Ethical Hacking With Android: Termux

Author Vaibhav Mishra Prime

Ethical Hacking With Android; Termux

~ Author Vaibhav Mishra

Copyright Notice:-

Liability Disclaimer:-

The information provided in this eBook is to be used for educational purposes only. The eBook creator is in no way responsible for any misuse of the information provided. All of the information in this eBook is meant to help the reader develop a hacker defense attitude in order to prevent the attacks discussed. In no way should you use the information to cause any kind of damage directly or indirectly. The word “Hack” or “Hacking” in this eBook should be regarded as “Ethical Hack” or “Ethical hacking” respectively. You implement the information given at your own risk.

About The Author

My Name is Vaibhav Mishra. I have basic knowledge of Ethical Hacking and Cyber Security. This is my first book. This book is for educational purpose only.

For Any Quries call this number: +917524839483

Instagram: vaibhav_mishra_prime

Whatsapp No:- +917524839483

Chapter 01

Q: How to Start hacking with Android?
Ans: Download Termux From Play Store and and start Hacking with termux.

Q: What is termux?
Ans: Termux is a terminal emulator plus Linux environment, that allows us to use the Linux environment on our android within few clicks.
According to Wikipedia," Termux is an Android terminal emulator and linux environment application that works directly with no rooting or setup required. A minimal base system is installed automatically, additional packages are available using the APT package manager."

Q: What is the use of termux?
Ans: Termux is a linux terminal Emulator application for android. A terminal emulator is a program that allows the user to access the command line

interface in a graphical environment. If you have studied the basic of computer, you must know about the shell and command line interface.

Q: Does Termux Useful For Hacking?
Ans: My Answer Is Yes. You can use Termux for Hacking, you can use some popular Hacking Tools in Termux.

Q: Does Termux Requires Root Permissions?
Ans: Not at All, Root is Not Necessary To Use Termux, if - You Have Root then you can do some advanced stuff, if you don't have root then nothing to worry still you can do the same stuff.

Q: Can i Became a Hacker by Using Termux App?
Ans: Apps / Tools doesn't Made Hackers, Hackers Made Tools. Perhaps you won't Be a Hacker unless you have the knowledge.

Q: Is Termux Useful for Programmers?
Ans: Of Course It will be Helpful but limited.

Q: Can i use Termux To Hack Websites?
Ans: My Answer is Yes, You Can use Termux to Hack Websites with the help of sqlmap an other hacking tools.

Q: Can i Hack Facebook, Gmail, Instagram using Termux?
Ans: Yes You Can, Only If You Know Which Tool You Should use.

Termux Basic Commands

Install package: pkg install [package name]

Remove package: pkg uninstall [package name]

List all packages: pkg list-all

Upgrading packages: pkg upgrade

Date : Date commnad is used to display currnet date and time of your system.

cal : cal command is also known as calendar command it will display calendar

clear : clear command is used to clear the screen.

whoami : this command is used for display the name of current logged in user

ls : ls command is known as listing command it is used to display all the files and directory of current directory

cd : cd is known as change directory it is used to change the current director

pwd : pwd is used to display the path of current director

cat : cat is used to read a file, create a new file and more

mkdir : it is used to make a new directory

rmdir : it is used to remove a directory

ifconfig: (configuration of all network interface / some information about network

history: previous command

pkg install sl: check whether termux is properly installed

termux-setup-storage: Grant storage permission

cd storage: move forward in directories

mkdir folder name: create a folder or a directory

cp-r: Used to copy any directory [including hidden files]

cp -f: Force copy by removing the destination files if needed

File Commands

ls - List current directory

ls -i: Display Inode number of File or Directory

ls -R: Shows recursively list of Sub-Directories

ls -l: Shows file or directory,size,modified date and time, file or folder name and owner of file and it's permission

ls -lh: Shows sizes in human readable format

ls -al: Formatted listing with hidden files

cd dir: Changed directory to dir

pwd: Show current directory

mkdir dir: Create a dir on your current directory

rm dir: Delete the dir

rm -r file: Delete the file

rm -f file: Force remove file

rm *: Delete all file in your current directory

rm a*: Delete all starting with a file

rm bet*as: Delete starting with as and ending with bet files

cp fileA fileB: Copy fileA to fileB

cp -r dir1 dir2: Copy dir1 to dir2.If there isn't dir2 it create a dir2

mv dir1 dir2: Move dir1 to dir2

ls -s file link: Create sembolic link for file

touch file- Create a file or update file

cat>file- Write input to in file

more file- Get informatin abouth file

head file- Get first 10 line of file

less text- Return content of text

comm fileA fileB- Compare fileA with fileB

Search Commands

locate fileA: Index other files in the directory where the file is located

find / -name foo: Search with gived name of file

find /home -iname file.txt: Find name is file.txt files in home directory

find / -type d -name file: Find all file files

find . -type f -name *.php: Find all .php file in file

find . -type f -perm 0777 - print: Find all permission 777 files

find ~ -empty: Find all empty file

find / -atime 50: Find changed files in 50 days

find / -cmin -60: Find changed files in 1 hour

find / -mmin -60: Find modified files in 1 hour

find / -size +50M -size -100M: Find between 500M and 100M files

lsattr: Find unalterable files in system

find -perm -4000: Find has suid_bites file

Archive Commands

bzip filename: Compress of unzip the bzip file

tar cf file.tar file: Convert file to file.tar

tar xf file.tar: Unzip file.tar

tar czf file.tar.gz file: Convert file to file.tar.gz

tar xzf file.tar.gz: Unzip file.tar.gz

tar cjf file.tar.bz2: Create a file.tar.bz2 with Bzip2

tar xjf file.tar.bz2: Unzip file.tar.bz2

gzip file: Convert file to file.gzip

gzip -d file.gz: Unzip file.gz

FTP Commands

ftp: Enter ftp client

-p: Use passive mode

-i: Shutdown request on multi transfer.

-v: Verbose mode

-d: Active Debugging

$: Run makro

account[password]: Provides password with remote control

ascii: Setting ascii protocol the transfer file

binary: Support transfer of Images

bye: Out the FTP

dir: Show your current files

open Host: Open connect to host

status: Show status of server

Network Commands

arp: Control your network card and show your ip

ifconfig: Show network interface

ping host: Send ping to address of host

whois domain: Get information of domain

dig domain: Get dns information of domain

wget adress: Download the information of adress

wget -c adress: Continue the download

netstat: Look connect of network and open the sockets

Permission Commands

chmod +r file: Give read permission to file

chmod +w file: Give to write permission to file

chmod u+rw file: Give writer and read permission to file

chmod a-x file: Remove the permission of all user for file

chmod +x file: Give run permission to file

chattr +i file: It's make file to unalterable file

chmod a+r file: Give read permission to file for All user

System Commands

date: Show date

date;who: Show date and user

sudo command: Run command with root

sudo su: Change the mode on terminal

cal: Show calendar

uptime: Show time of your system

whoami: Show your login account

fingure userName: Show information of userName

cat /proc/cpuinfo: Show CPU information

cat /proc/meminfo: Show memory information

df: Show disk usage

free: Show memory and swap area

whereis application: Show directory of application

which application: Show default application

ps aux: Show running application on your system

kill application: Shutdown the application

sensors: Show temperature of CPU

uname -letter: -m Show your system hardware.

-n Write Nodename. Nodename has usage for network communication.
-r Show kernel's release
-s Write name of system
-v Write name of OS
-a Write all information of up

alias: Create a shortcut for

dd: Usage for content of disk

shutdown: shutdown the system

apropos: Search a word in man's pages

chfn: Change information of finger

chgrp: Change group

clear: Clear the terminal

continue: continue the commands

deluser userName: Delete the userName

delgroup group: Delete the group

groupadd group: Create a new group

halt: Stop the system

help: Get help

lsb_release -a: Show information of distribution
dmidecode:Get data of system(bios,memory,cache etc).

Exp demicode --type bios, demicode --type memory

free -m: Show quantity of memory

history: Show used terminal commands

passwd : Change the password of userName

usermod -L: Lock the userName account

usermod -U: Re-active the userName

chage -E date(12.02.2022): Used to specify the user account's password expiration time.

echo $SHELL: Used to view the shell program used on your system.

Git Commands

git config –global user.name "User name": Determines default userName for git

git config –global email "mail adress": Determines default mail for git

git log: Show all changes on local report

git status: Show changes on log file

git clone repoAdress: Copy the repo to current path

git clone userName@host:"/patch/repo ": Copy repo to your current file

git add fileName: Add your file to index

git add *: Add all file to index

git commit -m " commit " : Add commit to index file

git push origin master: Push your files to repo

git checkout -b branchName: Create new a branch

git checkout master: Return to master branch

git branch -d branch: Delete the branch

git push origin branch: Your changes push to your branch

git pull: Get last changes

git merge branchName: Merge branch other branch

Apt Commands

apt-get update: Update your packages

apt-get upgrade: upgrade your all package

apt-get dist-upgrade: Upgrade your Debian version to last version

apt-get install package_name: Install the package

apt-get install package1 package2 package3 package4 package5 package6 . . .: Install multipackage

sudo apt-get purge package_name: Remove package with dependency

apt-get remove packageName: Remove the package

apt-get autoremove: Remove old packages

apt-get -f install: It tries to repair faulty packages

dpkg -i package.deb: Install package.deb

sudo apt-cache show package_name: Give information of abouth package

apt-get help: Get information about help

Termux Hacking Tools

01: 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
Run :
$ bash shellphish.sh
> select your option
it will generates phishing url ..Now send this url to victem for phishing.....
Note : During all these process you have to open your hotspot.....

SocialFish

socialFish ultimate phishing tool such as Twitter, stackoverflow, wordpress, github, Google, facebook.....
Installation :
$ apt update
$ apt upgrade
$ apt install git
$ apt install python2
$ git clone https://github.com/UndeadSec/SocialFish.git
$ cd SocialFish
$ chmod +x *
$ pip2 install -r requirements.txt
usage :
$ python2 SocialFish.py
Now select your target and it will generate an url using Ngrok then it send to victim...
Note : During all these process you have to open your hotspot.....

BlackEye

The most complete Phishing Tool, with 32 templates +1 customizable
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 select your option it will generate an url for phishing...
Note : During all these process you have to open your hotspot.....

Weeman

Weeman is a phishing tool
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
Note : During all these process you have to open your hotspot.....

02: Information Gathering

Red Hawk Information Gathering

Red Hawk = All in one tool for Information Gathering and Vulnerability Scanning
Scans That You Can Perform Using RED HAWK Basic ScanWhois 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..
Insatallation :
$ apt update && apt upgrade
$ apt install git��
$ apt install php
$ git clone https://github.com/Tuhinshubhra/RED_HAWK
$ 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 informatio 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 helpfull 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.

Pureblood Framework

A Penetration Testing Framework created for Hackers / Pentester / Bug HunterWeb Pentest, Information Gathering, Banner Grab, Whois, Tracerouter, DNS Record, Reverse DNS Lookup, Zone Transfer Lookup, Port Scan, Admin Panel Scan, Subdomain Scan, CMS Identify, Reverse IP Lookup, Subnet Lookup, Extract Page Links, Directory Fuzz (NEW), File Fuzz (NEW), Shodan Search (NEW), Shodan Host Lookup (NEW), Web Application Attack: (NEW), Wordpress, Auto SQL Injection.
Generator: Deface Page, Password Generator, Text To Hash
Installation :

```
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/cr4shcod3/pureblood
$ cd pureblood
$ chmod +x *
```

$ pip install -r requirements.txt
Run :
$ python2 pureblood.py
Now select your option, this tool will guide you...

ReconDog Tool

Recon Dog is an all in one tool for all your basic information gathering needs.
It uses APIs to gather all the information so your identity is not exposed.
Installaion :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ git clone https://github.com/UltimateHackers/ReconDog
$ cd ReconDog
$ chmod +x *
usage :
python2 dog.py
Now select your option which you want..

Crips IP Tool

Crips IP Tools : This Tools is a collection of online IP Tools that can be used to quickly get information about IP Address's, Web Pages and DNS records.
Menu : Whois lookup, Traceroute, DNS Lookup, Reverse DNS Lookup, GeoIP Lookup, Port Scan, Reverse IP Lookup
Installation :

```
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/Manisso/Crips
$ cd Crips
$ chmod +x *
$ ./install.sh
```

Run :

```
$ python2 crips.py
```

Now select your option, this tool can guide you easily..

EvilUrl IDN Homograph

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.py
select oprion 2
here paste that url it detects if that url is unicode or for phishing.. that's it..

Lazymux Tool

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 Kali Linux Tool

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-
$ 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.

Angry Fuzzer

AngryFuzzer = Tools for information gathering
Discover hidden files and directories on a web server.
The application tries to find url relative paths of the given website by comparing them with a given set Features
Fuzz url set from an input file, Concurrent relative path search, Configurable number of fuzzing workers, Fuzz CMS ==> Wordpress,Durpal,Joomla, Generate reports of the valid paths
Installation :

```
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/ihebski/angryFuzzer
$ cd angryFuzzer
$ pip2 install -r requirements.txt
$ pip2 install requests
$ chmod +x *
```

Usage :
$ python2 angryFuzzer.py -h
It shows all options of this tool
$ python2 angryFuzzer.py -u http:site.com
Now it starts collecting target information...

The Choice

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..

User Recon

Find usernames across over 75 social networks This is useful if you are running an investigation to determine the usage of the same username on different social networks.
Installation :
$ apt update && apt upgrade
$ apt install git
$ git clone https://github.com/thelinuxchoice/userrecon
$ cd userrecon
$ chmod +X *
usage :
$ ./userrecon.sh
[?] Input username : (Here user name to find)

IPGEOLOCATION-TRACEIP

Retrieve IP Geolocation information
Features
Retrieve IP or Domain Geolocation,
Retrieve your own IP Geolocation,
Retrieve Geolocation for IPs or Domains loaded from file, Each target in new line.
Define your own custom User Agent string. Select random User-Agent strings from file. Each User Agent string in new line.
Proxy support.
Select random proxy from file. Each proxy URL in new line.
Open IP geolocation in Google Maps using the default browser.
Export results to csv, xml and txt format.
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.Timezone
12.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..

Infoga-Collect Email-Information

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 was 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 its started collecting emails

and e-mails information [hostname, city, organization, longitude and latitude ports..]

03: Vulnerability Analysis

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 Vul scanner

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

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 victem 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 Framework

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

Sqliscan

Sqliscan by dork :
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install curl
$ git clone https://github.com/thelinuxchoice/sqliscan
$ cd sqliscan
$ chmod +x *
usage :
$ ./sqliscan.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 rotersploit
rsf> use "module name"
it shows how you can use that module....

Creadmap- Cheak Login Emails

Credmap is an open source tool that was created to bring awareness to the dangers of credential reuse. It is capable of testing supplied user credentials on several known websites to test if the password has been reused on any of these.
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/lightos/credmap
$ cd credmap
$ chmod +x *
usage :
$ python2 credmap.py -h
It shows all options to use this tool
$ python2 credmap.py --username king –email king56@email.com
king = is username of email
king56@email.com = this is email to check

Nikto Web Server Scanner

Nikto web server scanner and a web server assessment tool. It is designed to find various default and insecure files, configurations and programs on any type of web server Installation:

```
$ apt update && apt upgrade
$ apt install git
$ apt install perl
$ git clone https://github.com/sullo/nikto
$ cd nikto
$ chmod +x *
```

usage :

```
perl nikto.pl -H
```

it shows all options how you can use this tool

04: Exploitation Tools

Cmseek suit

CMS Detection and Exploitation suite - Scan WordPress, Joomla, Drupal and 100 other CMSs
Functions Of CMSeek :
Basic CMS Detection of over 80 CMS
Drupal version detection
Advanced Wordpress Scans
Detects Version
User Enumeration
Plugins Enumeration
Theme Enumeration
Detects Users (3 Detection Methods)
Looks for Version Vulnerabilities and much more!
Advanced Joomla Scans
Version detection
Backup files finder
Admin page finder
Core vulnerability detection
Directory listing check
Config leak detection

Various other checks
Modular bruteforce system
Use pre made bruteforce modules or create your own and integrate with it
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/Tuhinshubhra/CMSeeK
$ cd CMSeeK
$ chmod +x *
Run :
$ python cmseek.py
here select your oprion and use..

Zarp-Local Network Tool

zarp works in rooted mobiles. This is local network exploit tool. Execute these commands one by one to install sudo. first you must install sudo in termux
Installation :
$ apt update
$ apt upgrade
$ apt install git
apt install python2
$ git clone https://github.com/hatRiot/zarp
$ cd zarp
chmod +x zarp.py
Run :
sudo python2 zarp.py

Tm- Venom

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 helpfull 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
```

Metasploit Framework

If you wish to install the metasploit-framework all by itself
You can use a shell script to install it.
remember dont 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....

A-Rat Exploit

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 privious 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 (Dos Tool)

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 (Dos Tool)

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

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.

05: Notcatagorized

Darkfly Tool

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 :) Good
Installation :
$ 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

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

Apache2 HTTP Server

first update and update Termux .
$ apt update
$ apt upgrade
Now install apache2
$ apt install apache2
apache2 path =/data/data/com.termux/files/usr/share/apache2/default-site/htdocs/
for Example i have a file read.txt now you must move this file to apache2 path then type this command :
$ mv read.txt /data/data/com.termux/files/usr/share/apache2/default-site/htdocs/
Now start apache2 service with this command :
$ apachectl
Now opn browser and type :
localhost:8080
It shows IT WORKS !
Now access read.txt file with browser then type this command:
localhost:8080/read.txt

If you want to stop apache2 service then close termux application it will stop. That's it.

Hash Cracker

Hash cracker with auto detect hash in termux.
Hasher is a hash cracker tool that has supported more than 7 types of hashes.
support :
md4
md5
sha1
sha224
sha256
sha384
sha512
ripemd160
whirlpool
Execute these commands one by one to install.
Installation :

```
$ apt update
$ apt upgrade
$ apt install git
$ apt install python
$ apt install python2
$ git clone https://github.com/ciku370/hasher
```

cd hasher
Run :
python2 hash.py
simply paste hashes. {hit enter}
it ask the type of hash . then select your type of hash to Decrypt it.

Sudo Superuser

Sudo works on only rooted devices. sudo means superuser & root command. we can run root tools in termux using sudo. Execute these commands one by one to install sudo.
Installation :

```
 $ apt update
$ apt upgrade
$ apt install git
$ apt install tsu
$ apt install ncurses-utils
$ git clone https://github.com/termux-sudo
$ cd termux-sudo
$ cat sudo > /data/data/com.termux/files/usr/bin/sudo
$ chmod 700 /data/data/com.termux/files/usr/bin/sudo
sudo su
sudo tsu
```

Now you are a root user....

Wordlist Generate

Generateing wordlist using python.
Execute these commands one by one to install sudo.
Installation :
$ apt update
$ apt upgrade
$ apt install python
$ pip install wordlist
$ wordlist -h [to see all options]
$ wordlist -m 4 -M 6 -o wordlist.txt
12345678
-m = minimum length
-M = maximum length
wordlist.txt = to save all words
12345678 = here you can type alphabets also to make wordlist.
type this command : $ ls
here you get that file
name : wordlist.txt
now open this file type this command :
 $ cat wordlist.txt
here you get all words means passwords list

Speak Engine

with this script you guys can perform termux as speak engine
first you need to install these apps
1] Termux App
2] Termux API App
Now open Termux and follow these steps to install speak-Engine
installation :
$ apt update
$ apt upgrade
$ apt install git
$ apt install python2
$ git clone https://github.com/TechnicalMujeeb/Termux-speak
$ cd Termux-speak
$ chmod +x *
$ sh install.sh
usage :
python2 t-speak.py
select option 2
Enter Your Text to speak.
Enter pitch number
Enter rate number
Then it will speak that texts..

Gloom Framework

Gloom-Framework = Linux Penetration Testing Framework
Execute these commands one by one to install this tool.
works in rooted devices
Remember you have must installed sudo in Termux
after installation of sudo follow these steps
Installation :

```
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ apt install nmap
$ apt install tsu
$ git clone https://github.com/StreetSec/Gloom-Framework.git
$ cd Gloom-Framework
$ chmod +x *
$ sudo python2 install.py
$ sudo python2 gloom.py
$ pip2 install requests
```

if you get error for bs4 & beautifulsoup
then simply type
$ sudo pip2 install bs4
$ sudo pip2 install beautifulsoup
Run :
$ sudo python2 gloom.py
[gloom] help
it shows all modules to use any module
simply copy and paste that module name

Brutespray

BruteSpray takes nmap GNMAP/XML output and automatically brute-forces services with default credentials using Medusa.
BruteSpray can even find non-standard ports by using the -sV inside Nmap.
Installation :
$ apt update
$ apt upgrade
$ apt install gi
$ apt install python2
$ git clone https://github.com/x90skysn3k/brutespray
$ cd brutespray
$ pip2 install -r requirements.txt
usage :
$ python2 brutespray.py
First do an nmap scan with -oG nmap.gnmap or -oX nmap.xml.
$ python2 brutespray.py -h
$ python brutespray.py --file nmap.gnmap
$ python brutesrpay.py --file nmap.xml
$ python brutespray.py --file nmap.xml -i

Sublister (superdomain)

Sublist3r = Fast subdomains enumeration tool for penetration testers.It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting.
Installation :
$ apt update
$ apt upgrade
$ apt install git
$ apt install python2
$ git clone https://github.com/aboul3la/Sublist3r
$ cd Sublist3r
$ pip2 install requirements.txt
$ pip2 install requests
Run :
$ python2 sublist3r.py
$ python2 sublist3r.py -h
it shows all options how you can use this tool
$ python2 sublist3r.py -d site.com
-d = domain name

Download any Types Of Files

with the help of termux app we can download any type of files
such as..
apk, .jpg, .png, .txt, .mp3, .mp4, .md, .zip, .rar, .doc, .psd, .cdr, .eps, .anything...etc....
first you need to install these apps from playstore
1] Termux App
2] Termux API App
Now open Termux and follow these steps installation :
$ apt update
$ apt upgrade
$ apt install termux-api
[Downloading process:]
$ termux-download -d -t http://downlodingurl.com/file.apk
after -t you need to give downloading url to download any type of file after downloading goto your download folder

Termux send sms

send sms using termux app first you need to install these apps from playstore
1] Termux App
2] Termux API App
Now open Termux and follow these steps
installation :
$ apt update
$ apt upgrade
$ apt install termux-api
message sending process :
$ termux-sms-send -n 9999999999 text
9999999999 = Receiver number
text = your message here

Termux Make Call

first you need to install these apps from playstore
1] Termux App
2] Termux API App
Now open Termux and follow these steps
installation :
$ apt update
$ apt upgrade
$ apt install termux-api
call process :
$ termux-telephony-call 9999999999
9999999999 = number of victim

Termux 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 *
./kalinethunter
Now 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

Download Fb Videos

Facebook Video Downloader (CLI) For Linux Systems Coded in PHP with the help of this script you guys can download facebook videos by pasteing video url in termux.

Installation :

$ apt update && apt upgrade

$ apt install git

$ apt install php

$ git clone https://github.com/Tuhinshubhra/fbvid

$ cd fbvid

Run :

$ php fb.php

first here paste fb video url

Now here give a name to your video, it will start downloading your video and saved in current directory.

If you want to watch your downloaded video then move this video to sdacrd using mv command

$ mv video.mp4 /sdcard/

Now your video has moved to sdcrad, go to your sdcard and watch it ....

Matrix Effect

make matrix effect in termux ..hacker look in termux
Installation :
$ apt update && apt upgrade
$ apt install cmatrix
usage :
Type cmatrix to start matrix effect
$ cmatrix

Spammer Grab(sms Bomb)

Spams GAC (Grab Activation Code) SMS to a phone number repeatedly per 60 second.
"Spammer" uses Grab passenger API to make the GAC sms sent.
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/Noxturnix/Spammer-Grab
$ cd Spammer-Grab
$ chmod +x *
$ ./auto-install.sh
Run :
python2 spammer.py -h
It shows all the options of this tool for use..
use :
$ python2 spammer.py –delay 10 [Your number here]
Now it will start bombing on your given number.

Choicebot (instagram bot)

Choicebot is a bot written in Shell Script (the first one) to perform 'likes', 'comments' and 'follows' based on hastags.
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install curl
$ apt install nano
$ git clone https://github.com/thelinuxchoice/choicebot
$ cd choicebot
$ chmod +x *
usage :
$ nano hashtags.txt (put your hashtags here)
$ ./choicebot.sh

Create Zip Files

Fisrt update and install requirments ..
$ apt update
$ apt upgrade
$ apt install zip
$ apt install unzip
Creating Zip file :
$ zip name.zip [your files]
Here name.zip is the name for that zip file
your files means = your files to make zip such as .txt .md folder .png .jpg etc..,
Unzip process :
$ unzip name.zip
that's it it will unzip your zip file..

Create Zip Files

Fisrt update and install requirments ..
$ apt update
$ apt upgrade
$ apt install zip
$ apt install unzip
Creating Zip file :
$ zip name.zip [your files]
Here name.zip is the name for that zip file
your files means = your files to make zip such as .txt .md folder .png .jpg etc..,
Unzip process :
$ unzip name.zip
that's it it will unzip your zip file..

Goblin word Generator

Goblin word Generator tool is used to generate password list easily..
Installtion :
$ apt update
$ apt upgrade
$ apt install git
$ apt install python
$ apt install python2
$ git clone https://github.com/UndeadSec/GoblinWordGenerator
cd GoblinWordGenerator
$ chmod +x *
usage :
$ python3 goblin.py
i want to generate list that length 4 to 6 then type here : 4:6 {hit enter}
Give name to your wordlist like, : pass.txt {hit enter}
and select option which you want and {hit enter}
it will generate a pass.txt
to open this file type this command :
$ cat pass.txt

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.

Xerxes (Dos Tool)

XERXES the most powerful DoS tool
Installation:
$ apt update && apt upgrade
$ apt install git
$ apt install clang
$ git clone https://github.com/zanyarjamal/xerxes
$ cd xerxes
$ chmod +x *
usage :
$ clang xerxes.c -o xerxes
$ ./xerxes www.fakesite.com 80

Hunner Framework

Hunner Hacking framework = This framework is designed to perform penetration testing.
Its functions:
1.Scan sql vulnerability
2.Scan xxs vulnerability
3.Dos sites
4.Brutforce Ftp
5.Brutforse SSh
6.Brutforse mail Accounts
Installaion :
$ apt update && apt upgrade
$ apt install git
$ apt install python
$ git clone https://github.com/b3-v3r/Hunner
$ cd Hunner
$ chmod 777 hunner.py
usage :
$ python hunner.py
Now select your options to use..

Weevely Backdoor Webshell

Weevely is a stealth PHP web shell. itsimulate telnet like connections, it is an essential Tool for Web Applications post exploitation. itcan be used as stealth backdoor OR as a web shell
Installation
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ git clone https://github.com/glides/Weevely
$ cd Weevely
$ chmod +x *
usage :
$ python2 weevely.py
It shows all options how you can use this.
shell generateing process:
$ python2 weevely.py generate 123456 /$HOME/shell.php
123456 = is the password for shell
shell.php = name for the shell
it generate a shell in termux home directory

Wps scan WordPress scan

wpscan is a WordPress vulnerability scanner tool for legal Or security purpose to find the vulnerabilities and fix it.
Remember wpscan tool is only works in arm/arm64 device If you want to check your phone architecture
Type this command :-
$ dpkg-print-architecture
Or
$ uname -m
Installation of wpsacn :
$ apt install git
$ apt install ruby
$ git clone https://github.com/wpscanteam/wpscan
$ cd wpscan
$ chmod 777 wpscan.rb
install some gems one by one
$ gem install bundle
$ bundle install -j5
Run :
$ ruby wpscan.rb
$ ruby wpscan.rb< –url [wordpress url

Hashcode-Encode and Decode Text

Hashcode = Its purpose is to encode your desired hash text.
Encode & Decode as follows:
1. md5 [encode]
2. sha1 [encode]
3. sha224 [encode]
4. sha256 [encode]
5. sha384 [encode]
6. sha512 [encode]
7. base64 [encode/decode]
8. binary [encode/decode]
9. hexa decimal [encode/decode]
10. cipher of cesar [encode/decode]
11. reverse text
12. reverse words

Installation :

```
$ apt install git
$ apt install python
$ apt install python2
$ git clone https://github.com/Sup3r-Us3r/HashCode
$ cd HashCode
$ chmod +x *
```

Run :
$ python3 hashcode-en.py
Now select your option and enter your data it will encode/decode your data

Cyberscan

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.

Knockpy (Subdomain)

Knockpy is a python tool designed to enumerate subdomains on a target domain through a wordlist. It is designed to scan for DNS zone transfer and to try to bypass the wildcard DNS record automatically if it is enabled. Now knockpy supports queries to VirusTotal subdomains,
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ pip2 install dnspython
$ git clone https://github.com/guelfoweb/knock.git
$ cd knock $ python2 setup.py install
usage :
$ knockpy -h
it shows how you can use this tool
$ knockpy domain.com

A2SV- SSL VUL-Scan

A2SV = Auto Scanning to SSL Vulnerability
HeartBleed, CCS Injection, SSLv3 POODLE, FREAK... etc
Support Vulnerability
[CVE-2007-1858] Anonymous Cipher
[CVE-2012-4929] CRIME(SPDY)
[CVE-2014-0160] CCS Injection
[CVE-2014-0224] HeartBleed
[CVE-2014-3566] SSLv3 POODLE
[CVE-2015-0204] FREAK Attack
[CVE-2015-4000] LOGJAM Attack
[CVE-2016-0800] SSLv2 DROWN
Installation :

```
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/hahwul/a2sv
$ cd a2sv
$ chmod +x *
$ pip2 install -r requirements.txt
```

usage :
$ python2 a2sv.py -h
It shows all commands how we can use this tool
$ python a2sv.py -t 127.0.0.1
127.0.0.1 = target means here own device

Mapscii

$ apt update && apt upgrade
To display world map in termux terminal
Type this command :
$ telnet mapscii.me
press a = zoomin
press z = zoom out
press c = to quite
use arrow keys to goto left right up down

Optiva Framework

Optiva-Framework = Web Application Scanner
Features :
1.Infromation Modules
2.Hash Modules
3.Scanner Modules
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/joker25000/Optiva-Framework
$ cd Optiva-Framework
$ chmod +X *
$ bash installer.sh
select option 3 termux and press enter
usage :
$ python2 optiva.py
[optiva]$> help
to show all options of this tool
[optiva]$> info

to get some basic information
[optiva]$> show modules
it shows all modules of optiva framework
To use any module simply type module name, it will guide yo how you can use this tool.

Breacher

An advanced multithreaded admin panel finder written in pythonA script to find admin login pages and EAR vulnerabilites.

Features

1.Multi-threading on demand
2.Big path list (482 paths)
3.Supports php, asp and html extensions
4.Checks for potential EAR vulnerabilites
5.Checks for robots.txt
6.Support for custom patns

Installation :

```
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/s0md3v/Breacher
 $ cd Breacher
```

Run :

```
$ python2 breacher.py
```

Check all paths without threads

```
$ python2 breacher -u example.com
```

Dost-Webserver-Tool

Dost = WebServer Attacking Tools
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/verluchie/dost-attack
$ cd dost-attack
$ chmod 777 install.sh
$ ./install.sh
Run :
$ ./dost
It shows how you can use this tool

Striker

striker = Striker is an offensive information and vulnerability scanner
Features :
1.Check and Bypass Cloudflare
2.Retrieve Server and Powered by Headers
3.Fingerprint the operating system of Web Server
4.Detect CMS (197+ CMSs are supported)
5.Launch WPScan if target is using Wordpress
6.Retrieve robots.txt
7.Whois lookup
8.Check if the target is a honeypot
9.Port Scan with banner grabbing
10.Dumps all kind of DNS records
11.Generate a map for visualizing the attack surface
12.Gather Emails related to the target
13.Find websites hosted on the same web server
14.Find hosts using google

15.Crawl the website for URLs having parameters
16.SQLi scan using online implemention of SQLMap (takes < 3 min.)
17.Basic XSS scanning
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/s0md3v/Striker
$ cd Striker
$ pip2 install -r requirements.txt
Run :
$ python2 striker.py
it shows how you can use this tool

Harvester-email-info

E-mails, subdomains and names Harvester
theHarvester is a tool for gathering subdomain names, e-mail addresses, virtual hosts, open ports/ banners, and employee names from different public sources (search engines, pgp key servers).
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ git clone https://github.com/laramies/theHarvester
$ cd theHarvester
$ chmod +x *
usage :
$ python2 theHarvester.py
$ python2 theHarvester.py -d site.com -b google

Termux Wafwoof

WAFW00f is the inbuilt tool in Kali distribution or else you can install it manually.we can install this tool in termux also
It can detect around Top 22 web application firewall, so wafw00f is a phase of information gathering initially.
follow these steps :
Installation :
$ apt update && apt upgrade
$ apt install python2
$ apt install python
$ pip install wafw00f
usage :
$ wafw00f -h
It shows all options of wafw00f tool how you can use this tool
$ wafw00f [url]

Termux speedtest cli

sppedtest-cli this is used to find your download and upload speed of your internet connection.

Installation :

```
$ apt update && apt upgrade
$ apt install python2
$ apt install python
$ pip install requests
$ pip install speedtest-cli
```

usage :

```
$ speedtest -h
```

it shows all options

```
$ speedtest
```

Now it shows your internet's Download & upload speed.

Heartbleed Scanner

The heart bleed bug is a serious vulnerability in the popular Openssl port number 443. this weakness allows stealing the information protected,under normal conditiond by the SSL/Tls encryption used to secure the internet.
Installation :
$ apt update && apt upgrade
$ apt install git
$ git clone https://github.com/TechnicalMujeeb/HeartBleed.git
$ cd HeartBleed
$ chmod +x *
$ ./install.sh
=> usage
run another script
$ ./hbleed
here enter you site to check bug is present or not if present
then you can update your services and stay secure.

Smb Scanner

(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
```

Lazyfiglet

LazyFiglet is a bash script created By Technical Mujeeb. with the help of this tool we can display all fonts of figlet in one click. one click means it ask your name when you enter your name then this script starts Generating figlet fonts one by one
.In this script total 181+ figlet fonts are present and this is very easy to use.
[+] Requirments : here another file install.sh is also available. so you can simply run this install.sh to install all requirments packages which helps you to display figlet fonts.
Installation :
$ apt update && apt upgrade
$ apt install git
$ git clone https://github.com/TechnicalMujeeb/LazyFiglet
$ cd LazyFiglet
$ chmod +x *
$ sh install.sh
(This command install all requirements packages.)

usage :
$ sh lfiglet
[+] Enter you name : you text here
(Then this script starts generating 181+ figlet fonts on you terminal)
DOne !

Password Generator

Password-GeneratorPassGen = is a tool which generates a custom passwords with 20+ char ,easy to remember and cannot be bruteforced [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.

Sqlmap

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

Santet online

santet-online
Features :
1.netcat payload
2.fb group hijacking
3.sms-bomber
4.sms-spoof
5.dos attack
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ pip2 install requests
$ git clone https://github.com/Gameye98/santet-online
$ santet-online
$ chmod +x *
usage :
$ python2 santet.py
Now it shows all tool simply type number to use that tool

Autopixie wps

Autopixie-WPS = this script is meant for people who wants to check if someone can gain the wpa key, and or if you are protected from this attack Any illegal use of this program is strictly forbidden!.

FEATURES

Kill reaver as soon as e-hash2 is gained.
Manual input target router without scan
Wash scan > target router from scan list
Save resuslts to logfile
option to ignore router from wash scan if it has been cracked,
or if PixieWps failed to crack the hash
remember you must have an ecternal wifi adpter

Installation :

$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python

$ pip2 install requests
$ git clone https://github.com/nxxxu/AutoPixieWps
$ cd AutoPixieWps
$ chmod +x *
Run :
$ python2 autopixie.py
Now select any option it will guide you..

Visql (Sqli-vuln-scanner)

viSQL = Scan SQL vulnerability on target site and sites of on server.
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ pip2 install requests
$ git clone https://github.com/blackvkng/viSQL.git
$ cd viSQL
$ pip2 install -r requirements.txt
Run :
$ python2 viSQL.py --help
it shows options to use. very easy to use..

Visql (Sqli-vuln-scanner)

viSQL = Scan SQL vulnerability on target site and sites of on server.
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install python2
$ apt install python
$ pip2 install requests
$ git clone https://github.com/blackvkng/viSQL.git
$ cd viSQL
$ pip2 install -r requirements.txt
Run :
$ python2 viSQL.py --help
it shows options to use. very easy to use..

Termux Ubantu

termux-ubuntu = A script to install Ubuntu chroot in Termux
Installation :
$ apt update && apt upgrade
$ apt install git
$ apt install proot
$ apt install wget
$ git clone https://github.com/Neo-Oli/termux-ubuntu
$ cd termux-ubuntu
$ ls
$ chmod +x *
$ sh ubuntu.sh
Run :
After running it you can run "start-ubuntu.sh" to switch into your ubuntu
$ ./start.sh
Now you are in Ubuntu terminal..

Knockmail

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..

Knockmail

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..

Hakku Framework

Hakku framework offers simple structure, basic CLI, and useful features for penetration testing tools developing
Modules
apache_users
arp_dos
arp_monitor
arp_spoof
bluetooth_pod
cloudflare_resolver
dhcp_dos
dir_scanner
dns_spoof
email_bomber
hostname_resolver
mac_spoof
mitm
network_kill
pma_scanner
port_scanner
proxy_scout
whois
web_killer
web_scout

wifi_jammer
zip_cracker
rar_cracker
wordlist_gen
Installation :
$ apt update && apt upgrade
$ apt install python
$ git clone https://github.com/4shadoww/hakkuframework
$ cd hakkuframework
$ chmod +x *
Usage :
$ python hakku
$ show modules
to show all modules of hakku framework
to use any module simply type
$ use module name
$ show options
to show all options of that particular modules..

Termux Vibrate Mobile

first you need to install these apps from playstore
1] Termux App
2] Termux API App
Now open Termux and follow these steps
Installation :
$ apt update && apt upgrade
$ apt install termux-api
usage :
Type this command to vibrate your device
$ termux-vibrate -d 1500 -f
-d = duration
1500 = you can give any value to vibrate like 4090,etc...,

Install Jarvis Tool

```
$ apt update && apt upgrade
$ apt install git -y
$ pkg install mpv -y
$ git clone https://github.com/
AmshenShanu07/jarvis-welcome.git
$ cd jarvis-welcome chmod +x *
$ sh install.sh
```

Email Bombing

```
$ apt install python2
$ ls
$ git clone https://github.com/
zanyarjamal/Email-bomber.git
$ cd Email-bomber
$ ls
$ chmod +x * E-bomber.py
$ python2 E-bomber.py
```

Facebook ID Auto Report

$ apt update && apt upgrade
$ pkg install python2
$ pkg install git
$ pkg install unzip
$ pkg install tor
$ pkg install mechanize
$ git clone https://github.com/llayTamvan/Report.git
$ cd Report
$ unzip Report.zip
$ python2 Report.py
If this is now working then try this
open new session
$ git clone https://github.com/uhusmanhaider/facebook-report
$ cd facebook-report
$ ls
$ unzip Report.zip
$ python2 Report.py
Enter binary code of Facebook account.....

H4CK-FB-NEWS

FEATURES:
Facebook friend info fetcher
Get ID from friend
Get ID friend from friend
Get group member ID
Get email friend
Get email friend from friend
Get a friend's phone number
Get a friend's phone number from friend
Mini Hack Facebook(Target)
Multi Bruteforce Facebook
Super Multi Bruteforce Facebook
BruteForce(Target)
Yahoo Checker
Bot Reactions Target Post
Bot Reactions group Post
BOT COMMENT Target Post
BOT COMMENT group Post
Mass delete Post
Mass accept friends
Mass delete friend
ACreate Post
Create Wordlist
Account Checker

See my group list
Profile Guard
INSTALLATION
$ apt update && apt upgrade
$ pkg install python2
$ git clone https://github.com/ProjectorBUg/H4CK-FB-NEWS.git
$ cd H4CK-FB-NEWS
USAGE
$ sudo python2 tebas.py
or
$ python2 tebas.py

DDos

$ apt update && apt upgrade
$ pkg install python2
$ pkg install git
$ pkg install unzip
$ pkg install tor
$ pkg install mechanize
$ git clone https://github.com/Ha3MrX/DDos-Attack
$ ls
$ cd DDos-Attack
$ ls
$ chmod +x *
$ python2 ddos-attack.py
Now type target website ip address.
To find target website ip address open new session and type.....
ping www.yoursite.com
Then copy website ip and reopen old session and paste ip address of website.
and then
Lport- 4444
attack satrted.....

Theme & Colour

$ apt update && apt upgrade
$ pkg install python2
$ pkg install git
$ pkg install unzip
$ pkg install tor
$ pkg install mechanize
$ git clone https://github.com/saydog/termux-theme
$ cd termux-theme
$ chmod +x install.sh
$./install.sh
Run:-
$ python theme.py

Instagram Info Tool

```
$ apt update && apt upgrade
$ pkg install python2
$ pkg install git
$ pkg install unzip
$ pkg install tor
$ pkg install mechanize
$ git clone https://github.com/thelinuxchoice/instashell
$ cd instashell
$ ./instashell.sh
```

Spam Call

```
$ apt update && apt upgrade
$ pkg install python2
$ pkg install git
$ pkg install unzip
$ pkg install tor
$ pkg install mechanize
$ git clone https://github.com/Aditya021/spamCall
$ cd SpamCall
$ ls
$ php SpamCall.php
```

OSI.ig

```
$ pkg install -y git
$ git clone https://github.com/th3unkn0n/osi.ig.git && cd osi.ig
$ chmod +x install.sh && ./install.sh
```

• Usage

```
$ python3 main.py -u username
$ python3 main.py -h
usage: main.py [-h] -u USERNAME [-p] [-s] [-t]
optional arguments:
-h, --help show this help message and exit
-u USERNAME, --username USERNAME
username of account to scan
-p, --post get all uploaded images info
-s, --savedata save data to file ( save profile pic, info , post info )
-t, --tags list
```

Tstyle

```
$ apt update
$ apt install git -y
$ git clone https://github.com/htr-tech/tstyle
$ cd tstyle
$ bash setup.sh
```

Termux-shell

```
$ apt update
$ apt install git -y
$ git clone https://github.com/htr-tech/termux-shell.git
$ cd termux-shell
$ chmod +x *
$ sh install.sh
```

Termux-Login

```
$ apt update
$ apt install git -y
$ git clone https://github.com/htr-tech/termux-login.git
$ cd termux-login
$ chmod +x *
$ sh install.sh
```

Jarvis-Welcome

```
$ apt update
$ apt install git -y
$ pkg install mpv -y
$ git clone  https://github.com/AmshenShanu07/jarvis-welcome.git
$ cd jarvis-welcome
$ chmod +x *
$ sh install.sh
```