

---

# Wireless Assessment on a Budget

---

Joshua Wright, InGuardians  
josh@inguardians.com

# Your Speaker

- Joshua Wright
- Senior Security Analyst, InGuardians
- Senior SANS Instructor, Ethical Hacking Wireless course author
- [josh@inguardians.com](mailto:josh@inguardians.com)
- [josh@willhackforsushi.com](mailto:josh@willhackforsushi.com)



# Outline

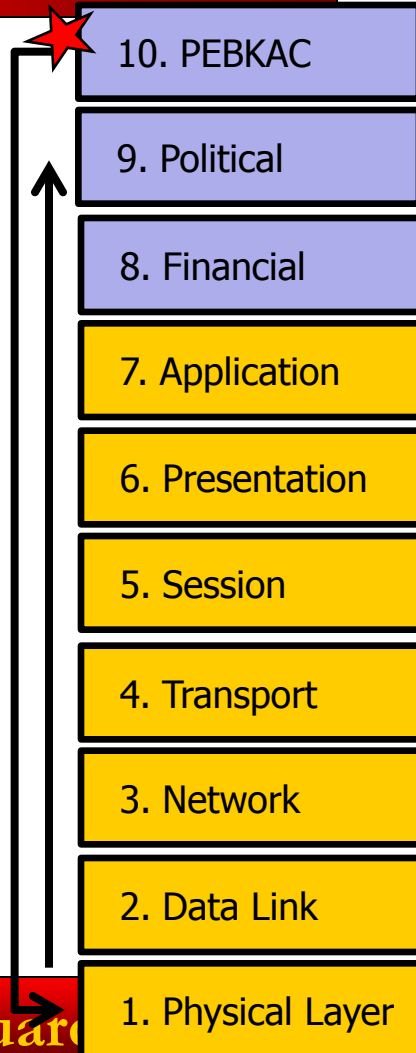
---

## Wireless Assessment Tasks and Tools

- Kismet Newcore to the Rescue
- Up and Running with Newcore
- Startup and Features
- Extensible Kismet
- Task Focus for Security, Auditing, Troubleshooting
- Conclusion

# Wireless Assessment Tasks

- Wired network troubleshooting is an established science
  - Layer 10, then troubleshoot layers 1-7
  - "Have you turned it off and on again?"
  - "Is it definitely plugged in?"



# Network World – 6/22/2009

- Wireless LAN Analysis Tool Comparison

Features vary among vendors

Company	Product	Version	List price	Type	Active survey	Passive survey
AirMagnet	Survey with Planner Module	6.0	\$4,695	P/A	•	•
Berkeley Varitronics Systems (BVS)	Swarm	1.5	\$2,500	A		•
Ekahau	Site Survey Pro	4.5.3	\$3,995	P/A	•	•
Motorola	LANPlanner	11.0	\$12,000	P/A	•	•
Motorola	SiteScanner	2.0.3	\$2,500	A	•	•
Nuts About Nets	Airhorn (with external antenna)	2.0.8359.0	\$135	Special		
Psiber	RF3D WiFiPlanner	1.0.21	\$795; \$395 for Lite version (up to 10 apps and 5 floors)	P		
VisiWave	Site Survey	2.0.6	\$549	A	•	•

# Wireless Assessments

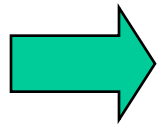
---

- Site survey planning and measurement
  - "Do we have enough coverage?"
- Security auditing
  - "Does the network comply with policy?"
- Penetration Testing and Vulnerability Assessment
  - "What opportunities are there to exploit the network?"
- Security Monitoring and IDS Analysis
  - "Is someone attacking my network?"

# Outline

---

- Wireless Assessment Tasks and Tools



## Kismet Newcore to the Rescue

- Up and Running with Newcore
- Startup and Features
- Extensible Kismet
- Task Focus for Security, Auditing, Troubleshooting
- Conclusion

# Kismet Introduction

---

- Console-based wireless analysis tool
- Passive; captures traffic from wireless cards in monitor mode
- Observes activity from all networks within range
  - With proper physical layer support
- Decodes activity and information of interest
- Wardriving tool of choice

# Kismet (Oldcore)

Network List (Autofit)								Info
Name	T	W	Ch	Pkts	Flags	IP Range	Size	Ntwrks
! 101	A	N	011	26		0.0.0.0	0B	49
+ ! Probe networks	G	N	---	1748		0.0.0.0	0B	Pckets
+ ! Adhoc networks	G	N	006	55080		0.0.0.0	3M	73623
! tsunami	A	N	001	12918	T4	192.168.6.48	140k	Cryptd
! <no ssid>	A	Y	003	163		0.0.0.0	1k	29
! linksys	A	N	006	1330	T4	192.168.1.102	16k	Weak
! colonie	A	Y	006	55		0.0.0.0	0B	0
! linksys	A	Y	006	1		0.0.0.0	0B	Noise
! 101	A	N	011	1		0.0.0.0	0B	98
! NYWLAN	A	N	003	25	T4	192.168.16.101	197B	Discrd
+ ! <Data networks>	G	N	---	1192		0.0.0.0	146k	98
! <no ssid>	A	Y	003	39		0.0.0.0	156B	
! 301a81	A	Y	006	57		0.0.0.0	78B	Discon
								00:01:14
Status								
Found new network "<no ssid>" bssid 00:02:2D:01:B7:26 Crypt N Ch 0 @ 0.00 mbit								
Found new network "DLW2" bssid 00:02:2D:1D:E9:40 Crypt Y Ch 1 @ 11.00 mbit								
Found IP 192.168.6.27 for tsunami::00:01:E6:45:37:D8 via UDP								
localhost:2501 TCP error: socket returned EOF, server has closed the connection.								
Battery: AC 190%								

# Kismet Newcore

---

- Development started in 2004 on a next-generation Kismet
- Legacy Kismet design had limitations
  - Monolithic functionality
  - No graceful error recovery
  - Static configuration and source detail
  - Non-intuitive configuration and UI
- Kismet Newcore adds functionality and features beyond what Oldcore provided

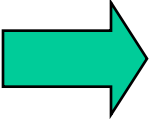
# Newcore Features

---

- New UI; all UI configuration done from through menu navigation
- Dynamic source add and removal
- New WIDS alerting and logging
- Graceful recovery from failures
- Plugin support
- Abstracted to support any wireless protocol (802.11 and DECT today)
- Free (as in free beer and free speech)

