REPORT TECNICO

HACKING CON METASPLOIT

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 19/01/2026

1. Introduzione

L’attività di oggi consiste nello sfruttare la vulnerabilità sul servizio “**vsftpd**” della macchina Metasploitable mediante l’utilizzo di **Metasploit**.

Una volta dentro dovremo creare una cartella chiamata test_metasploit all’interno della **root** dimostrando così di essere riusciti ad ottenere il totale controllo della macchina Target.

ATTENZIONE: l’attività viene svolta all’interno di un ambiente controllato per scopo didattico, non sono stati eseguiti exploit nei confronti di dispositivi all’esterno di tale ambiente.

2. Ambiente di Lavoro e Strumenti

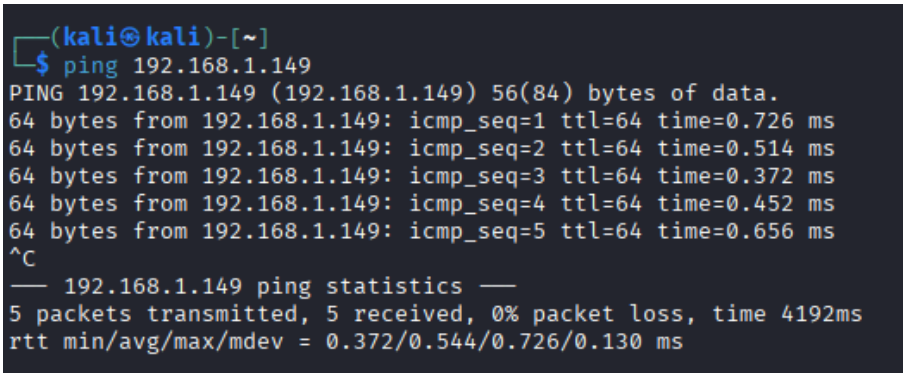
Configurazione del Laboratorio

L’ambiente di test sarà costituito da una macchina attaccante ed una macchina target collegate entrambe in NAT.

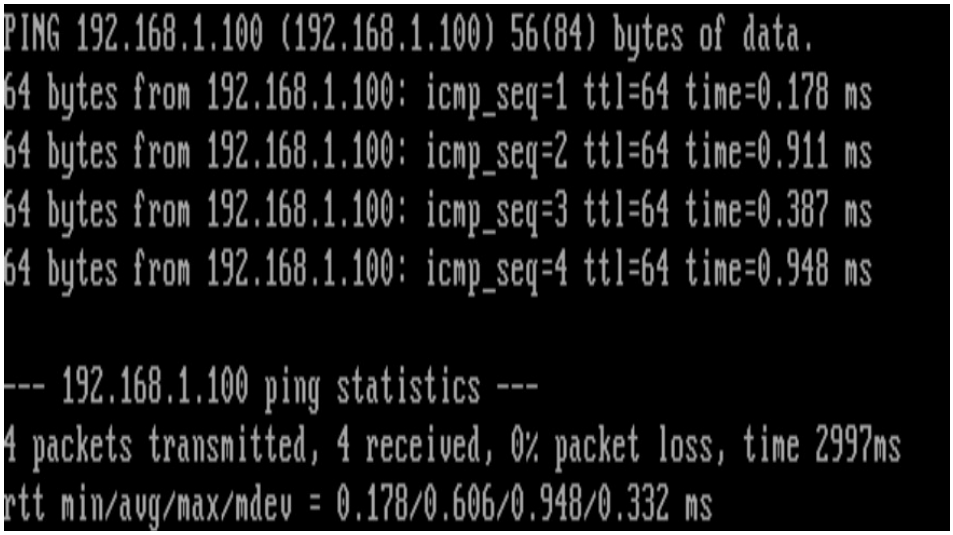
- **Macchina Attaccante:** Kali Linux 2025.3 - IP: 192.168.1.100
- **Macchina Vittima:** Metasploitable 2 - IP: 192.168.1.149
- **Rete:** Rete con Nat

Una volta configurato il nostro laboratorio virtuale eseguiamo il ping su entrambe le macchine per verificare che siano in comunicazione tra loro.

