

1. Introduction

My project was about securing a home network, and it required me to look into vulnerabilities that could pose a risk to home networks, as well as security aspects that could be put in place to help secure the network. My experiment required me to use penetration testing tools on a home network to determine how much of a risk they posed to a home network, and once I understood the risk, I had to introduce security features to the network to improve the security.

2. Aims and Objectives

Aims

The project's goals are to demonstrate the security vulnerability of a home network and how to secure the network in the long term.

Objectives

The project objectives are:

- Investigate network security and network vulnerabilities.
- Carry out network penetration testing.
- Analyse the results in order to take out security measures.
- Highlight the security measures implemented and report on how they will improve the network's security.

3. Experiment

Figure 1 depicts the usage of Ettercap to commit a man in the middle attack; this assault targeted a network device to capture data that was processed by the user; to do this, I employed the ARP Poisoning technique for the MITM attack.

Figure 2 depicts the use of Zenmap to commit a port scanning attack. The purpose of this attack is to gather information about the network in order to identify vulnerabilities and potential exploits that could be used to attack the network. The scan used was a vulnerability script to detect any potential vulnerabilities.

Following the execution of these attacks, security features such as stronger passwords, SSID change/deactivation, a firewall, firmware upgrades, and the disabling of any unused port forwarding were implemented in order to limit the risk of future attacks.

