

Analysis of Security Methods of Computer Networks

Joseph Williams(1902388), Computing (Computer Networks and Cyber Security) - BSc (Hons)

University of Wales Trinity St. David SA1 Campus

Email: 1902388@student.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

1. Introduction

Due to the rapid growth of IT both professionally and personally, network security has become even more crucial. This project focuses on an analysis of security methods by testing network attacks on an implemented network and the implementation of security methods to prevent these attacks from being successful. Research into studies to understand network attacks, IEEE standards and security methods were carried out as well as an experiment to test the network attacks and test if the security methods were effective in their purpose.

2. Aim & Objectives

The Aim of the project was to analyze security methods of computer networks to better understand their operations, functions, and effectiveness. The objectives were:

- Research into computer networks focusing on potential network attacks, network vulnerabilities and security methods that can be incorporated.
- Critical literature review based on the aim, objectives, and any research into the project topic area.
- Using the knowledge gathered from the literature review, design a network.
- Create a simulated network based on the design.
- Launch attacks on the network and record the outcome.
- Propose and implement security methods to overcome the attacks.
- Test the secured network and record the outcome.
- Analyse the security methods focusing on the results of the experiment.

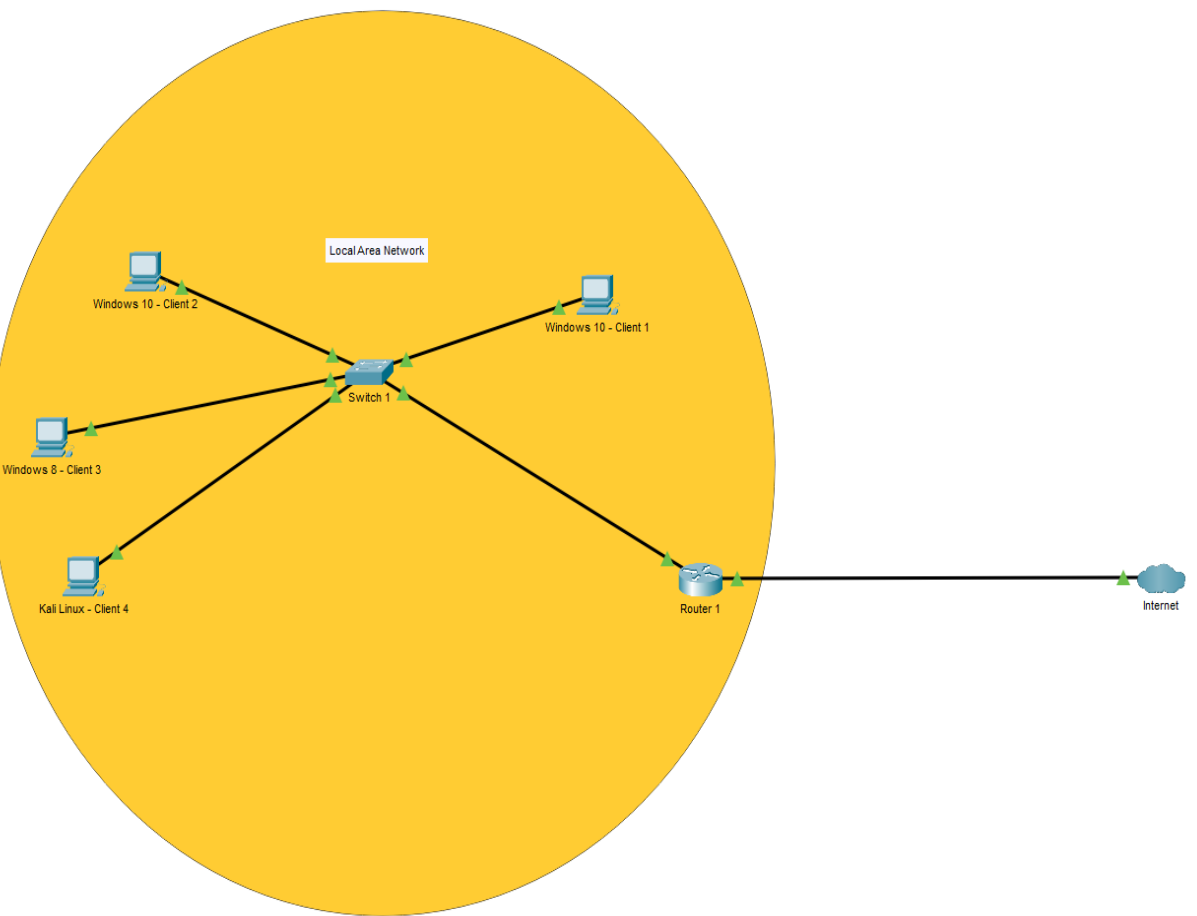
3. Sources

The project made use of sources such as books, journals, articles, conference papers as well as any other sources that related to network security. The sources used for the project helped to gain an understanding into the threats and attacks as well as security methods and standards that protect against them. Some works that were cited in this project include:

- Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions[1]
- Network Security Basics[2]
- A simplified defence mechanism against man-in-the-middle attacks[3]

