Internship Report:3.Wi-Fi Security Assessment of Home Network

1. Introduction

This task involved conducting a Wi-Fi security assessment on my personal home network to evaluate its resilience against unauthorized access and other vulnerabilities.
The goal was to identify weak points and recommend security improvements.

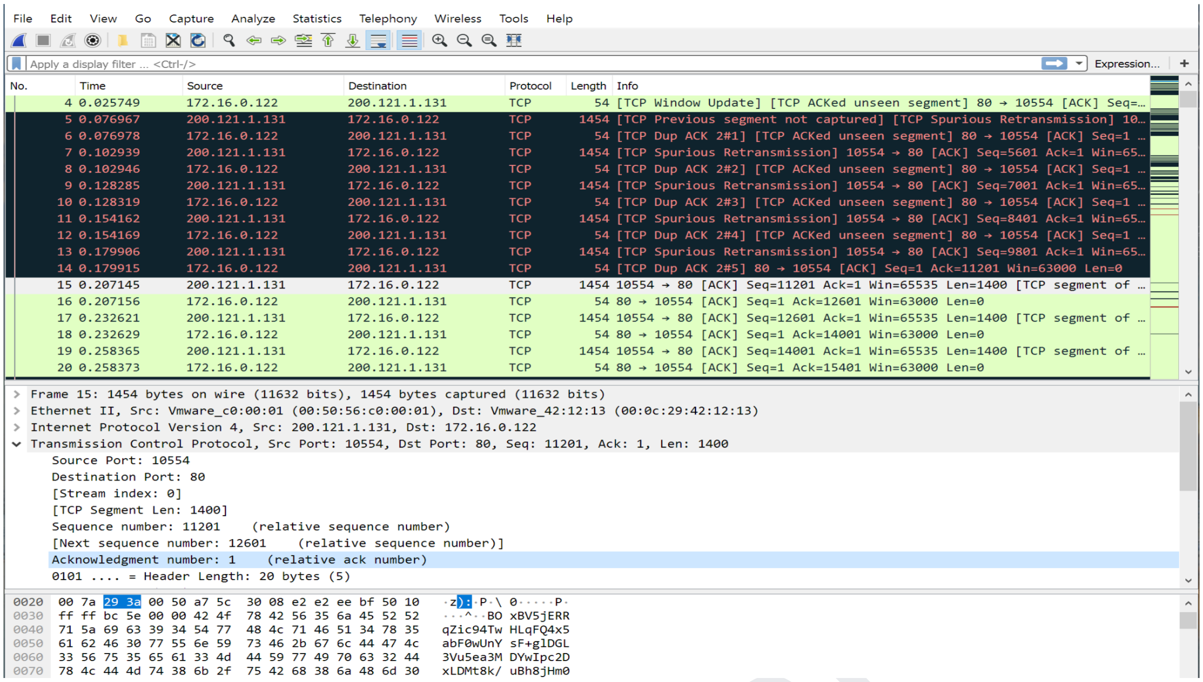
2. Tools Used

- **Wireshark** – For monitoring network traffic.
- **Aircrack-ng** – For assessing Wi-Fi password strength and encryption standards.
- **Nmap** – For scanning open ports and detecting connected devices.

