



Alignment • Clarity • Confidence

Latest Wireless Vulnerabilities & Wireless Incident Response

Michael Raggo, CISSP, NSA-IAM, CCSI, SCSA, ACE, CSI

Get Ready for the Wireless World!



"C'mon, c'mon — It's either one or the other."

Wireless Network Risks

(What do I need to look for?)

Traditional Wired Network

Well-Defined
Network Edge,
Straightforward
to Manage and
Secure

INTERNET

SECURE INTERNAL NETWORK

Server



Users

Wireless Security Concerns

Network Edge
Blurred, New
Attack Vectors
'Behind' the
Firewall

INTERNET

Hacker

1

Rogue AP Connected
to Network
Network Breach

3

Leaked Wired Traffic
& Insertion
Data Leakage

Server

INTRANET

AP

Laptop

Desktop

4

Non-Compliant AP
*Network Breach/Data Leakage/
Data Compromise*

5

Users Bypassing Network
Security Controls
Data Leakage/Network Backdoor



Muni Wi-Fi or Neighbors

Hotspot

Evil Twin

Mobile User

2

Hotspot Phishing
Data Leakage

ACCUVANT

Alignment • Clarity • Confidence

Common Infrastructure Vulnerabilities

Many people have fortified their sensitive wireless infrastructures by migrating away from Open or WEP configurations

Type	Comments	State
WEP Attack	<ul style="list-style-type: none">▪ Vulnerable for many years, including Cisco Migration Mode	Easily Cracked
WPA-PSK Attack	<ul style="list-style-type: none">▪ Can be vulnerable to dictionary attack	Can be attacked, especially 8 char PSKs
TKIP	<ul style="list-style-type: none">▪ 2009/2010 attack demonstrations	Targeted in POC

End-users have now become the low-hanging fruit!!!

Summary of 802.11 Vulnerabilities

Type	Attacks	Tools
Reconnaissance	<ul style="list-style-type: none">▪ Rogue APs▪ Open/Misconfigured APs▪ Ad Hoc stations	Netstumbler, Kismet, Wellenrighter
Sniffing	<ul style="list-style-type: none">▪ WEP, WPA, LEAP cracking▪ Dictionary attacks▪ Leaky APs	AirSnort, Wepcrack, Cowpatty, Wireshark, Cain, Ettercap
Masquerade	<ul style="list-style-type: none">▪ MAC spoofing▪ AirSnarf/HotSpot attacks▪ Evil Twin/Wi-Phishing attacks	AirSnarf, Hotspotter, HostAP, SMAC
Insertion	<ul style="list-style-type: none">▪ Multicast/Broadcast injection▪ Routing cache poisoning▪ Man in the Middle attack	Airpwn, WepWedgie, ChopChop, Vippr, irpass, CDPsniffer
Denial-of-Service	<ul style="list-style-type: none">▪ Disassociation▪ Duration field spoofing▪ RF jamming	AirJack, void11, Bugtraq, IKE-crack



Reconnaissance - Wired-Side Leakage

Wired Side Leakage (Router Broadcast Traffic)

Password for H/A on Core Router! Note that this is leaking from the wired network into the wireless airspace, unencrypted, even though the AP is using encryption for wireless users...

The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. Below the menu is a toolbar with various icons. A filter bar shows 'Filter:' and 'Expression... Clear Apply'. The main packet list table has columns for No., Time, Source, Destination, Protocol, and Info. The packets are as follows:

No.	Time	Source	Destination	Protocol	Info
717	217.000000	[REDACTED]	[REDACTED]	EAP	Response, Identity [RFC3748]
718	217.016000	[REDACTED]	[REDACTED]	EAP	Response, Identity [RFC3748]
32718	2063.375000	[REDACTED]	[REDACTED]	EAPOL	Key [Malformed Packet]
33291	2084.563000	[REDACTED]	[REDACTED]	EAPOL	Key [Malformed Packet]
708	216.985000	[REDACTED]	[REDACTED]	HSRP	Hello (state Active)
1186	238.297000	[REDACTED]	[REDACTED]	HSRP	Hello (state Standby)
1196	238.344000	[REDACTED]	[REDACTED]	HSRP	Hello (state Standby)
1197	238.344000	[REDACTED]	[REDACTED]	HSRP	Hello (state Active)
1229	238.438000	[REDACTED]	[REDACTED]	HSRP	Hello (state Active)
1231	238.453000	[REDACTED]	[REDACTED]	HSRP	Hello (state Standby)
1252	238.500000	[REDACTED]	[REDACTED]	HSRP	Hello (state Active)
1297	254.344000	[REDACTED]	[REDACTED]	HSRP	Hello (state Active)
1668	275.344000	[REDACTED]	[REDACTED]	HSRP	Hello (state Standby)
2022	286.031000	[REDACTED]	[REDACTED]	HSRP	Hello (state Active)
6362	469.703000	[REDACTED]	[REDACTED]	HSRP	Hello (state Active)
7270	511.781000	[REDACTED]	[REDACTED]	HSRP	Hello (state Standby)
8049	567.297000	[REDACTED]	[REDACTED]	HSRP	Hello (state Active)
8718	574.813000	[REDACTED]	[REDACTED]	HSRP	Hello (state Standby)

Below the packet list, the details pane shows the following information:

- State: Active (16)
- Hellotime: Default (3)
- Holdtime: Default (10)
- Priority: 100
- Group: 1
- Reserved: 0
- Authentication Data: Default (Cisco)
- Virtual IP Address: [REDACTED]

The bottom pane shows the raw packet data in hexadecimal and ASCII. The ASCII column shows the word 'Cisco' in blue, indicating a clear-text password leak.

Contains a clear-text character reused password... Packets: 49855 Displayed: 49855 Marked: 0 Profile: Default

Mobile Workers are the new low hanging fruit!!!

HOTEL



Am I connected to an insecure access point?

COFFEE SHOP



Am I connected to a real hotspot connection?

AIRPORT



Am I connected to another passenger in ad-hoc mode?

HOME



Is my laptop probing for SSIDs not on the safe list?

HEADQUARTERS



Are my employees using Municipal WiFi?

BRANCH OFFICE



Do I have wired & wireless on at the same time?

Wireless Phishing – Old School Method

```
root@wirelessdefence:/tools/wifi/karma-0.4
File Edit View Terminal Tabs Help
[root@wirelessdefence karma-0.4]# bin/karma etc/karma.xml
Starting KARMA...
Loading config file etc/karma.xml
ACCESS-POINT is running
DNS-SERVER is running
DHCP-SERVER is running
POP3-SERVER is running
FTP-SERVER is running
[2006-01-20 22:43:58] INFO WEBRick 1.3.1
[2006-01-20 22:43:58] INFO ruby 1.8.4 (2005-12-24) [i386-linux]
[2006-01-20 22:43:58] INFO WEBRick::HTTPServer#start: pid=4962 port=80
HTTP-SERVER is running
CONTROLLER-SERVLET is running
EXAMPLE-WEB-EXPLOIT is running
Delivering judicious KARMA, hit Control-C to quit.
AccessPoint: 00:20:A6:54:3E:ED associated
DhcpServer: 00:20:a6:54:3e:ed (dell5150) <- 169.254.0.254
DNS: 169.254.0.254.1128: 22333 IN::A www.mysecretwebsite.com
FTP: 169.254.0.254 myusername/mypassword
```



