Hacking con Metasploit

Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable.

Traccia dell'Esercizio

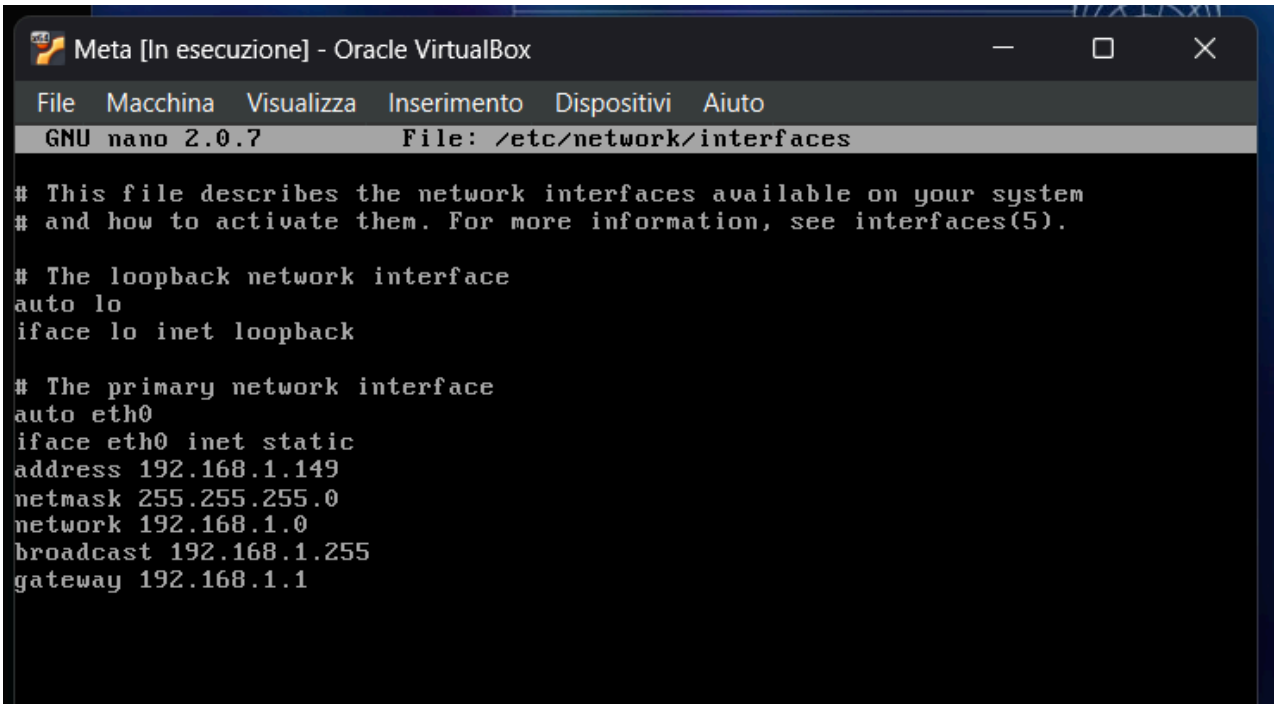
Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

