

Wireless Network Risks and Controls

Offensive Security Tools, Techniques, and Defenses

22 January 2015 – ISACA Phoenix Chapter – Phoenix, AZ



Presented by:
Ruihai Fang
Dan Petro
Bishop Fox
www.bishopfox.com

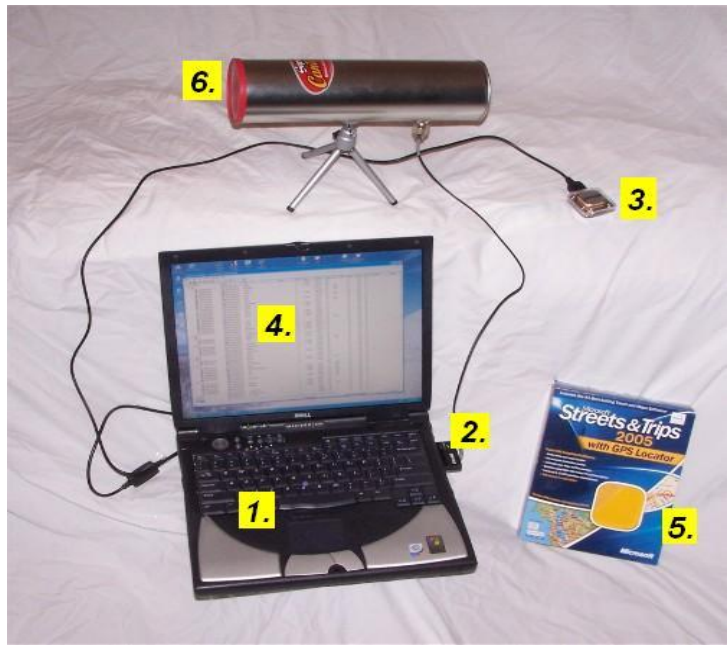


Introduction/Background

GETTING UP TO SPEED

Used to be a Pain

Lots to of heavy things to carry



let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid bandwidth
CLOSED NODE	ssid
WEP NODE	ssid access contact bandwidth

blackbeltjones.com/warchalking

Kali VM and USB Adapter

NOW EASY

- Kali Linux VM + TP-LINK - TL-WN722N (USB)



```
root@kali: ~
File Edit View Search Terminal Help
CH 4 ][ Elapsed: 52 s ][ 2013-11-05 18:29
CH 8 ][ Elapsed: 1 min ][ 2013-11-05 18:29

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
66:2A:2F:53:7C:99 -1    92         0   0  11  11  OPN             SETUP
08:3F:0E:73:AB:8F -59    4         0   0   4  54e  WEP            sport
E0:46:9A:4E:5C:57 -69    3         0   0   3  54e  WPA2  COMP  PSK  NETGEAR09
62:60:66:B2:81:99 -69   10         0   0  11  54e  WPA2  COMP  PSK  testing
5C:96:90:69:02:6B -70   41        15   0   6  54e  WPA2  COMP  PSK  bleh_5GHz
20:09:00:25:96:C5 -74   26        216  0   6  54e  WPA2  COMP  PSK  bleh_dlink
68:7F:74:CF:78:2E -74   22         0   0   6  54e  WPA2  COMP  PSK  Buttons
00:23:75:2A:B4:80 -70   39         3   0   1  54  WPA2  COMP  PSK  bleh
EC:1A:59:85:09:6C -76    8         0   0  11  54e  WPA2  COMP  PSK  LOMBARDI
00:16:B6:0C:DD:F3 -78   35         0   0  11  54  WPA2  COMP  PSK  MonkeyDo
00:00:00:00:00:00 -81   47         1   0   1  54  WPA  WEP    <length: 0>
00:24:7B:60:57:2C -82   14         0   0   1  54  WPA2  COMP  PSK  myquest3771
00:17:3F:03:D0:64 -84   13         7   0  11  54  WEP    WEP    TheBonerPalace
EC:1A:59:85:09:6F -84    8         0   0  11  54e  OPN             0...
08:86:3B:D7:00:D0 -99   12         8   0  11  54e  WPA2  COMP  PSK  be!kin.0d0
43:E1:DD:EB:85:AD -1    0         0   0   -1 -1
00:C1:C0:DF:4F:EE -74    3         0   0   6  54e  OPN             Cnet-guest
00:C1:C0:DF:4F:ED -72    4         0   0   6  54e  WPA2  COMP  PSK  Cnet

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
66:2A:2F:53:7C:99 00:80:92:86:6D:48 -87  0 - 1  227    94
(not associated)  24:77:03:26:9C:70 -36  0 - 1  0     14  bleh_5GHz
(not associated)  00:17:C4:47:41:AE -83  0 - 1  0     2
(not associated)  84:A6:C8:41:7F:26 -83  0 - 1  0     1
(not associated)  94:94:26:E8:F1:73 -86  0 - 1  0     1  bleh_5GHz
(not associated)  00:80:48:72:85:72 -69  0 - 1  0     1  KSD Bus
62:6C:66:B2:81:99 6C:88:14:62:A9:94 -82  0 - 6e 0     5  testing
```

Laptops, Netbooks (easier to conceal), and adapters



TP-Link Adapter
Capable of attaching a
YAGI antenna

Asus EEPc



YAGI Antennas – Directional

Very good for attacking from a distance, like from the comfort of your hotel room.



Antenna Connector Cables are Necessary



WiFi Hacking Using Android Phones



StarTech Micro USB
On-the-go Adapter



Samsung Galaxy S3



Alfa 1000mW 1W 802.11b/g USB
WiFi Adapter. Uses RTL8187 Chipset.



Wireless Hacking Tools

ACROSS VARIOUS OS'S

Wireless Tools

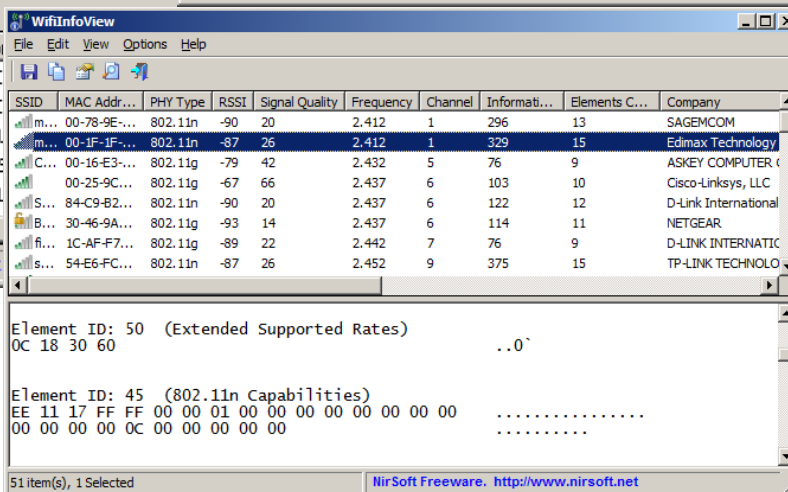
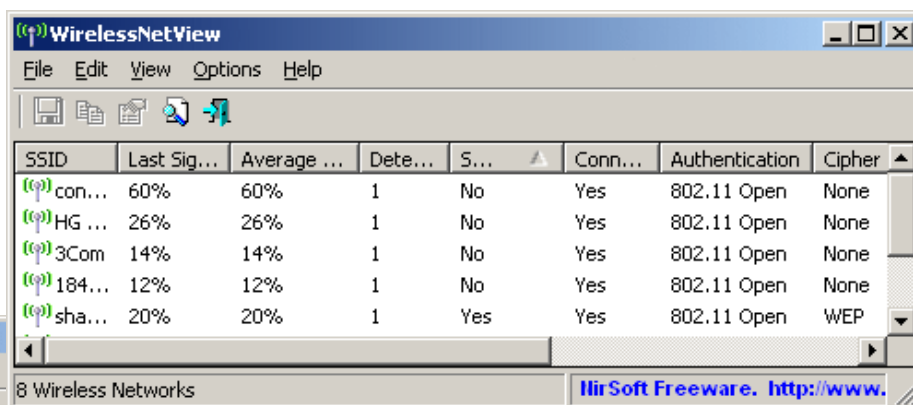
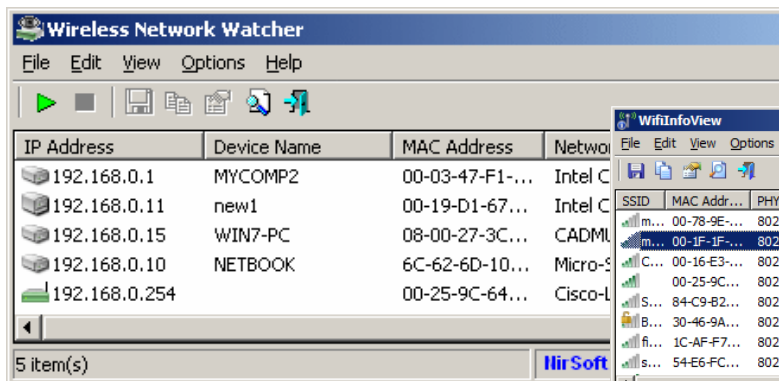
Discovery

- Supported operating systems
- Supported wireless protocols
- Active vs. passive scanning
- Packet capturing and decoding
- Distinguishes between AP, ad hoc, and client devices
- Statistics and reporting capabilities
- User interface
- Price

