

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?

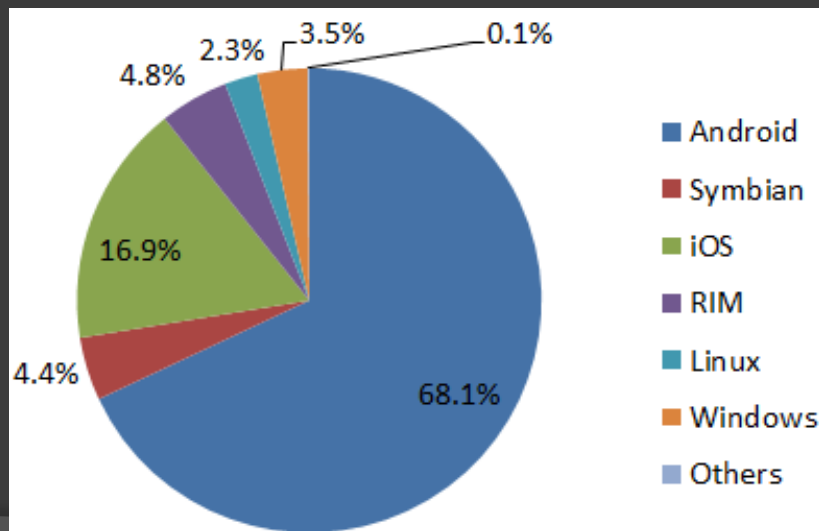
- ◉ Professional IT Security Trainer & Consultant
- ◉ Digital Forensic Investigator
- ◉ Professional Lecturer (Teach PostGraduate Students @ MTI UGM)
- ◉ CEO RootBrain IT Security Training & Consulting
- ◉ Past: Leader Information System Integration Team UGM (2009-Februari 2012)
- ◉ Contact: josh@rootbrain.com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



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 Povernya 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)

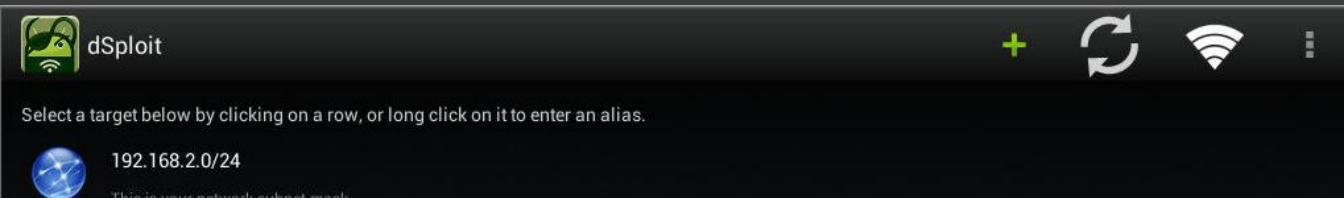
Pentest Tool in Android

◎ 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

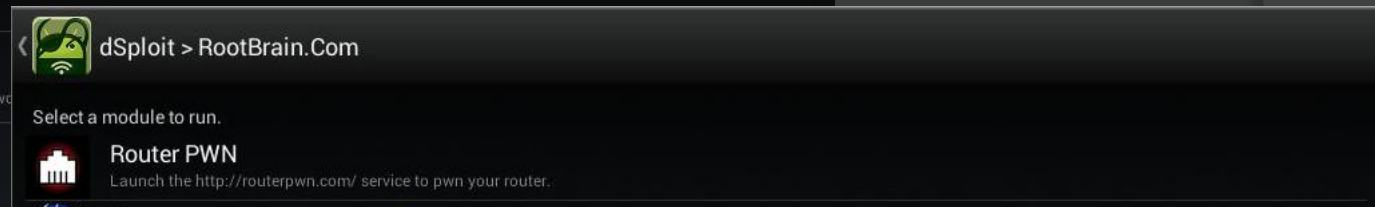
Pentest Tool in Android

dSploit



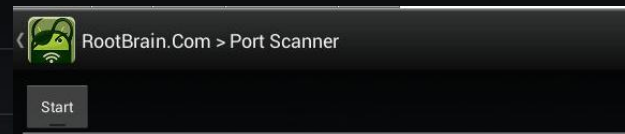
The dSploit main interface shows a list of network targets. At the top, there is a header with the dSploit logo, a plus sign, a refresh icon, a Wi-Fi icon, and a menu icon. Below the header, a message says "Select a target below by clicking on a row, or long click on it to enter an alias." The list includes:

