Android: From Rooting to Pwning
$ →

A Presentation by:
Acexor

Obligatory Introduction

Name: Acexor

Security Researcher / IT Professional

Interests:

- Networking
- Security
- Linux
- Android
- CTF

Why Android?

- Android controls 75% of the smart phone market
- Android phones now come with Multi-core processors, GSM, Wi-Fi, Bluetooth, and they run Linux =)
- Small easy to conceal
- Everyone nowadays has a phone making it less conspicuous when PWNing

Goals

- Discuss Rooting an Android Device
  - Security Implications of Rooting Device
- Installing Apps from “Unknown Sources”
  - Security Implication of Installing Any Apps
- Bloatware/Stock ROM and Flashing a Custom ROM
- Useful Apps once Phone is Rooted
- Security Related Apps
- Android Forensics Introduction

Rooting an Android Device

- Rooting is gaining root/admin over your phone
- Each phone has its own method of becoming Rooted
- Usually community driven exploits and methods for rooting come shortly after the release of the phone
- By using an exploit an application usually called SU.apk or SuperUser.apk is pushed to the phone which whenever root permission are needed this application is called.
- Definitive Rooting/Custom Roms Site is XDA Developers

Once Rooted

- Bye, Bye Warranty
- You are the Device Admin
- We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:
  - Respect the privacy of others.
  - Think before you type.
  - With great power comes great responsibility

Security Implications of Root

- Now that your phone has a root user Malicious apps and scripts can make use of your Superuser.apk
- Attacks targeted at users who have rooted devices
  - P2P-ADB will be discussed later
- Root + USB debugging + Allow Unknown Sources = Completely wide open

Installing Apps from “Unknown Sources”

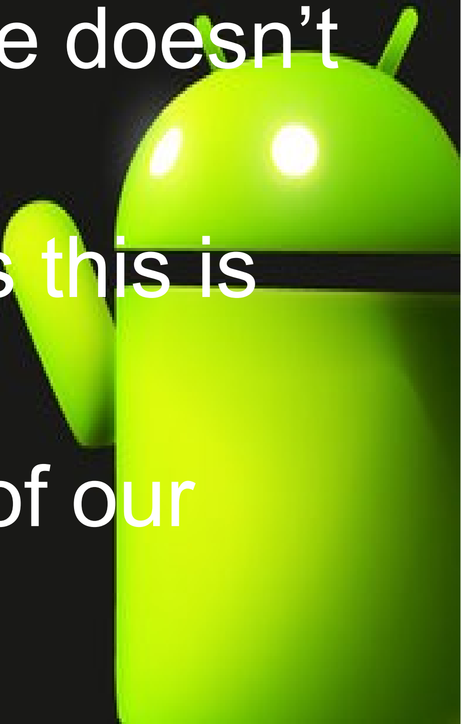
- What is needed?
  - Computer with Android SDK
  - Drivers for device on computer
  - Little Knowledge of ADB
  - “Unknown Source” application: .apk file
- It's best to put the SDK tools in your machines PATH aka Environment Variable
  - This allows for usage of SDK tools on the command line from any folder

Installing Apps from “Unknown Sources”

- Steps to Install *application*.apk
  - Devices has both USB debugging and Unknown Sources enabled
  - Make sure no other android devices are plugged into the computer
  - Make sure all other Drivers for other Android Devices are uninstalled
  - Download said application to a folder
  - Navigate to the Folder and run: *adb devices*
  - Run: *adb install application.apk*
  - Check your applications on your Device as it is now installed

Security Implications of Installing Any App

- Whenever installing any App always READ what permissions the app is requesting
  - Ask yourself why does Angry Birds need access to my:
    - Contact list / Read my Text Messages / Read my Phone Calls / ETC ......do you get the point yet?
- Just because an app is on the Play Store doesn’t mean its not malware/spyware
- When Installing “Unknown Source” Apps this is even more apparent
- Chinese/Russian's have databases full of our Smartphones information

