Settimana 7 - Esercizio 5

Alessio Golfetto 26/01/2024

Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

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.

Exploit

Cos’è e quali sono le differenze con un malware

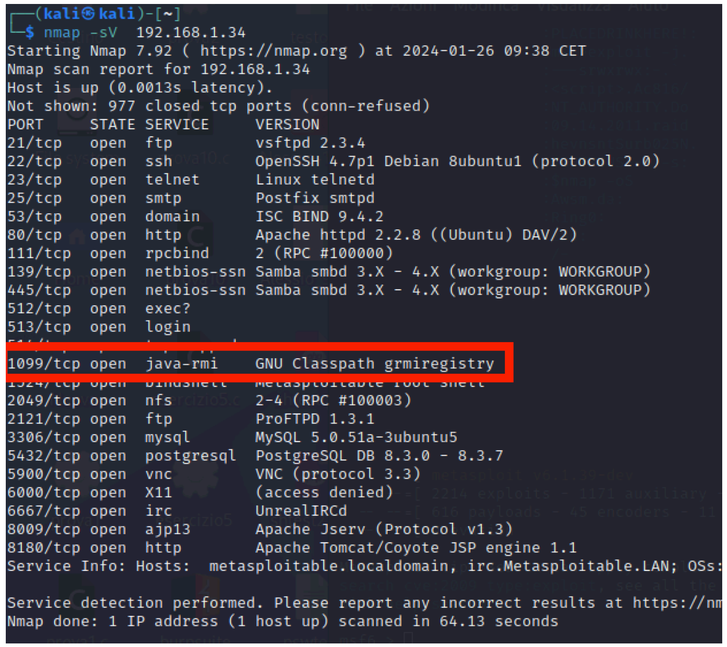
Exploit: un exploit è attacco che sfrutta le vulnerabilità presenti in applicazioni, reti o hardware. Gli exploit sono spesso utilizzati da hacker o malintenzionati per compromettere la sicurezza di un sistema, ottenere accesso non autorizzato o causare danni.

Malware: il termine "malware" (malicious software) è utilizzato per descrivere software progettato per danneggiare o compromettere un computer o un sistema informatico senza il consenso dell'utente. Il malware può assumere diverse forme e svolgere una vasta gamma di attività dannose, ad esempio *virus, worm, ransomware, trojan, spyware ecc*.

Possiamo notare quindi che la differenza tra exploit e malware sta nel fatto che i primi sfruttano una vulnerabilità già presente in un sistema/rete/hardware/software, mentre i secondi hanno scopo di crearne una.

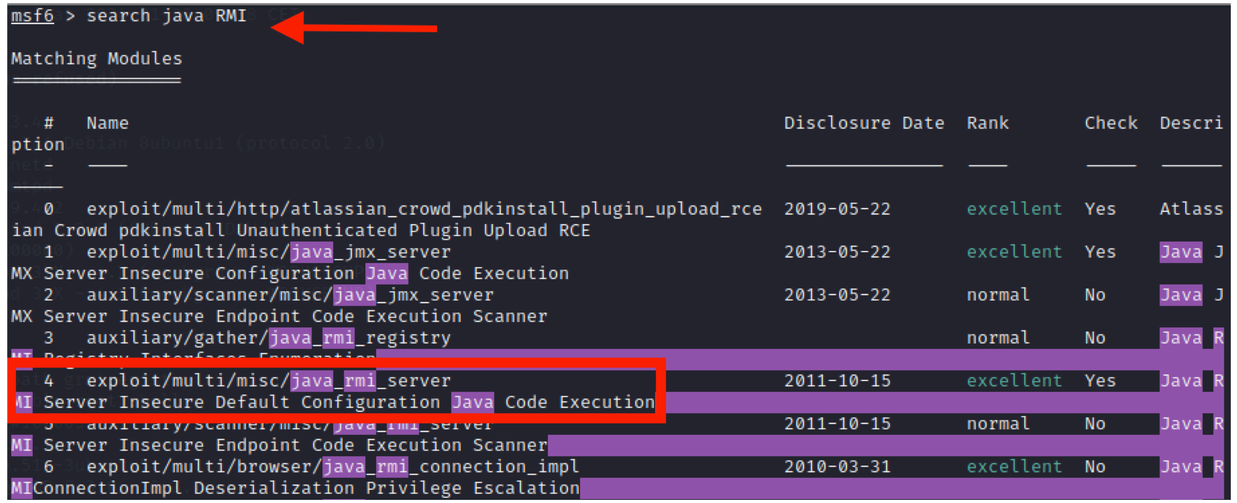
Scansione delle porte

- Come primo passaggio utilizziamo ***nmap*** e andiamo ad eseguire una scansione sulle porte della macchina target eseguendo il comando *nmap -sV 192.168.1.34* (-sV ci restituirà anche la versione del servizio che gira sulla determinata porta). La versione ci serve perché gli exploit funzionano su determinate versioni di applicazioni/servizi etc. Nel nostro caso il servizio e la porta che ci chiede di sfruttare l'esercizio è *java-rmi* sulla porta *1099*.