NirSoft Wireless Tools

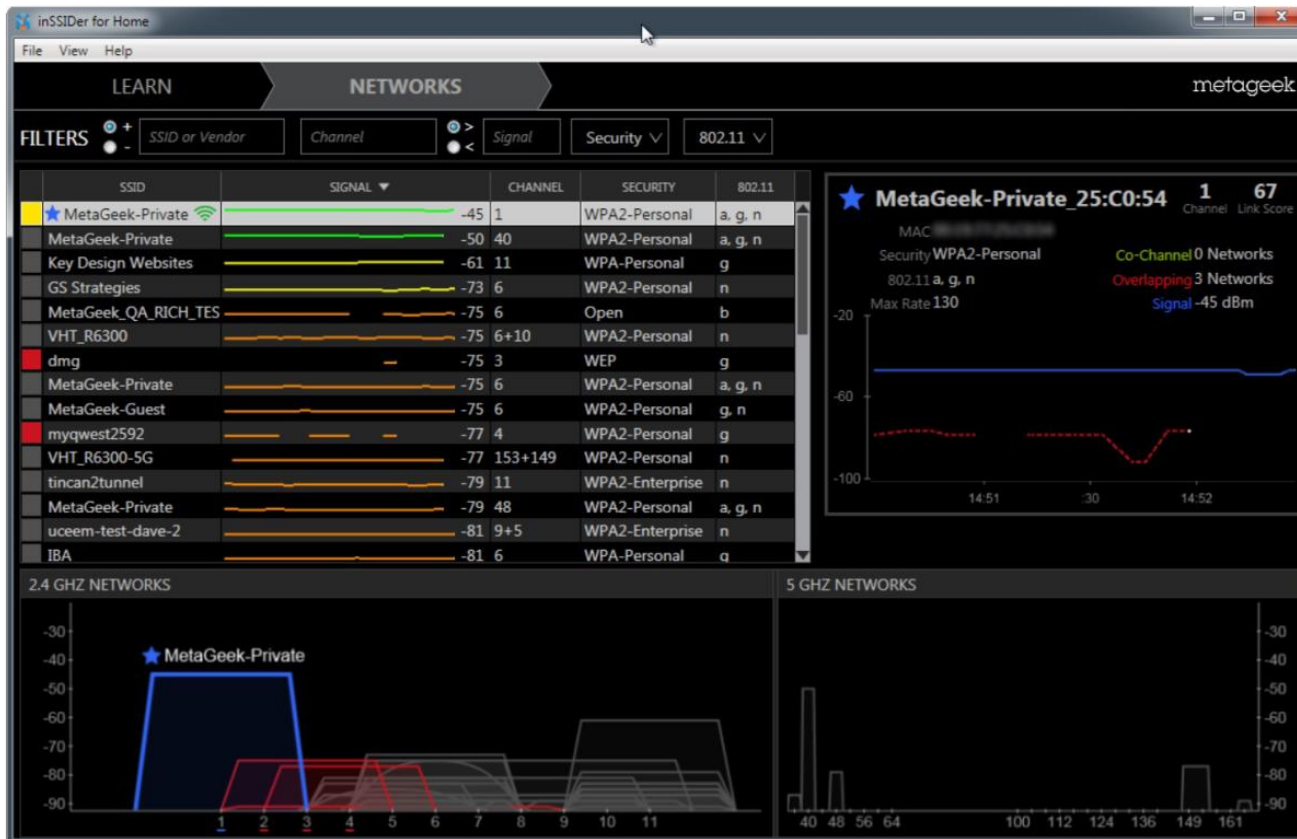
WINDOWS HACKING TOOLS

- NirSoft – WirelessNetView
- NirSoft – WifiInfoView
- NirSoft - Wireless Network Watcher



inSSIDer Wi-Fi Scanner

WINDOWS HACKING TOOLS



Aircrack-ng Suite

LINUX HACKING TOOLS

The aircrack-ng software suite includes:

Name	Description
aircrack-ng	Cracks WEP and WPA (Dictionary attack) keys.
airdecap-ng	Decrypts WEP or WPA encrypted capture files with known key.
airmon-ng	Placing different cards in monitor mode.
aireplay-ng	Packet injector (Linux, and Windows with CommView drivers).
airodump-ng	Packet sniffer : Places air traffic into PCAP or IVS files and shows information about networks.
airtun-ng	Virtual tunnel interface creator.
packetforge-ng	Create encrypted packets for injection.
ivstools	Tools to merge and convert.
airbase-ng	Incorporates techniques for attacking client, as opposed to Access Points
airdecloak-ng	removes WEP cloaking from pcap files
airdriver-ng	Tools for managing wireless drivers
airolib-ng	stores and manages ESSID and password lists and compute Pairwise Master Keys
airserv-ng	allows you to access the wireless card from other computers.
buddy-ng	the helper server for easside-ng, run on a remote computer
easside-ng	a tool for communicating to an access point, without the WEP key
tkiptun-ng	WPA/TKIP attack
wesside-ng	automatic tool for recovering wep key.

Kismet

LINUX HACKING TOOLS

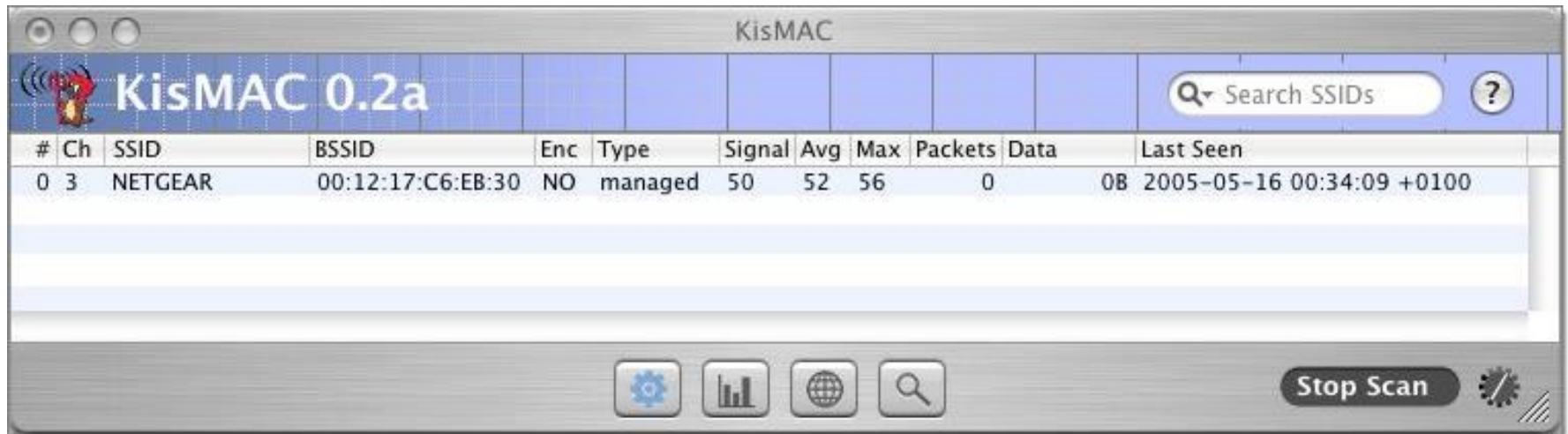
```
Kismet Sort View Windows
Name BSSID T C Ch Freq Pkts Size Bcn% Sig Clnt Manuf Cty Seen By
TRENDnet 00:14:D1:5F:97:12 A 0 1 2417 1 0B --- --- 1 TrendwareI --- wlan0
linksys_SES_45997 00:16:B6:1B:E4:FF A 0 6 2432 1 0B 10% -78 1 Cisco-Link --- wlan0
Autogroup Probe 00:13:E8:92:3F:CB P N --- ---- 2 0B --- 0 1 IntelCorpo --- wlan0
linksys 00:1A:70:D9:BC:13 A N 6 2437 2 0B 10% -86 1 Cisco-Link --- wlan0
WPA41 00:1F:90:E6:E0:84 A W 11 2462 3 0B --- -86 1 ActiontecE --- wlan0
6SI03 00:1F:90:FA:F4:C8 A W --- 2412 3 0B --- -83 1 ActiontecE --- wlan0
TFS 00:09:5B:D7:9D:B2 A N --- 2462 4 0B --- -68 1 Netgear --- wlan0
Xu Chen 00:18:01:F9:70:F0 A N 6 2437 4 0B 0% -75 1 ActiontecE US wlan0
TK421 00:18:01:FE:68:77 A 0 6 2437 4 0B --- -79 1 ActiontecE --- wlan0
meskas 00:18:01:F5:65:E1 A 0 11 2462 5 0B 10% -71 1 ActiontecE US wlan0
Elina-PC-Wireless 00:24:B2:0E:E6:E2 A 0 11 2462 7 0B 10% -45 1 Netgear --- wlan0
7J4R0 00:1F:90:E6:04:E1 A W 11 2462 7 0B --- -80 1 ActiontecE --- wlan0
Pickles 00:1F:33:F3:C5:4A A 0 2 2422 8 0B --- -75 1 Netgear --- wlan0
BSSID: 00:1F:33:F3:C5:4A Crypt: TKIP WPA PSK AESCCM Manuf: Netgear SeenBy: wlan0
38c8 00:16:CE:07:60:77 A W 6 2447 19 0B --- -82 1 HonHaiPrec --- wlan0
Danish_Penguin 00:13:10:35:59:CB A W 9 2462 331 2K 50% -32 5 Cisco-Link --- wlan0

No GPS info (GPS not connected)
45
0
Packets
Data

INFO: Detected new probe network "Danish_Penguin", BSSID 00:13:E8:92:3F:CB, encryption no, channel 0, 60.00 mbit
ERROR: Could not connect to the spectools server localhost:30569
INFO: Detected new managed network "linksys_SES_45997", BSSID 00:16:B6:1B:E4:FF, encryption yes, channel 6, 54.00 mbit
INFO: Detected new managed network "linksys", BSSID 00:1A:70:D9:BC:13, encryption no, channel 6, 54.00 mbit
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
wlan0
9
```

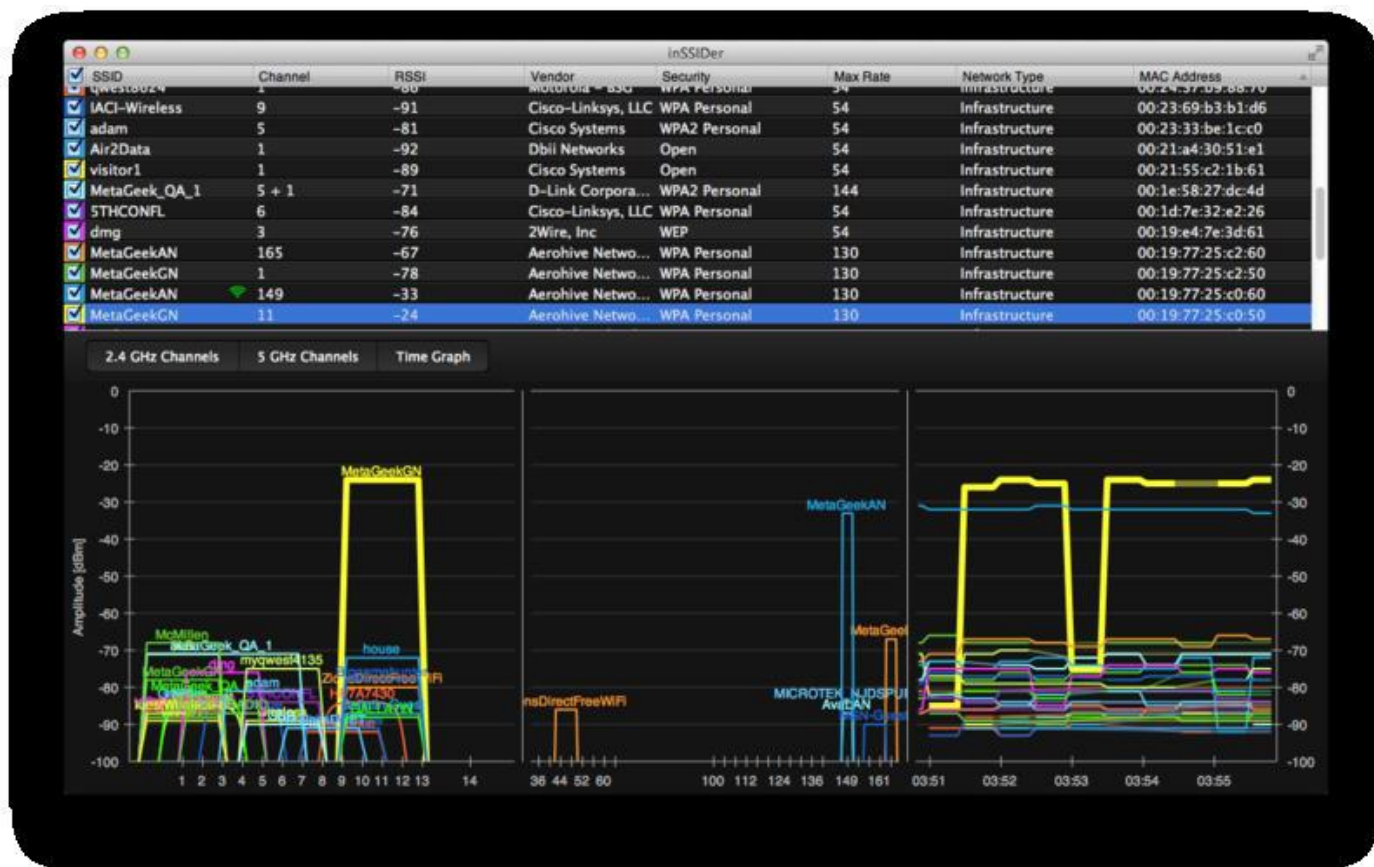
Kismac

MAC OS X HACKING TOOLS



inSSIDer for Mac

MAC OS X HACKING TOOLS





WiFi Pineapple

WIRELESS PENETRATION TESTING ROUTER

Features

WHAT CAN IT DO?

- Wireless Jamming (De-auth Attack)
- Man-in-the-Middle attack
- DNS Spoof on lure client
- Web base management
- Tether via Mobile Broadband
- Battery power and portable



Specs

THE HARDWARE

- Atheros AR9331 SoC at 400MHz
- 802.11 b/g/n 150 Mbps wireless
- 2x Ethernet, one PoE (Power-Over-Ethernet) capable
- USB 2.0 for expanded storage, WiFi Interface and Mobile Broadband
- Fast Linux Kernel 3.2 based Jasager Firmware

Methodology

Social Engineering

1. Karma (Rogue AP)

2. DNS Spoof & MITM

3. Phishing

Auto-Association

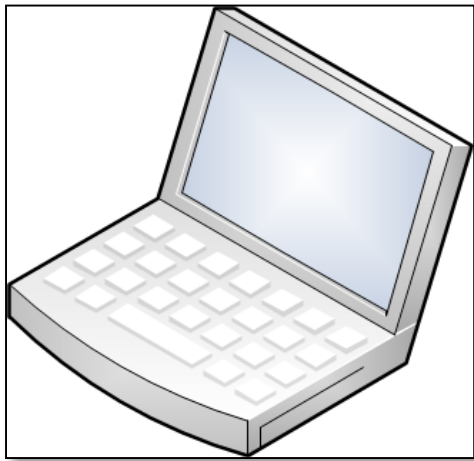
PROBLEM TO EXPLOIT



Karma

HOW DOES IT WORK?

- **Listen** to wireless probes from nearby wireless devices
- **Impersonate** as the requested wireless AP



I'm looking for
"Starbucks"



That's me. Let's connect.

Karma

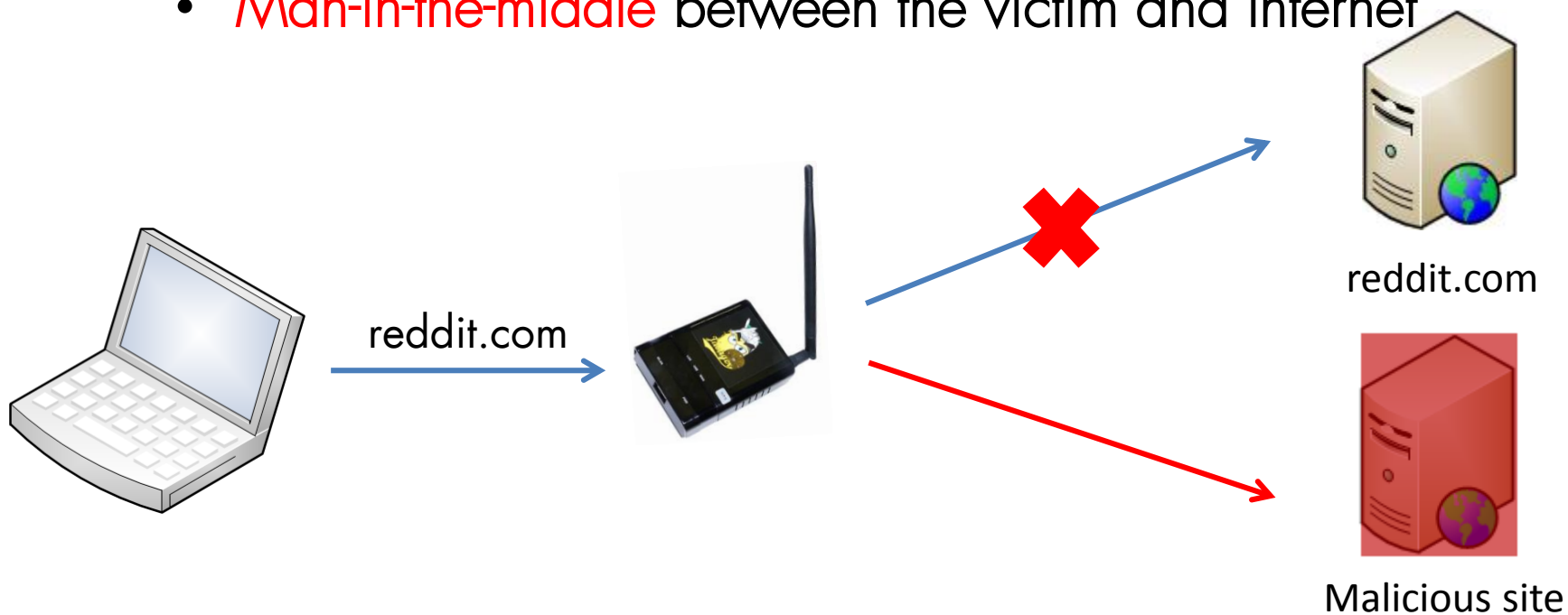
ROGUE AP



DNS Spoof

POISONING YOUR DNS

- **Modify** DNS records and point to a malicious site
- **Man-in-the-middle** between the victim and Internet



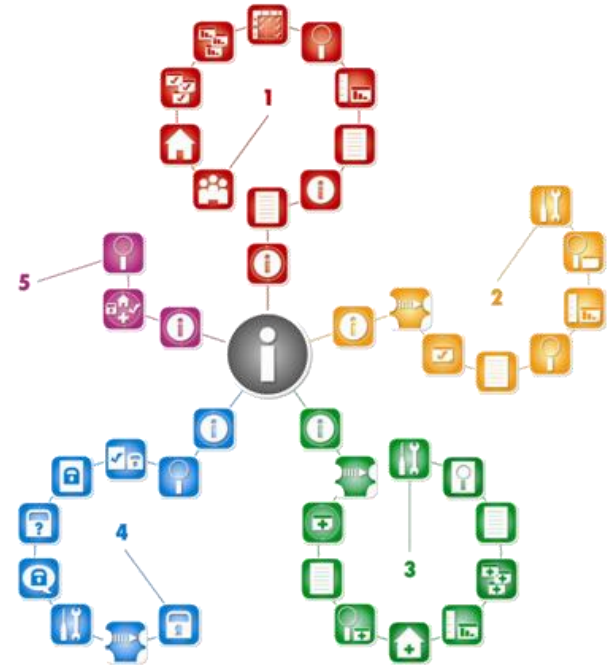
Phishing

PHISHING ATTACK

- **Clone** the official website (reddit.com)
- Implement **key logger**
- Deploy **malware** or **backdoor** on the forged website
- **Compromise** the victim