- 192.168.2.0/24: This is your network subnet mask.
- RootBrain.Com (192.168.2.1): 74:EA:3A:C9:08:08 - Tp-link Technologies Co. (Your network)
- 192.168.2.11: E4:D5:3D:10:CA:CD - Hon Hai Precision Ind. Co.
- Nexus 7 (192.168.2.12): 00:22:F4:16:AA:2A - Ampak Technology (This device)

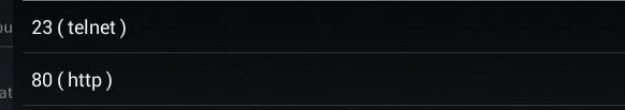


The interface shows the selection of a module to run on the RootBrain.Com target. The title bar reads "dSploit > RootBrain.Com". Below the title bar, a message says "Select a module to run." The list of modules includes:

- Router PWN: Launch the <http://routerpwn.com/> service to pwn your router.
- Trace: Perform a traceroute on target.
- Port Scanner: Perform a SYN port scanning on target.
- Inspector: Perform target operating system and services deep detection (slower than port scanner, but more accurate)
- Vulnerability Finder: Search for known vulnerabilities for target running services upon National Vulnerability Database
- Login Cracker: A very fast network logon cracker which support many different services.
- MITM: Perform various man-in-the-middle attacks, such as network sniffing, traffic manipulation, and session hijacking.
- Packet Forger: Craft and send a custom TCP or UDP packet to the target.

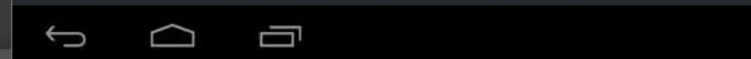


The interface shows the execution of the Port Scanner module on the RootBrain.Com target. The title bar reads "RootBrain.Com > Port Scanner". Below the title bar, there is a "Start" button.



The results of the Port Scanner module are displayed. The list shows:

- 23 (telnet)
- 80 (http)
- 8085 (unknown)



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

zANTI zScore 15

Foreign RootBrain.Com

IP	Description	ports
192.168.2.12/24	Target your entire LAN	n/a
192.168.2.1	adminugm	2
192.168.2.11		3
192.168.2.12	This Device	0
192.168.2.13	E4:D5:3D:10:CA:CD	0

Target @ 192.168.2.11

About Nmap scans

IP: 192.168.2.11
Mac:
Name:

3 Ports 0 Vulnerabilities

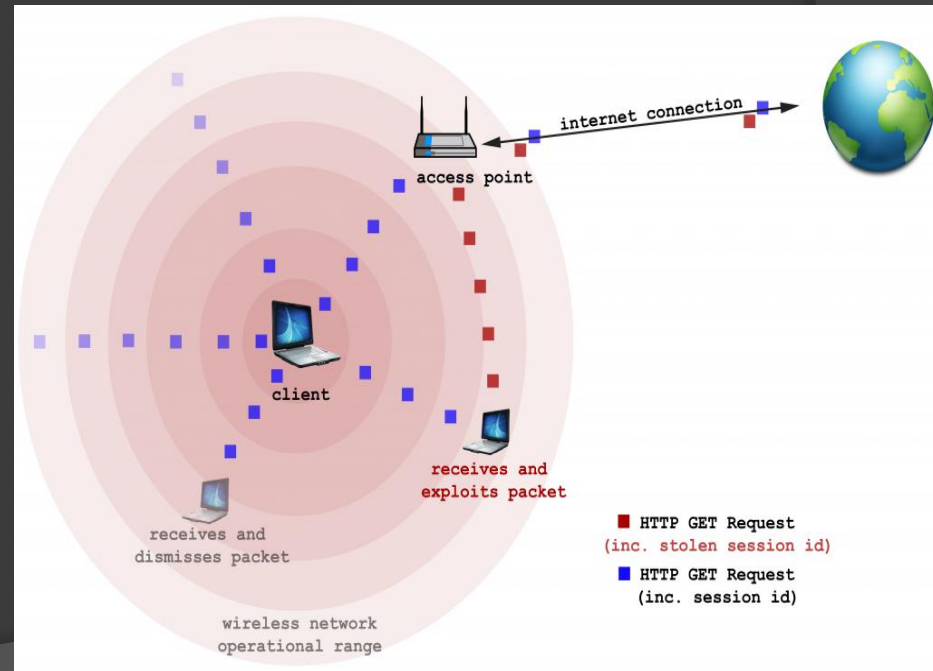
Actions

- Port Discovery: Detect devices on your network
- Establish connection to remote service: Establish connection to protocol
- Replace Img: Demonstrate packet manipulation by showing different images
- Sniffer: Discover unsecure cookies/urls/passwords on network
- MITM: Test Man-In-The-Middle filters
- Pentest ClientSide: Test for client-side vulnerabilities
- DoS: Audit Denial-of-Service vulnerabilities
- Password complexity audit: Protocol based password complexity test
- Pentest server side: Use Windows exploit to penetrate target