3. Methodology

3.1 Wi-Fi Traffic Analysis (Wireshark)

- Opened **Wireshark**.
- Selected the wireless network interface.
- Captured wireless packets to inspect any unencrypted traffic.
- Checked for suspicious activity or unauthorized data transmission.



```
No.   Time       Source          Destination     Protocol  Length Info
    4 0.025749   172.16.0.122    200.121.1.131   TCP         54 [TCP Window Update] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=…
    5 0.076967   200.121.1.131   172.16.0.122    TCP       1454 [TCP Previous segment not captured] [TCP Spurious Retransmission] 10…
    6 0.076978   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
    7 0.102939   200.121.1.131   172.16.0.122    TCP       1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=5601 Ack=1 Win=65…
    8 0.102946   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
    9 0.128285   200.121.1.131   172.16.0.122    TCP       1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=7001 Ack=1 Win=65…
   10 0.128319   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#3] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
   11 0.154162   200.121.1.131   172.16.0.122    TCP       1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=8401 Ack=1 Win=65…
   12 0.154169   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#4] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
   13 0.179906   200.121.1.131   172.16.0.122    TCP       1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=9801 Ack=1 Win=65…
   14 0.179915   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
   15 0.207145   200.121.1.131   172.16.0.122    TCP       1454 10554 → 80 [ACK] Seq=11201 Ack=1 Win=65535 Len=1400 [TCP segment of …
   16 0.207156   172.16.0.122    200.121.1.131   TCP         54 80 → 10554 [ACK] Seq=1 Ack=12601 Win=63000 Len=0
   17 0.232621   200.121.1.131   172.16.0.122    TCP       1454 10554 → 80 [ACK] Seq=12601 Ack=1 Win=65535 Len=1400 [TCP segment of …
   18 0.232629   172.16.0.122    200.121.1.131   TCP         54 80 → 10554 [ACK] Seq=1 Ack=14001 Win=63000 Len=0
   19 0.258365   200.121.1.131   172.16.0.122    TCP       1454 10554 → 80 [ACK] Seq=14001 Ack=1 Win=65535 Len=1400 [TCP segment of …
   20 0.258373   172.16.0.122    200.121.1.131   TCP         54 80 → 10554 [ACK] Seq=1 Ack=15401 Win=63000 Len=0

> Frame 15: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
v Transmission Control Protocol, Src Port: 10554, Dst Port: 80, Seq: 11201, Ack: 1, Len: 1400
    Source Port: 10554
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 1400]
    Sequence number: 11201    (relative sequence number)
    [Next sequence number: 12601    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)

0020  00 7a 29 3a 00 50 a7 5c  30 08 e2 e2 ee bf 50 10   ·z):·P·\ 0·····P·
0030  ff ff bc 5e 00 00 42 4f  78 42 56 35 6a 45 52 52   ···^··BO xBV5jERR
0040  71 5a 69 63 39 34 54 77  48 4c 71 46 51 34 78 35   qZic94Tw HLqFQ4x5
0050  61 62 46 30 77 55 6e 59  73 46 2b 67 6c 44 47 4c   abF0wUnY sF+glDGL
0060  33 56 75 35 65 61 33 4d  44 59 77 49 70 63 32 44   3Vu5ea3M DYwIpc2D
0070  78 4c 44 4d 74 38 6b 2f  75 42 68 38 6a 48 6d 30   xLDMt8k/ uBh8jHm0
```

3.2 Password and Encryption Testing (Aircrack-ng)

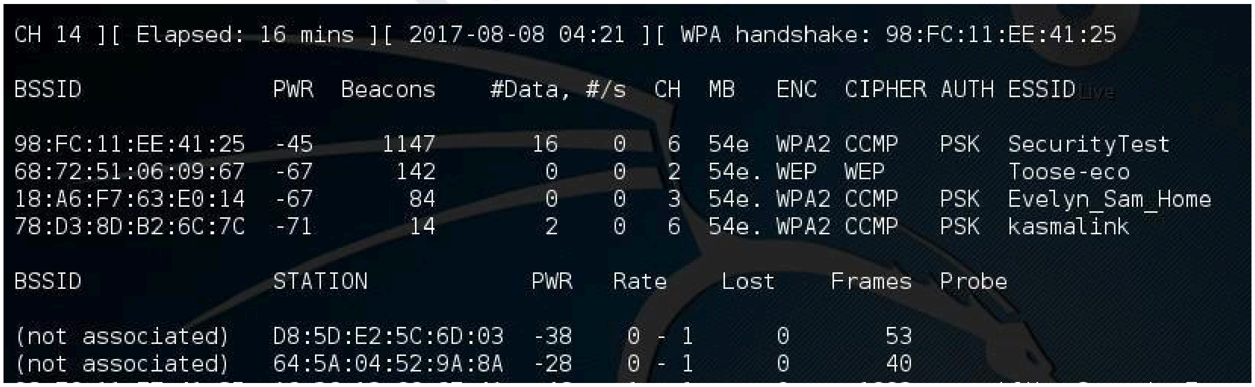
Used **Airmon-ng** to enable monitor mode:

```
sudo airmon-ng start wlan0
```

