Androsploit

ANDROID HACKING TOOL

Prashant Mishra, Prashansha Gupta | Network Security | 23 March 2017

ANDROID

- It is an operating system based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets
- Initially developed by Android Inc., which Google bought in 2005, Android was unveiled in 2007
- Beginning with the first commercial Android device in September 2008,
- The operating system has gone through multiple major releases, with the current version being 7.0 "Nougat" released in August 2016.
- Android applications ("apps") can be downloaded from the Google Play store,
- Which features over 2.7 million apps as of February 2017.
- In September 2015, Android had 1.4 billion monthly active users, and it has the largest installed base of any operating system. Android has been the best-selling OS on tablets since 2013; and on smartphones it is dominant.

ROOTED AND NON ROOTED ANDROID DEVICES

- Rooted Android phones provide a higher level of facility to the user. The user gets to customize and change application and settings of the system as desired. On the other hand, unrooted Android phones are the reverse of rooted android phones. Unrooted android phones do not provide these services of a super user. They have the original software.
- Rooted Android phones are those smart phones which provide a privileged control over the operating system. One gets access to the root of the files, and therefore the smart phone is termed as a rooted Android phone. A user gets the facility to install and run applications which can only be done with special privileges. It is also considered to be the same as jailbreaking (in reference to the Apple products). The main purpose of providing this facility is to customize the phone. One can easily search the instructions for rooting on the internet.
- Unrooted Android phones are just the opposite of rooted android phones. It refers to a brand new out of the box phone. It has the original software. This software contains various security levels which do not allow the user to make any type of changes that can damage the hardware. A rooted phone is also known as a stock phone. Another related term is 'unrooting', it refers to the turn around process of rooting.

- Rooting sounds to be interesting and therefore attracts the attention of a user; however, there are several disadvantages related to rooting an Android phone. One must clear all his or her doubts before thinking about rooting. For example, one must keep in mind that if a rooting process fails then it can lead to serious damage to the phone.
- Comparison between Rooted and Unrooted Android Phones:

	Rooted Android Phones	Unrooted Android Phones
Definition	Rooted Android phones are those smart phones which provide a privileged control over the operating system. One gets access to the root of the files, and therefore the smart phone is termed as a rooted android phone.	Unrooted Android phones are just the opposite of rooted android phones. It refers to a brand new out of the box phone. It has the original software. This software contains various security levels which do not allow the user to make any type of changes that can damage the hardware.
Advantages	• One can install custom themes, mods and ROMS • Speed and performance can be improved by changing the kernel version. • Battery life can be extended by the process of optimization. • One can install a custom bootloader for the back up of the device. • Unwanted applications can be removed • And many more	• It retains the warranty (one which has not be rooted) • No much security concerns • No risk of harming the phone
Disadvantages	• The phone's warranty will be lapsed • Malicious softwares might get installed	• No special privileges • Limited customization

	• Rooting may harm the phone	

ANDROID'S STOCK RECOVERY

- Android devices come with Google's recovery environment, which is often referred to as the "stock recovery." You can boot to the recovery system by pressing device-specific buttons as your phone or tablet boots or by issuing an adb command that boots your device to recovery mode. The recovery menu provides options to help recover your device — for example, you can reset your device to its factory default state from here. The recovery mode can also be used to flash OTA update files. if you want to flash a new ROM to your device — or re-flash the factory default ROM file — you'll need to boot to recovery mode first.
- The stock recovery is a minimal, limited system. It's designed to be ignored, and it can generally only flash OTA updates and ROMs provided by the device's manufacturer, not third-party ROMs.
- All Android devices ship with a recovery console that is basically a partition on the device's internal memory and can be booted into. The stock recovery of almost all Android devices provides a few basic yet handy options that allow you to factory reset your device and also to recover its operating system using an official ROM in zip format, but that's all you can do with it. That's where a custom recovery comes handy.

ANDROID'S CUSTOM RECOVERY

- A custom recovery replace stock recovery and in that way it bring various advance functions that stock recovery don't have. With a custom recovery, you can install both official (stock firmware) and unofficial ROMs as well as other updates including apps, themes, kernels etc. using zip files, can wipe not just user data but pretty much every partition on your device, mount the storage card for USB mass storage access without leaving recovery, partition your SD card, wipe Dalvik cache and battery stats, fix permissions, perform, manage and restore backups and so on. However, custom recovery mostly used for flashing or installing new ROMs.
- The first custom recovery that get fame was ClockworkMod recovery which developed by Kush, a well known Android developer. However, earlier releases of CWM recovery

don’t comes with touch feature (but now available in touch supported version) and to fulfil the gap the touch supported custom recovery TWRP comes out. Recently, developer Phil3759 rolled out an advance version of CWM recovery which we call PhilZ Touch 5 Recovery. It remove the boringness of custom recovery by offering various colourful customization features control

- Anyway, in this page we will discuss the easy installation guide of CWM recovery (currently the latest version is 6.0.3.3) and TWRP recovery (currently the latest version is 2.6.0.1). PhilZ Touch 5 Recovery comes with different installation option for various manufactured models, that’s why I’m not covering it here. The installation guide I discussed here require a rooted device, so you must have a rooted Android smartphone or tablet. This tutorial should work most devices including latest Galaxy S4, Xperia Z or HTC One.

