**Project Title:** Proper Vulnerability Detection for Legacy Systems

**Situation:**

How to maintain companies’ valuable data protected and secure from attackers, while depending on outdated security infrastructure?

**Problem:**

Recently in the news a major a consumer credit reporting agency Equifax was breached exposing financial information for 800 million Americans. The vulnerability that was exposes was the result of an Apache application not being remediated by the Equifax’s Informational Assurance (IA) security team. It is very hard for a third-party company to provide an immediate Zero-Day vulnerability update to any system; nevertheless, the Equifax’s IA security team is reasonable on finding and provide systems updates to their outdated infrastructure.

**Motivation:**

Performing a Nessus vulnerability scan on legacy operating system (OS) will reduce the risk for exposed vulnerabilities. Once vulnerabilities are detected, the IA security team is responsible for providing remediation or fix for the vulnerabilities that were found from the IA system scan.

**Purpose Statement (Goals):**

The goal for this project is to demonstrate the efficiency for proper vulnerability detection and patching within a legacy system.

**Methods/Approach:**

* Provide initial scan for Windows Server 2008 and Ubuntu OS
* Provide a snapshot displaying ‘Critical’ vulnerabilities generated by Security Center (scanning tool)
* Generate ‘.nessus’ file extracted by the Security Center
* Use Vulnerator tool to generating a Plan of Actions and Milestones (POA&M) excel document
* Provide solution/remediation on ‘Critical’ vulnerabilities generated
* Application of ‘Critical’ remediation or fixes which is considered the Engineering phase
* Produce a post-vulnerability scan on the affected OS demonstrating

**Resources:**

For the purpose of this project software tools and virtual machines (VM) with versions will be listed below:

* Nessus: version 6.10.2
* Security Center version 5.4.5
* VMware® Workstation 12 Pro version 12.5.0 build-4352439
* ACAS Server (VM)
  + Ubuntu Server version 16.0.4 VM which is hosting Nessus and Security Center tools
* Ubuntu Server version 16.0.4 (VM)
* Windows Server 2008 (VM)
* Vulnerator version 6.1.9

**Milestones/Schedule:**

Below is the propose schedule displaying both base and active time schedule:

