Wireless Tools

Training materials for wireless trainers
Goals

- to understand which are the software tools that may help you in:
  - monitor your WiFi network to identify problems
  - do a security auditing and prevent attacks
  - detect interferences
Types of wireless tools

- Network ESSID scanners
- Wireless protocol analyzers
- Encryption cracking tools
- Wireless device auditing and management
- “War driving” tools: network mapping
- Spectrum analysis
Built-in wireless clients
NetStumbler
http://www.stumbler.net
Kismet
http://www.kismetwireless.net/
KisMAC

http://www.kismac-ng.org/
Handheld wireless clients
extremely powerful wireless protocol analyzer
### aircrack 2.3

[00:00:02] Tested 2 keys (got 270169 IVs)

<table>
<thead>
<tr>
<th>KB</th>
<th>depth</th>
<th>byte(vote)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0/1</td>
<td>63 (61) A2 (12) 08 (12) 39 (6) FB (5) 74 (5)</td>
</tr>
<tr>
<td>1</td>
<td>0/1</td>
<td>68 (95) B2 (15) 3B (13) 8A (5) 44 (5) 0A (5)</td>
</tr>
<tr>
<td>2</td>
<td>0/1</td>
<td>85 (43) F7 (8) 37 (8) 1D (7) 6A (5) 40 (3)</td>
</tr>
<tr>
<td>3</td>
<td>0/1</td>
<td>63 (98) B1 (15) 19 (12) CC (5) EA (5) 35 (5)</td>
</tr>
<tr>
<td>4</td>
<td>0/1</td>
<td>6B (58) 6C (12) FE (12) 4F (9) 02 (9) CB (3)</td>
</tr>
<tr>
<td>5</td>
<td>0/1</td>
<td>70 (76) F8 (12) DE (8) 8B (6) 17 (5) 58 (5)</td>
</tr>
<tr>
<td>6</td>
<td>0/1</td>
<td>61 (75) C3 (15) 6E (12) 9E (10) 63 (10) 77 (8)</td>
</tr>
<tr>
<td>7</td>
<td>0/2</td>
<td>73 (34) 15 (26) 3D (10) 72 (9) A7 (8) 9A (6)</td>
</tr>
<tr>
<td>8</td>
<td>0/1</td>
<td>73 (87) E1 (15) B5 (12) B3 (10) DE (10) E0 (10)</td>
</tr>
<tr>
<td>9</td>
<td>0/1</td>
<td>77 (99) 9B (13) 36 (13) 0A (12) 5D (11) F6 (10)</td>
</tr>
<tr>
<td>10</td>
<td>0/4</td>
<td>6F (22) 82 (13) F2 (13) 49 (13) DE (10) 1A (10)</td>
</tr>
<tr>
<td>11</td>
<td>0/1</td>
<td>72 (154) A9 (16) FB (15) 73 (12) 5A (11) 05 (10)</td>
</tr>
<tr>
<td>12</td>
<td>0/2</td>
<td>64 (30) BF (25) DC (10) 48 (10) 00 (10) 43 (10)</td>
</tr>
</tbody>
</table>


Press Ctrl-C to exit.
- Implementation of an offline dictionary attack against WPA-PSK and WPA2-PSK networks

- WPA2-PSK Rainbow Tables: 1 million common passwords x 1,000 common SSIDs. 40 GB of lookup tables available on DVDs.
Etherpeg

http://www.etherpeg.org/
Driftnet
http://www.ex-parrot.com/~chris/driftnet/
Network and port scanner

Rogue AP detection

Scans any number of ports on any number of hosts

Sophisticated stealth scanning

Idle, undetectable service “scanning”

Available for all platforms

http://nmap.org/
The Dude

The Dude network monitor is a network auditing and monitoring tool by MikroTik.

The Dude automatically scans devices within specified subnets, draws a map of the networks monitors services and sends alerts when there are problems.

Only available for Windows.
Wi-Spy spectrum analyzer

http://www.metageek.net/
Chanalyzer
EaKiu
Conclusion

- **Network ESSID scanners** will find neighboring WiFi networks and provide basic information about them.

- **Wireless protocol analyzers** log captured data for later analysis.

- **Encryption cracking tools** can be used to test the security of your own networks.

- **Wireless device auditing and management tools** automate the process of managing access points on your network.

- **“War driving” tools** allow you to plot the physical range of your network on a map.

- **Spectrum analysis tools** can show you sources of radio interference not necessarily caused by WiFi.
Thank you for your attention

For more details about the topics presented in this lecture, please see the book *Wireless Networking in the Developing World*, available as free download in many languages at:

http://wndw.net