Report Hacking con Metasploit: Sfruttamento vulnerabilità vsftpd 2.3.4

Data: 19/01/2026
Studente: Nicola Cassandra
Obiettivo: Verifica della sicurezza del servizio FTP su server Linux e simulazione di accesso non autorizzato.

Introduzione e Configurazione dell'Ambiente

L'attività ha avuto come scopo la simulazione di un attacco informatico verso la macchina virtuale target Metasploitable. Come da indicazione sulla macchina target è stato impostato un indirizzo IP statico specifico per renderla raggiungibile all'interno della rete locale simulata.

Configurazione IP Target:

- **IP Assegnato:** `192.168.1.149`
- **Netmask:** `/24` (`255.255.255.0`)

Ho verificato la comunicazione tra le macchine tramite un ping test.

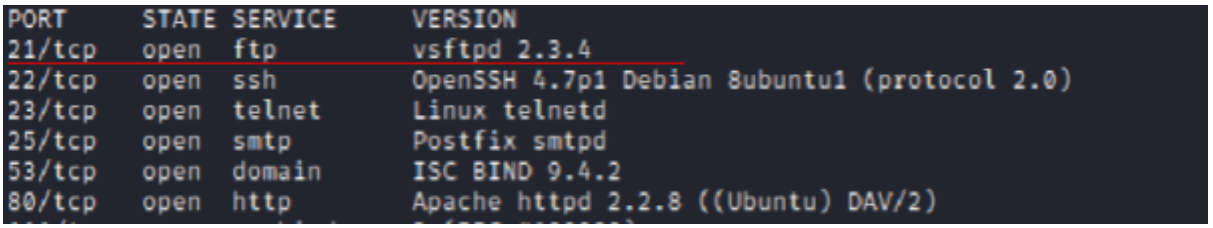
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=7.72 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=2.16 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=1.74 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=1.50 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=1.82 ms
^C
── 192.168.1.149 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4024ms
rtt min/avg/max/mdev = 1.498/2.986/7.720/2.376 ms
```

Metasploit Framework