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

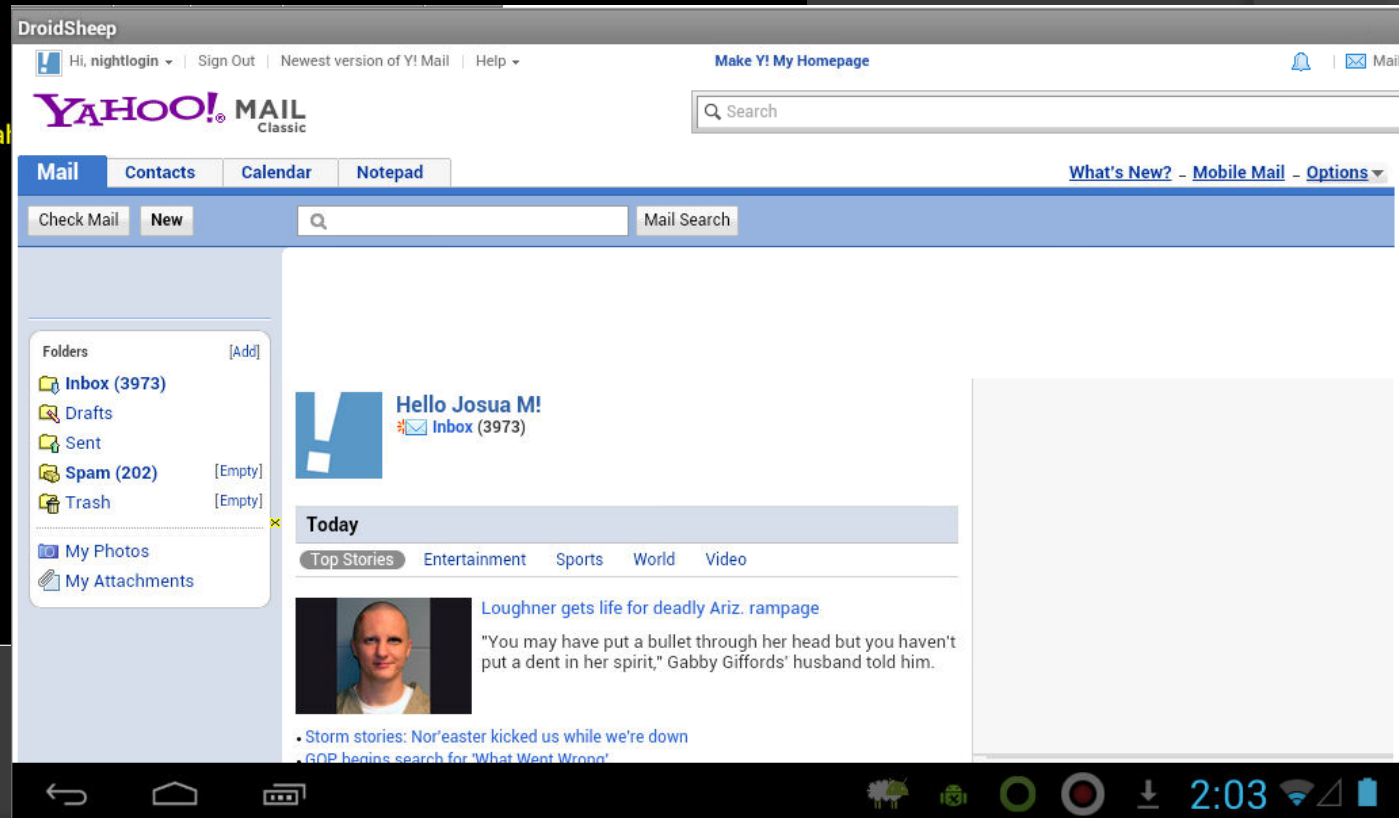
⦿ Droidsheep

Connected to ROOTBRAIN.COM
Spoofing IP: 192.168.2.1

-  <http://www.facebook.com>
ID: -640994517 << SAVED >>
-  <http://mail.yahoo.com>
ID: -302908845
-  <http://www.yahoo.com>
ID: -856713330
-  <http://3cp9lcoq32dpn-c.c.yom.mail.yal>
ID: 1565207839

ARP-Spoofing

RUNNING AND SPOOFING



The screenshot displays the DroidSheep application interface. At the top, it shows the connection status: "Connected to ROOTBRAIN.COM" and "Spoofing IP: 192.168.2.1". The main content area shows a spoofed Yahoo! Mail page. The page header includes "DroidSheep" and "Hi, nightlogin" with options for "Sign Out", "Newest version of Y! Mail", and "Help". The "YAHOO! MAIL Classic" logo is prominent. Below the logo, there are navigation tabs for "Mail", "Contacts", "Calendar", and "Notepad". The "Mail" tab is active, showing a "Check Mail" button, a "New" button, and a search bar. On the left side, there is a "Folders" list with "Inbox (3973)", "Drafts", "Sent", "Spam (202)", and "Trash". The main content area displays a "Hello Josua M!" greeting and a "Today" section with "Top Stories" for "Entertainment", "Sports", "World", and "Video". A news item is visible: "Loughner gets life for deadly Ariz. rampage" with a sub-headline: "You may have put a bullet through her head but you haven't put a dent in her spirit," Gabby Giffords' husband told him.

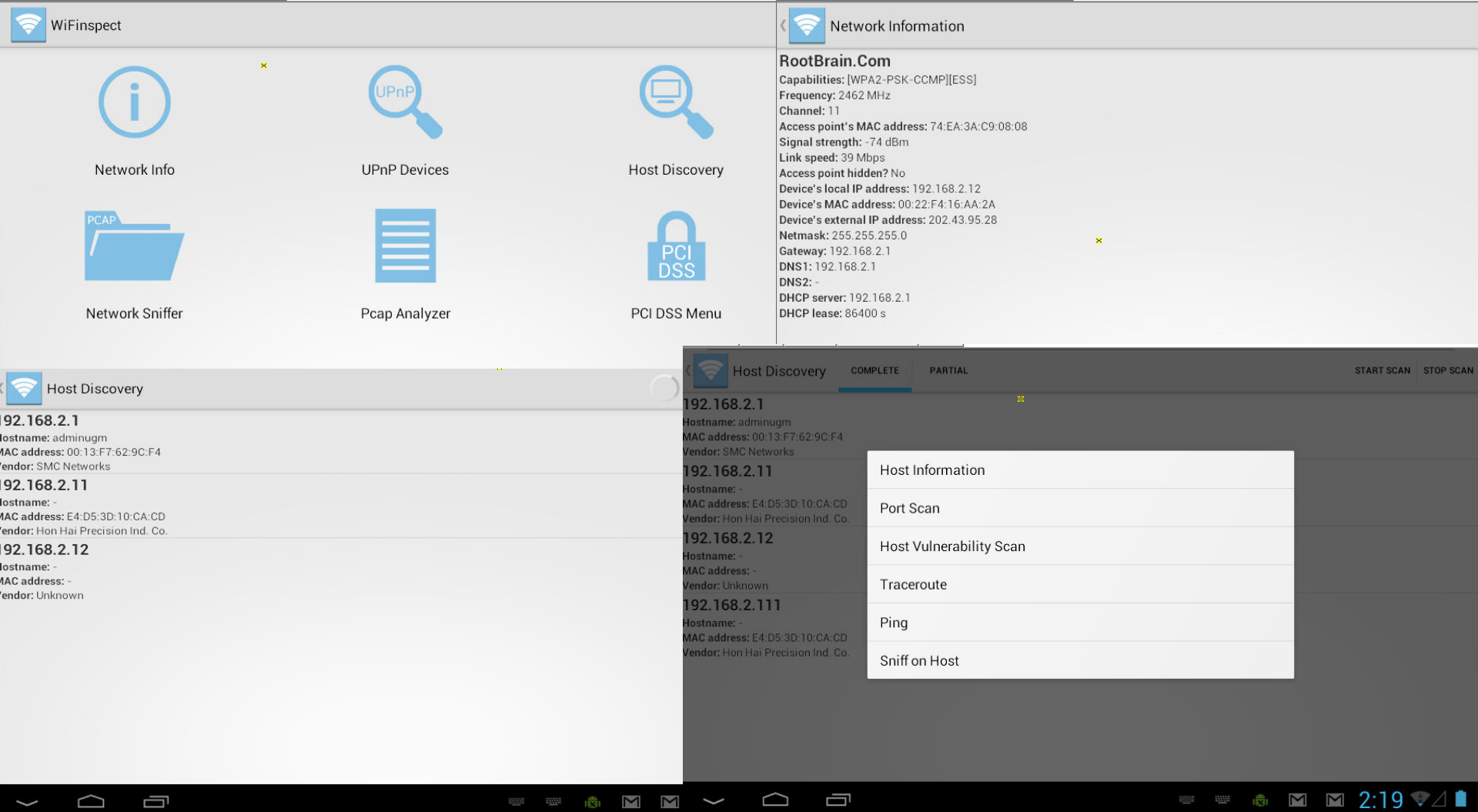
Pentest Tool in Android

◉ Wifilnspect

- 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

WiFinspect



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

The screenshot displays the Fing application interface on an Android device. The top status bar shows the time as 10:10 and battery level at 100%. The app header includes the title 'Fing', a refresh icon, a star icon, and a settings icon. Below the header, the network status is shown as 'RootBrain.Com Wireless network' with a signal strength indicator and '3/3 now'.

The main content area is divided into several sections:

- Network List:** Displays discovered devices. The first device is '192.168.2.1' with the name 'adminugm', manufacturer 'SMC Networks', and MAC address '00:13:F7:62:9C:F4'. The second device is '192.168.2.11 (+1)' with manufacturer 'Hon Hai Precision'.
- Device Detail (192.168.2.11):** Shows a status of 'up' and '6 min ago'. It includes a field to 'Enter a name' and 'Enter additional notes'. A table of device details is shown below:

IP Address	192.168.2.11
MAC Address	E4:D5:3D:10:CA:CD
Vendor	Hon Hai Precision
More IP Addresses	192.168.2.111
First seen	Nov 9 2:21 AM - 6 min ago
Last change	Nov 9 2:21 AM - 6 min ago
Log	
Scan services	
Ping	
Trace route	
Wake on LAN	

- Service Scan:** Shows detected services for the selected device. The scan results are:

Port	Service
23	telnet Telnet
80	http World Wide Web HTTP

The bottom of the screen shows the standard Android navigation bar with back, home, and recent apps icons.

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