



Building a Secure Home Network

Ibrahim Balogun (1901140) Computer Networks and Cybersecurity
Email: i.balogun95167@gmail.com



Project Summary

The plan for the experiment is to implement network security methods onto a network and then proceed to attack the network to demonstrate which security measures are more effective than others. Some of the tactics that will be used to protect the network are changing the connection password, using a DNS service provider and changing the router's default IP address if possible[1].

Aim & Objectives

The project aims to build and test a secure home network that will benefit home uses and home users. To fulfil the aim the objectives are to, conduct research into network security and network vulnerabilities, analyse the different methods that could be used, conduct the experiment, analysis the results, and use the results to produce a secure home network.

Methodology

The methods used in the experiment need to be controlled. The only way it can be controlled is if a variable is manipulated. The variables in the experiment are the attacking methods, as these will need to change when attacking the network. The constant in the experiment is the network itself, as changing this aspect will alter the whole experiment.

The methods the project will follow are, to start by gathering information on the different attack methods and networking, then planning out the attack strategy, proceed with the attacks and record the results.

References

- [1] L. Constantin, "How to secure your router and home network," Csoonline, 18 November 2019. [Online]. Available: <https://www.csoonline.com/article/3093385/how-to-secure-your-router-and-home-network.html>. [Accessed 20 December 2021].

WPA2 Crack

```
CH 3 [[ Elapsed: 1 min ]] 2022-04-27 17:49 [[ WPA handshake: C0:06:C3:19:9D:D8
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
C0:06:C3:19:9D:D8 -51 100 728 351 0 3 195 WPA2 CCMP PSK TP-Link_900S
BSSID STATION PWR Rate Lost Frames Notes Probes
C0:06:C3:19:9D:D8 70:66:55:4D:2B:C7 -51 1e-1e 0 283 TP-Link_900S

root@kali:~#
```

Figure 1: showing the WPA handshake

Conclusion & Reflections

The conclusion for the project as a networking student is primarily positive as furthering the understanding of computer systems and network work security; with the use and knowledge gained from the literature review, the student has gained extraordinary experience that will be carried on into the future.

The most significant area for further research is carrying out more real-world experiments on home networks, as this is the only way to gather enough information to build a secure home network.

MITM Attack

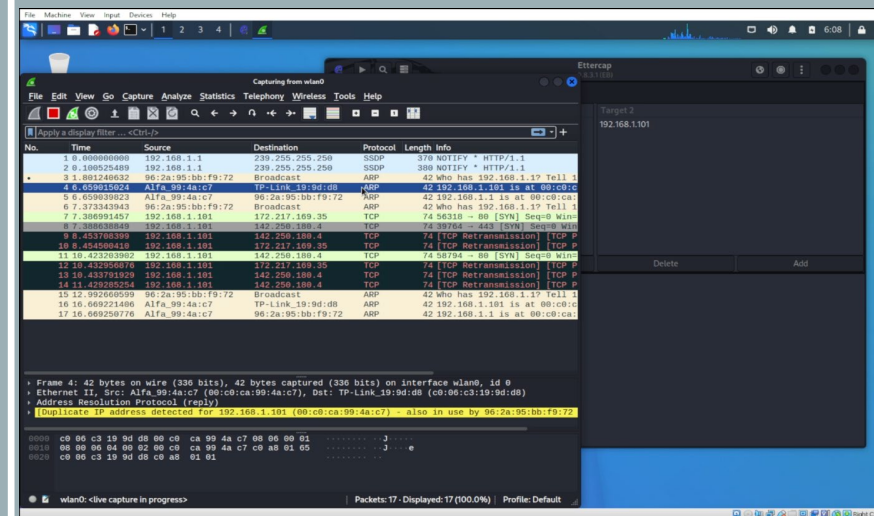


Figure 2: ARP poisoning of a device.

Design & Implementation

Figure 3 shows a laptop and a wireless AP this replicates the home network since the laptop will be used to set up a password on the router. The attack simulation will be executed on the desktop PC using Kali Linux software, and the desktop PC will be linked to the mobile devices as the mobile devices will function as a wireless access point for the desktop PC.

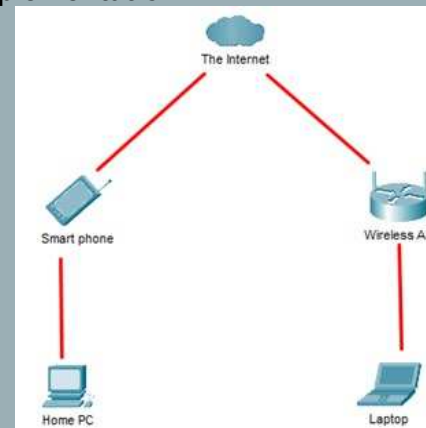


Figure 3: Shows the home network.