



1. INTRODUCTION

We live in a world full of technology, and hundreds of electronic devices surround us every day such as – phones, security cameras, laptops, printers, computers, cars and even more. In order to achieve a good understanding of security measures and structure, the three different perspectives will be compared, and a conclusion will be drawn. Also, the lack of knowledge and awarness of most home network owners is the topic that needs to be discussed so this project will focus on securing the home network to show how easy it is for hackers to penetrate the network and potentially ruin someone’s life by stealing banking details, identity or sensitive information. People tend to ignore topics like that until it hits them and they have to face the consequences of not being careful online. This project will discuss all these issues

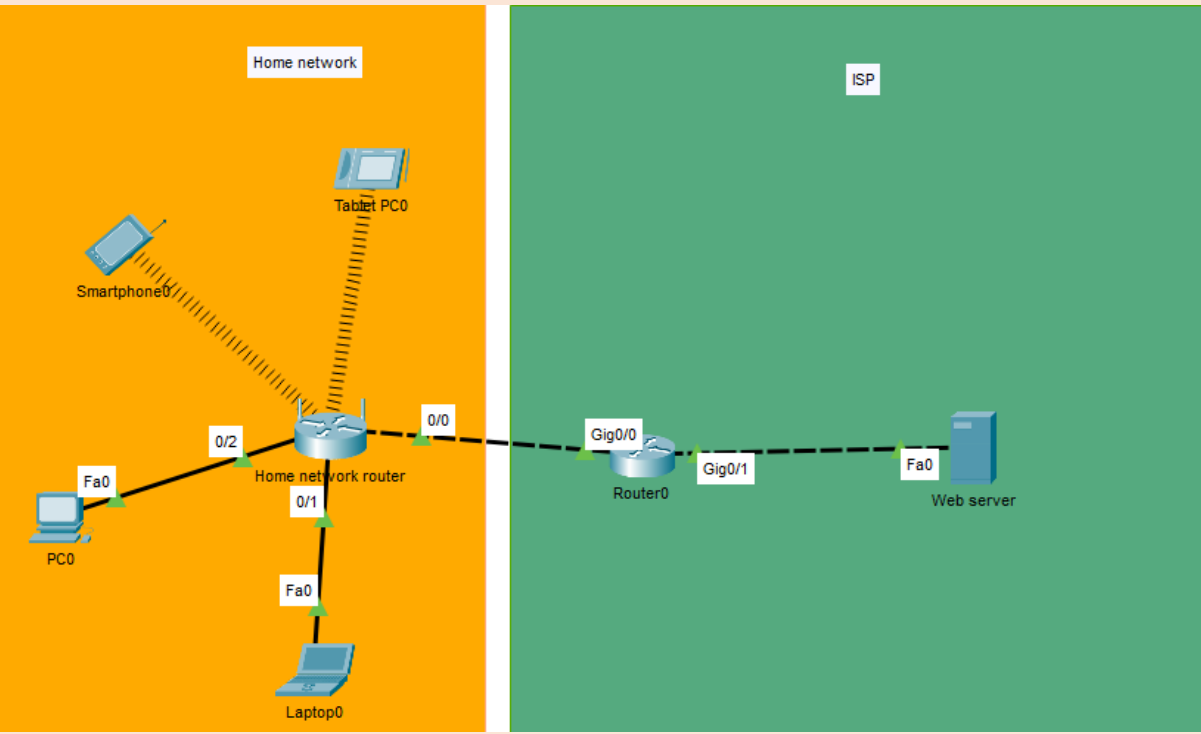
2. AIM & OBJECTIVES

The main aim of this report is to create a secure home network so it can be penetrated and tested to see if the network is fully secured and vulnerable to any type of attacks, if so then it will be fixed and prevented. However, the clarification of the issue and of how it was fixed will be provided and deeply explained. Gain a broad knowledge about the main subject of this project which is securing the home network and about vulnerable spots of the network as well as fixing the security gaps.

