Deauthentication Attack

It’s a type of Denial of Service attack that disrupts communication between a user a wireless access point. It exploits management frames that are normally used to maintain the link between the two devices.

When communication is completed a station (client) or an access point can send a Deauthentication to terminate the connection.

By spoofing either the AP or the client a hacker can constantly send these frames disconnecting the user and preventing them from reconnecting.

Testing

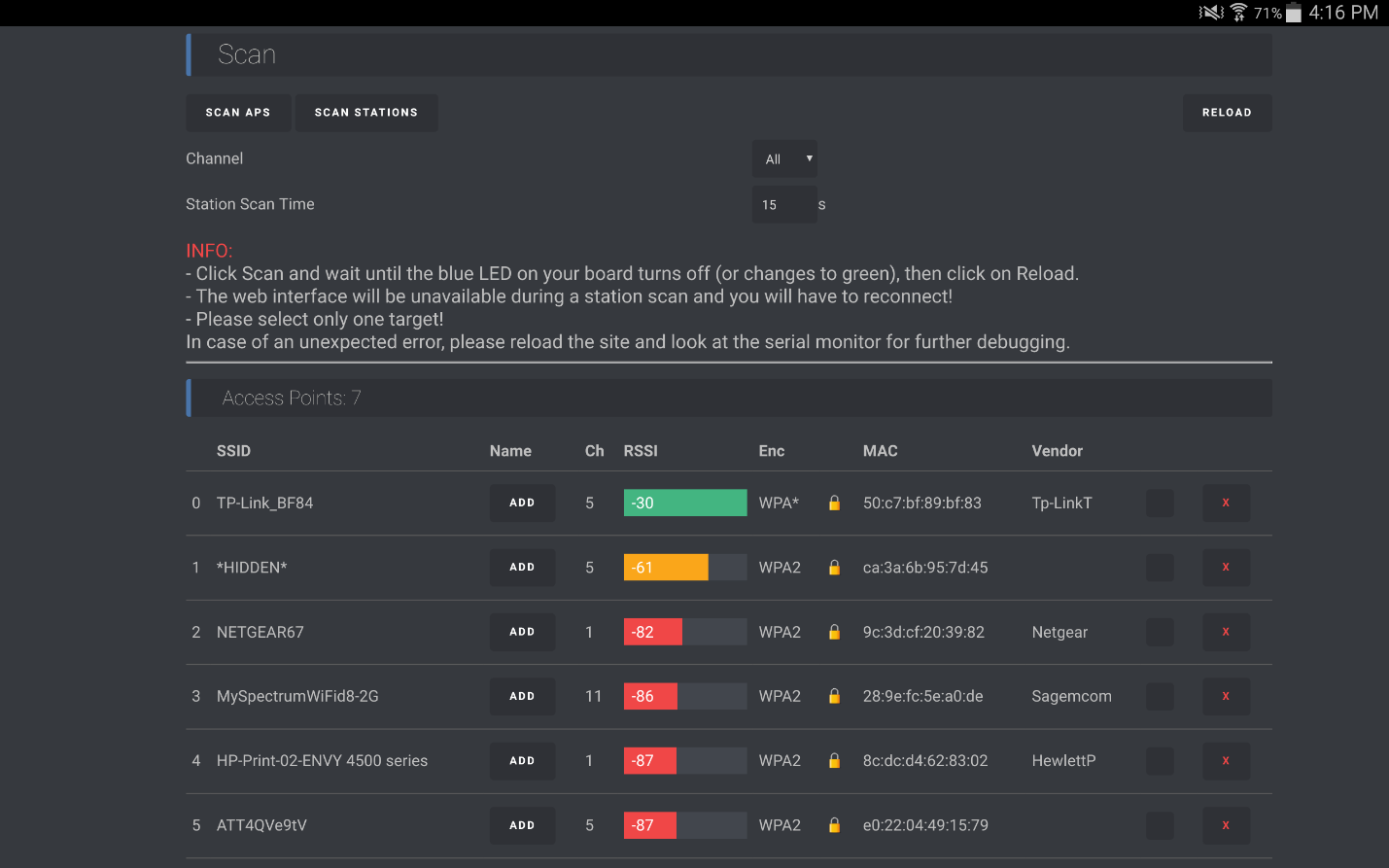
ESP8266- used to attack a wifi access point.

