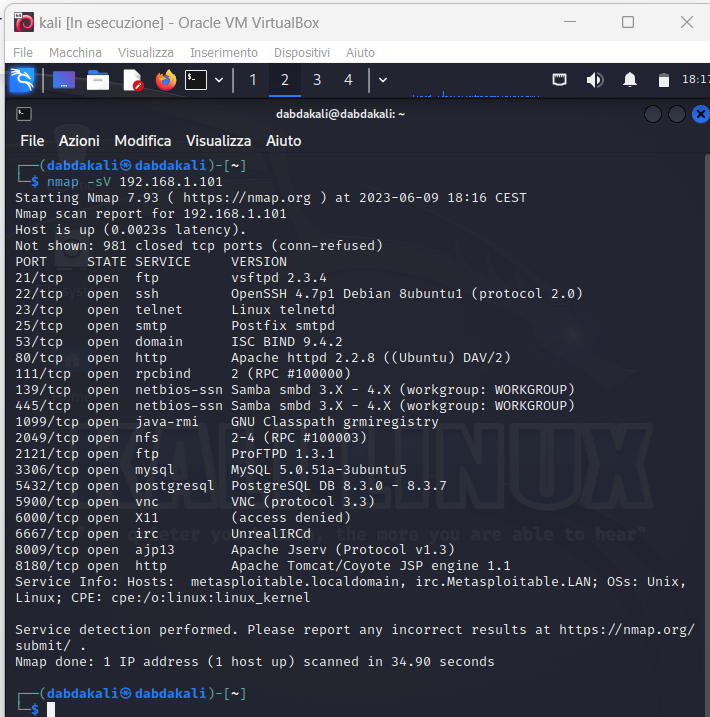
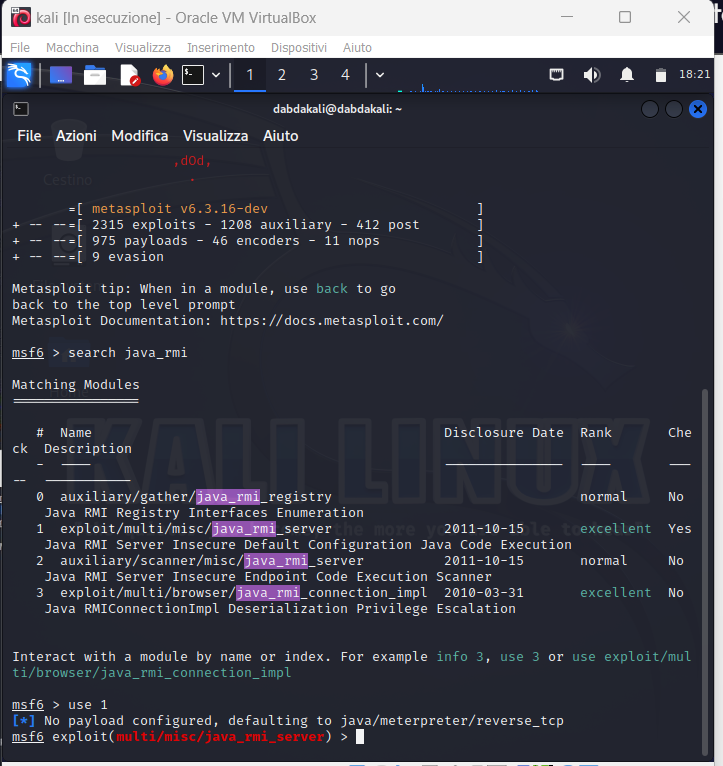
Vulnerabilità java\_rmi