Captured handshake packets using:

```
sudo airodump-ng wlan0mon
```

Attempted to analyze WPA2 encryption and test password strength with a wordlist.



```
CH 14 ][ Elapsed: 16 mins ][ 2017-08-08 04:21 ][ WPA handshake: 98:FC:11:EE:41:25

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

98:FC:11:EE:41:25  -45     1147       16    0   6  54e  WPA2 CCMP   PSK  SecurityTest
68:72:51:06:09:67  -67      142        0    0   2  54e. WEP  WEP         Toose-eco
18:A6:F7:63:E0:14  -67       84        0    0   3  54e. WPA2 CCMP   PSK  Evelyn_Sam_Home
78:D3:8D:B2:6C:7C  -71       14        2    0   6  54e. WPA2 CCMP   PSK  kasmalink

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   D8:5D:E2:5C:6D:03  -38    0 - 1      0       53
(not associated)   64:5A:04:52:9A:8A  -28    0 - 1      0       40
```

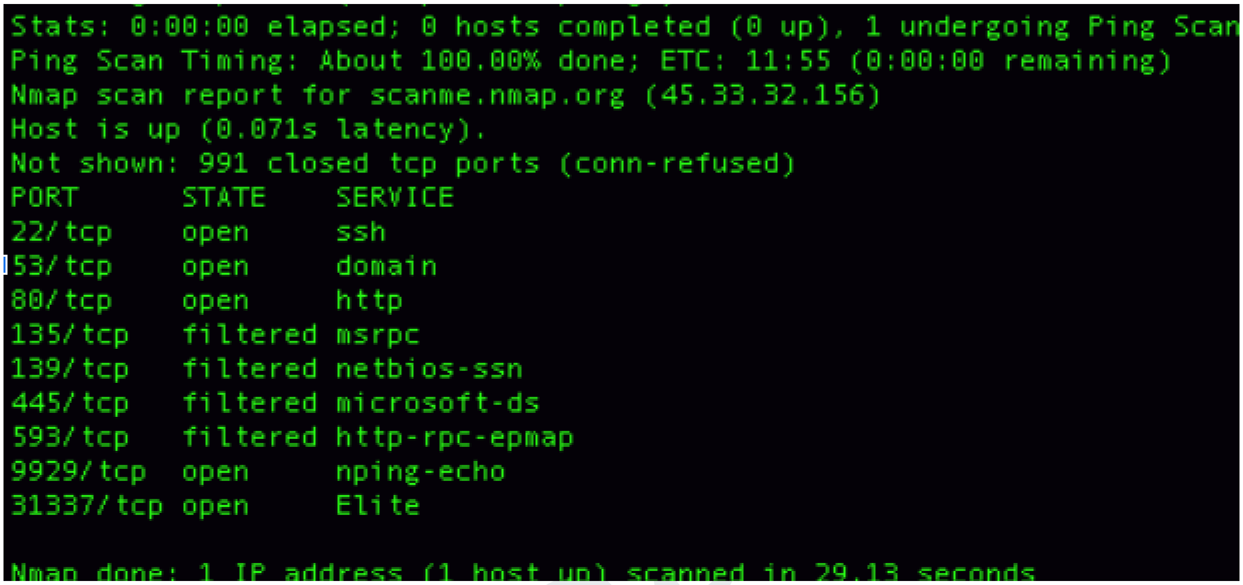
3.3 Network Scanning (Nmap)

Scanned the home network to detect active devices and open ports:

```
sudo nmap -sn 192.168.0.1/24
```

dentified all connected devices (phones, laptops, TVs, etc.)
Conducted a basic TCP port scan on the router:

```
sudo nmap -p- 192.168.0.1
```



```
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 11:55 (0:00:00 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.071s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
53/tcp    open     domain
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 29.13 seconds
```

4. Observations

Category	Observations
Wi-Fi Encryption	WPA2-Personal (AES)
Password Strength	Good (12+ characters, special symbols)
Unauthorized Devices	No unauthorized devices found
Open Ports on Router	Ports 80 (HTTP) and 443 (HTTPS) open
Traffic Monitoring	No unencrypted sensitive information detected

5. Vulnerabilities Identified

- **Default Router Login Credentials** were not changed.

- **HTTP management access** to router (unsecured web access).
- **No VPN** used for added encryption.

---

6. Recommendations

- **Change router admin credentials** from default to a strong, unique password.
- **Disable remote management** over HTTP; use HTTPS only if needed.
- **Enable MAC address filtering** to restrict access to known devices.
- **Regular firmware updates** for the router to patch vulnerabilities.
- **Use a VPN** for extra security while accessing the internet.