W16D4 Benchmark

Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti dell'esercizio sono:

-Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro…

Come da traccia o ottenuto accesso a Metasploitable2 mediante Metasploit usando l'exploit "explot/multi/misc/java_rmi_server che mi ha dato accesso remoto alla macchina in questione sfruttando la porta 1099 vulnerabile. Cosi facendo ho avuto accesso alle seguenti info:

Configurazione di rete:

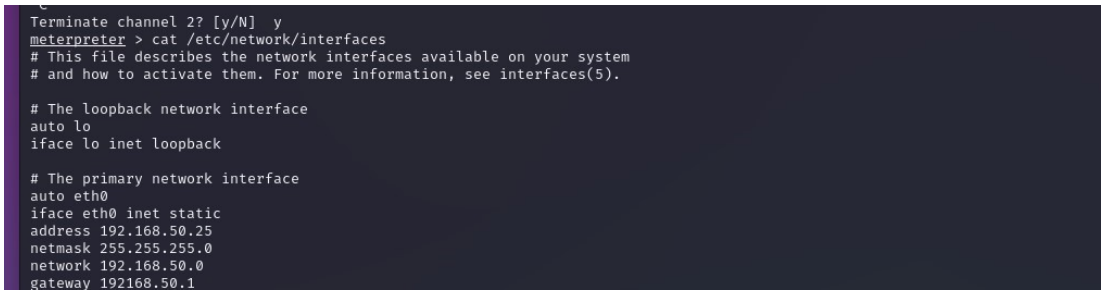
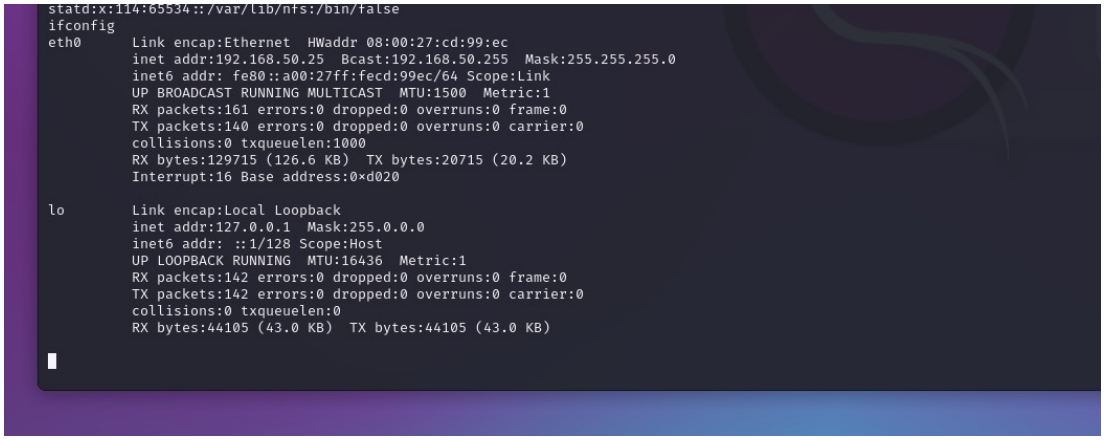
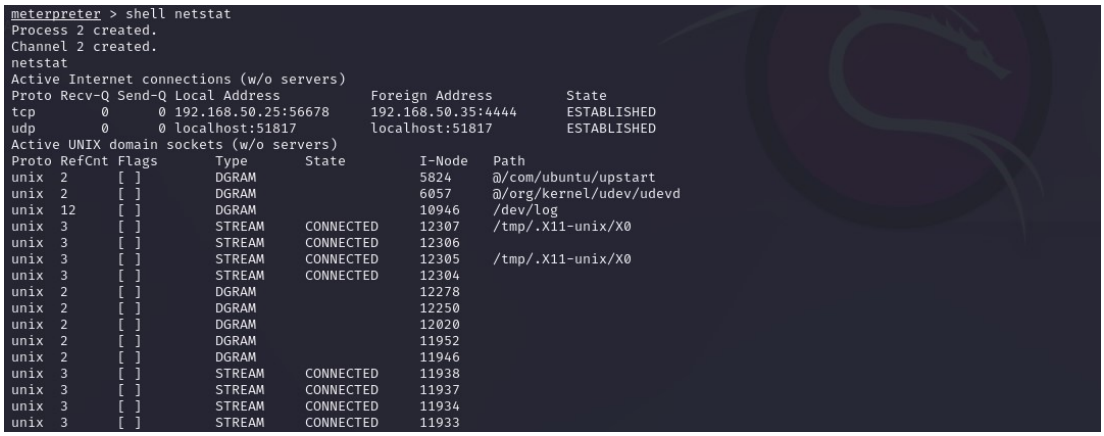


Tabela di rooting:

Ifconfig:



Netstat:



Info di sistema:

File con le hash delle password: