ICS009 ICS Lab 1 Wireless Networks

Lab Objective

The objective of this lab is to understand various techniques for discovering passwords and passphrases on Wired Equivalent Privacy (WEP) wireless networks.

In this lab, you will learn to:

- Crack WEP using the ***wifite*** wireless network utility

Lab Environment

This lab will requires a wireless laptop with Kali Linux flash drive and ICS lab kit.

Lab Duration

15 minutes

Lab Tasks

Attach a wireless laptop to an existing wireless network and obtain a WEP key. For this lab, a wireless laptop will be used to scan and access an inside wireless network.

Lab Scenario

Wireless networks are prone to password hacking attacks. This lab will simulate an inside attack on a wireless network that contains a PLC control system. After the access is successful using the *wifite* wireless attack utility, the network should be scanned for control devices. For this wireless network, WEP is used for wireless security. *Wifite* can also scan for more robust encryption mechanisms such as WPA2.

Lab Procedure-WiFi Sniffing using Kali Linux and wifite

1. Insert the provided flash drive that contains Kali Linux. Restart your laptop and choose to boot from USB drive. Select Live USB Persistent from the Kali boot options. Fig. 1
   - Username: **root** (admin in Windows)
   - Password: **toor** (root spelled backwards)
2. Select "**Applications**" in top left corner of the Desktop
3. Select "**Wireless Attacks**"
4. Select "***wifite***"

Fig. 1

5. When Kali terminal opens enter command: ***wifite –wep***. Fig. 2

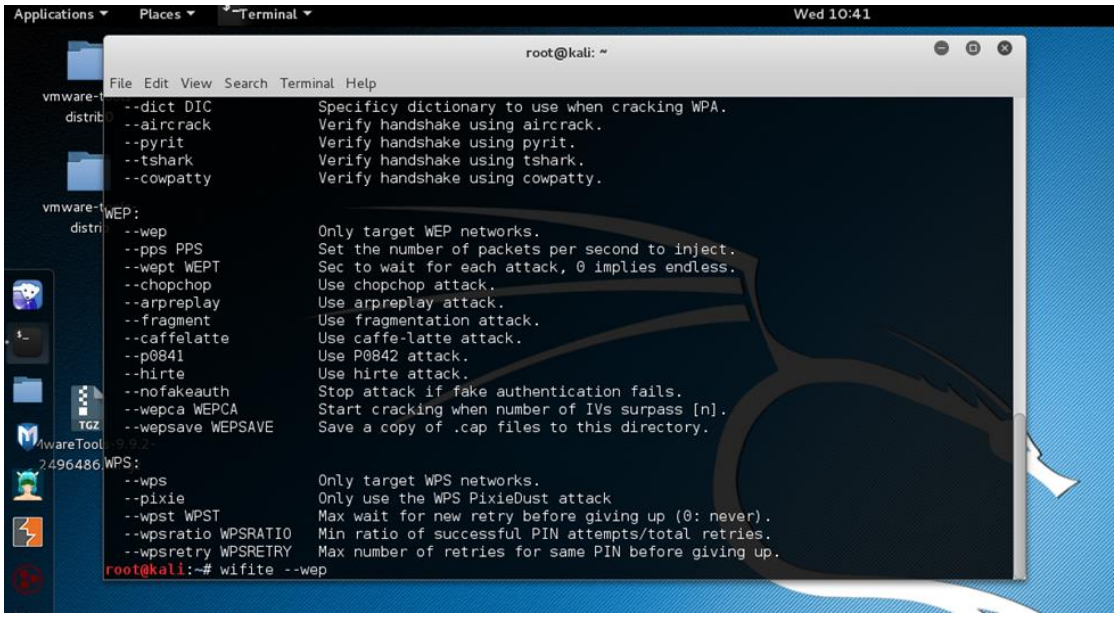

Fig. 2

- The Service Set Identifier (**SSID**) identifies the wireless network, which you will connect.
- The ***wifite*** WEP scan should discover the SSID of the network located in your ICS trainer kit.
- Select the on number the left hand side of the terminal that correlates with the SSID of your wireless network. Fig. 3