# Outline

---

- Wireless Assessment Tasks and Tools
- Kismet Newcore to the Rescue
-  Up and Running with Newcore
- Startup and Features
- Extensible Kismet
- Task Focus for Security, Auditing, Troubleshooting
- Conclusion

# Get Up and Running

---

- Some short steps to establish a system with Kismet Newcore
- Based on Backtrack 4 Pre-Final
  - Most current Backtrack release
- (Assuming you don't have a dedicated system for Kismet)

# Step 1. Download Backtrack

---

- Grab Backtrack 4 (pre-final or most current release)
- [www.remote-exploit.org/cgi-bin/fileget?version=bt4-prefinal-iso](http://www.remote-exploit.org/cgi-bin/fileget?version=bt4-prefinal-iso)
- 1.3 GB, MD5:  
b0485da6194d75b30cda282ceb629654

## Step 2. Burn a DVD

---

- Seriously, burn a DVD?
- I don't bother with optical media anymore
- Unetbootin for Windows or Linux
  - Makes any bootable ISO bootable on a USB drive
  - Faster, easier, greener
- Note: Still RO boot environment

<http://unetbootin.sf.net>

# UNetbootin

**UNetbootin**

☐ Distribution    == Select Distribution ==    == Select Version ==

Welcome to [UNetbootin](#), the Universal Netboot Installer. Usage:

1. Select a distribution and version to download from the list above, or manually specify files to load below.
2. Select an installation type, and press OK to begin installing.

☒ Diskimage    ISO    c:\Josh Wright\My Documents\My Virtual Machines\bt4-pre-final.iso    ...

☐ Custom    Kernel:    ...    Initrd:    ...

Options:    ...

☒ Show All Drives (Use with Care)

Type: USB Drive    Drive: E:\    OK    Cancel

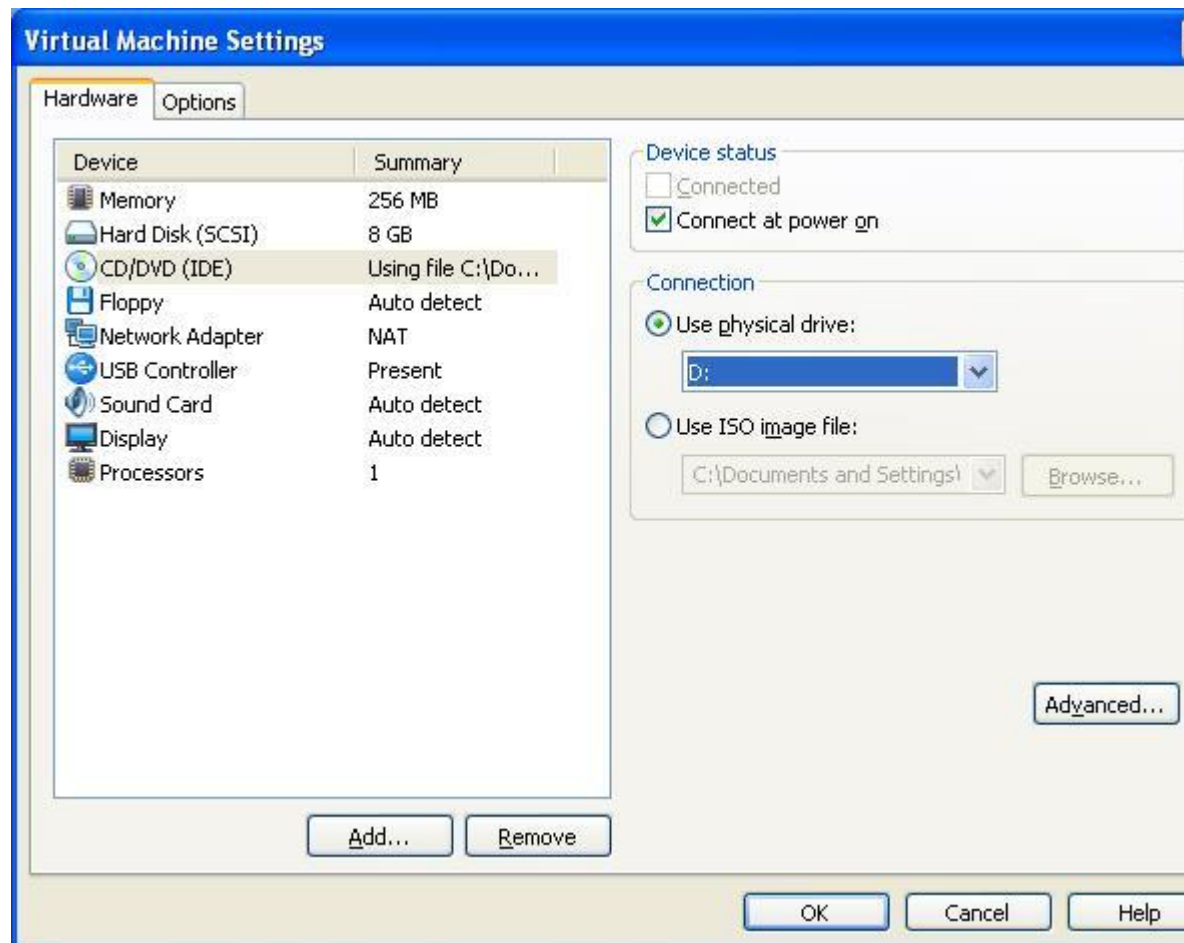
# Decisions, Decisions

---

- Option 1: Create a VMware Image
  - Little fuss, build a guest, distribute to multiple systems if desired
  - Only works for USB wireless adapters (seriously limits 802.11a support)
- Option 2: Boot from a USB Drive
  - Access to PC-Card and internal wireless adapters
  - Have to reboot out of native OS
  - Requires 8 GB USB drive or larger

# Option 1: VMware

- Grab VMware Server (free) or buy Workstation (\$190)
- Guest boots from real DVD or ISO file
- Any size HDD, 256MB RAM works well



