PENETRATION TESTING – ATTACCO SU METASPLOITABLE

Introduzione:

Gentile Prof,

questo report documenta le attività svolte durante un esercizio di penetration testing su un ambiente controllato, utilizzando **Kali Linux come macchina attaccante** e **Metasploitable come macchina vittima.** L'obiettivo dell'esercizio era **sfruttare** una vulnerabilità nel servizio Java RMI sulla porta 1099 di Metasploitable per **ottenere una sessione remota Meterpreter** e **raccogliere evidenze sulla configurazione di rete** e **la tabella di routing della macchina vittima.**

Dettagli delle macchine coinvolte:

Macchina Attaccante (Kali Linux):

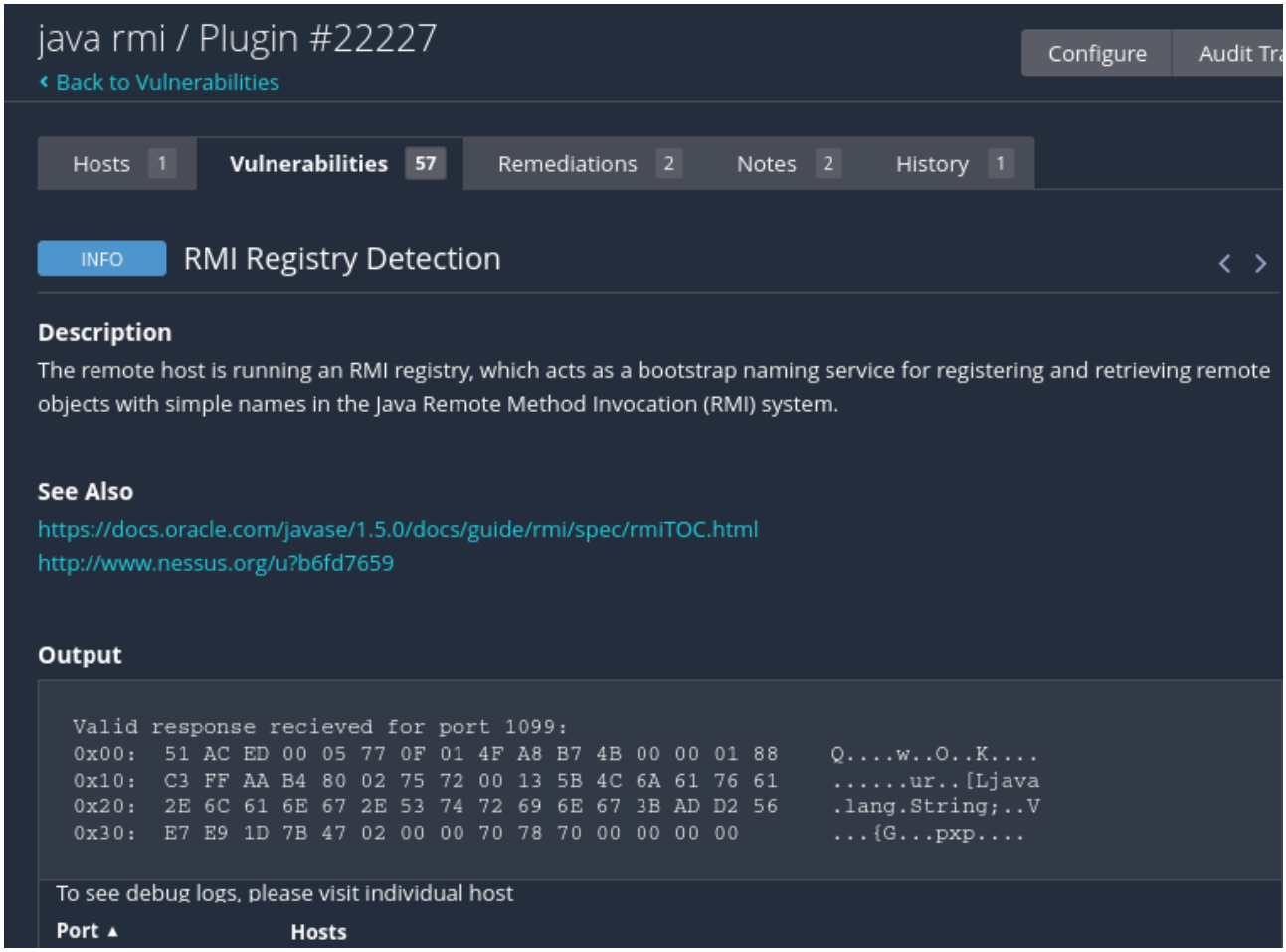
Indirizzo IP: 192.168.99.111

Macchina Vittima (Metasploitable):

Indirizzo IP: 192.168.99.112

Fase 1: Rilevamento delle vulnerabilità con Nessus:

Prima di eseguire l'attacco effettivo, è stata condotta una scansione di vulnerabilità utilizzando Nessus per confermare l'esistenza delle vulnerabilità note sulla macchina vittima. Durante la scansione, è stata identificata la presenza del servizio RMI Registry sulla porta 1099 di Metasploitable.

