ANDROID PENTEST TOOLS

Josua M. Sinambela, M.Eng
CEH, CHFI, ECSA|LPT, ACE, CCNP, CCNA, CompTIA Security+

Seminar Nasional,10 November 2012
UNS, Surakarta

Who Am I?

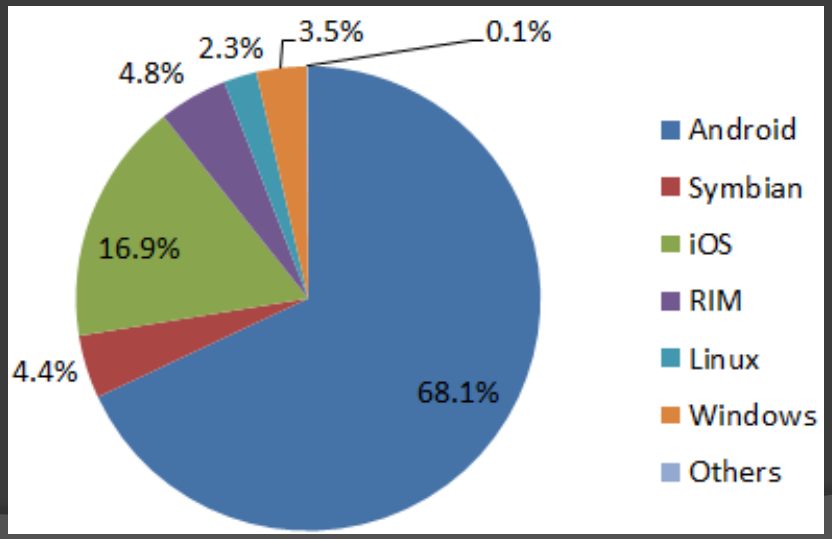
- Professional IT Security Trainer & Consultant
- Digital Forensic Investigator
- Professional Lecturer (Teach PostGraduate Students @ MTI UGM)
- CEO RootBrain IT Security Training & Consulting
- Past: Leader Information System Integration Team UGM (2009-Februari 2012)
- Contact: josh@rootbrain.com
- Website: http://josh.rootbrain.com

Outline

- Overview Mobile Devices
- Android Devices as a Weapon
- Pentest Tool in Android
- Backtrack 5 on Android
- Demo

Overview Mobile Devices

- Mobile *computers*:
  - Berupa : smartphones, tablets
    - Sensors: GPS, camera, accelerometer, etc.
    - Computation: powerful CPUs (≥ 1 GHz, multi-core)
    - Communication: cellular/4G, Wi-Fi, near field communication (NFC), etc.
- Worldwide Statistic : Android, iOS, RIM, Symbian, Windows



Source: IDC Worldwide Mobile Phone Tracker, August 8, 2012

Android Devices as a Weapon

- Mobile devices saat ini sering menjadi “target” para Hacker
- Mobile devices juga dapat digunakan sebagai senjata (weapon) bagi Hackers
- Mobile devices saat ini :
  - tidak sekedar perangkat dengan kemampuan terbatas (dulu hanya untuk SMS, MMS, Note)
  - merupakan komputer dengan Processor Dual-core/Quad-core
  - Portabilitas dan Powernya dapat digunakan untuk keperluan “Penetration Testing/Security Testing” a.k.a “*Hacking*”