4. Man in the middle attack

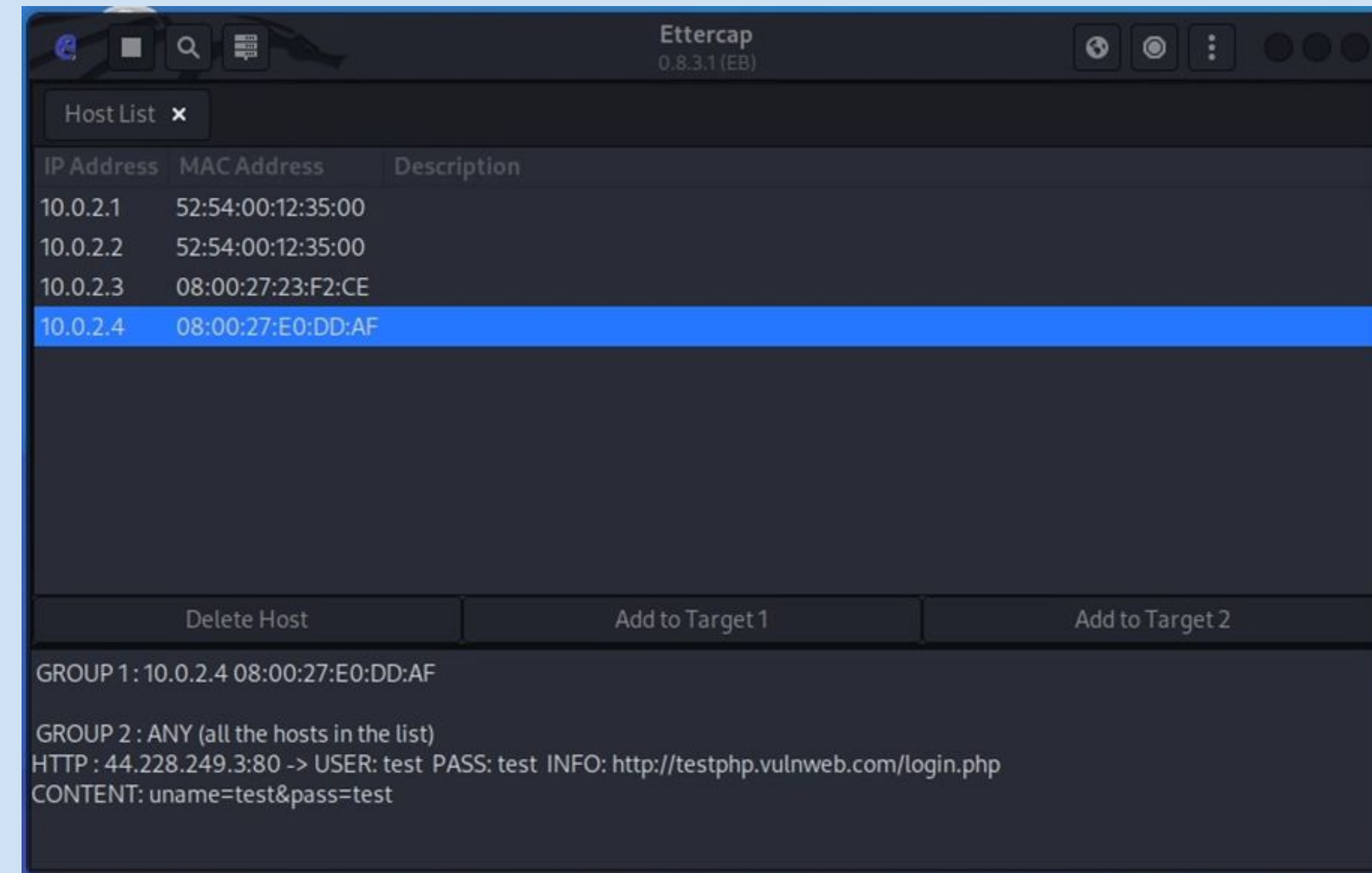


Figure 1: Using Ettercap for a MITMA

6. Design and Implementation

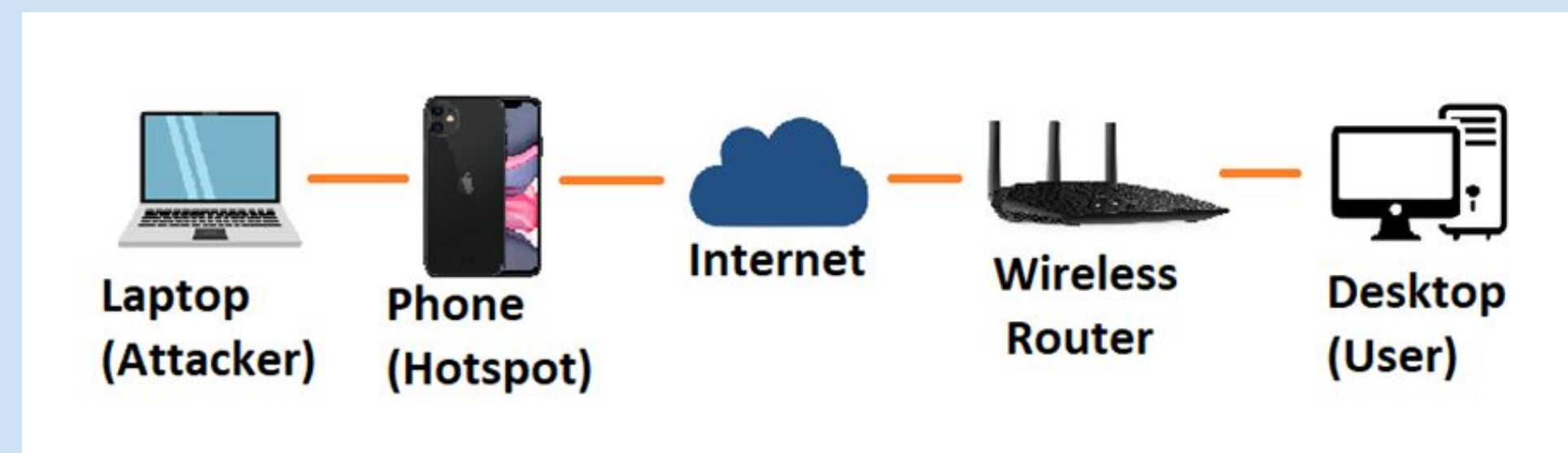


Figure 3: Network Design

Figure 3 depicts the network configuration utilised in the experiment; the home network includes a wireless router and a desktop to imitate a network connection, while the attacker's network has a laptop and a phone to represent a Hotspot connection, with both networks having internet access.

Kali Linux was utilised with pre-installed penetration tools for the attacker to use, however the tools required throughout the project were Ettercap and Nmap.