Kali → Metasploitable



Metasploitable → Kali



Strumenti Utilizzati

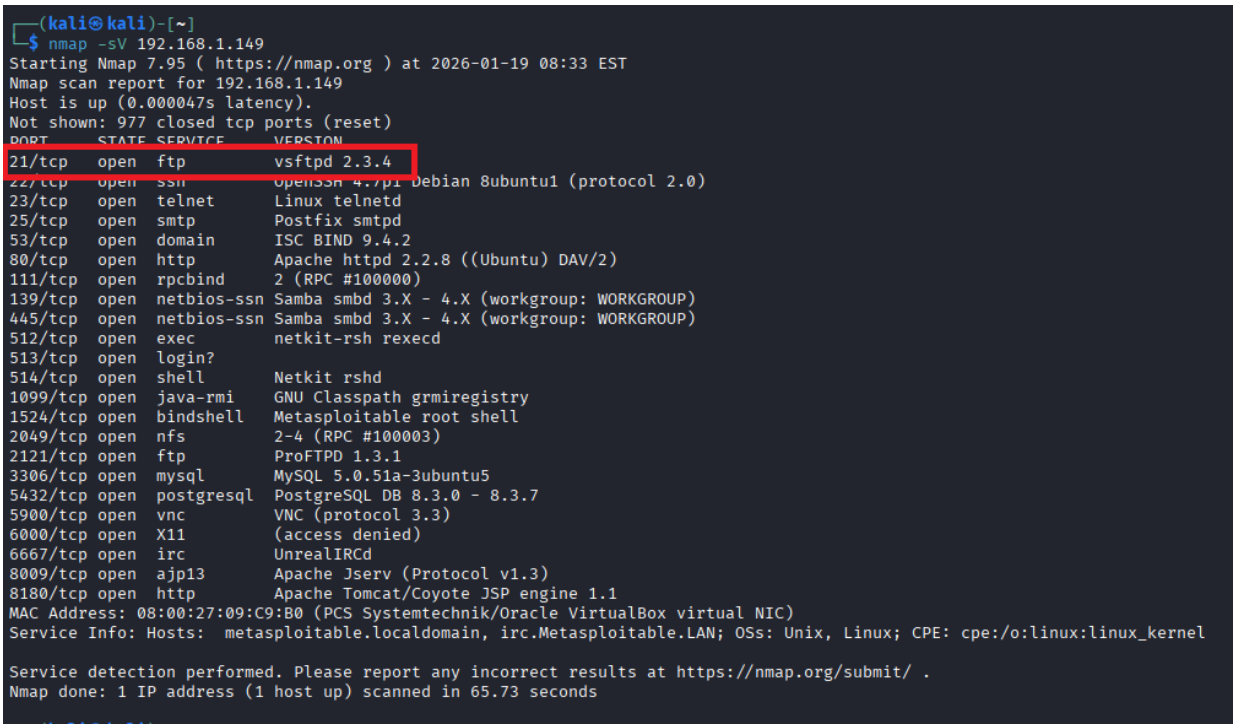
- **Nmap:** Questo tool è essenziale per la fase preliminare. Nelle slide viene mostrato come usarlo per scansionare l'indirizzo IP target
- **Metasploit Framework (msfconsole):** Lo useremo per cercare la vulnerabilità specifica del servizio FTP, configurare l'exploit ed eseguire l'attacco.

3. Attività Tecnica e Metodologia

Fase di Ricognizione

In questa fase utilizzerò **Nmap** per effettuare un'analisi approfondita sulla macchina Target. Lancerò il seguente comando:

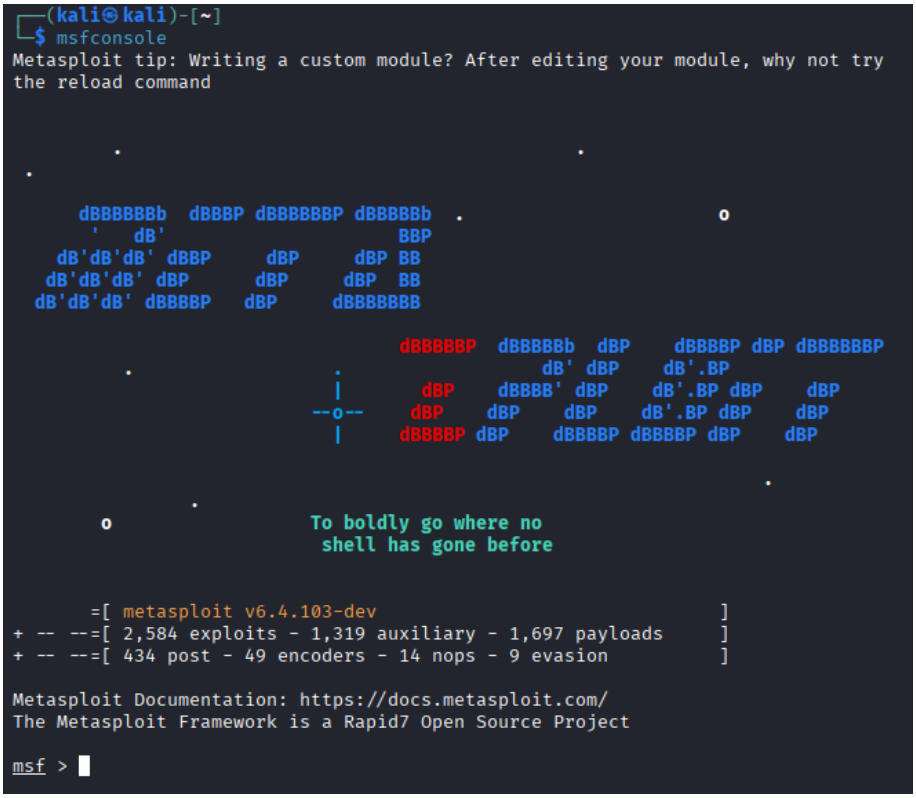
```
nmap -sV 192.168.1.149
```



Lo studio effettuato con nmap ci ha rivelato che la **porta 21/tcp** risulta aperta ed il servizio che utilizza è **vsftpd 2.3.4**.

Exploit

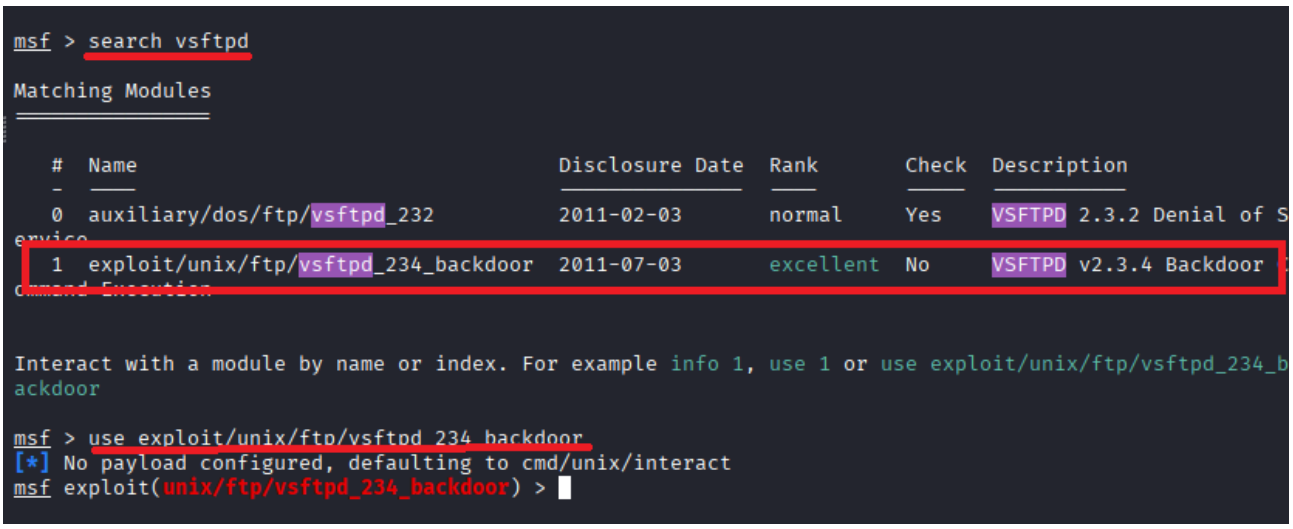
Accediamo alla console di Metasploit con il comando **msfconsole**.



