

LAB 1 - WPA CRACKING LAB

Module Leader: Dr Carlene Campbell.

PART1: Set up Wireless access point with WPA PSK encryption.

PART2: Capture WPA PSK four way handshake.

PART3: Crack the WPA PSK key with aircrack-ng.

Lab Exercises Equipment:

1. One wireless Router connected to the Internet.
2. One **Client** (victim machine) with WiFi card running Windows or Linux.
3. One **Attacking** machine (Hacker) with WiFi card running Kali Linux.

PART1: SET UP WIFE ACCESS POINT WITH WPA-PSK ENCRYPTION.

In this lab exercise we set up the wireless access point with WPA PSK authentication. In the second part of the lab we try to capture the four way handshake which takes place between the wireless client and access point. In the third part of the lab we crack the WPA PSK key with aircrack-ng.

1. Set up the wireless access point (router) with WPA PSK encryption. Open the web browser and type the IP address of the wireless access point in the address bar. When prompted for username and password enter your credentials. Let us assume username is: admin, and password is: password. Once you login to the router, go to wireless settings and change the security mode to WPA PSK.

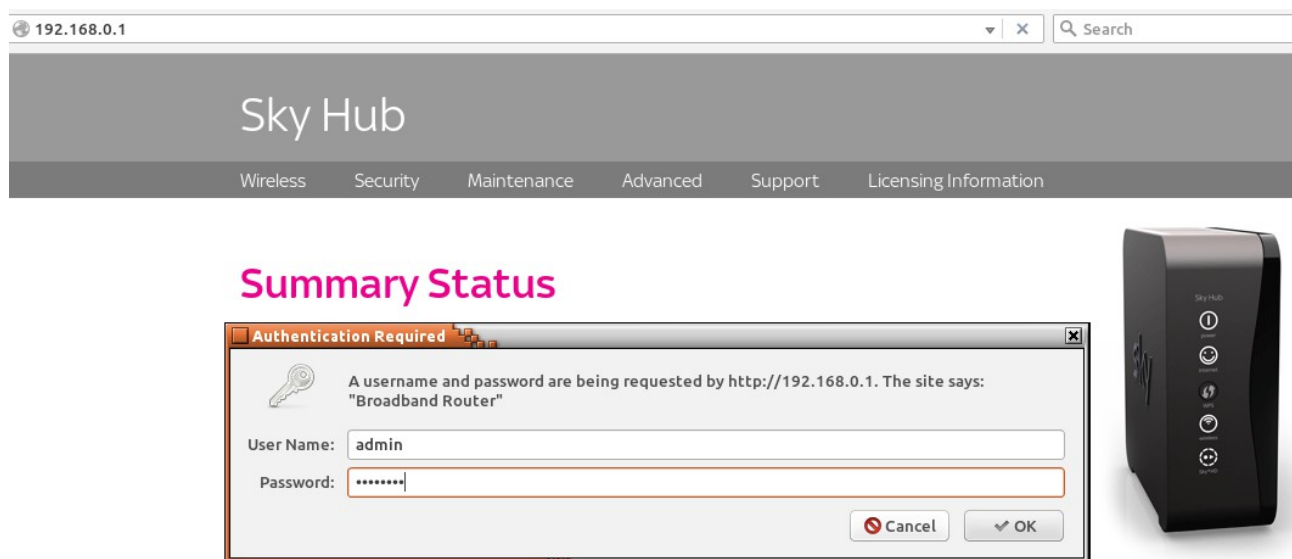


Fig 1: Shows access to the Broadband Router Settings.

