Hacking con Metasploit

Data: 19 Gennaio 2026

Autore: Francesco Sardi

Oggetto: Hacking con Metasploit

1. Obiettivo

L'attività ha lo scopo di condurre un attacco informatico controllato verso il servizio **vsftpd** in esecuzione sulla macchina target Metasploitable.

Gli obiettivi specifici sono:

1. Ottenere l'accesso remoto alla macchina sfruttando una vulnerabilità nota.
2. Scalare i privilegi fino a ottenere i diritti di root.
3. Eseguire azioni di post-exploitation creando una directory denominata "*test_metasploit"* nella root.

2. Executive Summary

In questo report viene documentata una sessione di hacking etico mirata al servizio FTP della macchina virtuale Metasploitable. Attraverso l'uso della distribuzione Kali Linux e del framework Metasploit, è stato possibile identificare una vulnerabilità critica ("Backdoor Command Execution") nel demone "*vsftpd v2.3.4"*. L'attacco ha avuto successo, permettendo l'apertura di una command shell con privilegi amministrativi e la conseguente modifica del file system del target.

3. Configurazione dell'Ambiente

Prima di avviare l'attacco, è stata configurata la rete isolata per permettere la comunicazione tra la macchina attaccante (Kali) e la macchina vittima (Metasploitable).

Modifica della configurazione di rete: È stato modificato il file */etc/network/interfaces* sulla macchina Metasploitable per assegnare un IP statico.

Metasploitable :

- Address 192.168.1.149
- Netmask 255.255.255.0
- Gateway 192.168.1.1

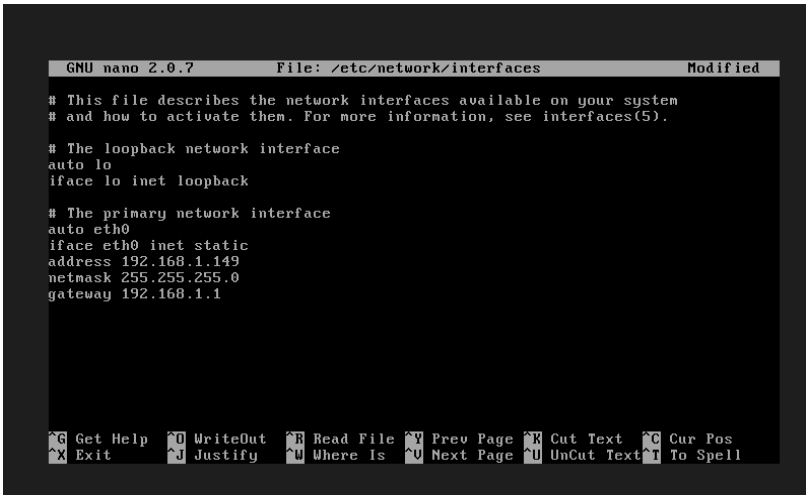
Kali :

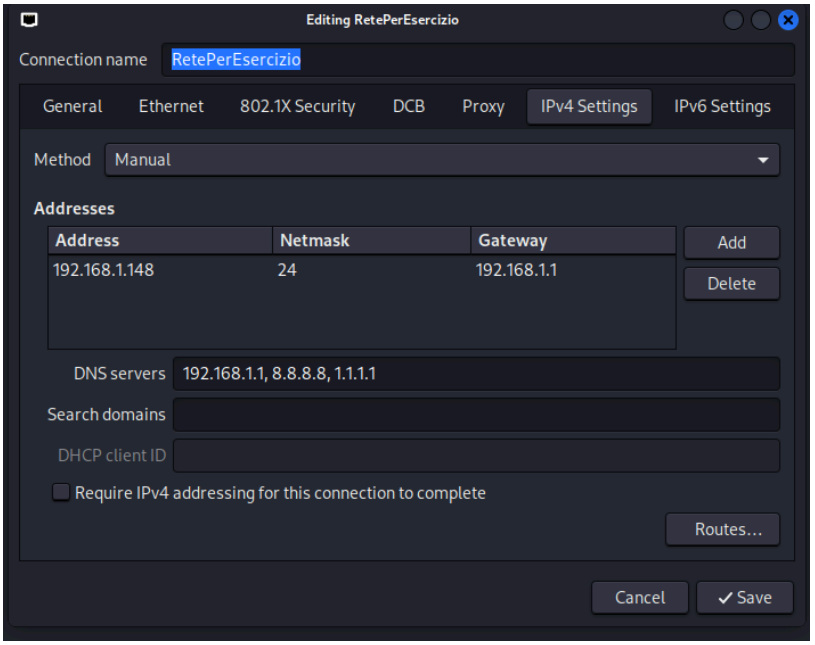
- Address 192.168.1.148
- Netmask 255.255.255.0

- Gateway 192.168.1.1

Comando :

