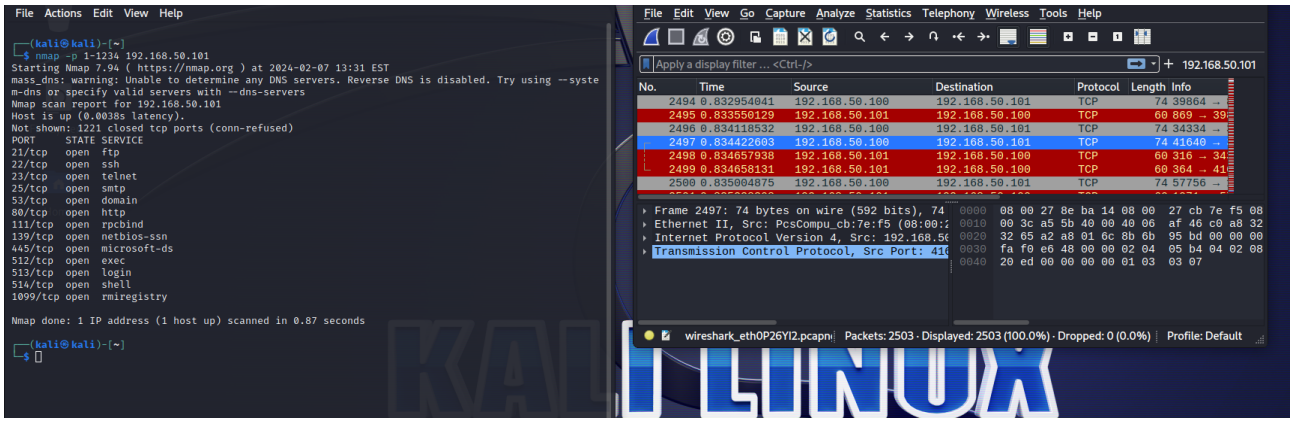
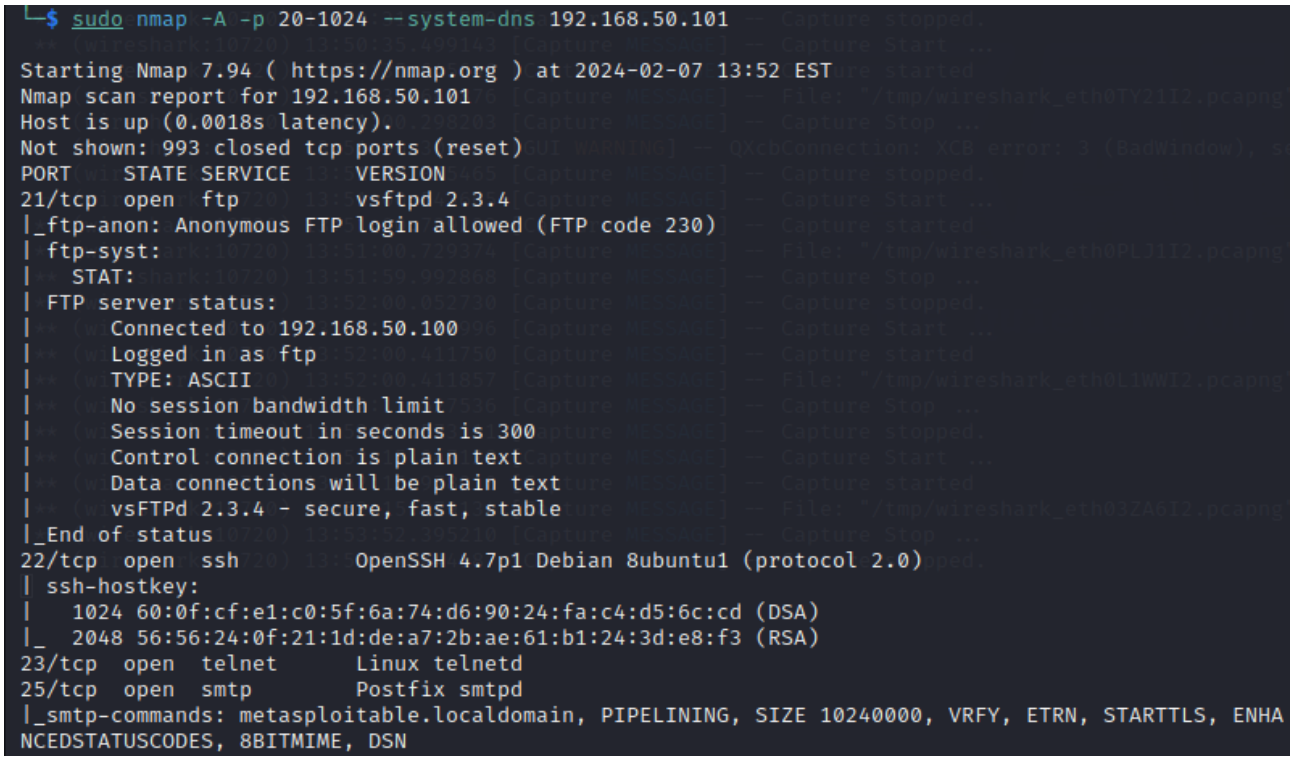
Report di Analisi con Nmap su Metasploitable: Scansione dei Servizi di Rete e Differenze tra Scansione TCP e SYN