DEMO



Mitigation

Things that you should be doing

1. **Disable** the "Connect Automatically" setting on all unsecured wireless networks.
2. Use **DNS Crypt** or **Google DNS**
3. **Don't** connect to any unsecured or unknown wireless network
4. Use a trusted **VPN tunnel** to encrypt the traffic on public network

Raspberry Pi

FRUITY WIFI



- Raspberry Pi – cheap alternative (~\$35)
 - Fruity WiFi – Raspberry Pi version of the WiFi Pineapple

```
status | config | modules | logs | logout | v1.6

Services
Wireless enabled. | stop
Supplicant disabled. | start | edit
  Karma enabled. | stop
URL Snarf enabled. | stop
DNS Spoof enabled. | stop
  Kismet disabled. | start | edit
  Squid disabled. | start | edit
sslstrip enabled. | stop

Interfaces/IP
eth0:
wlan0: 10.0.0.1
public: reveal ip

Stations

DHCP
```



Easy-creds

AUTOMATING WIFI CLIENT ATTACKS

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
#####  ##  #####  #  #  #####  #####  #####  #####  #####
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#####  #  #  #####  #  #####  #  #  #  #####  #  #  #####
#  #####  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#####  #  #  #####  #  #####  #  #  #  #####  #####  #####
EASY-CREDS Version 3.1-DEV - 12202010

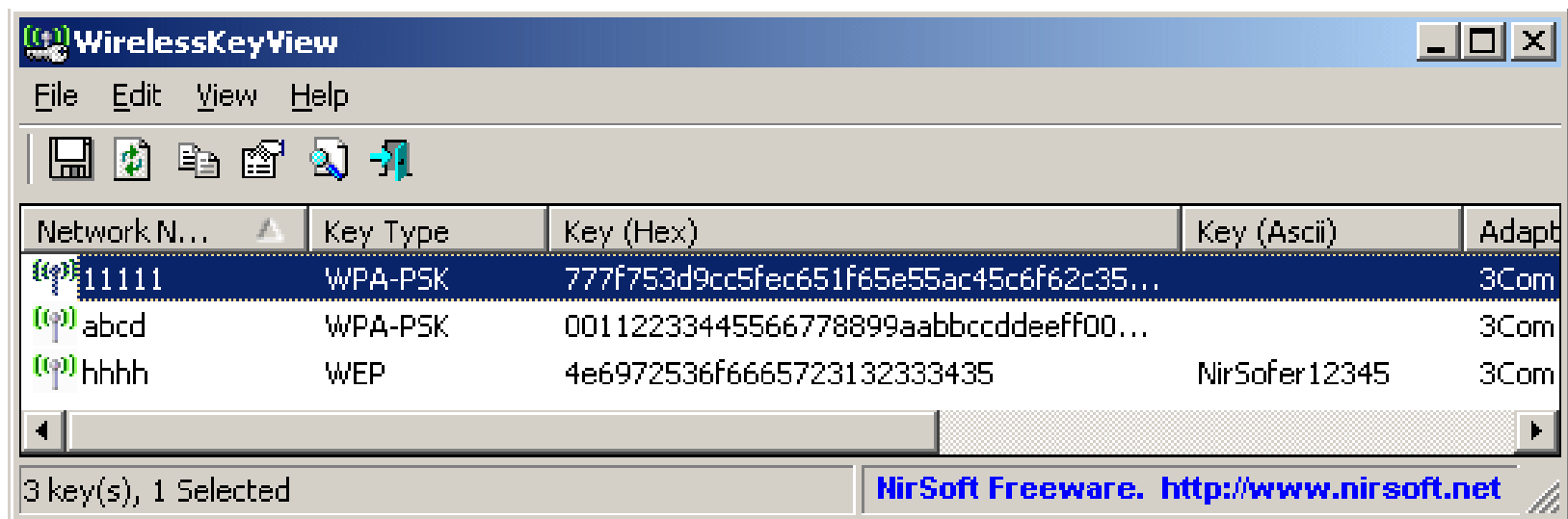
This script leverages tools for stealing credentials during a pen test

1. Standard ARP Poison
2. Oneway ARP Poison
3. DHCP Poison
4. ICMP Poison
5. FakeAP
6. Previous Menu
Choice : █
```



Dumping Keys

CLIENT EXPLOITING





Cracking WPA2-PSK with Pyrit

Using Kismet We've Decided on our Target Network

```
0
    Name: CorpWifi9
    BSSID: D8:D8:11:69:26:4C
    Manuf: Unknown
    First Seen: Nov 16 20:50:06
    Last Seen: Nov 17 14:11:21
    Type: Access Point (Managed/Infrastructure)
    Channel: 3
    Frequency: 2422 (3) - 3 packets, 75.00%
              2452 (9) - 1 packets, 25.00%
    Latest SSID: CorpWifi9

    SSID: CkTpWifi9
    Length: 9
    Type: Beacon (advertising AP)
    Encryption: None (Open)
    Beacon %: 10

    SSID: CorpWifi9
    Length: 9
    Type: Beacon (advertising AP)
```


Pyrit

<https://code.google.com/p/pyrit/>



Pyrit allows to create massive databases, pre-computing part of the IEEE 802.11 WPA/WPA2-PSK authentication phase in a space-time-tradeoff. Exploiting the computational power of Many-Core- and other platforms through ATI-Stream, Nvidia CUDA and OpenCL, it is currently by far the most powerful attack against one of the world's most used security-protocols.

During Recon Find What Channel Your Target is on and Capture only on that Channel to Increase Your Chances of Getting a Valid WPA Handshake

root@chime: ~/Hacking

Kismet Sort View Windows

Name	T	C	Ch	Pkts	Size
! BHN1201B	A	0	6	93454	1M
! CorpWiFi9	A	0	6	20018	2M
! The Dog House	A	0	11	21612	56M
. shytown	A	0	1	33221	121M

BSSID: AC:5D:10:33:C7:C9 Last seen: Nov 17 15:12:42 Crypt: TKIP WPA PSK AESCCM Manuf: Unknown

<Hidden SSID> A ? --- 199 0B

MAC	Type	Freq	Pkts	Size	Manuf
00:0D:4B:AB:60:A5	Wireless	2432	15044	3M	RokuLlc
00:14:60:66:4D:8D	Wireless	2417	1	24B	KyoceraW
00:6D:C5:AF:60:A5	Wireless	2412	1	349B	Unknown
04:43:7E:B2:8F:AC	Wired/AP	2417	1	80B	Unknown
18:08:CA:F6:BB:69	Wireless	2417	1	24B	Unknown
1C:AC:94:BE:13:7F	Wireless	2412	1	100B	Unknown
20:16:98:0B:2A:CB	Wireless	2412	1	88B	Unknown

83

0

0, 0.00 mbit

INFO: Detected new probe network "<Any>", BSSID 70:72:3C:6A:0D:E5, encryption no, channel 0, 54.00 mbit

INFO: Detected new managed network "<Hidden SSID>", BSSID BA:26:A1:E0:06:DD, encryption yes, channel 0, 0.00 mbit

CorpWiFi9 on Channel 6

Kismet_200

Elapsed 20:12.45

Networks 9497

Packets 1521853

Pkt/Sec 8

Filtered 0

Packets 0

Data

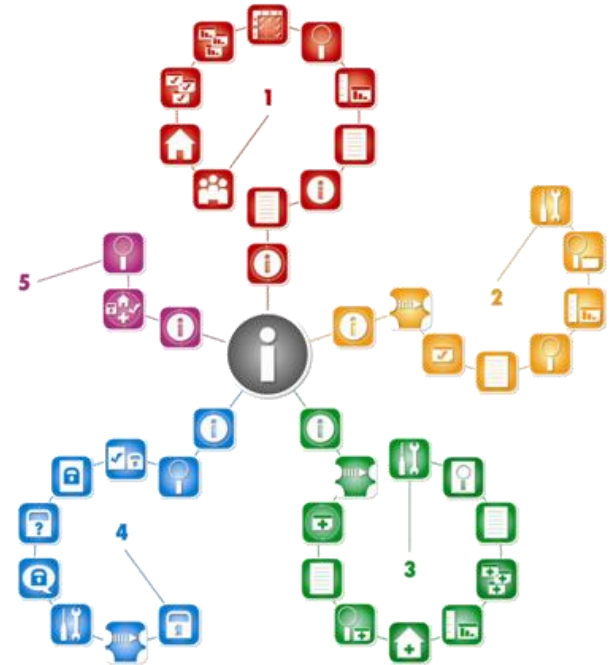
mon0 Hop

Passive Monitoring with Kismet

Running Kismet for 12 hours will capture lots of packets and PCAP files can be large.