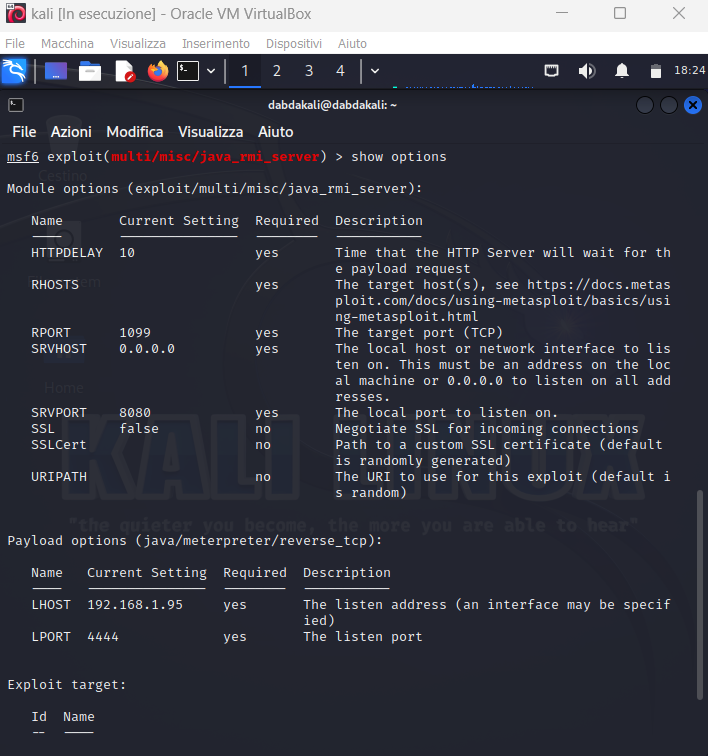


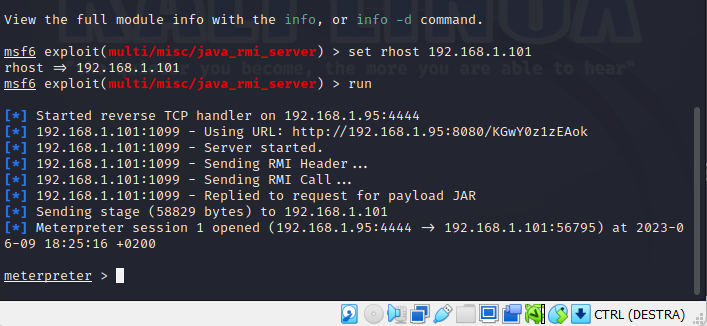
1) iniziamo dal principio , utilizziamo il nostro tool nmap per avere un quadro completo della nostra macchina vittima , oggi ci concentreremo sulla porta 1099 per sfruttare la vulnerabilità con il nostro payload di meterpeter

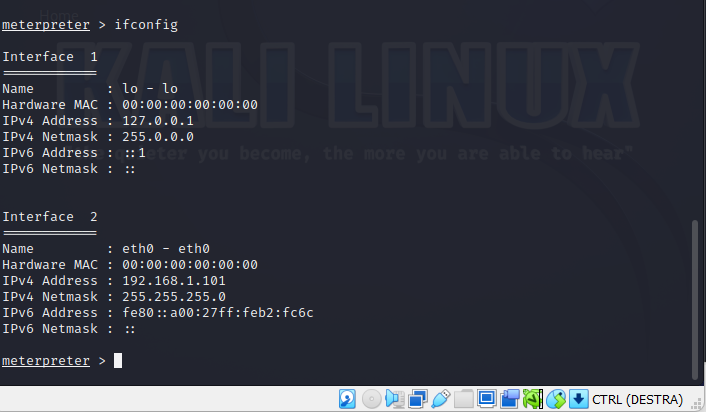


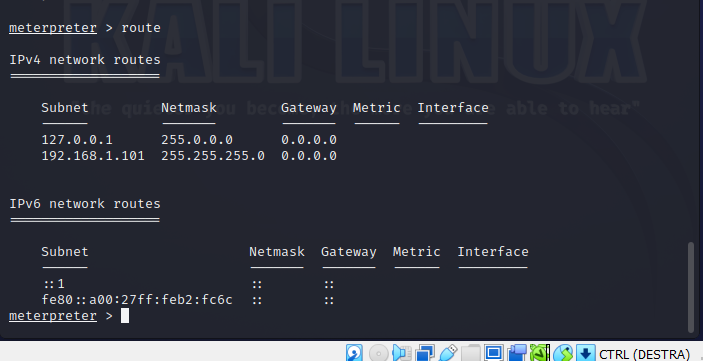
2) una volta completata la scansione effettuata con nmap , spostiamoci su un altro terminale e usiamo il nostro tool d’attacco msfconsole , una volta avviato cerchiamo specifici exploit efficaci contro la vulnerabilità java\_rmi , quindi cosa facciamo ora.. , dato che msfconsole mette a disposizione piu di 2000 exploit, capirete benissimo che cercare ogni singolo exploit fino a trovare ciò che serve non è la soluzione migliore , quindi usiamo il tag search e come parola chiave inseriamo java\_rmi , vedremo come mess output solo exploit che contengono la nostra parola chiava java\_rmi , una volta trovato il nostro exploit dobbiamo usarlo , quindi digitiamo use o si inserisce il numero identificativo o inseriamo il path dell’exploit , una volta usato vediamo che ci dice qualcosa , ci mostra a schermo il seguente messaggio , se non è stato configurato nessu tipo di payload, di default abbiamo il reverse\_tcp che a noi per quello che andremo a fare va molto piu

