# Hacking Windows

**Introduzione**

In questa esercitazione che prevedeva l'ottenimento di una sessione di Meterpreter su una macchina target Windows 10 utilizzando Metasploit. Di seguito, descrivo dettagliatamente il procedimento seguito e alcune considerazioni sulla vulnerabilità sfruttata.

**Preparazione e verifica della comunicazione**

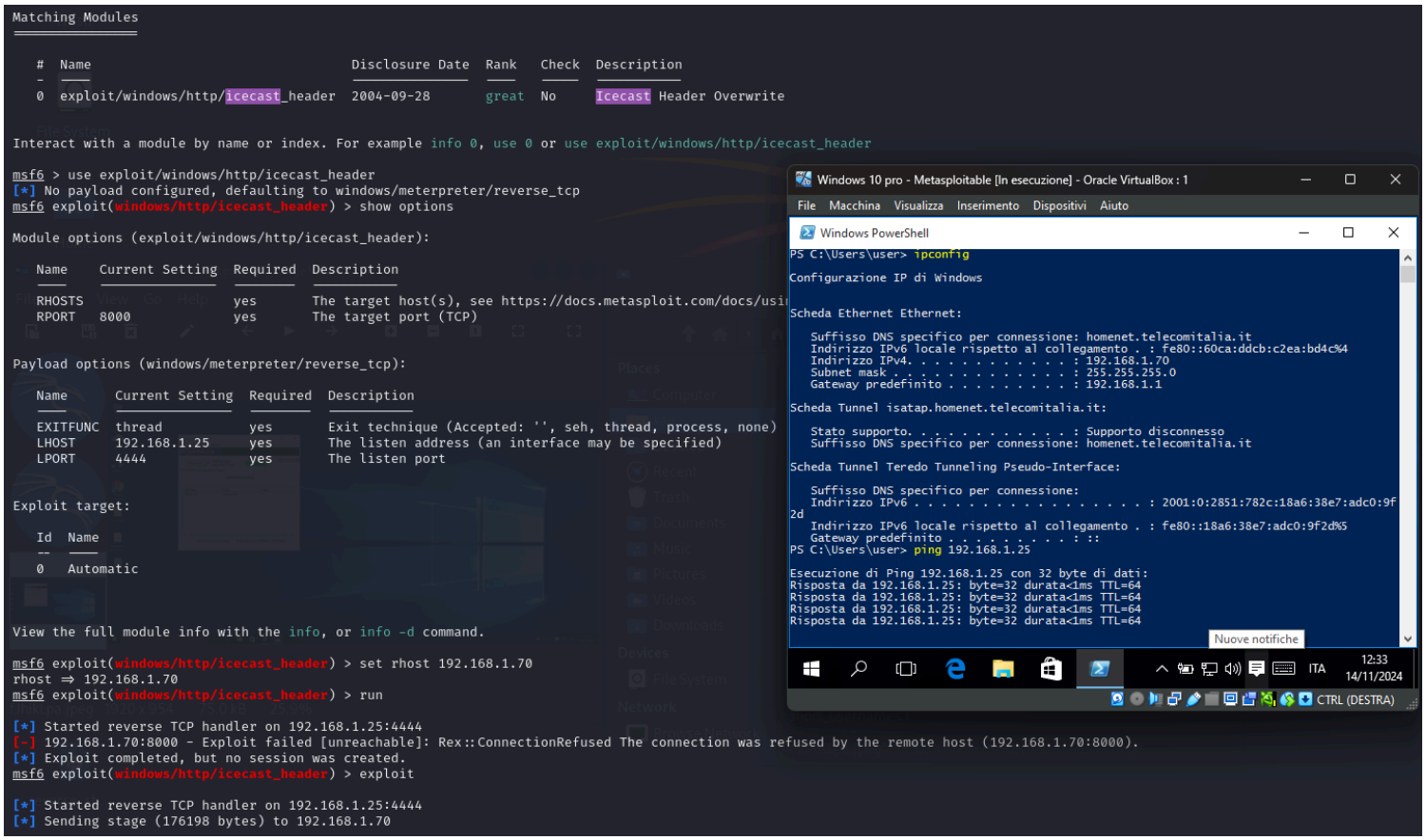
Prima di tutto, ho verificato che le due macchine coinvolte (attaccante e vittima) potessero comunicare correttamente tra loro. La macchina attaccante, Kali Linux, aveva l'indirizzo IP 192.168.1.25, mentre la macchina vittima, un Windows 10 Pro, aveva l'indirizzo IP 192.168.1.70. Ho usato il comando ping per controllare la connessione, e la risposta positiva mi ha confermato che le macchine erano in grado di comunicare.

**Avvio di Metasploit e ricerca dell'exploit**

Ho avviato Metasploit con il comando msfconsole e successivamente ho cercato un exploit adatto per una vulnerabilità conosciuta. In questo caso, ho scelto di sfruttare la vulnerabilità presente in Icecast, un software di streaming audio, tramite l'exploit exploit/windows/http/icecast_header. Questa vulnerabilità è nota per consentire l'esecuzione remota di codice arbitrario a causa di una cattiva gestione degli header HTTP, rendendo quindi possibile l'accesso non autorizzato al sistema della vittima.