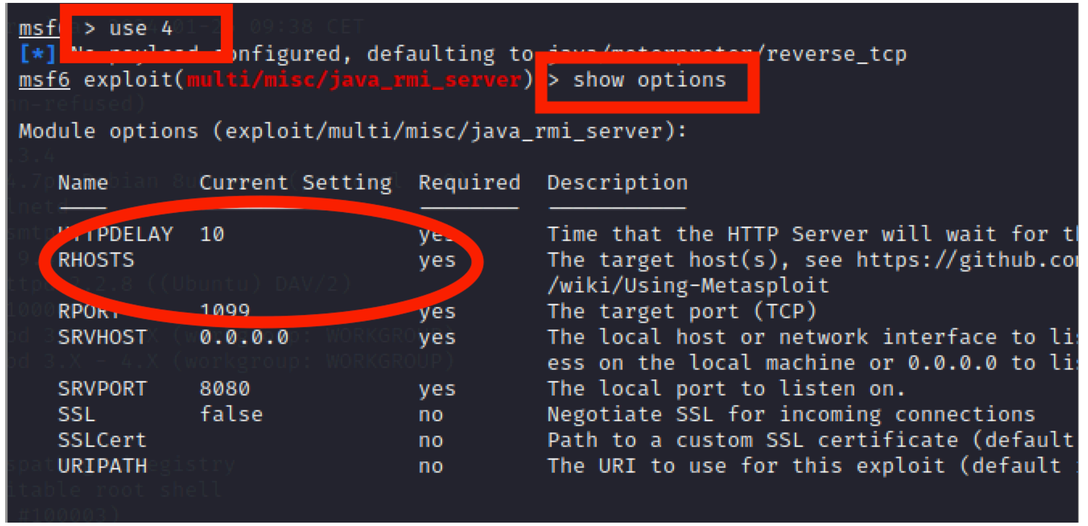
Metasploit e ricerca exploit

- A questo punto avviamo **Metasploit** da un terminale con il comando *msfconsole*. Metasploit è un framework open-source usato per il penetration testing e lo sviluppo di exploit. Fornisce una vasta gamma di exploit e numerosi vettori di attacco che si possono utilizzare contro diversi sistemi e tecnologie. Può essere utilizzato per creare ed automatizzare i propri exploit. Una volta avviato utilizziamo il comando per la ricerca *search java RMI* per ricercare gli exploit che possono tornarci utili nel nostro caso. Una volta ottenuto l'elenco degli exploit, si procede ad una prima analisi in cui scartiamo quelli che a noi sicuramente non serviranno (esempio: se dobbiamo attaccare una macchina windows scarteremo tutti quelli che si riferiscono a Linux e viceversa), i rimanenti andranno poi testati uno ad uno per verificare quale funzioni e quale no. Noi abbiamo selezionato il numero 4 che funziona e sfrutta la nostra vulnerabilità.