```
-rw-r--r-- 1 root root 387M 2013-11-17 15:13 Kismet-20131116-19-00-00-1.pcapdump
-rw-r--r-- 1 root root 204 2013-11-17 15:13 Kismet-20131116-19-00-00-1.gpsxml
-rw-r--r-- 1 root root 405K 2013-11-17 15:13 Kismet-20131116-19-00-00-1.alert
root@chime:~/Hacking#
```

DEMO



Stripping a PCAP File with Pyrit

```
root@ubuntu:~/Hacking/pyrit-0.3.0/WPA2_Handshakes# ls -lah Kismet-20131116-19-00-00-1.pcapdump
-rw-r--r-- 1 root root 387M Nov 17 17:11 Kismet-20131116-19-00-00-1.pcapdump
root@ubuntu:~/Hacking/pyrit-0.3.0/WPA2_Handshakes# pyrit -r Kismet-20131116-19-00-00-1.pcapdump -o Kismet_Stripped.pcap strip
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

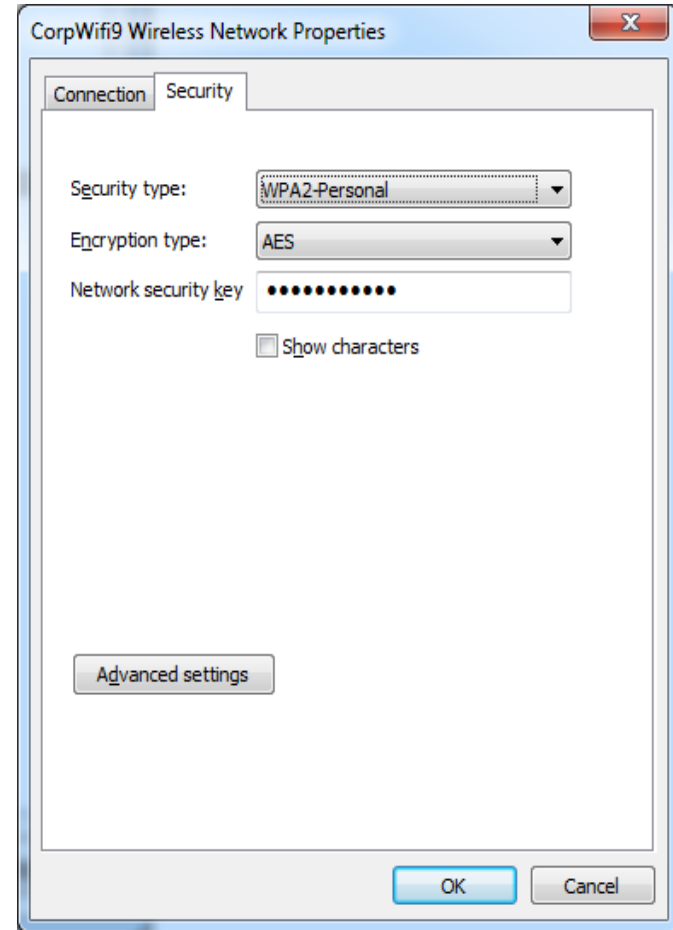
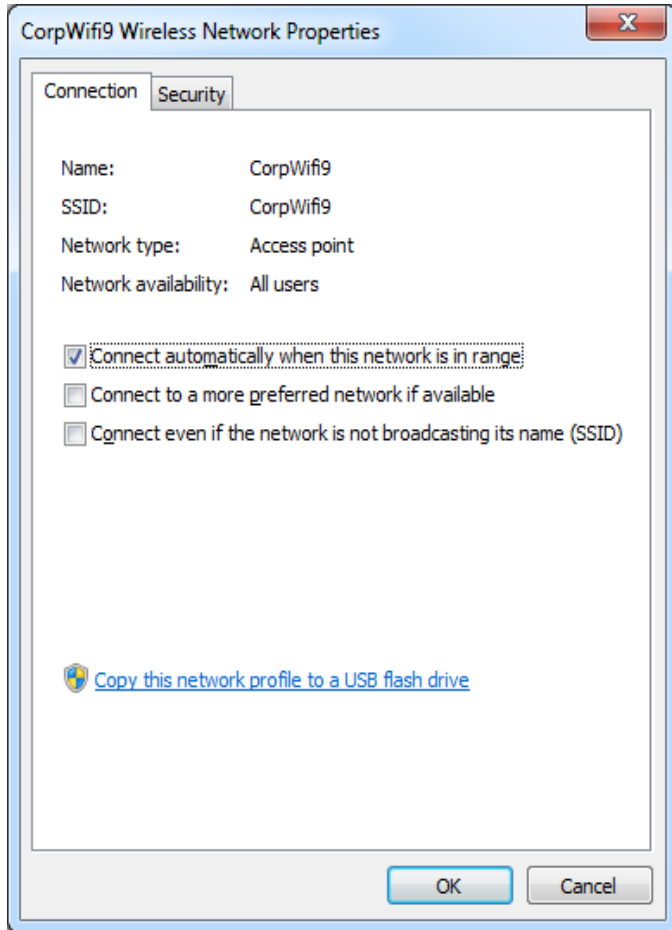
Parsing file 'Kismet-20131116-19-00-00-1.pcapdump' (1/1)
/usr/local/lib/python2.7/dist-packages/cpyrit/pckttools.py:507: UserWarning: Failed to compile BPF-filter. This may be due to a bug in Pyrit or because your version of libpcap is too old. Falling back to unfiltered processing...
  warnings.warn("Failed to compile BPF-filter. This may be due to " \

Parsed 1522469 packets (1508121 802.11-packets), got 14245 AP(s)
```

Randomly Captured WPA2 Handshake After Running Kismet for 12 hours in my apartment

```
#1: Station 4c:8d: [REDACTED], 2 handshake(s):  
  #1: HMAC_SHA1_AES, good, spread 2  
  #2: HMAC_SHA1_AES, good, spread 3  
#2: Station a4:67: [REDACTED]  
#3: Station d0:22: [REDACTED], 1 handshake(s):  
  #1: HMAC_SHA1_AES, workable, spread 1
```

A Typical Windows 7 Wireless Client Using WPA2



WPA 4-Way Handshake

android-Thu-Nov-14-16-17-53-EST-2013.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

No.	Time	Source	Destination	Protocol	Length	Info
467	19.933040	IntelCor_88:68:0c	Cisco-Li_69:26:4c	802.11	18	Acknowledgement, Flags=.....
468	19.934900	IntelCor_88:68:0c	Cisco-Li_69:26:4c	802.11	77	Association Request, SN=40, FN=...
469	19.935297	IntelCor_88:68:0c	IntelCor_88:68:0c	(802.11)	18	Acknowledgement, Flags=.....
470	19.936029	Cisco-Li_69:26:4c	IntelCor_88:68:0c	802.11	52	Association Response, SN=454, FN=...
471	19.936426	Cisco-Li_69:26:4c	IntelCor_88:68:0c	(802.11)	18	Acknowledgement, Flags=.....
472	19.937280	Cisco-Li_69:26:4c	IntelCor_88:68:0c	EAPOL	161	Key
473	19.937402	Cisco-Li_69:26:4c	Cisco-Li_69:26:4c	(802.11)	18	Acknowledgement, Flags=.....
474	19.944208	IntelCor_88:68:0c	Cisco-Li_69:26:4c	EAPOL	163	Key
475	19.945490	IntelCor_88:68:0c	IntelCor_88:68:0c	(802.11)	18	Acknowledgement, Flags=.....
476	19.946772	Cisco-Li_69:26:4c	IntelCor_88:68:0c	EAPOL	219	Key
477	19.947016	Cisco-Li_69:26:4c	Cisco-Li_69:26:4c	(802.11)	18	Acknowledgement, Flags=.....
478	19.948909	IntelCor_88:68:0c	Cisco-Li_69:26:4c	EAPOL	139	Key
479	19.950709	IntelCor_88:68:0c	IntelCor_88:68:0c	(802.11)	18	Acknowledgement, Flags=.....
480	19.967495	Netgear_19:df:ec	Broadcast	802.11	277	Beacon frame, SN=3914, FN=0, F...
481	19.988341	IntelCor_88:68:0c	Broadcast	802.11	134	Data, SN=43, FN=0, Flags=p...
482	19.988921	IntelCor_88:68:0c	IntelCor_88:68:0c	(802.11)	18	Acknowledgement, Flags=.....

Frame 472: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits)

- PPI version 0, 8 bytes
- IEEE 802.11 Data, Flags:F.
- Logical-Link Control
- 802.1X Authentication

```
0000 00 00 08 00 69 00 00 00 08 02 d5 00 24 77 03 88  ....i... ..$w..
0010 68 0c 98 fc 11 69 26 4c 98 fc 11 69 26 4c 70 1c  h...i&L ...i&Lp.
0020 aa aa 03 00 00 00 88 8e 02 03 00 75 02 00 8a 00  ..... ..u...
0030 10 00 00 00 00 00 00 00 00 b5 14 b0 c2 fd 87 7c  .....|.....
0040 07 9f e5 4a e3 39 85 6f 96 02 fe b0 84 0a 8b 2a  ...J.9.o .....*
0050 58 b6 4f 86 fd 42 af c9 7d 00 00 00 00 00 00 00  x.O..B.. }.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0080 00 00 00 00 00 00 00 00 00 00 16 dd 14 00 0f ac  .....
0090 04 2d 4f 2b ce 74 f2 cf f3 c7 5c 9b f9 f1 f7 1e  .-o+.t.. ..\.....
00a0 53
```

File: "C:\Users\Joe\Desktop\android-Thu-N... Packets: 1733 - Displayed: 17... Profile: Default

WPA 4-Way Handshake

android-Thu-Nov-14-16-17-53-EST-2013.cap [Wireshark 1.10.2 (SVN Rev 51934 from /tr...]

Filter: eapol

No.	Time	Source	Destination	Protocol	Length	Info
472	19.937280	Cisco-Li_69:26:4c	IntelCor_88:68:0c	EAPOL	161	Key
474	19.944208	IntelCor_88:68:0c	Cisco-Li_69:26:4c	EAPOL	163	Key
476	19.946772	Cisco-Li_69:26:4c	IntelCor_88:68:0c	EAPOL	219	Key
478	19.948909	IntelCor_88:68:0c	Cisco-Li_69:26:4c	EAPOL	139	Key

Frame 472: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits)

- PPI version 0, 8 bytes
- IEEE 802.11 Data, Flags:F.
- Logical-Link Control
- 802.1X Authentication
 - Version: 802.1X-2004 (2)
 - Type: Key (3)
 - Length: 117
 - Key Descriptor Type: EAPOL RSN Key (2)
 - Key Information: 0x008a
 - Key Length: 16
 - Replay Counter: 0
 - WPA Key Nonce: b514b0c2fd877c079fe54ae339856f9602feb0840a8b2a58...
 - Key IV: 00000000000000000000000000000000
 - WPA Key RSC: 0000000000000000
 - WPA Key ID: 0000000000000000
 - WPA Key MIC: 00000000000000000000000000000000
 - WPA Key Data Length: 22
 - WPA Key Data: dd14000fac042d4f2bce74f2c7f3c75c9bf9f1f71e53
 - Tag: Vendor Specific: Ieee8021: RSN