- Establish understanding of all the possible attacks that can happen at any time and find out which are the most common ones and provide a brief and clear solution to them and how to avoid them in the future by applying a few simple steps and features.
- Provide a critical literature review of the aim, objectives, and current research with the aim of providing the level of existing knowledge about the subject.
- Use and present the assets gathered from the research and literature review to produce a secure home network by creating a VMware network to try to break in and penetrate with all the possible attacks and resources so the weak spots are discovered and fixed as soon as possible. This will be approached in a few ways; phishing commonly known as creating a fake website, DoS attack which sends an enormous amount of packets towards victim’s router, DDoS where multiple machines are being used to send a large amount of packets against the server / router, Man-in-the-middle attack where the attacker gets in between the victim and application and finally password cracking and also create a Gantt Chart.
- Gain a broader understanding of all the methods used such as simple troubleshooting to fix the issues with the network, such as going back, troubleshooting every single device, and checking the configuration just to find the error, understand how it happened and fix it and avoid it in the future.
- Provide a brief and clear instruction and recommendation on how to avoid cyber-attacks and loss of sensitive, important, and valuable data and fully secure the network and devices connected to the network step-by-step and also provide a clear reflection on how the project went.

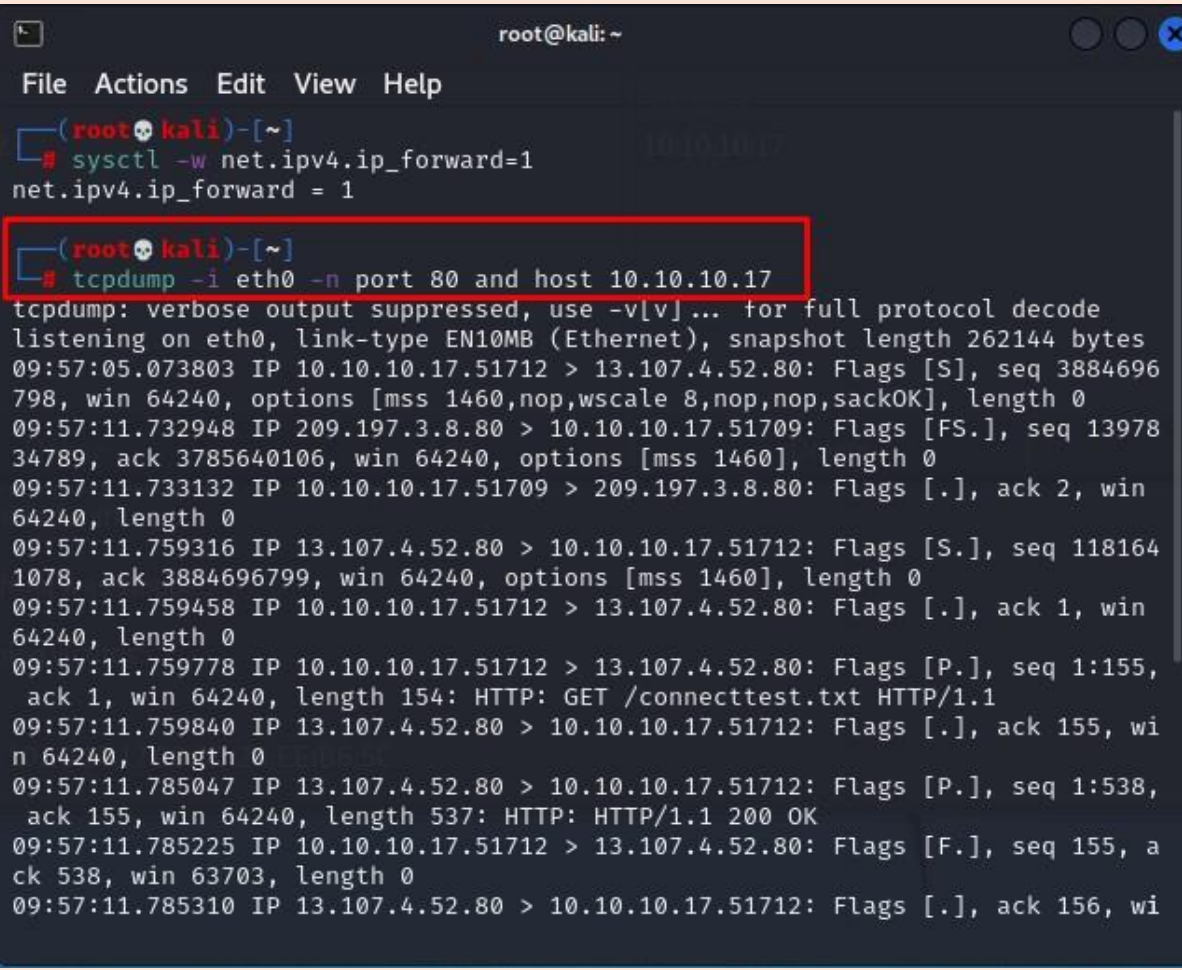
4. DESIGN & IMPLEMENTATION

According to the research, the most common home network setup is shown below. It consists of a few wired and wireless devices connected to the router that provides the internet connection. First the network was created in packet tracer and then it was created using VMware where the environment is safe and nothing dangerous or illegal can happen due to the attacks that will be executed. This will also carefully explained the stages of design and how the network was implemented.



