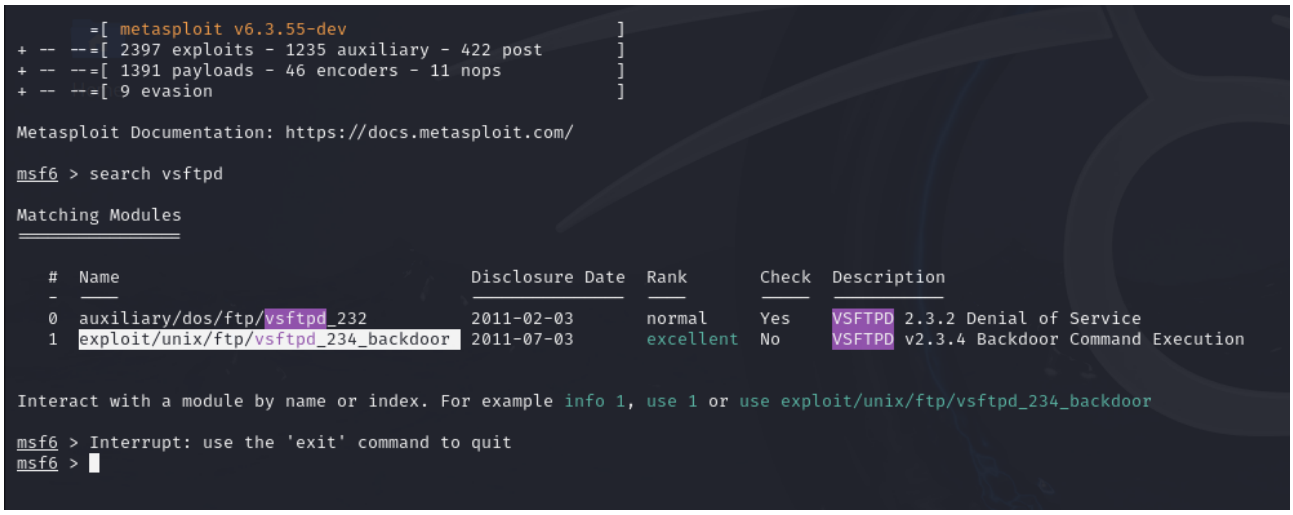
ESERCIZIO MSFCONSOLE



Avvio del programma **msfconsole** per procedere alla sessione di hacking.

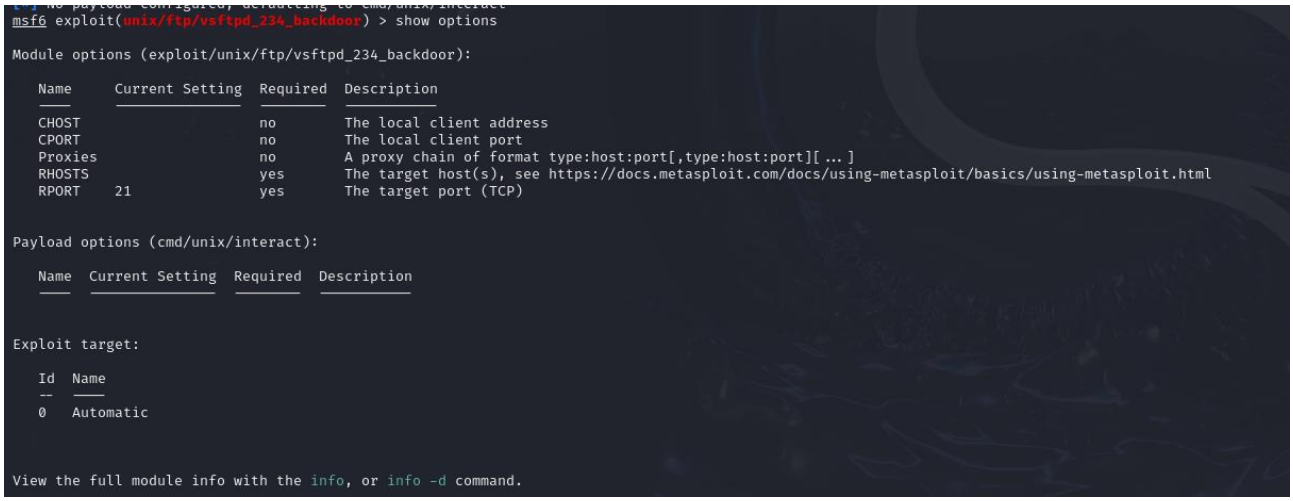
La sessione di hacking con il servizio di **vsftpd,** come primo commando la ricerca: **search vsftpd**

Introduzione

L'exploit vsftpd_234_backdoor è progettato per sfruttare una vulnerabilità nel server FTP vsftpd versione 2.3.4 che consente l'esecuzione remota del codice. Questa vulnerabilità è stata scoperta nel 2011 e può essere sfruttata da un attaccante per ottenere accesso non autorizzato al sistema target.

