Student Name: London Hester-Williams

Project Name: Court 17 Audit: Router Devices, Physical Controls, Threat Mode

Faculty Sponsor: D.C. Grant

Abstract

The objective of this project is to show the Court 17 staff another approach on finding out how the building is insecure, discovering the amount of router devices being used, and what controls can be put into place to make the building more secure. This project allowed me to utilize iStumbler similar to NetStumbler to perform Wi-Fi device scans to gather a device count of the building and allow the Court 17 staff to know that Xfinity routers are online. The physical control testing allowed me to confirm or deny the functionality of the Radio Frequency Identification (RFID) access control that exists at some entry points of the building, ensure that the controls were in place for locked doors, and the emergency doors were also properly set. The security of the building was determined based on the control testing inside the building, on all access points, elevators, ground floor doors, and garage entrances and exits. I utilized the Microsoft Threat Modeling Tool and found vulnerabilities on each floor under each of these categories: Spoofing, Tampering, Repudiation, Integrity, Denial of Service, and Elevation of Privilege (STRIDE). I used to show the Threat Model as a non-technical visual of the building for the staff along with STRIDE to express the weaknesses and vulnerabilities throughout the building with possible approaches on improving or fixing the problems.