Hacking with android :

Roadmap@dc0471:

A_little_about_me >> How_it_all_began >> root@myphone >> kill lockscreen

>> toolbox >> Setting_up_the_device >> install Termux >> Install nmap >>

Install metasploit >> ./Demo.sh

echo "A little about me :)"

- Associate Security Engineer
- Web and android pentesting
- Hunt Bugs
- Basketball and travel

How_it_all_began

- First commercial Android device launched in September 2008.
- A modified version of the Linux kernel
- It is free and open source software
- Continuously evolving

root@myphone:

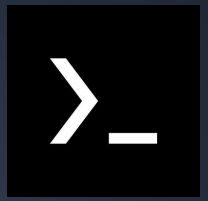
- First root
- Xda
- SuperSu + adb sideload
- Custom recovery

kill lockscreen;

- /data/system/
- Locate *.key file
- Remove the file
- Rename the file

```
vbox86p:/ # cd /data/system/
vbox86p:/data/system # ls
appops.xml                framework_atlas.config  install_sessions     locksettings.db-shm notification_log.db         screen_on_time       users
batterystats-daily.xml    gatekeeper.password.key install_sessions.xml locksettings.db-wal notification_log.db-journal sensor_service
batterystats.bin          gatekeeper.pattern.key  job                  log-files.xml       notification_policy.xml     shortcut_service.xml
device_policies.xml       heapdump                last-fstrim          ndebugsocket        packages.list               sync
dropbox                   ifw                     last-header.txt      netpolicy.xml       packages.xml                uiderrors.txt
entropy.dat               inputmethod             locksettings.db      netstats            procstats                   usagestats
```

cat toolbox;



- Termux
- Nethunter

  https://www.kali.org/docs/nethunter/nethunter-rootless/

- Xposed installer
- Zanti

  https://www.zimperium.com/zanti-mobile-penetration-testing

- HttpCanary

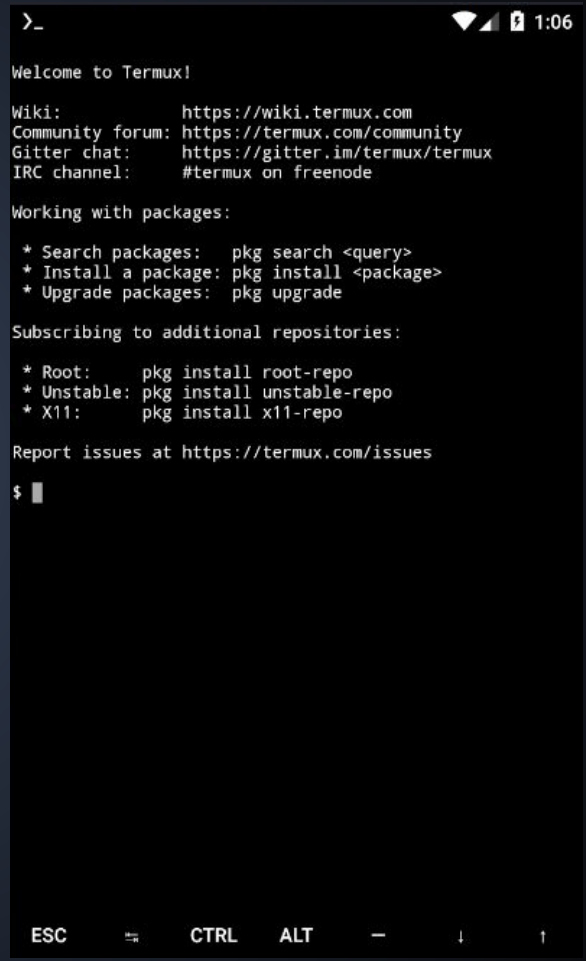
  https://httpcanary.com/en/

Setting_up_the_device 🛠️

- Termux
- Nmap
- Metasploit
- Kioptrix level one: https://www.vulnhub.com/entry/kioptrix-level-1-1,22/

Install Termux;

- https://wiki.termux.com/wiki/Main_Page
- https://wiki.termux.com/wiki/Hacking
- pkg upgrade
- pkg list-all
- pkg install [package name]
- pkg uninstall [package name]



nmap

- https://nmap.org/
- A free and open-source network scanner
- Used to discover hosts and services on a computer network

Install nmap;

- pkg upgrade
- pkg install nmap
- nmap --version

```
$ pkg install nmap
Checking availability of current mirror: ok
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  liblua53 libpcap netcat resolv-conf
The following NEW packages will be installed:
  liblua53 libpcap netcat nmap resolv-conf
0 upgraded, 5 newly installed, 0 to remove and 0 not upg
raded.
Need to get 4873 kB of archives.
After this operation, 26.9 MB of additional disk space w
ill be used.
Do you want to continue? [Y/n]
```

```
$ nmap --version
Nmap version 7.91 ( https://nmap.org )
Platform: i686-pc-linux-android
Compiled with: liblua-5.3.5 openssl-1.1.1h libssh2-1.9.0
 libz-1.2.11 libpcre-8.44 libpcap-1.9.1 nmap-libdnet-1.1
2 ipv6
Compiled without:
Available nsock engines: epoll poll select
$
```

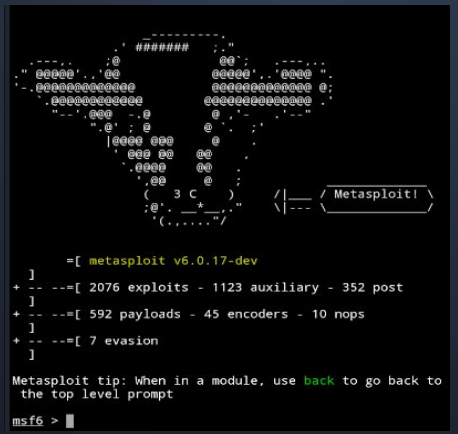
metasploit

- A tool for developing and executing exploit code against a remote target machine
- Contains several modules
- https://www.offensive-security.com/metasploit-unleashed/
- https://tryhackme.com/room/rpmetasploit

Install metasploit;

- pkg install unstable-repo
- pkg install metasploit
- msfd
- msfconsole

```
$ pkg install metasploit
Checking availability of current mirror: ok
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apr apr-util autoconf binutils bison clang gdbm git
  glib libandroid-shmem libexpat libffi libicu libllvm
  libltdl libsqlite libtool libuuid libxml2 libxslt
  libyaml m4 make ncurses-utils ndk-sysroot pcre2 perl
  pkg-config postgresql ruby termux-elf-cleaner wget
  zip
The following NEW packages will be installed:
  apr apr-util autoconf binutils bison clang gdbm git
  glib libandroid-shmem libexpat libffi libicu libllvm
  libltdl libsqlite libtool libuuid libxml2 libxslt
  libyaml m4 make metasploit ncurses-utils ndk-sysroot
  pcre2 perl pkg-config postgresql ruby
  termux-elf-cleaner wget zip
0 upgraded, 34 newly installed, 0 to remove and 0 not up
graded.
Need to get 89.6 MB of archives.
After this operation, 440 MB of additional disk space wi
ll be used.
Do you want to continue? [Y/n]
```



./Demo.sh

Q & A

https://dc0471.org/discord

Thank_you;