```
0000 00 00 08 00 69 00 00 00 08 02 d5 00 24 77 03 88  ....i...  ...$w..
0010 68 0c 98 fc 11 69 26 4c 98 fc 11 69 26 4c 70 1c  h....i&L ...i&Lp.
0020 aa aa 03 00 00 00 88 8e 02 03 00 75 02 00 8a 00  .....u....
0030 10 00 00 00 00 00 00 00 00 b5 14 b0 c2 fd 87 7c  .....|.....
0040 07 9f e5 4a e3 39 85 6f 96 02 fe b0 84 0a 8b 2a  ...J.9.o .....*
0050 58 b6 4f 86 fd 42 af c9 7d 00 00 00 00 00 00 00  X.o.B.. }.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0080 00 00 00 00 00 00 00 00 00 00 16 dd 14 00 0f ac  .....:.....
0090 04 2d 4f 2b ce 74 f2 cf f3 c7 5c 9b f9 f1 f7 1e  .-0+.t... \.....
00a0 53
```

WPA Key Data (eapol.keydes.data), 22 bytes P... Profile: Default

Decrypting WPA Packet Captures with Found Key in Wireshark

The screenshot displays the Wireshark interface for a packet capture file named 'android-TargetSelection.cap'. The main pane shows a list of captured packets. A red circle highlights the 'Decryption Keys' button in the 'Wireless Settings' menu. Two dialog boxes are open: 'Decryption Key Management' and 'Edit Decryption Key'. The 'Decryption Key Management' dialog shows a table of keys with 'WPA-PWD' and 'yellowstone' as the selected key. The 'Edit Decryption Key' dialog allows for modifying the selected key.

No.	Time	Source	Destination	Protocol	Length	Info
569	20.104288		CISCO-Li_09:20:4c	802.11	18	ACKnowledgement, Flags=.....
570	20.106668	IntelCor_88:68:0c	Cisco-Li_69:26:4a	802.11	130	Data, SN=71, FN=0, Flags=.p....T
571	20.106913		IntelCor_88:68:0c	(802.11)	18	ACKnowledgement, Flags=.....
572	20.107767	Cisco-Li_69:26:4a	IntelCor_88:68:0c	802.11	130	Data, SN=476, FN=0, Flags=.p....F
573	20.108011		Cisco-Li_69:26:4c	(802.11)	18	ACKnowledgement, Flags=.....
574	20.109415	Ci				0, Flags=....., BI=100, SSID=Corpwifi9
575	20.109781	Int				.p....T
576	20.110026				
577	20.111399	Int				=.pm...F.
578	20.112925	Int				=.pm...F.
579	20.114298	Int				=.pm...F.
580	20.115550	Int				=.pm...F.
581	20.116618	Int				=.pm...F.
582	20.118419	Int				=.pm...F.

Decryption Key Management

Type	Key
WPA-PWD	yellowstone

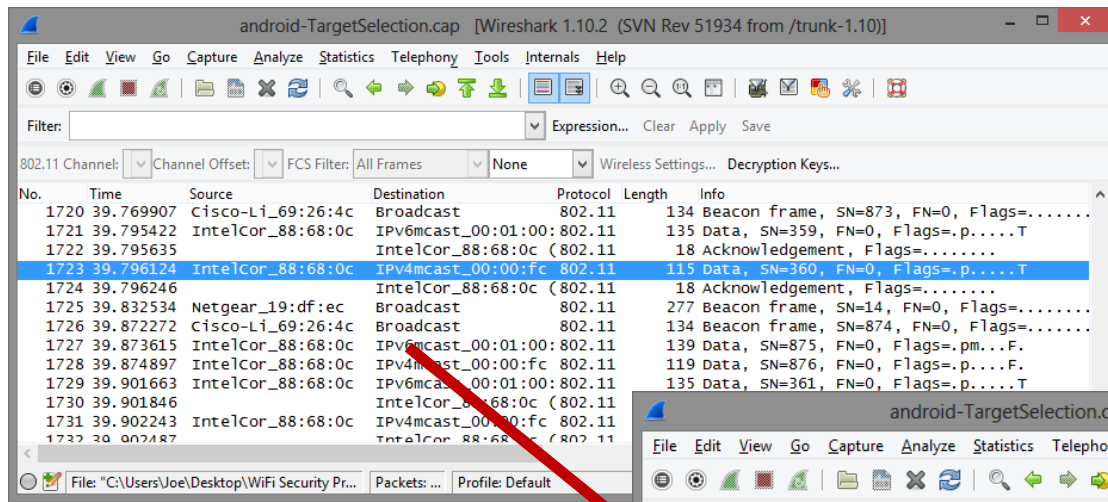
Edit Decryption Key

Modify Selected Key

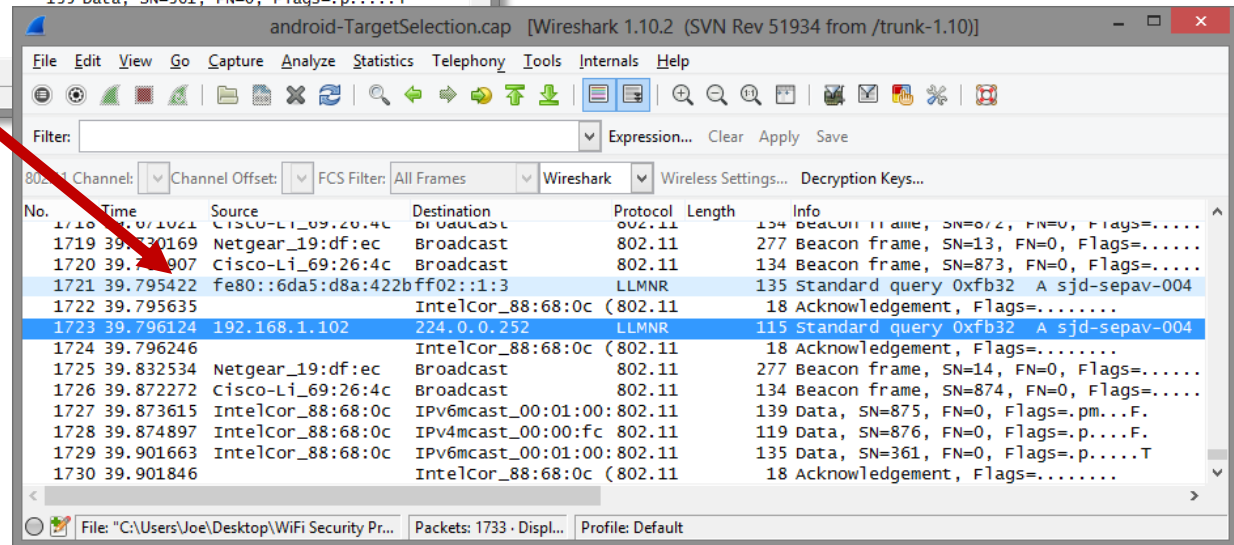
Type	Key
WPA-PWD	yellowstone

Before and After Decryption in Wireshark

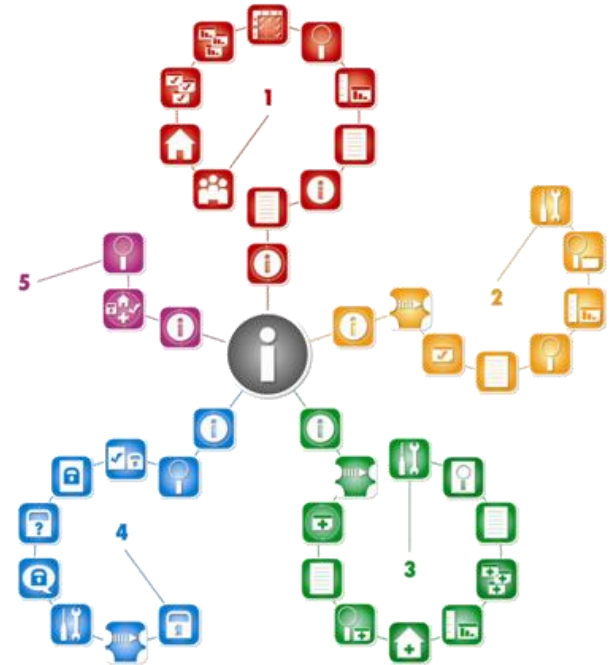
Before Applying WPA Key



After Applying WPA Key



Mobile WiFi Security Tools



Popular Mobile WiFi Hacking Tools



WiFi Sniffing on Android in Monitor Mode

