Paphos Group

Paphos Group
Risk & Security

Mobile App Security Testing

Gert Huisman
gert.huisman@paphosgroup.com

Introductie

- 10 jaar werkzaam geweest voor Achmea als Software Engineer
- 3 jaar als Security Tester
- Security Assessments op Netwerken en Web Applicaties

- Juni 2012 begonnen bij de Paphos Group als Security Consultant

Achtergrond

- Infrastructuur meestal wel op orde (firewalls, IDS/IPS e.d.)
- Focus werd door hackers verlegd naar Netwerk en Webapplicaties
- Mobiele applicaties worden steeds populairder
- Security testing van apps staat nog in de kinderschoenen

Referentiekader

- Nog geen standaard policies voor mobile apps
- PCI Mobile Payment Security Guidelines
- Development Security Guidelines (iOS, Android)
- Frameworks (ASEF, Mercury)
- Paphos Security Best Practices

Terminologie

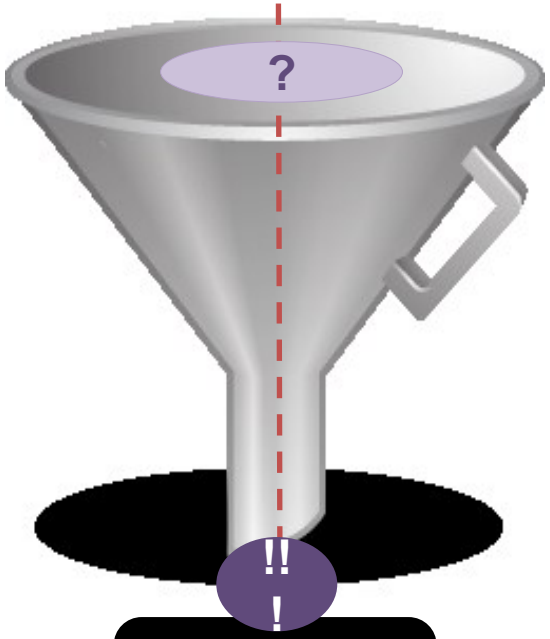
- Statische Code Analyse (Vulnerabilities)
  - Source code
- Vulnerability Scan (Vulnerabilities)
  - Netwerkomgeving (i.e. web- en applicatie servers, databases)
- Penetratie Test (Exploits)
  - Validatie van exploits
- CVSS Score
  - Op basis van complexiteit van vulnerability
  - CVE (Common Vulnerabilities & Exposures) http://cve.mitre.org