HOW TO INSTALL A CUSTOM RECOVERY

- Installing a Custom Recovery allows you to flash custom ROMs, backup your phone, restore from backups and much more. Every phone has a specific method to install a recovery, so in this post we will get you started with the basics then point you in the direction of more information. As always, make sure you have backed up your data before you begin.

You will need:

- Rooted Android Device
- USB Cable
- USB Drivers
- Custom Recovery File
- Android SDK

Step 1: Install USB Drivers

- Find the appropriate drivers for your device. You will need this for your computer to recognize your device properly. Below are links to drivers for the most popular devices, but you can also check our USB Driver guide for other OEMs.

Step 2: Choose a Custom Recovery

CMW

TWRP

- Step 3: Flash Recovery File
    - Before you proceed, put your phone in “USB Debugging Mode” by navigating Settings > About Phone > Tap Build Number 7 times (until developer confirmation) > Back out to settings > Developer options > Check USB Debugging
- Many devices will have software that makes flashing the recovery easy. Samsung has Odin, Nexus has WugFresh Toolkit, Sony has FlashTool and so on

ADB (ANDROID DEBUGGING BRIDGE)

- Android Debug Bridge (adb) is a versatile command-line tool that lets you communicate with an android device or emulator.
- It’s a “bridge” for developers to work out bugs in their Android applications. This is done by connecting a device that runs the software through a PC, and feeding it terminal commands. ADB lets you modify your device (or device’s software) via a PC command line.
- ADB is a client-server program that includes three components:
- **A client**, which sends commands. The client runs on your development machine. You can invoke a client from a command-line terminal by issuing an adb command.
- **A daemon (adbd)**, which runs commands on a device. The daemon runs as a background process on each device.

- **A server**, which manages communication between the client and the daemon. The server runs as a background process on your development machine.
- To run adb command on the client PC we “adb and fastboot Tools”
- For windows operating system “adb and fastboot tools” comes with “Android Studio” and “Android SDK” which is located in folder “sdk/platform-tools”
- For Linux operating PC’s users can either download full Android Studio by executing command on terminal window “apt-get install androidsdk” can download only platform-tools by executing command on terminal window “ apt-get install adb and fastboot”
- The basic adb command is “adb devices”.
    - Output:

        List of devices attached

        d93753a device

        “d93753a” is the device id which is connected to the pc

HOW THE APPLICATION WORKS

- When you start the application an adb client is started, the client first checks whether there is an adb server process already running. If there isn't, it starts the server process. When the server starts, it binds to local TCP port 5037 and listens for commands sent from adb clients.
- All adb clients use port 5037 to communicate with the adb server.
- The server then sets up connections to all running devices. It locates emulators by scanning odd-numbered ports in the range 5555 to 5585, the range used by the first 16 emulators. Where the server finds an adb daemon (adbd), it sets up a connection to that port. each emulator uses a pair of sequential ports
- An even-numbered port for console connections and an odd-numbered port for adb connections.
- For example:
    - Emulator 1

        - console: 5554
          adb: 5555
    - Emulator 2
        - console: 5556
          adb: 5557
    - And so on...

USB

- For USB connection command is “adb usb”
- Once the server has set up connections to all devices, you are good to go through this application can control any android device.
- **Note:** When you connect a device running Android 4.2.2 or higher, the system shows a dialog asking whether to accept an RSA key that allows the connection. This security mechanism ensures that adb commands cannot be executed unless you unlock the device and accept the dialog.
- But this verification can be bypassed by flashing custom recovery.

WIRELESS

- Connection can also be done over Wi-Fi.
- Through this application the android devices can be controlled wirelessly
- By injecting a payload which will turn the Wi-Fi and connect the device to the local Access point, and setting the target device to listen for a TCP/IP connection on port 5555.
- And can set the wireless port permanently turned on

INTERNET

- This application you can also inject rat (Remote Access Trojan) into the devices making the device available on the internet to control.

LIST OF FEATURES INCLUDED IN THE TOOL

- This application you can also inject rat (Remote Access Trojan) into the devices making the device available on the internet to control.
    - NON ROOT DEVICES
        - Scan Connected Victims
        - Wired ,Wireless Connection
        - List Base Files And Directories
        - Upload Data To Victim's Device
        - Extract Data From Victim's Device
        - Application Manager
        - Spy On Victim's Device Screen
        - Turn ON/Off Internet
        - Turn On/Off Wi-Fi
        - Unlock Device
        - Make Call From Victim's Device
        - Turn On/Off Flight Mode
    - ROOT DEVICES
        - Open Lock Screen
        - Turn On Bluetooth
        - Turn Off Bluetooth
        - Injecting RAT Mode
        - Download Build Prop
        - Tweak Build Prop

- Upload Build Prop
- Changing Developer Defined Build Properties.