<http://www.kismetwireless.net/android-pcap/>

Password Sniffing & Session Hijacking Using dSploit

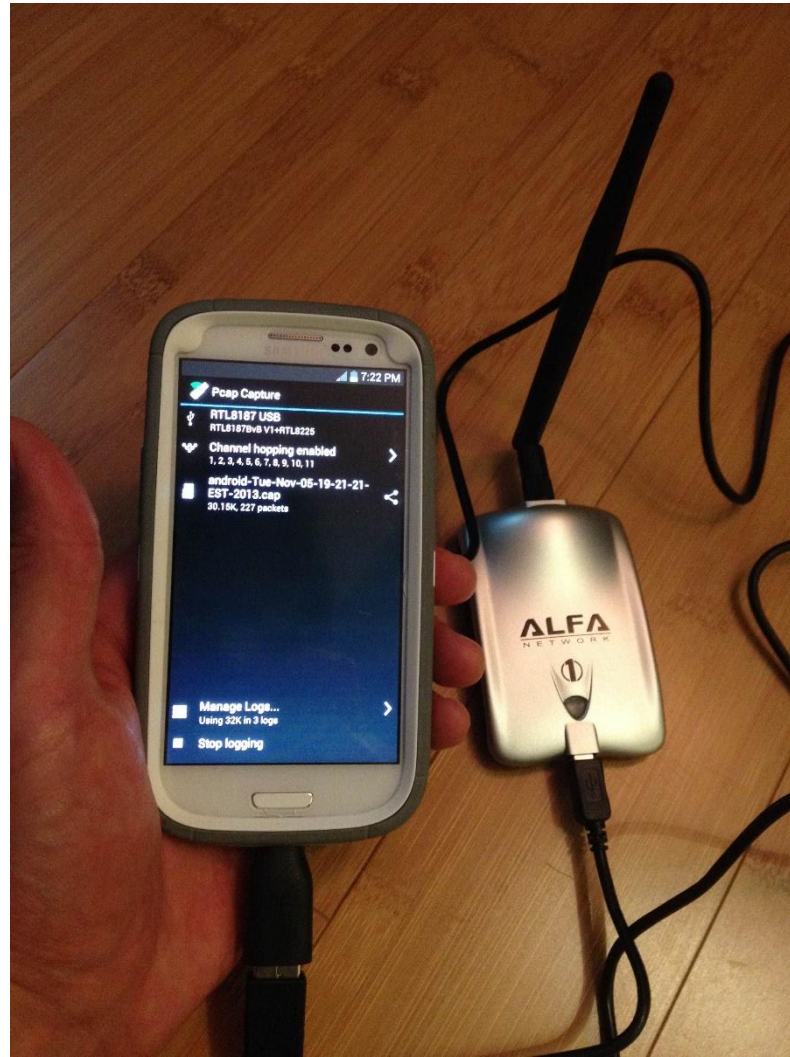
<http://dsploit.net/>



iphone-wireless

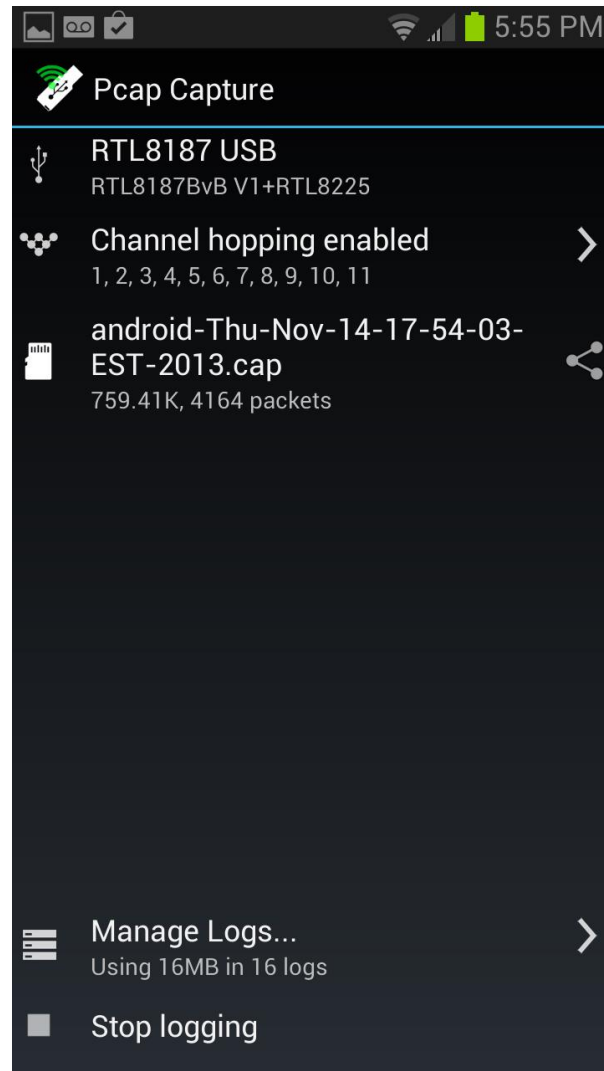
<https://code.google.com/p/iphone-wireless/wiki/Stumbler>

More Discreet Monitoring Using Alpha 1 802.11b/g



Model Number
AWUS036H. This uses
the RTL8187 Wireless
Chipset.

Android PCAP Monitor Mode on a Galaxy S3



Arp Spoofing & Detection

The screenshot shows a Wireshark capture of network traffic on a Wi-Fi interface. The main pane displays a list of ARP requests and replies. Frame 1432 is selected, and the packet details pane shows an ARP reply from source MAC 88:32:9b:0b:a8:06 to destination MAC 20:16:d8:c8:1a:34. A yellow warning message is displayed: "[Duplicate IP address detected for 192.168.1.254 (88:32:9b:0b:a8:06) - also in use by ac:5d:10:33:c7:c9 (frame 1431)]". A blue callout box points to this warning with the text: "88:32:9b:0b:a8:06 is actually the Android Phone pretending to be the default gateway at 192.168.1.254".

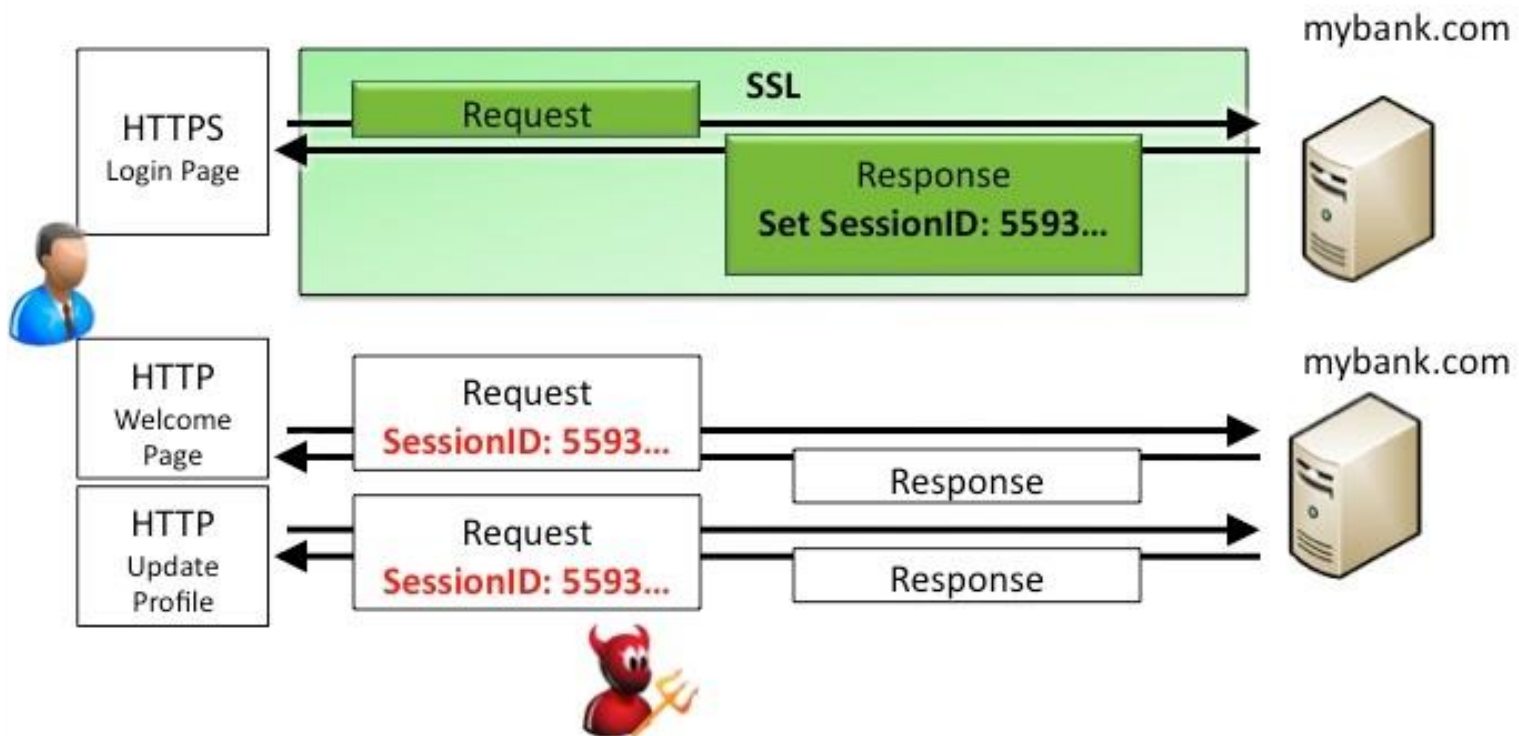
No.	Time	Source	Destination	Protocol	Length	Info
1183	29.6114490	SamsungE_0b:a8:06	LiteonTe_c8:1a:34	ARP	42	192.168.1.254 is at 88:32:9b:0b:a8:06
1427	30.5732440	SamsungE_0b:a8:06	LiteonTe_c8:1a:34	ARP	42	192.168.1.254 is at 88:32:9b:0b:a8:06
1432	31.6962180	SamsungE_0b:a8:06	LiteonTe_c8:1a:34	ARP	42	192.168.1.254 is at 88:32:9b:0b:a8:06
1433	32.5938430	SamsungE_0b:a8:06	LiteonTe_c8:1a:34	ARP	42	192.168.1.254 is at 88:32:9b:0b:a8:06
1442	33.6012160	SamsungE_0b:a8:06	LiteonTe_c8:1a:34	ARP	42	192.168.1.254 is at 88:32:9b:0b:a8:06
1448	34.5839120	SamsungE_0b:a8:06	LiteonTe_c8:1a:34	ARP	42	192.168.1.254 is at 88:32:9b:0b:a8:06

Frame 1432: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

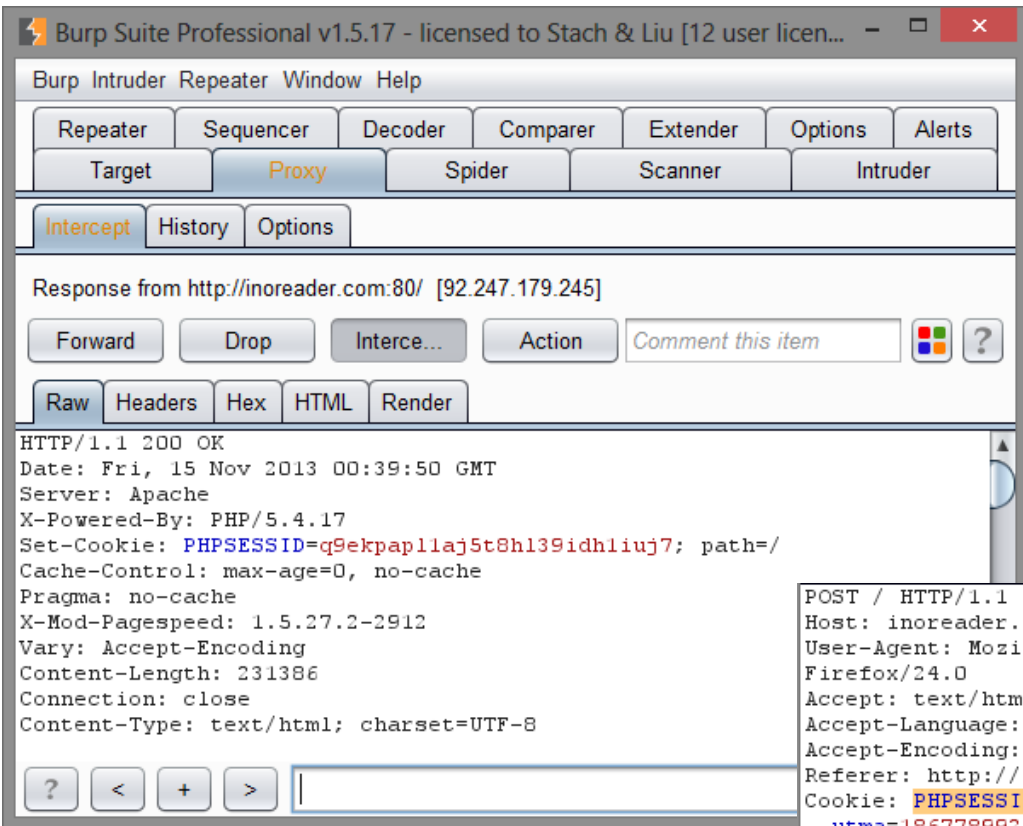
- Ethernet II, Src: SamsungE_0b:a8:06 (88:32:9b:0b:a8:06), Dst: LiteonTe_c8:1a:34 (20:16:d8:c8:1a:34)
- [Duplicate IP address detected for 192.168.1.254 (88:32:9b:0b:a8:06) - also in use by ac:5d:10:33:c7:c9 (frame 1431)]
- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (1)
 - Protocol type: IP (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: reply (2)
 - Sender MAC address: SamsungE_0b:a8:06 (88:32:9b:0b:a8:06)
 - Sender IP address: 192.168.1.254 (192.168.1.254)
 - Target MAC address: LiteonTe_c8:1a:34 (20:16:d8:c8:1a:34)
 - Target IP address: 192.168.1.205 (192.168.1.205)

