A BASTARD, A RAINBOW, AND A GREAT DANE

SHMOOCON 2006
Jan 13th, 2006- 1900 Hrs

Who are these people?

- Members in attendance:
  - Thorn
  - RenderMan
  - Joshua Wright – In the audience somewhere
  - Dutch – Via Video conference (we hope!)
- Many friends and fellow members helped
  - Streaker69
  - Goldfndr
  - Dragorn – (Buy this man a drink, He saved our ass!)

What is the CoWF

- Started originally by Blackwave
- Never really went anywhere
- Bought domain in 2005 for safe keeping
- Streaker69 made an offer of webspace
- A communal place to post our projects
- Pulling together all the various information scattered around the web
- Nothing serious, just having some fun
- Anyone can join. Must contribute though!

Projects

- Kiswin32 – Kismet for Windows
- 'JDUMAS' tool for WPA-PSK cracking; genpmk
- WDS fun
- The Evil Bastard
- Future work...

Kismet on Windows

- How-To available for manual build/install under Cygwin
- Kiswin32 available for stand alone install
- Both to be maintained and updated within a week of release
- New packages for the public
  - Windows Installer
  - Newcore on the way!

Kismet on Windows

- Auto-Drone script, download and install drone appliance binaries and files
- Windows based installer for Kiswin32
- Complete and simple Kismet on Windows install
- No excuse to not be monitoring your networks!
- Newcore building in features to make drones even more powerful – Dragorn takes requests!

WDS fun

- Wireless Distribution System
- Not in 802.11x spec, manufacturer added
- Chipset specific
- Repeat mode or Bridge mode
- Repeat mode: Repeats signal, still acts as access point
- Bridge Mode: No wireless clients allowed, Unit to Unit bridge
- WRT54G(S) supports WDS, but hides from user

WDS fun

- OpenWRT allows access to WDS functions
- Nvram set wl0_wds
- Can turn WRT54G into cheaper replacement for WET54G
- Half of bandwidth devoted to backhaul
- WDS does not act like a 'client', no logging!
- WDS does not require 2 way trust.... Anyone can repeat a signal.....
- Can repeat for 'like' chipsets

WDS fun

- If we can repeat any signal, as well as act like an access point.....
- Spoofed AP backhaul problem is solved
- Different manufacturers tend to use same chipset (broadcom)
- No record of client associations
- One way setup, no configuration on victim required
- All sorts of mayhem possible

The JDUMAS project

- Blame Chris (Roamer) for this one
- WPA-PSK cracking is time consuming
- Wardriving contest at DC13, spending 2 hours staring at laptops running coWPAtty
- We lost (Boo!, Death to PSKL!)
- Needed tools to do 2 things:
  - One to look for easy/dumb WPA-PSK passwords
  - One to pre-compute the hashes ahead of time

JDUMAS

- JDUMAS, as in user J. Dumb ass
- A Dumbass has his user name as his password
- Need to audit for this!
- CoWPAtty works, but takes time to run and is boring if presenting and not good for repeat audits
- There must be a faster way...

Quick WPA-PSK Primer

- PMK = PBKDF2(passphrase, ssid, ssidLength, 4096, 256)
- Key is seeded with SSID and SSID length, makes each network key unique
- Without knowing SSID, pre-computing the passphrase is useless
- We often know the network we'll be trying to crack, (or we can guess)
- Pre-compute keys ahead of time for near instant cracking on-site
- Pre-computed keys can also be saved for later!

The JDUMAS project

- Originally going to be a stand alone app
- Pre-compute hash tables and then compare capture to tables
- Joshua Wright steps into things:
  - Genpmk – prehashing of passphrases
  - CoWPAtty 3.0 supports checking of hash tables

CoWPAtty - Genpmk

- We can now pre-compute keys for later use
  - Off hours, night, multiple machines
- Can now pre-compute keys for **ANY** SSID
- Hmmmm?
- Pre-compute for default SSID's
- http://www.wigle.net/gps/gps/Stat/
  - Top 1000 SSID's (~50% of wigle.net networks)
- Perl script to compute a list of SSID's
- Close to Rainbow tables for WPA?