Attività eseguita

Il comando **use exploit/unix/ftp/vsftpd_234_backdoor** viene utilizzato all'interno del framework di penetration testing Metasploit (MSF6). Questo comando imposta Metasploit per utilizzare l'exploit vsftpd_234_backdoor come parte di un'attività di test di penetrazione.



Introduzione

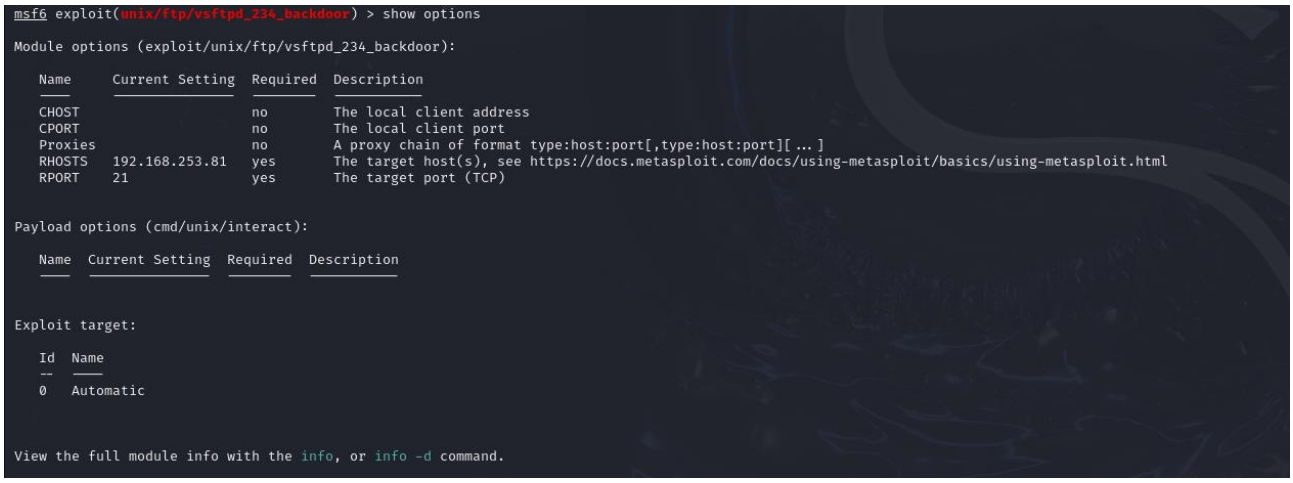
Ho esaminato le opzioni disponibili per l'exploit vsftpd_234_backdoor utilizzando il framework Metasploit (MSF6). Questo exploit mira a sfruttare una vulnerabilità nel server FTP vsftpd versione 2.3.4 al fine di ottenere l'accesso non autorizzato al sistema di destinazione.

Opzioni del Modulo

Il modulo dell'exploit fornisce diverse opzioni che possono essere configurate per personalizzare e adattare l'attacco:

- **RHOSTS**: Indica l'indirizzo del sistema di destinazione che si intende attaccare. È una opzione obbligatoria, che deve essere specificata.
- **RPORT**: Specifica la porta di destinazione del servizio FTP sul sistema bersaglio. È impostato di default su porta 21 (TCP).
- **CHOST**: Rappresenta l'indirizzo IP locale del client. Non è necessario per l'esecuzione dell'exploit.
- **CPORT**: Indica la porta locale del client. Anche questa opzione non è essenziale.
- **Proxies**: Consente di configurare una catena di proxy per l'attacco, ma non è richiesto per l'utilizzo di base dell'exploit.

E’ stato impostato l'indirizzo IP del sistema di destinazione (RHOST) a 192.168.253.81 nell'exploit vsftpd_234_backdoor all'interno di Metasploit (MSF6).



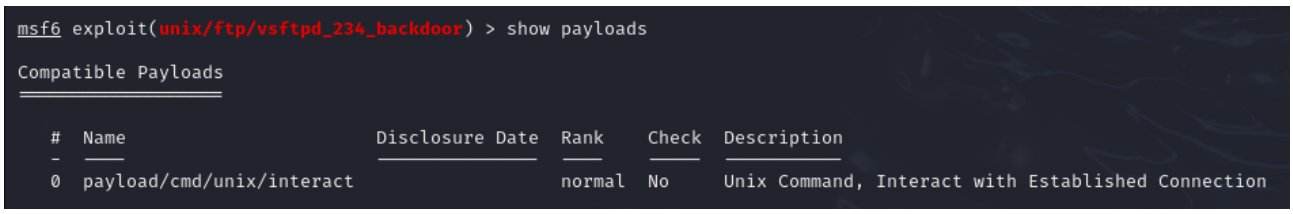
Nell'analisi delle opzioni dell'exploit vsftpd_234_backdoor all'interno di Metasploit, ho stato osservato un cambiamento:

- **RHOSTS**: L'indirizzo IP del sistema di destinazione è stato modificato da un valore vuoto a 192.168.253.81. Questo indica che l'exploit è stato configurato per mirare a un nuovo sistema di destinazione con l'indirizzo IP specificato.

Le altre opzioni rimangono invariate:

- **CHOST**, **CPORT**, e **Proxies**: Queste opzioni non sono state modificate e rimangono come impostazioni predefinite o vuote.
- **RPORT**: La porta di destinazione del servizio FTP rimane impostata su 21 (TCP), senza variazioni.

In breve, il cambiamento principale riguarda l'aggiornamento dell'indirizzo IP del sistema di destinazione, mentre le altre opzioni rimangono costanti.

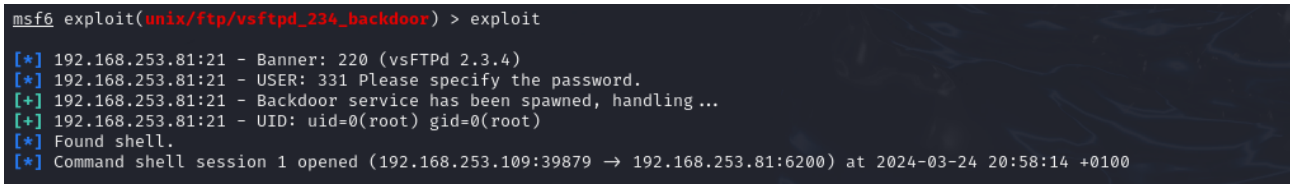


Nell'ambito dell'exploit vsftpd_234_backdoor all'interno di Metasploit (MSF6), sono state esaminate le payload compatibili:

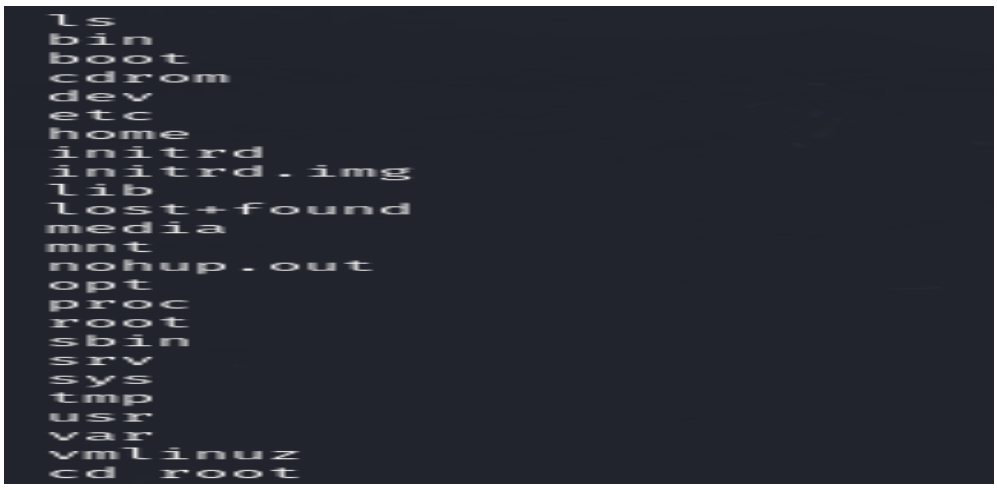
- **Payload Disponibile**: La sola payload compatibile è **payload/cmd/unix/interact**.

- **Descrizione**: Questa payload permette l'esecuzione di comandi Unix e consente all'attaccante di interagire direttamente con la connessione stabilita una volta che l'exploit ha avuto successo.
- **Classificazione**: La payload è classificata come "normale" in base al suo potenziale impatto.
- **Verifica**: Non è disponibile un metodo automatico per verificare se la payload può essere eseguita con successo sul sistema di destinazione senza interazione umana.

In conclusione, l'exploit vsftpd_234_backdoor supporta una sola payload, che offre all'attaccante la capacità di eseguire comandi Unix e interagire con la connessione compromessa.



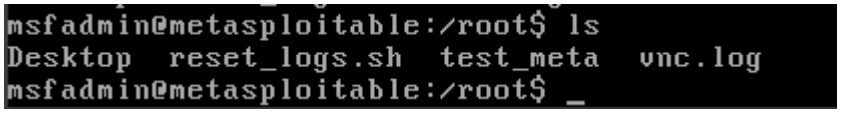
L'exploit è stato eseguito con successo contro l'indirizzo IP 192.168.253.81 sulla porta 21, dove è stato individuato un server vsFTPd 2.3.4. Dopo aver inviato il comando USER, è stato rilevato che il servizio backdoor è stato attivato e gestito correttamente. L'attacco ha avuto successo nel fornire una shell di comando con privilegi di root, consentendo all'attaccante di assumere il controllo completo del sistema bersaglio.



La lista delle cartelle di Metasploitable.

Spostamento nella directory root per la creazione di una nuova cartella.

Creazione di una nuova cartella **test_meta**, nella directory di root



È verificato che la cartella **test_meta** è stata creata, ed appare anche in metasploitable.