

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 side-by-side. The left window is a terminal running Nmap on Kali Linux. The right window is Wireshark, showing a live capture of network traffic on the eth0 interface.

Nmap Scan Results:

```
kali@kali: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds  
$ nmap -p 1-1023 192.168.0.104  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 13:37 EST  
Nmap scan report for 192.168.0.104  
Host is up (0.00097s latency).  
Not shown: 1011 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  
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds  
$
```

Wireshark Packet Capture:

Filter: ip.addr == 192.168.0.104

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

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0
Ethernet II, Src: TPLink_e3:ea:4a (9c:53:22:00:10:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

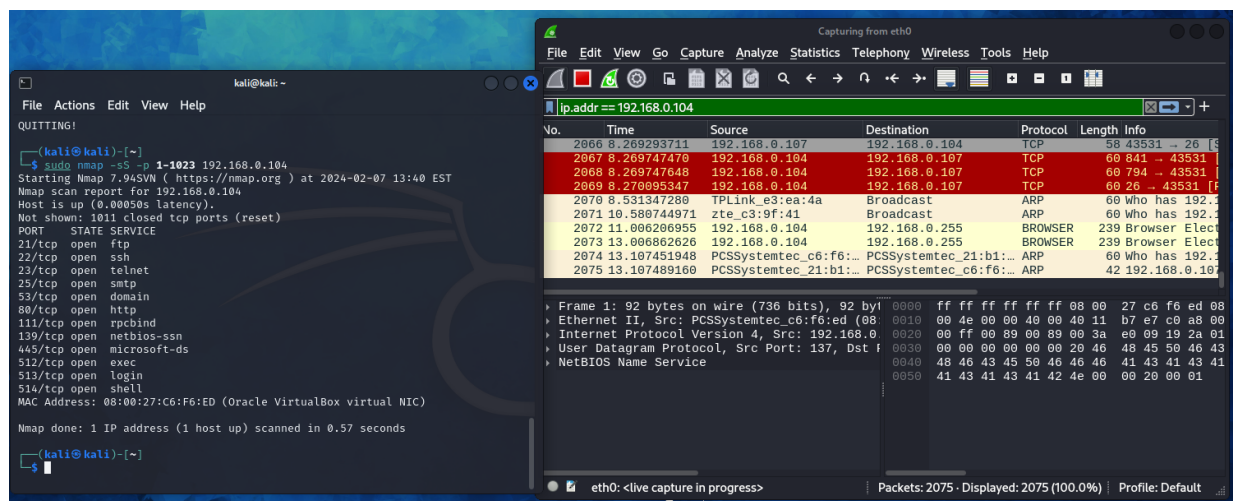
Tipo di pacchetti: La cattura TCP mostra principalmente pacchetti che utilizzano il protocollo TCP per stabilire connessioni tra i dispositivi di rete.

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:

