GDG DevFest 2014 Season

Thessaloniki

28-30 November 2014

Penetration Testing with Android Devices

Hacking with our pocket device, made easy!

Thomas Sermpinis a.k.a. Cr0wTom

Cr0w’s Place, DeltaHacker Magazine

Introduction :

Powerful Android devices are our daily companion. They are helping us with every type of task. Why not help us with Penetration Testing and everyday ethical hacking.

Why Android?

- Open Platform
- Root Access
- Hardware Reachability
- Top Specs

Prerequisites:

- Android Device (duh?)
- Root Privileges
- Full BusyBox Install
- Some Hardware Knowledge
- Some Programming Knowledge

Disclaimer!

Enterprise Solutions

Professional-grade applications

Zimperium - Introduction

- Founded on 2010
- Mobile Security
- zANTI
- Kevin Mitnick joins in 2012
- Simone Margaritelli (@evilsocket) joins in 2014
- zANTI 2 + zIPS + zConsole

ZIMPERIUM

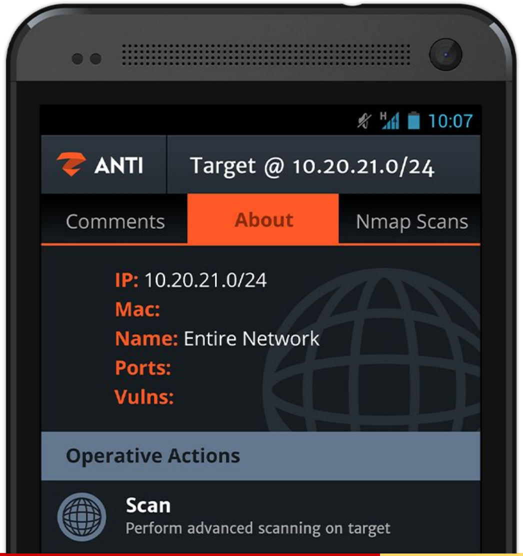
IPS
PROTECTION

CONSOLE
MANAGEMENT

ANTI
DIAGNOSTIC

Zimperium – zANTI 2

- Penetration testing suite
- Free community edition
- Innovative capabilities
- Sync with Zimperiums cloud service
- https://s3.amazonaws.com/zANTI/zANTI2.apk



Target @ 10.20.21.0/24

IP: 10.20.21.0/24
Mac:
Name: Entire Network
Ports:
Vulns:

Operative Actions

Scan
Perform advanced scanning on target

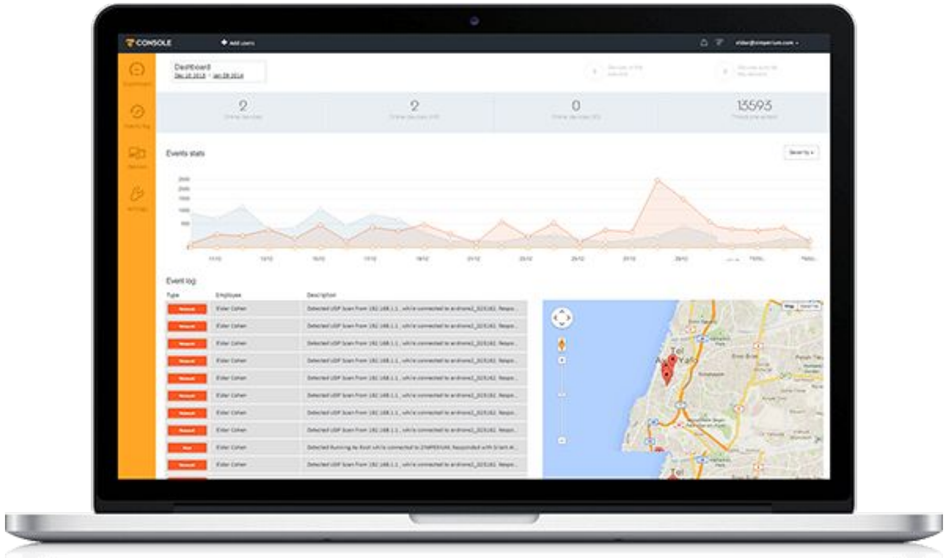
Demo

Let’s see what is all about!

Zimperium – zIPS

- Cloud based service
- Device specific attacks
- Network attacks
- Human based attacks
- Pop-Up windows

Zimperium - zConsole



- A window into advanced mobile threats
- Cloud based
- Online service
- zANTI and zIPS result demonstration

Offensive Security

- Founded 2006
- Backtrack Linux
- Kali linux in 2013
- Kali Linux NetHunter ROM for Android

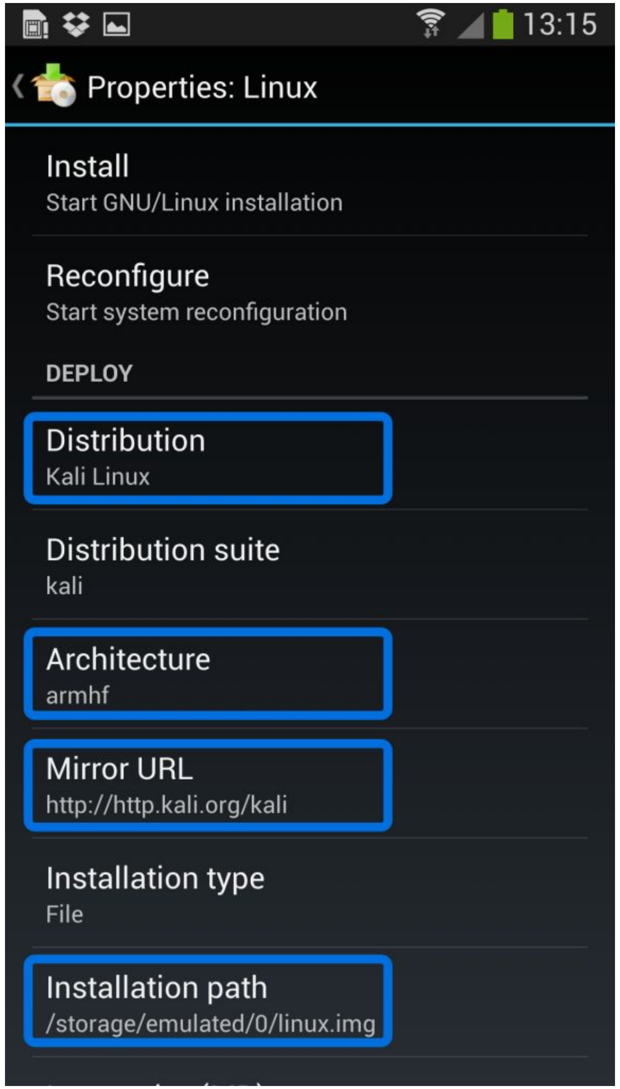
Offensive Security - Kali Linux NetHunter

- Penetration Testing Custom ROM
- Nexus Devices
- 802.11 Wireless Injection
- USB HID Keyboard attacks - BadUSB
- MITM attacks

Offensive Security - Kali Linux NetHunter

Offensive Security – Kali Linux ARM

- Installation with Linux Deploy app
- Complete Linux distribution
- Hardware enchantments
- SSH or VNC connectivity
- Build for ARM devices



13:15

Properties: Linux

Install
Start GNU/Linux installation

Reconfigure
Start system reconfiguration

DEPLOY

Distribution
Kali Linux

Distribution suite
kali

Architecture
armhf

Mirror URL
http://http.kali.org/kali

Installation type
File

Installation path
/storage/emulated/0/linux.img

Applications

Quality hacking applications from random developers

dSploit – Penetration Testing Suite

- **Development stop in 2014**
- Simone Margaritelli (@evilsocket)
- Extensive network scanning
- MITM attacks
- Exploitation with Metasploit Framework

DroidSheep – DroidSheep Guard

- Simplicity
- Session hijacking fast and easy
- Safety from session hijacking with DroidSheep Guard
- Android ARP-Table monitoring

Demo

Let’s see what is all about!

Shark for Android (Shark for Root)

- Network traffic sniffer
- Works on 3G and WiFi
- Based on tcpdump tool
- Dump file can be viewed in Wireshark

WiFi Protocol Cracking

WEP, WPA/WPA2 , WPS Cracking

Monitor Mode Hardware

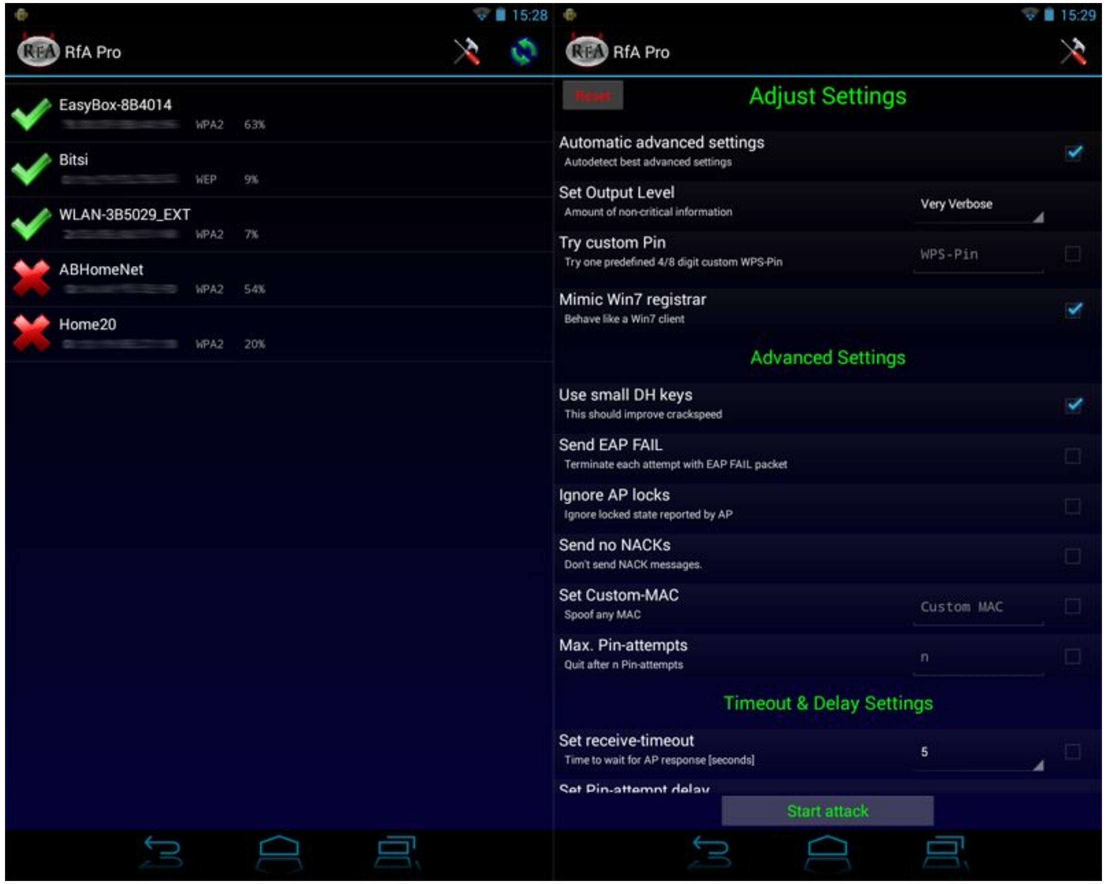
- bcm4329/4330 internal wifi chipset
- Many external cards over OTG cable (RTL8187 chipset)
- Kernel Integration

Aircrack-NG Suite

- 802.11 WEP and WPA-PSK key recovery
- Cross-Platform
- Variety of attacks
- GPU implementation
- Internal or external chipset support
- Runs in terminal emulators

Reaver-GUI for Android

- Graphic User Interface
- WPA(2) Key recovery via WPS vulnerability
- Wide range of chipset support
- 2-10 hours key recovery
- Bcmon = companion app



✓ EasyBox-8B4014 [redacted] WPA2 63%

✓ Bitsi [redacted] WEP 9%

✓ WLAN-3B5029_EXT [redacted] WPA2 7%

✗ ABHomeNet [redacted] WPA2 54%

✗ Home20 [redacted] WPA2 20%

Adjust Settings

Automatic advanced settings – Autodetect best advanced settings ☑

Set Output Level – Amount of non-critical information: Very Verbose

Try custom Pin – Try one predefined 4/8 digit custom WPS-Pin: WPS-Pin ☐

Mimic Win7 registrar – Behave like a Win7 client ☑

Advanced Settings

Use small DH keys – This should improve crackspeed ☑

Send EAP FAIL – Terminate each attempt with EAP FAIL packet ☐

Ignore AP locks – Ignore locked state reported by AP ☐

Send no NACKs – Don't send NACK messages. ☐

Set Custom-MAC – Spoof any MAC: Custom MAC ☐

Max. Pin-attempts – Quit after n Pin-attempts: n ☐

Timeout & Delay Settings

Set receive-timeout – Time to wait for AP response [seconds]: 5 ☐

Set Pin-attempt delay

Questions?

Thank you for listening!

http://cr0wsplace.wordpress.com

e-mail: cr0wsplace1993 [at] gmail [dot] com
YouTube Channel: https://www.youtube.com/channel/Cr0wsPlace
DeltaHacker.gr

Google
Developers