

Tyler Steiner

Linux Wireless.

Around the year 1997 a wireless networking standard called 802.11. This standard allowed for TCP/IP and other networking protocols to be used over various radio frequencies. This new standard allowed networks to travel and move where wired 802.3 standards did not allow. Many of us use wireless at home, work, school, or even at the local café. With the popularity of the Wifi standard came more programs, hardware, drivers, and streaming devices.

Linux was left in the dust when it came to wireless devices. Drivers were hard to come by, and getting them to work was almost as hard. As time went on driver sources were opened up and utilized, or reverse engineered to work in linux. Drivers became functional and in most cases better than windows drivers. Atheros, Prism, Intel, and Ralink drivers because far more mature. The drivers not only supported the popular encryption protocols, but have more features than the windows counterparts. These features are what make the Linux wifi scene far more popular to wifi enthusiasts than windows.

Promiscuous mode was such a feature that windows users were never able to openly use without very expensive drivers via Wild Packets Airopcap. Linux users are able to utilize this feature out of the box with most drivers. Promiscuous mode allows for the “listening” of packets as they come across the airwaves. Windows and Linux users have been doing this for a long time, but on the 802.3 standards (Ethernet) the program ethereal or wire shark do the same thing. This capturing of arbitrary packets has led to much advancement in the 802.11 standard, most notably encryption.

With Linux drivers being able to arbitrarily capture packets, the Wired Equivalent Privacy (WEP) became a target for hacker, engineers, and others. With people breaking the different security protocols, newer, stronger ones were designed. WPA, WPA2, TKIP, and RADIUS.

WEP

WEP uses a 40 or 104 bit key to encrypt, and uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. With the header being visible to devices in promiscuous mode, the WEP encryption was easily broken. WEP uses the same initialization vector (IV) over and over again, which proves to be its weakness.

Programs

There are quite a few programs that are Linux specific to wireless and its uses. Due to the nature of its open source drivers, the programs that utilize them can do things that most windows PC's can not. The most popular one is called Kismet.

Kismet is a wireless packet capturing program. This program captures packets as they fly by, analyzes the headers and displays the packet information (SSID, SIZE, IP RANGE, MAC, and CLIENTS MAC's). This operates differently from Netstumbler in windows as it does not send out probe requests, which means it is virtually undetectable.

```

root@wirelessdefence:~
File Edit View Terminal Tabs Help
Network List (Autofit)
Name          T W Ch  Packts  Flags  IP Range
default       A N 006    9  F    192.168.0.1
! iyonder.net A N 005   42  U4   10.254.178.254
! iyonder.net A N 001   22  A3   10.254.178.0
! eurospot    A N 001   19  U4   204.26.5.166
! NETGEAR     A 0 006    5    0.0.0.0
. eurospot    A N 011   14    0.0.0.0
! belkin54g   A Y 011   17    0.0.0.0
! iyonder.net A N 011   16  A3   10.254.178.0
! tsunami     A Y 007   17    0.0.0.0
! <no ssid>   A 0 003   11    0.0.0.0
Probe Networks P N ---    3    0.0.0.0
! iyonder.net A N 008   35    0.0.0.0
. <no ssid>   A Y 011    5    0.0.0.0
NCDT_NET      A Y 006    1    0.0.0.0
<no ssid>     A Y 011    1    0.0.0.0

Info
Ntwrks      16
Pckets      228
Cryptd       4
Weak         0
Noise        0
Discrd       0
Pkts/s       8
Elapsd      00:00:20

Status
Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\0
36\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0
bssid 00:0A:8A:A2:C8:7F
Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP
Battery: AC 107%

```

The **Air crack-NG** suite is another set of programs that aids in the cracking of WEP keys. Although this program is available in windows, the windows version does not include airtraf, aireplay, or airedecap. These are most vital to the success of the program.

```

aircrack 2.3

[00:00:04] Tested 23757 keys (got 139994 IVs)

KB    depth  byte(vote)
0     0/ 1     CB( 42) 0D( 15) 33( 15) B2( 15) 78( 13) 10( 12)
1     0/ 1     A3( 87) 01( 16) 1F( 15) F4( 15) 4F( 13) F8( 13)
2     0/ 1     C3( 88) 7C( 29) E4( 20) 4F( 18) 36( 12) 59( 12)
3     0/ 1     BA( 132) 74( 25) C7( 24) B1( 20) 8D( 18) A1( 17)
4     0/ 1     C3( 98) C5( 28) 53( 15) 88( 15) ED( 15) 93( 13)
5     0/ 1     4B( 93) C8( 23) 3D( 20) 22( 18) 71( 16) 4A( 14)
6     0/ 1     4C( 58) 34( 27) 91( 23) A6( 23) 79( 20) CE( 18)
7     0/ 1     4A( 64) 51( 28) 79( 24) 3E( 23) 4D( 20) 91( 20)
8     0/ 1     BA( 164) 2E( 29) 20( 17) 26( 17) 24( 16) 93( 15)
9     0/ 5     B4( 28) 5A( 18) 1D( 16) 45( 15) 60( 14) FE( 13)
10    0/ 1     B5( 331) 67( 18) 00( 15) 47( 15) 48( 15) 9D( 15)

KEY FOUND! [ CB:A3:C3:BA:C3:4B:4C:4A:BA:B4:B5:5C:CB ]

```

Airpwn is a framework for 802.11 (wireless) packet injections. Airpwn listens to incoming wireless packets, and if the data matches a pattern specified in the config files, custom content is injected "spoofed" from the wireless access point. From the perspective of the wireless client, airpwn becomes the server. (Be careful if searching on this topic, as the creator did not choose a good picture to demonstrate with.)

Linux Drivers

Installing drivers under Linux can be easy or hard, depending on the driver you are wishing to install, and the flavor of Linux you are installing it on. Most modern distributions come with some sort of package manager that will fetch or compile a set of drivers for your system. Most systems however come with the driver built into the kernel, or installed by default. All others can be compiled from source.

Links

<http://www.kismetwireless.net/>

<http://en.wikipedia.org/wiki/802.11>

<http://www.aircrack-ng.org>

<http://madwifi.org/>

<http://hostap.epitest.fi/>

<http://prism54.org/>

<http://bcm43xx.berlios.de/>

<http://sourceforge.net/projects/airpwn>