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 fonte dello scan

-Il target dello scan

-Il tipo di scan

-I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)

REPORT W9D1 PRATICA 2

Fonte dello scan	Target dello scan	Tipo di scan	Risultati ottenuti
Kali Linux	192.168.0.104	Scansione SYN su porte well-known	Trovati 13 servizi attivi sulla macchina. Porte aperte: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514.
Kali Linux	192.168.0.104	Scansione TCP su porte well-known	Trovati 13 servizi attivi sulla macchina. Porte aperte: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514.
Kali Linux	192.168.0.104	Scansione con switch "-A" sulle porte well-known	Dettagli dei servizi: FTP (vsftpd 2.3.4), SSH (OpenSSH 4.7p1 Debian 8ubuntu1), Telnet (Linux telnetd), SMTP (Postfix smtpd), DNS (ISC BIND 9.4.2), HTTP (Apache httpd 2.2.8), RPCbind (versione 2), NetBIOS-SSN (Samba smbd), Servizio di esecuzione remota (netkit-rsh rexecd), Login, TCPwrapped.

I risultati delle scansioni condotte sulla macchina Metasploitable forniscono una panoramica dettagliata dei servizi attivi e delle porte aperte sulla macchina

bersaglio. Le scansioni sono state eseguite utilizzando diversi metodi, tra cui la scansione TCP sulle porte well-known, la scansione SYN sulle porte well-known e la scansione con lo switch "-A" per ottenere informazioni dettagliate sui servizi trovati.

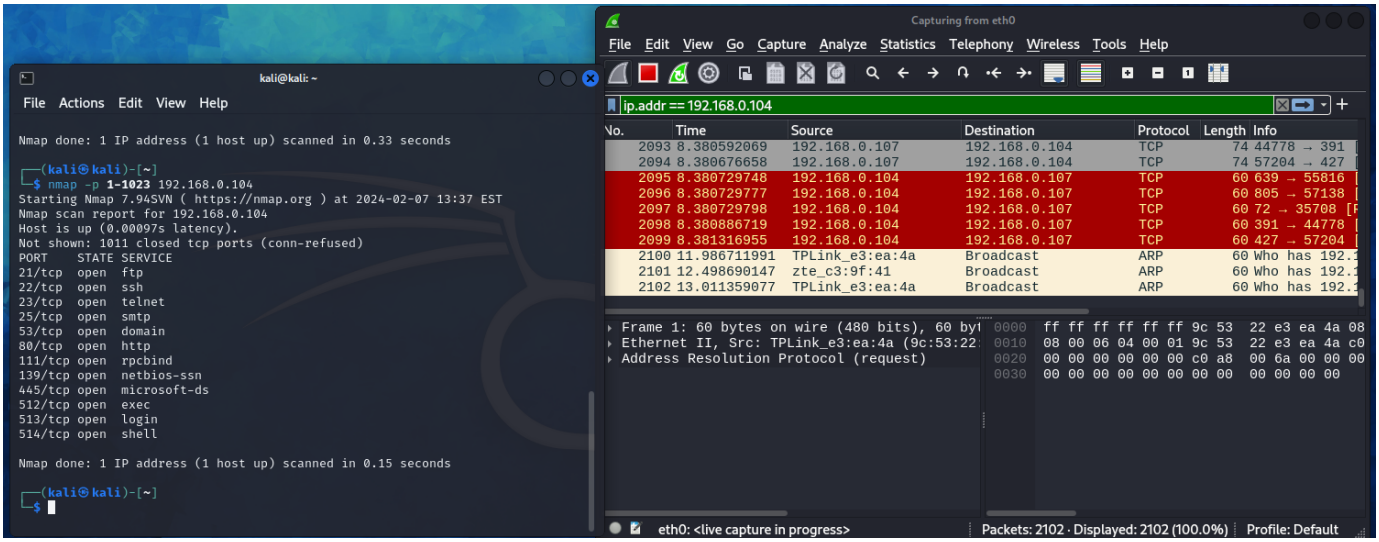
Dalla scansione TCP e dalla scansione SYN, è emerso che sono attivi 13 servizi sulla macchina Metasploitable, con le stesse porte aperte in entrambe le scansioni. Questi servizi includono FTP, SSH, Telnet, SMTP, DNS, HTTP, RPCbind, NetBIOS-SSN, e altri.

