Attacco al Servizio vsftpd con Metasploit

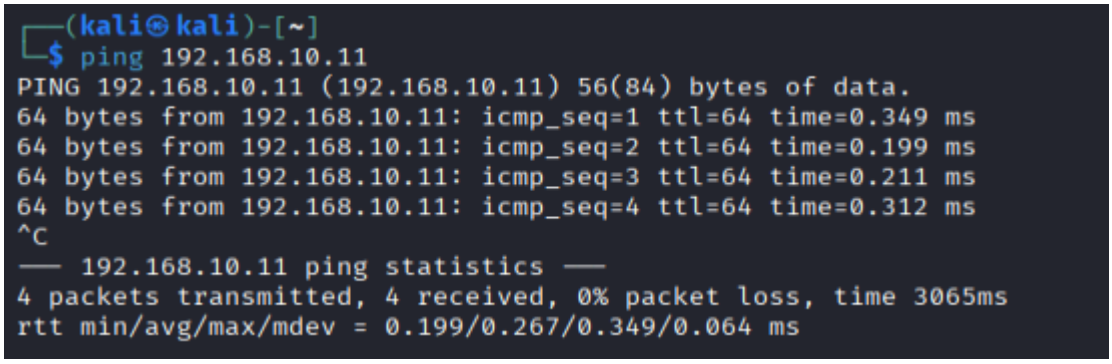
Introduzione

L'obiettivo è stato quello di eseguire un attacco mirato al servizio vsftpd su una macchina virtuale Metasploitable utilizzando il framework Metasploit.

Il compito finale richiedeva la creazione di una cartella denominata "test_metasploit" nella directory root della macchina compromessa.

Verifica della Connettività di Rete

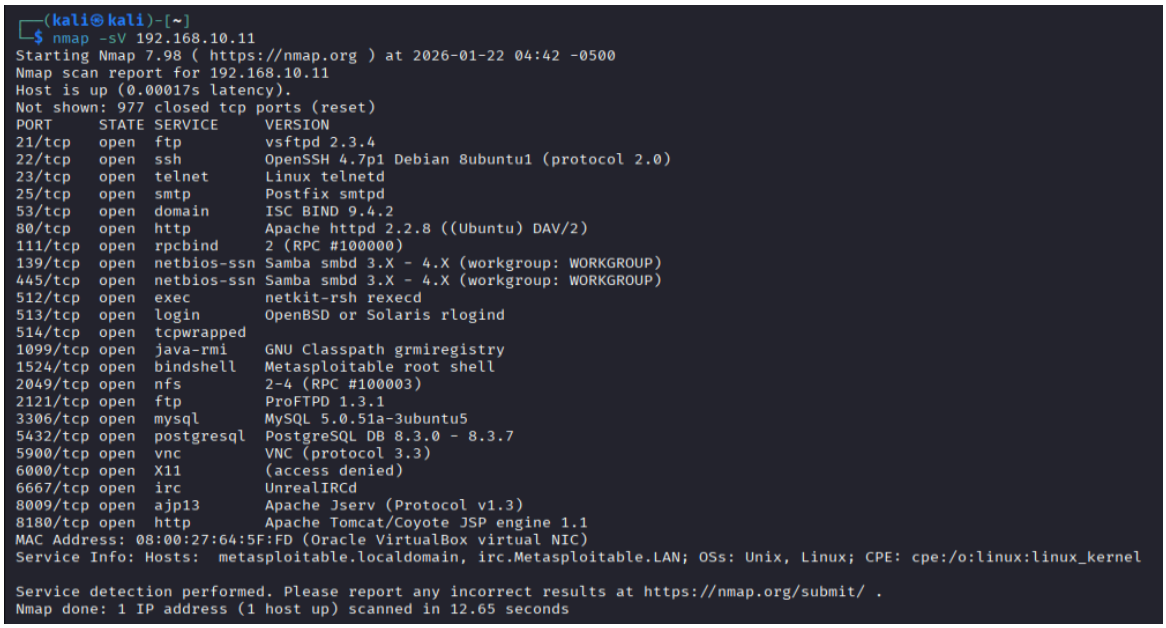
Ho iniziato il mio lavoro verificando se la macchina Metasploitable fosse effettivamente raggiungibile e attiva sulla rete.



Questo primo passaggio è cruciale: senza una connessione di rete funzionante, non sarebbe stato possibile procedere con l'attacco.

Scansione del Bersaglio con Nmap

Dopo aver confermato la connettività, ho proceduto con una scansione di rete approfondita utilizzando lo strumento nmap con il flag `-sV` per rilevare i servizi e le loro versioni.



