# Esame S7-L5

Innanzitutto, ho settato gli indirizzi ip correttamente delle due macchine che useremo per questo esame.  
Kali: 192.168.11.111  
Metasploitable: 192.168.11.112

Dopo di ció, effettuo una scansione nmap per vedere i servizi attivi nelle varie porte  
Immagine che contiene testo, schermata

Descrizione generata automaticamente  
possiamo notare come da esercizio che la porta 1099 è aperta e presenta il servizio Java RMI, che andremo ad esploitare subito.

Tramite msfconsole apriamo Metasploit e cerchiamo Java RMI  
Immagine che contiene testo, schermata

Descrizione generata automaticamente

Selezioniamo la 8 in questo caso, essendo il piú adatto

In seguito, settiamo i vari HOST per bene e lanciamo l’exploit  


Immagine che contiene testo, Carattere, schermata

Descrizione generata automaticamente

Infine, tramite Meterpreter recuperiamo le informazioni riguardo la connettivitá e il routing del target

Immagine che contiene testo, Carattere, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Grazie!