Per l'esecuzione di questo test è stato utilizzato **Metasploit**, una piattaforma dedicata principalmente al penetration testing e alla ricerca in merito a vulnerabilità. Questo strumento è considerato uno standard da parte della comunità e la sua funzione principale è permettere ai professionisti della sicurezza di identificare, sfruttare e verificare le vulnerabilità presenti nei sistemi target. Metasploit si distingue per la sua vasta libreria di **exploit** e **payload** (codici che vengono eseguiti una volta ottenuto l'accesso, come ad esempio una shell di comando). Grazie alla sua versatilità e alla capacità di automatizzare test complessi, è lo strumento ideale per simulare attacchi reali in un ambiente controllato.

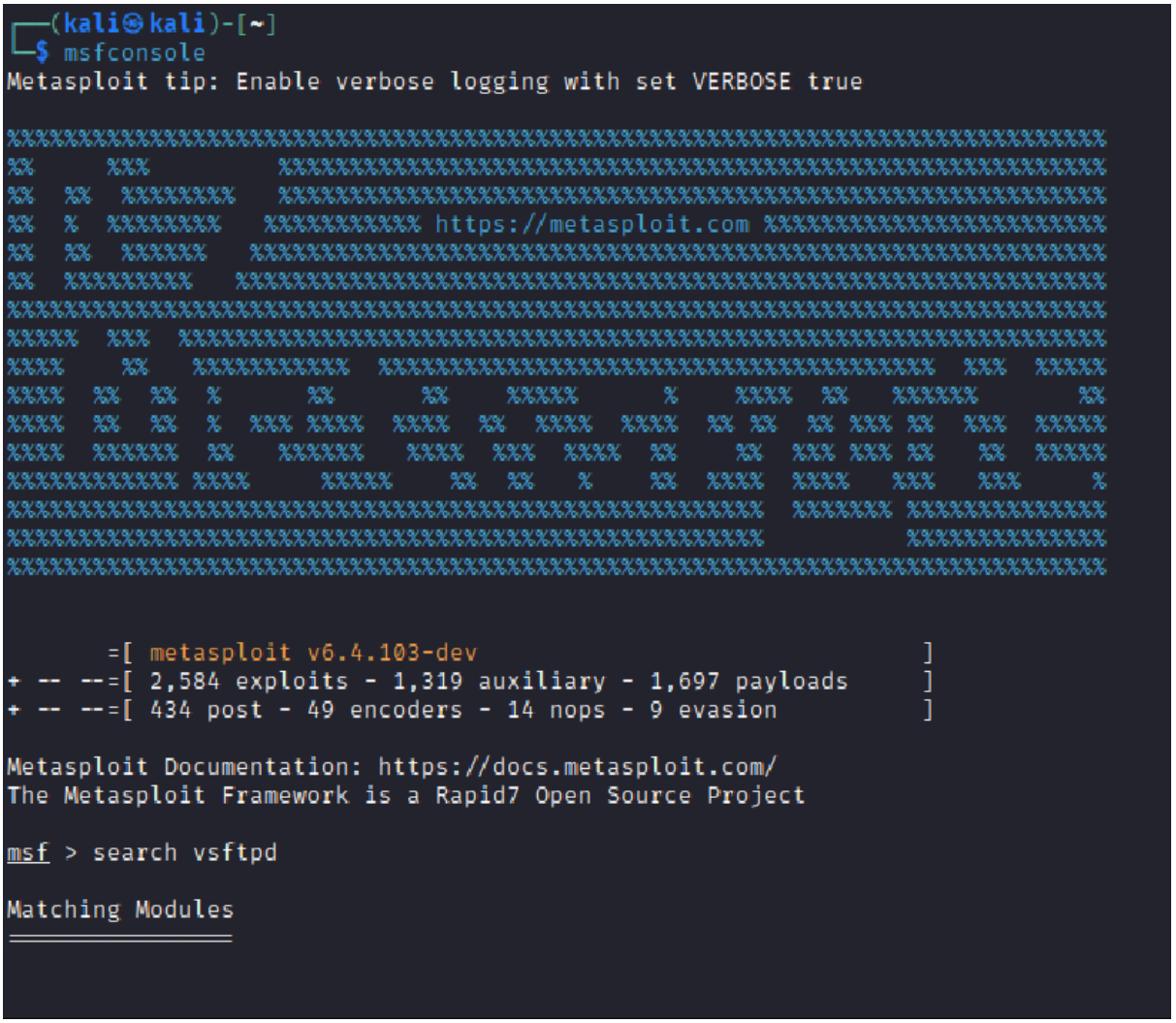
Analisi della Vulnerabilità

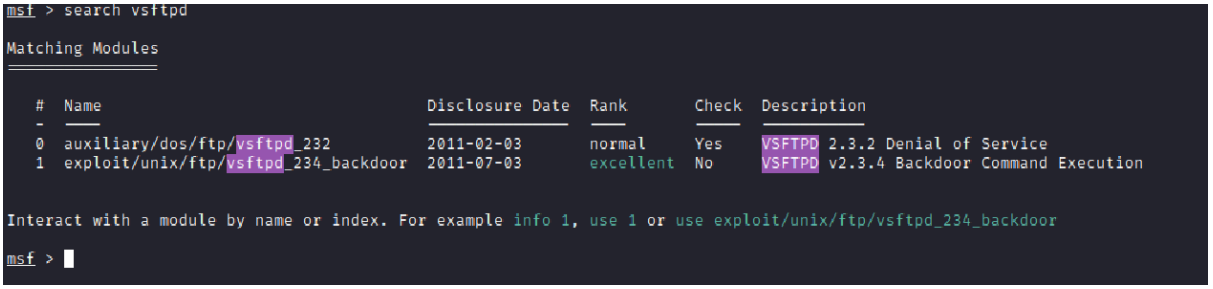
L'analisi si è concentrata sul servizio FTP attivo sulla porta standard **21**. Ho effettuato una scansione tramite lo strumento NMAP per verificare la versione del servizio tramite il comando nella schermata sottostante:



Questa specifica versione è nota per contenere una grave vulnerabilità di tipo "Backdoor Command Execution". Quest'ultima, se sfruttata, permette a un attaccante esterno di ottenere l'esecuzione di comandi entrando con i privilegi più alti disponibili (ROOT).

