Information Gathering - Metasploitable

Il presente report documenta l'attività di information gathering effettuata sulla macchina target Metasploitable (192.168.50.101) da una macchina attaccante Kali Linux (192.168.50.101). L'obiettivo è raccogliere il maggior numero di informazioni possibili sul target utilizzando vari strumenti di reconnaissance.

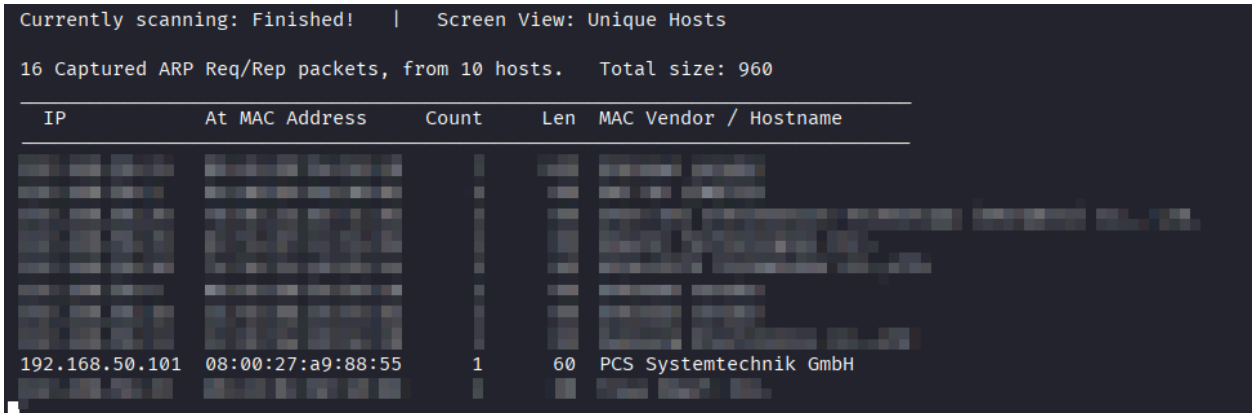
Host Discovery - Netdiscover

È stato utilizzato **Netdiscover**, uno strumento di ARP scanning per identificare tutti gli host attivi sulla rete locale attraverso richieste ARP.

Risultati: Sono stati catturati 16 pacchetti ARP Request/Reply da 10 host diversi (dimensione totale: 960 bytes). Tra gli host identificati:

- **192.168.50.101**: MAC Address 08:00:27:a9:88:55 - PCS Systemtechnik GmbH (Oracle VirtualBox)

L'ARP scan ha confermato la presenza dell'host target e ha fornito informazioni sul vendor della scheda di rete virtuale.



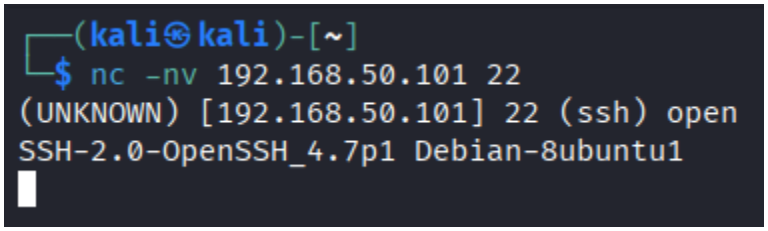
Banner Grabbing - Netcat

È stato utilizzato **netcat (nc)** per verificare la connettività verso specifiche porte (la 22 in questo caso) del target.

Test porta SSH (22): **Comando**: `nc -nv 192.168.50.101 22`

Risultato: Connessione riuscita alla porta 22 (SSH). Il banner rivela: `SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1`

Questo conferma che il servizio SSH è attivo e funzionante, con versione OpenSSH 4.7p1 su Debian/Ubuntu.