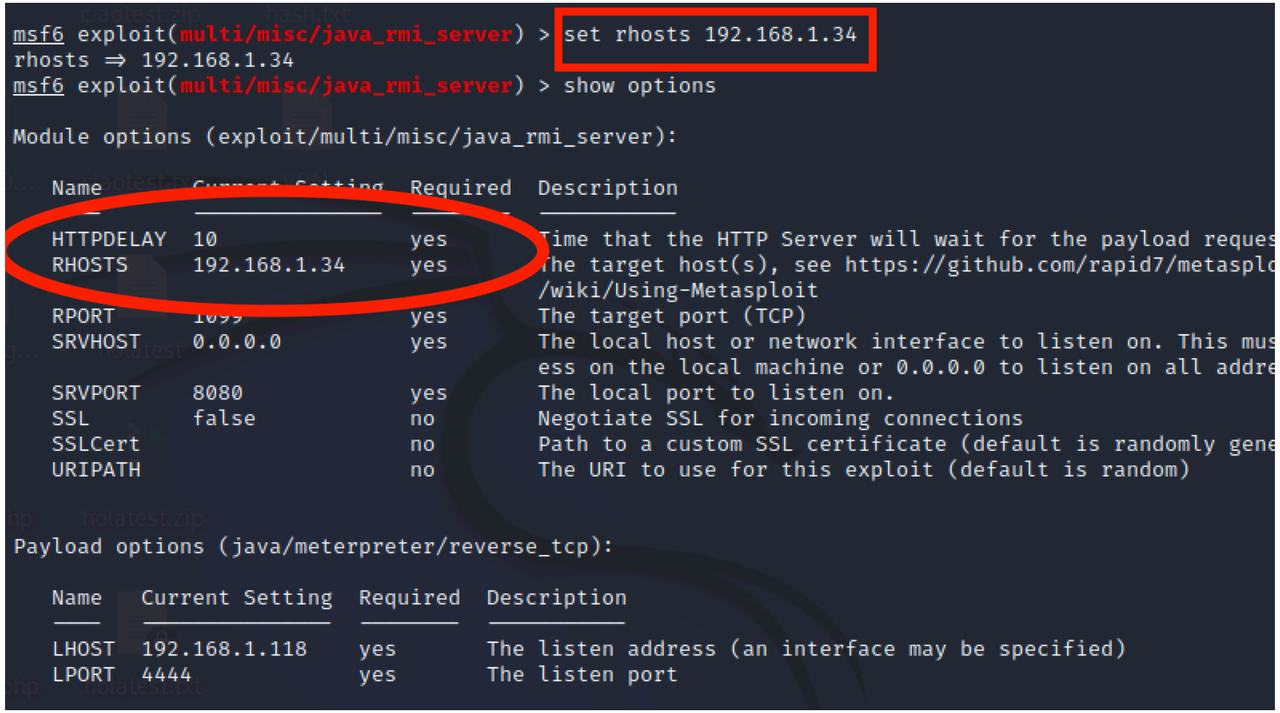


Scelta payload e settare le opzioni

- Individuato l'exploit da utilizzare lo selezioniamo con il comando *use*. Per utilizzare nella pratica un exploit, serve un payload. Nella sicurezza informatica e dei test di penetrazione, il termine "payload" si riferisce specificamente a un insieme di istruzioni o codice che viene eseguito da un software dannoso o da un exploit dopo che questo ha sfruttato con successo una vulnerabilità del sistema. Ora possiamo scegliere se utilizzare il payload che metasploit ci consiglia, oppure sceglierne un altro che si adatti alle nostre necessità con il comando *show payloads*. Noi utilizziamo quello proposto da metasploit e utilizziamo il comando *show options* per vedere quali parametri sono necessari per lanciare il nostro exploit (nel nostro caso manca solo il parametro RHOSTS perché nella colonna "Required è riportata la scritta YES").

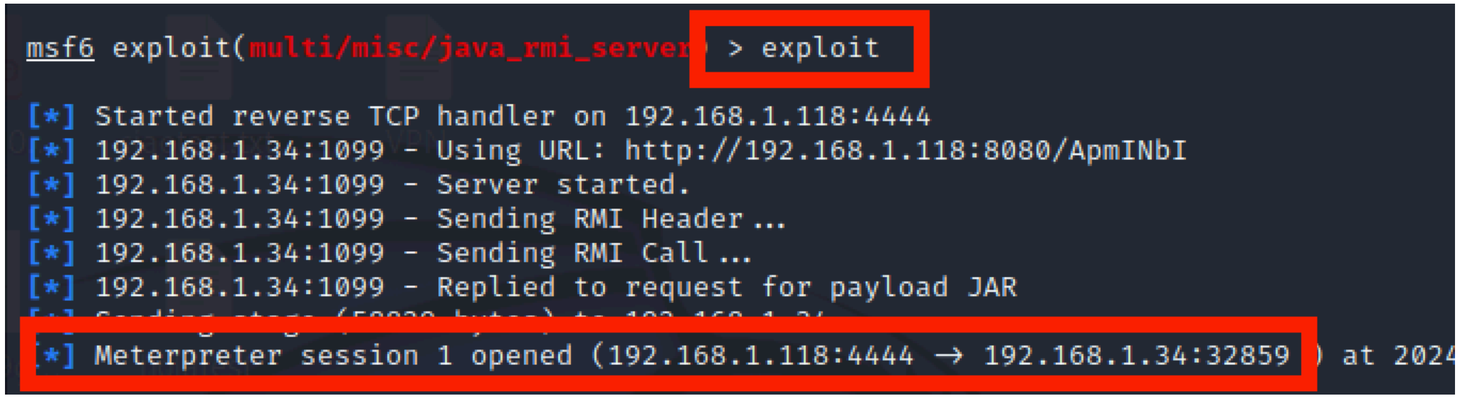


- Andiamo quindi a settare il nostro ip target come hosts con il comando *set rhosts 192.168.1.34* . Dopodiché rilanciamo il comando *show options* per controllare che le modifiche siano state salvate.