Risico differentiatie

Potentieel Risico

Vulnerability scan resultaten
75 vulnerabilities

Mogelijk te misbruiken



Reëel Risico

Penetratie test
8 exploits

Bewezen te misbruiken

Security Testing

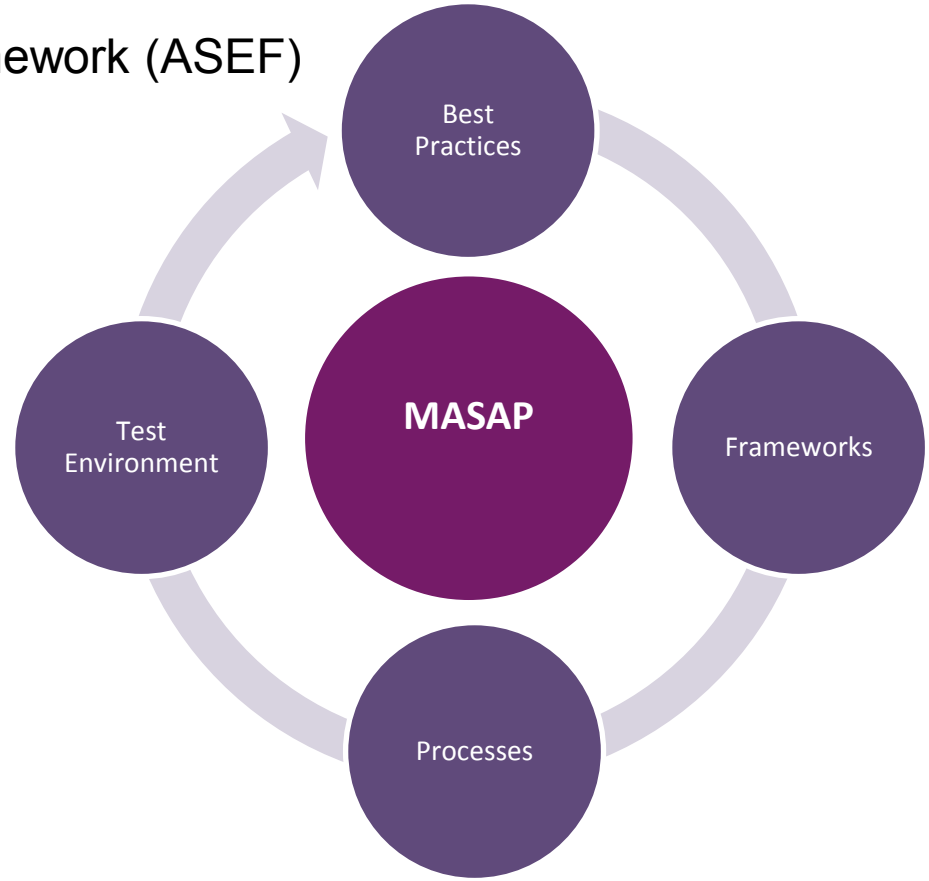
- **Methodiek**
  - Systems: Information Systems Security Assessment Framework (ISSAF)
  - (Web)Applications: OWASP Application Security Verification Standard (ASVS)
  - Penetration tests: Combinatie van ISSAF en ASVS
  - Mobile Apps: MASAP

- **Verificatie**
  - OWASP Top 10
  - OWASP Mobile Top 10 Risks (Nieuw!)

- **Proces**
  - Service Validation & Testing (SVT)

Testmethodiek Mobile Apps

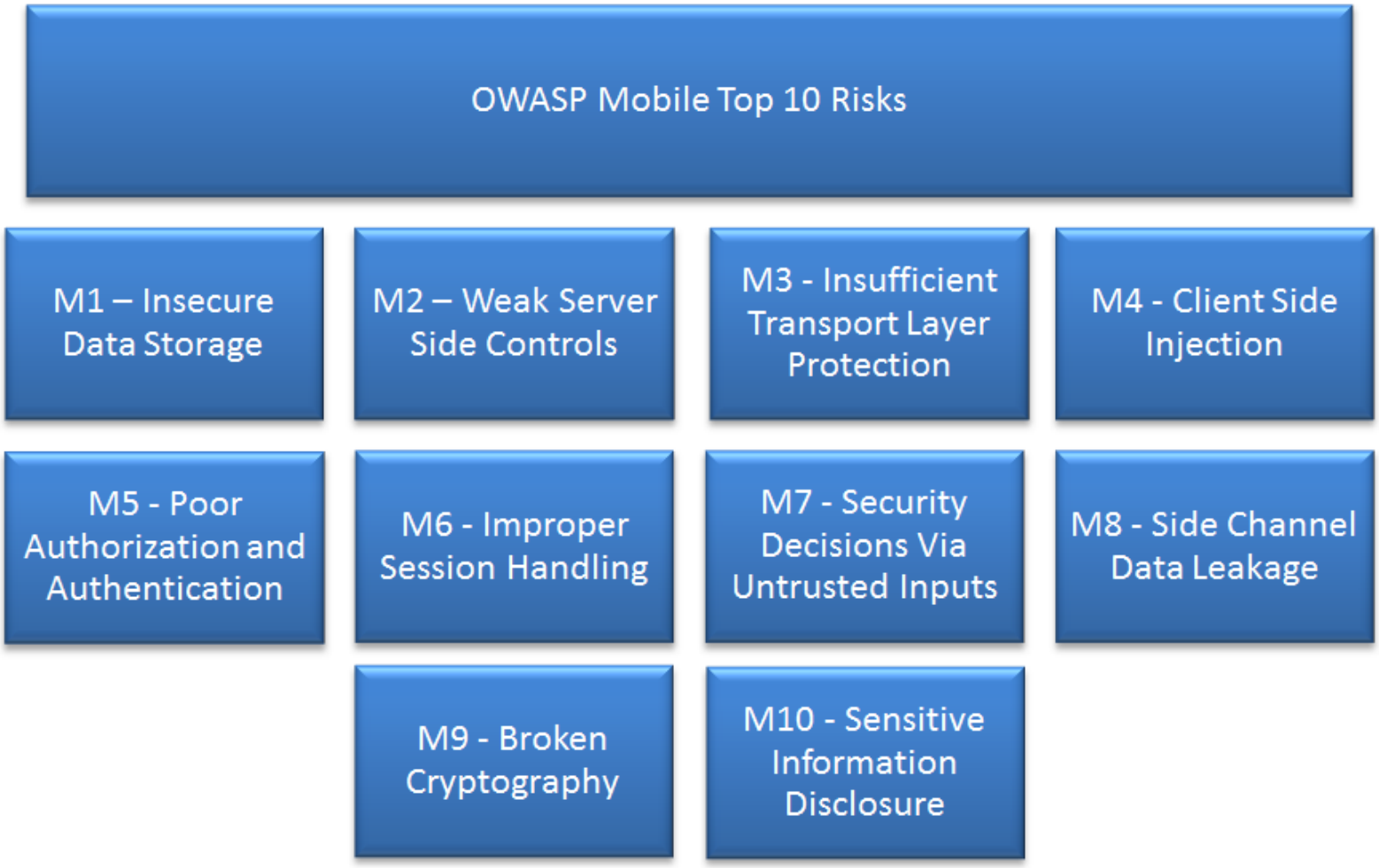
- **Frameworks**
  - Android Security Evaluation Framework (ASEF)
  - Mercury
- **Best Practices**
  - Secure Development Guides
  - Paphos Best Practices
- **Policies**
  - PCI Standards
  - OWASP Mobile Top 10 Risks



Voorbeelden van vulnerabilities

- Geen gebruik maken van SSL (HTTPS)
- Connectie maken met kwaadaardige sites (Malware)
- Lokaal opslaan van gevoelige data (NAW, bankgegevens)
