**Ex. No.: 14.b. WIRELESS AUDIT**

**Date:**

**Aim:**

To perform wireless audit on Access Point and decrypt WPA keys using aircrack-ng tool in Kalilinux OS.

**Algorithm:**

1. Check the current wireless interface with the iwconfig command.

2. Get the channel number, MAC address and ESSID with the iwlist command.

3. Start the wireless interface in monitor mode on a specific AP channel with airmon-ng.

4. If processes are interfering with airmon-ng then kill those processes.

5. Again start the wireless interface in monitor mode on a specific AP channel with airmon-ng.

6. Start airodump-ng to capture Initialization Vectors(IVs).

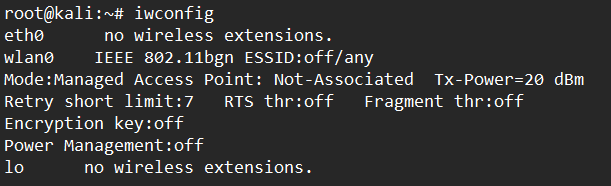
7. Capture IVs for at least 5 to 10 minutes and then press Ctrl + C to stop the operation.

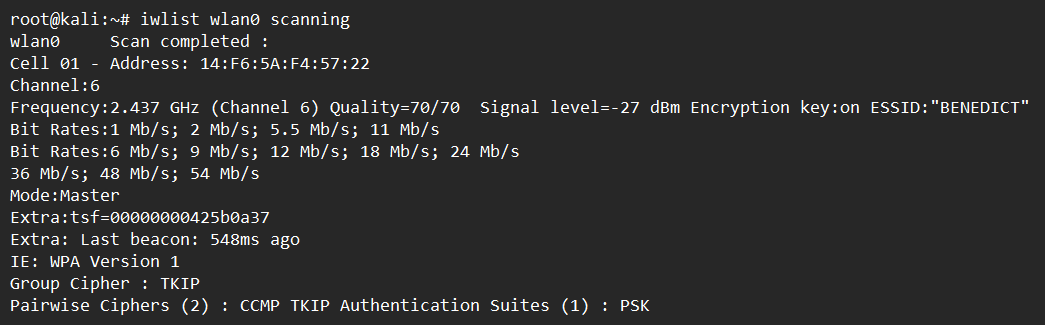
8. List the files to see the captured files

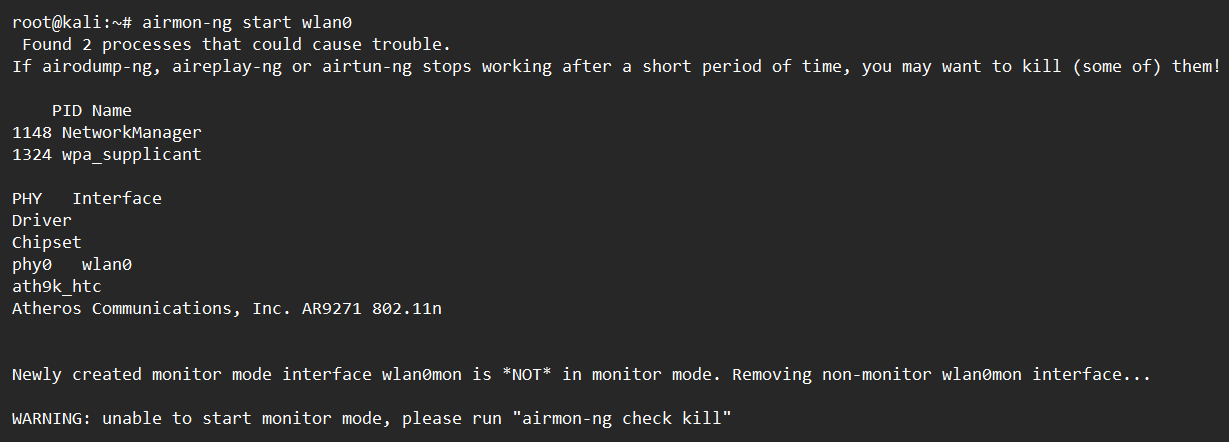
9. Run aircrack-ng to crack key using the IVs collected and using the dictionary file rockyou.txt

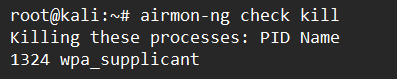
10. If the passphrase is found in the dictionary then Key Found message displayed; else print Key Not Found.

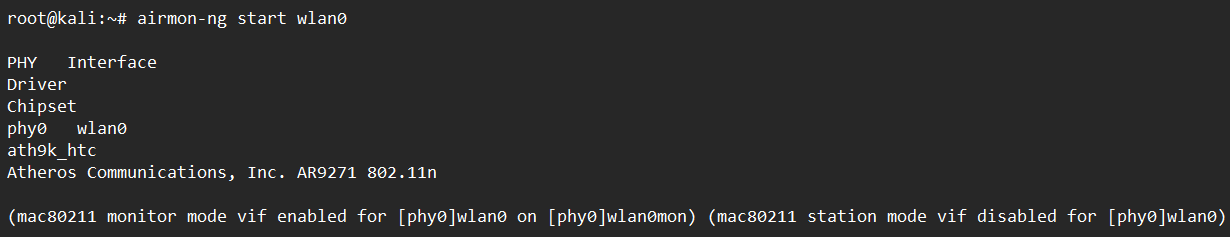
**Output:**

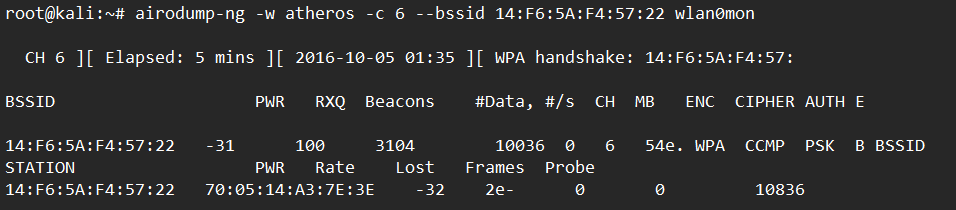
****

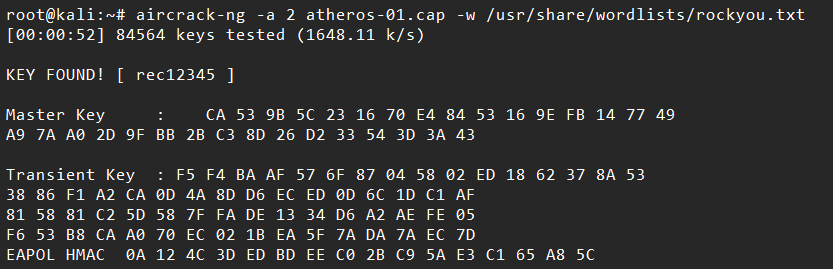












**Result:** Thus Wireless Audit in Kali Linux is implemented Successfully.