## Option 2: USB Drive

---

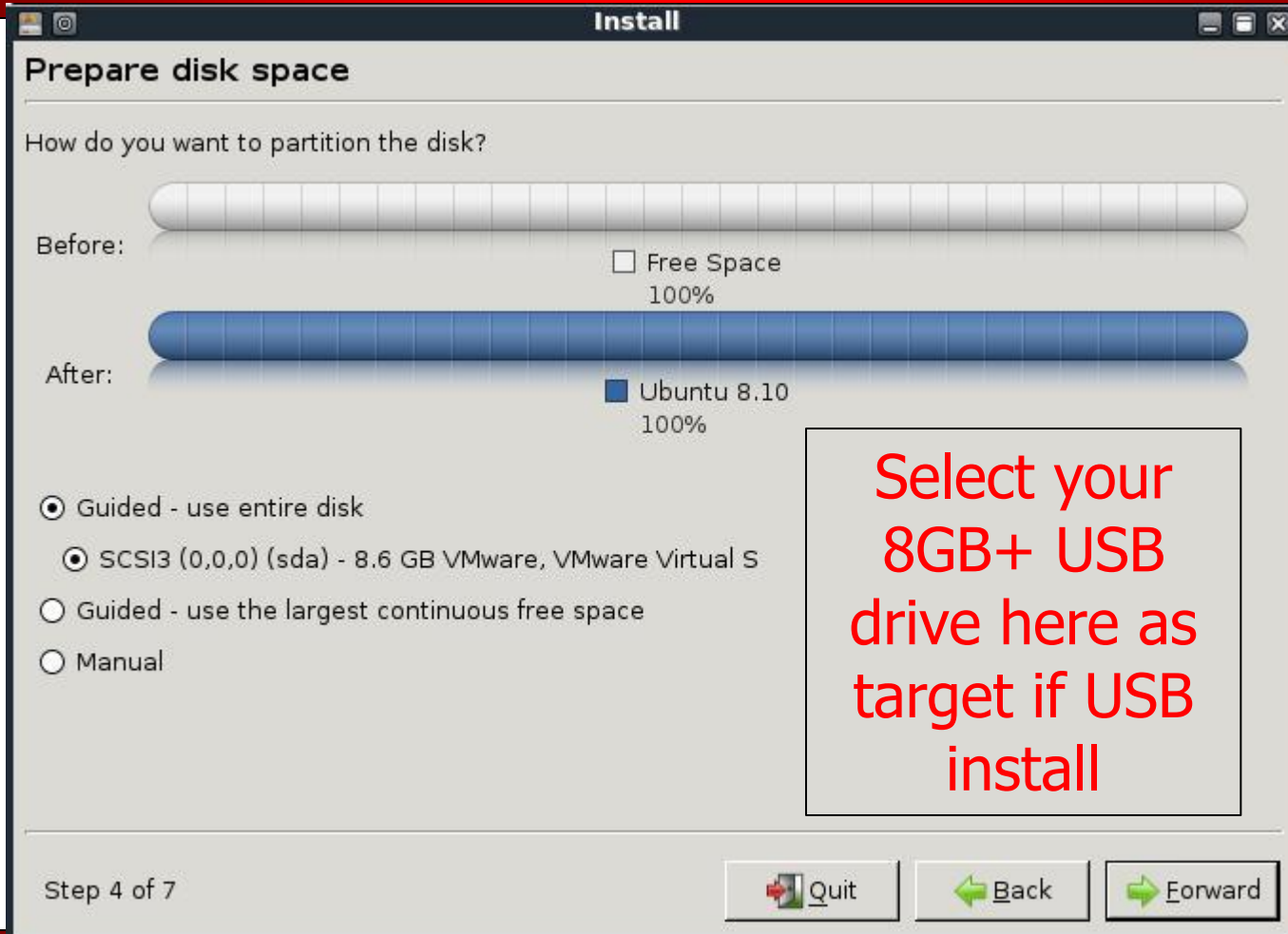
- Boot from DVD (or UNetbootin USB drive)
- If UNetbootin, will require a second USB drive for OS install
  - USB install target must be 8 GB or greater

# Step 3. Boot and Install

---

- Select default option from boot menu
- Run "startx" from "root@bt:~#" prompt
  - If USB install, insert target drive now
- Single-click "install.sh" on Desktop
  - Select "Continue anyway" at "Language crashed" dialog
- Follow install wizard steps for persistent Backtrack 4 installation

# Partitioner



Select your  
8GB+ USB  
drive here as  
target if USB  
install

# Step 4. Download and Install Newcore

---

- Doesn't BT4 already have Kismet Newcore?
  - Yes, but it's broken, and we need the source for additional functionality

```
# dhclient eth0
# cd /usr/src
# svn co https://www.kismetwireless.net/code/svn/trunk kismet
# cd kismet
# ./configure --prefix=/opt && make && make install
```

Update Kismet at any time

```
# cd /usr/src/kismet
# svn up
# make && make install
```

# Step 5. Start Kismet

```
# cd /dir/where/you/want/kismet/logging/files
# /opt/bin/kismet
```

```
~ Kismet Sort View Windows
Name          T C Ch Pkts Size
[ --- No networks seen --- ]

Kismet
Not
Connected

Terminal colors
Some terminals don't display some colors (notably, dark grey)
correctly. The next line of text should read 'Dark grey text':
Dark grey text
Is it visible? If you answer 'No', dark grey
will not be used in the default color scheme. Remember, you
can always change colors to your taste by going to
Kismet->Preferences->Colors.

0 [ No ] [ Yes ]
```

# Outline

---

- Wireless Assessment Tasks and Tools
- Kismet Newcore to the Rescue
- Up and Running with Newcore

## Startup and Features

- Extensible Kismet
- Task Focus for Security, Auditing, Troubleshooting
- Conclusion

# Startup

- Kismet will prompt to start the Kismet Server at startup
- Once the Kismet server has started, you will be prompted for the first packet source

```
No sources
Kismet started with no packet sources defined.
No sources were defined or all defined sources
encountered unrecoverable errors.
Kismet will not be able to capture any data until
a capture interface is added.  Add a source now?
[ No ] [ Yes ]
```



```
Add Source
Interface wlan0
Name
Opts
[ Cancel ] [ Add ]
```