- Geen toestemming aan gebruiker vragen (GPS, camera, SMS)

OWASP Mobile Top 10 Risks



Op welke devices testen?

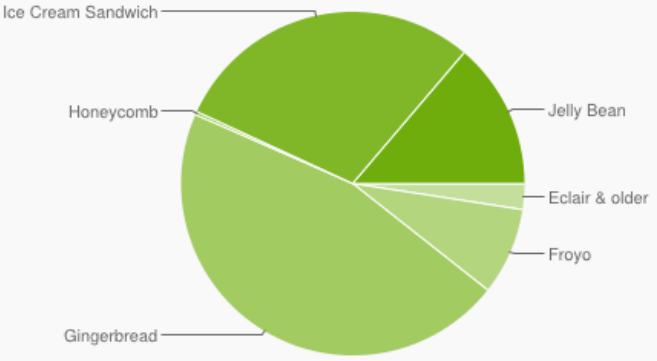
- **Smartphones**
  - o.a. Samsung Galaxy, Sony Xperia, LG (Android)
  - Apple iPhone (iOS)
  - o.a. Nokia Lumia 920, HTC 8X, Samsung ATIV S (Windows 8)

- **Tablets**
  - Apple (iPad)
  - o.a. Samsung Galaxy Tab, Asus Transformer (Android)
  - o.a. Acer Iconia, Asus Taichi, Dell XPS (Windows 8)

Op welke OS versie testen?

