

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.

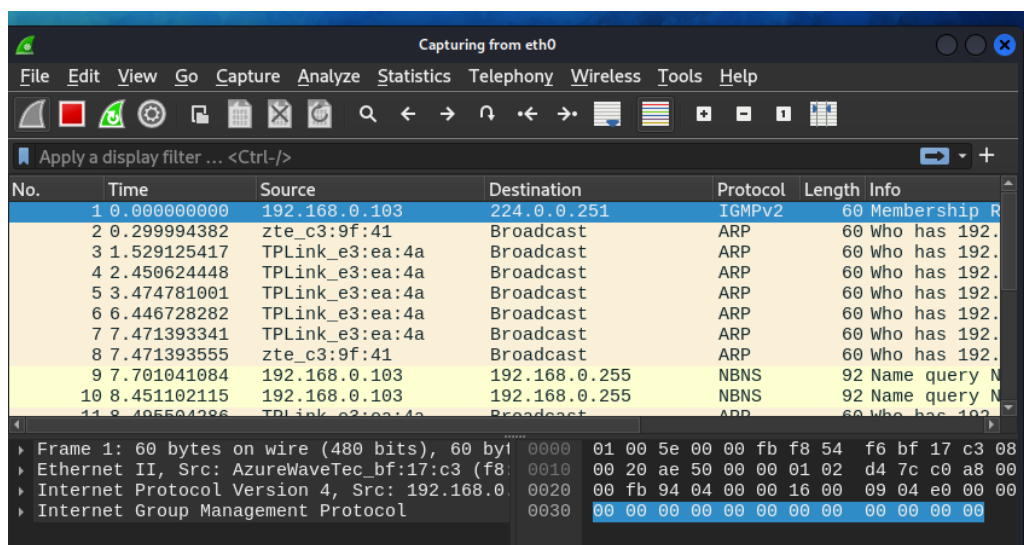
Dalla scansione TCP e dalla scansione SYN, è emerso che sono attivi 13 servizi sulla macchina Metasploitable, con le stesse porte aperte in entrambe le scansioni. Questi servizi includono FTP, SSH, Telnet, SMTP, DNS, HTTP, RPCbind, NetBIOS-SSN, e altri.

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:



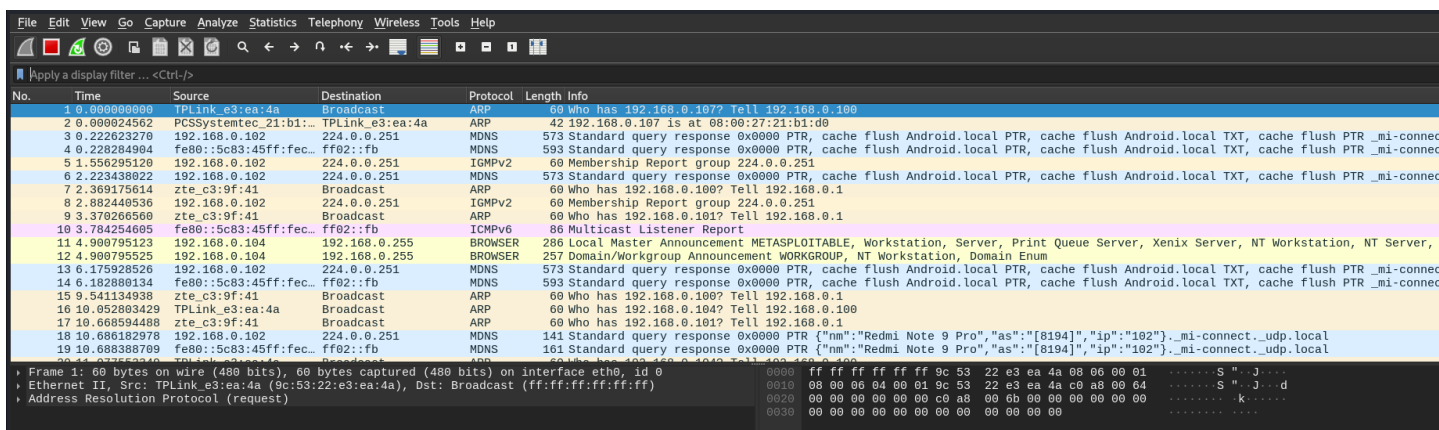
Tipo di pacchetti: La cattura TCP mostra principalmente pacchetti che utilizzano il protocollo TCP per stabilire connessioni tra i dispositivi di rete.

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:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	TPLink_e3:ea:4a	Broadcast	ARP	60	Who has 192.168.0.107? Tell 192.168.0.109
2	0.000024562	PCSSystemtec_21:b1:...	TPLink_e3:ea:4a	ARP	42	192.168.0.107 is at 08:00:27:21:b1:08
3	0.222623278	192.168.0.102	224.0.0.251	MDNS	573	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local TXT, cache flush PTR _mi-connect...
4	0.22824904	fe80::5c83:45ff:fec...	ff02::fb	MDNS	593	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local TXT, cache flush PTR _mi-connect...
5	1.556295128	192.168.0.102	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
6	2.223438822	192.168.0.102	224.0.0.251	MDNS	573	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local TXT, cache flush PTR _mi-connect...
7	2.369175614	zte_c3:9f:41	Broadcast	ARP	60	Who has 192.168.0.100? Tell 192.168.0.1
8	2.882448536	192.168.0.102	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
9	3.378266568	zte_c3:9f:41	Broadcast	ARP	60	Who has 192.168.0.101? Tell 192.168.0.1
10	3.784254605	fe80::5c83:45ff:fec...	ff02::fb	ICMPv6	86	Multicast Listener Report
11	4.980795123	192.168.0.104	192.168.0.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server,
12	4.980795525	192.168.0.104	192.168.0.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
13	6.175928526	192.168.0.102	224.0.0.251	MDNS	573	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local TXT, cache flush PTR _mi-connect...
14	6.182880134	fe80::5c83:45ff:fec...	ff02::fb	MDNS	593	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local TXT, cache flush PTR _mi-connect...
15	9.541134938	zte_c3:9f:41	Broadcast	ARP	60	Who has 192.168.0.100? Tell 192.168.0.1
16	10.052803429	TPLink_e3:ea:4a	Broadcast	ARP	60	Who has 192.168.0.104? Tell 192.168.0.109
17	10.68594488	zte_c3:9f:41	Broadcast	ARP	60	Who has 192.168.0.101? Tell 192.168.0.1
18	10.686182978	192.168.0.102	224.0.0.251	MDNS	141	Standard query response 0x0000 PTR {"nm":"Redmi Note 9 Pro","as":["8194"],"ip":["102"]}_mi-connect._udp.local
19	10.688388709	fe80::5c83:45ff:fec...	ff02::fb	MDNS	161	Standard query response 0x0000 PTR {"nm":"Redmi Note 9 Pro","as":["8194"],"ip":["102"]}_mi-connect._udp.local

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 capture. The packet list table is as follows:

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

Packet details for Frame 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)

Packet bytes (hex):

```

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.