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
- 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

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

<table>
<thead>
<tr>
<th>Network</th>
<th>Type</th>
<th>Channel</th>
<th>Packets</th>
<th>Flags</th>
<th>IP Range</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>AN</td>
<td>011</td>
<td>26</td>
<td></td>
<td>0.0.0.0</td>
<td>0B</td>
</tr>
<tr>
<td>Probe networks</td>
<td>GN</td>
<td>---</td>
<td>1748</td>
<td></td>
<td>0.0.0.0</td>
<td>0B</td>
</tr>
<tr>
<td>Adhoc networks</td>
<td>GN</td>
<td>006</td>
<td>55080</td>
<td></td>
<td>0.0.0.0</td>
<td>3M</td>
</tr>
<tr>
<td>tsunami</td>
<td>AN</td>
<td>001</td>
<td>12918</td>
<td>T4</td>
<td>192.168.6.48</td>
<td>140k</td>
</tr>
<tr>
<td>&lt;no ssid&gt;</td>
<td>AY</td>
<td>003</td>
<td>163</td>
<td></td>
<td>0.0.0.0</td>
<td>1k</td>
</tr>
<tr>
<td>linksys</td>
<td>AN</td>
<td>006</td>
<td>1330</td>
<td>T4</td>
<td>192.168.1.102</td>
<td>16k</td>
</tr>
<tr>
<td>colonie</td>
<td>AY</td>
<td>006</td>
<td>55</td>
<td></td>
<td>0.0.0.0</td>
<td>0B</td>
</tr>
<tr>
<td>linksys</td>
<td>AY</td>
<td>006</td>
<td>1</td>
<td></td>
<td>0.0.0.0</td>
<td>0B</td>
</tr>
<tr>
<td>101</td>
<td>AN</td>
<td>011</td>
<td>1</td>
<td></td>
<td>0.0.0.0</td>
<td>0B</td>
</tr>
<tr>
<td>! NYWLAN</td>
<td>AN</td>
<td>003</td>
<td>25</td>
<td>T4</td>
<td>192.168.16.101</td>
<td>197B</td>
</tr>
<tr>
<td>&lt;Data networks&gt;</td>
<td>GN</td>
<td>---</td>
<td>1192</td>
<td></td>
<td>0.0.0.0</td>
<td>146k</td>
</tr>
<tr>
<td>&lt;no ssid&gt;</td>
<td>AY</td>
<td>003</td>
<td>39</td>
<td></td>
<td>0.0.0.0</td>
<td>156B</td>
</tr>
<tr>
<td>301a81</td>
<td>AY</td>
<td>006</td>
<td>57</td>
<td></td>
<td>0.0.0.0</td>
<td>78B</td>
</tr>
</tbody>
</table>

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
- Abstrated 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
- 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

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 
  \{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:
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 Terminal Output](image)
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
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

<table>
<thead>
<tr>
<th>Name</th>
<th>T.C</th>
<th>Ch</th>
<th>Pkts</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>something_clever</td>
<td>A</td>
<td>0</td>
<td>56</td>
<td>1K</td>
</tr>
<tr>
<td>Nicole</td>
<td>A</td>
<td>N</td>
<td>11</td>
<td>39</td>
</tr>
<tr>
<td>linksys</td>
<td>A</td>
<td>N</td>
<td>6</td>
<td>19</td>
</tr>
<tr>
<td>Autogroup Probe</td>
<td>P</td>
<td>N</td>
<td>---</td>
<td>14</td>
</tr>
<tr>
<td>NETGEAR</td>
<td>A</td>
<td>N</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>Salty Swan</td>
<td>A</td>
<td>O</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>

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

Elapsed: 00:01.33
Networks: 8
Packets: 165
Pkts/Sec: 10

Packets: 0
Filtered: 0

Data

wlan0
Hop
UI Configuration
Navigating Networks

<table>
<thead>
<tr>
<th>Name</th>
<th>T</th>
<th>C</th>
<th>Ch</th>
<th>Pkts</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>! NETGEAR</td>
<td>A</td>
<td>N</td>
<td>11</td>
<td>22</td>
<td>0B</td>
</tr>
<tr>
<td>! Nicole</td>
<td>A</td>
<td>W</td>
<td>11</td>
<td>42</td>
<td>0B</td>
</tr>
<tr>
<td>. Salty Swan</td>
<td>A</td>
<td>O</td>
<td>06</td>
<td>28</td>
<td>0B</td>
</tr>
<tr>
<td>. boydhome</td>
<td>A</td>
<td>O</td>
<td>06</td>
<td>42</td>
<td>724B</td>
</tr>
<tr>
<td>freedom</td>
<td>A</td>
<td>O</td>
<td>06</td>
<td>10</td>
<td>0B</td>
</tr>
<tr>
<td>! linksys</td>
<td>A</td>
<td>N</td>
<td>06</td>
<td>64</td>
<td>0B</td>
</tr>
<tr>
<td>+! Autogroup Probe</td>
<td>P</td>
<td>N</td>
<td>---</td>
<td>4</td>
<td>0B</td>
</tr>
<tr>
<td>! somethingclever</td>
<td>A</td>
<td>O</td>
<td>01</td>
<td>136</td>
<td>2K</td>
</tr>
<tr>
<td>BSSID: 00:14:BF:0F:03:32 Last seen: Jul 6 06:28:43 Crypt: TKIP WPA PSK Manuf: Cisco-Li</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;Hidden SSID&gt;</td>
<td>A</td>
<td>?</td>
<td>06</td>
<td>3</td>
<td>0B</td>
</tr>
</tbody>
</table>