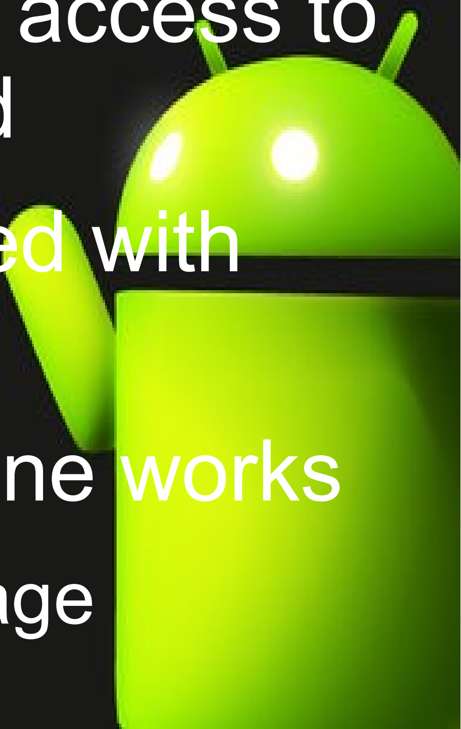


Stock Rom/Bloatware

- A Stock Rom is the ROM a phone comes with by default
- Bloatware is software applications that are installed on the phones Stock Rom
- Bloatware usually ties in with the Stock ROM so removing it is annoying/impossible (possible bricking)
- Bloatware is also known as Proprietary Spyware
- I Value my privacy …..not really I'm using a smartphone LOL

Custom ROMS / Custom Kernels

- Again XDA is the go to place for custom ROMS/Kernels
- Use tools to Backup your Android! Trust me DO IT!
- Most Custom ROMs remove bloatware and change the interface sometimes giving access to versions of android that are unreleased
- Possibly using different launchers paired with custom Icons and backgrounds
- Custom Kernels affect the way the phone works
  - Battery Life/ CPU overclocking / RAM usage



Useful Apps for Rooted Devices

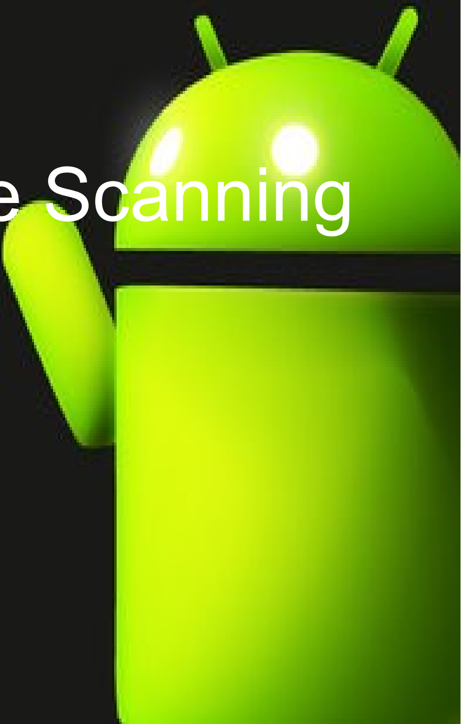
- Titanium Backup
  - Takes all sorts of Backups for your device (Nandroid, ROM, contacts, Applications, Application preferences)
- Clockwork Recovery Mod
  - Tool for Backing up/Flashing Custom ROMs and Kernels
  - Another boot loader for your phone
- Busybox
  - Gives Full features of Unix/Linux Commands to Android Device

Useful Apps for Rooted Devices

- Wi-Fi Tether for Root
  - An application for turning your android device into a hotspot
- Terminal Emulator
  - Allows you to run commands on your android device
- Hacker's Keyboard (Thanks to Nat)
  - A multi-touch keyboard with Alt, Ctrl and Esc keys

Security Related Apps

- Torbot (Play Store)
  - Everyone's Favorite anonymous Network for your android
- Connectbot (Play Store)
  - Popular SSH / Telnet Client for Android
- Fing (Play Store)
  - Popular Network Scanner Supports Service Scanning and Ping / Trace route
- Connect Cat (Play Store)
  - Port Knocker Netcat on android



Security Related Apps

- RouterPwn (Play Store)
  - Exploit tool for a huge list of Home routers
- WiFiKill (On da Internetz)
  - Tool for watching traffic / Killing Wi-Fi Connections
- InSSIDer (Play Store)
  - Comprehensive Wi-Fi Scanner / Spectrum Analyzer
- Dsploit (On da Internetz)
  - Full featured exploitation Framework (MiTM / Vulnerability Scanner / Exploit Launcher)
- WiFinspect (Play Store)
  - WiFi Scanner + Pcap Tool / Analyzer

