

S7L5

L'obiettivo del compito di oggi è cambiare gli indirizzi ip delle macchine kali linux e metasploitable2 , avviare una sessione di meterpreter, raccogliere la configurazione di rete e le informazioni sulla tabella di routing. Per prima cosa dobbiamo cambiare gli indirizzi ip alle nostre macchine, per farlo ci basterà eseguire il comando `"sudo nano etc/network/interfaces"` in modo tale da modificare la configurazione di rete, vale sia per kali linux che metasploitable2. Dopodichè avviamo una sessione di metasploit con il comando `"msfconsole"` e utilizziamo il comando di ricerca per gli exploit di java che è il seguente `"search java_rm"`. Una volta trovato l'exploit verifichiamo se ha tutto quello di cui ha bisogno per poter procedere con il comando `"show options"` e ci farà notare che manca il RHOSTS, quindi l'indirizzo ip della macchina target e che l'HTTPDELAY è settato su 10. Inseriamo l'indirizzo ip tagret con il comando `"set RHOSTS 192.168.11.112"` e modifichiamo l'HTTPDELAY su 20 con il comando `"set HTTPDELAY 20"`. Dobbiamo cambiare l'HTTPDELAY perchè se no ci uscirà un errore che ci dice che l'HTTPDELAY 10 è scaduto e non può procedere con l'esecuzione. Una volta configurato tutto eseguiamo con il comando exploit, una volta dentro la sessione meterpreter per trovare le informazioni sulla tabella di routing ci basterà utilizzare il comando `"route"` mentre per la confiugurazione di rete utilizziamo il comando `"ifconfig"`.