Inoltre, la scansione con lo switch "-A" ha fornito dettagli specifici sui servizi individuati, inclusi i nomi e le versioni dei servizi come vsftpd 2.3.4 per FTP, OpenSSH 4.7p1 Debian 8ubuntu1 per SSH, e così via. Queste informazioni sono preziose per valutare la sicurezza della macchina e identificare potenziali vulnerabilità che potrebbero essere sfruttate.

Complessivamente, le scansioni hanno fornito una comprensione approfondita dello stato dei servizi sulla macchina bersaglio, facilitando l'analisi della sua sicurezza e la pianificazione delle azioni successive.

DIFFERENZE TRA LE SCANSIONI INTERCETTANDO I PACCHETTI CON WIRESHARK

Cattura TCP:



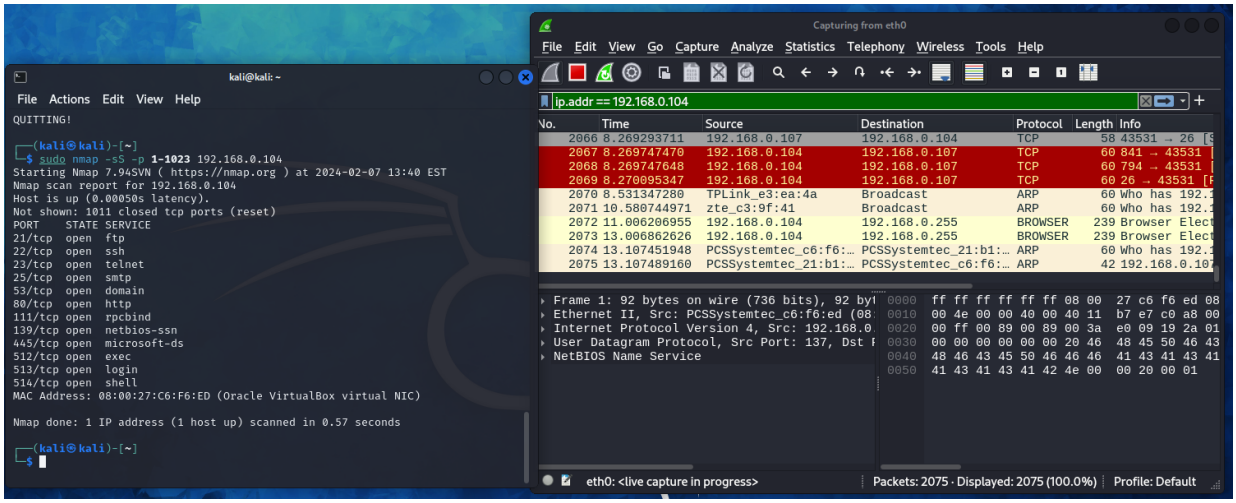
Tipo di pacchetti: La cattura TCP mostra principalmente pacchetti che utilizzano il protocollo TCP per stabilire connessioni tra i dispositivi di rete.

Sinossi dei pacchetti: Include pacchetti di tipo SYN, SYN-ACK, ACK, e altre fasi del protocollo TCP, tipiche di una connessione TCP completa.

Scopo principale: Questa cattura mira a monitorare le connessioni TCP e le loro fasi di negoziazione e trasferimento di dati.

Evidenze specifiche: È probabile trovare flussi di dati bidirezionali, con pacchetti che portano dati nelle due direzioni tra mittente e destinatario.