“sudo nano /etc/network/interfaces “

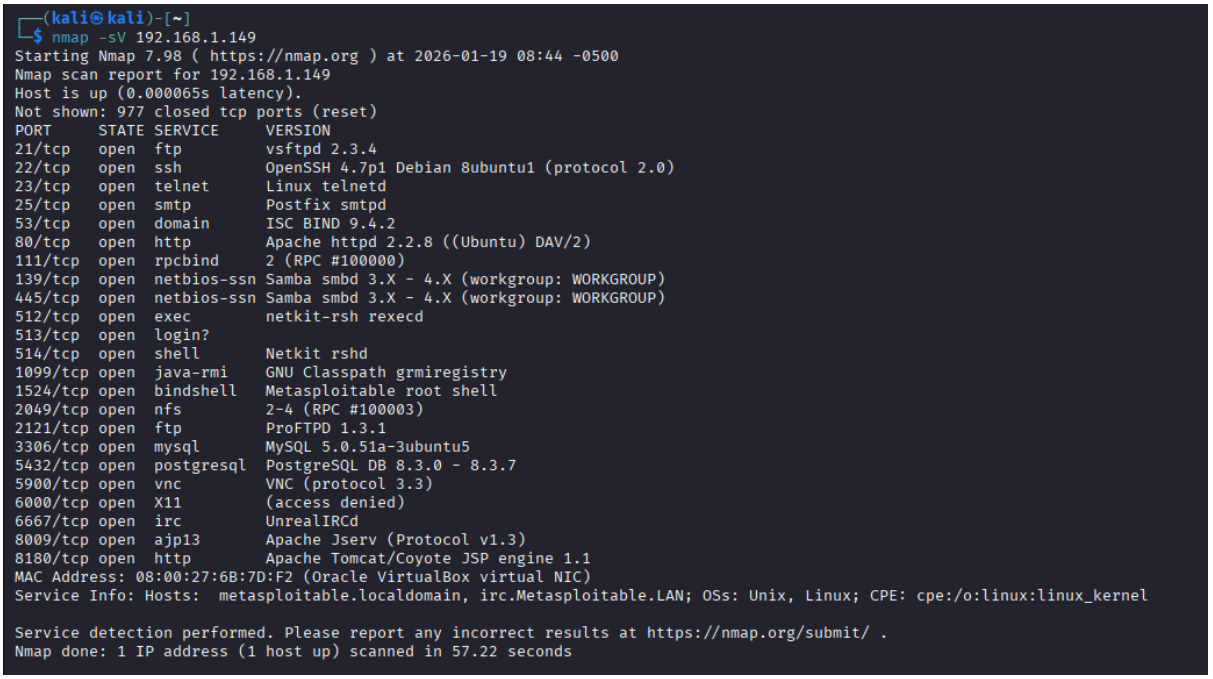




4. Scansione superficie d’attacco

Per analizzare la superficie d'attacco, è stato utilizzato il tool **Nmap** verso l'indirizzo IP del target *(192.168.1.149)*. L'obiettivo è identificare le porte aperte e le versioni dei servizi in ascolto.

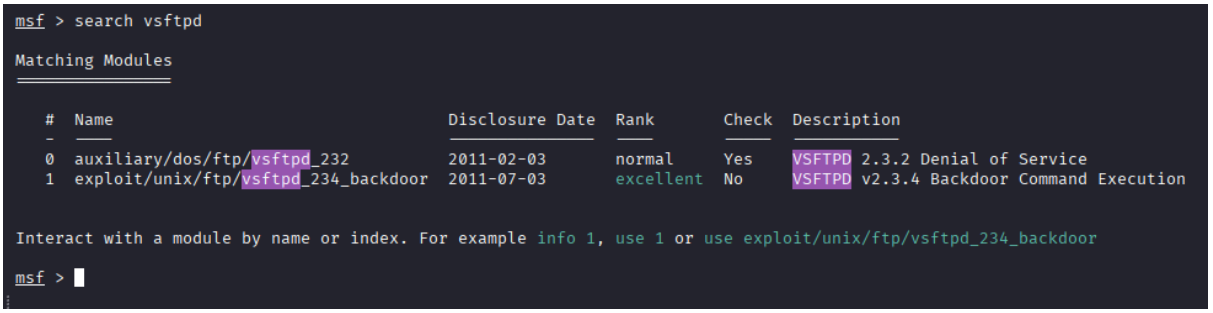
Risultati della scansione: Dall'output di Nmap è emerso che sulla **porta 21** è attivo il servizio **vsftpd versione 2.3.4**.



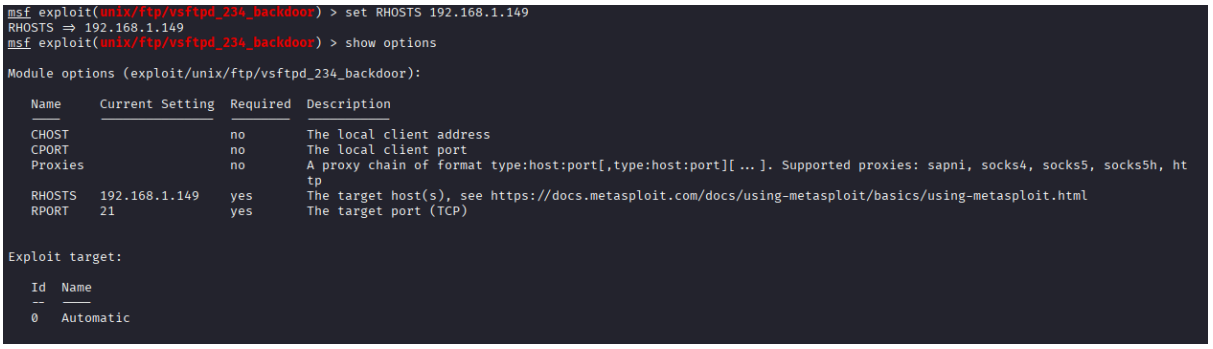
5. Fase 2: Vulnerability Assessment & Exploitation

