



Testing security of networks against Denial-of-Service attacks

Mikolaj Michalski 1900885@student.uwtsd.ac.uk

Conclusion

The project was completed in which the network was successfully attacked. All the tested attacks penetrated the network and because of this its recommendations have been made to which could prevent the attacks from being successful. The aims and objectives of the project have been adequately met and future work that could be done has been covered.

4. Related works

Here are some of the related articles or conferences that helped gain a better understanding in the topic areas.

1. Paper covering DDoS attacks and securing of a smart home network. [1]
2. Article covering DDoS prevention and protection against the attack. [2]
3. Article that covered securing a home network. [3]

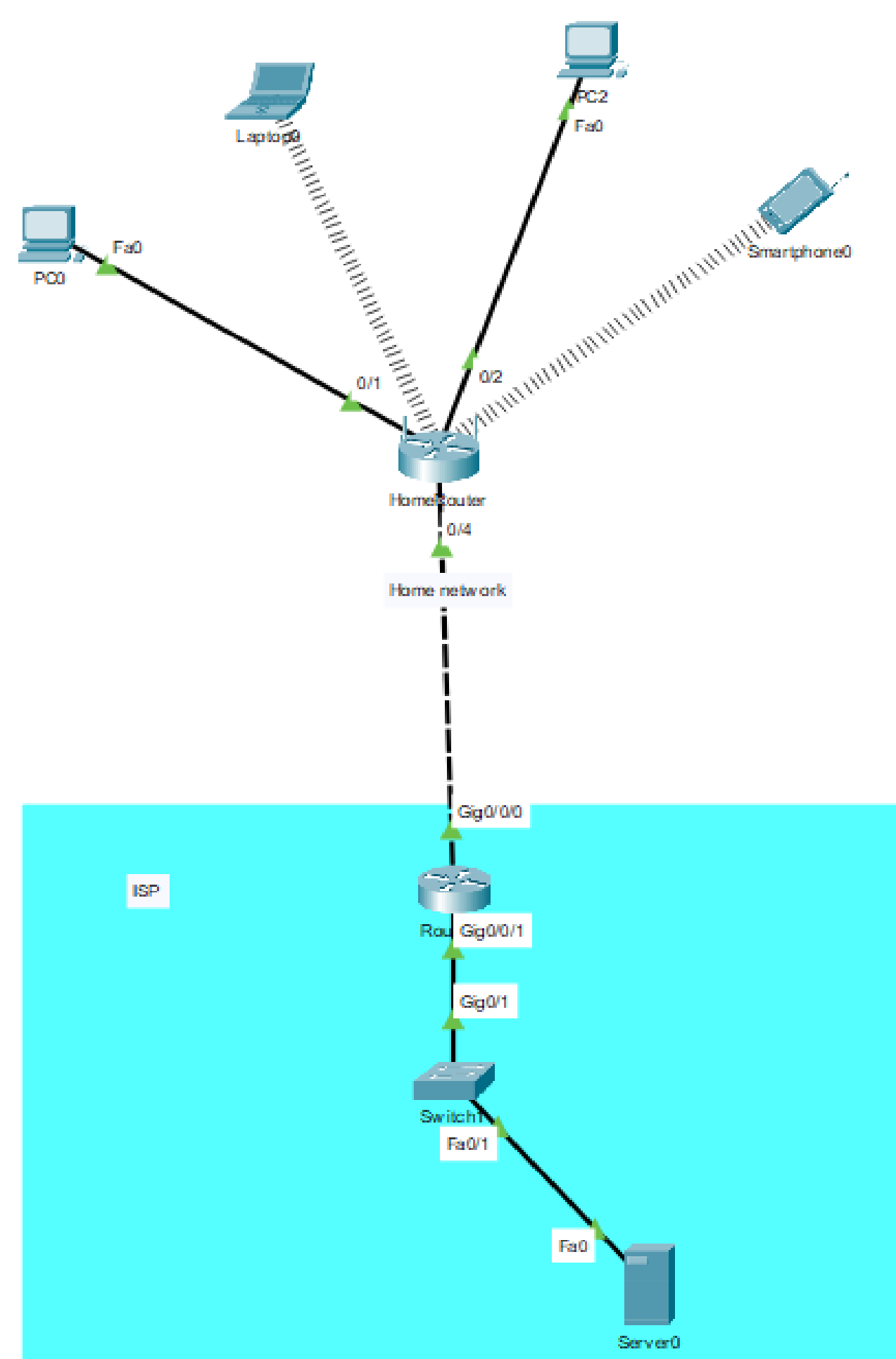


Fig 1

1. Introduction

The project will investigate security measures that can be set up to protect a home network from a botnet attack. This will first be demonstrated in a simulation and then attempted to be recreated in VM software for safety and legal reasons. This project will help show how to secure the home network to be protected against DDoS attacks.