Pentest Tool in Android

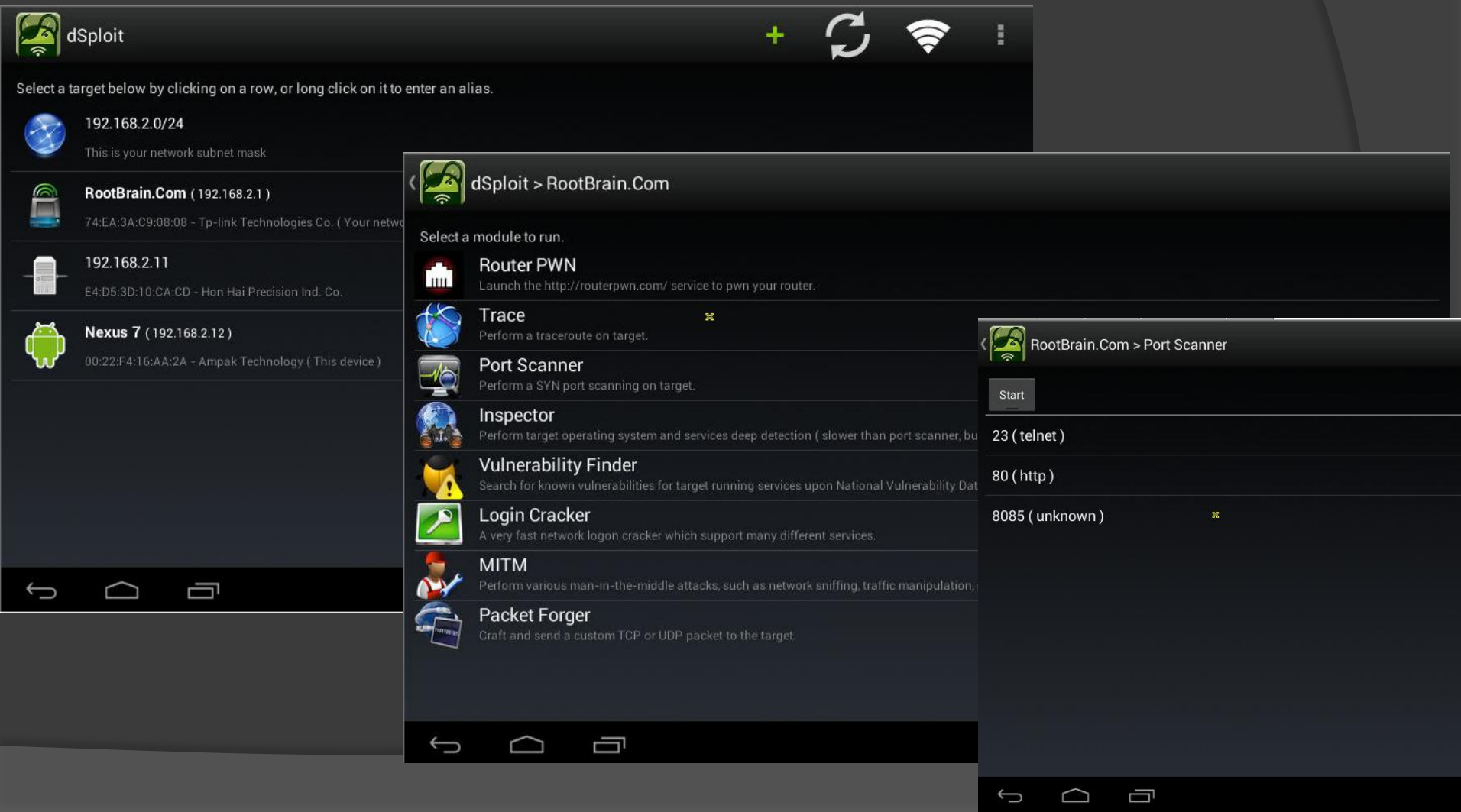
- Terdapat cukup banyak Hacking Tools di Android
- Beberapa diantaranya bahkan lebih “user friendly” dibanding tools di PC
- Umumnya membutuhkan status “ROOTED” untuk menggunakannya.
  - ROOTED artinya memodifikasi System Android sehingga memberikan pengguna akses penuh/tidak terbatas ke handphone
  - ROOTED dapat menghilangkan garansi
  - ROOTED dapat mempermudah sistem tersusupi malware (virus/trojan/worm)

Pentest Tool in Android

- dSploit
  - an Android network analysis and penetration suite
  - Fitur-fitur: easily map your network, fingerprint alive hosts operating systems and running services, search for known vulnerabilities, crack logon procedures of many tcp protocols, perform man in the middle attacks such as password sniffing (with common protocols dissection), real time traffic manipulation, etc, etc