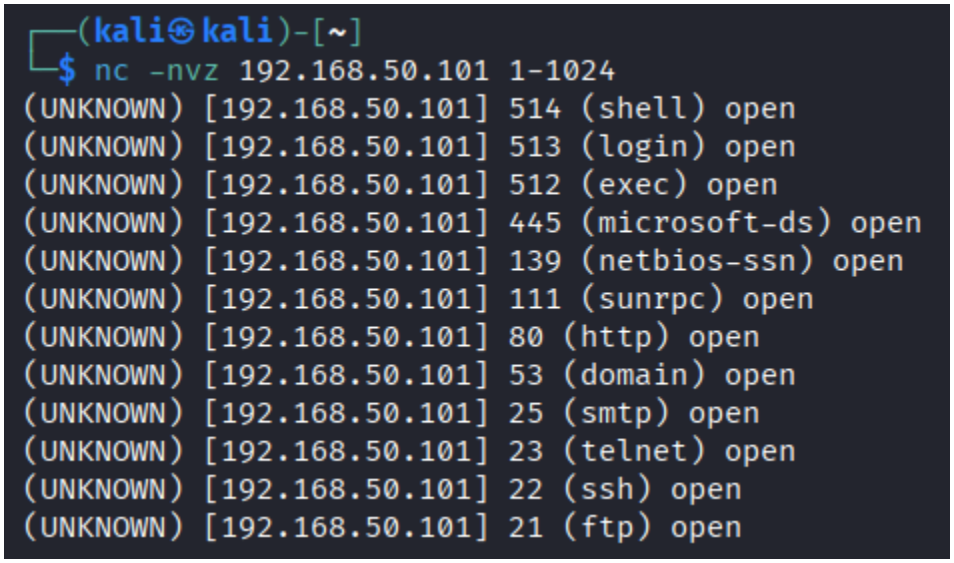


Port Scanning - Netcat

Test multiplo porte con range: **Comando**: `nc -nvz 192.168.50.101 1-1024`

Risultati: Netcat ha identificato numerose porte aperte nel range 1-1024:

La scansione ha confermato la presenza di molteplici servizi di rete attivi, inclusi servizi legacy potenzialmente vulnerabili.

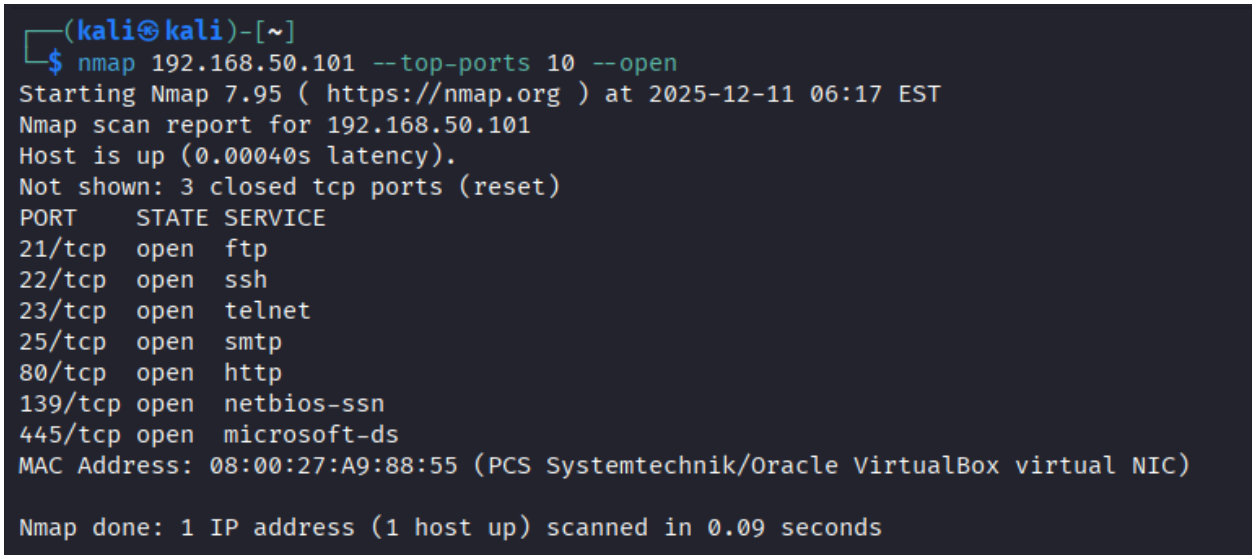


Port Scanning - Nmap (Top Ports)

È stata effettuata una scansione Nmap focalizzata sulle prime 10 porte più comuni.

Comando: `nmap 192.168.50.101 --top-ports 10 --open`

La scansione è stata completata in 0.09 secondi, confermando rapidamente i servizi principali esposti.