Security Related Apps

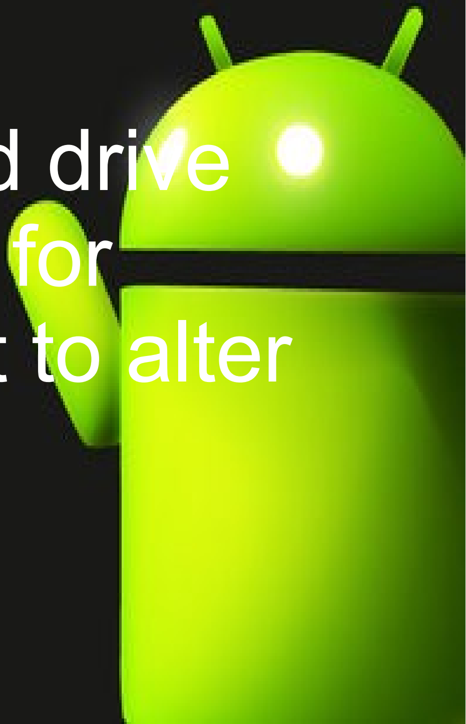
- Droidsheep (On da Internetz)
  - MitM Cookie collector (Firesheep for Android)
- FaceNiff (On da Internetz)
  - Another MitM cookie stealer / Session Hijacker
- Zanti (on da Internetz)
  - Another Full Featured Exploit Framework / Network Scanner (Make you buy credits to use full functionality.... lame -_-
- Droidwall (Play Store)
  - IPTables for Android nuff said

P2P-ADB

- A set of tools Developed by Koz for performing Physical Android attacks using an OTG cable
- Attacks are more effective against Rooted / Custom modded phones
- AntiGuard is a tool used to crack lock screens on androids
- Other features include Stealing Pictures / Contacts / Txt Messages / Gestures
- Steal the users Google password in a Hash
- Use the Hash to Generate a SSO effectively bypassing Two-Factor Authentication

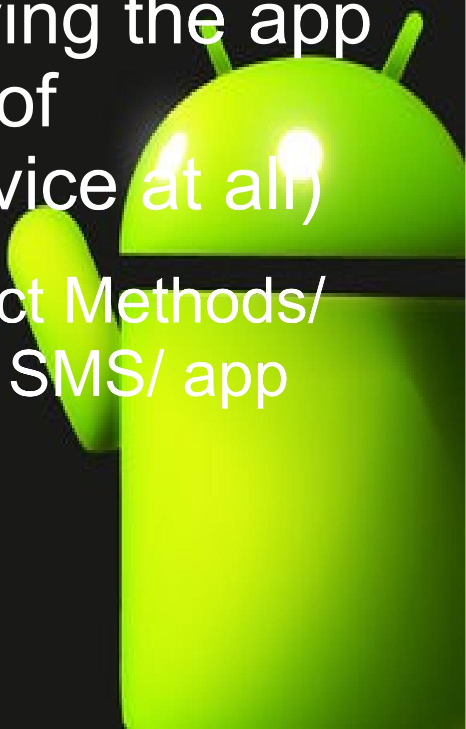
Introduction to Android Forensics

- Applications in Android are developed in Java
- These applications are run inside of a Dalvik Virtual Machine
- Each application only has access to the data specific to that DVM unless another application and user intervention occurs
- Since androids don't have a typical hard drive there are specific steps and challenges for forensic examiners since the goal is not to alter any data on the device



Types of Analysis

- SD Card Analysis
  - Involves creating a copy of the SD card whether it be internal or external (File System is FAT32)
- Local Analysis
  - Involves installing an App to the phone, running the application to capture the data, then removing the app for analysis (This is one of the Challenges of Forensics on android of not altering the device at all)
  - Can Acquire: Browser History/ Call Logs/ Contact Methods/ (Metadata from Images, Audio, and Video)/ MMS/ SMS/ app list/ app versions/ contact settings/ etc
  - Exports as CSV / XML



Types of Analysis

- Physical Analysis
  - Acquire a dd image of the NAND
  - Filesystem Type is YAFFS2
    - YAFFS2 is a log structured filesystem
    - Possibility for “point-in-time” Analysis
  - Open your favorite hex editor and start digging
- OSAF-Toolkit
  - An Ubuntu 11.10 VM with Android SDK
  - Comes with many scripts and tools for Android Forensics and Malware analysis

Sources and Links

- XDA Developers (Rooting, Cusom Mods/Kernels, and all things Android)
  - http://www.xda-developers.com/
- Smartphone Market Information
  - http://www.ucstrategies.com/unified-communications-newsroom/android-now-enjoying-
- Koz's Talk on Hak5 / GitHub
  - http://hak5.org/episodes/hak5-1205
  - https://github.com/kosborn/p2p-adb/
- DFI Android Forensics
  - http://www.dfinews.com/article/introduction-android-forensics
- OSAF
  - http://sourceforge.net/projects/osaftoolkit/
- Hackmiami
  - http://www.hackmiami.org

Contact Me

- @acexor on twitter
- ac3x04@gmail.com
- ac3x04 on irc usually on freenode in #hackmiami channel
- Ac3x04 on AIM

The End

Thank you