# Kismet Sources

---

- Specify the available wireless interface as a packet source
  - e.g. "wlan0", "wlan1", etc.
- Kismet will identify the needed information, place the interface in passive capture mode
- Add as many sources as you want from Kismet → Add Source
- Can also specify libpcap wireless packet capture files as sources

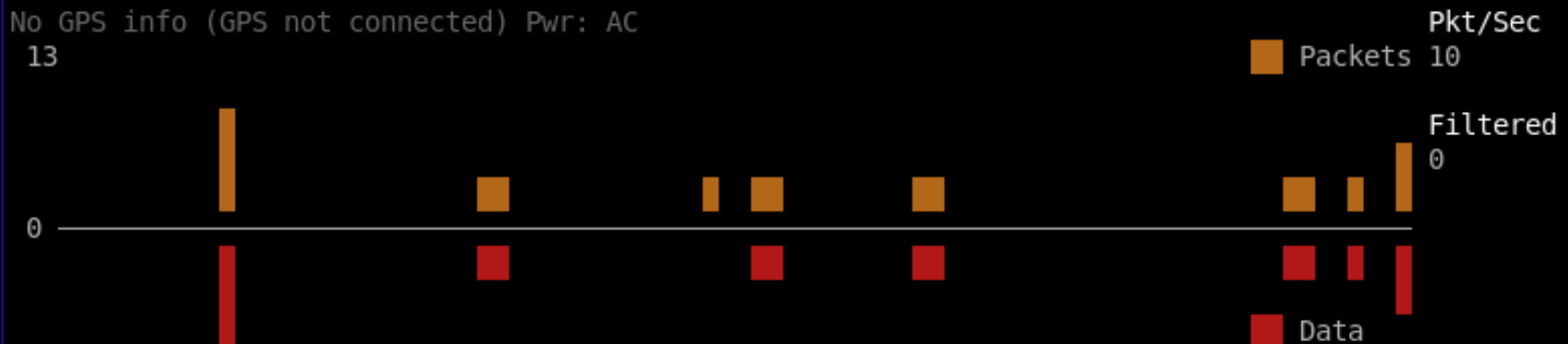
# Kismet Newcore Navigation



~ Kismet Sort View Windows

Name	T	C	Ch	Pkts	Size	Kismet_200
somethingclever	A	O	1	56	1K	
Nicole	A	W	11	39	0B	Elapsed
linksys	A	N	6	19	0B	00:01.33
+ Autogroup Probe	P	N	---	14	0B	
NETGEAR	A	N	11	2	0B	Networks
Salty Swan	A	O	6	2	0B	8

No GPS info (GPS not connected) Pwr: AC  
13



encryption yes, channel 6, 54.00 mbit  
INFO: Detected new managed network "NETGEAR", BSSID 00:1E:2A:03:F0:76, encryption  
no, channel 11, 54.00 mbit  
INFO: Detected new probe network "<Any>", BSSID 00:22:69:01:35:71, encryption no,  
channel 0, 54.00 mbit

wlan0  
Hop

# UI Configuration

~ Kismet Sort View Windows

Name

- . Belkin N1\_Wireles
- ! NETGEAR
- ! Nicole
- . Salty Swan
- . boydhome
- ! freedom
- ! linksys
- ! somethingclever

BSSID: 00:14:BF:0

<Hidden SSID>

33

0

Network List Column Preferences

Column	Show	Description
shortname	No	Shortened name or SSID
packdata	No	Number of data packets
packllc	No	Number of LLC/Management packe
packcrypt	No	Number of encrypted data packe
bssid	No	BSSID
clients	No	Number of associated clients
beaconperc	No	Percentage of expected beacons
signal_dbm	No	Signal (in dBm, depends on sou
signal_rssi	No	Signal (in RSSI, depends on so
freq_mhz	No	Frequency (MHz)
manuf	No	Manufacturer
11dcountry	No	802.11d Country

Select with space, change order with +/-

[ Cancel ] [ Save ]

