REPORT: Hacking con metasploit

Introduzione

L'obiettivo di questa attività di laboratorio è stato condurre un vulnerability assessment e un successivo penetration test contro la macchina target "Metasploitable". L'attività si è concentrata sull'analisi del servizio FTP, identificato come punto critico.

Sfruttando una vulnerabilità nota nel demone ***vsftpd v2.3.4***, è stato possibile eseguire codice remoto (RCE) non autenticato. L'attacco ha permesso di ottenere una shell di comando con privilegi di livello **root**, garantendo il controllo completo del sistema target. Come prova dell'avvenuta compromissione (Proof of Concept), è stata creata una directory specifica nel filesystem della vittima.

Configurazione

Per l'esecuzione del test è stato predisposto un laboratorio virtuale isolato:

- **Macchina Attaccante:** Kali Linux
- **Macchina Target:** Metasploitable 2
- **IP Target:** 192.168.1.149
- **Strumenti utilizzati:** Metasploit Framework (msfconsole), Nmap.

Fasi dell'Attacco

Fase di Ricognizione

È stata effettuata una scansione preliminare per identificare i servizi attivi sul target **192.168.1.149**. La scansione ha evidenziato la porta TCP 21 aperta, con in esecuzione il servizio **vsftpd 2.3.4.**

Analisi della Vulnerabilità

La versione 2.3.4 di **vsftpd** è nota per contenere una "backdoor" malevola introdotta nel codice sorgente dagli sviluppatori (o da un attaccante) nel 2011. Se un utente tenta il login con un username che contiene una "faccina" :), il servizio apre un ascolto sulla porta 6200 garantendo accesso shell.