- Android
  - Gingerbread (3.6)
  - Ice Cream Sandwich (ICS) (4.0)
  - Jelly Bean (4.1 and higher)
- iOS
  - 5.1
  - 6.0.1
  - 6.1
- Windows 8
  - Basic
  - Pro
  - RT en Enterprise

Version	Codename	API	Distribution
1.6	Donut	4	0.2%
2.1	Eclair	7	2.2%
2.2	Froyo	8	8.1%
2.3 - 2.3.2	Gingerbread	9	0.2%
2.3.3 - 2.3.7		10	45.4%
3.1	Honeycomb	12	0.3%
3.2		13	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	29.0%
4.1	Jelly Bean	16	12.2%
4.2		17	1.4%



Data collected during a 14-day period ending on February 4, 2013

Hoe en wat testen?

- Source code (eventueel decompileren)
- Code review
- Configuratiebestanden (soms binair)
- Systeemrechten van de app

- Netwerkverkeer analyseren
- Databases (lokaal of op server)
- Achterliggende web- of applicatieserver (standaard security scans)

Testomgeving

- Mac OS X (virtual) machine (Xcode)
- Backtrack 5 (virtual) machine (Android SDK)

- Test device met geïnstalleerde app
- Root of admin rechten op het device (jailbreak of rooten)
- Noodzakelijk om álle bestanden te kunnen zien
- Zonder restricties applicaties installeren

Voorbeeld van analyse netwerkverkeer

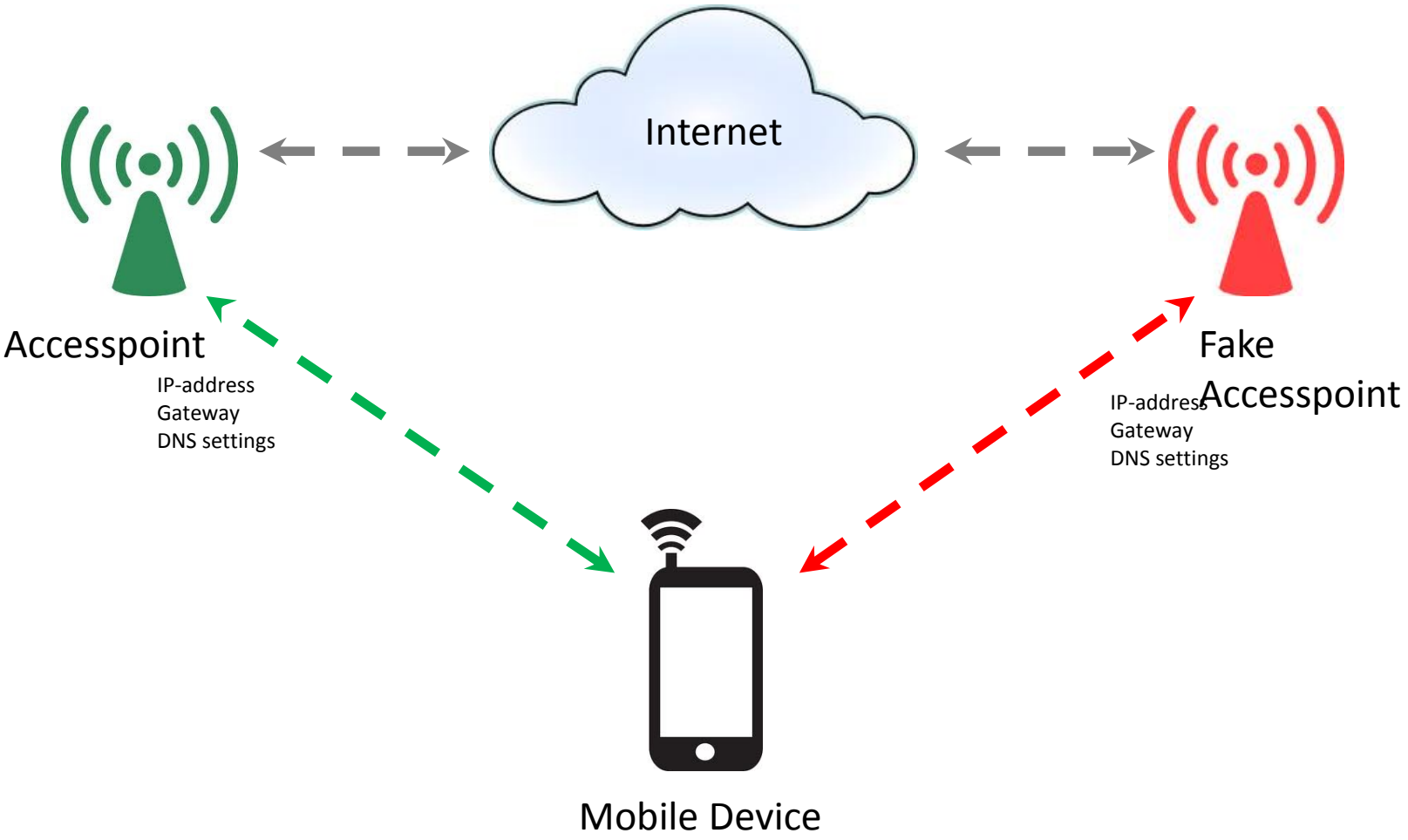
- Test device (Android) met app geïnstalleerd
- Testomgeving (Backtrack)
- Proxy (BurpSuite)
- Wireshark