Grazie al comando "**search vsfpd**" sarò in grado di filtrare unicamente i moduli che fanno riferimento proprio alla versione del servizio che vogliamo sfruttare.

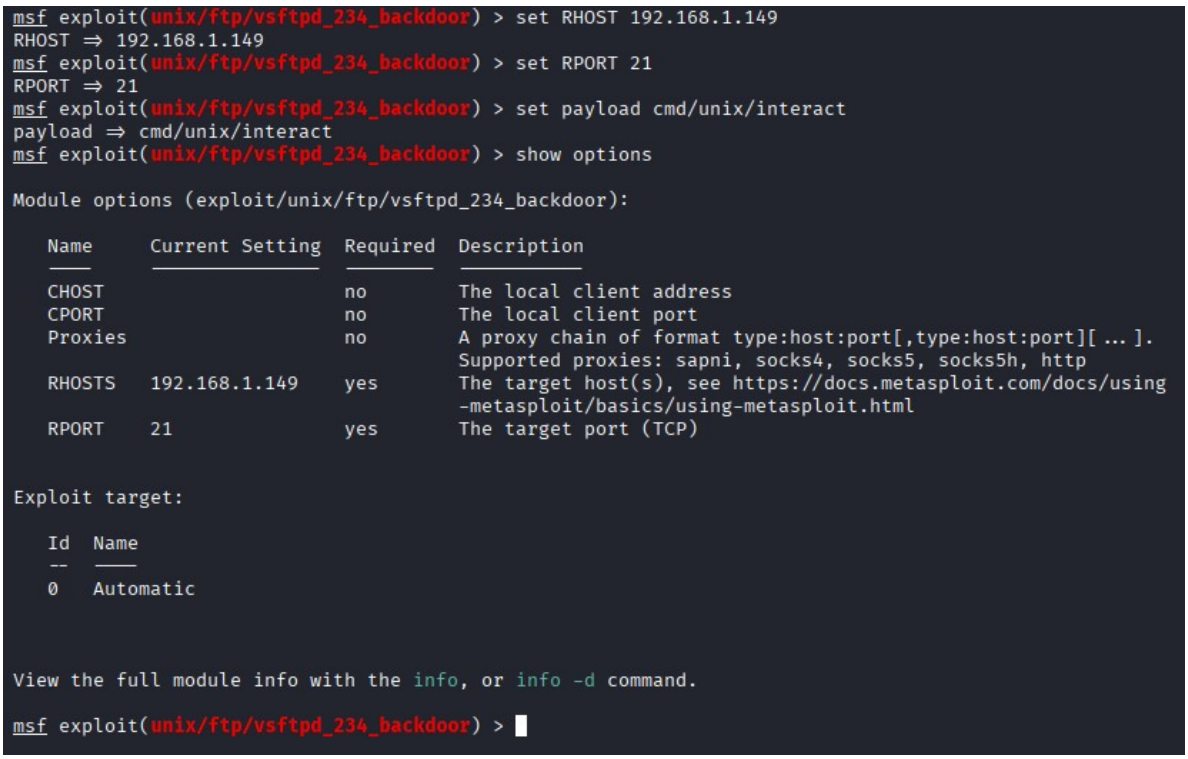
Una volta trovato selezioniamolo con il comando:

`use exploit/unix/ftp/vsftpd_234_backdoor`



Adesso dobbiamo impostare tramite il comando set tre diversi valori e verifichiamo attentamente che:

- **RHOSTS** è impostato correttamente su `192.168.1.149` (l'IP Target)
- **RPORT** è correttamente sulla porta `21` (la porta del servizio FTP)
- **Payload** è impostato su **`cmd/unix/interact`**, che è quello corretto per questo exploit specifico.

