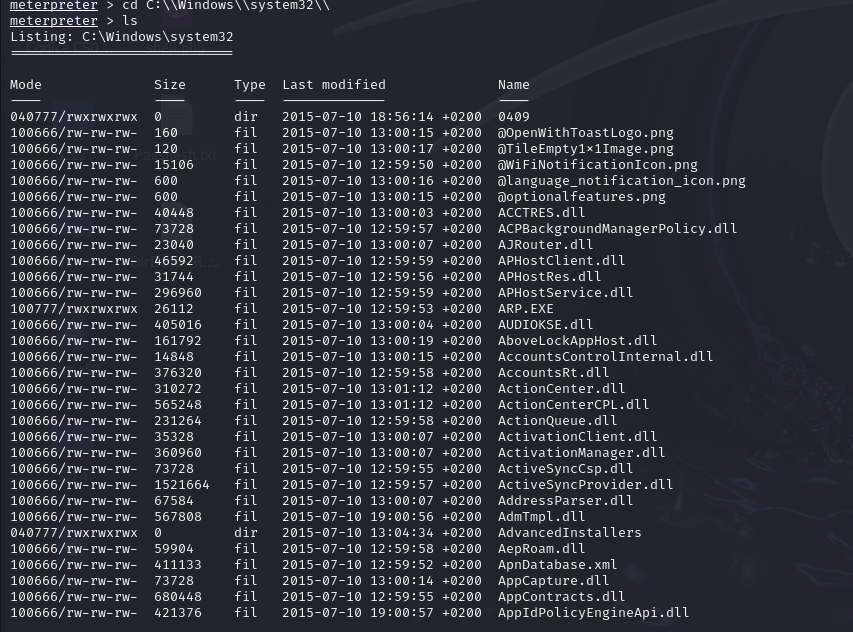
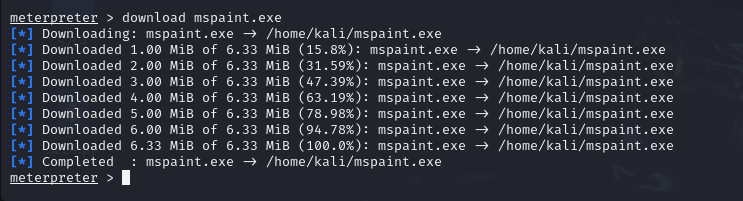
EXTRA S7L2

Avvio l’exploit per windows 10



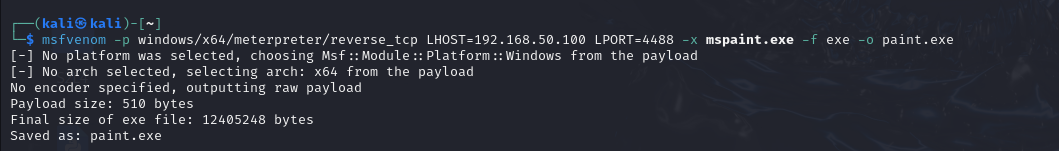


Mi muovo dentro le cartelle di Windows 10 e trovo l’app PAINT

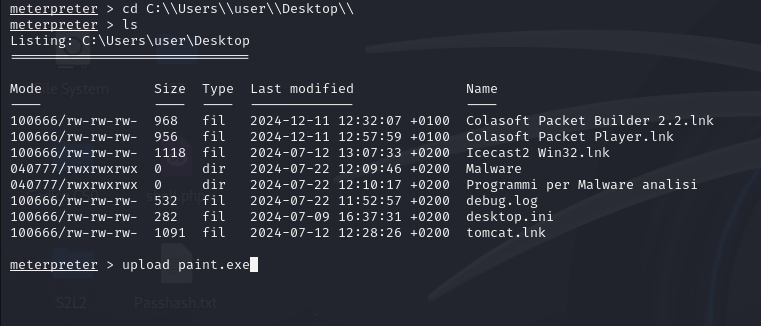


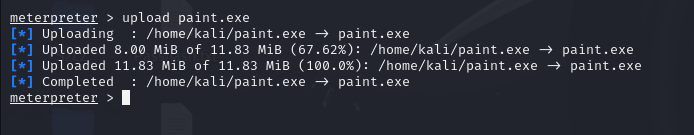
Scarico l’app dal Windows alla Kali

Con MSFVENOM Inserisco il payload di un reverseTCP all’interno dell’app PAINT con il comando:



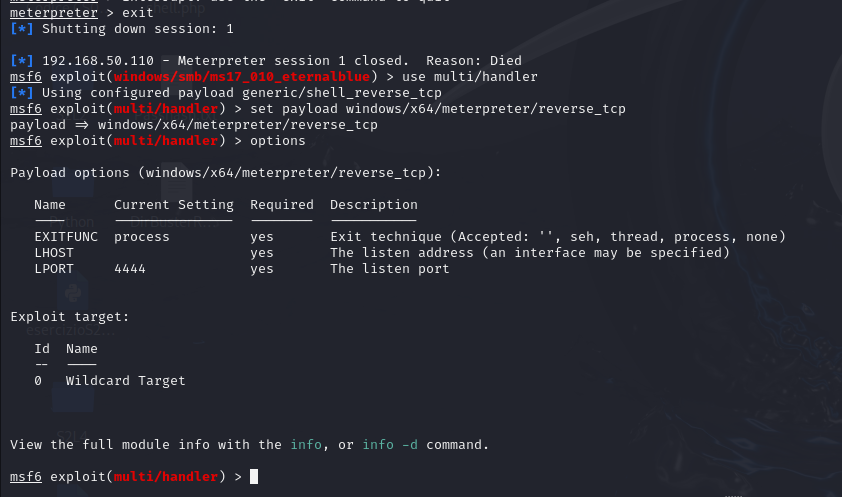
Faccio un UPLOAD di PAINT(modificata) sul desktop di Windows10

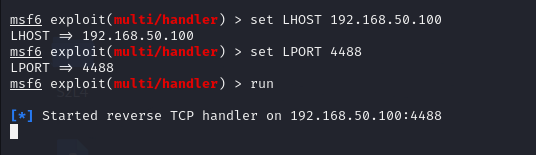






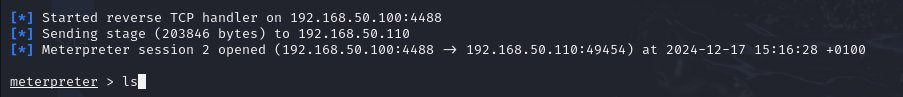
Configuro la macchina KALI con Metasploitable

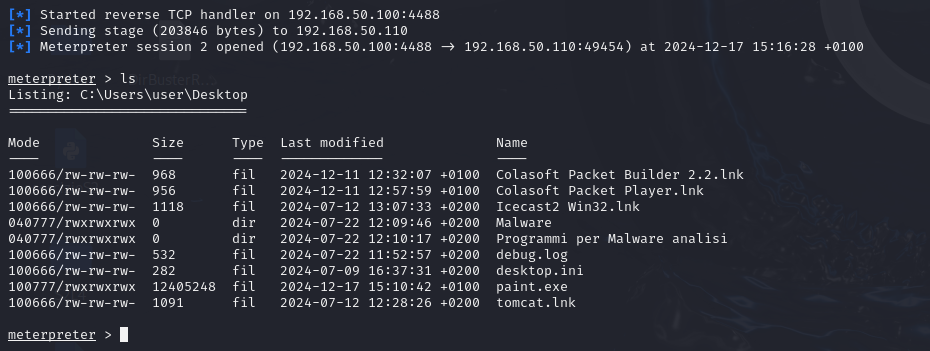




Avvio l’exploit sulla KALI e avvio l’app PAINT su Windows10

L’app PAINT apre una backdoor su Windows10 che sfrutto con la Metasploitable





CHIUDO L’APP PAINT che continua a funzionare in background