```
0000 20 16 d8 c8 1a 34 88 32 9b 0b a8 06 08 06 00 01    ....4.2 .....
0010 08 00 06 04 00 02 88 32 9b 0b a8 06 c0 a8 01 fe    .....2 .....
0020 20 16 d8 c8 1a 34 c0 a8 01 cd                    ....4.. ..
```


Stealing Unencrypted Session IDs



Web Session Hijacking using dSploit



```
POST / HTTP/1.1
Host: inoreader.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:24.0) Gecko/20100101
Firefox/24.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://inoreader.com/
Cookie: PHPSESSID=q9ekpap11aj5t8h139idhliuj7;
__utma=186778992.969814715.1384476039.1384476039.1384476039.1;
__utmb=186778992.1.10.1384476039; __utmc=186778992;
__utmz=186778992.1384476039.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 58

username=joewalko%40gmail.com&password=<redacted>&x=15&y=9
```

PwnPad

NEXUS 7 PENTEST DEVICE



Toolkit includes:

Wireless Tools

- Aircrack-ng
- Kismet
- Wifite
- Reaver
- MDK3
- EAPeak
- Asleep
- FreeRADIUS-WPE
- Hostapd

Bluetooth Tools:

- bluez-utils
- btscanner
- bluelog
- Ubertooth tools

Web Tools

- Nikto
- W3af

Network Tools

- NET-SNMP
- Nmap
- Netcat
- Hping3
- Macchanger
- Tcpdump
- Tshark
- Ngrep
- Dsniff
- Ettercap-ng
- SSLstrip
- Hamster & Ferret
- Metasploit
- SET
- Easy-Creds
- John (JTR)
- Hydra
- Pyrit
- Scapy



Defenses

A V O I D B E I N G P R O B E D

Defenses

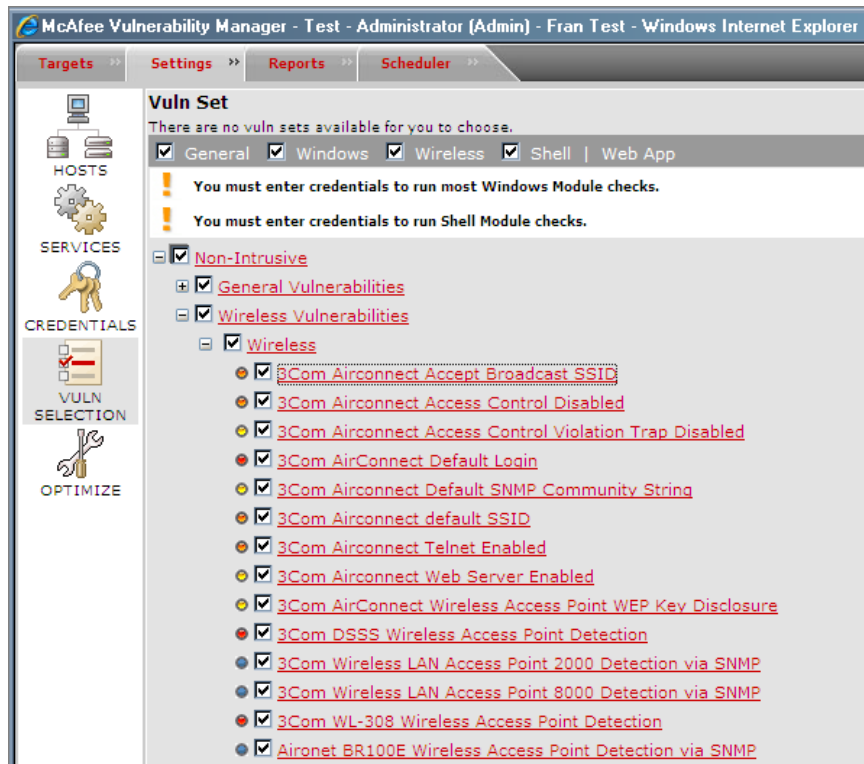
R E C O M M E N D A T I O N S

- Conduct regular wireless assessments
- Employ strong encryption and authentication methods
- Employ wireless IDS/IPS
- Secure wireless clients (laptops, phones, ...)

Defenses

RECOMMENDATIONS

Use “wireless checks” of network vulnerability scanners



Defenses

RECOMMENDATIONS

Physically track down rogue access points and malicious devices



**Device Finder
Directional Antenna**

Accurately discover unknown interference

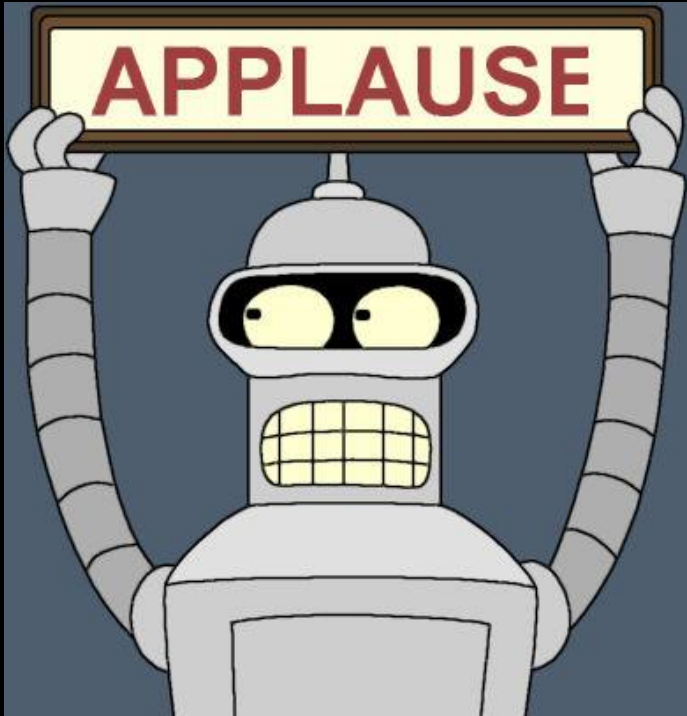
Don't let mystery devices stay a mystery.

Take control of your wireless environment with our purpose-made Device Finder Directional Antenna to quickly track down offending signals in the most common Wi-Fi spectrum – for only \$99.

Our directional antenna, when connected to a Wi-Spy, gives you greater ability to discover exactly which direction a 2.4 GHz transmission is coming from.

Device Finder only works with [Chanalyzer Pro](#) software.

Thank You



Bishop Fox – see for more info:
<http://www.bishopfox.com/>