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

Risultati Chiave:

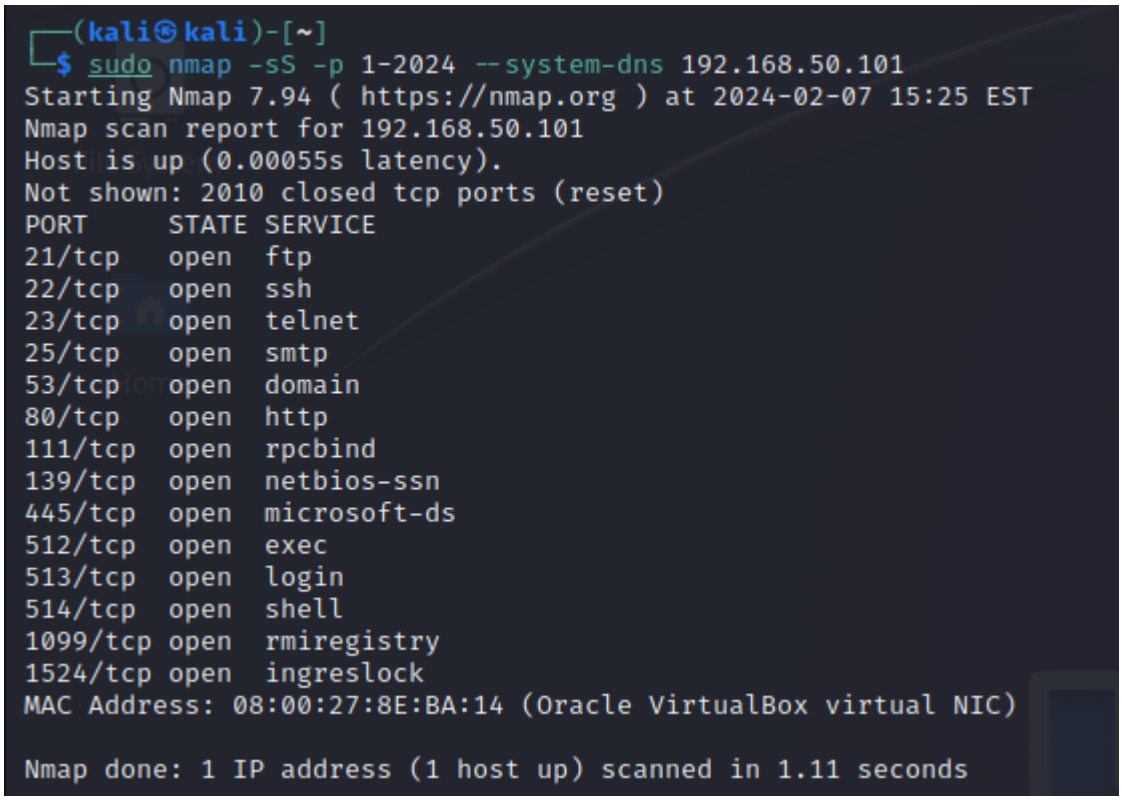
- Scansione SYN su porte well-known da 1 a 1023.
- Utilizzo del comando **sudo** per ottenere privilegi elevati e rilevare servizi su porte comuni.
- Identificati servizi come FTP, SSH, Telnet, HTTP, e altri.
- Adatta per una scansione rapida focalizzata su porte comunemente utilizzate.



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.



. 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.