Androsploit

Android Hacking Tool

Prashant Mishra

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.

ADB

- Android Debug Bridge (adb) is a versatile command-line tool that lets you communicate with a 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.

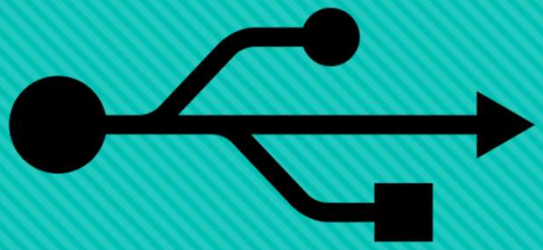
ADB

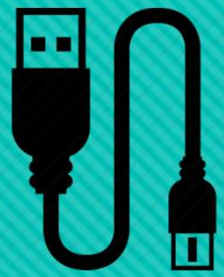
- ADB is a client-server program that includes three components:
- **A client**, which sends commands. The client runs on your development machine. You can invoke a client from a command-line terminal by issuing an adb command.
- **A daemon (adbd)**, which runs commands on a device. The daemon runs as 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.

How The Application Works

- When you start the application an adb client is started, the client starts the server process, the server 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.
- Sever locates devices by scanning odd-numbered ports in the range 5555 to 5585, When 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 port for console and an odd port for adb — . For example:
- Emulator 1 Emulator 2
- console: 5554 console: 5556
  adb: 5555 adb: 5557
- And so on...

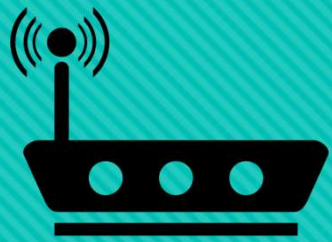
USB





- Once the server has set up connections to all devices, your r good to go through this application you 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

- 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
- Rooted 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.

Thank You