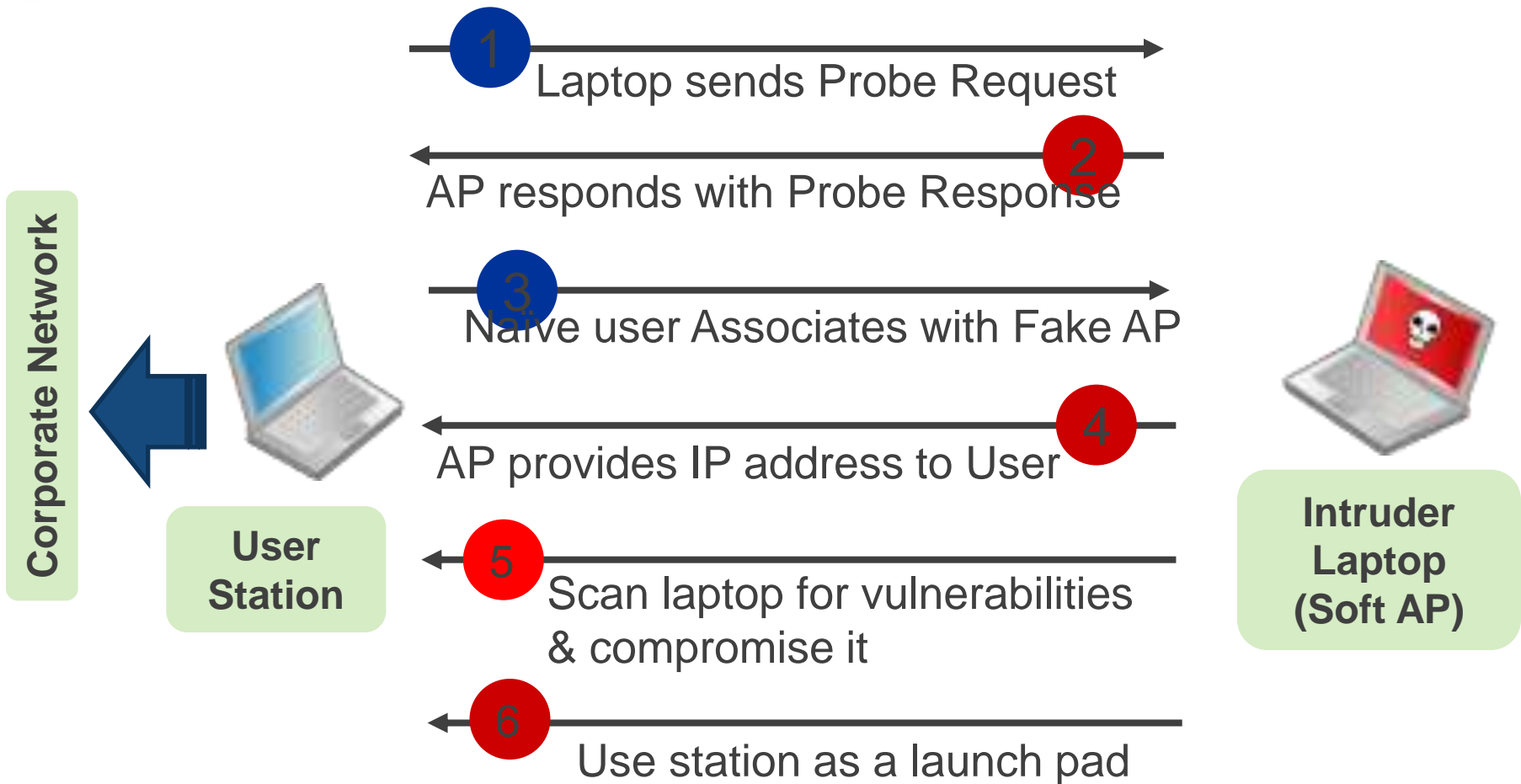
Tools such as Karma can Respond to ANY Client Probe Request

Variety of Services (POP, FTP and HTTP) to Lure Unsuspecting Users

No Authentication of “Pervasive Wireless Cloud”

Automatic Network Selection in Windows (Zero Configuration Client)

Malicious Associations



Hotspot Phishing, Evil Twin, SoftAP, etc.

New School Method - Direct attacks on Wireless Clients using Cellphone

Palm Pre with Hacked Mobile Hotspot

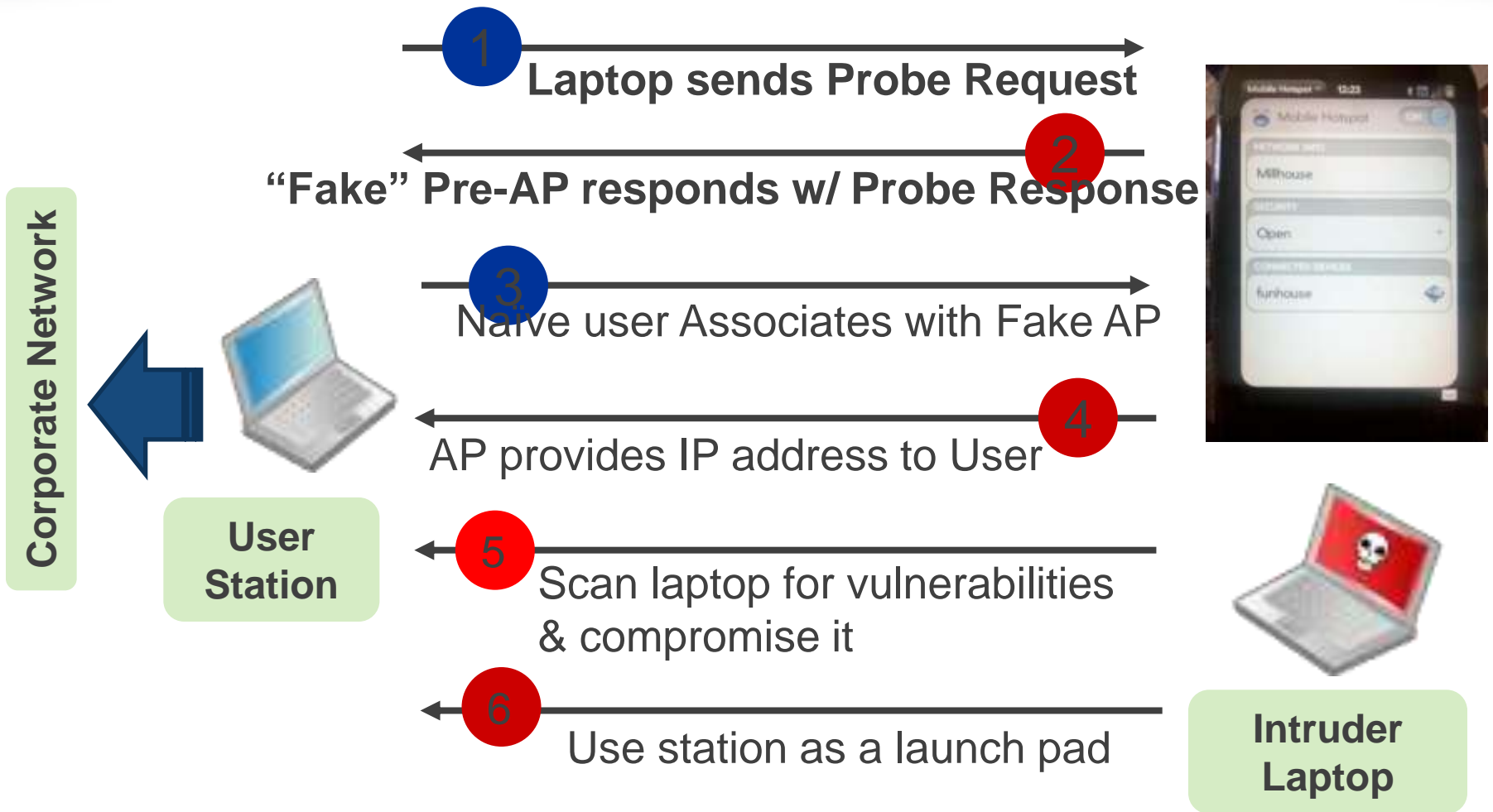


2 New School Hotspot Phishing
Data Leakage

Attack vector on any wifi enabled cell phone...

Got a WiFi iPad, iPod, Mac? ☺

Malicious Associations - Cell Phone hotspot



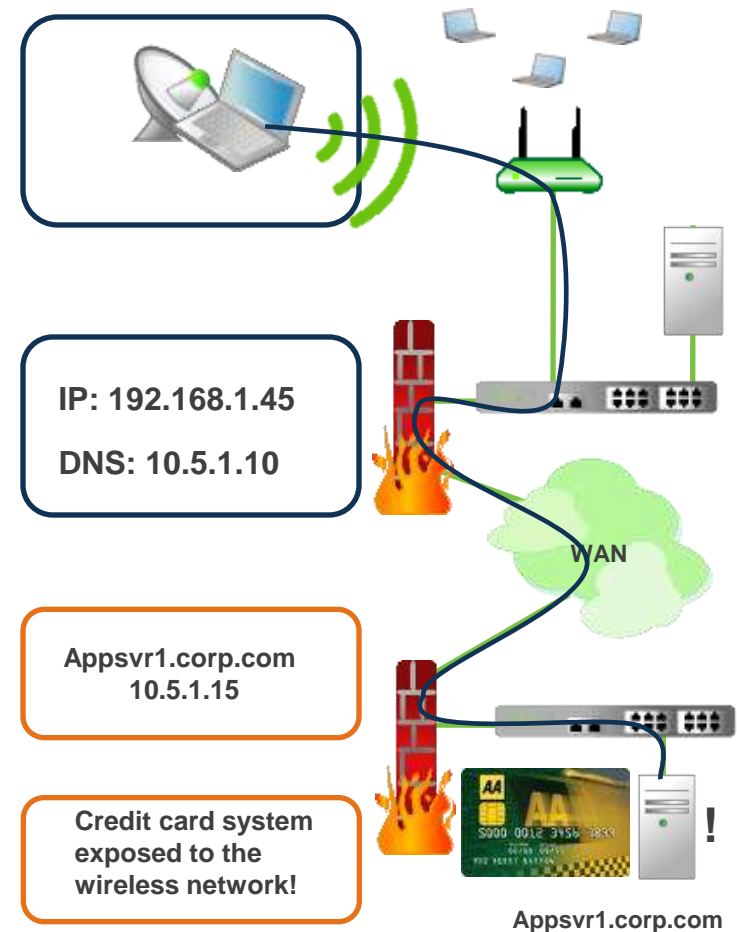
Captive Portal Bypass – Guest Access

Captive portal doesn't allow "access" until authenticated via the portal

- But it does allow access to the wireless network, and provides an IP...