2. The Aim

This project aims to see how secure a home network is against different types of DDoS attacks. The results will be compared to a direct security approach against DDoS attacks to see how well it competes at securing a network.

3. The Objectives

The objectives for this project are:

- Create a critical literature review of the research conducted to demonstrate the knowledge gained.
- Document and cover different types of research that can be used for the project. Create a project plan to show the time management over the course of the project.
- Utilise the knowledge gained from the review to recreate a network and experiment with different security measures to successfully protect and secure the network.
- Testing the security implemented in the network to see if it will protect it from a DDoS attack.
- Creating methods that will resolve any of the vulnerabilities found during the tests, (if it's possible to secure in the timeframe). These methods would then be retested to ensure the new network improvements have made it more secure.
- To evaluate whether the security issues in the network are caused by the users or by out-of-date security.

5. Implementation

There were 3 different denial of service attacks that were conducted in this project. These attacks were the DoS SYN flood attack, the DDoS attack, and a botnet DDoS attack. Figures 2, 3 & 4 cover the attacks that were launched in the project.

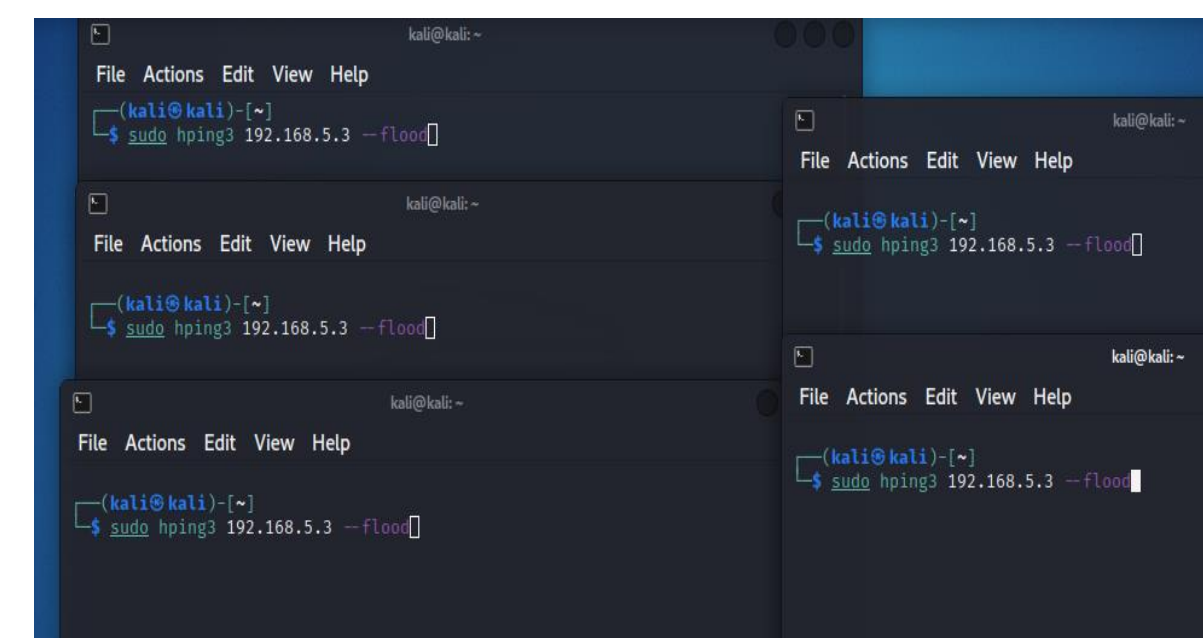


Fig 4

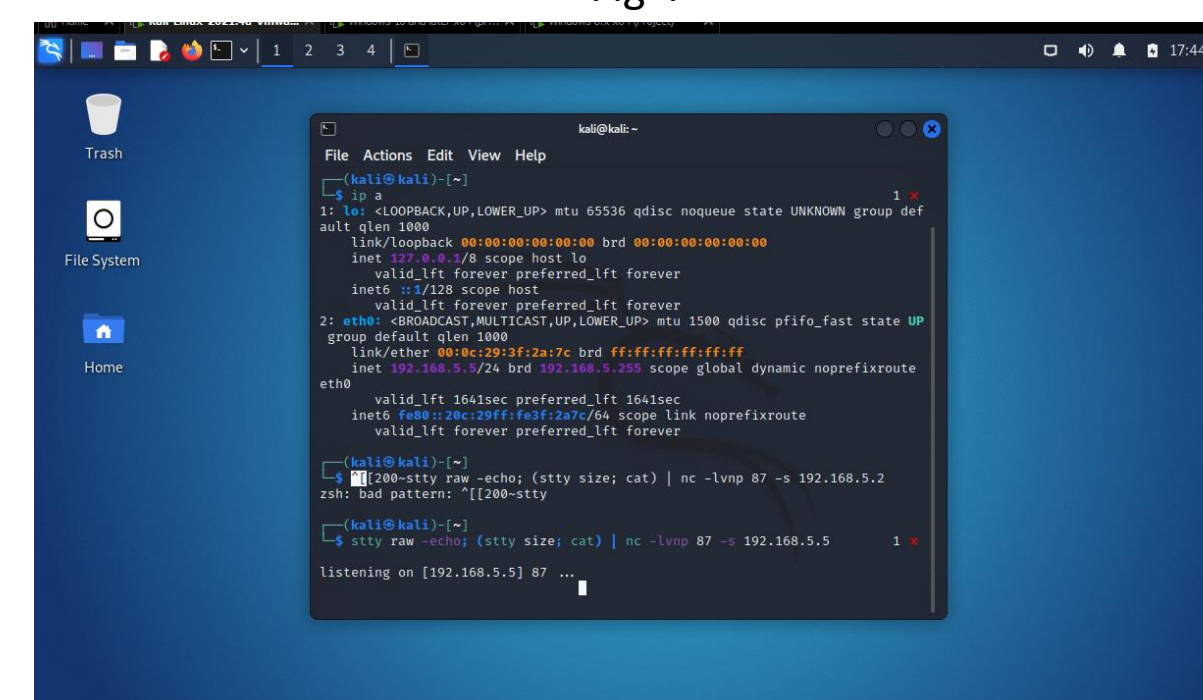


Fig 3

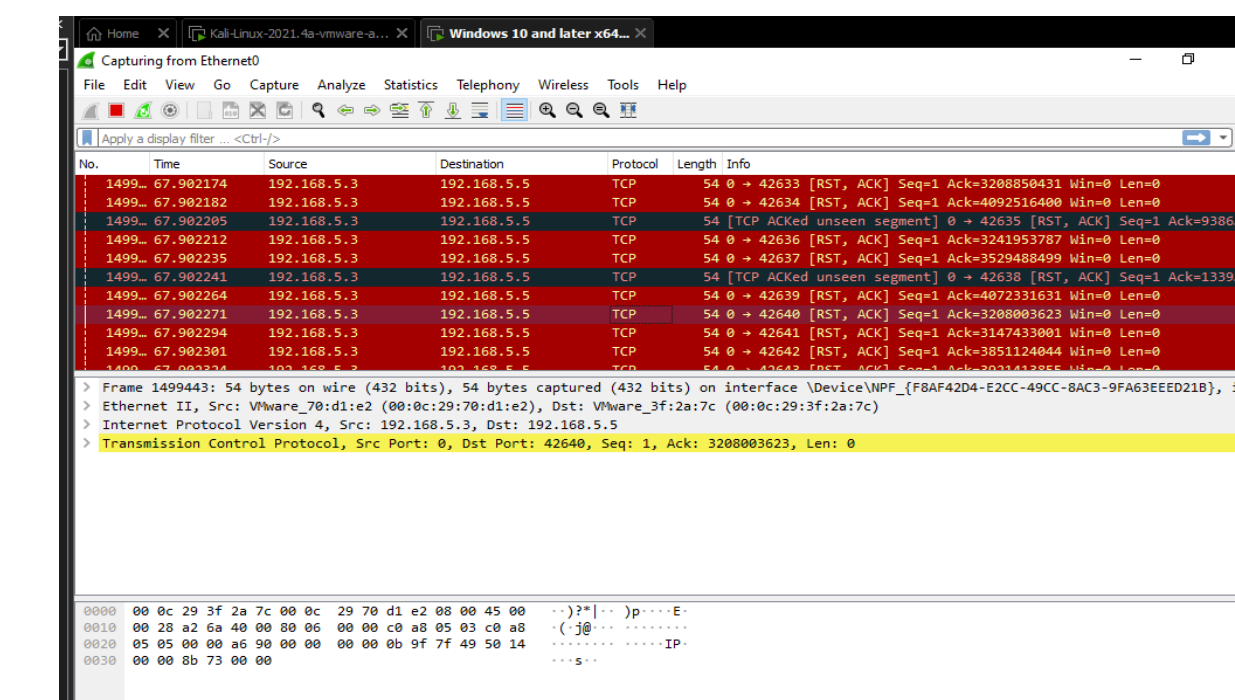


Fig 2

References & Figures

- [1] N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242-2270, 2015.
- [2] U. Saxena, J. Sodhi and Y. Singh, "A Comprehensive Approach for DDoS Attack Detection in Smart Home Network Using Shortest Path Algorithm," in *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, 2020.
- [3] D. Shin, K. Yun, J. Kim, P. V. Astillo and J.-N. Kim, "A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks," *"A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks"*, vol. 7, pp. 142531-142550, 2019.

Figure 1: Network Diagram

Figure 2: Wireshark displaying the DoS SYN flood attack

Figure 3: Echoing on a port for reverse shell (Botnet attack)

Figure 4: Launch of the DDoS attack