Aircrack-ng

Airdecap-ng

Description

With airdecap-ng you can decrypt WEP/WPA/WPA2 capture files. As well, it can also be used to strip the wireless headers from an unencrypted wireless capture.

It outputs a new file ending with "-dec.cap" which is the decrypted/stripped version of the input file.

Usage

```
airdecap-ng [options] <pcap file>
```

Option	Param.	Description
-l		don't remove the 802.11 header
-b	bssid	access point MAC address filter
-k	pmk	WPA/WPA2 Pairwise Master Key in hex
-e	essid	target network ascii identifier
-p	pass	target network WPA/WPA2 passphrase
-w	key	target network WEP key in hexadecimal

Wildcards may be used on the input file name providing it only matches a single file. In general, it is recommended that you use a single file name as input, not wildcarding.

Usage Examples

The following removes the wireless headers from an open network (no WEP) capture:

```
airdecap-ng -b 00:09:5B:10:BC:5A open-network.cap
```

The following decrypts a WEP-encrypted capture using a hexadecimal WEP key:

```
airdecap-ng -w 11A3E229084349BC25D97E2939 wep.cap
```

The following decrypts a WPA/WPA2 encrypted capture using the passphrase:

```
airdecap-ng -e 'the ssid' -p passphrase  tkip.cap
```

Usage Tips

WPA/WPA2 Requirements

The capture file must contain a valid four-way handshake. For this purpose having (packets 2 and 3) or (packets 3 and 4) will work correctly. In fact, you don't truly need all four handshake packets.

As well, only data packets following the handshake will be decrypted. This is because information is required from the handshake in order to decrypt the data packets.

How to use spaces, double quote and single quote in AP names?

See this FAQ entry

Usage Troubleshooting

None at this time.

---

airdecap-ng.txt · Last modified: 2009/09/26 20:07 by darkaudax