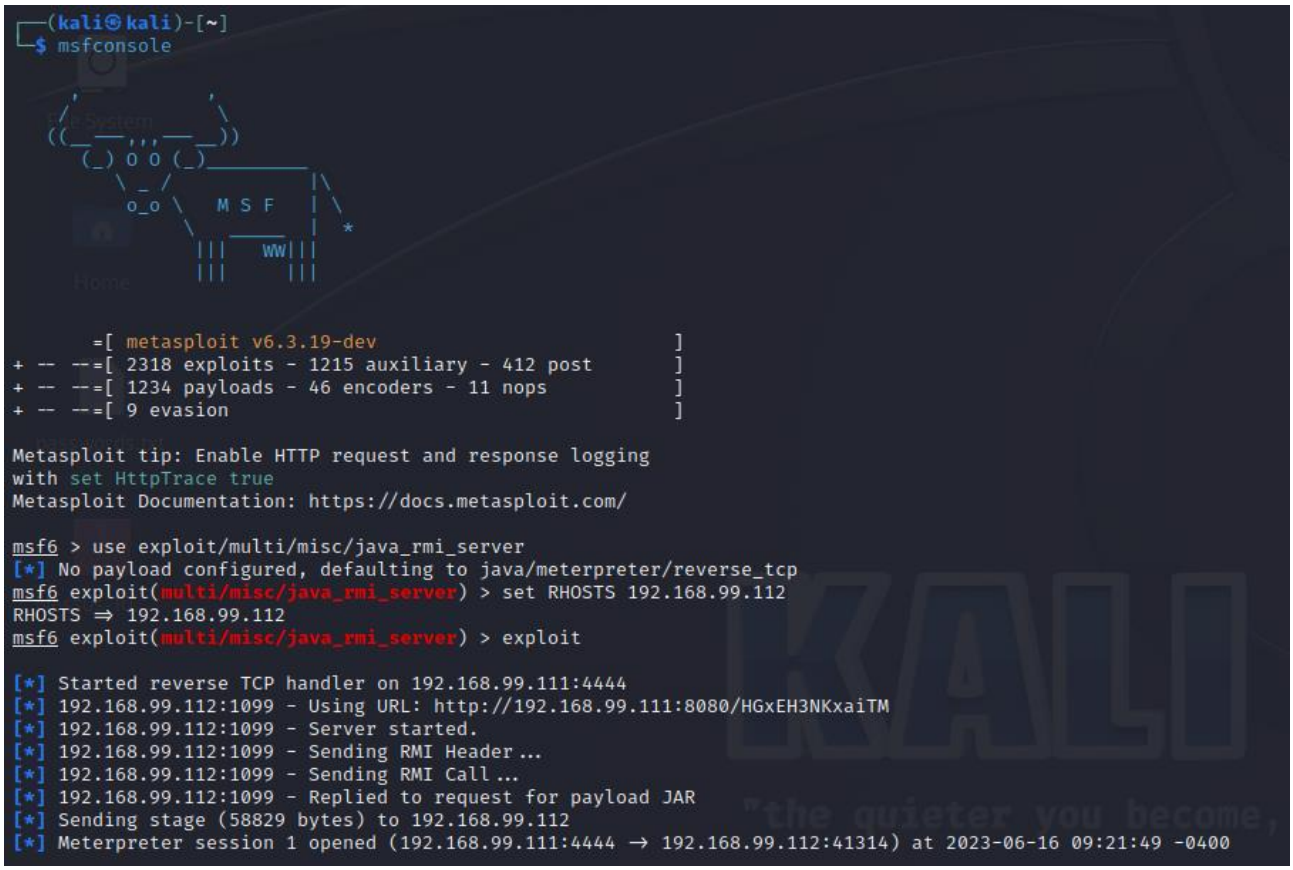


Dettagli della Vulnerabilità Rilevata:

Plugin: java rmi / Plugin #22227
Hosts: 1
Vulnerabilità Rilevate: 57
Azioni correttive: 2
Note: 2
Cronologia: 1

Fase 2: Esecuzione dell'attacco con Metasploit:

Dopo aver confermato la presenza delle vulnerabilità, abbiamo proceduto con l'utilizzo di Metasploit Framework per eseguire l'attacco sulla macchina Metasploitable. Abbiamo utilizzato il modulo "exploit/multi/misc/java_rmi_server" di Metasploit per sfruttare la vulnerabilità RMI sulla porta 1099.

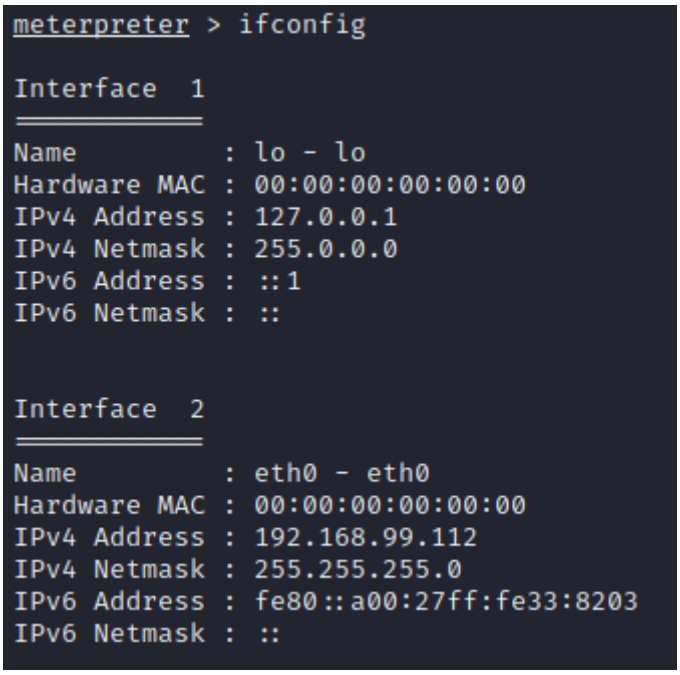


Passaggi dell'attacco eseguiti:

Avvio di Metasploit Framework sulla macchina attaccante mediante il comando "msfconsole";
Selezione del modulo di exploit "exploit/multi/misc/java_rmi_server";
Impostazione dell'indirizzo IP della macchina vittima (192.168.99.112) come RHOSTS;
Esecuzione dell'attacco mediante il comando "exploit".

Fase 3: Ottenimento della sessione remota Meterpreter:

L'attacco ha avuto successo, e come risultato, è stata stabilita una sessione remota Meterpreter sulla macchina vittima. Attraverso questa sessione, siamo stati in grado di eseguire comandi sulla macchina vittima e raccogliere le seguenti evidenze richieste:



Configurazione di rete della macchina vittima:
Utilizzando il comando "ifconfig" nella sessione Meterpreter, abbiamo ottenuto informazioni sulla configurazione di rete della macchina vittima, tra cui l'indirizzo IP della scheda di rete, il gateway predefinito e altri dettagli rilevanti.