Cattura SYN:



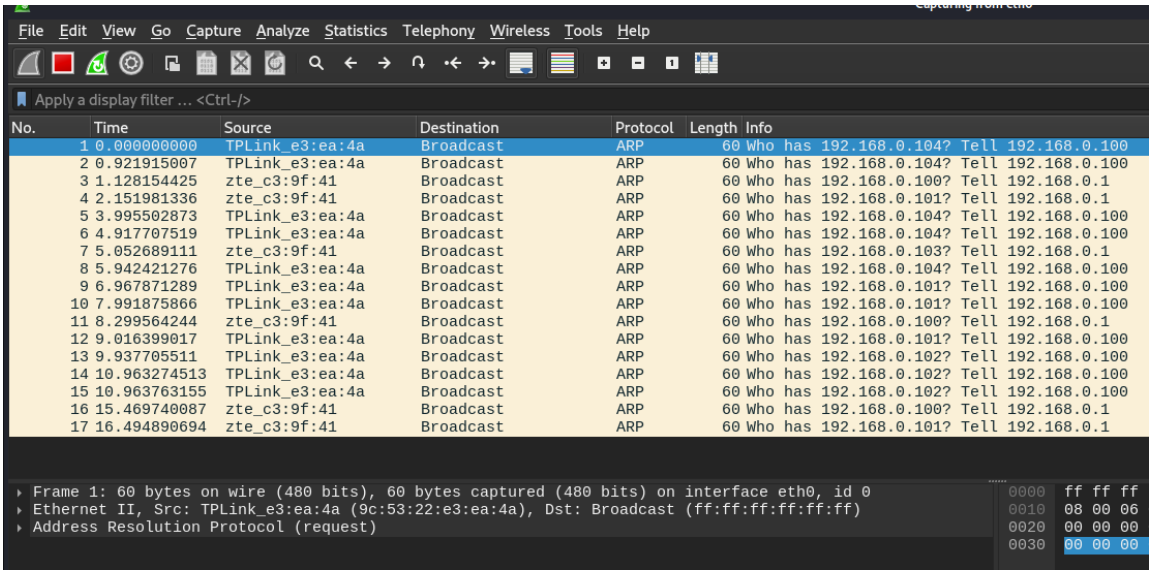
Tipo di pacchetti: La cattura SYN mostra principalmente pacchetti di tipo SYN inviati durante la fase di handshake di una connessione TCP.

Sinossi dei pacchetti: Include principalmente pacchetti SYN inviati da un host per avviare una connessione TCP.

Scopo principale: Questa cattura è utilizzata per individuare le scansioni di porte, in cui un mittente cerca di stabilire connessioni TCP con più destinazioni per identificarne lo stato.

Evidenze specifiche: Molti pacchetti con flag SYN impostato e pochi pacchetti di tipo SYN-ACK o ACK, indicando che l'host sta cercando di stabilire nuove connessioni.

Cattura con switch - a:



Tipo di pacchetti: La cattura con switch - a mostra principalmente pacchetti ARP e altri pacchetti di servizio di rete, come NBNS.

Sinossi dei pacchetti: Include principalmente pacchetti ARP, che vengono utilizzati per la risoluzione degli indirizzi MAC, e pacchetti di servizi di rete locali.

Scopo principale: Questa cattura è utile per monitorare l'attività di rete locale, compresa la scoperta degli indirizzi MAC e le richieste di servizi di rete locali.

Evidenze specifiche: Molteplici pacchetti ARP con richieste "Chi ha" e risposte "Io ho", indicando un'attività di risoluzione degli indirizzi IP-MAC nella rete locale.

Confronto generale:

La cattura TCP è focalizzata sul monitoraggio delle connessioni TCP.

La cattura SYN è utilizzata per individuare le scansioni di porte e le tentate connessioni TCP.

La cattura con switch - a è orientata alla monitoraggio dell'attività di rete locale, inclusa la risoluzione degli indirizzi IP-MAC e le richieste di servizi di rete locali.