Kismet\_200

Elapsed  
00:03.31

Networks  
16

Packets  
: Cisco-Li 1461

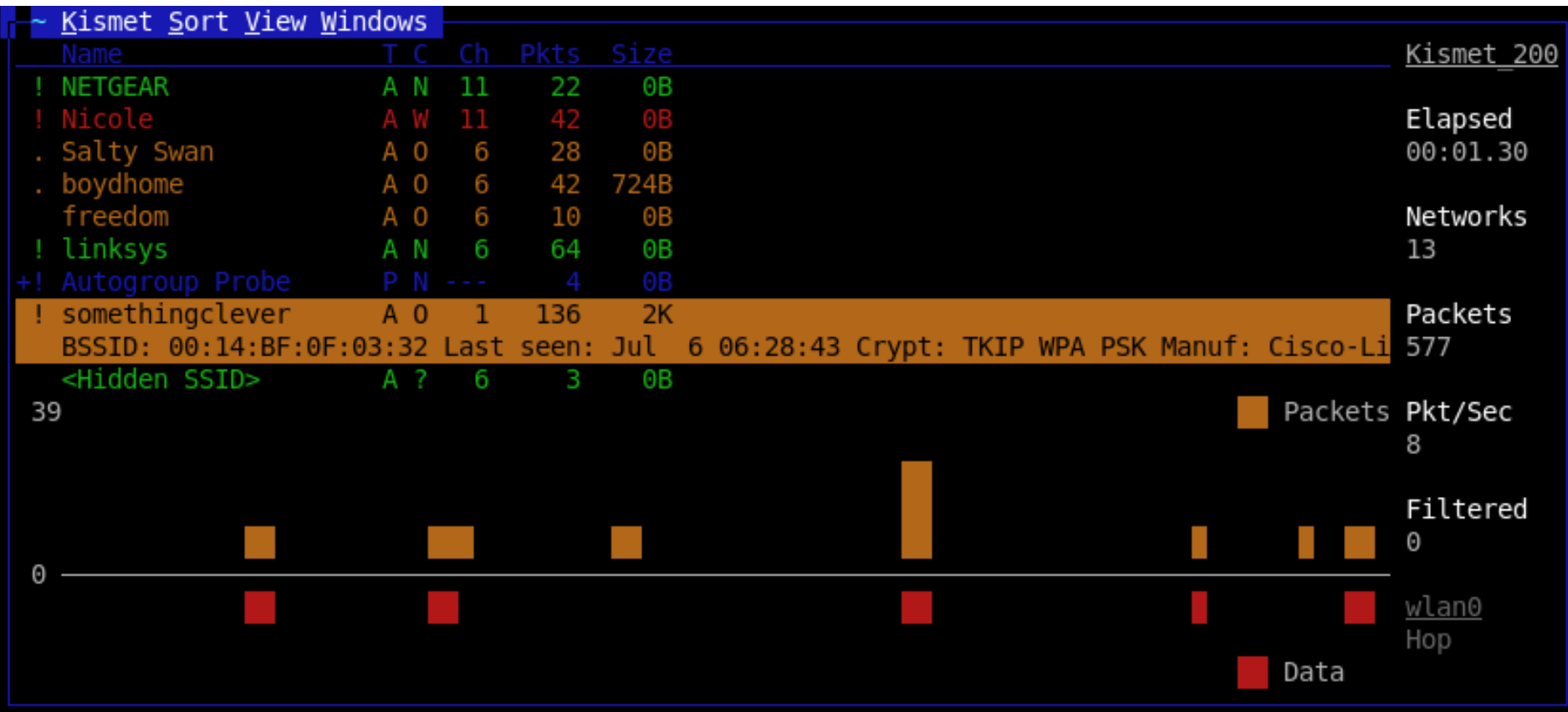
Packets Pkt/Sec  
0

Filtered  
0

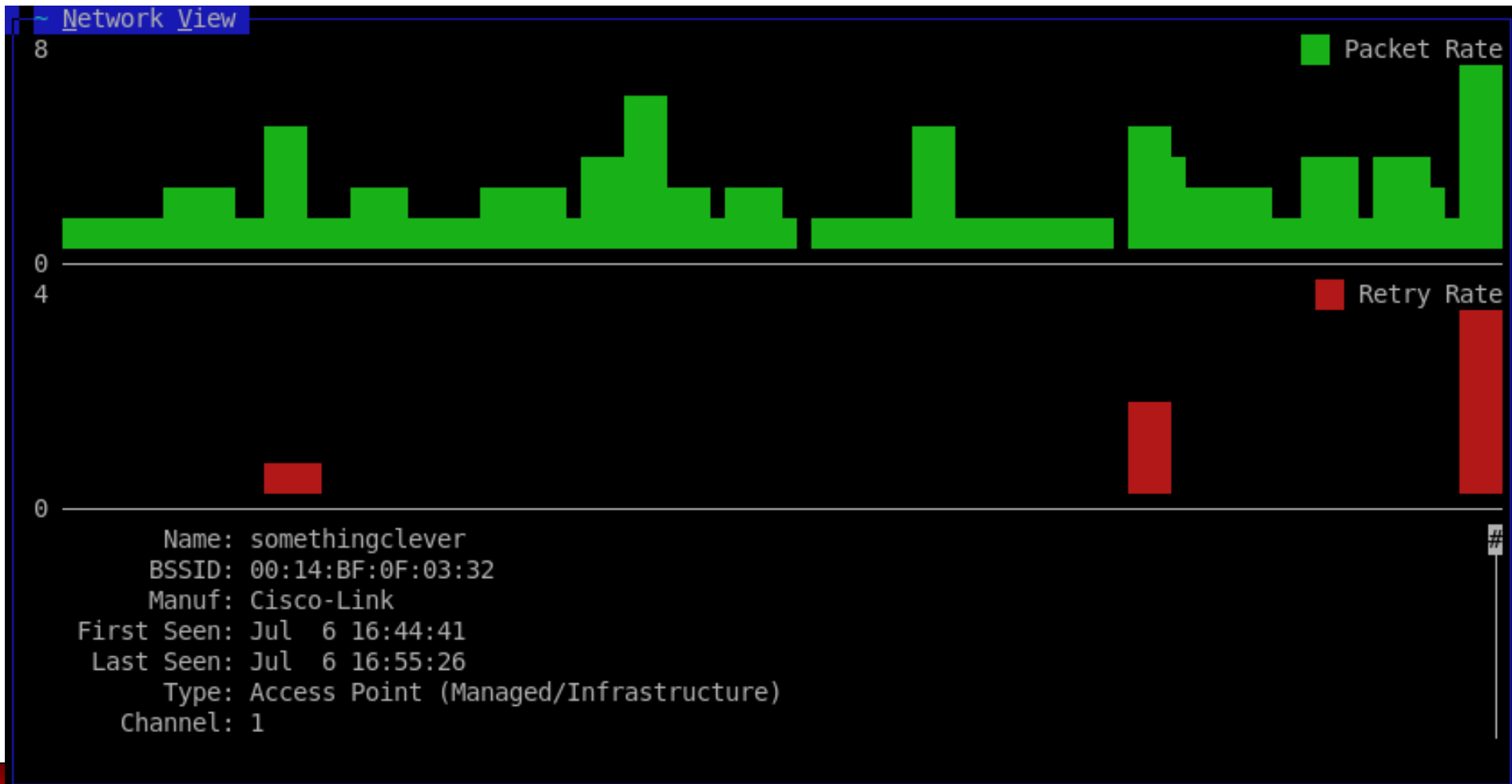
wlan0  
Hop

Data

# Navigating Networks



# Network Detail



# Client Detail

~ Clients Sort Windows

Selected network: 00:02:2D:00:41:05 (DEFCON)

