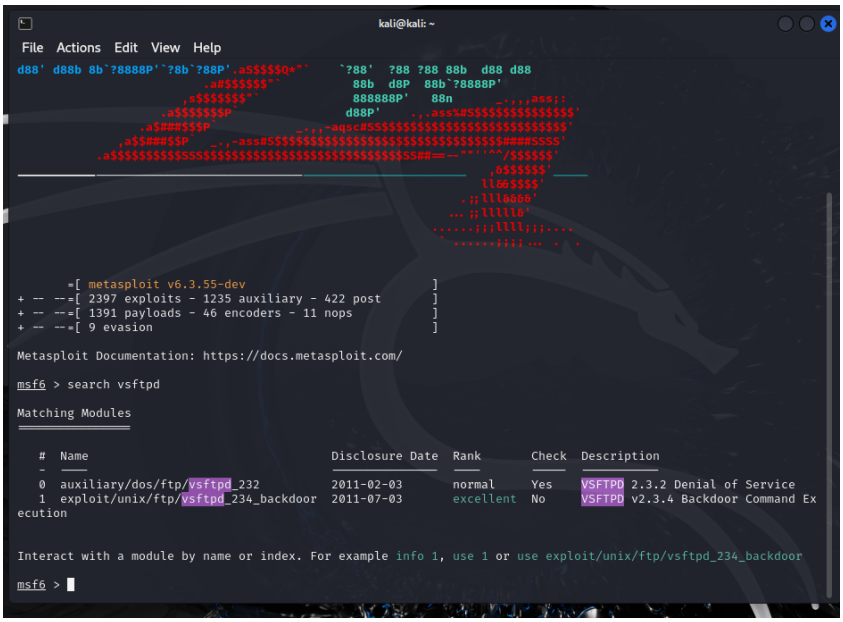
Esercizio W15D4

Traccia: Partendo dall'esercizio guidato visto nella lezione teorica, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica). L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

1. **Configurazione dell'ambiente**:
    - La macchina Metasploitable è stata configurata con l'indirizzo IP **192.168.1.149**.
    - La macchina Kali Linux è stata configurata con l'indirizzo IP **192.168.1.120**.
2. **Avvio di Metasploit**:
    - Metasploit è stato avviato nella macchina Kali Linux eseguendo il comando **msfconsole**.

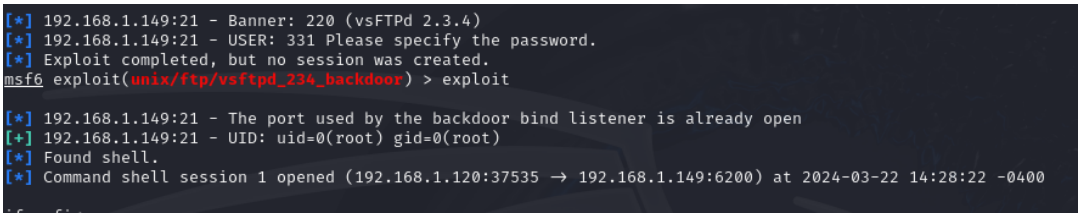


3. **Identificazione dell'exploit**:
    - Utilizzando il comando **search vsftpd**, abbiamo individuato l'exploit **exploit/unix/ftp/vsftpd_234_backdoor**.
4. **Configurazione dell'exploit**:
    - Abbiamo selezionato l'exploit **exploit/unix/ftp/vsftpd_234_backdoor**.
    - Abbiamo impostato l'indirizzo IP della nostra macchina Kali Linux come LHOST utilizzando il comando **set LHOST 192.168.1.149**
5. **Avvio dell'exploit**:

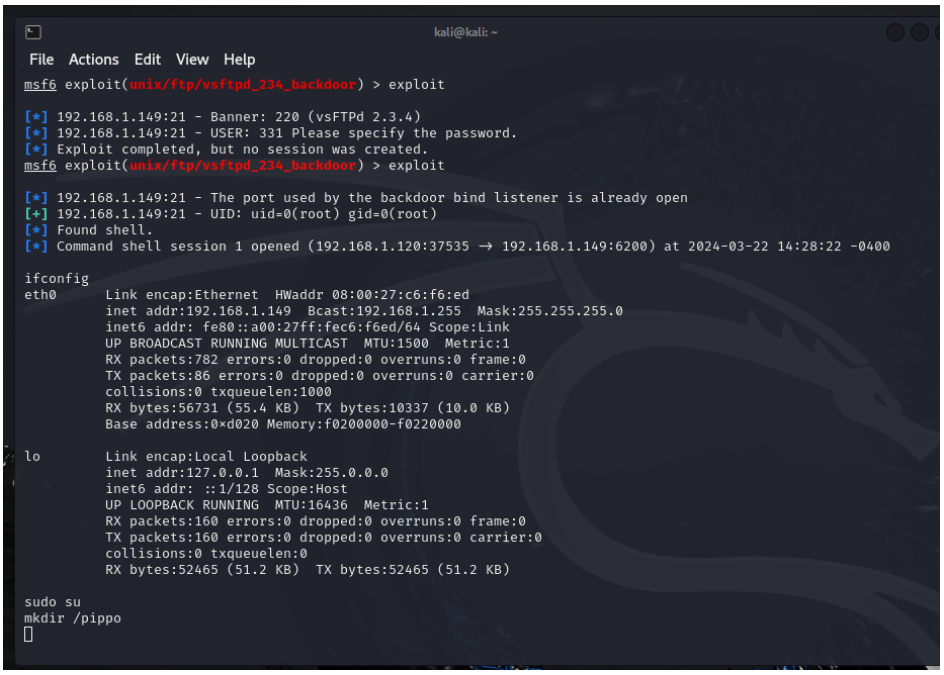
- Dopo aver impostato correttamente l'indirizzo IP della nostra macchina Kali Linux e quello della macchina Metasploitable, abbiamo eseguito l'exploit utilizzando il comando **exploit**.

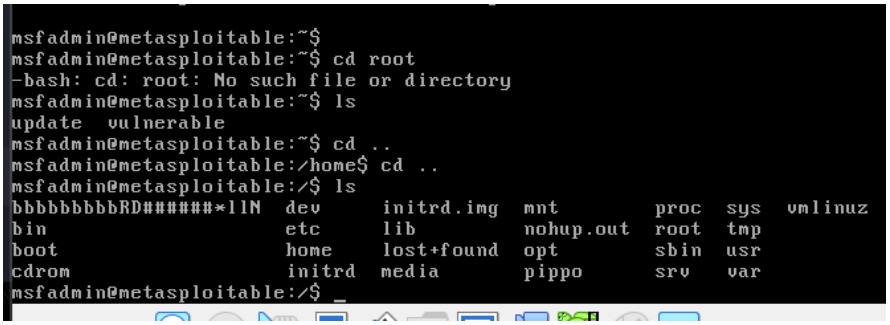
6. **Risultato dell'exploit**:

   - Abbiamo avuto successo nell'ottenere il controllo della shell di Metasploitable attraverso l'exploit su VSFTPD.



   - Abbiamo eseguito con successo il comando per creare la cartella "pippo" nella directory di root (/) sulla macchina Metasploitable.





7. **Prossimi passi**:

   - Possiamo esplorare ulteriori opportunità di attacco sulla macchina Metasploitable