Hacking

From Termux Wiki

Jump to: navigation, search

Termux is capable of performing penetration testing. We provide a number of utilities for that and you also can build and install your own.

Disclaimer

Termux developers do not provide any assistance with hacking and related activity including the configuration and usage of related utilities. No matter whether you have permission to do so or not, whether you are doing so for education, pranking, etc.

If you are interested in hacking, it's expected that you are experienced user. We are not helping script kiddies.

Phishing, carding and other activity strongly tied with fraud and such that cannot be treated as anything other than crime is strongly discouraged. Such activity is not ethical hacking or pentesting and there no place for it in our community.

FAQ

How do I install utility X?

If you are asking this, then you should start with basics. Learn OS basics, shell scripting, some programming language, finally the README files of your "utility" sources and this question will just disappear.

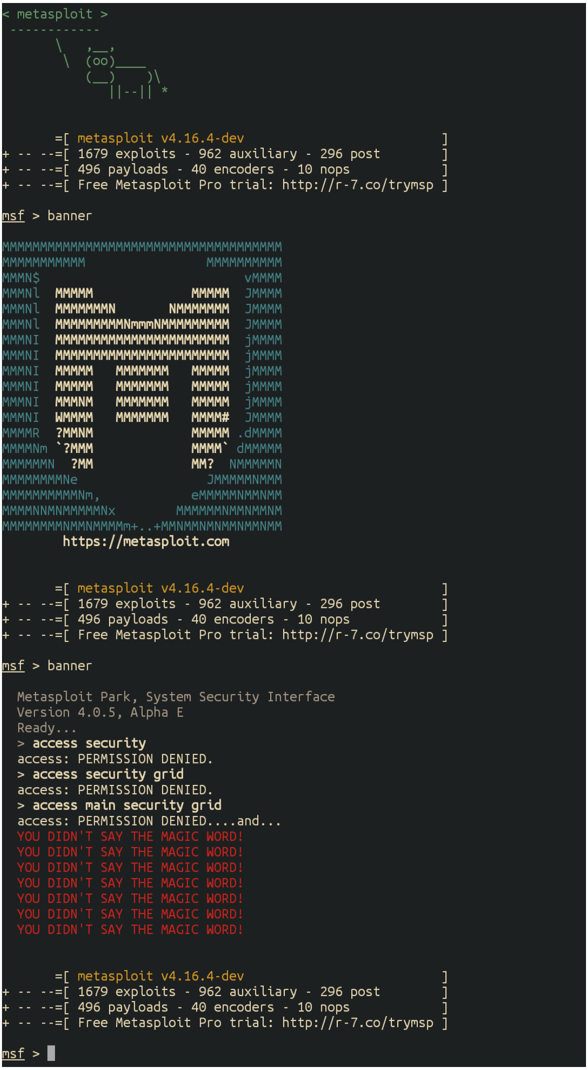
I got an error in utility X, what should I do?

What you should really do is to read the error message and understand its origin. In most cases that will give you a solution.

Can I root my device with Termux?

Yes, you can if your device has known vulnerabilities with exploits available publically.

