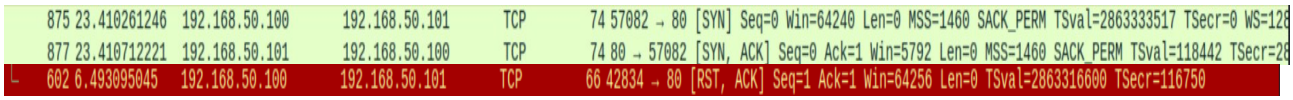
Evidenziare la differenza tra la scansione tra TCP/SYN

Utilizzando wireshark un software che intercetta il traffico dati in questo case della macchina (virtuale) linux, avviamo una connessione TCP creando una comunicazione tra server ed client.
Creando cosi il three way handshake che scambia la sincronizzazione di scambio e riconoscimento dei pachetti.
Inserendo il seguente filtro)tcp.port ==||upd.port

==80) come da foto si stabilizza la communicazione tra SYN,SYN/ACK e ACK



Diversamente dal TCP la scansione SYN non porta al termine il three way handshake e di conseguenza avviene lo scambio con SYN,SYN/ACK ed RST non porta la termine la connessione con RST



Scansione TCP

Fonte dello scan:192.168.50.100
Target dello scan:192.168.50.101
Tipo di scan: -sT -p 0-1023 192.168.50.101
Risultati ottenuti: 12 risultati

Scansione SYN

Fonte dello scan:192.168.50.100
Target dello scan:192.168.50.101
Tipo di scan: -sS -p 0-1023 192.168.50.101
Risultati ottenuti:12 risultati

Scansione con switch <← A>>

Fonte dello scan:192.168.50.100
Target dello scan:192.168.50.101
Tipo di scan: -A -p 0-1023 192.168.50.101
Risultati ottenuti: 12 risultati