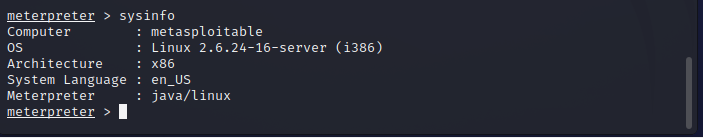
che bene

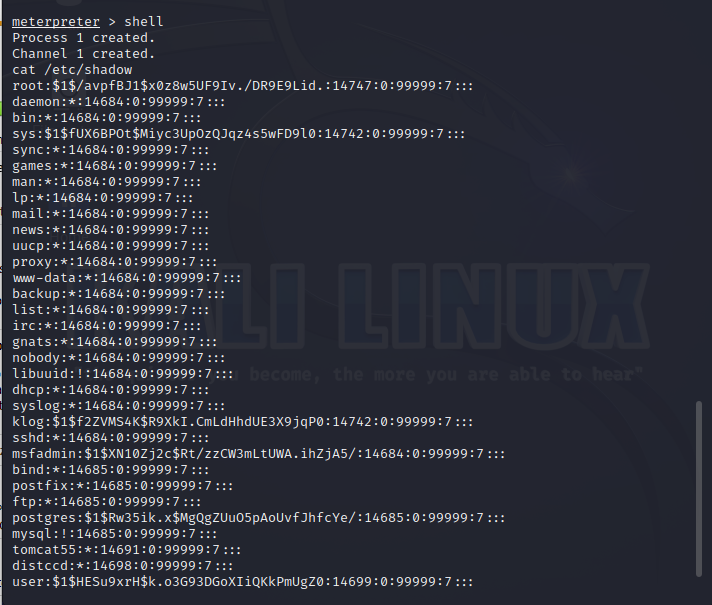


3)una volta usato il nostro exploit , scriviamo show options per andare a configurare determinati parametri per il quali senza di essi il nostro exploit non avrebbe alcun effetto ,concentriamoci ora sulla voce required dove le risposte che possiamo trovare sotto questa voce sono solo yes/no , tutti i campi dove troviamo il valore yes significa che sono obbligatori , alcuni campi sono gia settati di default mentre alcuni dobbiamo configurarli manualmente , prendiamo per esempio il secondo campo dove troviamo scritto rhosts, rhost è l’indirizzo della nostra macchina vittima dove noi ora andremo a settarlo 

4) come si settta un parametro ?? abbiamo visto che il campo rhost era obbligatorio e per di più anche vuoto , per configurare un qualsiasi valore nel nostro exploit bisogna digitare set seguito dal nome che vogliamo configurare , in questo caso scriviamo set rhost dove andiamo a inserire l’indirizzo della nostra macchina vittima , fatto ciò potete nuovamente digitare il tag show options per verificare se il nostro exploit è pronto per essere utilizzato , come visto in precedenza solo la voce rhosts andava configurata fatto ciò possiamo lanciare il nostro exploit , e lo lanciamo usando il comando run/exploit. Come vedete voi stessi dai seguenti messaggi a schermo l’attacco è andato a buon fine , ma da dove vediamo che l’attacco è riuscito ?? , concentriamoci sull’ultima riga , dove appunto vediamo scritto meterpreter, questo vuol dire che si è aperta una sessione di meterpreter verso la nostra macchina vittima 

5) digitiamo il comando ifconfig , questo ci darà dei seguenti risultati , ma questi risultati di chi sono e soprattutto come siamo sicuri che sono della macchina vittima e non i nostri ?? , concentriamoci sulla voce ipv4 address , leggiamo che finisce con 101 , quando noi siamo 95 , quindi solo questo risultato ci mostra che siamo nella macchina vittima , e d’ora in poi oggi messaggio che riporterà a schermo sarà unicamente della macchina target , quindi con il seguente comando ifcongig , noi possiamo leggere oltre al suo ipv4 anche il suo ipv6 e il suo mac address 

6) La tabella di routing è un componente fondamentale nella gestione delle reti informatiche. Essa contiene una lista di percorsi (routes) che definiscono come i pacchetti di dati devono essere instradati da un nodo di rete a un altro. Ogni riga della tabella di routing specifica un indirizzo di rete di destinazione e l'interfaccia di rete associata attraverso cui i pacchetti devono passare per raggiungere tale destinazione. ora vogliamo ottenere informazioni sulla sua tabella di routing , per fare ciò digitiamo il seguente comando route 

7) SystemInfo è un'utility in grado di visualizzare, in maniera veloce ed estremamente compatta, tutte le informazioni essenziali sull'hardware, coem potete vedere , leggiamo il nome del computer in questo caso metaspolitable , il suo sistema operativo ,l’architettura ecce cc.

8) parte importante di questo esercizio , una volta entrati in una macchina oltre a mantere gli accessi si possono usare altre strategie per continuare ad avere un collegamento con la macchina target senza aver il bisgono di usare sempre un exploit. In questo caso utilizziamo il comando hasdump per windows mentre per linux digitiamo cat /etc/shadow , il messaggio che ci mostra sono tutti i nomi utenti e i loro rispettivi hash ,piccolo consiglio , tutti gli utenti che hanno come hash il seguente valore iniziale “\*” “!”, significa che per qell’utente il valore hash o è nullo o inesistente , una volta avuto ciò , copiamo i seguenti valori ci spostiamo su un altro terminale ed utilizziamo tool di cracking( haschcat ,hydra) , il tutto in locale nella nostra macchina , quando avremo in chiaro nome utente e password , capirete benissimo che sfruttare altre vulnerabilità verso la macchina target è ormai obsoleto , abbiamo le credenziali ormai , possiamo fare tutto ciò che vogliamo con il minimo impegno