How can I hack



```
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.16.4-dev                          ]
+ -- --=[ 1679 exploits - 962 auxiliary - 296 post        ]
+ -- --=[ 496 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > banner

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v4.16.4-dev                          ]
+ -- --=[ 1679 exploits - 962 auxiliary - 296 post        ]
+ -- --=[ 496 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > banner

  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v4.16.4-dev                          ]
+ -- --=[ 1679 exploits - 962 auxiliary - 296 post        ]
+ -- --=[ 496 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

(/wiki/File:Meta2.png)

Facebook/Instagram/Whatsapp or etc?

In short - you cannot. Major companies care about their security and finding flaws may be very difficult. Basing on your question, for you that will be "mission impossible".

Credentials for certain accounts may be stolen through phishing, but that has nothing to do with hacking or pentesting. That's just a fraud.

How can I hack Wi-Fi?

With `aircrack-ng` and only if it uses WEP security or WPA with weak password. An attack on routers where WPS PIN is configured is possible too, but only in case if router is old. Most of them have rate-limit on WPS connection attempts.

Many Wi-Fi routers and client devices are also vulnerable to KRACK (https://www.krackattacks.com/) attacks.

Usage of `aircrack-ng`, `reaver` and similar tools will require a Monitor Mode support in your Wi-Fi chipset firmware, packet injection kernel patches and MAC80211 drivers.

Available packages

Package	Need root?	Installation instructions

aircrack-ng	yes	`pkg install root-repo`
		`pkg install aircrack-ng`

bettercap	yes	`pkg install root-repo`
		`pkg install bettercap`

metasploit	no	`pkg install unstable-repo`
		`pkg install metasploit`

nmap	recommended	`pkg install nmap`

tshark	yes	`pkg install root-repo`
		`pkg install tshark`

sqlmap	no	`pkg install unstable-repo`
		`pkg install sqlmap`

wireshark-gtk	yes	`pkg install x11-repo`
		`pkg install wireshark-gtk`

Known issues

Aircrack-NG:

Requires monitor mode support in the firmware of your Wi-Fi module. Most devices do not support it.

What you can do is purchase a USB Wi-Fi stick and compile own kernel for your device with all necessary drivers or patches. Alternatively you can search on xda-developers forums (https://forum.xda-developers.com/) for Nethunter kernel builds supported by your device.

Metasploit:

As we cannot package Ruby modules dependencies, Metasploit package sideloads their sources and builds them during package installation. This makes package potentially unstable.

Monitor mode

Wi-Fi monitor mode allows you to intercept raw packets transmitted over wireless channel without being associated with access point. Primarily used by tools like Aircrack-NG, Reaver, etc.

(/wiki/File:WLAN_monitor_mode_devices.jpg)

Rooted device, USB-OTG adapter + cable and Wi-Fi USB stick.

Here will be shown few tips on getting monitor mode on your device. However, make sure that following conditions apply:

- You are experienced user and is familiar with use of desktop Linux distribution.

- You understand the details on how Android OS kernel is build & flashed on device.
- You have kernel source code and default configuration file applicable for your device.
- You have USB OTG adapter and Wi-Fi USB stick.
- Your device is rooted.
- You understand that this is not a kernel compilation guide.

Kernel source, defconfig, how to root device - all this info can be found on https://forum.xda-developers.com/ (https://forum.xda-developers.com/). Boot image build steps also should be on XDA, otherwise you'll have to figure them on your own or use boot.img repack kitchen.

(/wiki/File:Configuring_kernel.png)

Configuring USB WLAN drivers.

You may also check whether Nethunter kernel builds are available for your device - they have all necessary drivers enabled and probably are pre-compiled.

Configuring custom kernel

Use "make menuconfig" to launch the text-based interface for kernel configuration.

You want these 2 things:

1. CONFIG_MAC80211 - Generic IEEE 802.11 Networking Stack, available in N*etworking support* → *Wireless*.

2. A driver for USB Wi-Fi stick, for example CONFIG_RT2800USB. They are available at *Device Drivers* → *Network device support* → *Wireless LAN*.

Note: some drivers require a firmware blobs. Check the https://wiki.debian.org/Firmware (https://wiki.debian.org/Firmware) and download ones you need. Files should be put to `/system/etc/firmware`.

(/wiki/File:Enable_mon0_iface.png)

Enable monitor mode interface.

Acquiring monitor mode on device

You will need an utility "iw" to be installed which lately will be used to modify Wi-Fi module configuration:

```
pkg upgrade
pkg install root-repo
pkg install iw
```

Plug in the Wi-Fi USB stick and execute next command:

```
iw phy phy1 interface add mon0 type monitor
```

There shouldn't be any error if kernel is properly configured and drivers support monitor mode. To check whether monitor mode is active, use `iw dev`.

(/wiki/File:Termux_airodump-ng.jpg)

Running command "airodump-ng mon0" (SSIDs/MACs are censored).

Retrieved from "https://wiki.termux.com/index.php?title=Hacking&oldid=5725 (https://wiki.termux.com/index.php?title=Hacking&oldid=5725)"