Pentest Tool in Android

- dSploit

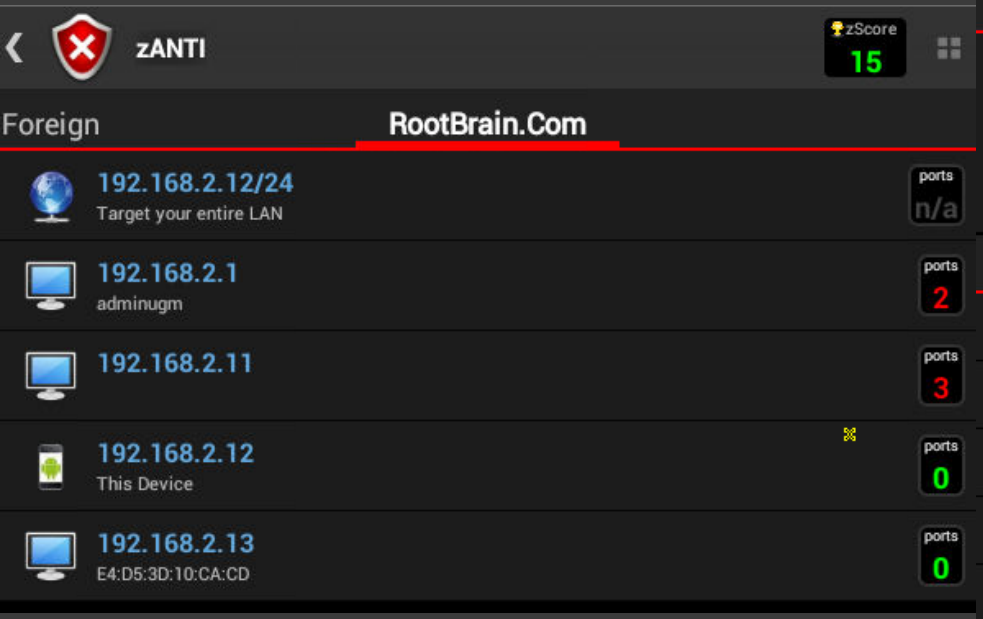


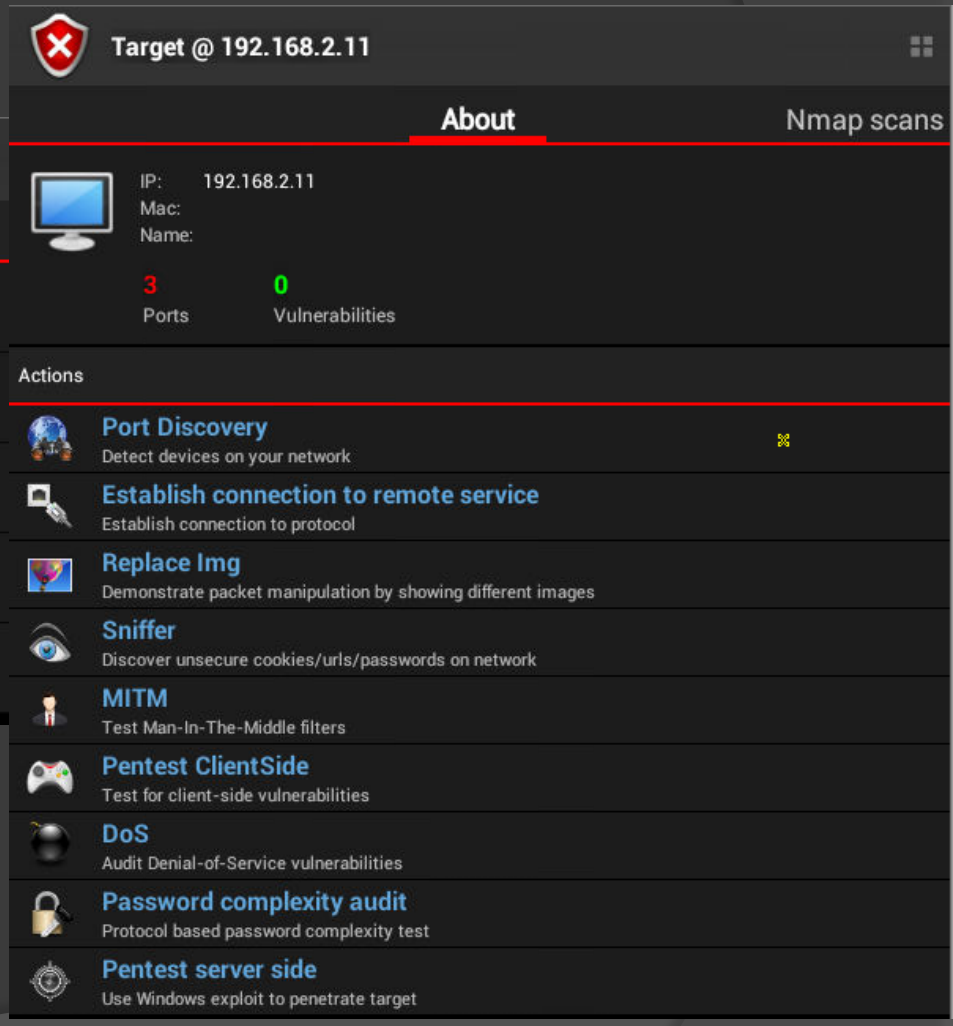
Pentest Tool in Android

- zANTI
  - Zimperium Android Network Toolkit
  - Digunakan Pen-testers/Administrator untuk Network Assessment
  - Fitur-Fitur :
    - Search for common vulnerabilities
    - Get a detailed cloud-based report to fix recognized vulnerabilities including wise analysis for critical flaws.
    - Perform password audit to check for password complexity.
    - Find mis-configuration of devices firewall by detecting open ports.
    - Check if network is vulnerable to MITM and common Client side, Server side vulnerabilities.
    - Discover insecure traffic and cookies affecting network's privacy.
    - Visualise your network by watching captured images, recorded from unsecured network communication.