4. Design and Implementation

Local area network diagram – Star Topology

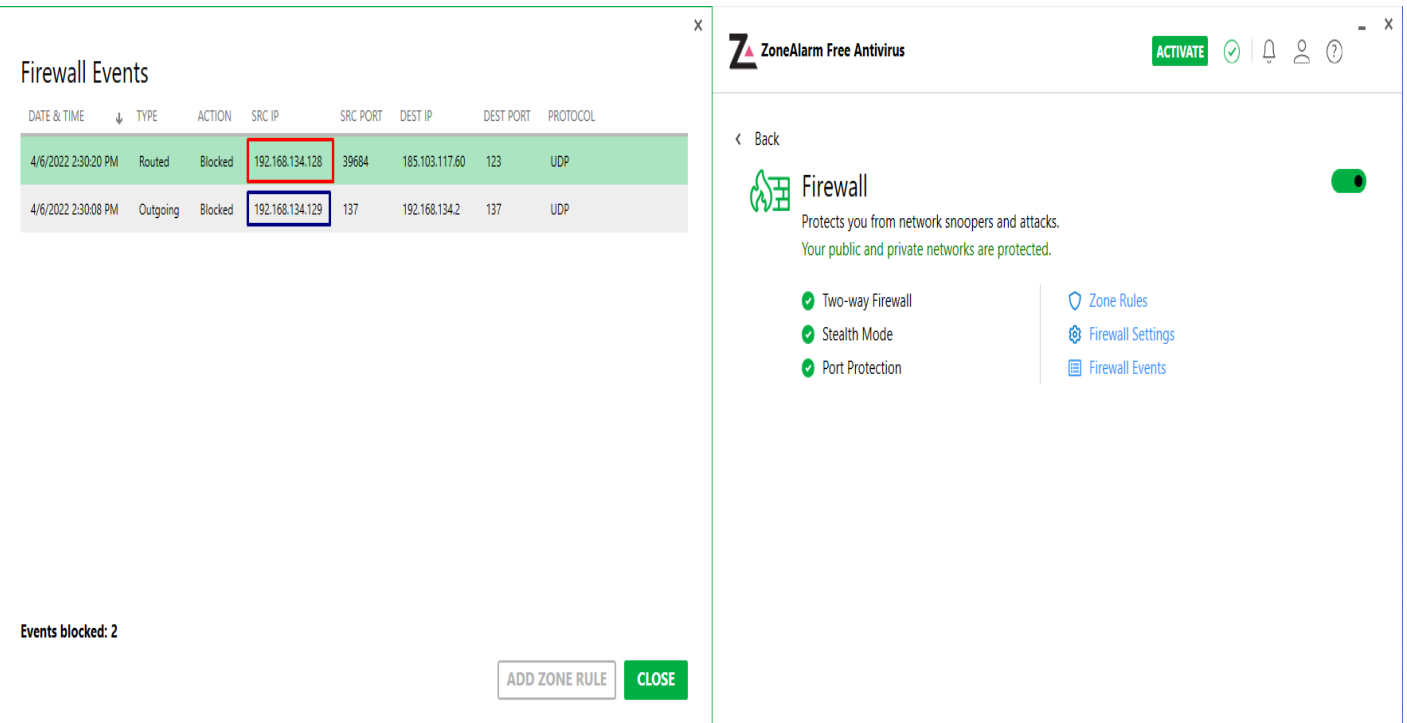


8. Results

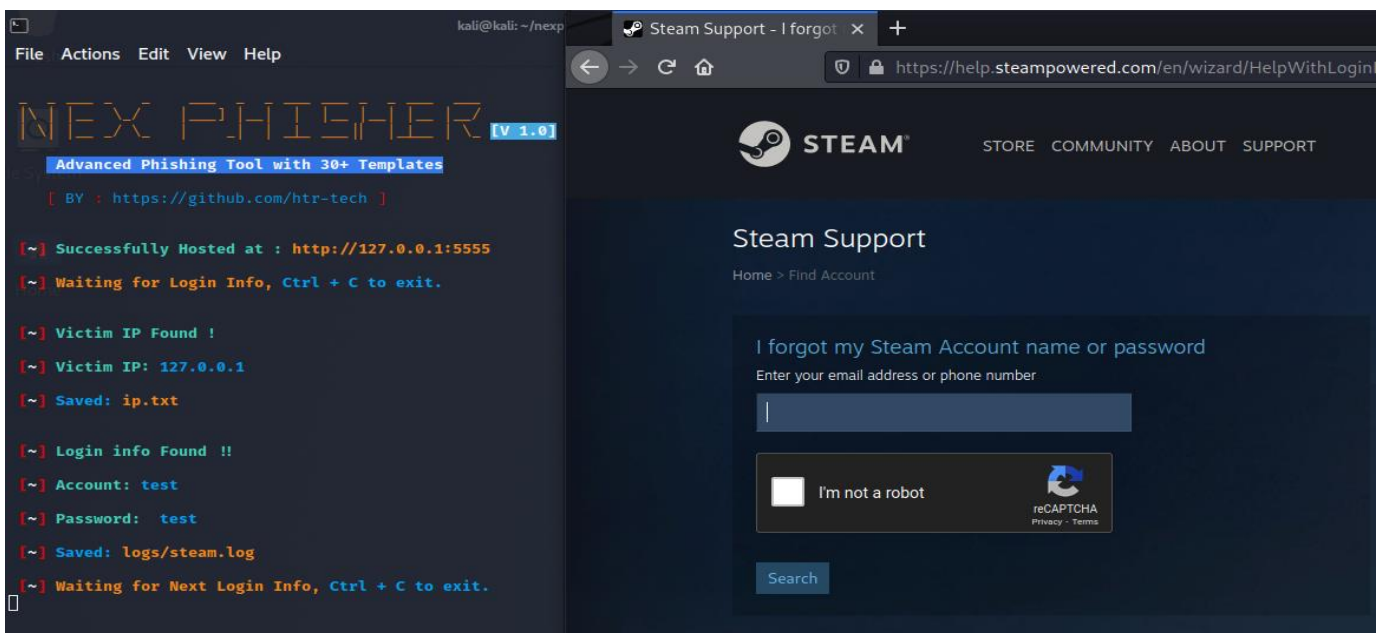
The results of the experiment show that initially, all three of the attacks (Man-in-the-middle, Phishing and SYN flood) were successful. However, after the implementation of the security methods (VPN, Anti-virus software, Firewall software), these attacks failed because the security methods were effective in neutralising the threat.

