REPORT 10-11-2022

FACCILONGO DOMENICO

NETWORK SCANNING CON NMAP

TASK

1. Scansione TCP sulle porte well-known
2. Scansione SYN sulle porte well-known
3. Scansione con switch <<-A>> sulle porte well-known

Successivamente per ognuno degli scan effettuati riportare:

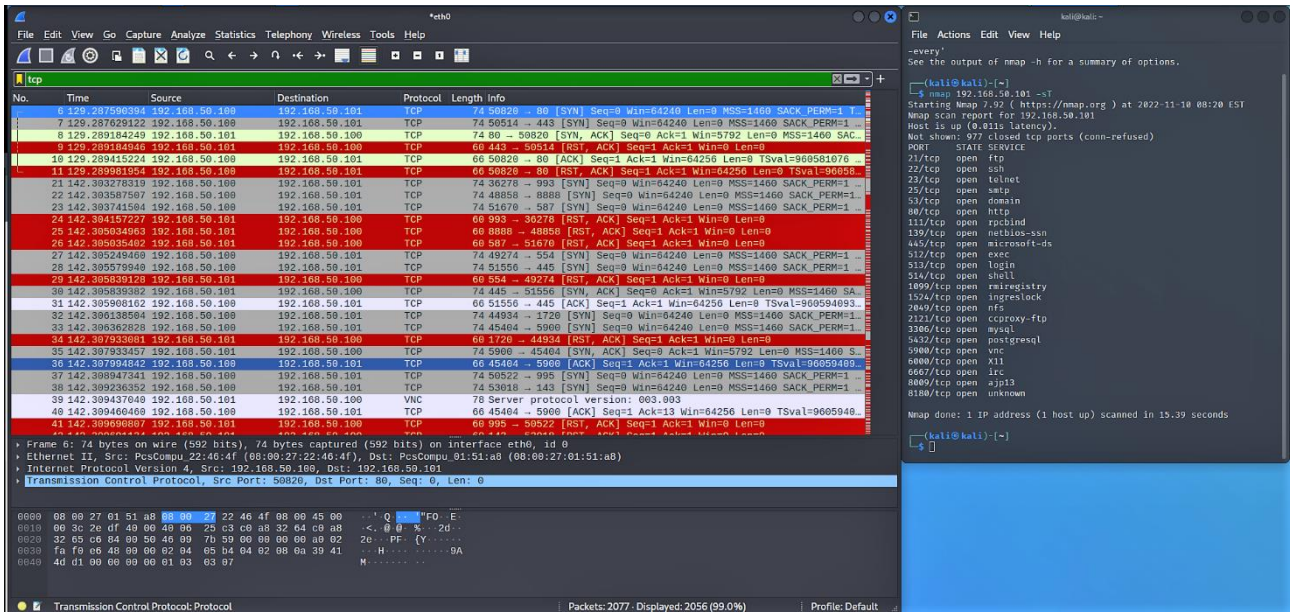
- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti

ANALISI E VALUTAZIONI

Innanzitutto dobbiamo effettuare lo scan come richiesto, di fatti elenchiamo una tabella con le diverse caratteristiche:

FONT SCAN	TARGET SCAN	TYPE SCAN	RESULTS SCAN
192.168.50.100	192.168.50.101	nmap 192.168.50.101 -sT	12 porte well-known aperte trovate
192.168.50.100	192.168.50.101	nmap 192.168.50.101 -sS	12 porte well-known aperte trovate
192.168.50.100	192.168.50.101	nmap 192.168.50.101 -A	12 porte well-known aperte trovate