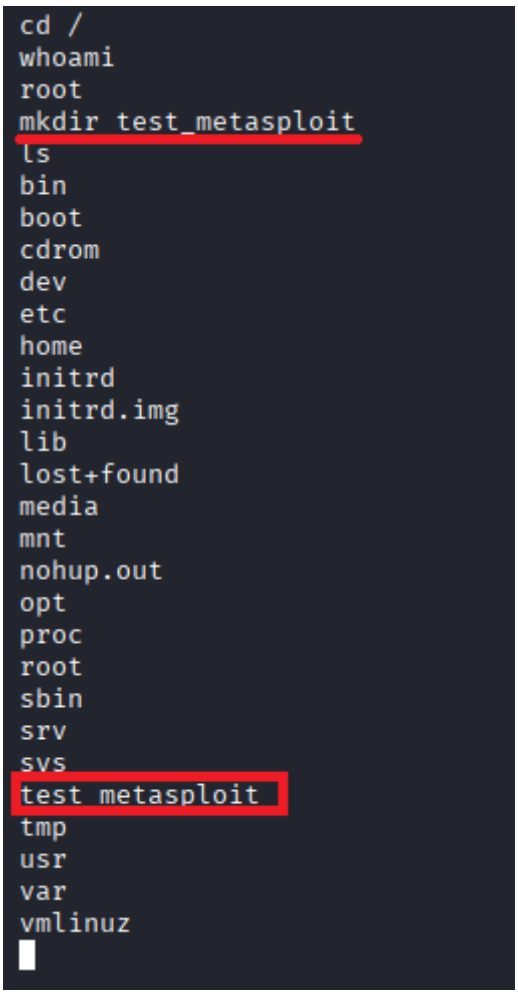


Non ci rimane che digitare “**run**” o “**exploit**” e l’attacco inizierà.

Creazione cartella in Root

Una volta terminata la fase di exploit saremo all’interno della macchina target ed avremo già i **permessi root**.

Con i permessi root avremo modo di spostarci liberamente tra le cartelle e potremo creare la cartella test_metasploit tramite il comando **mkdir**.



4. Risultati e Analisi

Vulnerabilità o Criticità Rilevate

Dall'analisi effettuata, è emersa una vulnerabilità critica sul servizio **FTP**.

- **Vulnerabilità:** Backdoor Command Execution in **VSFTPD v2.3.4.**
- **Livello di Rischio: CRITICO**.
- **Descrizione:** Il servizio **`vsftpd`** (*Very Secure FTP Daemon*) nella versione 2.3.4 contiene una **backdoor** malevola nel codice sorgente. Questa vulnerabilità permette a un attaccante di aprire una shell di comando sulla porta 6200 con i permessi root.

Interpretazione dei Dati

L'ottenimento di una shell con privilegi di **root** implica la compromissione totale della macchina vittima: l'attaccante ha il **pieno controllo su file**, configurazioni e servizi, potendo potenzialmente installare **malware persistenti** o utilizzare la macchina come ponte per attaccare altri dispositivi nella rete.

5. Conclusioni

Riepilogo

L'obiettivo dell'attività è stato pienamente raggiunto. Attraverso la fase di **Information Gathering** con Nmap è stato possibile identificare la versione vulnerabile del servizio FTP. Successivamente, utilizzando il **Framework Metasploit**, è stata sfruttata la vulnerabilità di "Backdoor Command Execution" presente in **`vsftpd 2.3.4`**.

È stato possibile stabilire una connessione e dimostrare il controllo totale del sistema target creando la directory **`/test_metasploit`**, come richiesto.

5.2 Raccomandazioni (Remediation)

Per mitigare la vulnerabilità riscontrata e mettere in sicurezza il sistema, si raccomanda di:

- **Aggiornare il Software:** Procedere all'immediata disinstallazione della versione corrente di `vsftpd` e aggiornarla all'ultima versione stabile
- **Configurazione Firewall:** Limitare l'accesso alla porta 21 (FTP) consentendo le connessioni solo dagli indirizzi IP strettamente necessari e fidati.
- **Monitoraggio:** Implementare sistemi di IDS/IPS (Intrusion Detection System) per rilevare tentativi di connessione anomali, come quelli diretti verso porte non standard
- **Disabilitazione Servizi:** Se il trasferimento file FTP non è strettamente necessario per l'operatività del server, si consiglia di **disabilitare** il servizio o sostituirlo con protocolli più sicuri come **SFTP** (*SSH File Transfer Protocol*).