Pentest Tool in Android

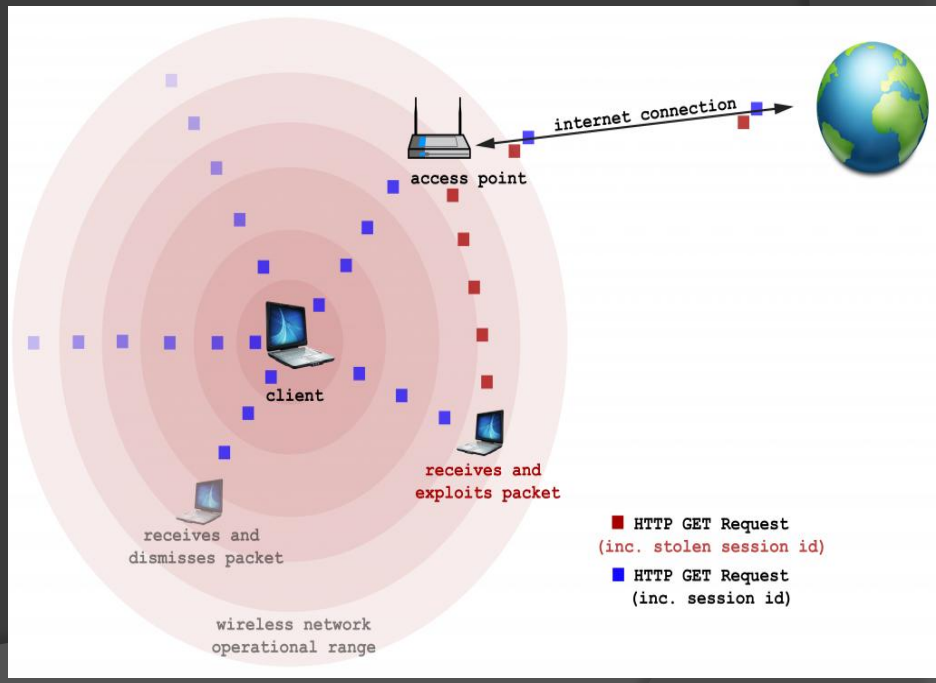
- zANTI





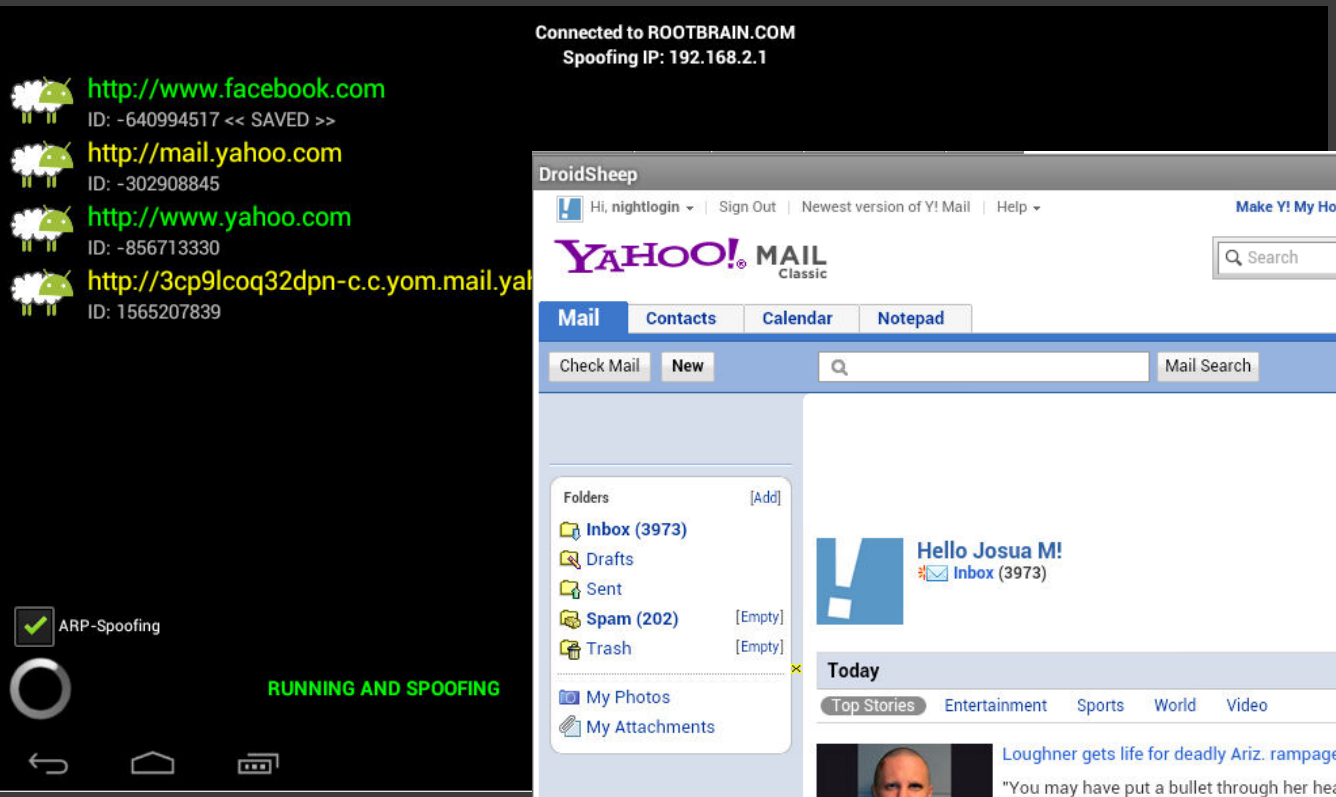
Pentest Tool in Android

- Droidsheep
  - an Android app for Security analysis in wireless networks and capturing facebook, twitter, linkedin and other accounts
  - Menyadap/mencuri SessionID dan menggunakannya tanpa sepengetahuan pengguna