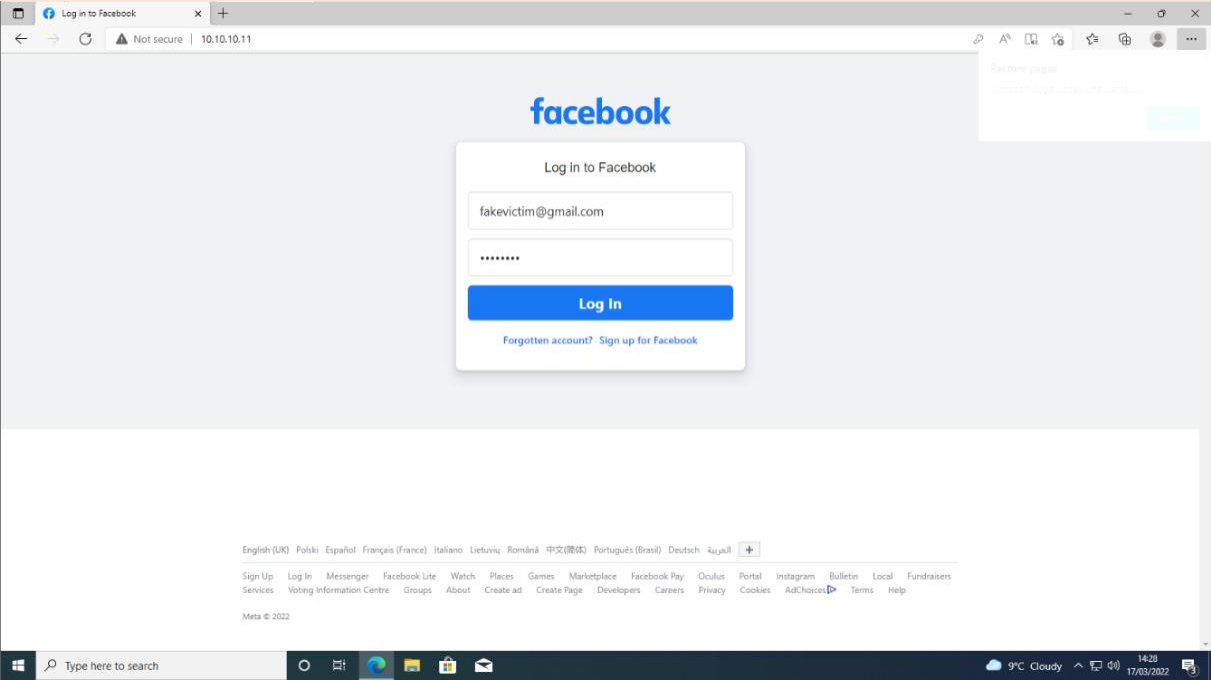
5. MAN IN THE MIDDLE ATTACK

Man in the middle attack allows the hacker to sniff the packets that are being sent between the user and the application. The hacker just sits there and listens without any notification to the user. The tools that were used to execute this attack are ettercap and also tcpdump to sniff the traffic between the attacker and the victim.



6. PHISHING

Phishing is a type of attack to get the victim to enter the credentials by pretending that the website, text message etc. Comes from a legitimate source. The type of phishing that has been done in this project is spear phishing which could be also called credential harvester attack. A fake linkedin login page has been created thanks to Social Engineering toolkit, the victim has accessed the post back IP address configured during the creation of the website which is the Kali Linux IP address. The victim has accessed the page, entered the credentials and the tool has generated a report which clearly showed the email and password entered.

