8. WPA and WPA2 Cracking

Both, WPA and WPA2 can be cracked using the same methods. They are made ti adress the issues in WEP and made much more secure. Each packet is encrypted using a unique tempoary key.

- Packets contain no useful information

WPA and WPA2 Cracking

- both can be cracked using the same methods
- they are made to close he security holes of WEP
- and are way more secure
- each packet is encrypted using a unique tempoary key

Packets contain no useful information

ARP Request Replay

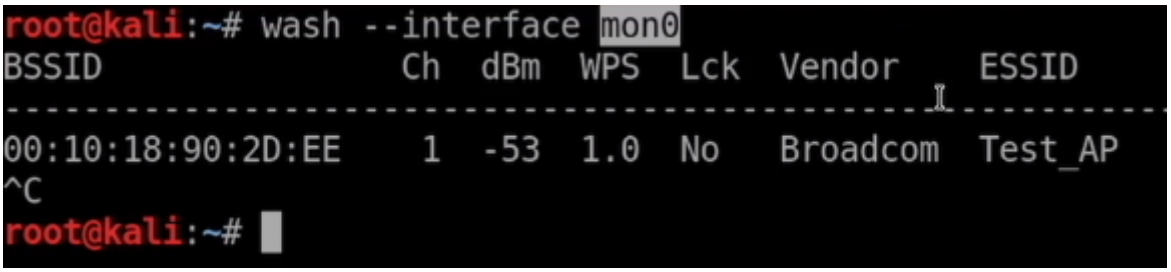
- WPS is a feature that can be used with WPA and WPA2.
- Allows clients to connect without the password
- Authentication is done using a 8 digit pin
  - 8 Digits are very small
  - We can try all possible pins in relatively short time
  - Then the WPS pin can be used to compute the actual password.

PS: This only works if the router is configured not to use PBC (Push Button Authentication)

Check if Nework has WPS active

```
wash --interface wlan0
```

The Output should look like this:



Here you can see WPS is labled as 1.0. This doesn't tell you if it uses Pushbutton Authentication, you just have to try.

lets associate with the network

Revision #5
Created 10 February 2023 20:38:32 by tinfoil-hat
Updated 9 March 2023 18:16:12 by tinfoil-hat