REPORT S7/L1

TEST DI PENETRAZIONE E VULNERABILITÀ

Attaccante: Victor Rosati

Data: 20 Gennaio 2026

Target: Metasploitable 2 (IP: 192.168.1.149)

Attaccante: Kali Linux (IP: 192.168.1.100)

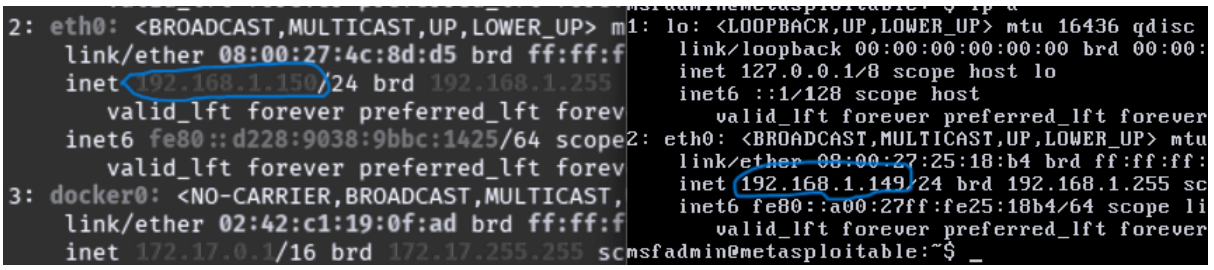
OBIETTIVO DELLA TASK

L'obiettivo dell'esercitazione consiste nel testare la sicurezza di un server FTP specifico, identificare una vulnerabilità nota e sfruttarla tramite il framework Metasploit per ottenere l'accesso amministrativo. Al termine dell'accesso, è richiesta la creazione di una cartella denominata `/test metasploit` nella root del sistema vittima.

FASE 1: CONFIGURAZIONE DELLA RETE

Per garantire la comunicazione tra le macchine virtuali, è stata configurata una rete locale statica:

- **Kali Linux:** IP impostato su `192.168.1.100` tramite comando `ifconfig`.
- **Metasploitable:** IP impostato su `192.168.1.149` per rispettare le specifiche della traccia.



FASE 2 & 3: SCANNING ED ENUMERAZIONE

È stata eseguita una scansione delle porte tramite **Nmap** per identificare i servizi attivi sul target.

- **Risultato Scanning:** Identificata la porta **21/TCP** (FTP) in stato `open`.

- **Risultato Enumeration:** Il servizio è stato identificato come **vsFTPd 2.3.4**, versione nota per contenere una backdoor pre-installata.

FASE 4: VERIFICA MANUALE (MANUAL CHECK)

Prima di procedere con l'attacco automatizzato, è stata effettuata una connessione manuale al server FTP per confermare il banner del servizio.

- **Comando utilizzato:** `ftp 192.168.1.149`.
- **Accesso:** Effettuato con successo tramite utente `anonymous`.
- **Conferma:** Il banner ha restituito esattamente `220 (vsFTPd 2.3.4)`.

FASE 5: EXPLOITATION (METASPLOIT)

Per ottenere l'accesso remoto, è stato utilizzato il framework Metasploit.

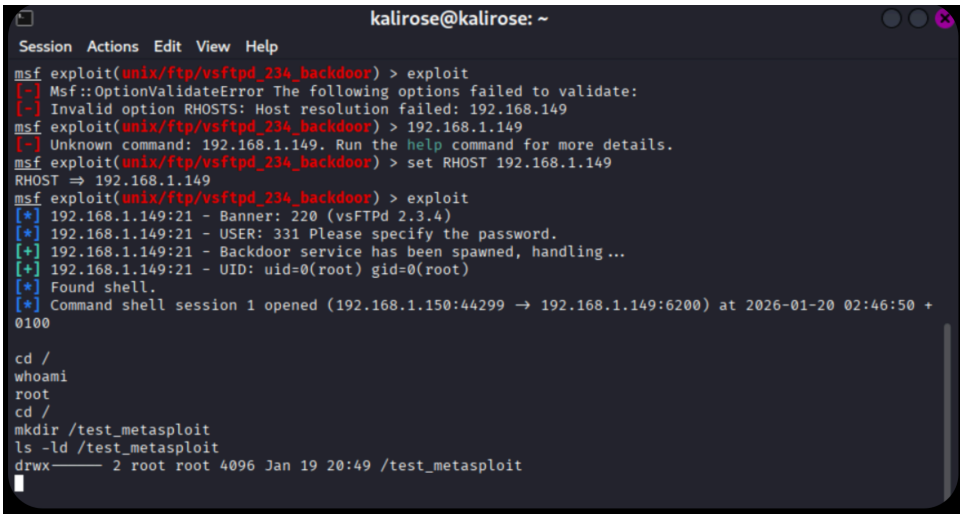
- **Modulo:** `exploit/unix/ftp/vsftpd_234_backdoor`.
- **Payload:** `cmd/unix/interact` (configurato automaticamente).
- **Target IP (RHOSTS):** `192.168.1.149`.

L'esecuzione del comando `exploit` ha permesso l'apertura di una **Command Shell session** con privilegi di **root** (`uid=0`).

FASE 6: POST-EXPLOITATION E COMPLETAMENTO

Una volta all'interno del sistema vittima, è stato verificato l'utente tramite `whoami` (risultato: `root`) e completata l'operazione richiesta dalla task.

- **Navigazione:** `cd /` (spostamento nella directory root).
- **Creazione Cartella:** `mkdir /test_metasploit`.
- **Verifica finale:** Il comando `ls -ld /test_metasploit` ha confermato la corretta creazione della directory con privilegi amministrativi.



NOTE TECNICHE E CONCLUSIONI

Il test ha confermato l'estrema vulnerabilità della versione **vsFTPd 2.3.4**, che permette l'accesso come root in pochi secondi.

Durante l'attività sono stati gestiti con successo due imprevisti critici:

- **Configurazione di rete:** Risolti problemi iniziali di instradamento e comunicazione tra le VM per allinearle sulla stessa sottorete locale.
- **Troubleshooting:** Gestito un crash improvviso del sistema target (**Kernel panic**) durante la fase di attacco. La stabilità è stata ripristinata tramite riavvio forzato e riconfigurazione rapida dei servizi, permettendo il completamento della task.

Gestire questi intoppi tecnici ha dimostrato che un Penetration Tester deve possedere non solo competenze di hacking, ma anche solide basi di networking e capacità di risoluzione problemi in tempo reale.