5. SYN flood - DOS Attack

```
root@kali:~# hping3 -S 192.168.134.128 -a 192.168.134.129 -p 135 --flood
HPING 192.168.134.128 (eth0 192.168.134.128): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```



6. Phishing Attack



Web Protection by Bitdefender

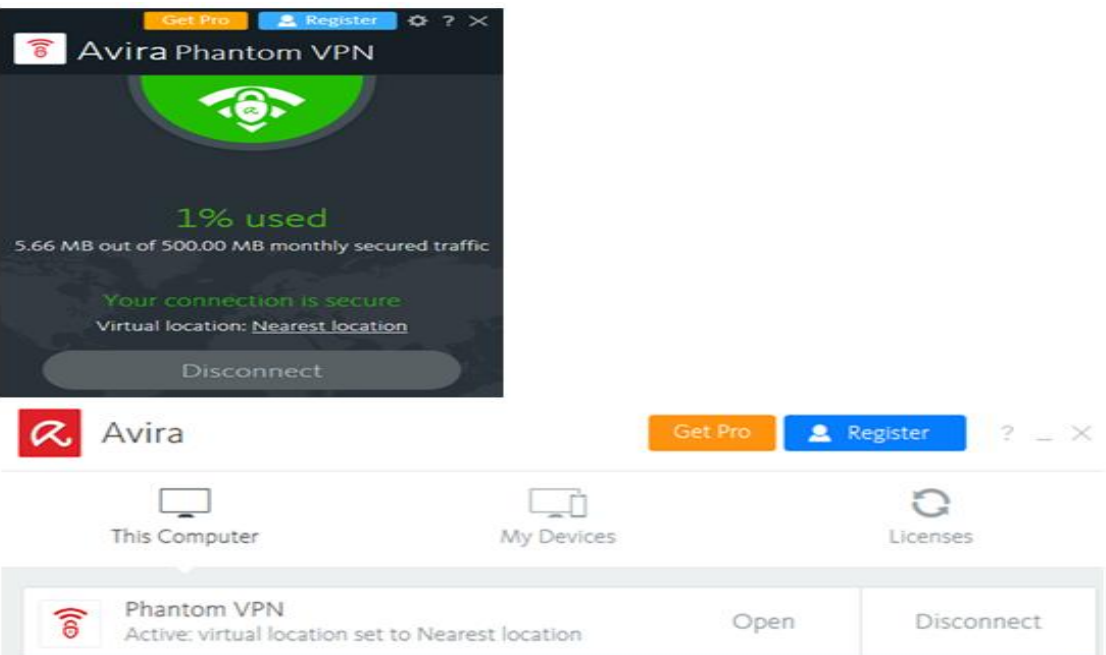
Phishing page blocked for your protection

TAKE ME BACK TO SAFETY

7. Man-in-the-middle Attack

```
root@kali:~# sudo nmap -sT 192.168.134.2/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-07 11:38 EDT
Nmap scan report for 192.168.134.1
Host is up (0.00030s latency).
MAC Address: 00:50:56:C9:00:08 (VMware)
Nmap scan report for 192.168.134.2
Host is up (0.00000s latency).
MAC Address: 00:50:56:C9:00:08 (VMware)
Nmap scan report for 192.168.134.129
Host is up (0.00016s latency).
MAC Address: 00:50:56:FE:C2:83 (VMware)
Nmap scan report for 192.168.134.254
Host is up (0.00075s latency).
MAC Address: 00:50:56:FE:C2:83 (VMware)
Nmap scan report for 192.168.134.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.02 seconds
```

```
root@kali:~# sudo ettercap -T -S -i eth0 -M arp:remote /192.168.134.2// /192.168.134.129//
```



References

1. B. B. Gupta, N. Arachchilage and K. Psannis, “Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions,” Telecommunication Systems, vol. 67, 2018.
2. G. Marin, “Network Security Basics,” Security & Privacy, IEEE, vol. 3, pp. 68-72, 2005.
3. A. Pandey and J. Saini, “A simplified Defense Mechanism Against Man-In-The-Middle Attacks,” International Journal of Engineering Innovation & Research, vol. 1, no. 5, pp. 385-389, 2012.

9. Conclusion

The aim of the project was to analyse security methods of computer networks. This aim was achieved and the project demonstrated the implementation of security methods (VPN, Anti-virus, Firewall) to protect against a man-in-the-middle attack, phishing attack and a SYN flood attack. These implementations were completed using VMware to create a simulated network in order to ensure that the testing environment was safe and isolated. This was to ensure that there were no risks to the main network of the researcher.