5. Port Scanning

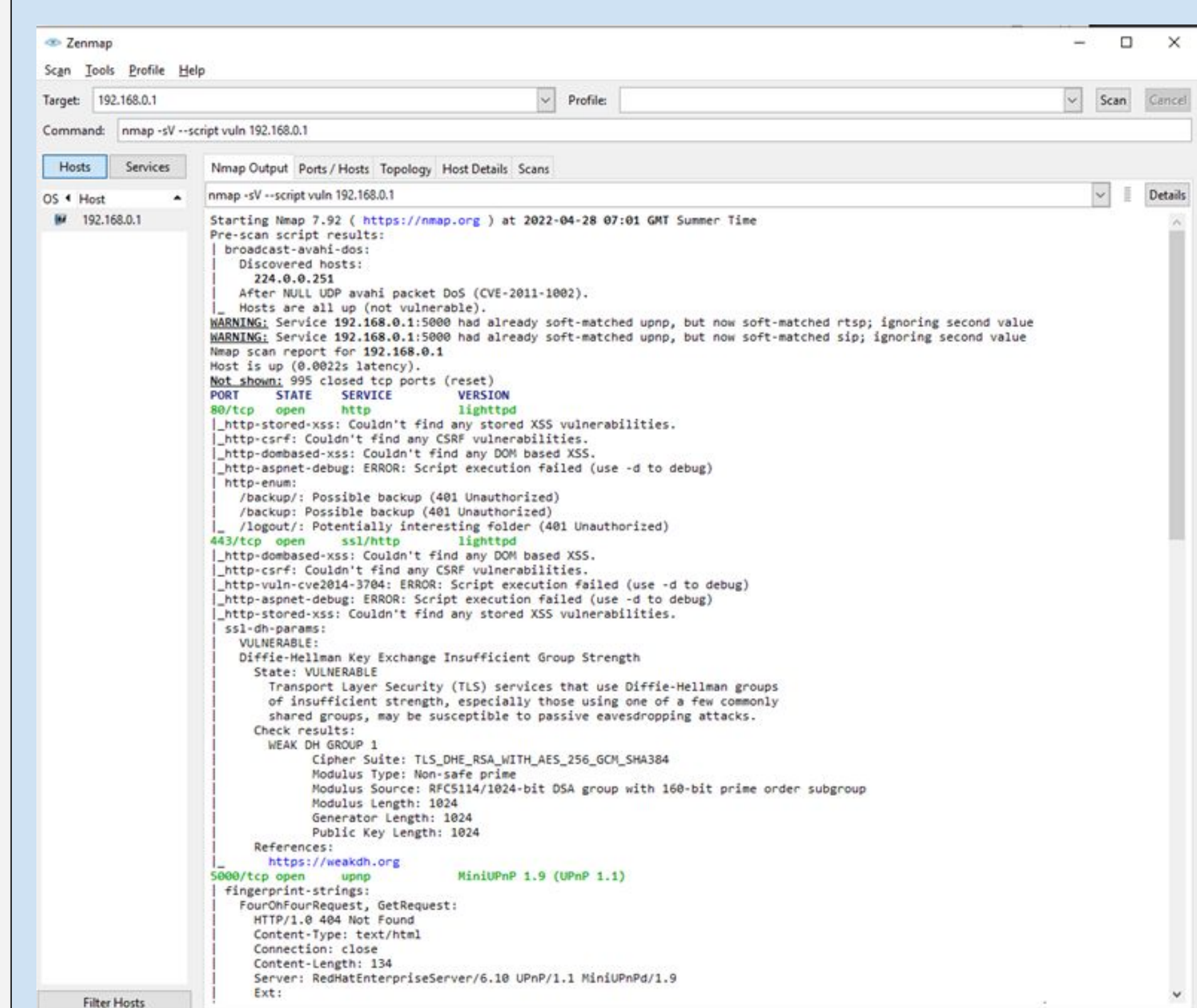


Figure 2: Using Zenmap for Port scanning

7. Conclusion

The project's goal was to learn about the security flaws in a home network and how to fix them. Throughout the experiment, many discoveries were made about the potential vulnerabilities of a home network and how they could be affected, as well as solutions that was discussed throughout the project on how the most common vulnerabilities could be patched by introducing simple configurations and security procedures to home networks, resulting in a much more secure network.

The project assisted in gaining more knowledge about networks and potential vulnerabilities that could be used to attack a network, as well as security procedures that could be implemented to reduce the chances of an attack. This will be useful in the future whether the student decides to pursue a job in cyber security or continue with studies.