What can I do with access to the local network?

- Unless PSPF is enabled, hacker can scan and target other users of the wireless network
- Exploit their laptop and steal credentials for other wireless networks (metasploit anyone?)
- Validate if portal ACL rules are properly prohibiting access
- Virtually every captive portal we tested was only controlling HTTP/HTTPS access to the Internet and internal networks
- We could ping, ssh, telnet, ftp, etc. without EVER authenticating to the portal!!!



Captive Portal Bypass

Captive Portals

We later determined that the attackers got to the corporate network through a unauthorized wired bridge installed by an employee

This secondary local subnet was discovered by listening to wireless traffic for the entire airspace, and identifying IPs for the corporate network

They then attempted to access the network through the captive portal, and were successful. And this DIDN'T require any authentication to the captive portal! They already had access to the local network!!!

	A	B	C	D	E	F	G	H	I
1	Location	Sensor	Access Point	IP Address	Hostname	Port	ICMP	Policy	Vulnerability
2	WIPS - Def	00:16:5d:2 00:1a:1e:		4.2.2.2	4.2.2.2		YES	Not Allowed	Unapproved device is accessible
3	WIPS - Def	00:16:5d:2 00:1a:1e:		4.2.2.2	4.2.2.2	80			
4	WIPS - Def	00:16:5d:2 00:1a:1e:		4.2.2.2	4.2.2.2	443			
5	WIPS - Def	00:16:5d:2 00:1a:1e:		10.3.9.0	10.3.9.0/24		YES	Not Allowed	
6	WIPS - Def	00:16:5d:2 00:1a:1e:		10.3.9.0	10.3.9.0/24	21			
7	WIPS - Def	00:16:5d:2 00:1a:1e:		10.3.9.0	10.3.9.0/24	22			
8	WIPS - Def	00:16:5d:2 00:1a:1e:		10.3.9.0	10.3.9.0/24	23			
9	WIPS - Def	00:16:5d:2 00:1a:1e:		10.3.9.0	10.3.9.0/24	80			

Guest network allows access to the Internet without authenticating to Portal, for non-HTTP(S)

CAPTIVE PORTALS COMMONLY ALLOW THE PORTAL TO BE BYPASSED!!!

Intrusion Detection & Forensic Analysis

Wireless attacks



Layer 1

- RF Jamming
- Bluetooth
- Malicious Interference



Layer 2

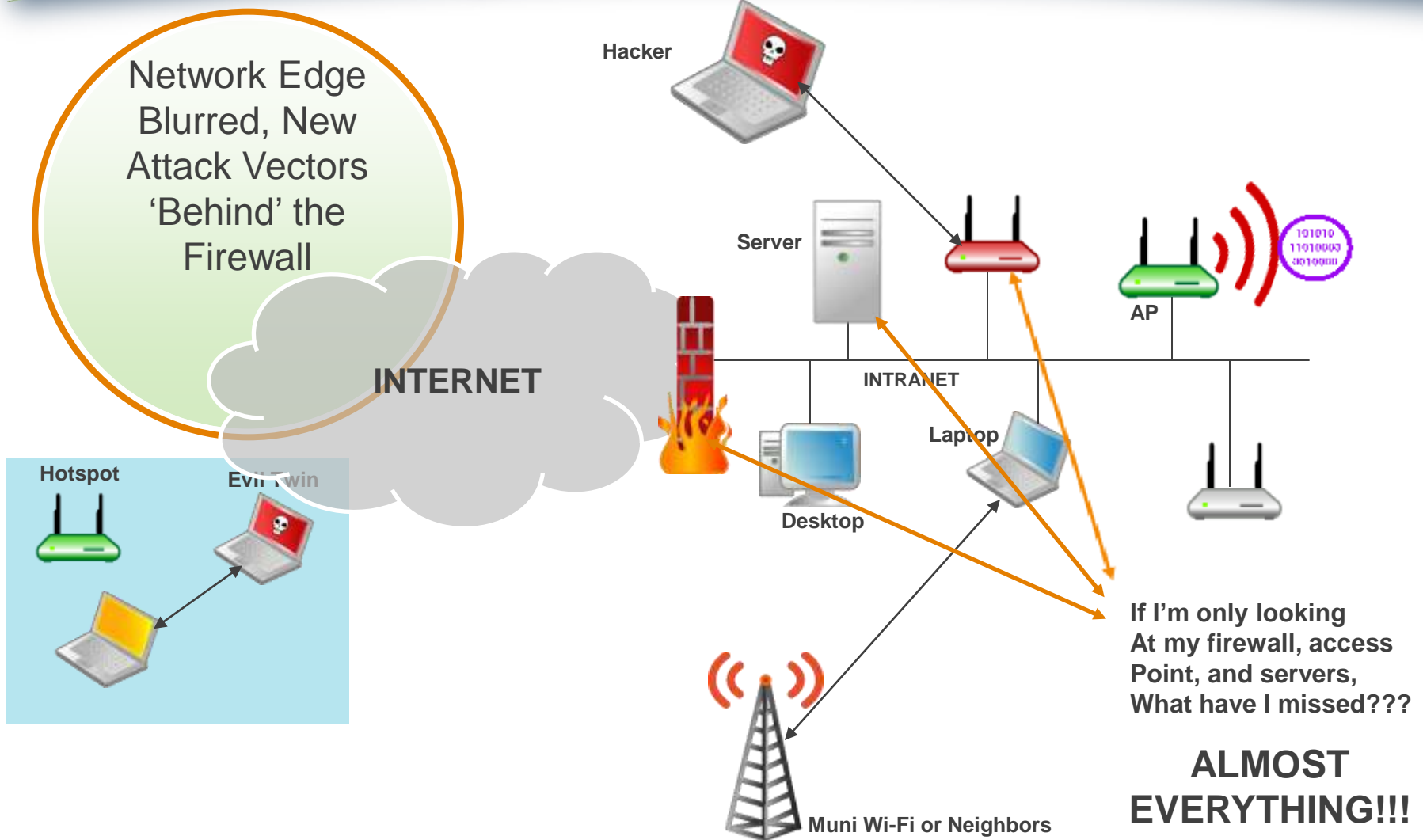
- Impersonation Attacks
- Active Attacks
- DoS
- Rogue Activity
- Anomalous Behavior
- Extrusions
- Performance
- List does on and on...



Layer 3 and above

- Impersonation Attacks
- Active Attacks
- DoS
- Rogue Activity
- Anomalous Behavior
- Performance
- Possibilities are endless...

Incident Response – Old School of thought

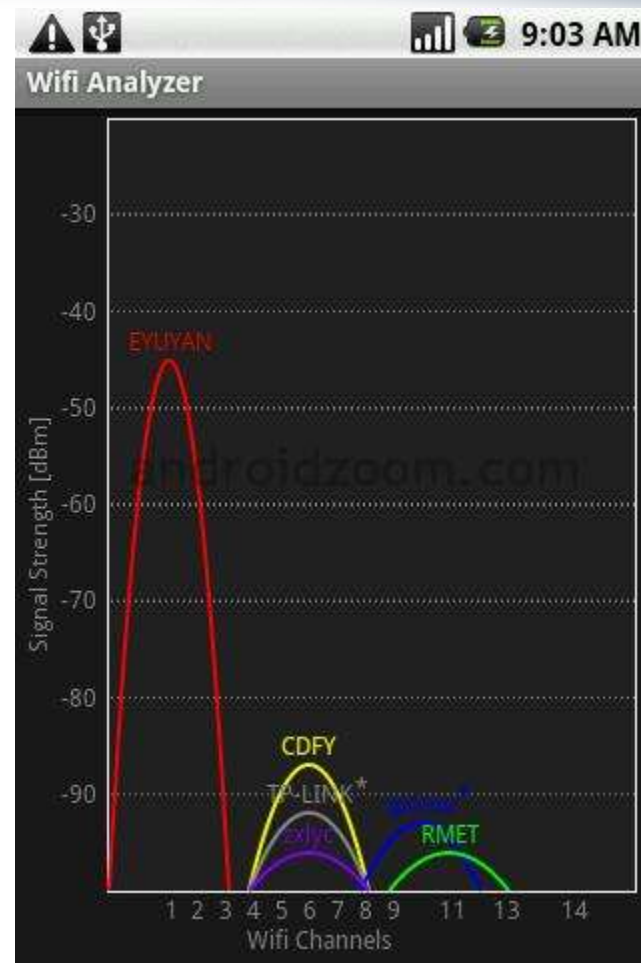


Wireless Incident Response and Forensics Requires Wireless Analysis!!! Let's begin with Live Analysis...