MAC	Pkts	Data	Type	DHCP	Host	DHCP	OS	Best-Guess	IP
00:02:2D:61:82:0F	7	7	Wired/AP	---	---	---		0.0.0.0	
00:02:2D:64:0F:E2	1	1	Wired/AP	---	---	---		0.0.0.0	
00:02:2D:7B:AD:34	11	11	Wired/AP	---	---	---		69.69.69.46	
00:02:2D:86:65:AF	7	7	Wired/AP	---	---	---		0.0.0.0	
00:02:2D:90:0B:D2	1	1	Wired/AP	---	---	---		0.0.0.0	
00:02:6F:03:FE:63	7	7	Wired/AP	---	---	---		172.23.5.109	
00:02:8A:3A:EE:1F	1	1	Wired/AP	---	---	---		0.0.0.0	
00:03:93:EA:EA:A8	6	6	Wired/AP	---	---	---		69.69.69.249	
00:04:5A:CD:C2:E9	6	6	Wired/AP	belle	MSFT	5.0		0.0.0.0	
00:04:E2:07:F9:69	8	5	Wireless	---	---	---	Linux 2.4.0	0.0.0.0	
Last seen: Jul 6 08:27:26 IP: 0.0.0.0									
00:05:3C:08:86:E2	5	5	Wireless	dev-MSELLE	MSFT	5.0		0.0.0.0	
00:06:25:01:46:6B	8	8	Wired/AP	---	---	---		172.168.21.252	
00:06:25:01:CB:CC	1	1	Wired/AP	---	---	---		0.0.0.0	
00:06:25:15:4E:7A	1	1	Wired/AP	---	---	---		0.0.0.0	
00:06:25:2A:20:7E	4	4	Wired/AP	---	---	---		0.0.0.0	
00:06:25:42:2C:D6	1	1	Wired/AP	---	---	---		0.0.0.0	
00:06:25:A9:7F:20	59	59	Wired/AP	---	---	---		192.168.16.253	
00:06:25:AE:D2:12	1	1	Wired/AP	rxawxpvlk	MSFT	5.0		0.0.0.0	

# Outline

---

- Wireless Assessment Tasks and Tools
- Kismet Newcore to the Rescue
- Up and Running with Newcore
- Startup and Features

## Extensible Kismet

- Task Focus for Security, Auditing, Troubleshooting
- Conclusion

# Device Manufacturer Name

MAC	Type	Freq	Pkts	Size	Manuf
00:23:69:96:2A:6D	Wired/AP	2457	988	48K	Unknown
00:22:69:01:35:71	Wireless	2462	244	26K	HonHaiPrec
00:0D:56:32:25:8B	Wired/AP	2457	74	7K	DellPcbaTe
00:23:69:96:2A:6B	Wired/AP	2447	44	16K	Unknown
00:24:1E:BF:50:53	Wired/AP	2437	6	956B	Unknown

- Kismet relies on Wireshark's "manuf" file to identify manufacturers
- File can be updated with make-manuf script (not distributed with BT4)

```
# wget http://anonsvn.wireshark.org/wireshark/trunk/wka.tmpl
# wget http://anonsvn.wireshark.org/wireshark/trunk/manuf.tmpl
# wget http://anonsvn.wireshark.org/wireshark/trunk/make-manuf
# perl make-manuf
# mv manuf /usr/share/wireshark
```

# Logging

---

- .pcapdump – Libpcap capture
- .alert – WIDS alert events
- .gpsxml – GPS logging data
- .nettxt – Network summary info
- .netxml – XML-formatted network detail info

# Netxml Logging File

---

- Can be imported into Excel for post-processing analysis
  - Rename to ".xml", select "read-only workbook" when opening
- Requires Internet access to download Kismet DTD file
- Allows you to graph results, add details for additional analysis

# Reporting on AP Uptime

$$"=U267/(1000000 * (60 * 60 * 24))"$$

Microsoft Excel window: Kismet-20090706-08-46-13-1.xml [Read-Only] - Microsoft Excel

Formula Bar:  $(60 * 60 * 24) = 1 \text{ day in sec}$   
 $1000000 = \text{usec in 1 second}$

	T	U	AE	AF	CE	CF	CG
1			AP Uptime				
2	/wireless-network/	/wireless-network/	bsstimestamp	/wireless-netw	/wireless-net	/wireless-network/	/wireless-network/SSID
253	00:22:69:01:35:71	0		0 HonHaiPrec			
254	00:22:69:01:35:71	0		0 HonHaiPrec			
255	00:22:69:01:35:71	0		0 HonHaiPrec			
256	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link			
257	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link			
258	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link			
259	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link			
260	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link			
261	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link			
262	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link			
266	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link	PSK	boydhome	FALSE
267	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link	AES-CCM	boydhome	FALSE
268	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link			
269	00:23:69:96:2A:6D	8.23216E+11	9.527966819	Cisco-Link			

Ready | Kismet-20090706-08-46-13-1 | Average: 14.65730799 | Count: 292 | Sum: 4265.276625 | 100%

# Plugins

---

- Kismet includes a plugin architecture to extend functionality
  - Written in C++
  - Retrieve packet details, previously decoded data
  - Modify UI to add menu's, new windows, detail lines, columns, etc.
- Distributed with Kismet: Aircrack-PTW, Spectools
- Third-party: DECT wireless sniffing

# Building Plugins

```
# cd /usr/src/kismet/plugin-ptw
# export KIS_SRC_DIR=/usr/src/kismet # Only if src is diff.
# export KIS_DEST_DIR=/opt
# make && make install
```

- Kismet → Plugins
  - Status of plugins, version information
  - Enable or disable UI plugins
  - See list of Kismet Server plugins

```
For more information about Kismet UI plugins see the README
Select a plugin and press enter to toggle loaded/unloaded
Kismet UI Plugins:
Client Plugin      Auto Load  Loaded
spectools ui.so    yes         Pending
dect_cliplugin.so  yes         Pending

Server plugins cannot currently be loaded/unloaded from the UI
Kismet Server Plugins:
Server Plugin      Version    Description
DECT                1.0.0      DECT sniffer interface
SPECTOOL           2009-05-R  Aircrack PTW Plugin
AIRCRAK-PTW        1.0.0      Aircrack PTW Plugin

[                               Close                               ]
```

# Plugin Ideas – More?

---

- Deauth selected user
  - Useful for recovering cloaked SSID or identifying authentication in use
- Client fingerprinting
  - Leverage active or passive device fingerprinting techniques
- Metasploit integration
  - Send driver exploits to every/any target

# Outline

---

- Wireless Assessment Tasks and Tools
- Kismet Newcore to the Rescue
- Up and Running with Newcore
- Startup and Features
- Extensible Kismet
- ➡ Task Focus for Security, Auditing, Troubleshooting
- Conclusion

# System Administrators

---

- Poor performance on the wireless network complaint
- Things to observe:
  - What AP are the clients connecting to?
  - Are all AP's properly configured?
  - Lots of retries indicating poor connections or noise
  - Lots of missed beacons indicating noise or faulty Aps
  - What channels are being utilized?

# ~ Kismet Sort View Windows

Name	T	C	Ch	Pkts	Manuf	Clnt	Cty	Bcn%	Sig	Kismet 200
! somethingclever	A	O	1	124	Cisco-Link	4	---	80%	-51	
BSSID: 00:14:BF:0F:03:32 Last seen: Jul 6 10:38:32 Cr: TKIP WPA PSK Manuf:										Elapsed
Autogroup Probe	P	N	---	3	HonHaiPrec	1	---	---	---	00:00.30
Nicole	A	W	11	31	BelkinInte	1	US	40%	-77	
boydhome	A	O	6	11	Cisco-Link	3	---	---	---	Networks
NETGEAR	A	N	11	12	Netgear	1	---	20%	-77	6
MAC	Pkts	Data	Type	DHCP	Host	DHCP	OS	Best-Guess	IP	
00:06:DC:42:18:24	1	1	Wired/AP	---	---	---	---	0.0.0.0	---	Packets
! 00:14:BF:0F:03:32	87	0	Wired/AP	---	---	---	---	0.0.0.0	---	228
! 00:18:8B:AD:2A:C7	10	10	Wired/AP	---	---	---	---	0.0.0.0	---	
! 00:21:5C:7E:70:C3	26	26	Wireless	---	---	---	---	0.0.0.0	---	Pkt/Sec
										17
										Filtered
										0

## ~ Network View

Length: 15

Type: Beacon (advertising AP)

Encryption: WPA TKIP PSK

Beacon %: 100

Signal: -74dBm (max -40dBm)

Noise: -67dBm (max -67dBm)

Packets: 7104

Data Packets: 5685

Mgmt Packets: 1419

Crypt Packets: 5098

Fragments: 0/sec

Retries: 34/sec

Retries are normal in  
small numbers;  
more than sustained  
10% is a problem



Signal and Noise/Channel

Packet Rate (real time)

Data Frames (cumulative)

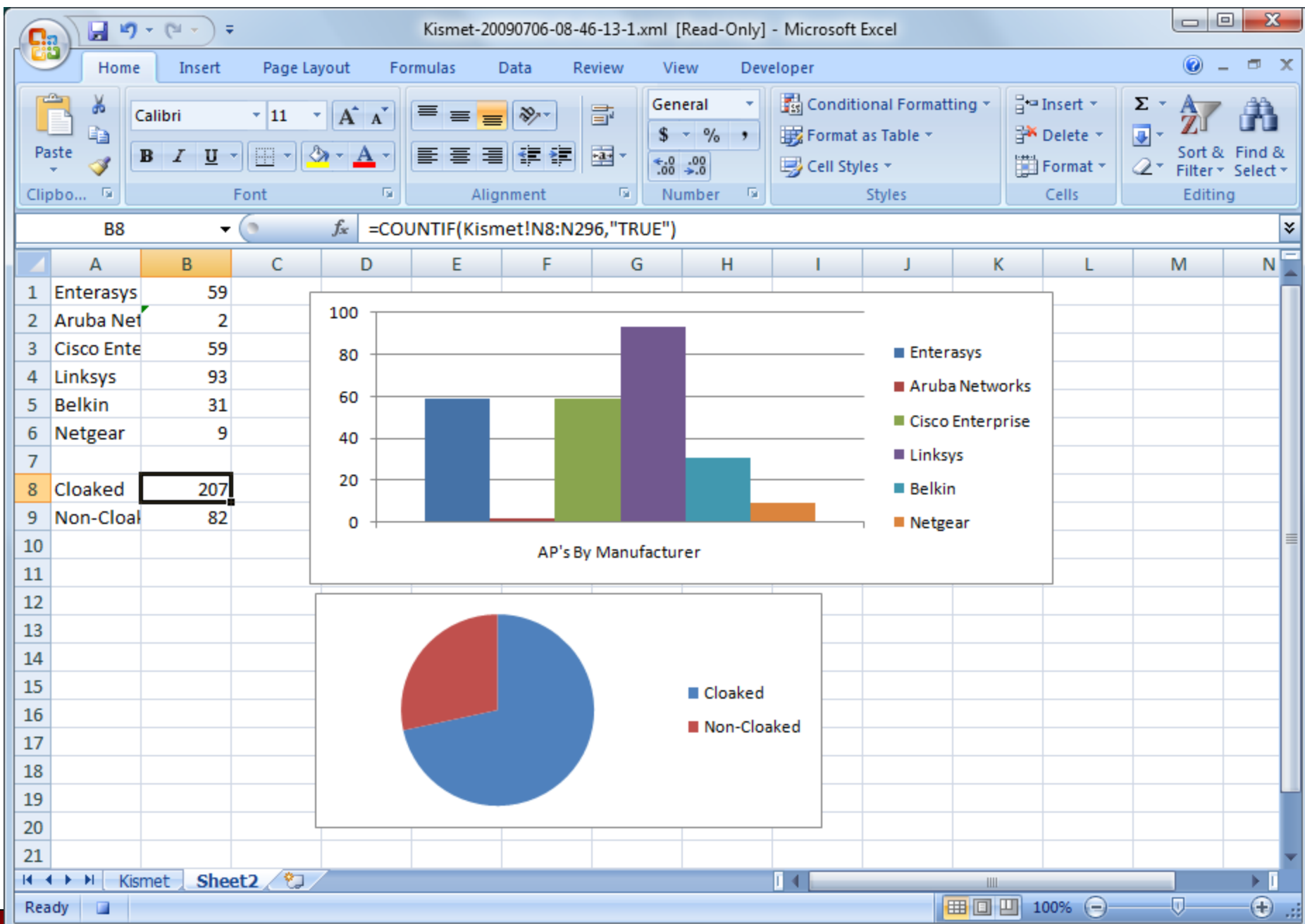
Networks Count (Yellow is historic, green is currently active)

Detail View (scroll with arrow keys)

# Auditors

---

- Are the networks configured per specification?
  - SSID cloaking enabled/disabled?
  - Appropriate encryption and authentication settings?
  - Are there unencrypted networks (when there shouldn't be)?
- Kismet walkthrough while channel hopping, post-processing analysis



# Security Analysts

---

- Network discovery and analysis
  - Are there open APs or weak crypto?
  - What are the clients on the network?
  - What kind of EAP types are in use?
- Post-processing data evaluation
  - Third-party tools with Kismet pcap files, XML records, nettxt summaries