Per procedere, ho avviato la console **MSFConsole** (l'interfaccia a riga di comando di Metasploit) e ho interrogato il database interno per cercare exploit relativi a questo servizio utilizzando il comando `search`.





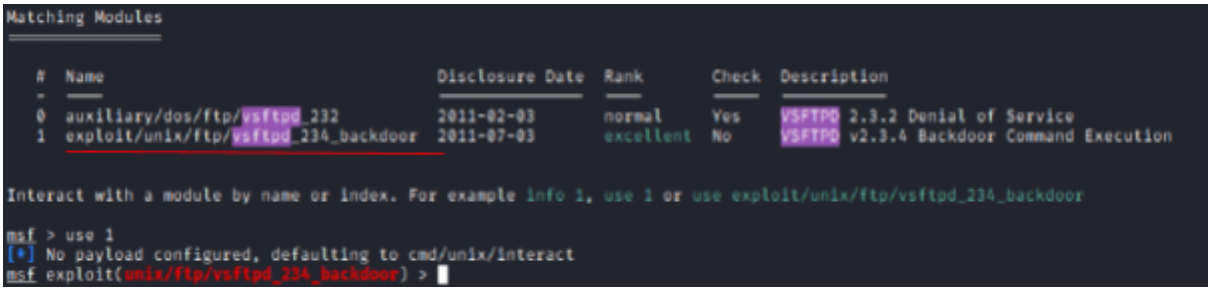
Selezione e Configurazione dell'Exploit

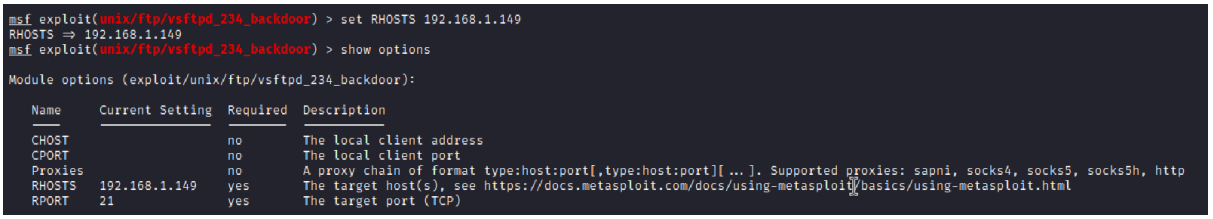
Dalla ricerca è emerso un modulo specifico: `exploit/unix/ftp/vsftpd_234_backdoor`

Ho caricato il modulo con il comando `use` e analizzato le opzioni richieste per il suo funzionamento tramite il comando `show options`.

La configurazione ha richiesto l'impostazione del parametro **RHOSTS** (Remote Host), che ho valorizzato con l'indirizzo IP della macchina vittima precedentemente configurato

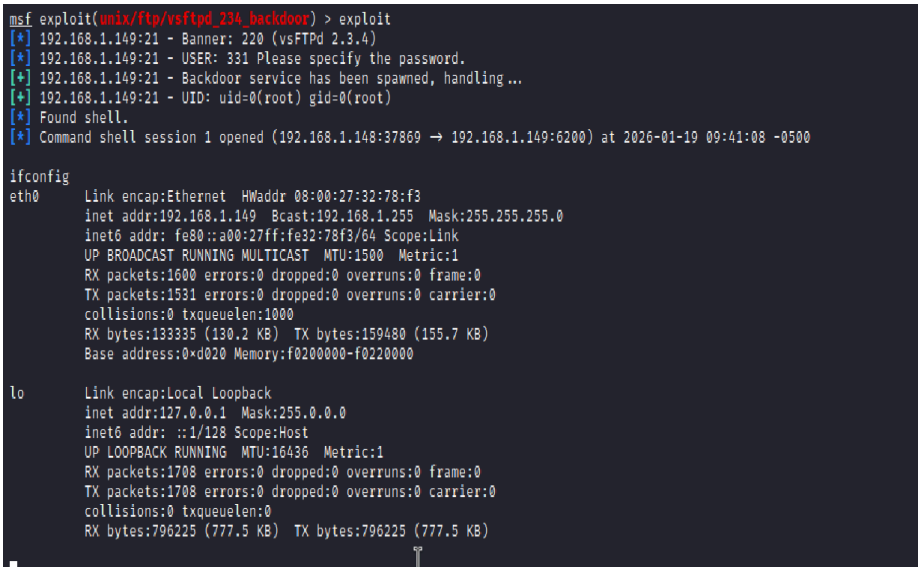
(192.168.1.149). La porta target (**RPORT**) era già correttamente impostata di default sulla 21.





Esecuzione dell'Attacco: Exploitation

Una volta terminata la configurazione, ho lanciato l'attacco tramite il comando `exploit`. Il framework ha inviato il payload verso il bersaglio. La vulnerabilità è stata sfruttata con successo: la backdoor presente nel codice di vsftpd si è aperta, garantendo l'accesso al sistema e l'apertura di una shell pronta all'utilizzo.

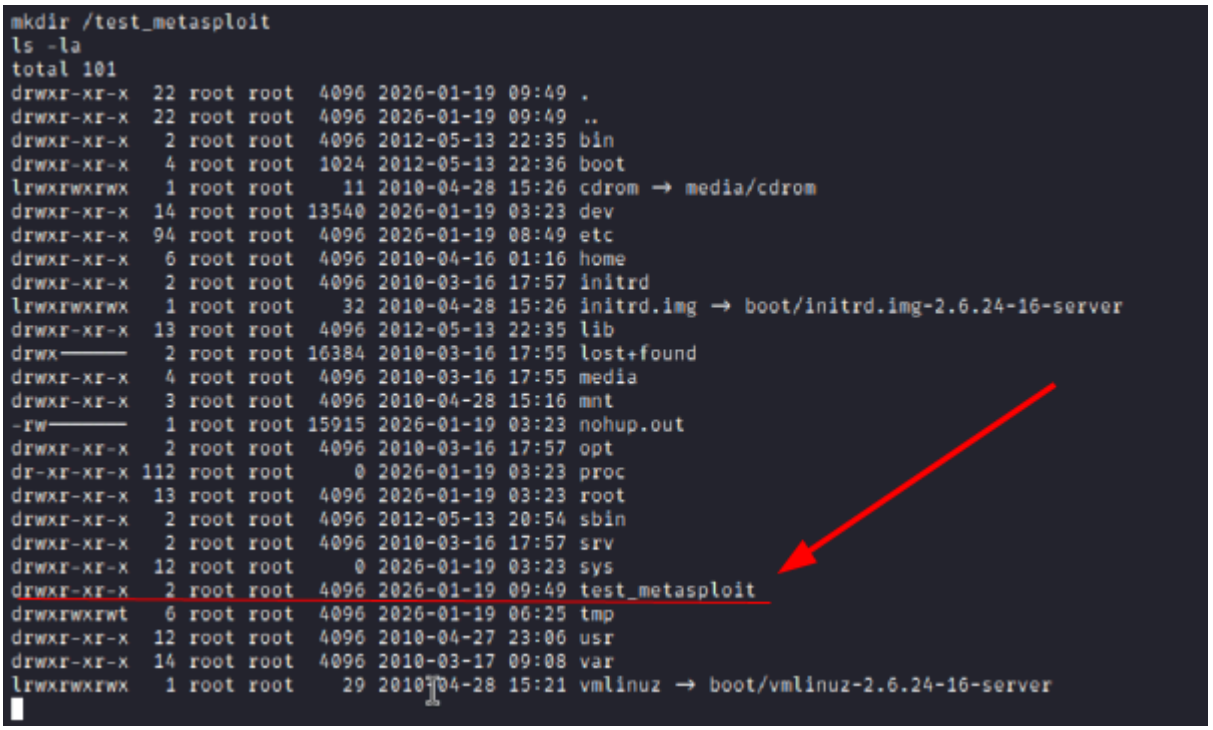


Per confermare l'identità della macchina, ho eseguito il comando `ifconfig`, che ha confermato l'indirizzo IP 192.168.1.149.

Post-Exploitation e Verifica Privilegi

Per completare l'obiettivo del test e dimostrare il livello di compromissione del sistema, è stata richiesta la creazione di una directory specifica. Poiché l'exploit fornisce accesso con privilegi di **root**, ho potuto agire direttamente sulla directory root(`/`).

Ho eseguito il comando `mkdir /test_metasploit` per creare la cartella richiesta. Successivamente, ho verificato la creazione della cartella e i permessi associati tramite il comando `ls -la` e il risultato ha confermato la presenza della directory `test_metasploit` e la sua appartenenza all'utente root, dimostrando il pieno controllo del sistema.



Conclusioni

L'attacco ha dimostrato come un software non aggiornato (in questo caso una vecchia versione di vsftpd) possa compromettere l'intera sicurezza di un server. Per mitigare questo rischio le soluzioni sono:

1. Aggiornare il servizio FTP all'ultima versione stabile disponibile che non presenti la backdoor.
2. Implementare firewall per limitare l'accesso alla porta 21 solo agli indirizzi IP autorizzati.
3. Monitorare i log di sistema per rilevare tentativi di connessione anomali.