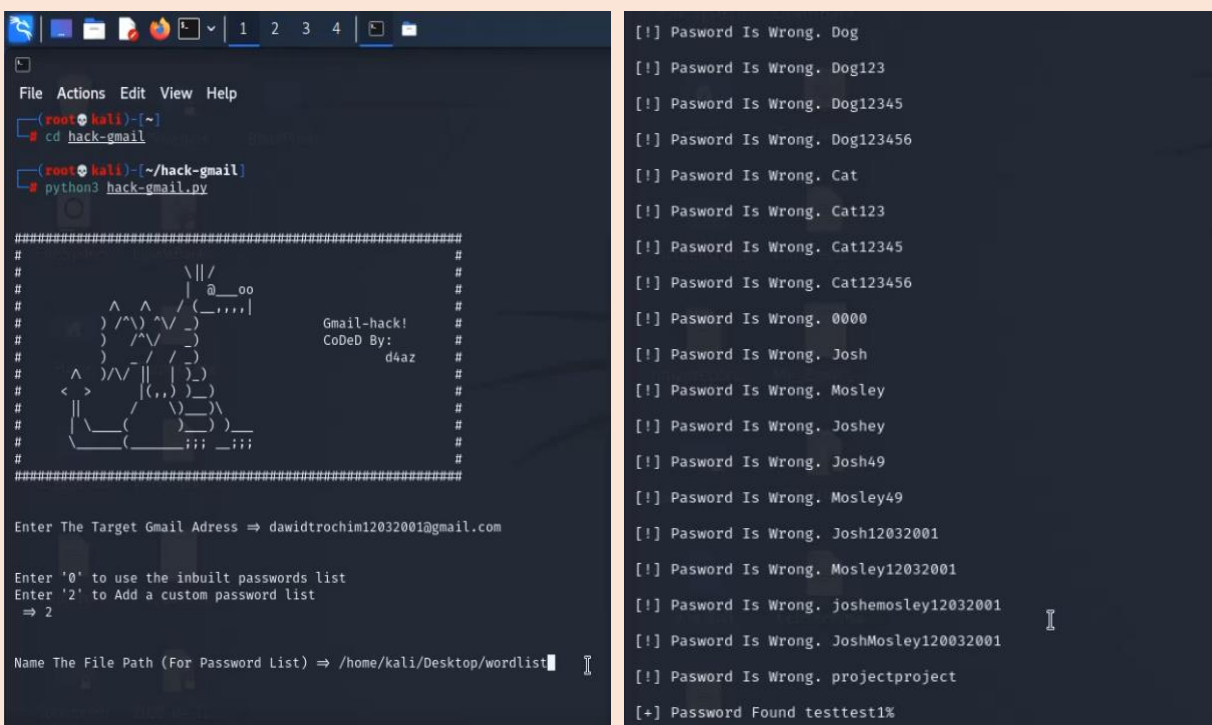


7. DOS AND DDOS

Both attacks are meant to disrupt the performance of the network or shut it down. However, DDoS attack in this project was used by using two machines to DDoS another client, however in real-life scenario there would be many machines doing the attack. The hping and ping command were used to shut the connection on a local network machine. The DoS attack was done using metasploit Synflood method that targeted the TCP port 135. Local firewall has been enabled and configured along with the anti-virus installed to prevent the machines from becoming a bot that the hacker controls.

8. PASSWORD CRACKING

Password cracking is an attack where the word list of usernames and passwords was given to the tool and then the tool went through the list and tried to find a match of username and the passwords by attempting to log in to the link that was specified in the tool. Hack-gmail was used in this case and it was git cloned. The email was specified along with the password list when the match was found there was a notification.



9. METHODOLOGY

The research methodology that was chosen is called exploratory research and this methodology is well-suited to it since it supports the understanding of the matter, supporting the investigator in understanding how and why the certain things happened, and enabling the researcher to develop an extremely informative conclusion about the subject area. An explorative approach is a methodological approach that focuses primarily on describing the multiple aspects of a research project. To use this methodology, the researcher will begin with a broad concept and afterwards implement their discoveries as a single component that will result in future subjects. It is suitable for this project because expanding knowledge of the subject is quite essential in this case and allows for some very useful conclusions to be formed, and the subject of this project has not been properly discussed earlier, however the threats and attacks are still occurring.

10. CONCLUSION

Overall, the project has been successfull and 5 attacks were executed successfully. The literaturew review, methodology, design, implementation and conclusion were done. The related works really helped with any knowledge gaps and helped to understand the area of study and the project itself. The aim and objectives were clearly outlined and provided a guidance throughout the project and helped to stay on track. The Gantt Chart documented the journey with dates and duration. Methodology was also a good indication of where to direct my research, which path should be taken in order to carry out a good research. The implementation part had some issues where the VMware would drop the connection randomly and the fix was to reset network settings to default in VMware and just leave it as it was.