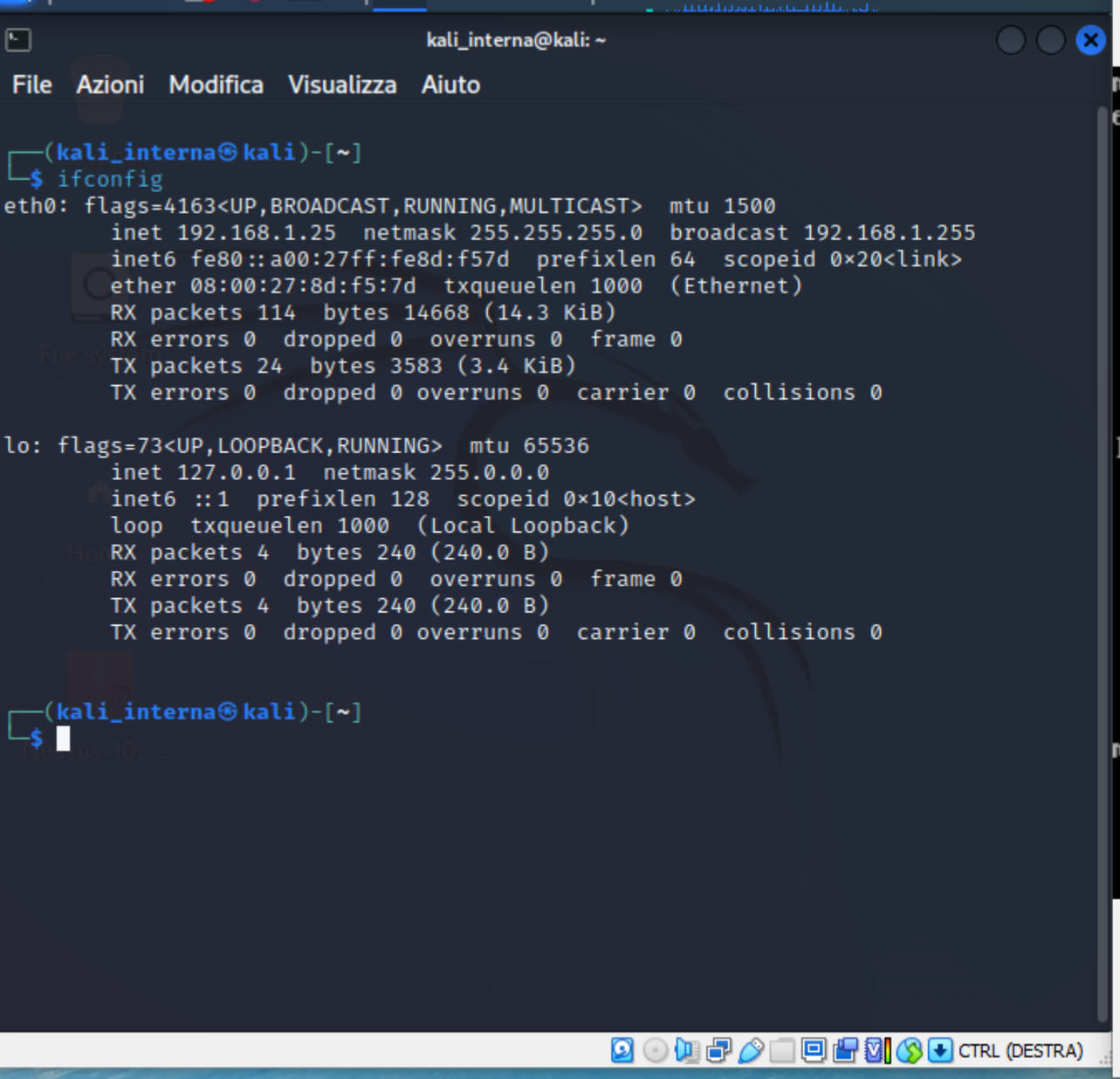
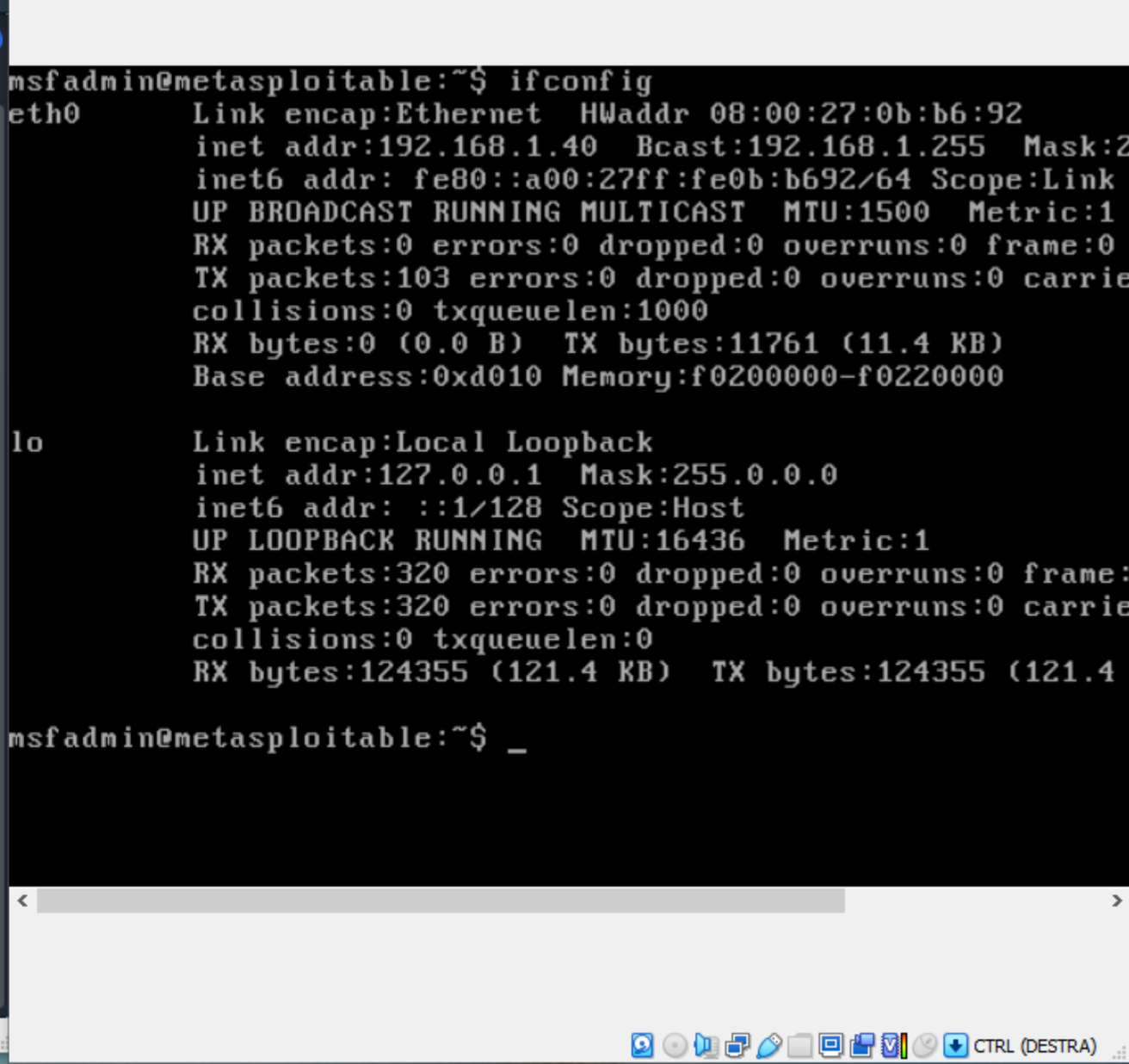
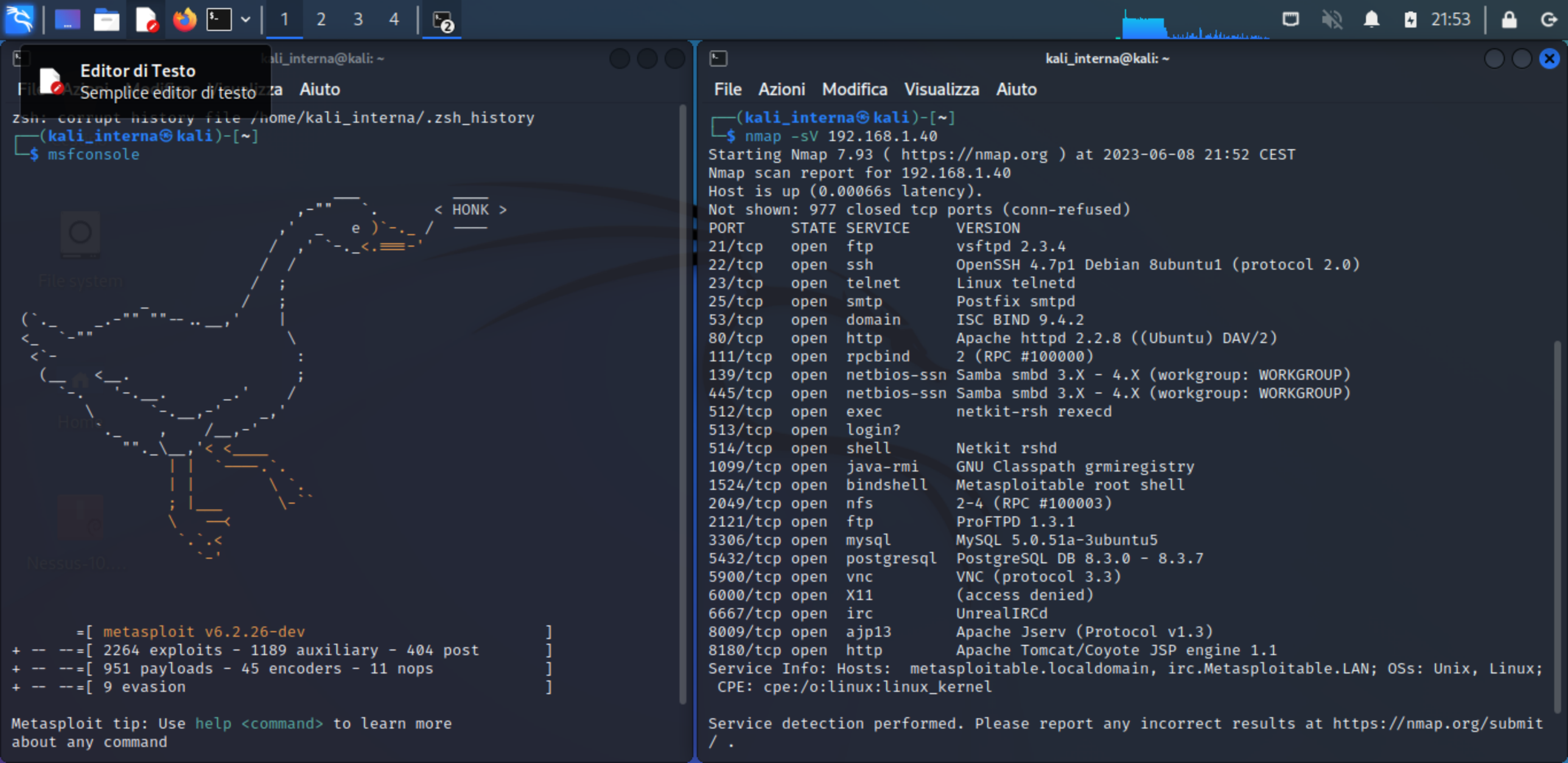
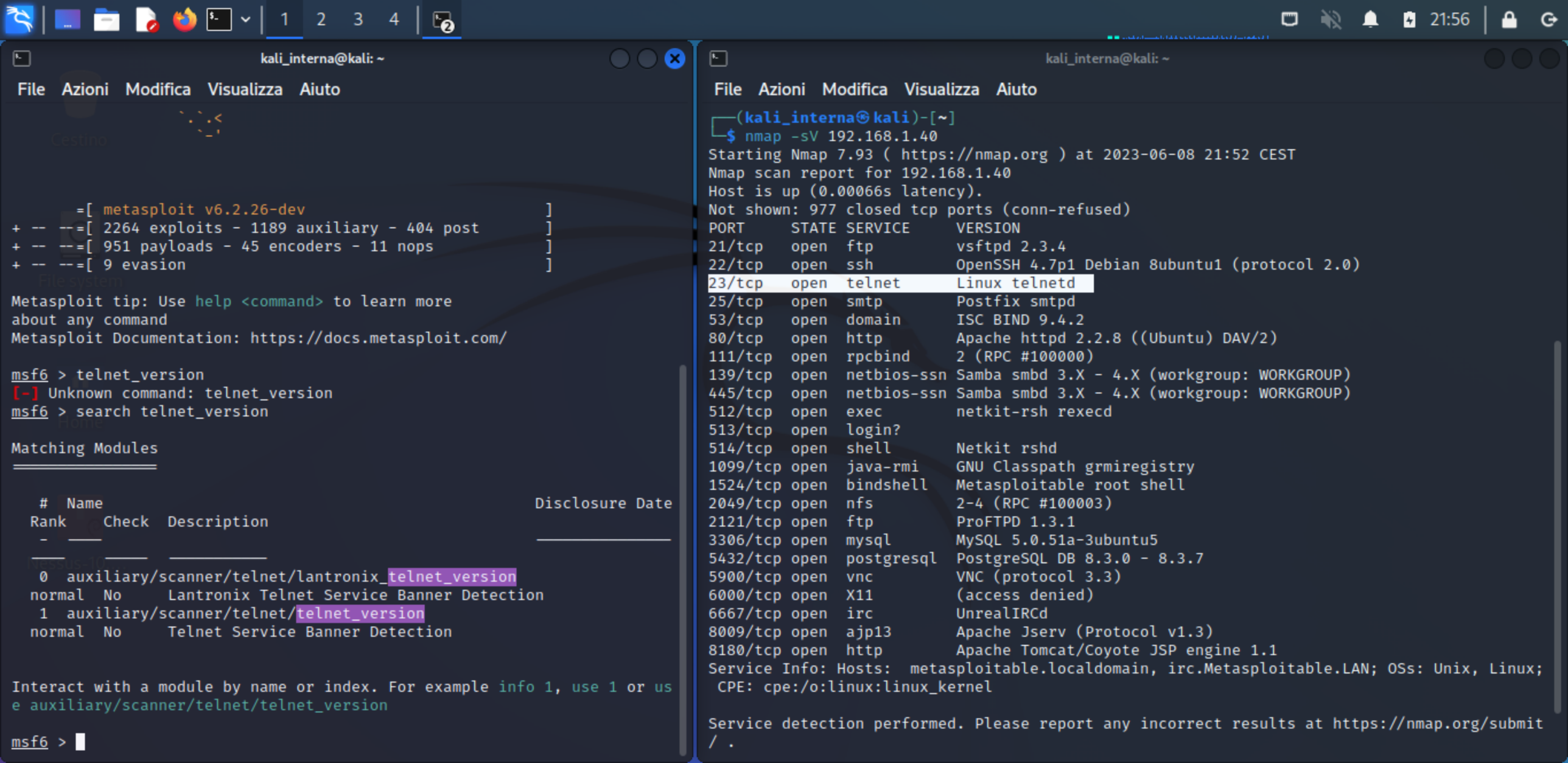
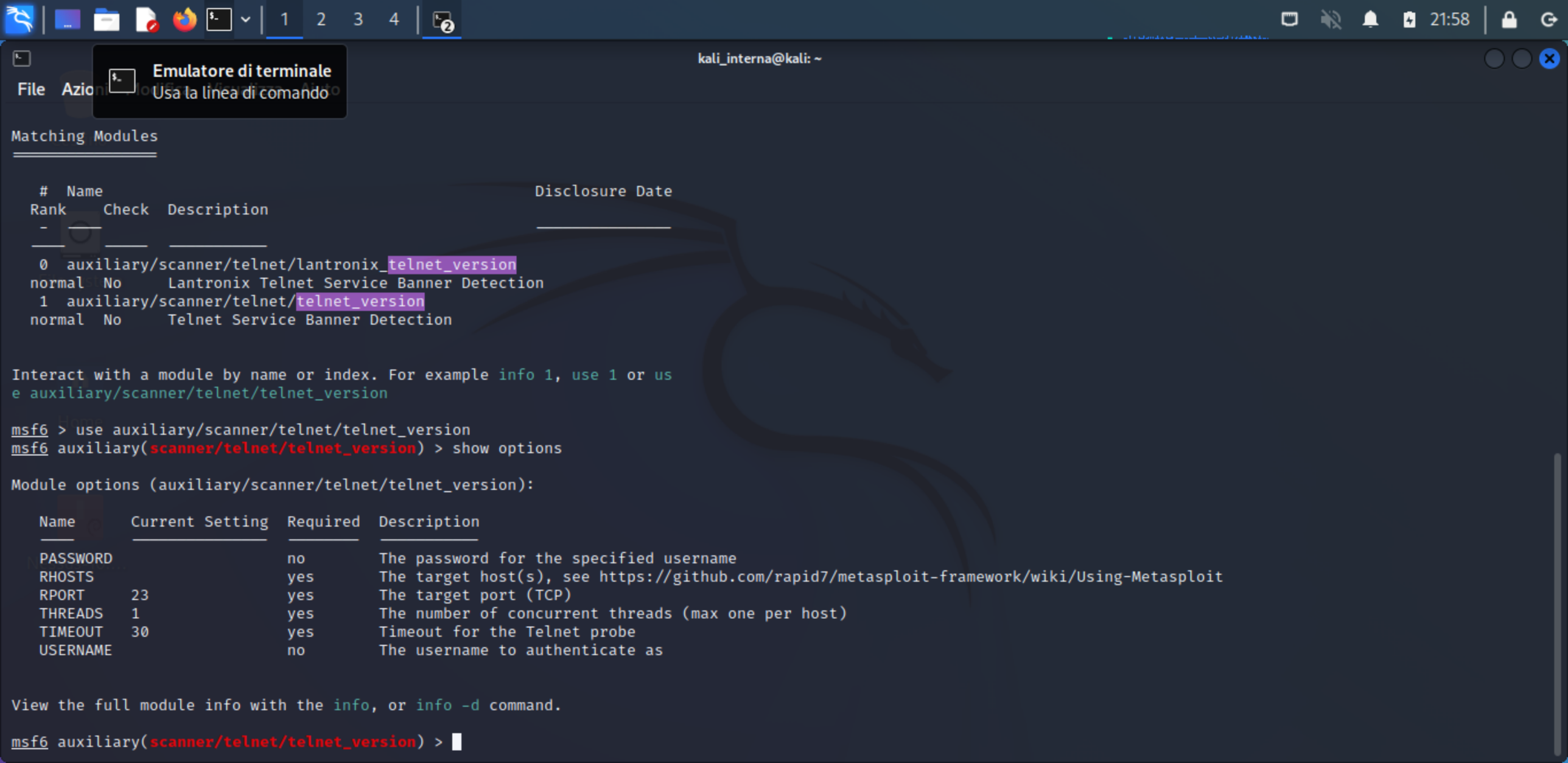

kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
(kali_interna㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::a00:27ff:fe8d:f57d prefixlen 64 scopeid 0x20<link>
ether 08:00:27:8d:f5:7d 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)

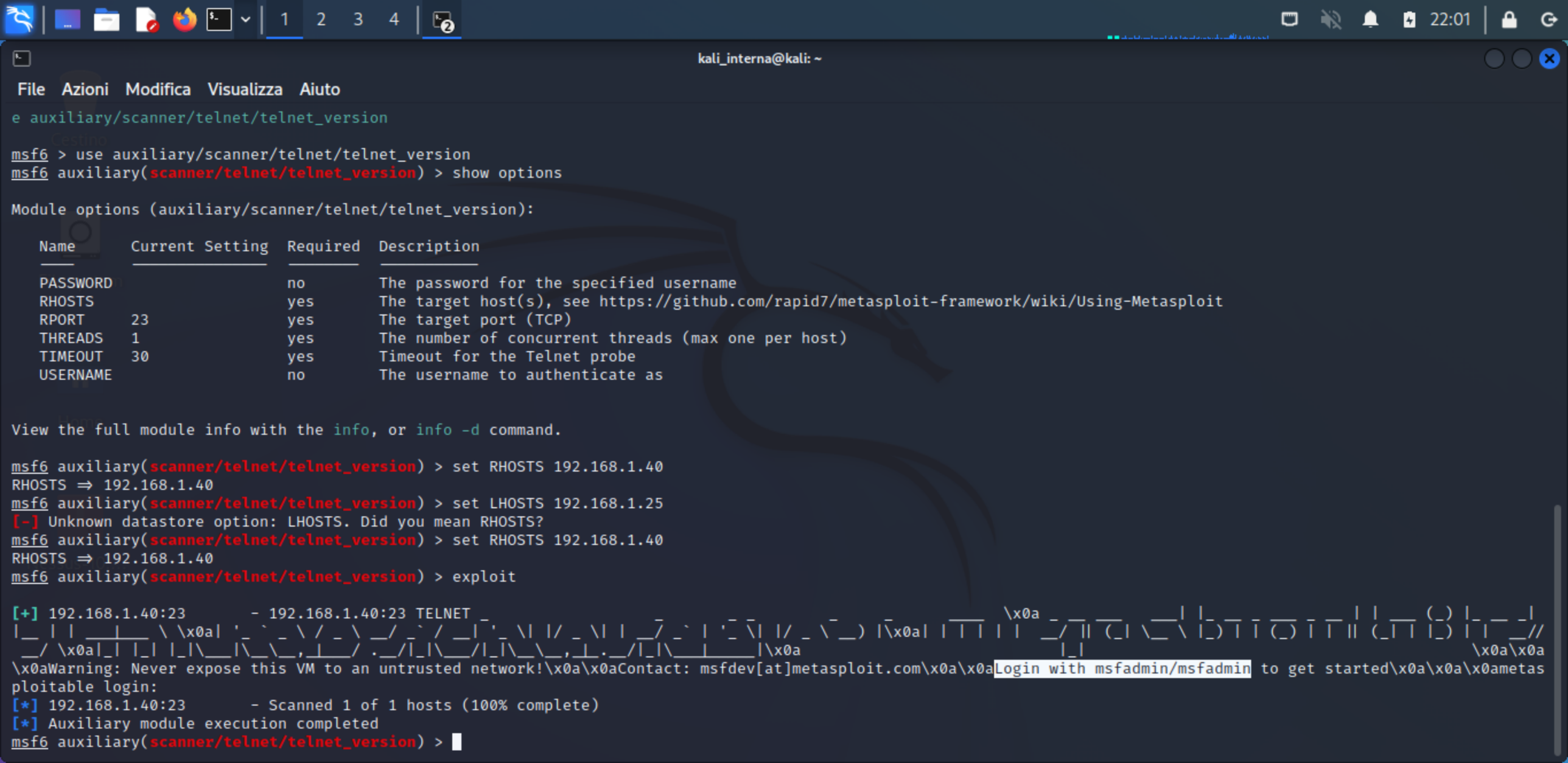

msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:0b:b6:92
inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:2
inet6 addr: fe80::a00:27ff:fe0b:b692/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:103 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)


Editor di Testo
Semplice editor di testo
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
zsh: corrupt history file /home/kali_interna/.zsh_history
(kali_interna㉿kali)-[~]
$ msfconsole
< HONK >
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Use help <command> to learn more about any command
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 21:52 CEST
Nmap scan report for 192.168.1.40
Host is up (0.00066s 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
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Use help <command> to learn more about any command
Metasploit Documentation: https://docs.metasploit.com/
msf6 > telnet_version
[-] Unknown command: telnet_version
msf6 > search telnet_version
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/telnet/lantronix_telnet_version normal No Lantronix Telnet Service Banner Detection
1 auxiliary/scanner/telnet/telnet_version normal No Telnet Service Banner Detection
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version
msf6 >
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 21:52 CEST
Nmap scan report for 192.168.1.40
Host is up (0.00066s 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/ .




```
Matching Modules
================

   #  Name                                                Disclosure Date
  Rank    Check  Description
   -  ----                                                ---------------
   0  auxiliary/scanner/telnet/lantronix_telnet_version
  normal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version
  normal  No     Telnet Service Banner Detection


Interact with a module by name or index. For example info 1, use 1 or us
e auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf6 auxiliary(scanner/telnet/telnet_version) >
```


1 2 3 4
22:01
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
e auxiliary/scanner/telnet/telnet_version
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
Name Current Setting Required Description
PASSWORD no The password for the specified username
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 23 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 30 yes Timeout for the Telnet probe
USERNAME no The username to authenticate as
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > set LHOSTS 192.168.1.25
[-] Unknown datastore option: LHOSTS. Did you mean RHOSTS?
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET _ _ _ _ _ ____ \x0a _ __ ___ ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _|
|__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | __/ || (_| __ \ |_) | | (_) | | || (_| | |_) | | __//
__/ \x0a|_| |_| |_|___|____,_|___/ .__/|_|___/|_|____,_|__.__/|_|___|_____|\x0a |_| \x0a\x0a
\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametas
ploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >


1 2 3 4
22:03
Editor di Testo
Semplice editor di testo
kali_interna@kali: ~
Aiuto
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Thu Jun 8 16:59:51 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/