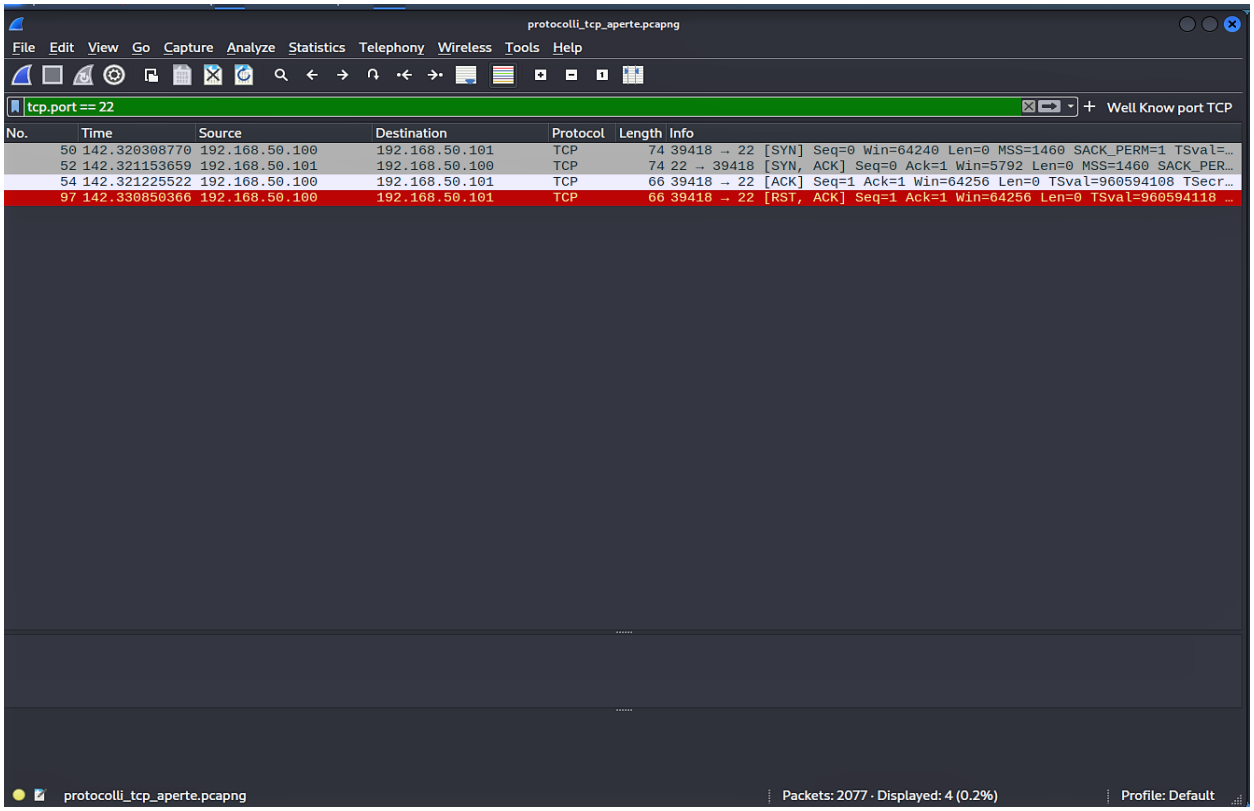
1. **SCAN TCP:** Partiamo nello scansionare il protocollo TCP sulle porte well-known le quali sono le porte che vanno da 0 a 1023. Per riuscire a identificare quali sono le porte aperte del protocollo ci basterà effettuare uno scan su di un server target il quale sarà il nostro metaspoitable. Di fatti il comando da utilizzare sarà <<nmap 192.168.50.101 -sT>>. L'indirizzo IP utilizzato è proprio quello di metaspoitable, pertanto verranno fuori i servizi con i protocolli di tipo TCP di cui di seguito:



Poiché dobbiamo considerare solo le porte well-known allora saranno quest'ultime:

PORT	STATUS	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	Logic
514/tcp	Open	shell

Ricordando che protocolli TCP sono quei protocolli che effettuano la connessione di tipo 3-way-handshake ovvero che attraverso 3 passaggi tra client-server si instaura la connessione. Di fatti andando a filtrare i risultati ottenuti su di una singola porta possiamo effettuare un analisi:



Come si può notare i passaggi effettuati sono effettivamente “4” (l’ultimo per chiudere la connessione):

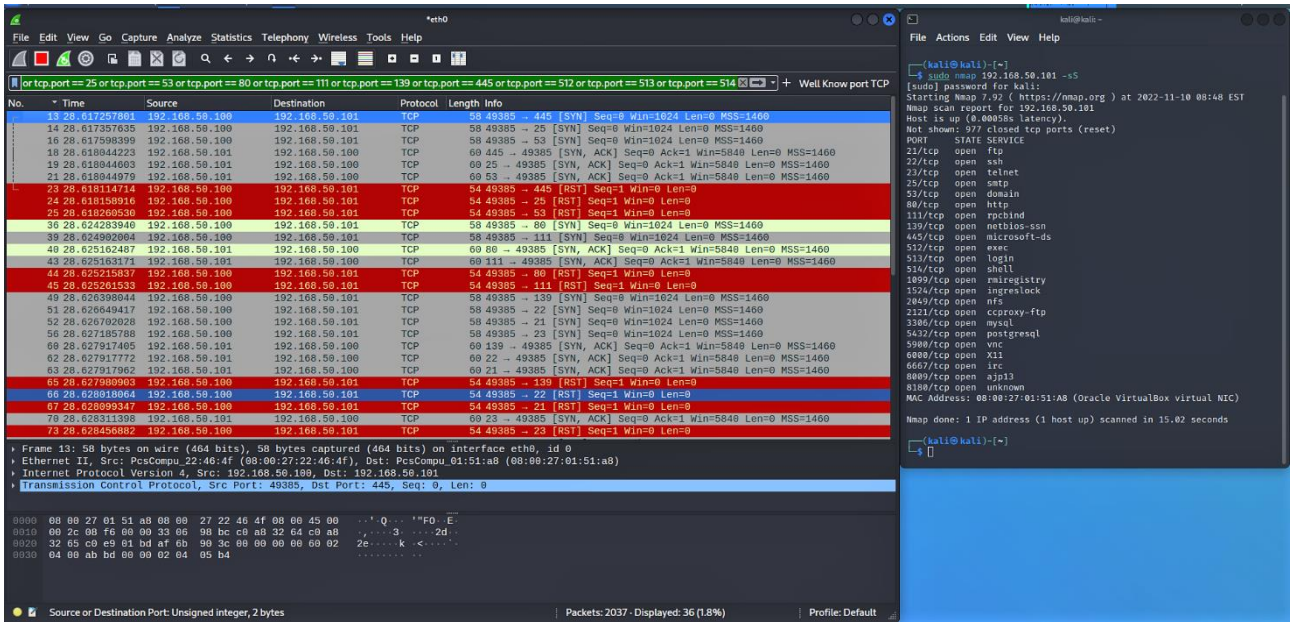
1. SYN da kali a metaspoitable
2. SYN+ACK da metaspotable a kali
3. ACK da kali a metaspoitable
4. RESET(RST) chiusura connessione da parte di metaspoitable

N.B. E’ possibile andare ad analizzare proprio questi passaggi andando dal menù “Transmission