# Multiple Interface Control

~ Kismet Sort View Windows

Name	T	C	Ch	Pkts	Size	BSSID	Clnt	Cty	Bcn%	Seen	By	Kismet_200
+ Autogroup Probe	P	N	---	3	0B	00:20:48:00:30:41	0	---	---	---		
Beacon Wi-Fi Network	A	N	11	7	0B	00:03:52:96:50:B0	1	---	---	wlan0		Elapsed
! Beacon Wi-Fi Network	A	N	11	10	0B	00:03:52:A2:61:40	1	---	10%	wlan0		00:00.52
Belkin_N1_Wireless_A	A	N	6	9	128B	00:1C:DF:A4:8C:93	1	---	---	wlan0		
Dynex	A									wlan0		Networks
Johnswireless	A									wlan0		17
! NETGEAR	A									wlan0		
NETGEAR	A		wlan1							wlan0		Packets
! Nicole	A									wlan0 wlan		372
BSSID: 00:1C:DF:B2:E6:4										kinInte		
. Salty Swan	A									wlan0		Pkt/Sec
! boydhome	A									wlan0 wlan		1
default	A									wlan0		
freedom	A									wlan0		Filtered

31 Rate 5

( ) Lock (\*) Hop ( ) Dwell

Channels 1,5,9,2,6,10,3,7,11,4,8

Cancel [ Change ]

0

One interface channel hops, the other sticks to a channel of interest.

■ Packets 0

■ wlan0 Hop

■ wlan1 6

■ Data

# Passive WEP Cracking Plugin

~ Kismet Sort View Windows

Name	T	C	Ch	Pkts	Manuf	Clnt	Cty	Bcn%	Sig	Kismet	200
erahs	A	W	8	15488	Cisco	206	---	---	---		
BSSID: 00:0D:29:4A:B8:5A Last seen: Jul 6 17:59:55 Crypt: WEP M											Elapsed
+ Autogroup Probe	P	N	---	892	Mixed	0	---	---	---		00:01.58
erahs	A	W	11	462	Cisco	31	---	---	---		
Hearst	A	W	6	430	Cisco	4	---	---	---		Networks
hhonors	A	N	11	329	Cisco	4	---	---	---		67
Hearst	A	W	9	313	Cisco	1	---	---	---		
MAC	Pkts	Data	Type	DHCP	Host	DHCP	OS	Best	Packets		
00:01:23:45:67:FF	1	1	Wired/AP	---		---		0.0.	159338		
00:01:F4:EC:63:BB	145	141	Wireless	---		---		0.0.			
00:02:2D:0E:05:9E	254	254	Wired/AP	---		---		0.0.	Pkt/Sec		
00:02:2D:46:1A:3D	19	19	Wired/AP	---		---		0.0.	0		
00:02:2D:58:95:84	4	4	Wired/AP	---		---		0.0.			
00:02:2D:59:2E:9B	1707	1705	Adhoc	---		---		0.0.	Filtered		
00:02:2D:69:4A:93	1	1	Wired/AP	---		---		0.0.	0		

ERROR: Pcap file reached end of capture

INFO: Failed to crack WEP key on 00:0D:29:4A:B8:5A: Not enough data collected yet

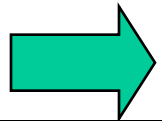
INFO: Trying to crack WEP key on 00:0D:29:4A:B8:5A: 79906 IVs

INFO: Cleaned up WEP data on 00:0D:29:4A:B8:5A

# Outline

---

- Wireless Assessment Tasks and Tools
- Kismet Newcore to the Rescue
- Up and Running with Newcore
- Startup and Features
- Extensible Kismet
- Task Focus for Security, Auditing, Troubleshooting



Conclusion

# It's Not All Rosy:

---

- Lack of cumulative counters (N/sec for fragments, retries)
- Missing functionality over Oldcore (data strings dump, Cisco AP name decoding, BSS timestamp reporting)
  - These features could be user-contributed plugins
- No more 1-keystroke navigation
- No more gpsmap :( replaced with kismap.py using Google Maps, but not scaling well to lots of data
- Still some bugs to work out
  - EAP-type decoding is not working

# Summary

---

- Kismet continues to be a powerful analysis tool
- New interface has useful features
- Extensibility gives Kismet lots of usefulness now and in the future
- Still developing, but recommend getting to know and use it now!

# Thank You -- Q+A

---

Joshua Wright  
Office/Mobile: 401-524-2911  
[www.inguardians.com](http://www.inguardians.com)

[josh@inguardians.com](mailto:josh@inguardians.com)  
[josh@willhackforsushi.com](mailto:josh@willhackforsushi.com)  
[www.willhackforsushi.com](http://www.willhackforsushi.com)

**SANS Ethical Hacking Wireless Course**  
[www.sans.org/training/description.php?mid=3](http://www.sans.org/training/description.php?mid=3)

Also check out my presentation on  
Saturday night – Smart Grid Security  
Challenges and Opportunities!

Twitter:  
[joswr1ght](https://twitter.com/joswr1ght)

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

# Hands-On Bonus

---

- DVD of Backtrack4 Pre-Final
- Chance to use Kismet Newcore hands-on in the classroom
- You will need a wireless card
  - Built-in or external
  - Sorry SEC617 students, AirPcap adapters not working ... yet

# Short Instructions

---

- Accept default boot selection, run "startx" at "root@bt4:~#" prompt
- Click terminal icon to start a shell
  - Black square on bottom-left corner with ">\_"
  - Consider maximizing the window and reducing the font size with Settings → Font → Shrink Font
- Connect to the network and update Kismet Newcore to the latest version
- Run Kismet, experiment with menu interface and network details
- Call Josh over to help with any questions or problems

# After Booting

Note: DVD is Non-Persistent (you'll need to do this each time until you do a BT4 install)

```
root@bt4:~# iwconfig wlan0 essid SANS-ROGUE01
root@bt4:~# dhclient
root@bt4:~# apt-get update
root@bt4:~# apt-get install kismet-newcore
root@bt4:~# killall dhclient
root@bt4:~# kismet
```

Answer the prompts that follow, use tab to navigate to different fields.

When prompted to add a source, select "Yes" then specify "wlan0" as the Intf, leaving Name and Opts blank.

Backtick or tilde (`/~) opens the menu, use arrow keys for navigation.