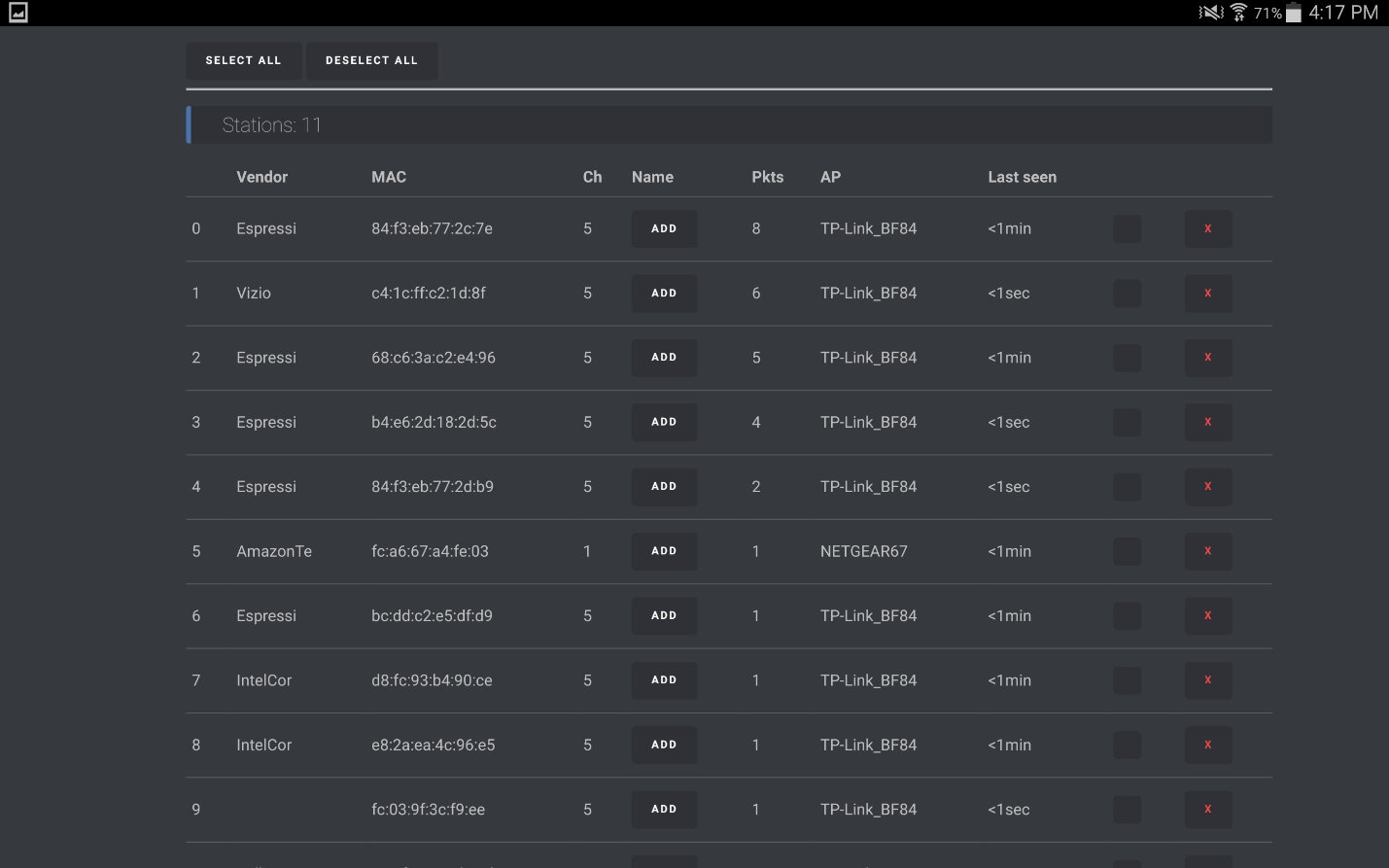
Alternative was Lunix running Aircrack-ng