- Probleem: Android apps en proxy
- Oplossing: Fake accesspoint

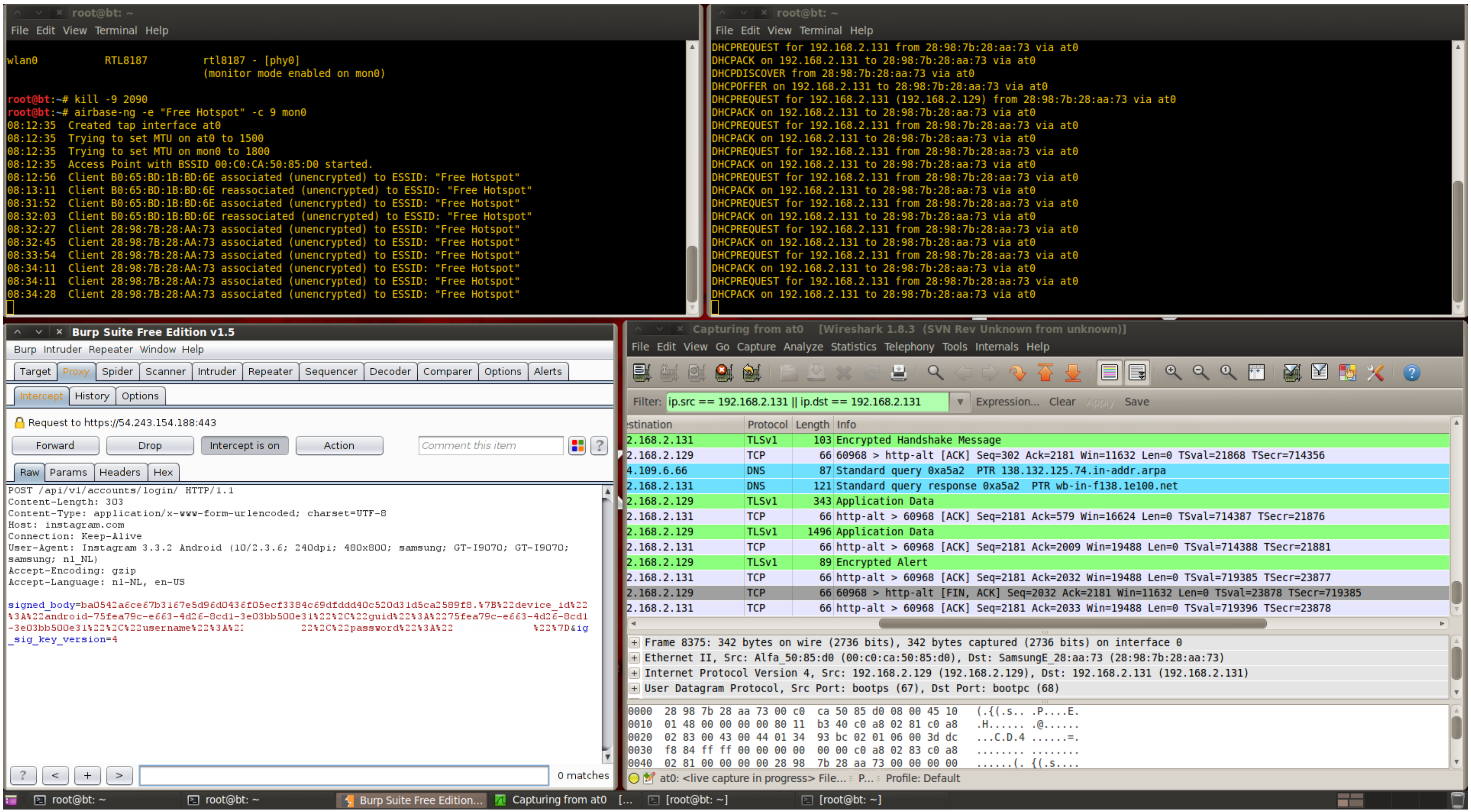
Fake Accesspoint

- (Virtuele) Linux machine (Backtrack)
- Aircrack-ng
- USB WiFi Netwerkkaart
- DHCP Server
- Verbinding met internet
- WireShark
- Burpsuite Proxy

Fake Accesspoint (vervolg)



