# Overview

Lab 3 – Network Security Monitoring

In this lab we will practice configuring a tool to monitor the current status of the components of our network in regards to potential security concerns that can be observed, and what is visible of the device on the network. We will using the community version of an enterprise class tool that can be used for security monitoring and tracking remediation, the Greenbone Vulnerability Manager (formerly OpenVAS). Using the Kali-Greenbone custom template provided, you will use the GVM that has been pre-installed for you to explore a good toolkit for a “portable” assessment platform.

This lab must be completed online, with all work being done and written as it is done into Word 365 Online. Use the Lab Book Template and upload to your Word 365 Online and begin working there. You must also share an edit link from Word 365 Online in the comments of the assignment document submission (export a PDF and upload it to eConestoga). Not following these instructions and showing ongoing work through the change revisions tracked in the online Word mean a score of zero on the lab.

# Preparation

* Familiarize yourself with class work done introducing the use of GVM, and the installation of Kali Linux (latest)
* Work is to be done on vSphere
* The Kali-Greenbone template provided uses DHCP, so ensure you have DHCP enabled on your pfSense in order for it to connect to the Internet

# Deliverables

* Install the Kali-Greenbone template to a machine named “8590-id1234-K01”, where id is your initials and 1234 is the last 4 numbers of your student ID
* Demonstrate a vulnerability scan using GVM inside your pfSense network, scanning the internal IP of your pfSense device, as well as a Windows 10 desktop. Scan both at the same time by scanning your entire network range using CIDR notation. Show a second scan without the Windows 10 firewall running, scanning just the one host.

## 

## Screenshots

* Appropriate screenshots that demonstrate the above was done and all is working

## Reflection

* 1. Record any of your own observations, solutions, or comments about the work you did. What problems did you have, how did you work through them, what was not clear, what did you take away that you value? Explain your configuration choices. This is mandatory. You may refer back to your observations in completing this task.
  2. What are the uses of GVM or similar tools within an organization?
  3. Discuss the results of your scans. What do you know about your network and these hosts based on the scans? What have your learned/observed?

CAS – Network Components and Monitoring

Lab 3 –Network Security Monitoring |1