Identificata la versione del servizio, è stata effettuata una ricerca all'interno del database di **Metasploit Framework** per verificare l'esistenza di exploit noti.

1. **Ricerca dell'Exploit:** La ricerca ha confermato che la versione 2.3.4 di vsftpd è affetta da una grave vulnerabilità di tipo *Backdoor Command Execution*.



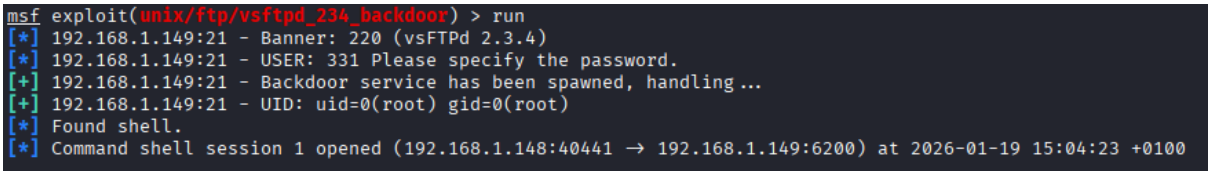
Configurazione dell'Exploit: È stato selezionato l'exploit appropriato e configurate le opzioni obbligatorie, specificando l'indirizzo IP del target nel parametro *RHOSTS*.



Esecuzione dell'Attacco: Una volta verificato il payload e i parametri, è stato lanciato l'attacco.

Comando d’attacco:

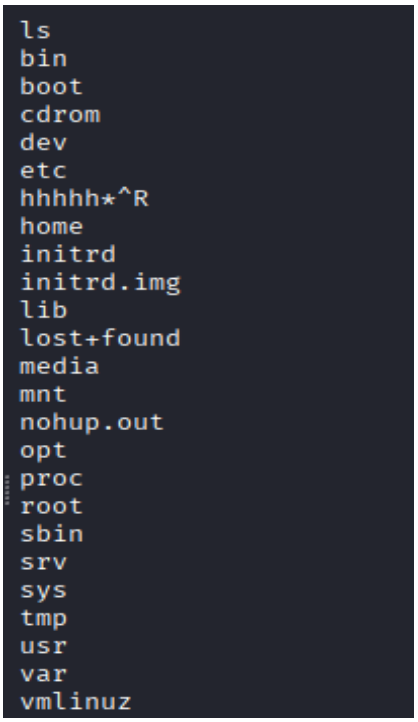
“run”



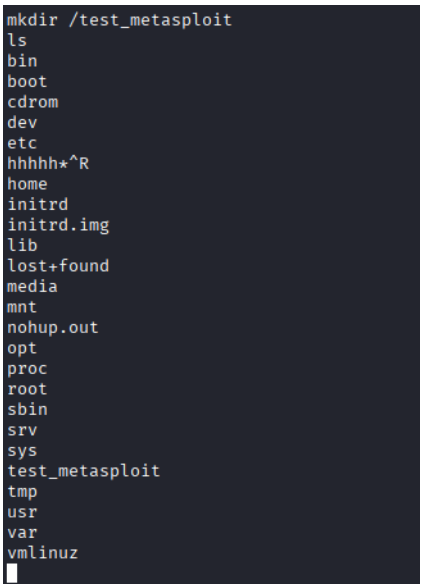
6. Fase 3: Post-Exploitation

L'exploit ha avuto successo aprendo una shell di comando sulla macchina target. A questo punto sono state eseguite le operazioni richieste per dimostrare il controllo del sistema.

1. **Verifica e Navigazione:** Utilizzo della shell per visualizzare il contenuto attuale e navigare nel filesystem.



Creazione della Cartella: È stata creata la directory test_metasploit *(“mkdir /test_metaspoit”)* nella root del sistema e successivamente verificata la sua presenza tramite il comando di ls.



7. Conclusioni

L'attività ha dimostrato come una configurazione obsoleta o software non aggiornato (in questo caso *vsftpd 2.3.4*) possa esporre un intero sistema a compromissione totale. L'utilizzo di **Metasploit Framework (msf)** è risultato efficace per automatizzare il processo di sfruttamento della vulnerabilità, utilizzando un *payload* specifico per aprire un canale di comunicazione non autorizzato. Questo evidenzia l'importanza cruciale del *Patch Management* e del monitoraggio costante dei servizi esposti in rete.