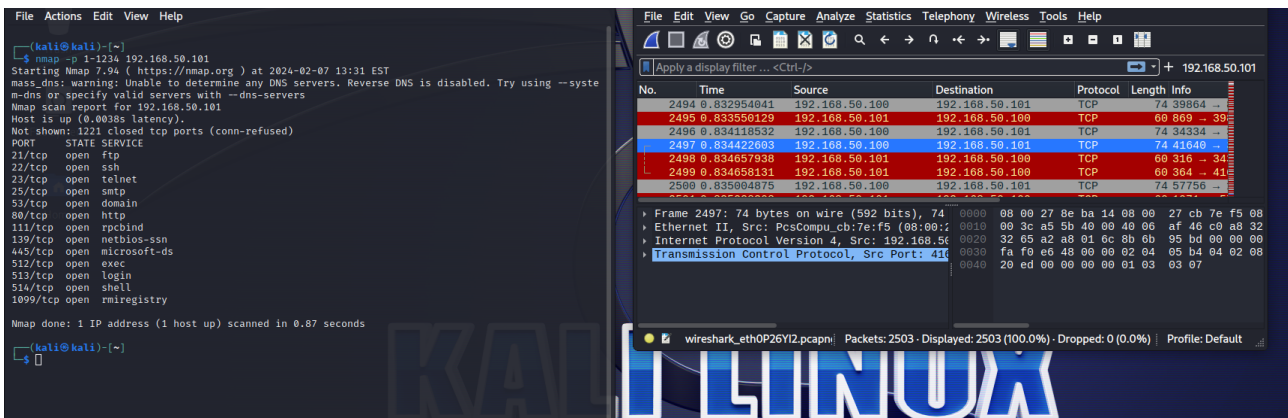


Report di Analisi con Nmap su Metasploitable: Scansione dei Servizi di Rete e Differenze tra Scansione TCP e SYN



Scansione TCP su Porte Well-Known (Commando: `sudo nmap 192.168.50.101 -p 1-1023`)

Risultati Chiave:

- Scansione SYN su porte well-known da 1 a 1023.
- Utilizzo del comando **sudo** per ottenere privilegi elevati e rilevare servizi su porte comuni.
- Identificati servizi come FTP, SSH, Telnet, HTTP, e altri.
- Adatta per una scansione rapida focalizzata su porte comunemente utilizzate.

```

$ sudo nmap -A -p 20-1024 --system-dns 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 13:52 EST
Nmap scan report for 192.168.50.101
Host is up (0.0018s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|  STAT:
|_FTP server status:
| * Connected to 192.168.50.100
| * Logged in as ftp
| * TYPE: ASCII
| * No session bandwidth limit
| * Session timeout in seconds is 300
| * Control connection is plain text
| * Data connections will be plain text
| * vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

```

Scansione Dettagliata con Rilevamento (Commando: `nmap -A -p 1-2024 --system-dns 192.168.50.101`)

Risultati Chiave:

- Scansione completa con rilevamento, inclusi sistema operativo, versioni dei servizi e analisi NSE.
- Specifica la scansione delle porte da 1 a 2024 con l'utilizzo del sistema DNS del sistema.
- Rivelati dettagli su servizi come FTP, SSH, MySQL, e altri.
- Importante per una valutazione completa della sicurezza e delle potenziali vulnerabilità.

```
(kali㉿kali)-[~]
$ sudo nmap -sS -p 1-2024 --system-dns 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 15:25 EST
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).
Not shown: 2010 closed tcp ports (reset)
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
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
MAC Address: 08:00:27:8E:BA:14 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```

. Scansione SYN su Porte Well-Known e Altre (Commando: nmap -sS -p 1-2024 --system-dns 192.168.50.101)

Risultati Chiave:

- Scansione SYN su porte da 1 a 2024 con utilizzo del sistema DNS.
- Identificati servizi su un'ampia gamma di porte.
- Opzione **-sS** per una scansione SYN leggera e discreta.
- Utile per ottenere una visione completa dei servizi senza completare le connessioni.

Fonte	Scar	Target	Scan	Tipo Scan	Risultati ottenuti
Nmap		192.168.50.101		SYN su tutte le porte	Trovati 20 servizi attivi sulla macchina. Porte aperte includono FTP (21/tcp), SSH (22/tcp), Telnet (23/tcp), HTTP (80/tcp), DNS (53/tcp), ecc.

Nmap		192.168.50.101		Scansione con switch «-A» sulle porte well-known	Porta 21/tcp (FTP) aperta con vsftpd 2.3.4, Porta 22/tcp (SSH) aperta con OpenSSH 4.7p1 Debian 8ubuntu1, Porta 23/tcp (Telnet) aperta con Linux telnetd, Porta 25/tcp (SMTP) aperta con Postfix smtpd, Porta 53/tcp (Domain) aperta con ISC BIND 9.4.2, ecc.
------	--	----------------	--	--	--

Nmap		192.168.50.101		TCP su tutte le porte	Trovati 80 servizi attivi sulla macchina. Porte aperte includono FTP, SSH, HTTP, Telnet, ecc.
------	--	----------------	--	-----------------------	---

- Le scansioni SYN forniscono una visione rapida delle porte aperte senza completare le connessioni.
- Scansioni TCP su tutte le porte offrono una panoramica completa dei servizi disponibili sulla macchina.
- La scansione completa con rilevamento è fondamentale per ottenere informazioni dettagliate, inclusi OS e versioni di servizi.
- La specificità delle scansioni su porte specifiche (20-1024) consente una focalizzazione mirata.

Conclusioni Generali:

Ogni comando adotta un approccio diverso alla scansione di Metasploitable, offrendo livelli variabili di dettaglio e discrezione.

La scansione completa con rilevamento (-A) è essenziale per una valutazione completa della sicurezza.

Le scansioni SYN su porte well-known sono rapide e forniscono informazioni su servizi comuni.

L'uso del sistema DNS del sistema contribuisce alla precisione delle risoluzioni DNS durante la scansione.