Layer 1 – Spectrum Analysis

Android WiFi Analyzer App

- Nice (and free) WiFi Analyzer
- Handy for walking around watching the signal strength get stronger as you get closer to the suspect AP
- Limited to 802.11b/g (no 802.11a)



Wireless Analyzer

Netstumbler/Kismet – Great (and free) tools BUT:

- Are you scanning 802.11a and 802.11n also?

If you're built-in card only supports 802.11b/g, then you're missing 802.11a devices!!!

(>50% of the PCI QSA reports we've seen, do not include any 802.11a analysis, that's means they've missed half of the potential wireless devices, therefore Rogues may still exist in your environment)

Make sure your analysis is COMPREHENSIVE!!! USE A DUAL-BAND CARD

Otherwise you may be missing half the picture!

Wireshark

Wireless Sniffing on Windows usually requires a licensed product

- note that we're sniffing Layer 2 WiFi packets, not Layer 3 as if you were already connected to the AP and have an IP address...

Use your laptop with BackTrack and a compatible wireless card and you can perform wireless sniffing for free!

- New Link: <http://www.backtrack-linux.org>
- Some 802.11a/b/g Card Options:
 - Ubiquiti (can have external antennas)
 - NetGear WAG511

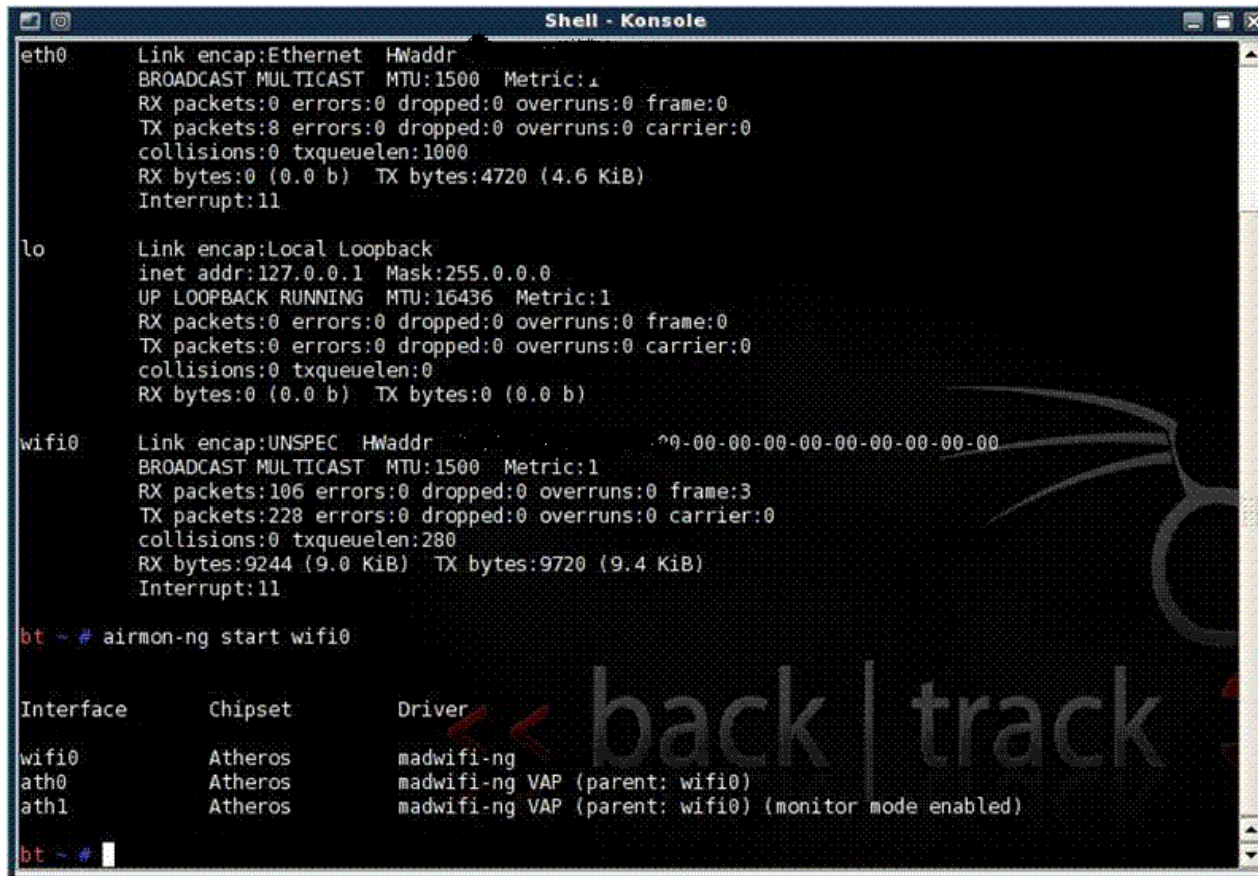
What about 802.11n? Remember that 802.11n APs operate in both the 2.4GHz and 5GHz spectrums and are typically visible in either spectrum and backward compatibility, so you're probably good!

Layer 2 - Wireless Sniffing

Sniffing with BackTrack

1. Enable monitor mode for the wireless card to allow packet capture

```
# airmon-ng start wifi0
```



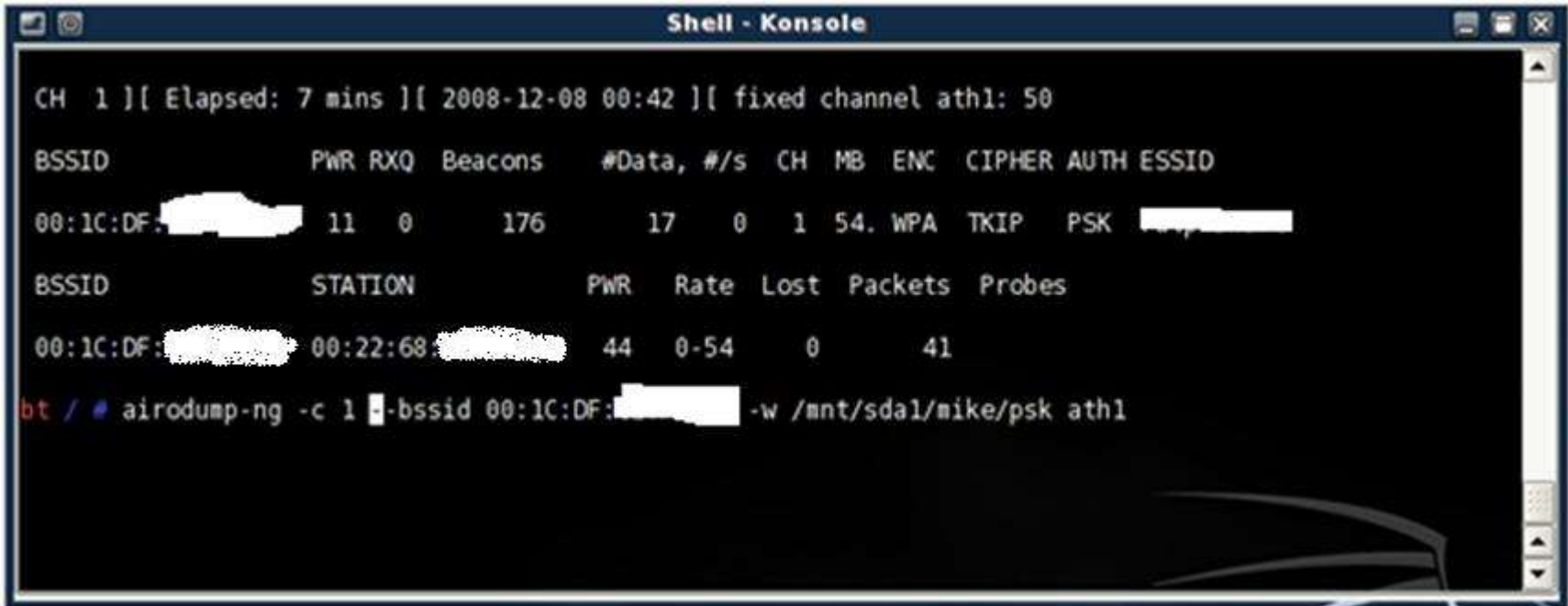
```
eth0      Link encap:Ethernet  HWaddr 82:50:00:00:00:00  
          BROADCAST MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 b)  TX bytes:4720 (4.6 KiB)  
          Interrupt:11  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)  
  
wifi0     Link encap:UNSPEC  HWaddr 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00  
          BROADCAST MULTICAST  MTU:1500  Metric:1  
          RX packets:106 errors:0 dropped:0 overruns:0 frame:3  
          TX packets:228 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:280  
          RX bytes:9244 (9.0 KiB)  TX bytes:9720 (9.4 KiB)  
          Interrupt:11  
  
bt ~ # airmon-ng start wifi0  
  
Interface  Chipset  Driver  
wifi0      Atheros  madwifi-ng  
ath0       Atheros  madwifi-ng VAP (parent: wifi0)  
ath1       Atheros  madwifi-ng VAP (parent: wifi0) (monitor mode enabled)  
  
bt ~ #
```