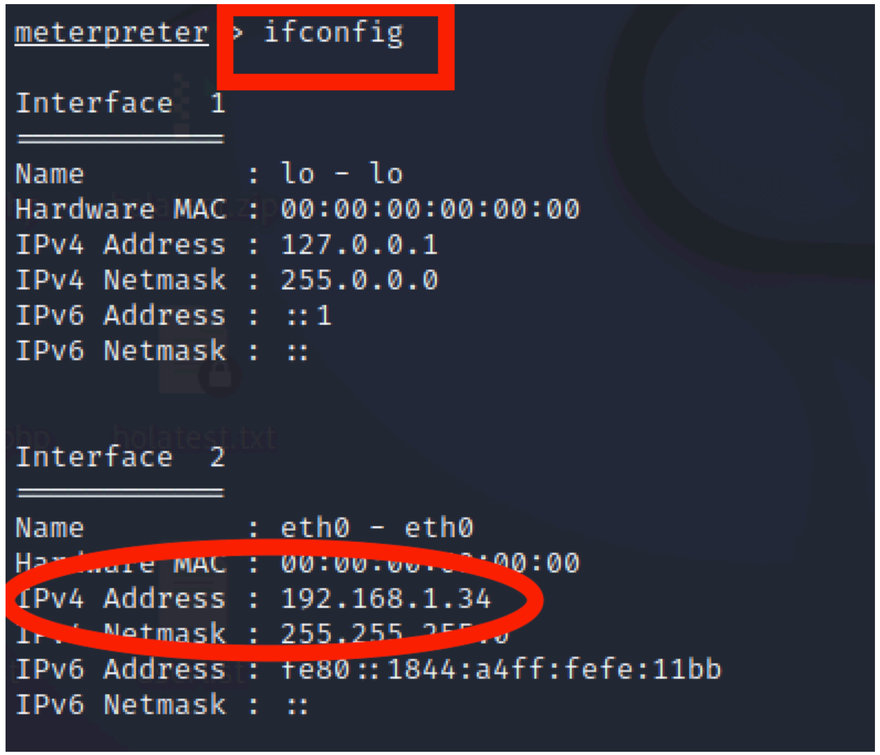
Lanciare exploit e verifica buona riuscita

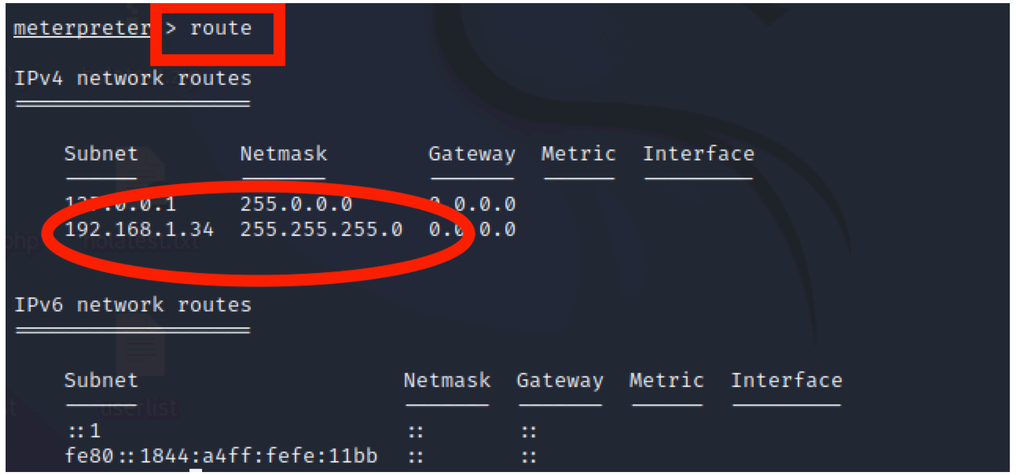
- Verificato che i parametri richiesti siano stati inseriti correttamente e salvati andremo a lanciare l'attacco con il comando *exploit*. Al termine ci restituirà una linea dove ci confermerà che la nostra sessione di meterpreter è stata iniziata con successo. Meterpreter è un payload con molte funzionalità, e molto utile agli scopi di un penetration testing. Meterpreter è una shell molto potente che gira su applicazioni e servizi vulnerabili di diverse tecnologie e sistemi operativi. Le sue funzionalità avanzate consentono movimenti laterali per entrare sempre più nei sistemi, fino ad ottenere accesso completo alle rete obiettivo.



Ricerca configurazione rete e info tabella routing della macchina target

- Ottenuta la sesione di meterpreter possiamo andare tramite il comando *ifconfig* a verificare quale sia la configurazione di rete della macchina target (possiamo utilizzarlo anche come conferma di sessione andata a buon fine) ed il comando *route* per vedere le informazioni della tabella di routing della macchina vittima.





Fine