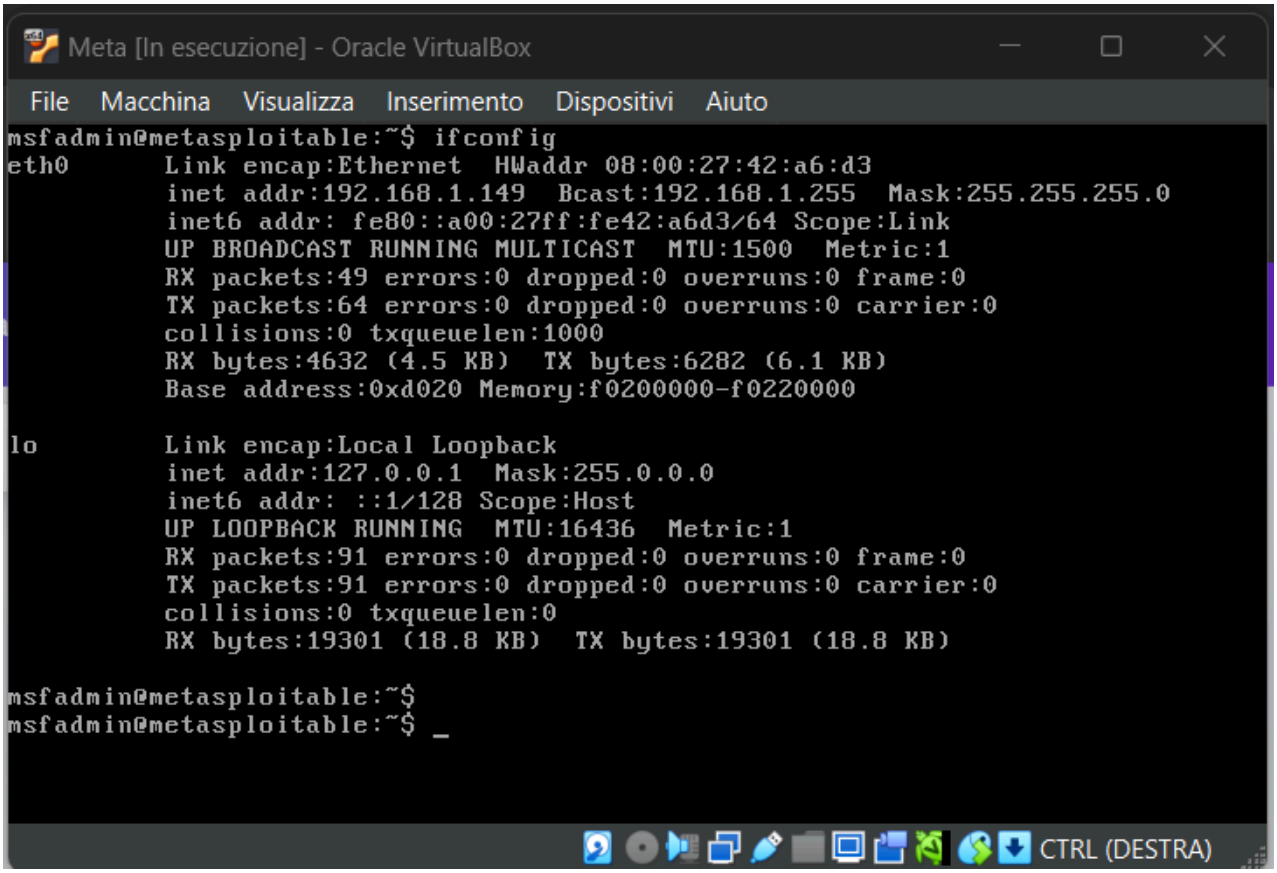
Dettagli dell'Attività

Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable.
Configurate l'indirizzo come segue: 192.168.1.149/24

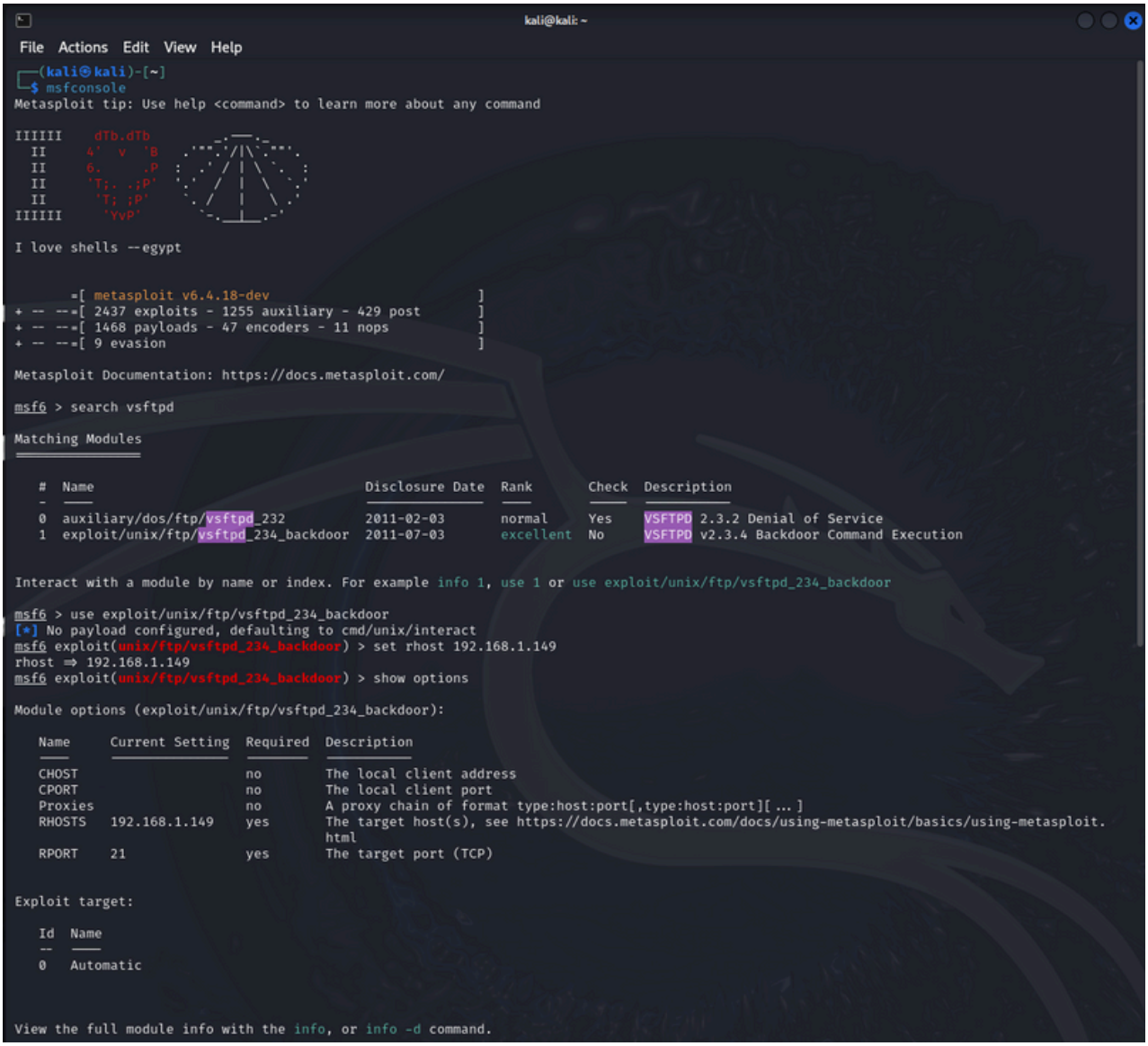
- Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
- Creazione di una Cartella Una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir. mkdir /test_metasploit