Layer 2 - Wireless Sniffing

Sniffing with BackTrack

2. Run airodump-ng with the following options:

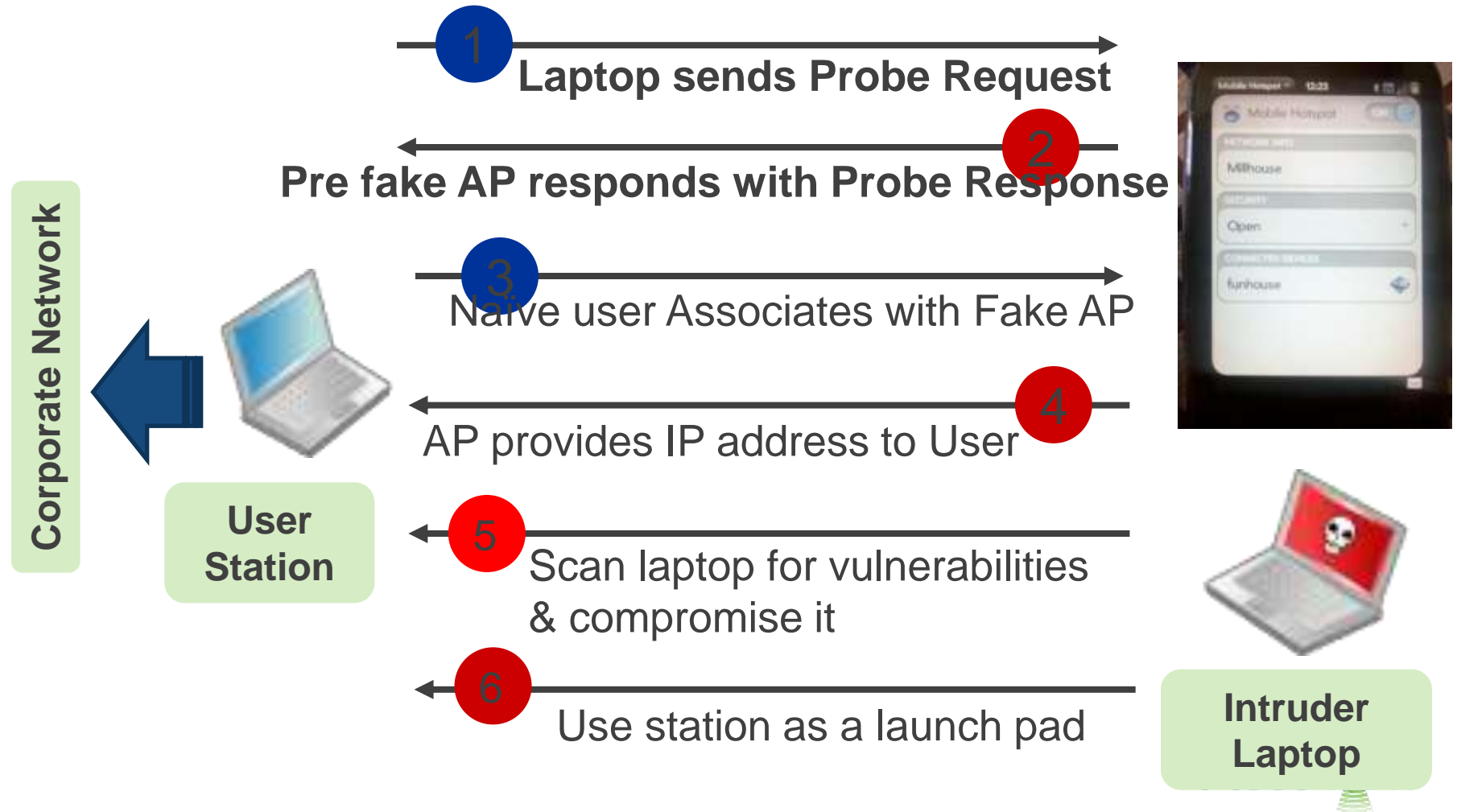
```
# airodump-ng -c <channel> -bssid <MAC of AP>  
ath1 -w <target capture file>
```



```
CH 1 ][ Elapsed: 7 mins ][ 2008-12-08 00:42 ][ fixed channel ath1: 50  
BSSID          PWR RXQ Beacons  #Data, #/s  CH MB ENC  CIPHER AUTH ESSID  
00:1C:DF:[redacted] 11  0    176     17  0   1 54. WPA  TKIP  PSK  [redacted]  
BSSID          STATION      PWR  Rate Lost Packets Probes  
00:1C:DF:[redacted] 00:22:68:[redacted] 44  0-54  0     41  
bt / # airodump-ng -c 1 -bssid 00:1C:DF:[redacted] -w /mnt/sda1/mike/psk ath1
```

Comparing packets from Access Points versus Wireless Clients

Why is a Palm Pre sending Beacons & probe responses???



Wireless Layer 2 – Suspicious Activity

Hotspot Phishing, Evil Twin, SoftAP attacks

The image shows a Wireshark packet capture of a wireless network. The packet list at the top shows a series of frames: a Beacon frame (No. 1) and several Probe Response frames (Nos. 34-82). The Beacon frame is highlighted with a red box, and its details are expanded below. The details pane shows the frame control, duration, destination address (broadcast), source address (Palm_), BSS ID (Palm_), fragment number (0), and sequence number (2611). The IEEE 802.11 wireless LAN management frame details are also expanded, showing fixed and tagged parameters. A red text overlay asks why a Palm Pre is sending these frames using the corporate SSID. A hex dump at the bottom shows the raw data of the frame.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Palm_	Broadcast	IEEE 802	Beacon frame, SN=2611, FN=0, Flags=....., BI=100, SSID="Millhouse"
34	9.052221	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2705, FN=0, Flags=....., BI=100, SSID="Millhouse"
37	9.062458	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2706, FN=0, Flags=....., BI=100, SSID="Millhouse"
39	9.071678	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2707, FN=0, Flags=....., BI=100, SSID="Millhouse"
76	20.281593	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2822, FN=0, Flags=....., BI=100, SSID="Millhouse"
77	20.282621	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2822, FN=0, Flags=...R..., BI=100, SSID="Millhouse"
78	20.283645	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2822, FN=0, Flags=...R..., BI=100, SSID="Millhouse"
79	20.286205	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2822, FN=0, Flags=...R..., BI=100, SSID="Millhouse"
80	20.286715	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2822, FN=0, Flags=...R..., BI=100, SSID="Millhouse"
81	20.336893	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2823, FN=0, Flags=....., BI=100, SSID="Millhouse"
82	20.337916	Palm_	HonHaiPr_	IEEE 802	Probe Response, SN=2823, FN=0, Flags=...R..., BI=100, SSID="Millhouse"

Why is a Palm Pre sending Beacons and Probe Responses, Using the Corporate SSID? That looks suspicious...

(Wireshark Analysis)

Frame 1 (75 bytes on wire, 75 bytes captured)
IEEE 802.11 Beacon frame, Flags:
Type/Subtype: Beacon frame (0x08)
Frame Control: 0x0080 (Normal)
Duration: 0
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: Palm_
BSS Id: Palm_
Fragment number: 0
Sequence number: 2611
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Tagged parameters (39 bytes)

0000
0010
0020
0030
0040

..

0. v.&....

Millhouse.

.. \$.

.0 H]

Frame (frame), 75 bytes
Packets: 1306 Displayed: 1306 Marked: 0
Profile: Default

Hidden Identity

- An experience hacker will most likely change his MAC address
- Many times these modified MACs stand out as anomalies
 - 55:44:33:22:11:00 – common
 - 8F:21:47:AB:55:70 – unknown OUI, suspicious
 - Organizationally Unique Identifier (OUI) – 1st Three Octets
 - Duplicate MACs, two different devices, different RSSI values
 - Received Signal Strength Indication
- Lookout for strange MAC addresses, wireshark mappings to OUIs can easily help you identify these oddities

Layer 3 Evidence – Rogue Wireless Client IP Spoofing and MITM Attacks

Valid wireless client			Valid wired host			
194	48.995777	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply	
195	48.995829	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request	
197	49.995806	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply	
198	49.995855	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request	
355	121.199941	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply	
356	121.199985	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request	
357	122.195951	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply	
358	122.196001	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request	
362	123.195696	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply	
363	123.195748	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request	

Frame 197 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: IntelCor_2d:15:2a (00:1b:77:2d:15:2a), Dst: DellPcba_e5:03:5b (00:0d:56:e5:03:5b)

Internet Protocol, Src: 172.16.0.247 (172.16.0.247), Dst: 172.16.0.252 (172.16.0.252)

Internet Control Message Protocol

No. ↓	Time	Source	Destination	Protocol	Info
188	46.996242	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply
189	46.996251	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request
191	47.995864	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply
192	47.995911	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request
194	48.995777	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply
195	48.995829	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request
197	49.995806	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply
198	49.995855	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request
355	121.199941	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply
356	121.199985	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request
357	122.195951	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply
358	122.196001	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request
362	123.195696	172.16.0.247	172.16.0.252	ICMP	Echo (ping) reply
363	123.195748	172.16.0.252	172.16.0.247	ICMP	Echo (ping) request
+ Frame 357 (98 bytes on wire, 98 bytes captured)					
+ Ethernet II, Src: DellEsgP_71:71:b5 (00:0b:db:71:71:b5), Dst: DellPcba_e5:03:5b (00:0d:56:e5:03:5b)					
+ Internet Protocol, Src: 172.16.0.247 (172.16.0.247), Dst: 172.16.0.252 (172.16.0.252)					
+ Internet Control Message Protocol					

**Some of the other attack vectors
that we're seeing lately...**

Bluetooth Hacks picking up steam (again)

Bluetooth Hacks

“PIN pads replaced at “a fast food chain” to steal payment card details

More payment cards have been skimmed (financial details hijacked) as a result of PIN pads being replaced. This time the breach occurred at “a fast food chain” in a busy part of Edmonton, Canada. *A “Bluetooth” device was used in the phony PIN pads to transmit all the card details, using a wireless connection.*

The fraud was discovered when a large number of Edmonton cards started showing up with unusual activity in Montreal.”

Edmonton Police, March 18, 2007

Bluetooth

Bluetooth Specs

All Bluetooth devices operate at the 2.4 GHz band

Bluetooth defines 79 channels for communication on the 2.4 GHz band each channel being separated by 1 MHz

The frequency range 2.402 GHz - 2.480 GHz

Allows for 1600 frequency hops per second

Class	Maximum Permitted Power		Range (approximate)
	mW	dBm	
Class 1	100	20	~100 meters
Class 2	2.5	4	~10 meters
Class 3	1	0	~1 meters

```

bt ~ # hciconfig reset hci0
hci0:  Type: USB
      BD Address: 00:00:00:00:00:00 ACL MTU: 0:0 SCO MTU: 0:0
      DOWN
      RX bytes:0 acl:0 sco:0 events:0 errors:0
      TX bytes:0 acl:0 sco:0 commands:0 errors:0

bt ~ # hciconfig hci0 up
bt ~ # hciconfig
hci0:  Type: USB
      BD Address: 00:04:61: [REDACTED] ACL MTU: 192:8 SCO MTU: 64:8
      UP RUNNING
      RX bytes:85 acl:0 sco:0 events:9 errors:0
      TX bytes:30 acl:0 sco:0 commands:8 errors:0

bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
00:1D: [REDACTED]
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan

```

Bluetooth Detection

Identifying the services on the bluetooth device

Backtrack:

- hcitool – identify devices
- sdptool – identify services on device

Using this approach we can identify Bluetooth devices within 10 meters, and distinguish the radio types

Bottomline, we're looking for anomalies (strange bluetooth radios that might be imbedded in a POS system)

```
Shell - Konsole
bt ~ # hcitool scan
Scanning ...
00:1D:11:11:11:11 Palm Pre
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
^[[Abt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
bt ~ # hcitool scan
Scanning ...
bt ~ # sdptool browse 00:1D:11:11:11:11
Browsing 00:1D:11:11:11:11 ...
Service Description: Palm Smartphone
Service RecHandle: 0x10000
Service Class ID List:
"PnP Information" (0x1200)

Service Name: Audio/Video Service
Service Provider: Palm
Service RecHandle: 0x10001
Service Class ID List:
"Audio Source" (0x110a)
Protocol Descriptor List:
"L2CAP" (0x0100)
PSM: 25
"AVDTP" (0x0019)
uint16: 0x102
Profile Descriptor List:
"Advanced Audio" (0x110d)
Version: 0x0102

Service Name: Phonebook Access PSE
Service RecHandle: 0x10002
Service Class ID List:
"Phonebook Access - PSE" (0x112f)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 2
"OBEX" (0x0008)
Profile Descriptor List:
"Phonebook Access" (0x1130)
Version: 0x0100

Service RecHandle: 0x10003
Service Class ID List:
"AV Remote Target" (0x110c)
Protocol Descriptor List:
"L2CAP" (0x0100)
PSM: 23
"AVCTP" (0x0017)
uint16: 0x100
```


Windows 7 Virtual WiFi

Windows 7 – A whole new possibility of Rogue AP threats

Windows 7 (all version) provide Virtual Wifi with the operating the system, essentially allowing any desktop user to setup a Virtual Wireless Access Point!!!



Note that this is not an adhoc network, but an actually virtual access point that behaves, lives, and breathes like an actual Access Point!

Windows 7 Virtual WiFi

How?

Setup at the DOS Prompt

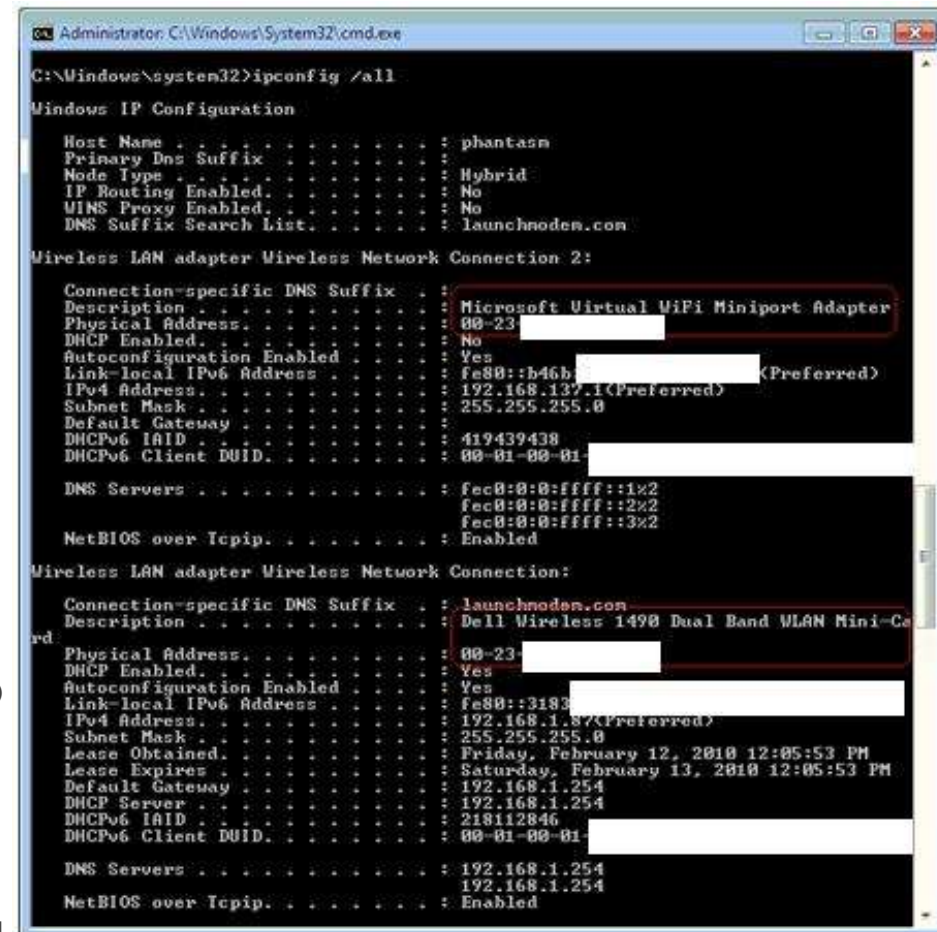
Share either a Wired or Wireless connection

The user can share their own desktop (like an ad-hoc network)

And the user can share their network connection with others

Wireless network may use authentication and encryption, BUT the user can share that connection with others, allowing those users to connect to the corporate network with weaker authentication & encryption

Note: This is native to the operating system! In all versions of Windows 7 (Starter through Ultimate)



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : phantasm
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : launchmodem.com

Wireless LAN adapter Wireless Network Connection 2:

Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Virtual WiFi Miniport Adapter
Physical Address. . . . . : 80-23-
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b46b
IPv4 Address. . . . . : 192.168.137.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 419439438
DHCPv6 Client DUID. . . . . : 00-01-00-01-

DNS Servers . . . . . : fec8:0:0:ffff::1%2
                        fec8:0:0:ffff::2%2
                        fec8:0:0:ffff::3%2
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Wireless Network Connection:

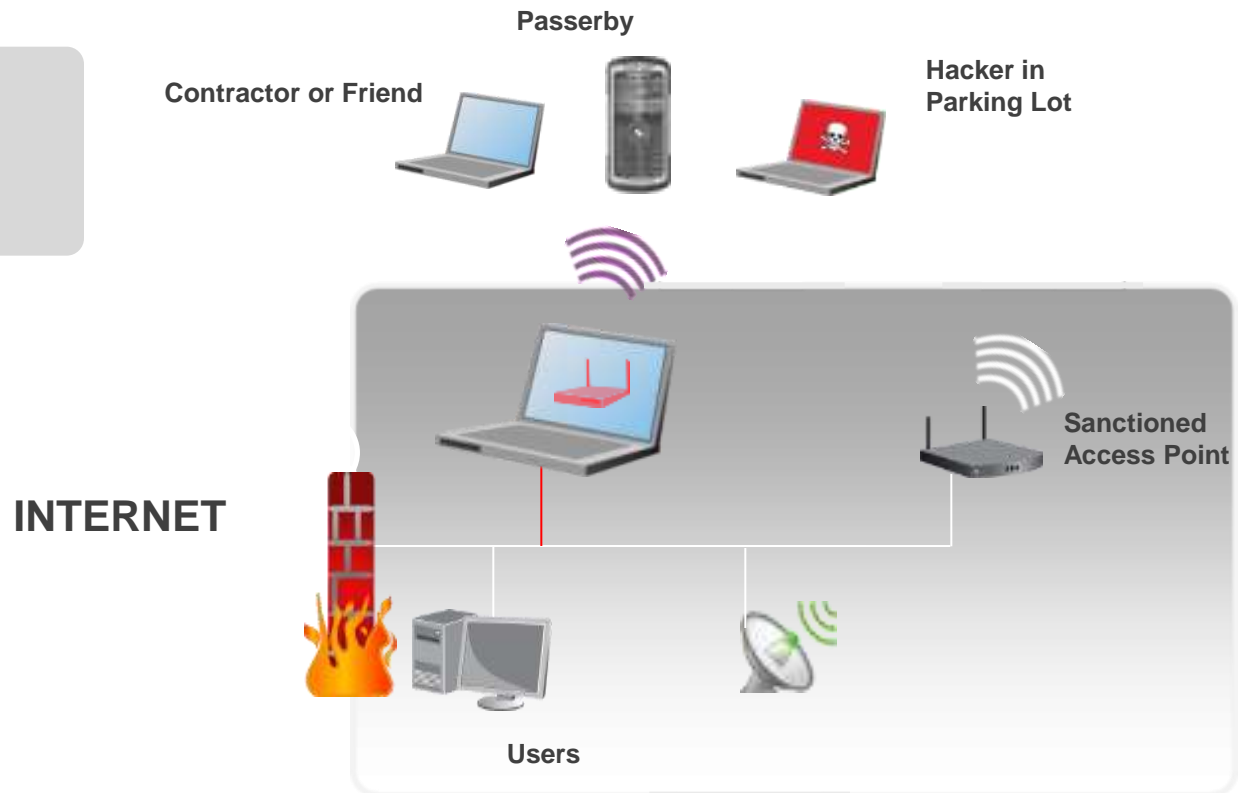
Connection-specific DNS Suffix . : launchmodem.com
Description . . . . . : Dell Wireless 1490 Dual Band WLAN Mini-Card
Physical Address. . . . . : 80-23-
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::3193
IPv4 Address. . . . . : 192.168.1.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, February 12, 2010 12:05:53 PM
Lease Expires . . . . . : Saturday, February 13, 2010 12:05:53 PM
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 218112846
DHCPv6 Client DUID. . . . . : 00-01-00-01-

