Olivia Gallucci
gallucci@protonmail.com
She/Her/Hers

Effectiveness of Threat Mitigation in Layers of the Open Systems Interconnection Model

6 January 2020

COURSE DESCRIPTION

Introduction to Routing and Switching (NSSA-241) provides an introduction to wired network infrastructures, topologies, technologies, and the protocols required for effective end-to-end communication. Basic security concepts for TCP/IP based technologies are introduced. Networking layers 1, 2, and 3 are examined in-depth using the International Standards Organization's Open Systems Interconnection and TCP/IP models as reference. Course topics focus on the TCP/IP protocol suite, the Ethernet LAN protocol, switching technology, and routed and routing protocols common in TCP/IP networks. The lab assignments mirror the lecture content, providing an experiential learning component for each topic covered. The lecture instructor and advisor for this project is Professor Sylvia Perez-Hardy.

BACKGROUND

The Open Systems Interconnection model (OSI model) is a conceptual model that illustrates layers of a telecommunication or computing system. The OSI model consists of seven layers: physical, data link, network, transport, session, presentation, and application. The first OSI layer is the physical layer, while the last OSI layer is the application layer. Each layer has security issues and mitigations. The OSI model is relevant today because it illustrates how data is processed and transported over the internet.

OVERVIEW

In this honors option, I will use modules in NSSA-241 to learn about the OSI model. Under the guidance of Professor Sylvia Perez-Hardy, I will critically examine past networking research that evaluates the effectiveness of security mitigations for each layer of the OSI model. I will create presentation slides and a script for each layer of the module. This task will involve extensive

reading of published research, journal articles, and press articles on security threats and mitigations.

The development of this research project will enhance my understanding of networking, and assist in my hands-on application of vulnerability mitigation. This complex study of security mitigation will explore historical threats, and enable me to learn from historical failures. After the completion of this project, I will possess a better understanding of cybersecurity and networking, which will improve my abilities to evaluate cyber risk.

DELIVERABLES

The course is divided up into ten to twelve modules. Each module introduces a layer of the OSI model. During each module, I will investigate vulnerabilities, and mitigations for those vulnerabilities. I will document my research, and prepare presentation slides on my research. In addition, I will make a script for each slide. Once the module is completed, I will submit my slides and script to a private folder on myCourses. Professor Sylvia Perez-Hardy will review my submission and suggest changes by the following week.

Professor Sylvia Perez-Hardy and I will address my progress for each week. Professor Sylvia Perez-Hardy will oversee my research and critique my slide submissions.

I will present my research to the class on May 3rd, 2021. I will also present my research in RITSEC, and/or WiCyS.