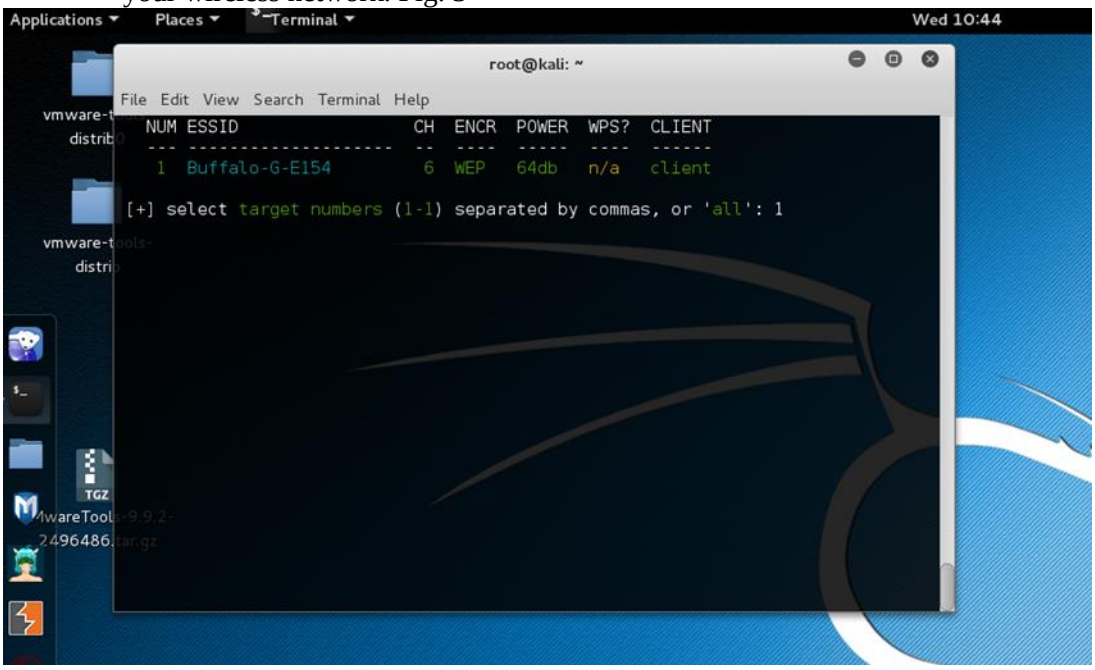

Fig. 3

- In order to crack the key, traffic must be present on the wireless network. Generate traffic on the network.

6. An **initialization vector** (IV) is an arbitrary number that can be used along with a secret key for data encryption. The goal of this step is for ***wifite*** to collect as many arbitrary numbers as possible to facilitate key decryption.
    - The *wifite* scan will start to collect IVs to decrypt the password key.
    - The scan will need between **10,000-30,000 IVs** to decrypt the key with every 10,000 IVs *wifite* will attempt to crack the password key

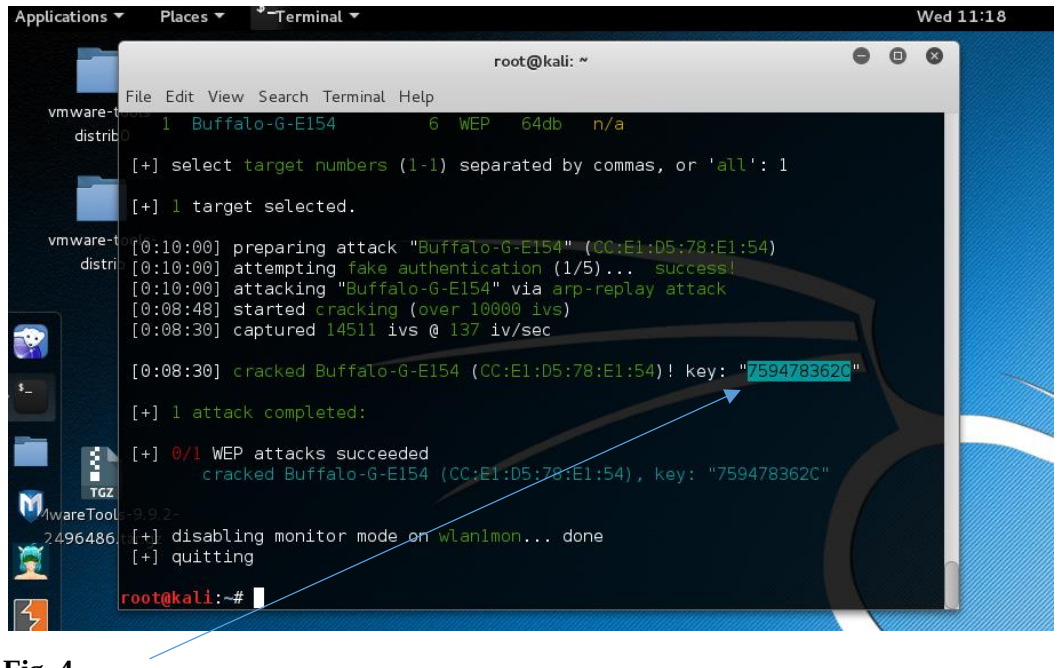

Fig. 4

- Once the key is known, you can now connect to the network to scan for devices. Fig. 4

7. Connect to your wireless network to begin the scanning process.
    - From the top right corner of your Desktop, select the dropdown arrow and click Select Network.
    - Select wireless network and provide decrypted key you obtained from ***wifite*** to connect. Fig. 5

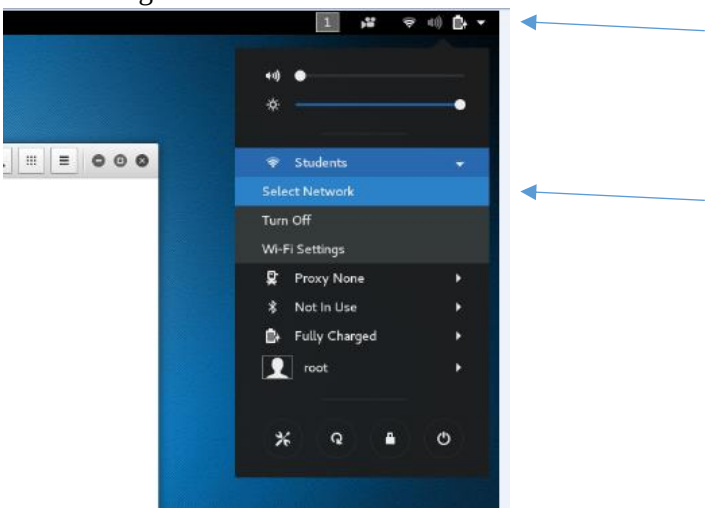

Fig. 5