**Configurazione dell'exploit e attacco**

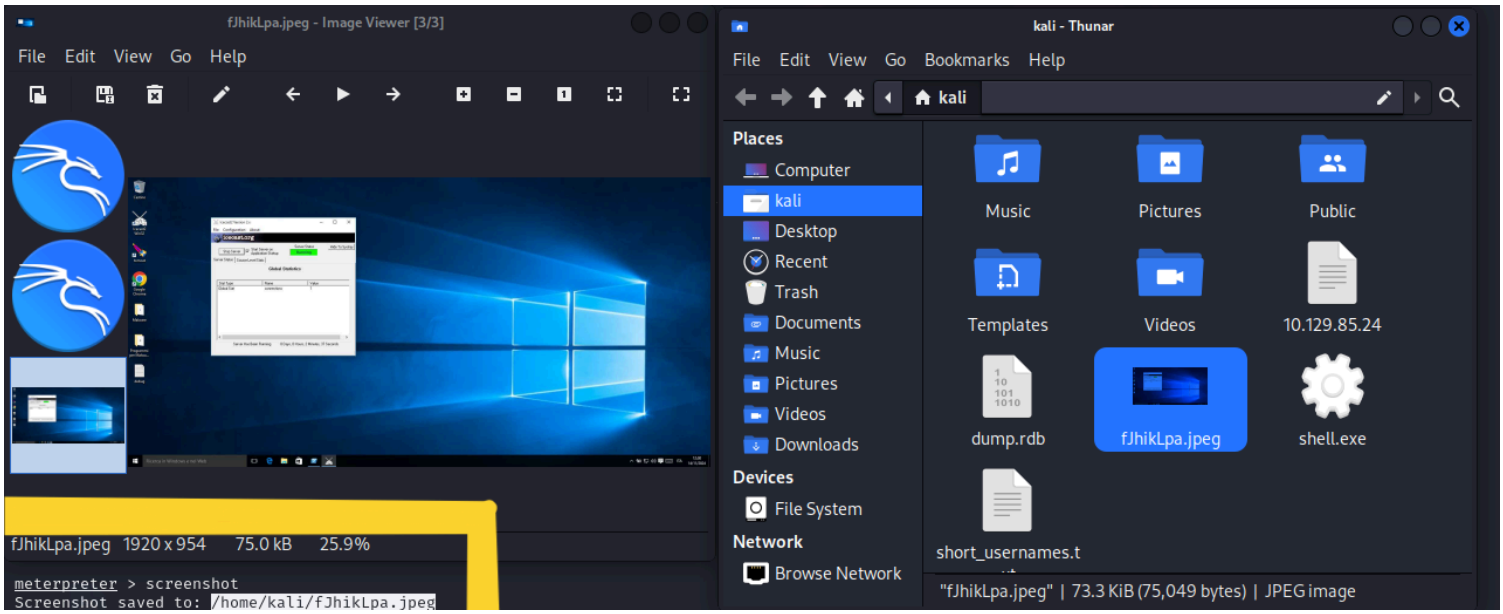
Una volta selezionato l'exploit, ho impostato l'indirizzo IP della vittima come RHOST, utilizzando set RHOST 192.168.1.70. Dopo aver configurato i parametri necessari, ho lanciato l'attacco con il comando exploit. L'attacco è stato eseguito con successo e ho ottenuto una sessione di Meterpreter sulla macchina Windows 10.




**Utilizzo della sessione Meterpreter**

Con la sessione attiva, ho eseguito il comando help per esplorare le varie opzioni disponibili e familiarizzare con i comandi di Meterpreter. Una delle richieste specifiche dell'esercizio era quella di ottenere l'indirizzo IP della macchina vittima, per cui ho usato il comando ipconfig, che mi ha restituito l'output confermando l'IP 192.168.1.70.

Successivamente, per soddisfare la richiesta di catturare uno screenshot della macchina vittima, ho utilizzato il comando screenshot. Questo comando ha catturato un'immagine della schermata attiva di Windows 10, che è stata salvata automaticamente sul sistema Kali nel percorso /home/kali/fjhikLpa.jpeg. Ho verificato che il file fosse stato salvato correttamente e visualizzato l'immagine per confermarne il contenuto.




**Considerazioni sulla vulnerabilità**

La vulnerabilità sfruttata, legata a Icecast, è particolarmente critica poiché consente l'accesso remoto e l'esecuzione di codice arbitrario sul sistema vittima. Questo tipo di vulnerabilità rappresenta un rischio significativo in ambienti in cui il software non viene aggiornato regolarmente. Icecast è un'applicazione open source ampiamente utilizzata per lo streaming audio, il che rende la sua sicurezza particolarmente importante per proteggere i dati e l'integrità dei sistemi.

In conclusione, l'esercizio mi ha permesso di approfondire l'uso di Metasploit e di Meterpreter, comprese le tecniche di sfruttamento delle vulnerabilità e il controllo post-exploit. Questo tipo di pratica è essenziale per comprendere non solo come avvengono gli attacchi, ma anche per apprendere come implementare contromisure efficaci e proteggere i sistemi da minacce reali.