BETTERCAP is more advanced version of ettercap.

1. Open terminal.
2. If config to see all the network interfaces.
3. Makes sure that we have a wireless adapter connected to the kali Linux box so that we can sniff packets in the environment.
4. Command “bettercap -iface Wlan0 “

Wlan0 is the interface that we are scanning.

This would lead us to an interactive mode.

1. Now you're in interactive mode. Enter “help” this will show all the processes that we are running inside better cap.
2. We need to check if the WiFi module is running. If not we need turn on the WiFi module using “WiFi.recon on”.This will turn on the WiFi module for better cap.
3. This will make the adapter in promiscuous mode and start to sniff all the data on the network.
4. If we want to see all the access points on the network we need to run “ wifi.show”.
5. This wil show all the various SSID’S on the network and the longer we have the connection established for the more clients associated with the SSID we will capture.
6. We will pick up the SSID IN question and look for it's channel number. For example let's assume it's 3.
7. Set WiFi.recon.channel 3

This will.set the reconnaissance to only channel 3.

Will require to reset reconnaissance.

1. Set net.sniff.verbose true
2. Set net.sniff.filter ether proto 0x888e
3. Set net.sniff.output wpa.pcap

This will save the output in the wpa.pcap file

1. Net.sniff on
2. WiFi.show
3. This will show all the the devices connected to that specific SSID.
4. Now we can grab the BSSID FOR THE SSID in question.which can be taken from step 7.
5. Run command “ WiFi.deauth BSSID number”
6. This will deauth all the clients that are associated with the network.
7. Once this is actioned you should be able to see “WiFi.client.probe” which is all the deauthenticated devices attempting to re authenticate. This will allow us to capture the TCP handshake.
8. Now we can exit bettercap interactive mode.
9. When we look in the file explorer we should be able to see the cap file.
10. Open with Wireshark.
11. One way is to go to Wireshark , open the cap file , go to tools and then credentials. It will list all the username or passwords that Wireshark has captured from the loaded file.
12. Other way to get it done is load the pcap file , click on edit and then find packet.
13. Change the packet in the heading for column to packet details and it is set to strings.
14. In the search field add username.
15. This will allow us to pick the username and password.