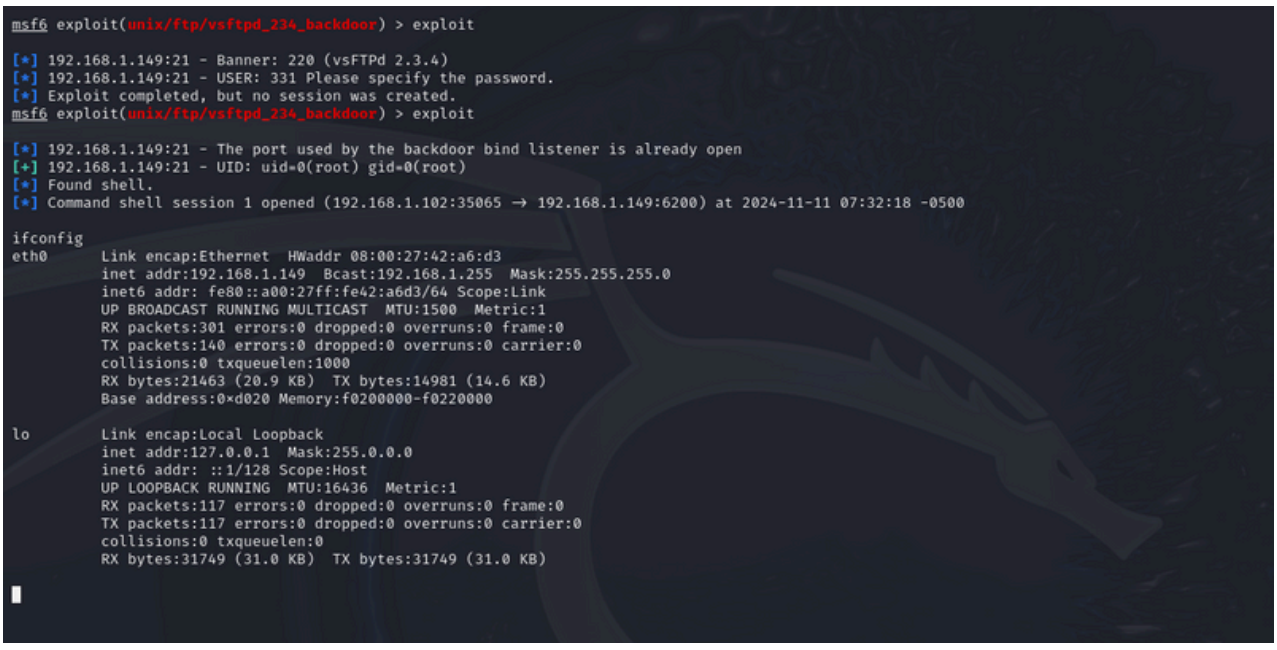
Modifica ip meta



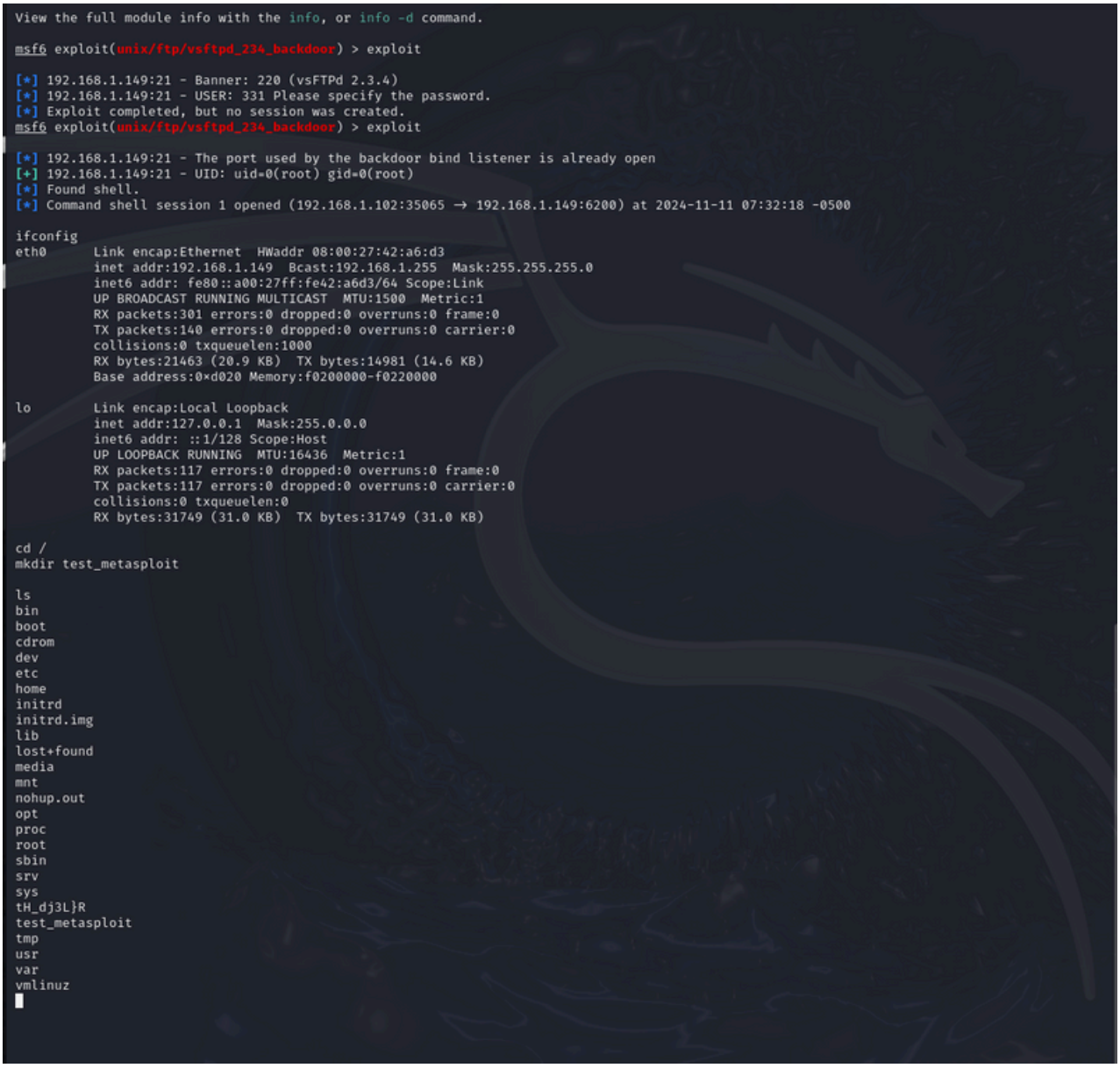


msfconsole + rhosts





Creazione cartella



Relazione

In questo esercizio ho sfruttato una debolezza nel servizio "vsftpd" della macchina Meta utilizzando Metasploit. Ho iniziato utilizzando Metasploit, cercando il servizio specifico "vsftpd". Ho selezionato “exploit/unix/ftp/vsftpd_234_backdoor”, impostato l’ip che volevo attaccare con “set rshots 192.168.1.149”, ho verificato di averlo inserito correttamente con “show options”, e poi ho effettuato l’exploit. Al primo tentativo non è andato a buon fine e l’ho eseguito una seconda volta. Una volta collegato alla macchina e preso il controllo ho creato una cartello chiamata “test_metasploit”. Con “cd /” sono andato nella directory root, con il comando “mkdir nome_cartella” ho creato la cartella e con “ls” sono andato a elencare tutti i file presenti. Come si può vedere la cartella è stato correttamente creata. Con questo esercizio si è dimostrato come si può sfruttare una vulnerabilità e prendere il controllo di un sistema compromesso, permettendo cosi di eseguire delle azioni al proprio interno. Come nel nostro caso la creazione di una cartella.