Pentest Tool in Android

- Droidsheep



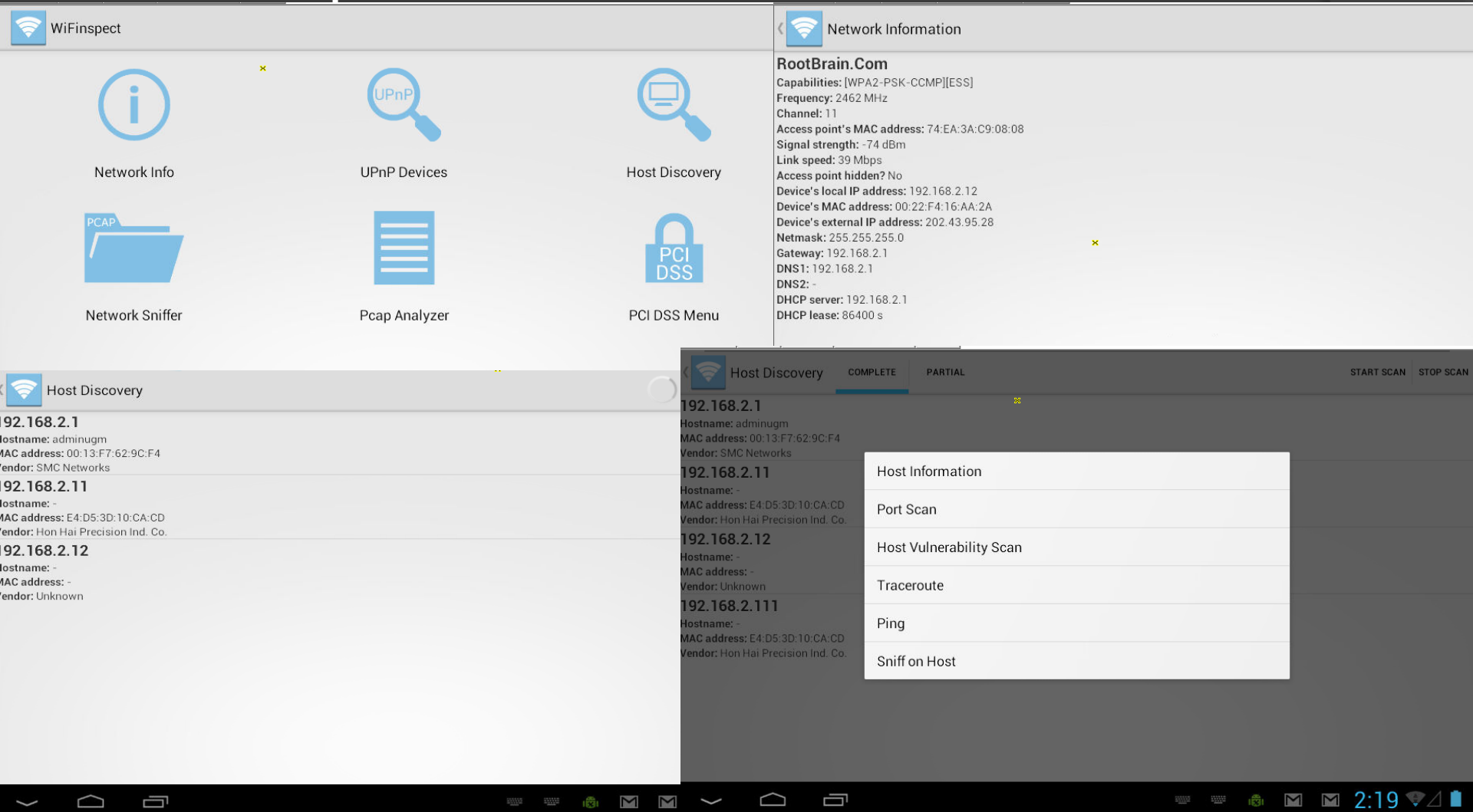
Pentest Tool in Android

- WifiInspect
  - is a multi-tool intended for Computer Security professionals and other advanced users that wish to monitor the networks they own or have permission (ethical hacking)
  - Fitur-Fitur:

    * Network Information
    * UPnP Device Scanner
    * Host Discovery
    * Network Sniffer
    * Pcap Analyzer (three options)
    * PCI DSS Menu
    - Access Point Default Password Test (requirement 2.1.1.c)
    - Access Point Security Test (requirement 4.1.1)
    - Access Point Scanner (requirement 11.1)
    - Internal Network Vulnerability Scanner (requirement 11.2.1)
    - External Network Vulnerability Scanner (preparation for requirement 11.2.2)
    * Host Information
    * Port Scan
    * Host Vulnerability Scan
    * Traceroute
    * Ping