DNS Servers . . . . . : 192.168.1.254
                        192.168.1.254
NetBIOS over Tcpip. . . . . : Enabled
```

Windows 7 Virtual Wifi

Windows 7 Virtual WiFi – Rogue AP on Wired Network

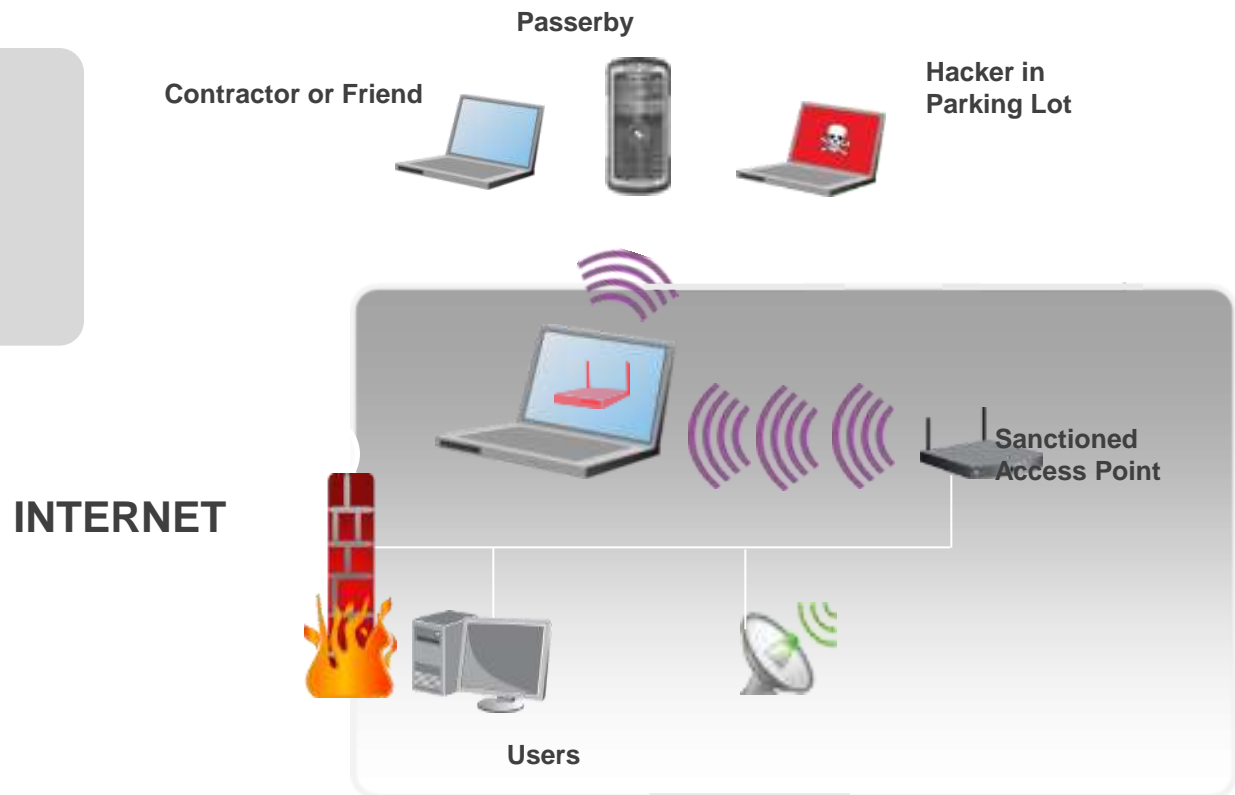
Windows 7 Virtual WiFi
Rogue AP on Wire



Windows 7 Virtual Wifi

Windows 7 Virtual WiFi – Rogue AP on Wireless Network

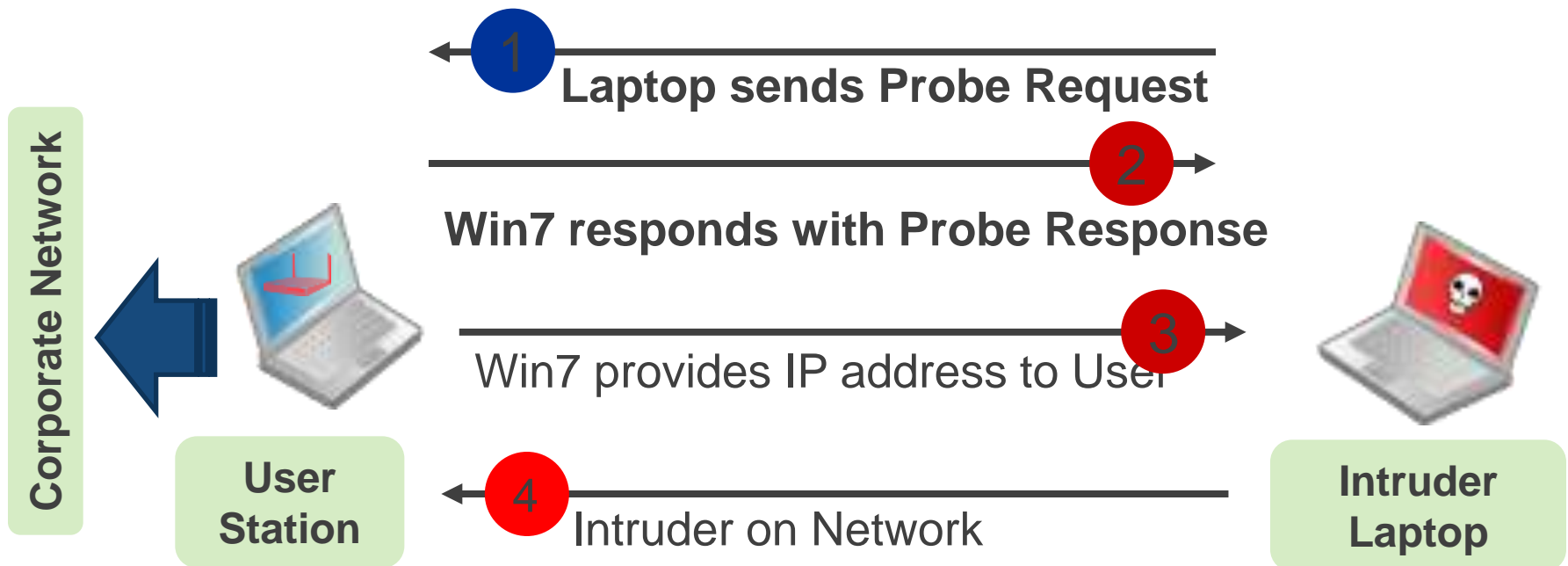
Windows 7 Virtual WiFi
Rogue AP on Wireless
(Wireless Bridge)



Win7 - Comparing packets from Access Points versus Wireless Clients

Your Windows 7 Laptop is now a Rogue AP on your network

How many Windows 7 laptops are in your network???



Wireless Layer 2 – Use are previous approach to detect Win7 Virtual WiFi



Incident Response & Forensic Analysis

Sources for analyzing wireless attacks



Historical

- Device logs/syslog
- Firewall logs (wireless switches, Access Points, Wired Firewall)
- Wireless IDS alarms, events, logs
- Wired IDS alarms, events, logs
- Remnants on wireless clients (registry, saved wireless networks, etc.)



Live

- Wired Sniffing
- Wireless Sniffing
- Spectrum Analysis
- Bluetooth
- RF Analysis, Heat Maps/Location Tracking
- Live analysis on IPS, WIPS, Firewalls, etc.
- Roaming behavior (from AP to AP, or client to client attacks)
- Others...

Final words...

Recommendations

Live Analysis

- Great, but you're probably conducting it post-breach
- still helpful if suspicious devices are still present

Wired Firewall, Access Points, Wireless Switches, and Servers
may provide very limited visibility into wireless attacks

- Probably NO visibility into wireless client attacks

**Windows SMS policies can possibly be used to disable Win7
Virtual WiFi**

- note that other operating systems are working on this feature as well...
- Currently available on Windows Server 2008, Windows 7, and drivers for Windows XP available from the Microsoft Research website

Final words...

Recommendations

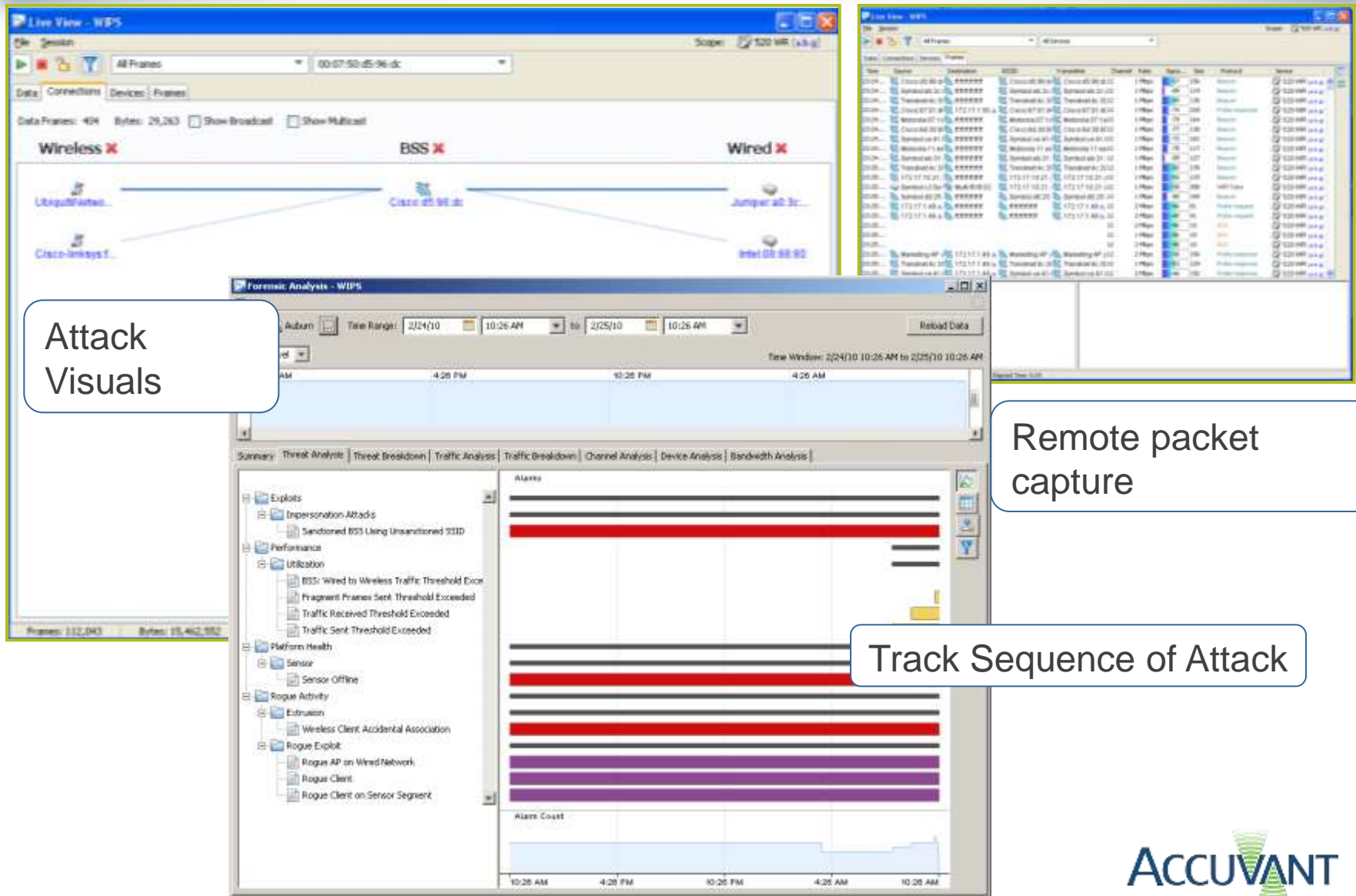
Mobile devices such as wifi-enabled phones are just as susceptible to wireless sniffing and wireless attacks, especially in insecure deployments.

- Products exist for enforcing policies on mobile phones

Wireless Intrusion Detection & Prevention can provide 24/7 monitoring

- Historical audit trails and forensic analysis of the steps leading up to a breach
- Mitigation & prevention of many of the aforementioned attacks
- Whether you have wireless or not, this is a must-have for a critical network.

Wireless Intrusion Detection & Prevention



Additional reading materials

Sites

The Greatest Hacking Breach in Cyber History

<http://hakin9.org/magazine/1528-email-security>

Joshua Wright

<http://www.willhackforsushi.com/>

AirDefense.net

What Hackers know that you don't (whitepaper)

Wireless Security Blog

<http://communities.motorola.com/>

Q&A

Thank You

mraggio@accuvant.com