ESP-running open source code written by Stefan Kremser

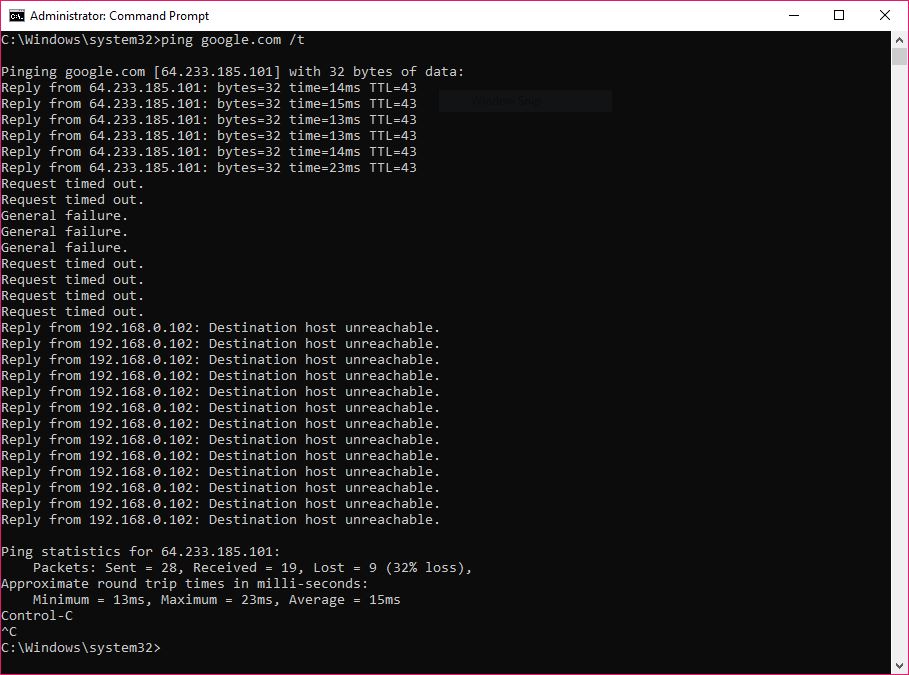
<https://github.com/spacehuhn/esp8266_deauther>

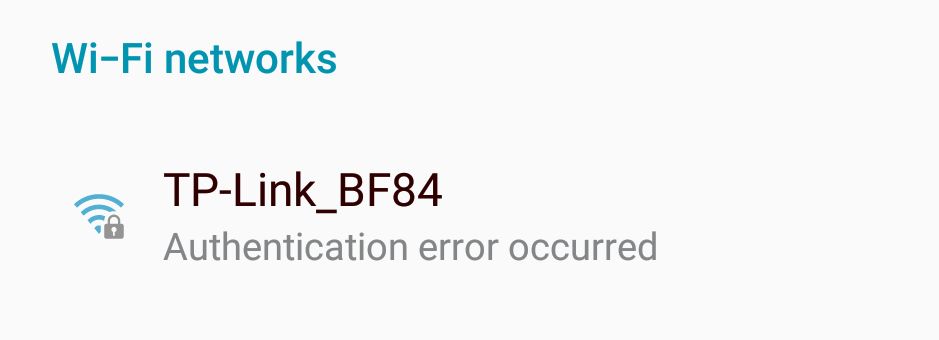
Main Menu





After attacking TP-Link\_BF84





Prevention of this attack

Protected Management Frames 802.11w

Which prevents eavesdropping, forging. Not implemented on all devices.