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

Building a Secure Home Network

WILLIAM THOMAS

INTRODUCTION

The purpose of the research project is to build a more secure home network The poster will have information on what aims and objectives I aim to complete by the end of the project, The methods that will be used to reach the objectives and what risks might be involved throughout the process.

AIMS

I. To exploit the current state of a regular home broadband users router (To show that just by buying the product and using it does not mean the security is up to date or at least working).

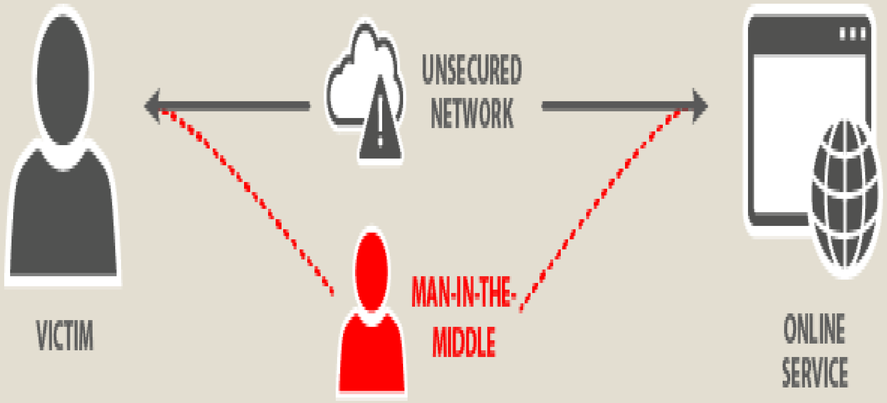
II. To create a more secure home network from the point of inside the home and outside. This includes WIFI snoopers, IP logging (Public Address Shown) or even DHCP attacks inside the network.

OBJECTIVES

I. To create three simulation networks which will show basic network attacking methods from inside and outside of the network and If the network can withhold the attack.

II. To configure the three simulation networks differently. Sim1 will be setup as a regular broadband router with regular security. Sim2 uses free security software such as free VPN's, Sim3 uses paid protection.

[1]



[2]

METHODS

I. Packet tracer – To create the three network simulations on which each of them will be tested on level of security. [3]

II. Questionnaire – To gather information on the amount of people who have just installed the broadband router and didn't add extra security (Free security or paid security).

RISKS

I. The Questionnaire must add extra information to make sure that all users with and without networking knowledge can understand the questions clearly to answer correctly.

II. The Packet Tracer software must support the necessary protocols on which it can act as a normal everyday router. The software must also support methods on which it can be used to exploit vulnerabilities inside and outside of the network.

REFERENCES

1. http://www.pngall.com/wp-content/uploads/2016/07/Networking-PNG-Image.png

2. https://hypersecu.com/images/blog/MITM-attack-diagram-01.png

3. https://www.netacad.com/courses/packet-tracer-download/