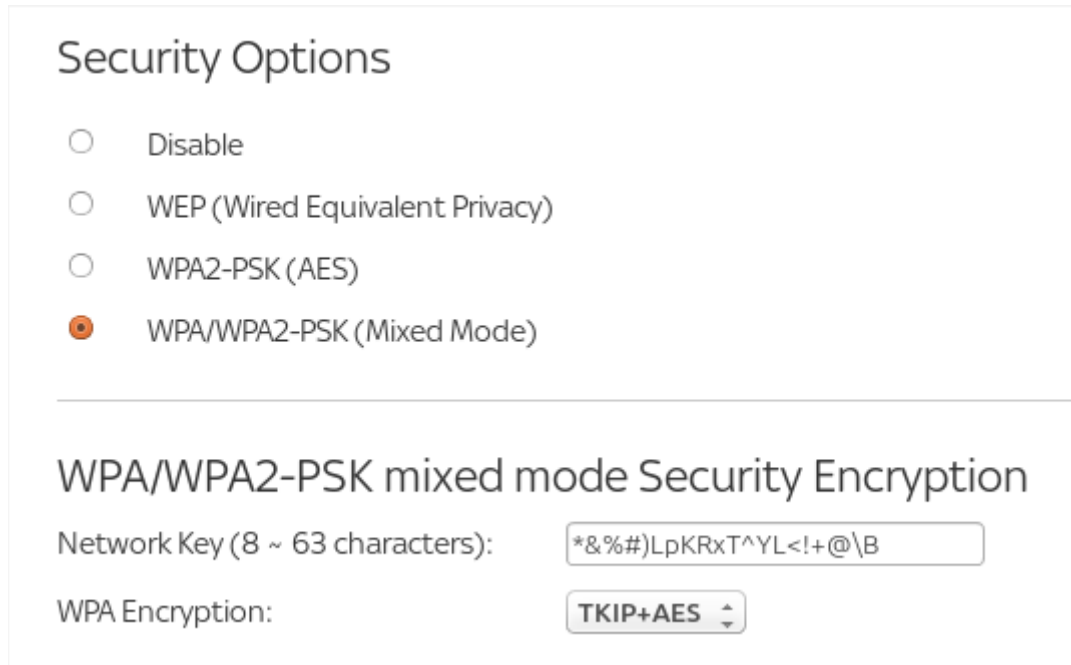
2. It depends on the type of wireless router you are using. The following screenshots are for Sky Hub router. The wireless security option will be available on all new modern wireless routers. Change the wireless security to WPA PSK and enter the password of your choice. The password should be minimum 8 characters in length. If you have any trouble finding the correct settings for your model of router, refer the manual which came along with the router. Once you apply the settings reboot the router.

Security Options

Security Mode: **WPA-PSK.**

Encryption Key: ***&%#)LpKRT^YL<!+@B**

Save the settings and reboot the router.



Security Options

- ☐ Disable
- ☐ WEP (Wired Equivalent Privacy)
- ☐ WPA2-PSK (AES)
- ☒ WPA/WPA2-PSK (Mixed Mode)

WPA/WPA2-PSK mixed mode Security Encryption

Network Key (8 ~ 63 characters):

WPA Encryption:

Fig 2: Shows Changing the encryption system from WPA2-PSK to WPA-PSK.

Once rebooting, it can take up to 2 minutes for the router to come up, depending on the make and model. Once the access point is up, our attack plan is to sniff the channel on which the router is functioning. This is achieved by connecting the **Client** machine to the Router, while the attack machine is already sniffing on the data channel data. The **Attacking** machine will capture the fourway handshake which took place between the Client and access point. In the third part of the lab exercise the captured file is used to crack the key with aircrack-ng.

Fig 3

PART2: CAPTURING WPA-PSK FOUR-WAY HANDSHAKE.

3. On the attack machine, run the command terminal. Bring the card up and create a monitor mode interface on the wireless card using the following command.

```
#ifconfig wlan0 up  
#airmon-ng start wlan0
```

Fig 4

4. Once you created the monitor mode interface, scan the air for available wireless networks. To do this you need to run airodump-ng.

```
#airodump-ng
```

Fig 5

This command will scan all the 14 channels in 2.4 Ghz frequency and shows the list of wireless access points in the range. In the output below we can see our access point named “**Your Access Point SSID**” with WPA PSK authentication enabled. The access point may be functioning on channel 9.

Fig 6

5. From the airodump output in Fig 6 above, it is clear that the access point is on channel 9, we should sniff on channel 9 for capturing the handshake. To capture traffic on channel 9 use the following command.

```
#airodump-ng -w labfiles/wpacrack/wpa-Seclab -c 9 mon0
```

Options:

-c	Specifies the Channel to sniff
-w	Specifies the file to save the captured data

Fig 7

6. Go to the **Client** machine and connect to “**Your Access Point SSID**” network. You will be asked for the WPA PSK password. Enter the same password you set in the access point.

Fig 8

7. Go to attacker machine, in the airodump-ng output see top right corner which indicates successful capture of handshake.

Fig 9

PART3: CRACKING THE WPA-PSK KEY WITH aircrack-ng.

8. Use aircrack-ng to crack the key.

```
#aircrack-ng [name of the file containing capture 4-way handshake]
```

Fig 10

The figure below shows that aircrack-ng is successful in cracking the WPA PSK key. The key is shown in plain text. You can speed up the process of cracking using Rainbow Tables.

Fig 11

CONCLUSION

In the first part of this lab we set up the wireless router with WPA PSK encryption system activated. In the second part of the lab we captured the four way handshake when wireless Client machine connected to the network. In the third part of the lab we cracked the WPA PSK key with aircrack-ng