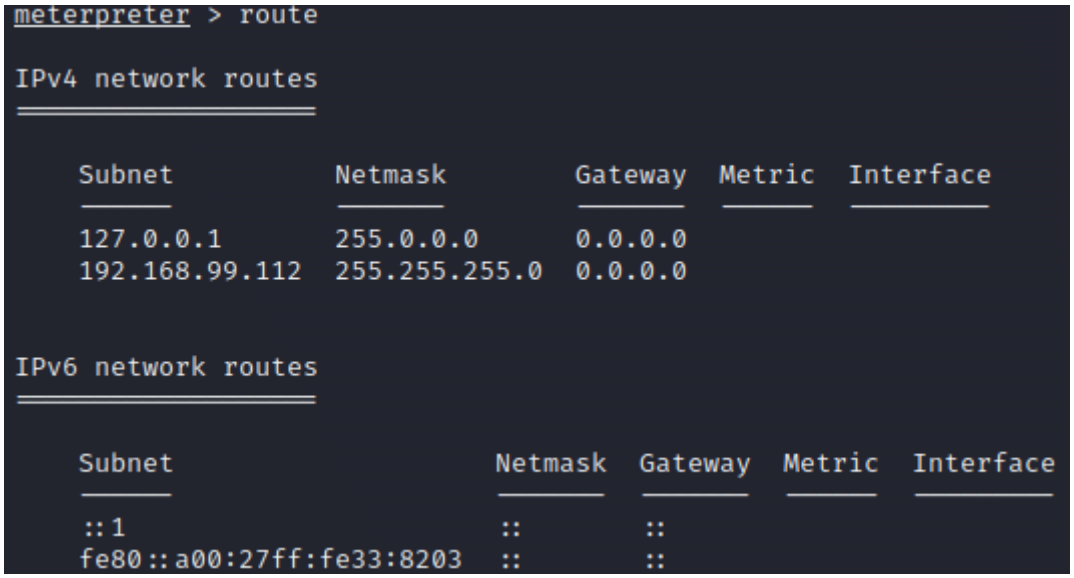


Tabella di routing della macchina vittima:
Per ottenere informazioni sulla tabella di routing della macchina vittima, abbiamo utilizzato il comando "route" nella sessione Meterpreter.

Conclusioni:

Durante l'esercizio di penetration testing su Metasploitable, abbiamo condotto con successo un attacco sfruttando una vulnerabilità nel servizio Java RMI sulla porta 1099. Questa vulnerabilità ha consentito l'accesso non autorizzato alla macchina vittima e l'ottenimento di una sessione remota Meterpreter.

Attraverso la sessione Meterpreter, siamo stati in grado di raccogliere importanti informazioni sulla configurazione di rete della macchina vittima. Utilizzando il comando **"ifconfig"**, abbiamo ottenuto dettagli riguardanti l'indirizzo IP, la subnet mask, l'indirizzo MAC e altri parametri di rete. Queste informazioni sono fondamentali per comprendere l'infrastruttura di rete della macchina vittima e identificare eventuali vulnerabilità o configurazioni non sicure.

Tuttavia, non siamo stati in grado di ottenere una visione completa della tabella di routing della macchina vittima a causa di limitazioni nell'ambiente di esecuzione. Le informazioni di routing che siamo riusciti a raccogliere indicano che il traffico destinato all'indirizzo di loopback (127.0.0.1) viene instradato internamente, mentre il traffico destinato all'indirizzo IPv4 della macchina vittima (192.168.99.112) viene instradato tramite l'interfaccia predefinita.

In conclusione, l'esercizio ha dimostrato l'efficacia dell'utilizzo di Metasploit e l'exploit basato sulla vulnerabilità Java RMI per ottenere accesso remoto non autorizzato a una macchina vittima. È fondamentale che le organizzazioni proteggano le proprie risorse IT e mitigano le vulnerabilità presenti nei loro sistemi per evitare accessi non autorizzati e proteggere i dati sensibili.

Il report delle evidenze raccolte fornisce una panoramica delle informazioni acquisite durante il penetration testing e dei comandi eseguiti sulla macchina vittima.