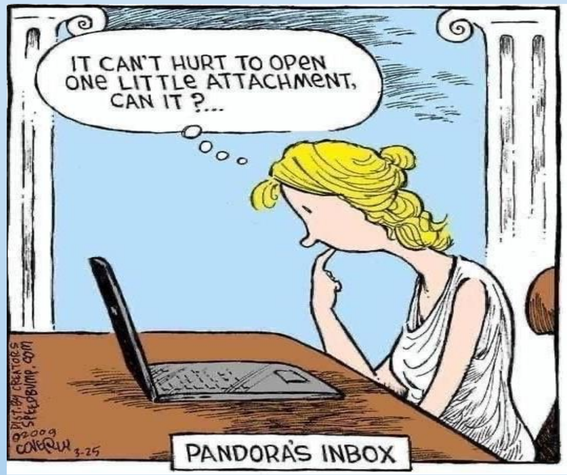
Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Design, Build and Test a Secure Home Network

Nick Alexander
P147734
UWTSD 2021

Introduction

This is a project that researches into current threats facing home networks, it examines a typical modern home in order to identify some of the weaknesses. Experiments demonstrate how common attacks are carried out, as well as methods to prevent these attacks, that would be easy for any home user to follow.

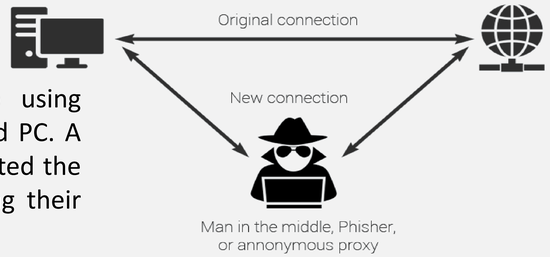


Project Aim

The aim of this project is to set up a typical home network and test its security by using cyberattacks, in order to identify the vulnerabilities, then provide a solution to ensure the home network remains secure.

Design & Implementation

Experiment 1: Man-In-The-Middle Attack



This experiment was setup using EvilGinX2 running on a hosted PC. A fake website secretly intercepted the victim's login details, including their 2FA info.

Experiment 2: Phishing Email

The Link that EvilGinX created was embedded into an email so that a 'victim' would be tempted into clicking the link, and opening the fake website.

Experiment 3: WiFi Attacks

A variety of wireless routers and extenders were hacked – complex passwords took longer, and needed to use 'Hashcat' to decrypt – a program that uses the power of the graphics card to brute-force attack it.

Experiment 4: Shodan Recreation

Shodan is the world's first search engine for Internet-connected devices and is used by hackers to gain access to home & business computer networks.

Experiment 5: Windows Attacks

After gaining access to the network (either by WiFi or Shodan), can then start to attack the Windows computers in the home.

Results

After attacking a typical home network a few different ways, I discovered several points of weakness and ways of avoiding them such as:

- WiFi attacks were less successful against long + complex passwords, and reduced further by using a device such as a 'Firewalla'.

This device plugs into the existing home router and increases the security by adding a VPN, alerting when a new user connects etc

- IoT devices need to be updated and have standard passwords changed, to prevent scripted attacks through Shodan.
- Windows devices are much more secure when regularly updated and running Antivirus software.
- MITM attacks were prevented using a USB token.

USB tokens can stop account takeovers, replace passwords, improve 2FA and mitigate MITM attacks

Conclusion

The research done during the literature review inspired experiments which tested home networks, home computers and their users to see how they could be affected by these threats. 4 experiments were chosen which successfully demonstrated weaknesses, and also methods were tested and proven to mitigate these threats.