

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:

The screenshot displays two windows from a Kali Linux environment. The left window shows the terminal output of an Nmap scan performed on 192.168.0.104. The scan identified 13 open ports, each with a corresponding service: 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 512/tcp (exec), 513/tcp (login), and 514/tcp (shell). The right window shows the Wireshark network protocol analyzer interface, capturing traffic on the eth0 interface. The packet list shows several TCP packets (No. 2093, 2094, 2095, 2096, 2097, 2098, 2099) and two ARP requests (No. 2100, 2101). The packet details for the first ARP request (No. 2100) are expanded, showing the Ethernet II header and the ARP request structure.

No.	Time	Source	Destination	Protocol	Length	Info
2093	8.380592069	192.168.0.107	192.168.0.104	TCP	74	44776 → 391
2094	8.380676659	192.168.0.107	192.168.0.104	TCP	74	57204 → 427
2095	8.380729748	192.168.0.104	192.168.0.107	TCP	60	639 → 55816
2096	8.380729777	192.168.0.104	192.168.0.107	TCP	60	895 → 57138
2097	8.380729798	192.168.0.104	192.168.0.107	TCP	60	72 → 35708
2098	8.380886719	192.168.0.104	192.168.0.107	TCP	60	391 → 44778
2099	8.381316955	192.168.0.104	192.168.0.107	TCP	60	427 → 57204
2100	11.986711991	TPLink_e3:ea:4a	Broadcast	ARP	60	Who has 192.168.0.104
2101	12.498698147	zte_c3:9f:41	Broadcast	ARP	60	Who has 192.168.0.104
2102	13.011359077	TPLink_e3:ea:4a	Broadcast	ARP	60	Who has 192.168.0.104

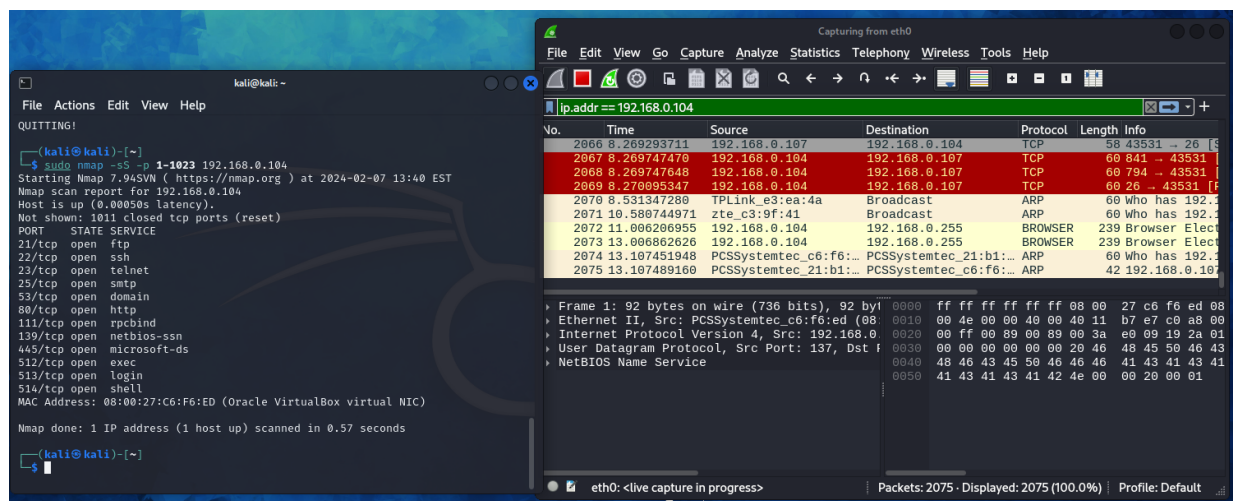
Tipo di pacchetti: La cattura TCP mostra principalmente pacchetti che utilizzano il protocollo TCP per stabilire connessioni tra i dispositivi di rete.

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:

Wireshark interface showing a network traffic capture. The packet list displays 17 ARP requests. The packet details pane shows the structure of the first packet: Ethernet II, Src: TPLink_e3:ea:4a, Dst: Broadcast, and Address Resolution Protocol (request). The packet bytes pane shows the raw data in hexadecimal.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.104? Tell 192.168.0.100
2	0.921915007	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.104? Tell 192.168.0.100
3	1.128154425	zte_c3:9f:41	Broadcast	ARP	60	who has 192.168.0.100? Tell 192.168.0.1
4	2.151981336	zte_c3:9f:41	Broadcast	ARP	60	who has 192.168.0.101? Tell 192.168.0.1
5	3.995502873	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.104? Tell 192.168.0.100
6	4.917707519	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.104? Tell 192.168.0.100
7	5.052689111	zte_c3:9f:41	Broadcast	ARP	60	who has 192.168.0.103? Tell 192.168.0.1
8	5.942421276	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.104? Tell 192.168.0.100
9	6.967871289	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.101? Tell 192.168.0.100
10	7.991875866	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.101? Tell 192.168.0.100
11	8.299564244	zte_c3:9f:41	Broadcast	ARP	60	who has 192.168.0.100? Tell 192.168.0.1
12	9.016399017	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.101? Tell 192.168.0.100
13	9.937705511	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.102? Tell 192.168.0.100
14	10.963274513	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.102? Tell 192.168.0.100
15	10.963763155	TPLink_e3:ea:4a	Broadcast	ARP	60	who has 192.168.0.102? Tell 192.168.0.100
16	15.469740087	zte_c3:9f:41	Broadcast	ARP	60	who has 192.168.0.100? Tell 192.168.0.1
17	16.494890694	zte_c3:9f:41	Broadcast	ARP	60	who has 192.168.0.101? Tell 192.168.0.1

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
 Ethernet II, Src: TPLink_e3:ea:4a (9c:53:22:e3:ea:4a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

0000 ff ff ff
 0010 08 00 06
 0020 00 00 00
 0030 00 00 00

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.