Kismet Sort View Windows

Kismet 200
Elapsed 00:01:30
Networks 13
Packets 577
Pkt/Sec 8
Filtered 0
wlan0 Hop

Data

Wireless Assessment on a Budget © 2009, InGuardians
Network Detail

Name: somethingclever
BSSID: 00:14:BF:0F:03:32
Manuf: Cisco-Link
First Seen: Jul 6 16:44:41
Last Seen: Jul 6 16:55:26
Type: Access Point (Managed/Infrastructure)
Channel: 1
### Client Detail

<table>
<thead>
<tr>
<th>MAC</th>
<th>Pkts</th>
<th>Data Type</th>
<th>DHCP Host</th>
<th>DHCP OS</th>
<th>Best-Guess IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:2D:61:82:0F</td>
<td>7</td>
<td>Wired/AP</td>
<td>---</td>
<td>---</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>00:02:2D:64:0F:E2</td>
<td>1</td>
<td>Wired/AP</td>
<td>---</td>
<td>---</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>00:02:2D:7B:AD:34</td>
<td>11</td>
<td>Wired/AP</td>
<td>---</td>
<td>---</td>
<td>69.69.69.46</td>
</tr>
<tr>
<td>00:02:2D:86:65:AF</td>
<td>7</td>
<td>Wired/AP</td>
<td>---</td>
<td>---</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>00:02:2D:90:0B:D2</td>
<td>1</td>
<td>Wired/AP</td>
<td>---</td>
<td>---</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>00:02:6F:03:FE:63</td>
<td>7</td>
<td>Wired/AP</td>
<td>---</td>
<td>---</td>
<td>172.23.5.109</td>
</tr>
<tr>
<td>00:02:8A:3A:EE:1F</td>
<td>1</td>
<td>Wired/AP</td>
<td>---</td>
<td>---</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>00:03:93:EA:EA:A8</td>
<td>6</td>
<td>Wired/AP</td>
<td>---</td>
<td>---</td>
<td>69.69.69.249</td>
</tr>
<tr>
<td>00:04:5A:CD:C2:E9</td>
<td>6</td>
<td>Wired/AP</td>
<td>belle</td>
<td>MSFT 5.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>00:04:E2:07:F9:69</td>
<td>8</td>
<td>Wireless</td>
<td>---</td>
<td>Linux 2.4</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

Last seen: Jul 6 08:27:26 IP: 0.0.0.0

- 00:05:3C:08:86:E2 5 Wireless, dev-MSELLE, MSFT 5.0, 0.0.0.0
- 00:06:25:01:46:6B 8 Wired/AP
- 00:06:25:01:CB:CC 1 Wired/AP
- 00:06:25:15:4E:7A 1 Wired/AP
- 00:06:25:2A:20:7E 4 Wired/AP
- 00:06:25:42:2C:D6 1 Wired/AP
- 00:06:25:9A:7F:20 59 Wired/AP
- 00:06:25:AE:D2:12 1 Wired/AP

---

[Wireless Assessment on a Budget © 2009, InGuardians](#)
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

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

<table>
<thead>
<tr>
<th>MAC</th>
<th>Type</th>
<th>Freq</th>
<th>Pkts</th>
<th>Size</th>
<th>Manuf</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:23:69:96:2A:6D</td>
<td>Wired/AP</td>
<td>2457</td>
<td>988</td>
<td>486</td>
<td>Unknown</td>
</tr>
<tr>
<td>00:22:69:01:35:71</td>
<td>Wireless</td>
<td>2462</td>
<td>244</td>
<td>26E</td>
<td>HonHaiPrec</td>
</tr>
<tr>
<td>00:0D:56:32:25:8B</td>
<td>Wired/AP</td>
<td>2457</td>
<td>74</td>
<td>72E</td>
<td>DellPcbaTe</td>
</tr>
<tr>
<td>00:24:1E:BF:50:53</td>
<td>Wired/AP</td>
<td>2437</td>
<td>6</td>
<td>956E</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

# 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

\[ \frac{U267}{(1000000 \times (60 \times 60 \times 24))} \]

\( (60 \times 60 \times 24) = 1 \text{ day in sec} \)

\( 1000000 = \text{usec in 1 second} \)
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

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

```bash
# 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
```
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?
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
The Excel sheet contains two charts. The first chart, titled "AP's By Manufacturer," shows a bar chart with the following data:

- **Enterasys**: 59
- **Aruba Networks**: 2
- **Cisco Enterprise**: 59
- **Linksys**: 93
- **Belkin**: 31
- **Netgear**: 9
- **Cloaked**: 207
- **Non-Cloaked**: 82

The second chart, also titled "AP's By Manufacturer," is a pie chart showing the distribution of cloaked and non-cloaked APs.

The formula in cell B8 is `=COUNTIF(Kismet!N8:N296,"TRUE")`.
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

One interface channel hops, the other sticks to a channel of interest.
Passive WEP Cracking Plugin
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 tstamp 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

josh@inguardians.com

www.willhackforsushi.com

SANS Ethical Hacking Wireless Course
www.sans.org/training/description.php?mid=3

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

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.