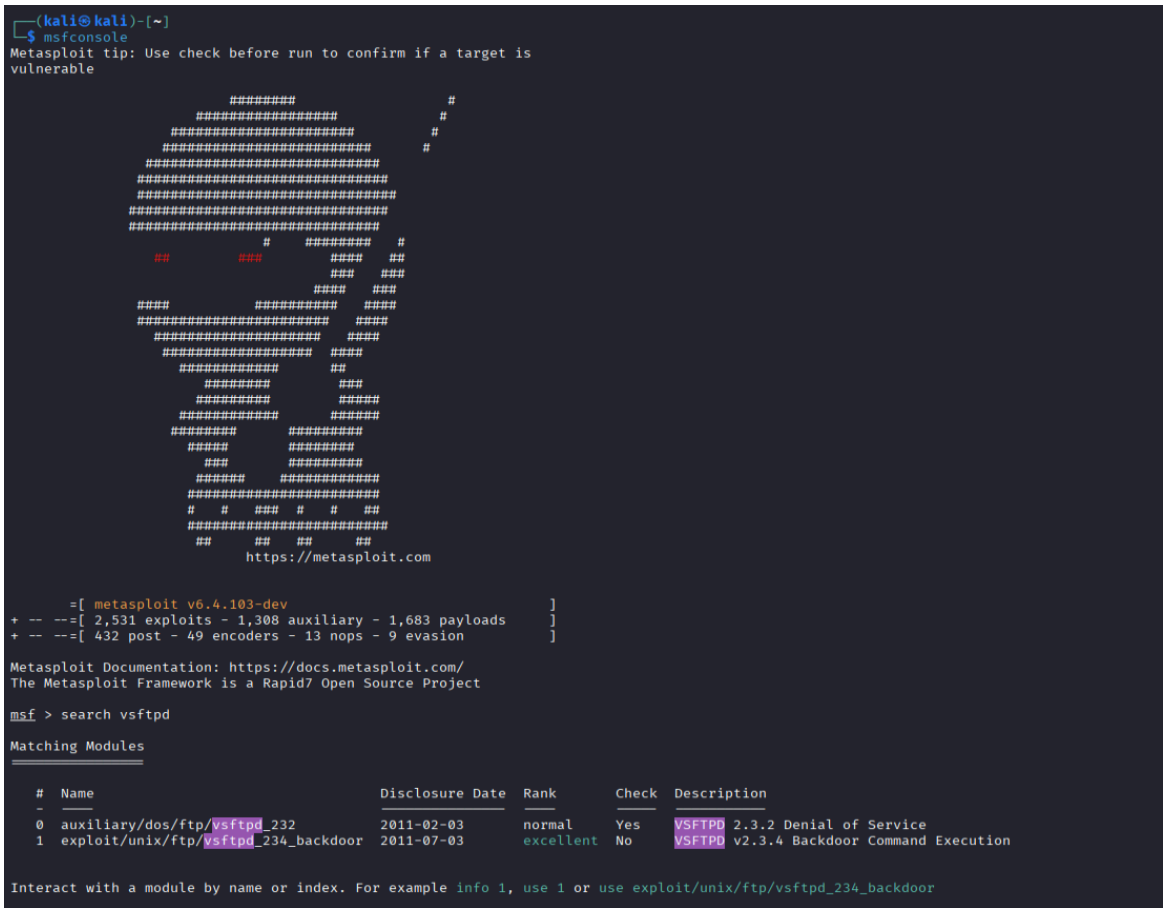
La scansione ha rivelato numerosi servizi attivi sulla macchina Metasploitable. In particolare, ho identificato il servizio che mi interessava:

- **Porta 21/tcp**: FTP - vsftpd 2.3.4

Questo era esattamente il bersaglio dell'esercizio.

Accesso a Metasploit e Ricerca dell'Exploit

Ho avviato Metasploit e ho cercato i moduli di exploit disponibili per vsftpd.



Sono stato presentato con due moduli principali.

Ho scelto il secondo modulo poiché era quello con ranking più alto ("excellent") e corrispondeva perfettamente alla versione 2.3.4 identificata sulla macchina bersaglio.

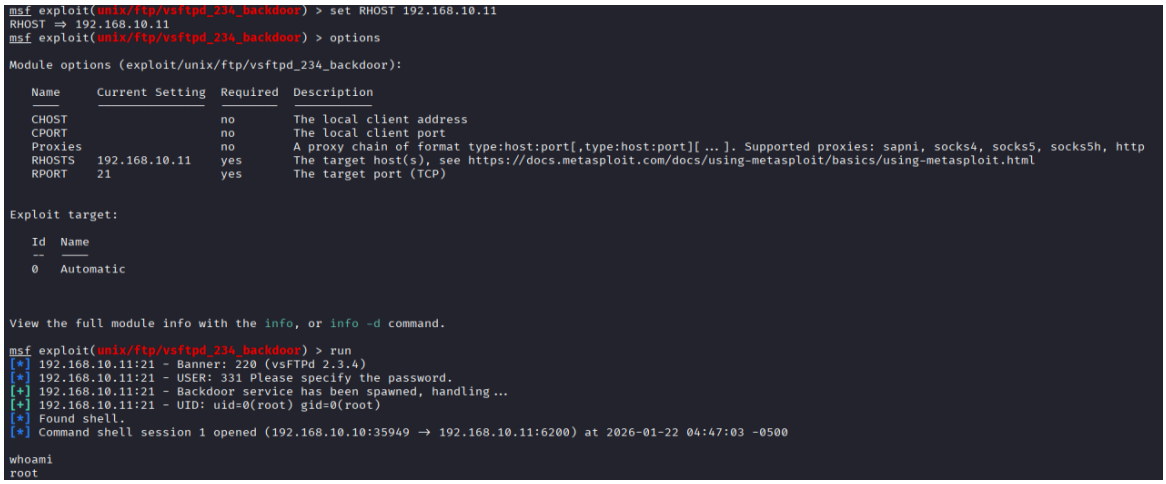
Configurazione ed Esecuzione dell'Exploit

