

1. Introduction

The project focuses on how to build a secure home network. Essentially, this is a network that can protect its users and data from specific attacks. New threats are introduced every day meaning it is very difficult to secure a network against every threat.

2. Aims and Objectives

The main aim of this project is to build a home network that can be used to conduct experiments to find the vulnerabilities and provide solutions to secure the network.

Objectives:

- Research different devices that are in home networks
- Research threats/vulnerabilities
- Research solutions for the identified threats
- Design and implement a home network
- Conduct the experiment by completing the attacks

3. Related Work

Three main papers were used when conducting this project, the key topics from each of these can be seen below.

1. This paper looks into how WPA2 attacks can be performed within Kali Linux [1]
2. This paper looks at an approach to a P-SCAN. This paper looks into every devices security within the network [2]
3. This paper looks into how secure IoT devices are [3]

4. Design and Implementation

A physical network was designed and built to produce the results for analysis. The implementation included the following.

- Wireless Router
- Network Devices
- IoT devices
- Smart devices
- Kali Linux operating system

5. Results

The results from the project experiments can be seen in figure 1-3. Figure 1 identifies open ports within the device that was tested. Figure 2 shows the results from the man-in-the-middle attack. Figure three is used to show that the WPA2 password was cracked “X-Win32_v6”.

6. Conclusion

This project was completed to investigate the security within home networks. This enabled the author to provide solutions so that a secure network could be built. The aim and objectives of the project have been met and future work was identified.

- Knowledge of Kali Linux operating system
- Security implementations and software on the market today
- Security threats that are affecting networks today

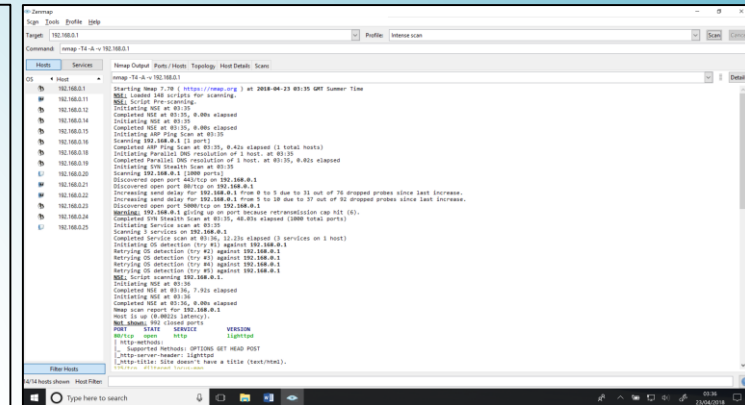


Figure 1

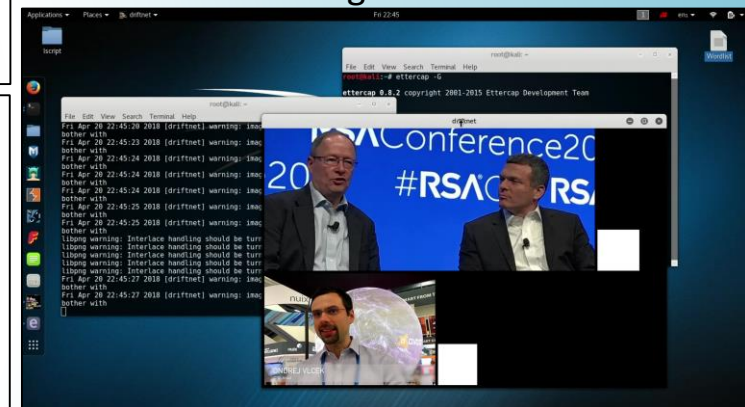


Figure 2

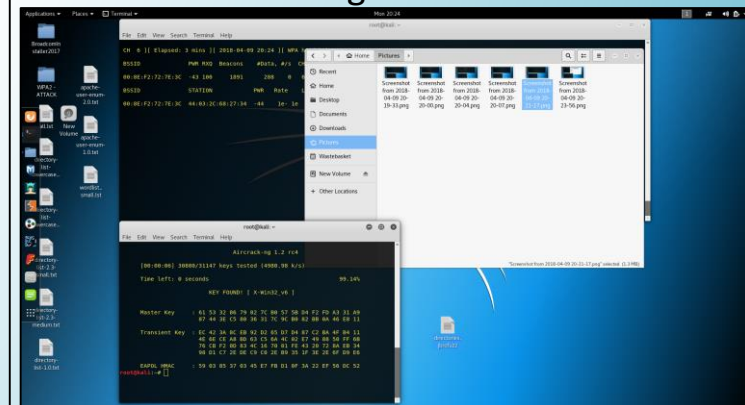


Figure 3

References

1. Profiling and mitigating brute force attack in home wireless LAN (2014)
2. IoT security assessment through the interfaces P-SCAN test bench platform (2018)
3. Vulnerability scanning of IoT devices in Jordan using Shodan (2017)

Table of Figures

1. Port Scanning
2. Man-in-the-middle
3. WPA2 Password Cracking