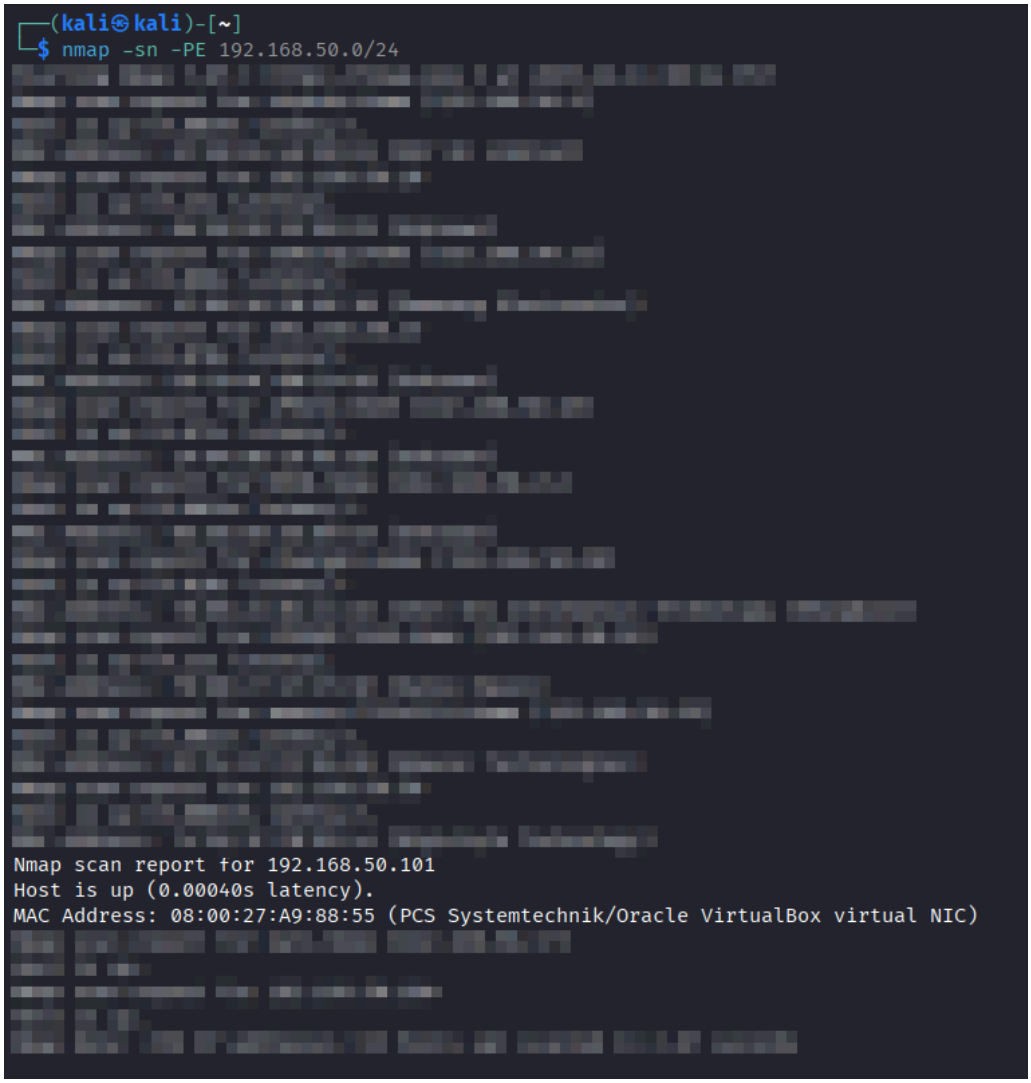
Host Discovery - Nmap

Comando: `nmap -sn -PE 192.168.50.0/24`

Risultati: La scansione ha completato l'enumerazione della rete 192.168.50.0/24 identificando l'host 192.168.50.101 come attivo con latenza di 0.00040s.

MAC Address: 08:00:27:A9:88:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Questa scansione ha confermato la presenza del target sulla rete e le sue caratteristiche hardware virtuali.



Conclusioni

La fase di information gathering ha permesso di raccogliere informazioni dettagliate sul target Metasploitable. L'host presenta una configurazione volutamente vulnerabile con numerosi servizi esposti, molti dei quali utilizzano protocolli obsoleti o non sicuri. Le informazioni raccolte costituiscono una base solida per eventuali fasi successive di vulnerability assessment e penetration testing. La combinazione di diversi strumenti (**masscan**, **netcat**, **nmap**) ha permesso di ottenere una visione completa e accurata del target da diverse prospettive.