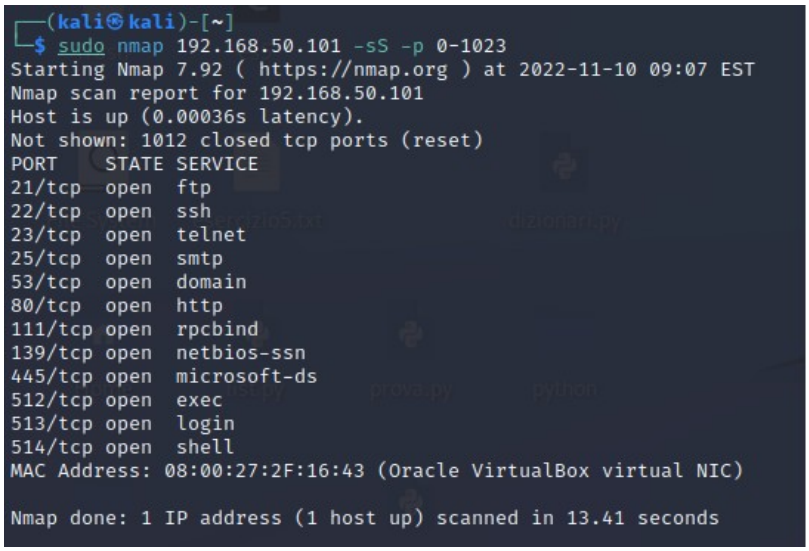
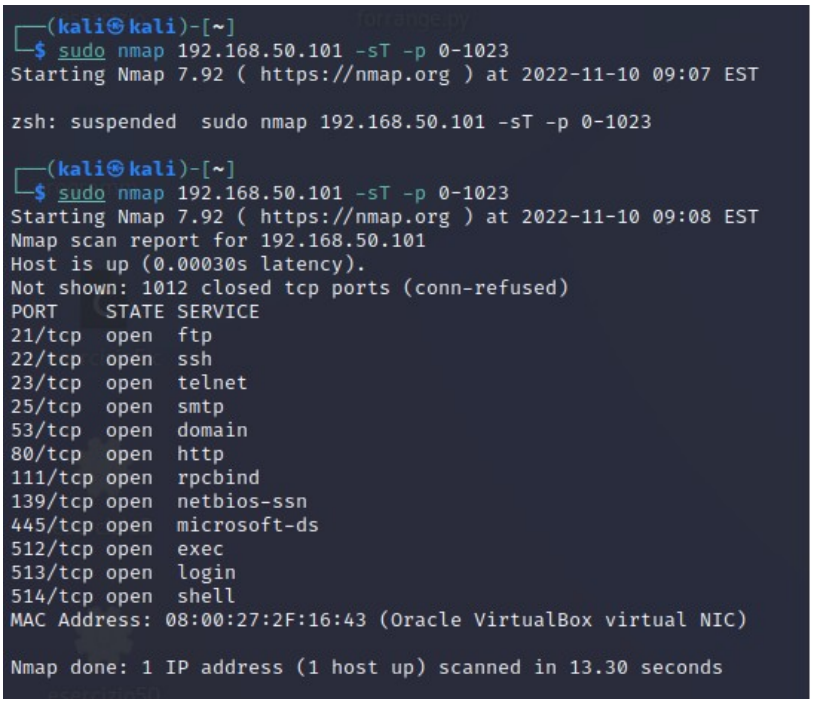
REPORT 10/11/2022 Lorenzo Scorbaioli

UTILIZZO DELLO STRUMENTO NMAP PER EFFETTUARE VARI TIPI DI SCANSIONE SU MACCHINA METASPLOITABLE

Dopo avere avviato entrambe le macchine all'interno della virtual box ed aver configurato la loro connessione su rete interna ho proceduto lanciando una serie di comandi dal terminale di linux kali. Il primo comando di scansione è stato "sudo nmap 192.168.50.101 -sT -p 0-1023" per avviare una scansione TCP sulle porte well-known. La foto qua sotto riporta il risultato di questa scansione:

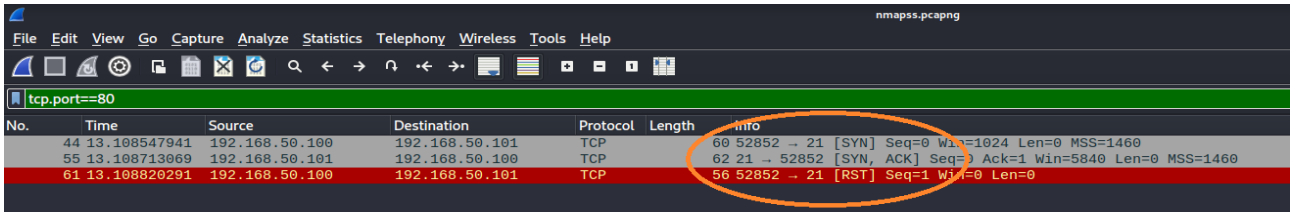


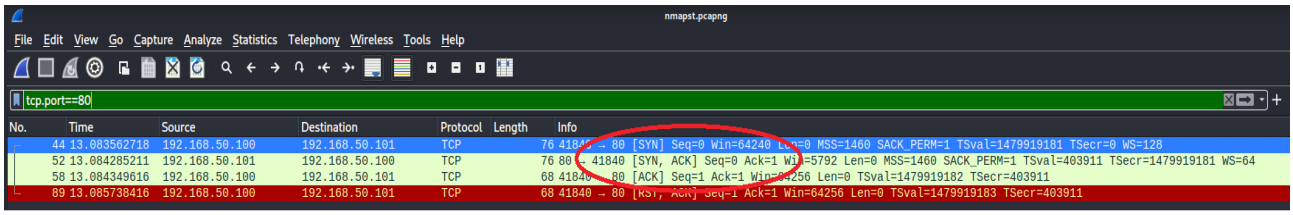
Successivamente sono andato a fare la scansione SYN sempre limitandola alle porte well-known tramite il comando "sudo nmap 192.168.50.101 -sS -p 0-1023", ottenendo questo risultato:



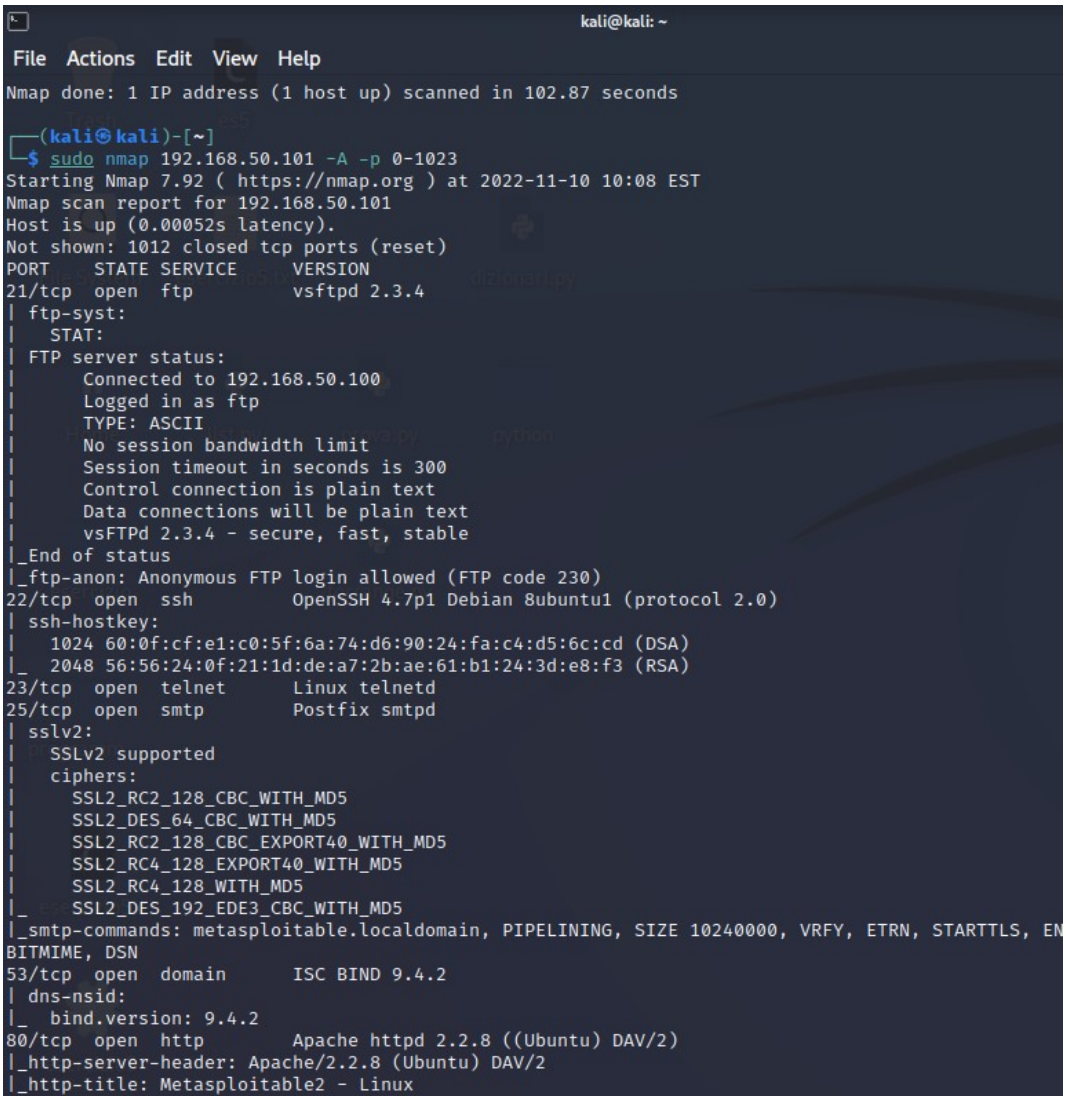
In entrambi i casi le porte della categoria well-known che risultano essere attive sono 12. Andando tramite Wireshark ad intercettare le richieste inviate dalla macchina linux kali possiamo vedere la differenza nei 2 tipi di scansione.

Prendiamo la porta 80 come punto di riferimento: nella scansione SYN se andiamo ad intercettare i pacchetti possiamo vedere come la connessione tra le 2 macchine non viene completata (cerchiato in arancione possiamo vedere RST che chiude la comunicazione). Nella scansione TCP infatti possiamo vedere come la three way handshake viene completata al contrario dell'altra (nel cerchio rosso possiamo vedere come viene completata la sequenza SYN-SYN+ACK-ACK)





Andando a fare uno scan usando sempre nmap ma con lo switch -A eseguiamo una scansione aggressiva ed avanzata che ci permette di vedere informazioni aggiuntive, come possiamo vedere dall'immagine qui sotto:



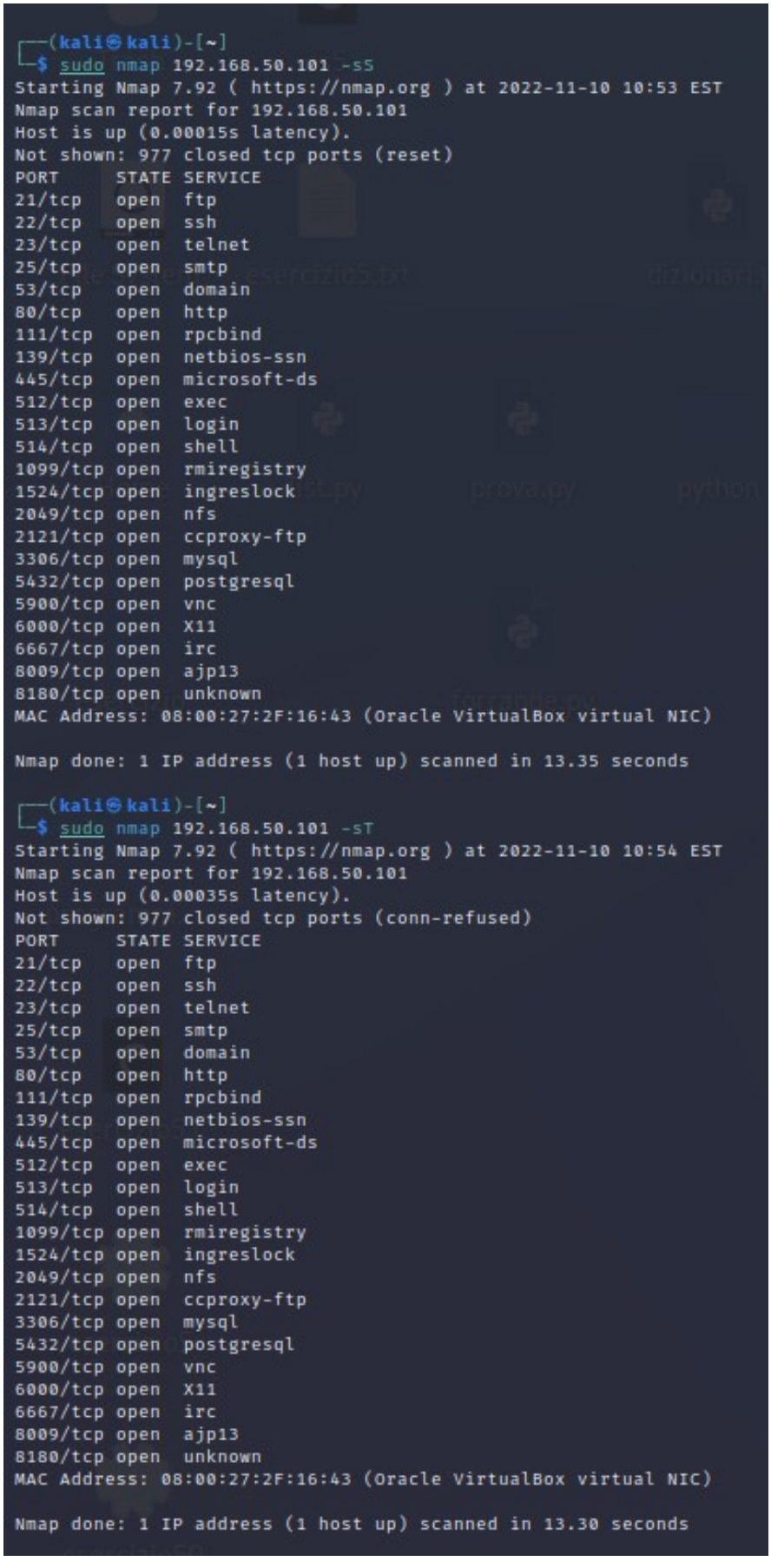
La seguente tabella riporta l’analisi della scansione SYN effettuata sulle porte well-know:

SOURCE	DESTINATION	TIPO DI SCAN	SERVIZIO
192.168.50.100:52852	192.168.50.101:21	SYN	ftp
192.168.50.100:52852	192.168.50.101:22	SYN	ssh
192.168.50.100:52852	192.168.50.101:23	SYN	telnet
192.168.50.100:52852	192.168.50.101:25	SYN	smtp
192.168.50.100:52852	192.168.50.101:53	SYN	domain
192.168.50.100:52852	192.168.50.101:80	SYN	http
192.168.50.100:52852	192.168.50.101:111	SYN	rpcbind
192.168.50.100:52852	192.168.50.101:139	SYN	Netbios-ssn
192.168.50.100:52852	192.168.50.101:445	SYN	Microsoft-ds
192.168.50.100:52852	192.168.50.101:512	SYN	exec
192.168.50.100:52852	192.168.50.101:513	SYN	login
192.168.50.100:52852	192.168.50.101:514	SYN	shell

La prossima tabella invece riporta l’analisi della scansione TCP

SOURCE	DESTINATION	TIPO DI SCAN	SERVIZIO
192.168.50.100:59206	192.168.50.101:21	TCP	ftp
192.168.50.100:37338	192.168.50.101:22	TCP	ssh
192.168.50.100:44908	192.168.50.101:23	TCP	telnet
192.168.50.100:37970	192.168.50.101:25	TCP	smtp
192.168.50.100:47332	192.168.50.101:53	TCP	domain
192.168.50.100:41840	192.168.50.101:80	TCP	http
192.168.50.100:37888	192.168.50.101:111	TCP	rpcbind
192.168.50.100:52240	192.168.50.101:139	TCP	Netbios-ssn
192.168.50.100:34548	192.168.50.101:445	TCP	Microsoft-ds
192.168.50.100:47844	192.168.50.101:512	TCP	exec
192.168.50.100:50254	192.168.50.101:513	TCP	login
192.168.50.100:41732	192.168.50.101:514	TCP	shell

I entrambi i tipi di scansione abbiamo visto che le porte well-known aperte sono 12. Se invece andiamo ad eseguire le scansioni SYN e TCP senza limitarci alle porte well-knwown otteniamo questo risultato:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.101 -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 10:53 EST
Nmap scan report for 192.168.50.101
Host is up (0.00015s latency).
Not shown: 977 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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:2F:16:43 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.101 -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 10:54 EST
Nmap scan report for 192.168.50.101
Host is up (0.00035s latency).
Not shown: 977 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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:2F:16:43 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```