A study of security attacks in a SOHO network in GNS3

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

Elliot Barnett (1801749), BSc Computer Networks and Cybersecurity

Introduction

Cyber-attacks are becoming more prevalent on a daily basis, affecting many SoHo (Small office home office) network across the world. With an increasing number of cyber-attacks taken place on networks there is a need to secure these networks to reduce the risks of these attacks becoming successful. This study aims to show and analyse how different cyber-attacks occur on SoHo networks, then to produce recommendations and show how adding more security reduces the risk of cyber-attacks.

Materials

- GNS3
- VMWorkstation
- Windows server 2016, Kali Linux, Windows 7
- Cisco 3725 router
- Ethernet switch

Figure 4

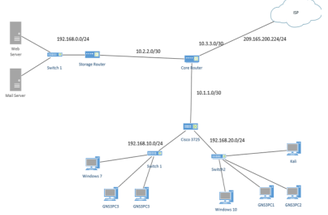
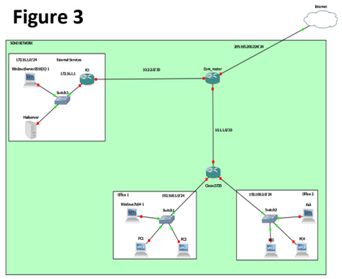


Figure 3



Hypothesis
More vulnerabilities were exploitable on the unsecured network rather than the secured network.
Null Hypothesis
More vulnerabilities were exploitable on the secured network rather than the unsecured network.

Experiment

To determine which hypothesis is correct, there will be an experiment that will be run. This experiment consists of

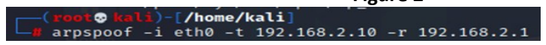
1. Running a Penetration test on the implemented SOHO network
2. Analysis of results of the first pen test to produce recommendations
3. Hardening of the network implementation
4. Penetration test on the secured SOHO network
5. Analysis of results

Penetration test on the SOHO network

The first penetration test found different vulnerabilities within the GNS3 implementation. These vulnerabilities were discovered through the use of running different attacks in the SOHO network. These attacks include, ICMP DDOS attack, SYN Flood attack, ARP Spoofing attack, SQL injection attack.

Figure 1

Figure 2



Hardening of the SOHO network

SYN DDOS Flood	ICMP DDOS	ARP Spoofing	SQL Injection
Increasing backlog size, SYN Cookies, Firewall, Updating OS/firewall, Packet filtering.	Firewall, Disable ICMP packets.	Static ARP entries, ARP inspection, switch security.	PDO technology, CSRF-token.

The table below shows all the recommendations to preventing these attacks from taking place.

Penetration test on the Secured SOHO network

To check whether the countermeasures implemented were successful another penetration test was run on the secured SOHO network. The results to this experiment are located in the results section.

Results

Below is a table showing the overall results of the experiment

Overall Results		
Attack	**Unsecure SOHO network**	**Secured SOHO network**
ICMP DDOS Attack	Successful	Unsuccessful
SYN flood attack	Successful	Unsuccessful
ARP Spoofing attack	Successful	Predicted Unsuccessful
SQL Injection attack	Successful	Unsuccessful

From these results we can determine that the hypothesis was correct of 'more attacks were successful on the unsecured SOHO network rather than on the secured SOHO network'

Conclusions & Future Work

The project as a whole showed that with more security measures in place, there will be a decrease in the risk of an attacker attacking the network. This project has allowed the writer to gain not only more technical skills but other soft skills such as time management, risk analysis.

The future scope for this project would to implement the SOHO network into a real environment and run both penetration test on the both networks to compare the simulated results to the real

Further Information

Email: elliot.barnett@btconnect.com

Table of Figures

Figure 1— ICMP DDOS exploit

Figure 2— ARP spoofing exploit

Figure 3— Implementation

Figure 4— Design

References

[1] Das, Resul & Bitikçi, Burak. (2020). Analysis of Different Types of Network Attacks on the GNS3 Platform. Sakarya University Journal of Computer and Information Sciences. 10.35377/saucis.03.03.721364.

[2]L. A. Mohammed, "On the design of SOHO networks," in *Technological Developments in Networking, Education and Automation*, 2010, pp. 555–560, doi: 10.1007/978-90-481-9151-2_97.

[3] H. Shriram Salunkhe, S. Jadhav, and N. Mumbai Vijay Bhosale, "Analysis and Review of TCP SYN Flood Attack on Network with Its Detection and Performance Metrics." Accessed: Apr. 22, 2021. [Online]. Available: www.ijert.org.

[4] H. A. Mangut, A. Al-Nemrat, C. Benzaïd and A. H. Tawil, "ARP Cache Poisoning Mitigation and Forensics Investigation," 2015 IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 1392-1397, doi: 10.1109/Trustcom.2015.536.