Resultaat



root@bt: ~
File Edit View Terminal Help
wlan0 RTL8187 rtl8187 - [phy0]
(monitor mode enabled on mon0)
root@bt:~# kill -9 2090
root@bt:~# airbase-ng -e "Free Hotspot" -c 9 mon0
08:12:35 Created tap interface at0
08:12:35 Trying to set MTU on at0 to 1500
08:12:35 Trying to set MTU on mon0 to 1800
08:12:35 Access Point with BSSID 00:C0:CA:50:85:D0 started.
08:12:56 Client B0:65:BD:1B:BD:6E associated (unencrypted) to ESSID: "Free Hotspot"
08:13:11 Client B0:65:BD:1B:BD:6E reassociated (unencrypted) to ESSID: "Free Hotspot"
08:31:52 Client B0:65:BD:1B:BD:6E associated (unencrypted) to ESSID: "Free Hotspot"
08:32:03 Client B0:65:BD:1B:BD:6E reassociated (unencrypted) to ESSID: "Free Hotspot"
08:32:27 Client 28:98:7B:28:AA:73 associated (unencrypted) to ESSID: "Free Hotspot"
08:32:45 Client 28:98:7B:28:AA:73 associated (unencrypted) to ESSID: "Free Hotspot"
08:33:54 Client 28:98:7B:28:AA:73 associated (unencrypted) to ESSID: "Free Hotspot"
08:34:11 Client 28:98:7B:28:AA:73 associated (unencrypted) to ESSID: "Free Hotspot"
08:34:11 Client 28:98:7B:28:AA:73 associated (unencrypted) to ESSID: "Free Hotspot"
08:34:28 Client 28:98:7B:28:AA:73 associated (unencrypted) to ESSID: "Free Hotspot"
root@bt: ~
File Edit View Terminal Help
DHCPREQUEST for 192.168.2.131 from 28:98:7b:28:aa:73 via at0
DHCPACK on 192.168.2.131 to 28:98:7b:28:aa:73 via at0
DHCPDISCOVER from 28:98:7b:28:aa:73 via at0
DHCPOFFER on 192.168.2.131 to 28:98:7b:28:aa:73 via at0
DHCPREQUEST for 192.168.2.131 (192.168.2.129) from 28:98:7b:28:aa:73 via at0
DHCPACK on 192.168.2.131 to 28:98:7b:28:aa:73 via at0
Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept History Options
Request to https://54.243.154.188:443
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /api/v1/accounts/login/ HTTP/1.1
Content-Length: 303
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Host: instagram.com
Connection: Keep-Alive
User-Agent: Instagram 3.3.2 Android (10/2.3.6; 240dpi; 480x800; samsung; GT-I9070; GT-I9070; samsung; nl_NL)
Accept-Encoding: gzip
Accept-Language: nl-NL, en-US
signed_body=ba0542a6ce67b3167e5d96d0436f05ecf3384c69dfddd40c520d31d5ca2589f8.%7B%22device_id%22%3A%22android-75fea79c-e663-4d26-8cd1-3e03bb500e31%22%2C%22guid%22%3A%2275fea79c-e663-4d26-8cd1-3e03bb500e31%22%2C%22username%22%3A%22 %22%2C%22password%22%3A%22 %22%7D&ig_sig_key_version=4
0 matches
Capturing from at0 [Wireshark 1.8.3 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.src == 192.168.2.131 || ip.dst == 192.168.2.131
Expression... Clear Apply Save
Destination Protocol Length Info
2.168.2.131 TLSv1 103 Encrypted Handshake Message
2.168.2.129 TCP 66 60968 > http-alt [ACK] Seq=302 Ack=2181 Win=11632 Len=0 TSval=21868 TSecr=714356
4.109.6.66 DNS 87 Standard query 0xa5a2 PTR 138.132.125.74.in-addr.arpa
2.168.2.131 DNS 121 Standard query response 0xa5a2 PTR wb-in-f138.1e100.net
2.168.2.129 TLSv1 343 Application Data
2.168.2.131 TCP 66 http-alt > 60968 [ACK] Seq=2181 Ack=579 Win=16624 Len=0 TSval=714387 TSecr=21876
2.168.2.129 TLSv1 1496 Application Data
2.168.2.131 TCP 66 http-alt > 60968 [ACK] Seq=2181 Ack=2009 Win=19488 Len=0 TSval=714388 TSecr=21881
2.168.2.129 TLSv1 89 Encrypted Alert
2.168.2.131 TCP 66 http-alt > 60968 [ACK] Seq=2181 Ack=2032 Win=19488 Len=0 TSval=719385 TSecr=23877
2.168.2.129 TCP 66 60968 > http-alt [FIN, ACK] Seq=2032 Ack=2181 Win=11632 Len=0 TSval=23878 TSecr=719385
2.168.2.131 TCP 66 http-alt > 60968 [ACK] Seq=2181 Ack=2033 Win=19488 Len=0 TSval=719396 TSecr=23878
Frame 8375: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Alfa_50:85:d0 (00:c0:ca:50:85:d0), Dst: SamsungE_28:aa:73 (28:98:7b:28:aa:73)
Internet Protocol Version 4, Src: 192.168.2.129 (192.168.2.129), Dst: 192.168.2.131 (192.168.2.131)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
at0: <live capture in progress> File... P... Profile: Default
root@bt: ~ root@bt: ~ Burp Suite Free Edition... Capturing from at0 [... [root@bt: ~] [root@bt: ~]

Uitdagingen

- Automatiseren van tests
- Policies
- Reguleren van aanbod uit Markets/Stores
- Near Field Communication (NFC)
- Nieuwe mobile OS’s

Vragen

Paphos Group

VRAGEN?