Ho selezionato il modulo di exploit e ho proceduto alla sua configurazione.

Figure 4: Configurazione iniziale dell'exploit vsftpd_234_backdoor

Nella figura 4, è visibile il processo di configurazione. Ho eseguito i seguenti passaggi:

1. Selezionato il modulo con il comando: `use exploit/unix/ftp/vsftpd_234_backdoor`
2. Impostato l'indirizzo IP bersaglio (RHOSTS) con: `set RHOSTS 192.168.1.11`
3. Verificato le opzioni disponibili con: `options`



Ho lanciato l'exploit utilizzando il comando `run`, e il sistema ha proceduto con l'attacco.

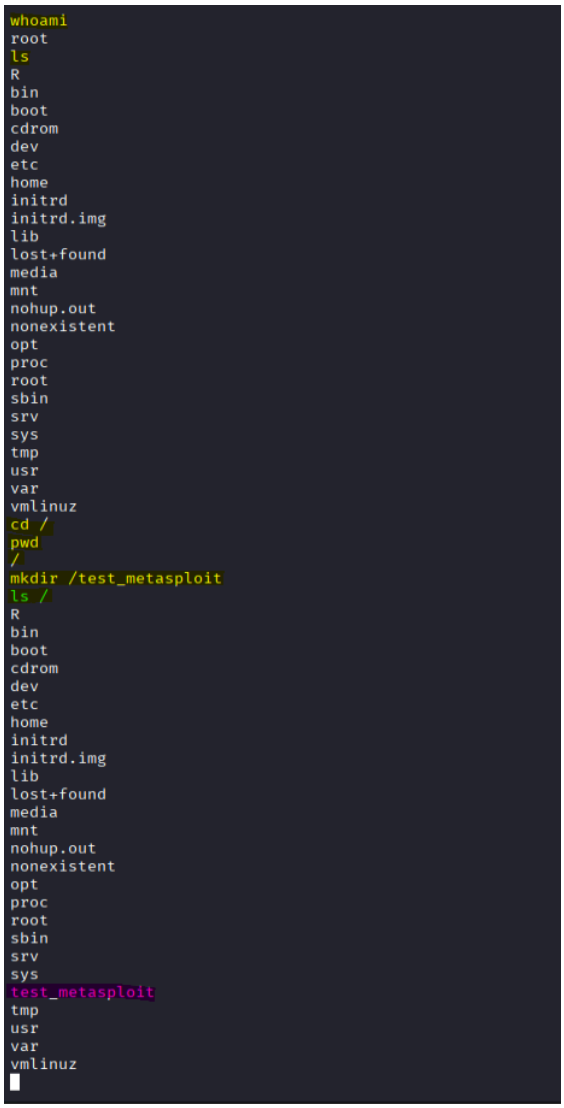
L'exploit ha:

1. Identificato il banner del servizio vsftpd versione 2.3.4
2. Inviato il payload dannoso al servizio FTP
3. Triggerato il "backdoor" (porta di fondo) presente nella versione vulnerabile
4. Ottenuto una shell di comando con privilegi di root (uid=0)

Una volta che ho digitato *`whoami`*, il sistema ha confermato che ero loggato come utente "root", il che significava avere i più alti privilegi sulla macchina bersaglio.

Navigazione e Creazione della Cartella

Dopo aver ottenuto accesso alla macchina Metasploitable, ho proceduto a completare il compito finale: creare la cartella "test_metasploit" nella directory root.



Ho eseguito i seguenti comandi:

1. `cd /` - per navigare alla directory root del sistema
2. `pwd` - per confermare la mia posizione (risultato: `/`)
3. `mkdir /test_metasploit` - per creare la cartella richiesta
4. `ls /` - per verificare che la cartella fosse stata creata

La cartella è stata creata con successo ed è visibile nelle ultime righe dell'output

Conclusioni

Questa esperienza pratica mi ha permesso di comprendere come i framework di penetration testing come Metasploit semplificano il processo di identificazione e sfruttamento delle vulnerabilità note. La vulnerabilità in vsftpd 2.3.4 era una backdoor intenzionalmente inserita

in quella versione specifica, e il fatto che Metasploit disponga di un exploit perfettamente calibrato per questo bersaglio dimostra l'importanza di mantenere i sistemi aggiornati e di monitorare costantemente le versioni dei servizi critici.