Hacker tool talk: Kismet

CIPS Edmonton Dinner Meeting – October 2011
“Security through knowledge”

Chris Hammond-Thrasher
chris.hammond-thrasher <at> ca.fujitsu.com
Fujitsu Edmonton Security Lab
October 2011
• Network: Fool-open
• http://kismet.nfshost.com/
Agenda

• Why are we here?
• Setting up a wireless security lab
• About Kismet
• Installing Kismet
• Kismet demo
• What’s next?
Why are we here?
Ethics and motives

“Every single scam in human history has worked for one key reason; the victim did not recognize it as a scam.”

- R. Paul Wilson
Setting up a wireless security lab
Wireless security lab reqs

• It’s actually pretty easy to setup
  – Wireless access point (AP)
    • Recommendation: Almost any will do
  – Attack/dev box
    • Wireless card and driver that supports packet injection
    • On Windows there is only one choice: AirPCAP from CACE (starting at US $200)
    • PCAP compliant network packet analyzer
    • Aircrack-ng wireless cracking and audit suite
    • Recommendation: OS: Backtrack Linux, Packet tool: Wireshark, H/W: ALFA AWUS36H for 802.11b/g (~$40)
  – Target box
    • Wireless card and driver compatible with your AP
  – Logging/monitoring box (Optional)
    • Wireless card and driver that supports monitor mode
Choices

• If you have a shortage of hardware, you can employ virtualization to cut down on the number of boxes in your lab. However, VMs can only use USB wireless cards.

• Booting from a Backtrack DVD or other bootable device is often the best option for the attack/dev box; it has Kismet and drivers for many wireless chipsets.
Caution

• Unless your lab is in a rural area or in a Faraday cage, there will be innocent networks within range of your equipment
• You are welcome to attack your own equipment, but attacking others’ networks without permission is potentially illegal
About Kismet
History

• Kismet is one of the longest running and most successful open source wireless tool projects – dates back to the early 2000s
• The Kismet project is lead by Dragorn (aka Mike Kershaw)
• It was originally created to fill a void for an affordable full featured wireless scanner
• Kismet-newcore is the recently released total rewrite of Kismet
• Kismet-newcore is included in the latest Backtrack 4 release
Features

• Kismet is a passive 802.11a/b/g/n network sniffer (assuming you have the right drivers and hardware)
• Broad support for wireless chip sets and reliable driver auto-detection
• ncurses interface
• GPS integration (+ Google Earth KML mapping tool)
• Packet capture
• Wireless protocol dissection and analysis
• Some wireless IDS features
• Can be deployed in a distributed architecture with remote sensors (drones) linked to a central console
• Extensible plug-in framework (WEP crack and DECT sniffing via plug-ins)
• Free (as in beer and speech)
Kismet vs. others

• Kismet passively monitors wireless networks – it never transmits
  – Cannot be detected
  – Can see non-beaconing networks if they are in use
  – Recovers cloaked SSIDs by listening to connection handshakes

• Stumblers broadcast probes and listen for responses
  – Can be detected
  – Find many networks faster
  – Cannot find non-beaconing networks
  – Cannot recover cloaked SSIDs
  – Cannot packet capture
Legit uses of Kismet

• 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?"

Props to Josh Wright for this slide
**h4X0r$**

- **Undetectable eavesdropping**
  - “Do you have unencrypted data on the airwaves?”
- **Undetectable WEP cracking (with plug-in)**
  - “Do you ‘protect’ your data with the worst encryption protocol ever published by the IEEE?”
- **Undetectable reconnaissance in advance of another attack**
  - “Do you reveal any vulnerabilities that I can exploit?”

* Bill Arbaugh of the University of Maryland Computing Science department uses WEP as an example of how not to design a cryptographic protocol.
Installing Kismet
Choices

• **Easiest: Get latest Backtrack (BT5R1 right now)**
  http://www.backtrack-linux.org/downloads/

• **Linux power user: Use your distro’s package manager to install the latest binary**
  ```
  sudo apt-get install kismet
  ```

• **Windows power user (with AirPCAP adaptor): Get the latest win32 installer from the Kismet site**
  http://www.cacetech.com/downloads.html

• **Developer: Get latest snapshot from svn and compile with gcc**
  ```
  svn co https://www.kismetwireless.net/code/svn/trunk kismet
  cd kismet
  ./configure --prefix=/opt && make && make install
  ```
Kismet demo
Kismet demo

• Starting it up
• Tour through Kismet screens
• Eavesdropping on open networks
• [Cracking WEP keys]
What’s next
Learn more

• Read Josh Wright’s much better (but slightly dated) intro to Kismet

• Read Josh Wright’s book
Act locally

• At home
  – Turn on WPA2 PSK using a strong password
  – Try using Kismet on your laptop to determine your home network range – note that the range at which you can listen to your network is different from the range at which you can connect to your network
  – Use Kismet to audit your community league, church, friend’s store, parents’ networks to make sure they are configured securely
Act locally

• At home
  – Watch your network for high volumes of retransmitted packets – this may indicate interference from nearby networks or other wireless devices (or your microwave)
  – Warwalk your neighborhood to determine the channel with the least interference for your home network
  – Use Kismet to help diagnose wireless network connectivity issues
Final Thoughts

• SSID broadcast: yes or no?
• SSID cloaking?
• MAC address filtering?
• Understanding Open vs WEP vs WPA2*

Cryptanalysis Procedure

Every deck has the same cards with the same letters. For the sake of fairness it is important to follow this procedure to the letter.

1. Unpack your special deck being careful to not alter the order of the cards
2. Hold the deck face down in whichever hand is the most comfortable
3. Deal exactly 24 cards off of the top of the deck face down onto the table forming a single pile
4. Riffle shuffle the two packs together *just once* (If you cannot riffle, ask for help)
5. Now deal down exactly 12 cards off the top of the deck onto the table forming a single pile
6. Do this three more times to form 4 piles
7. When your facilitator signals, look at your cards and try to use up all of your letters spelling one or more English words. Proper nouns and common acronyms are fair game. Cards labeled “space” can be used as a space between two words.
Thank you!

Want more presentations like this?  
Is there a particular tool or hack that you would like to see demoed?

Chris Hammond-Thrasher  
Fujitsu Edmonton Security Lab  
Email: chris.hammond-thrasher <at> ca.fujitsu.com  
Twitter: @thrashor