control protocol” → “Conversation completeness” → “Complete”

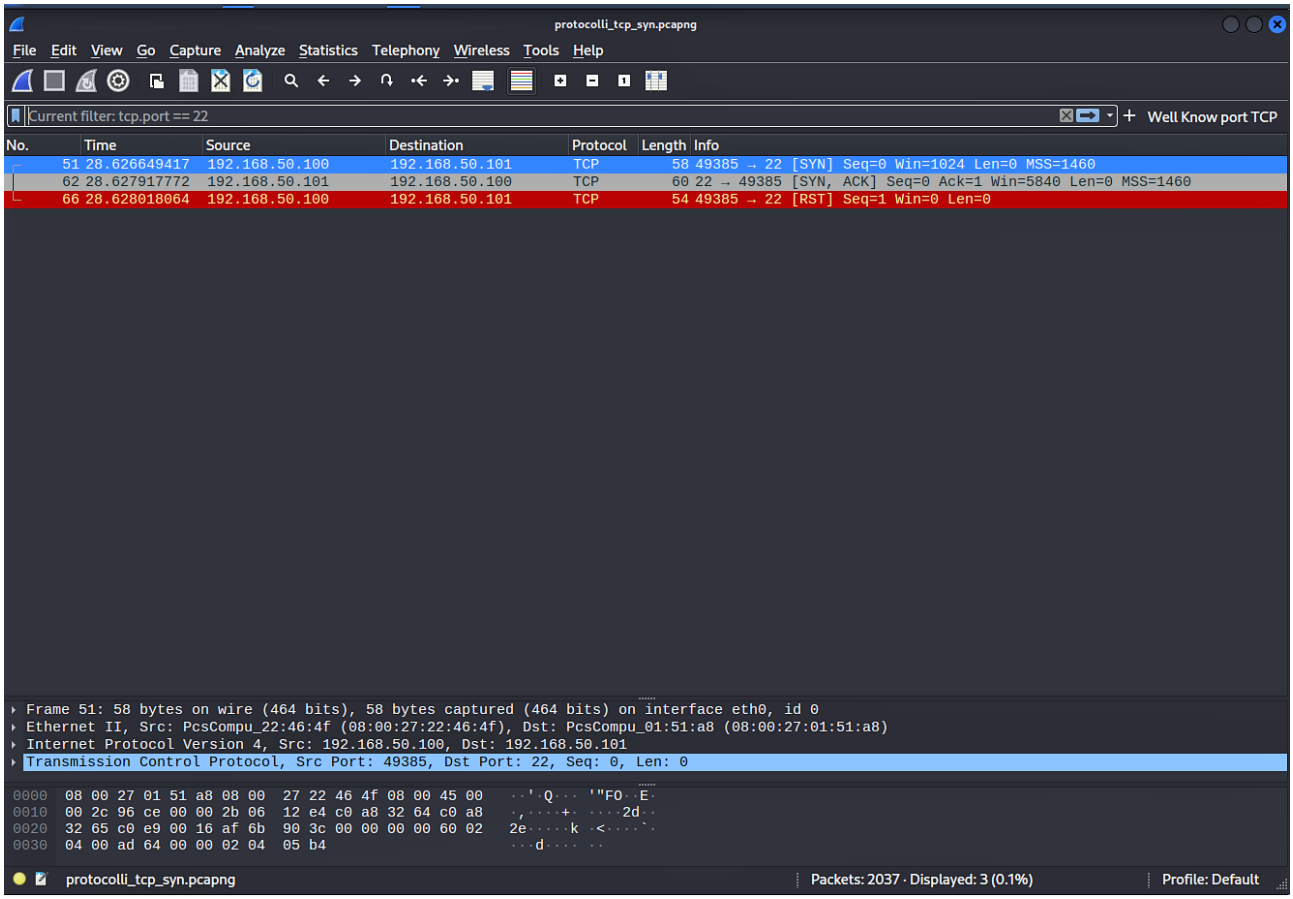
2. **SCAN SYN:** Successivamente andiamo a scansionare SYN, tramite il comando <<sudo nmap 192.168.50.101 -sS>> (Sudo perché richiede i permessi) e tra le porte well-known ritroviamo le seguenti:

PORT	STATUS	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	Logic
514/tcp	Open	Shell

In pratica avremo le stesse porte. Ora attraverso wireshark andiamo ad intercettare i pacchetti, e il risultato sarà il seguente:



Andando ora ad esaminare una delle porte (es.22 la stessa esaminata precedentemente) noteremo in effetti che in questo caso avremo "3" pacchetti, in quanto nella scansione SYN la connessione non viene conclusa, ma si ferma e si chiude dopo il primo ACK inviato, di fatti:

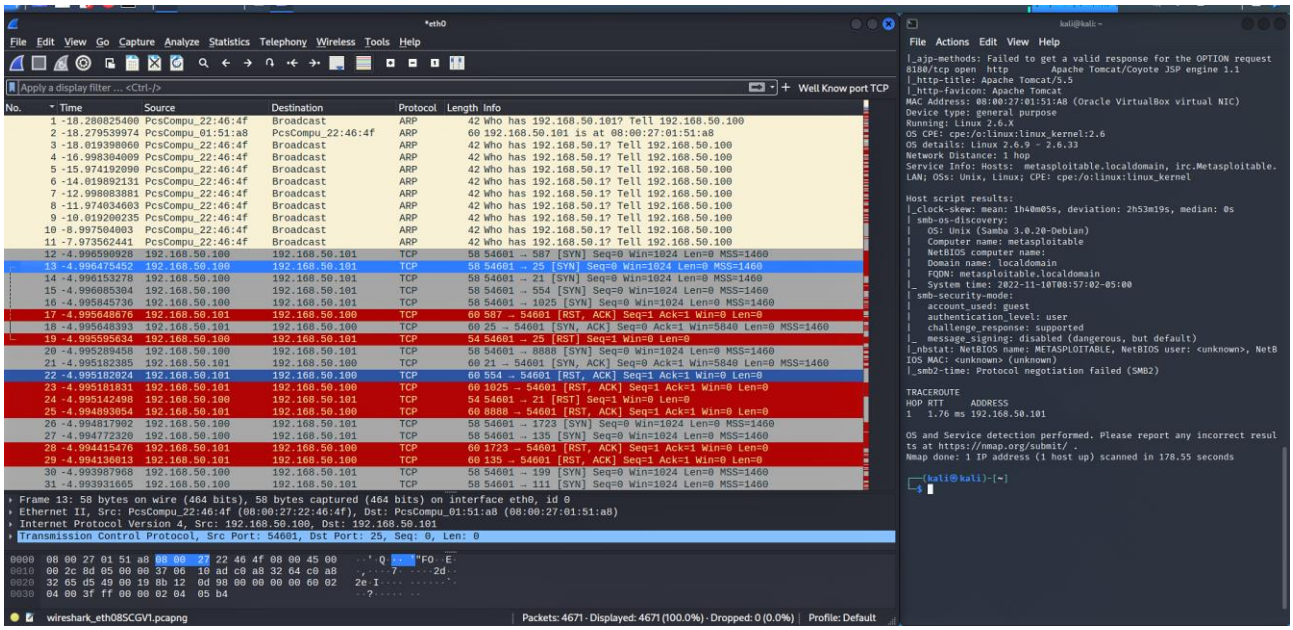


I passaggi sono:

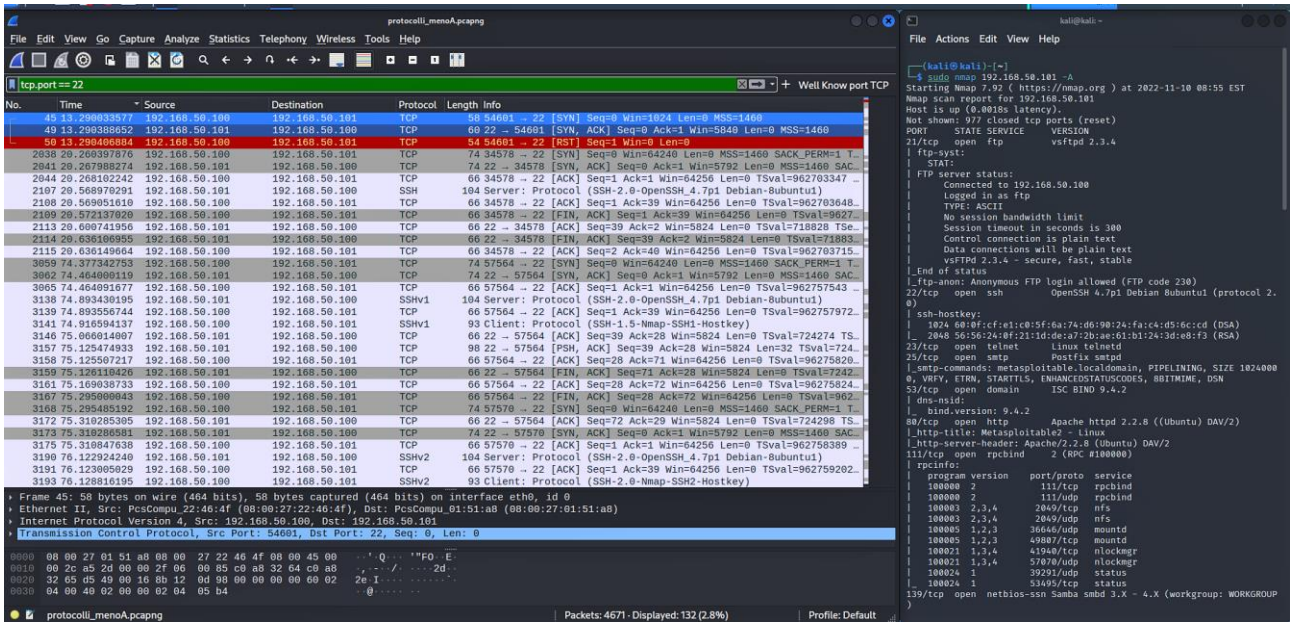
1. SYN da parte di kali per metaspoitable
2. SYN+ACK da parte di metaspoitable per kali
3. RESET(RST) in questo caso kali termina la connessione con metaspoitable

N.B. Anche in questo caso possiamo andare ad analizzare questi 3 semplici passaggi andando su "Transmission control Protocol" → "Conversation completeness" → "Incomplete"

3. **SCAN -A:** Infine come ultimo passaggio andiamo ad effettuare la scansione, con target metaspoitable, con il comando <<nmap 192.168.50.101 -A>>, in tal caso troveremo molti più pacchetti scambiati da protocolli diversi, non solo TCP, di fatti il risultato ottentuto sarà del tipo:



Dove se andassimo ad analizzare una sola porta in questione, ovvero la n.22 otterremo pacchetti di questo risultato:



Tale scansione è molto più approfondita di fatti essa ci fornisce molte più informazioni riguardo ai pacchetti trasmessi delle porte aperte, soprattutto dall'interfaccia del terminale.