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

Investigating Security of ISP Routers

School of Applied Computing

Introduction

For many years, security has always been the main need when creating a home network. However, recently they have become the primary target for malicious activity, where the attacker manipulates the network to possess data stored or even control the connected devices for their own personal gain. This investigation consists of analysing Internet Service Provider routers that are present in modern day home networks.

Objectives

- To develop an understanding of existing security problems with home networks by analysing the research gathered in the Literature Review.
- To replicate a home network and test the security that is implemented on the ISP routers, to be able to produce results and compare them against own understanding that has been learned from the literature review.
- To critically analyse the results gathered from the experiment to provide recommendations.

Method

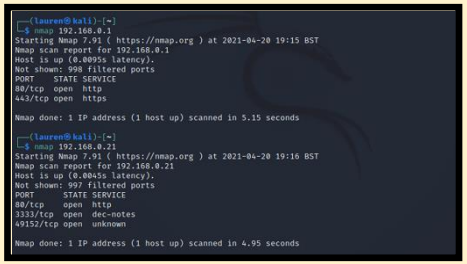
The best method to ensure that research was conducted effectively is by following the standards of quantitative data methods, as it is used to establish facts about a certain area. For this experimental study, the use of two ISP routers were used; there were limitations faced due to the current climate.

Example of References Used

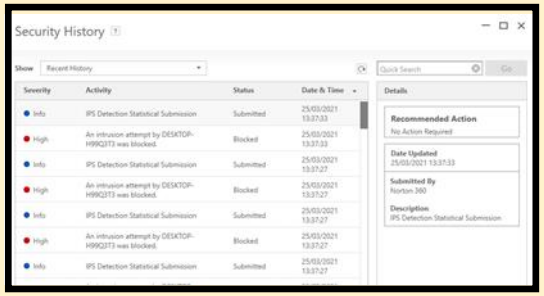
A DDos Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN
N. Tuan, P. Hung, N. Nghia, N. Tho, T. Phan and N. Thanh
Adaptive Security Monitoring for Next-Generation Routers
C. Mansour & D. Chasak
Secure the Internet, One home at a time
K. Xu, F. Wang and X. Jia
Not All ISPs Equally Secure Home Users an Empirical Study Comparing Wi-Fi Security Provided by UK ISPs
Z. Cliffe Schreuders, Adil M. Bhat

Testing

In this experiment the following was carried out, the first step must gather a variety of routers to be able to detect any vulnerabilities that could be exploited by attackers.



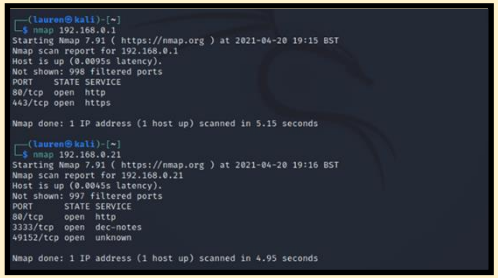
With the use of Routersploit to analyse the network, the experiment made it clear that even connected devices can allow a chance of attacks against network systems, showing that any device that get allowed access on the home network, would have to be configured from their defaults settings.



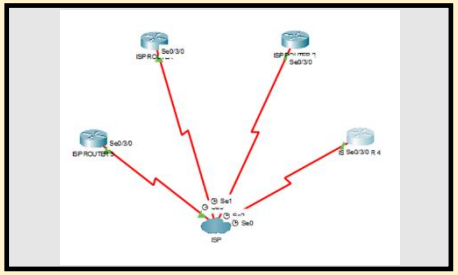
During testing of an ISP router, there became an interference of anti-virus (Norton), blocking attacks on a connected device on the mini network created. Further testing was carried out to compare the benefits of a paid subscription vs a free version.

	Norton 360 (Paid)	AVG (Free)
Smart Scan	✓	✓
Password Manager	✓	X
VPN	✓	X
Dark Web Monitoring	✓	X
Parental Controls	✓	X
Web Protection	✓	✓
Performance Checks	✓	✓
Cloud Back up	✓	X
Reports	✓	X
Anti-Virus Protection	✓	✓

Conclusion



After analysing the results that were gathered in the Testing Phase, ISP routers still sustained forms of vulnerabilities. This study enforced that ISPs must introduce new randomised configurations and make it more apparent to their consumers how fundamental security is on their network.



Further research would be the implementation of Software Defined Networks in home networks. By adapting Machine Learning, ISPs can benefit from the security elements and analysing the traffic patterns of attacks against routers, in turn deploying counter measures.

Contact:
Lauren Carrie Davies
Networking & Cybersecurity BSc
laurencarriesdaviesit@gmail.com