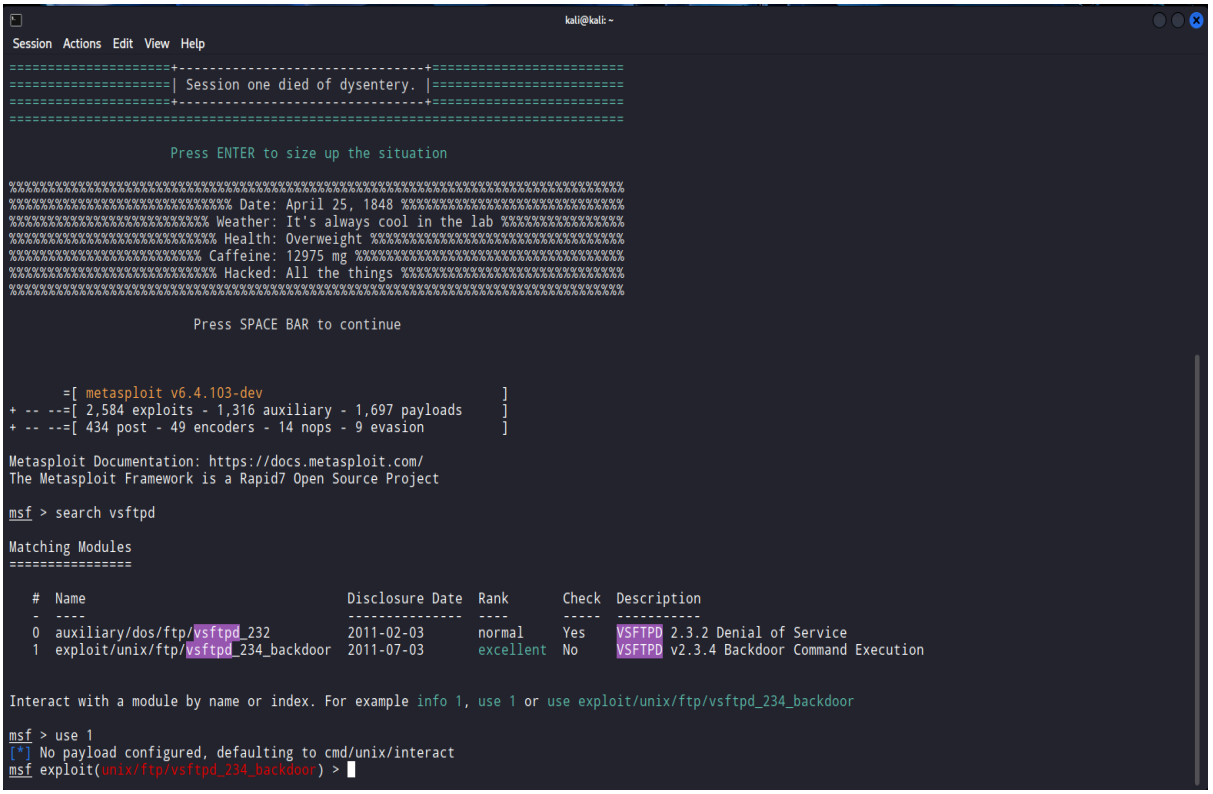
Exploitation con Metasploit

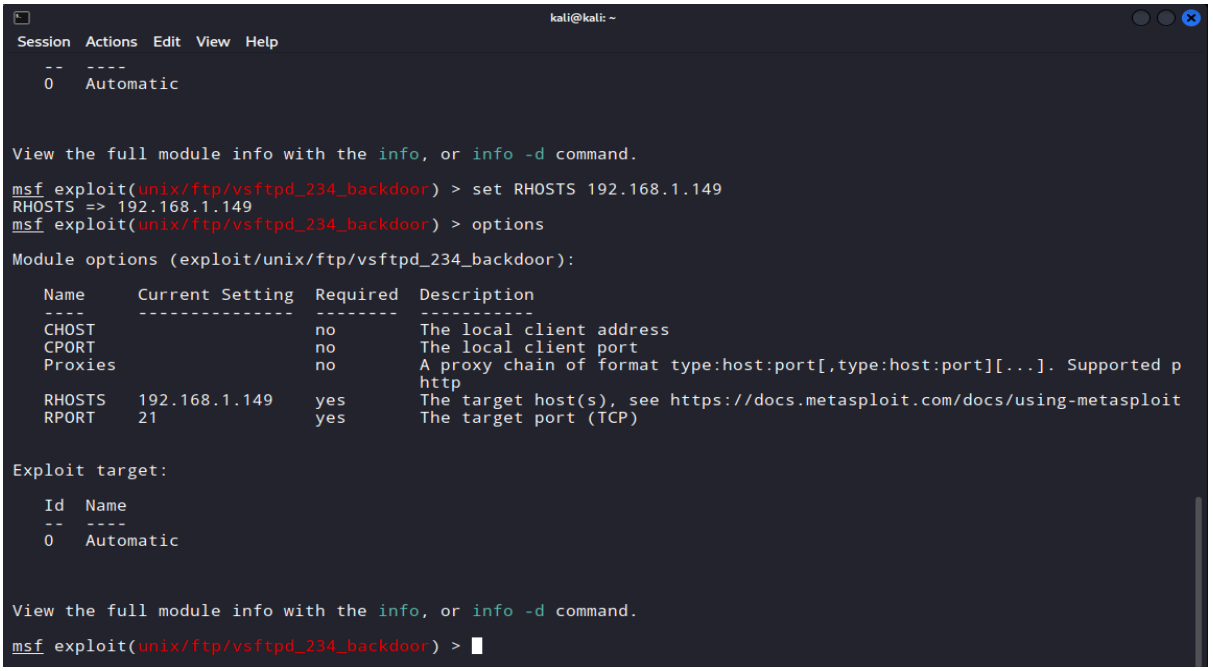
Per automatizzare l'attacco è stato utilizzato il framework Metasploit.

Comandi eseguiti:

1. Avvio della console: **msfconsole**
2. Ricerca vsftpd **: search vsftpd**
3. Selezione del modulo: **use 1**
4. Configurazione del target: **set RHOSTS 192.168.1.149**

Evidenza Configurazione:





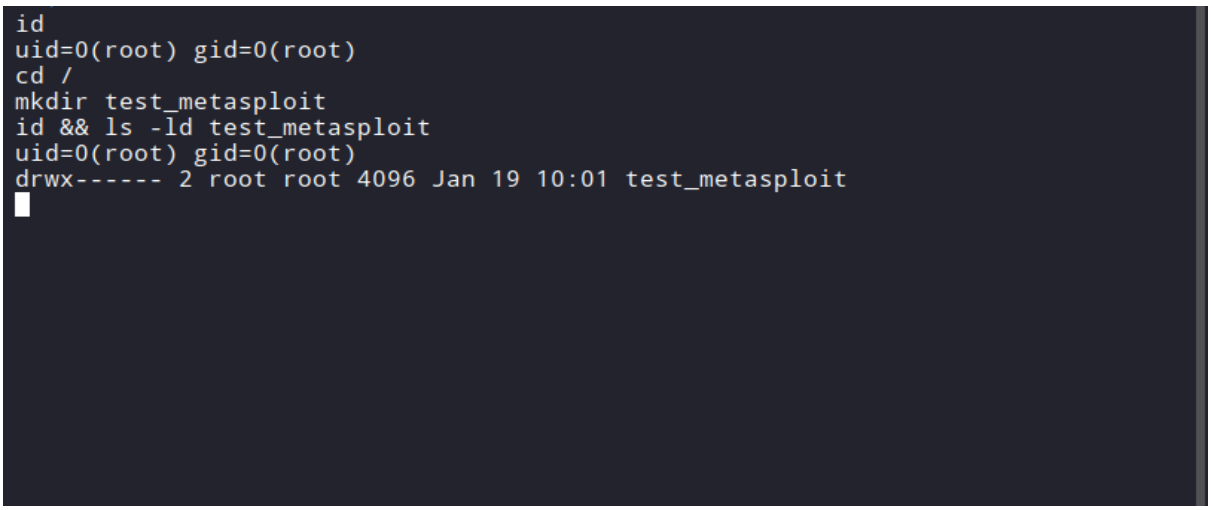
Esecuzione e Post-Exploitation

Lanciando il comando **exploit**, il modulo ha attivato la backdoor. È stata stabilita una connessione con privilegi elevati (Root).

Per soddisfare i requisiti dell'esercizio, sono state eseguite le seguenti azioni sulla macchina compromessa:

1. Navigazione alla root directory: **cd /**
2. Creazione della directory richiesta: **mkdir test_metasploit**
3. Verifica dei permessi e della creazione.

Evidenza del Compromesso (PoC): L'immagine seguente mostra l'accesso shell ottenuto, la verifica dell'identità (**uid=0(root)**) e la presenza della cartella creata.



Conclusioni e Misure Correttive (Remediation)

L'esito del test è stato positivo e ha confermato la criticità della vulnerabilità riscontrata nel sistema.

Raccomandazioni per la Sicurezza: Per garantire la messa in sicurezza del sistema, si raccomanda di attuare le seguenti azioni:

1. **Aggiornamento o Sostituzione del Servizio:** Disinstallare la versione 2.3.4 di **vsftpd** e procedere con l'installazione dell'ultima versione stabile e sicura, prelevandola dai repository ufficiali.
2. **Filtro di Rete (Network Filtering):** Implementare una restrizione all'accesso sulla porta 21 tramite configurazione del firewall, consentendo la connessione esclusivamente agli indirizzi IP preventivamente autorizzati.