WPA-PSK – Precomputed tables

- Mix in the top 1000 SSID's
- Add Websters (~170,000 word) dictionary
- Remove words < 8 or >64 characters
- Many hours of CPU time
- = CoWF WPA lookup tables!
- Demo – Think happy thoughts

WPA-PSK – Precomputed tables

- We precomputed common SSID's with common words
- Saves a lot of time in cracking WPA-PSK
- If you spend the time computing a table, please share with us and others!
- Password list **must** be in unix format!
- Many thanks to Dragorn for some stepping in with some massive computing power and saving the day!

Evil Bastard

- Based off of 'Evil Twin' (rogue squadron) idea
  - (Evil twin is a dumb media created name, BTW)
- Twin - *n* - *One of two identical or similar people, animals, or things; a counterpart.*
- Bastard – *n* - *Something that is of irregular, inferior, or dubious origin.*
- *Slang: A person, especially one who is held to be mean or disagreeable.*
- Which is a better description?

Evil Bastard

- Rogue Squadron only snarfs hotspot passwords (captive portal). There's so much more that can be done
- Project goal: Take the spoofed AP concept as far (and evil) as it can go **quietly**
  - Self contained, non interactive (after initial setup)
  - Snarf as much as possible
  - Easy to use
  - Must not be easily detectable by users
  - Overall, be very quiet in it's operation

Evil Bastard

- WRT54GS (v1.0) Running OpenWRT
- Wi-Viz modified to provide 'Point 'n spoof' interface
- SD card mod allows for storage of snarfed data and WPA-PSK lookup tables
- Configurable for snarfing specific types of data
- Can use WDS to backhaul into victim network, allowing continued access to resources
- Autocrack if target encrypted (WEP, WPA-PSK)
- Not trying to be FaruziaWRT

Evil Bastard - Tools

- **Dsniff – Snarf un-encrypted passwords**
- **Dnsspoof – Hijack DNS and go phishing**
  - **Paypal, ebay, banks, whatever**
- **Webmitim – Spoof SSL/HTTPS sessions**
- **Driftnet – Snarf images from web traffic**
- **Msgsnarf/Mailsnarf – Snarf Mail and IM data**
- **Filesnarf – Snarf files over NFS**
- **Kismet_drone – For good measure**
- **Thttpd – Web server for config and for log viewing**
- We **ARE** the man in the middle

Evil Bastard – How To

- Get near target
- Select target for spoofing from interface
- Select snarf options
- Commit, unit reboots and spoofs target
- Clients should drift over and begin being snarfed (targeted void11 may be necessary)
- If network encrypted, will automatically attempt to crack network (WEP and WPA-PSK)
- If using WDS backhaul, clients won't notice missing network resources

Evil Bastard

- Snarfed data can be sent over email, NFS, ftp or viewed from internal web server
- Potential for instant 'Wall of Sheep' (WoS) device
  - Display usernames with masked passwords
  - Display driftnet images

Current and Future projects

- Dragorn, Joshua Wright? Anything to add?
- WPG11 – Wireless presentation gateway
  - Linux based + VGA out + Prism WIFI card=???
- Kismet Newcore tricks
- Wifi-Grenade???
- Bigger lookup tables?

Conclusion

- Join the CoWF, contribute, collaborate
- Wifi attacks are not old news
- Is Render still sober?
- Discussion continues outside at/near the bar

Sites

- www.churchofwifi.org
- www.renderlab.net
- www.blackthornsystems.com
- www.remote-exploit.org
- www.netstumbler.org
- www.evsmail.com - Donated processor time
- www.kismetwireless.net - Dragorn parallelized genpmk to save our butts