Pentest Tool in Android

- WifiInspect



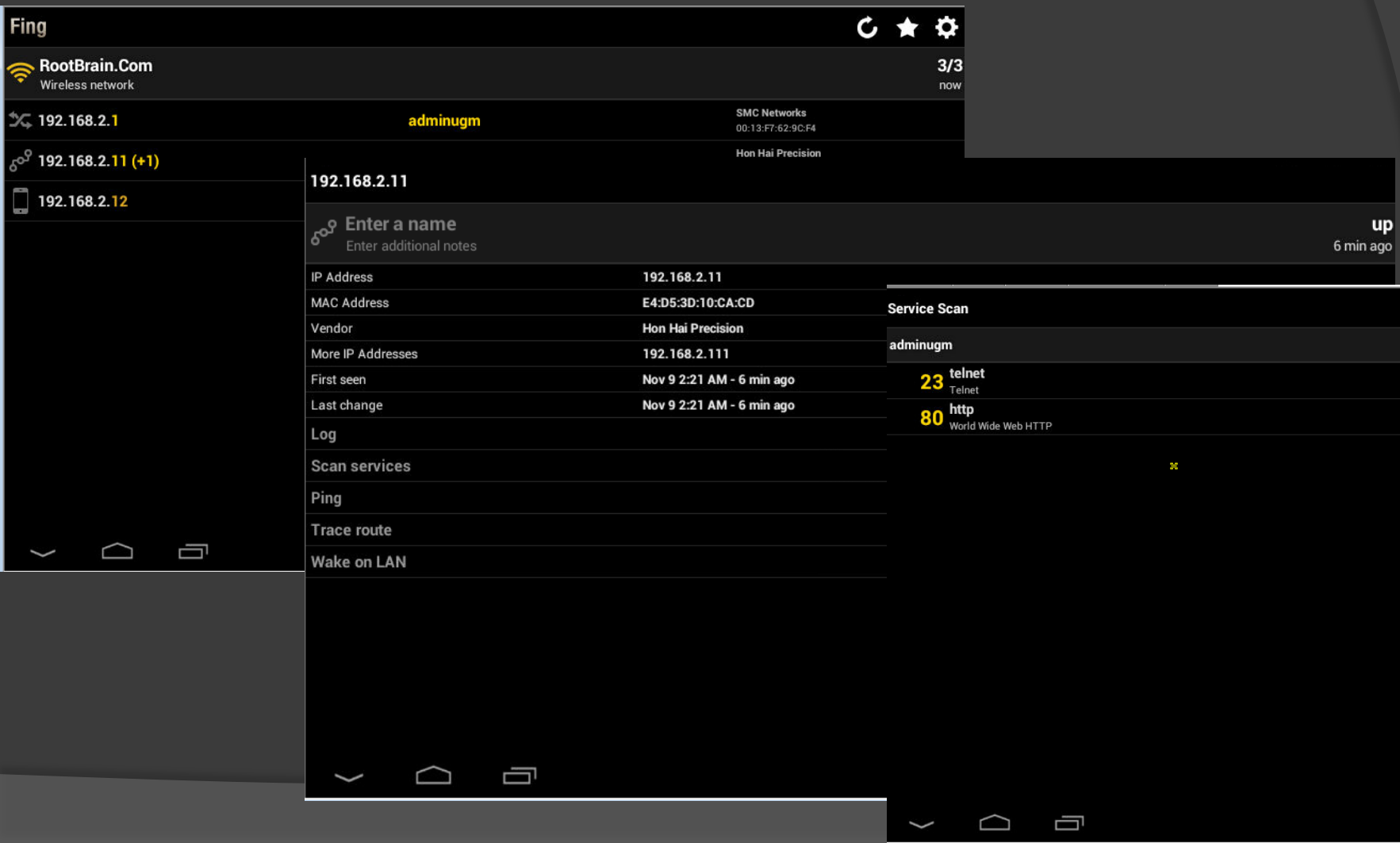
Pentest Tool in Android

- Fing
  - is the ultimate toolkit for network management
  - Fitur Fitur:

    * network discovery
    * service scan (TCP port scan)
    * ping
    * traceroute
    * DNS lookup
    * Wake on LAN
    * Fingbox (sync, backup, merge, monitor, notifications)
    * TCP connection tester
    * MAC address and vendor gathering
    * customizable host names and icons
    * connectivity detection
    * geolocation
    * Integrated launch of third-party Apps for SSH, Telnet, FTP, FTPS, SFTP, SCP, HTTP, HTTPS, SAMBA

Pentest Tool in Android

- Fing



Pentest Tool in Android

- Other tools:
  - NetworkSpoofer
  - exploitDB
  - NetworkDiscovery
  - Net Swiss Tool
  - LAN Droid
  - PortKnocker
  - Routerpwn
  - Reveal Wifi
  - WiEye
  - WifiKill

Backtrack 5 on Android (ARM)

- Backtrack: Distribusi GNU/Linux yang dikhususkan untuk digital forensics dan penetration/security testing
- Backtrack 5 di Android berjalan dalam chroot system (Tidak secara native, Backtrack dijalankan diatas sistem Android)
- Requirement:
  - ROOTED Android Device
  - Complete Linux Installer (from PlayStore)
  - Terminal Emulator (from PlayStore)
  - Android VNC (from PlayStore)
  - Backtrack 5 for ARM Image (from: backtrack-linux.org)

Backtrack 5 on Android (ARM)

Demo

- Diskusi & Tanya-jawab

Terimakasih