

1. Introduction

57% of the current population are connected to the internet one way or another. As technology continues to advance, so does the risk of network intrusions and cyber-attacks due to the advancement of new software. Intrusion can occur to any network devices connected to the internet for example (end devices such as PC's, Mobile Phones etc.) Hackers can identify weak spots in a network from unprotected router passwords to outdated security services such as (firewalls, antivirus etc.).

2. Aims and Objectives

The main aim of this project is to test the current state of standard internet security provided by internet service providers by performing different type of attacks and recording to results to see if these attacks targeted at the home network were successful .

- Research state of network security and network tools.
- Design & Implement a home network.
- Analyse results of the tests on the network.

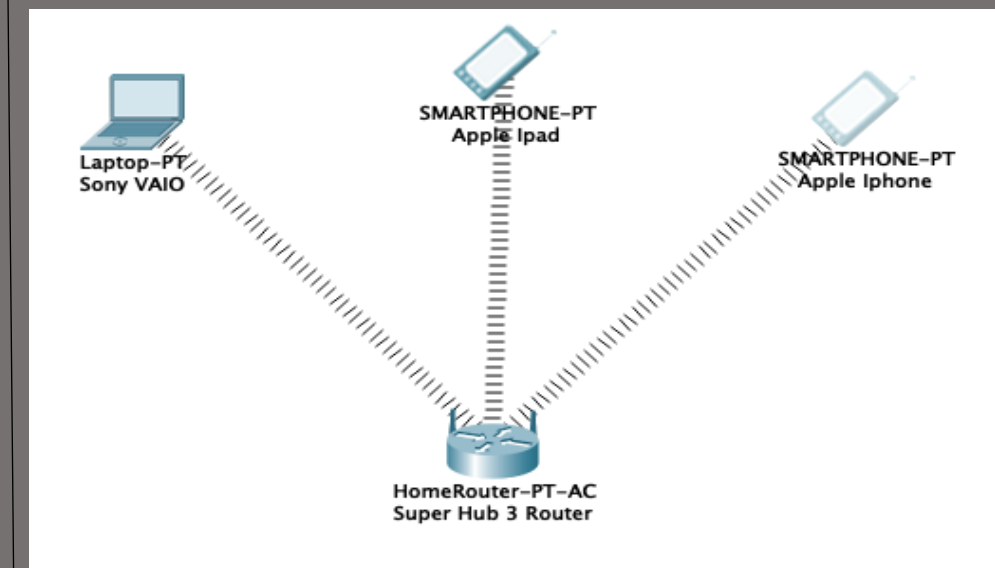
3. Research

Wireless security are mainly governed by the 'WEP, WPA and WPA2 protocols with weaknesses found within all protocols.

Poorly secured Networks are prone to intrusion attacks such as the Man in the middle attack, Phishing & WPA2 Krack attack

4. Design

- Components; Laptop, Smartphone, tablet device, Wireless Router
- Designed on Cisco Packet Tracer
- Limited to three end devices to avoid any unnecessary network traffic



5. Results

ARP Spoofing allowed the cyber attacker to eavesdrop network traffic between client and server on all devices connected to the network. Kali Linux command terminal and Wireshark allowed the cyber attacker to overlook the network traffic.

Clone Phishing acquired login credentials from end devices after cloning social media websites on the network. Setoolkit available on the Kali Linux terminal was used to perform the attack.

```
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=iphonelogin
POSSIBLE USERNAME FIELD FOUND: session[password]=iphonelogin
POSSIBLE PASSWORD FIELD FOUND: session[password]=iphonelogin
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

```
192.168.0.21 - - [04/May/2020 20:24:28] "POST /sessions HTTP/1.1" 302 -
192.168.0.34 - - [04/May/2020 20:24:50] "GET / HTTP/1.1" 200 -
```

6. Evaluation

- Kali Linux penetration tools cause many problems for typical home networks.
- Once an intruder gains access into the system it is almost inevitable that they can use penetration tools to extract data such as network traffic.
- Basic security systems are almost doomed if a cyber attacker attempted to intrude the network.

7. Conclusion

- There are many flaws with basic internet service provider settings with risk of intrusion.
- Kali Linux command terminal offer many free penetration tools available to the general public.
- Essential to use Intrusion Detection System such as an Anti-virus.