Lab 4 – Network IDS and IPS Tools

# Overview

In this lab we will practice configuring a basic IDS/IPS using Suricata with a virtual pfSense firewall in your vSphere lab environment.

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). Requirements and importance of this are the same as Labs 1 and 2.

# Preparation

# Familiarize yourself with class work done introducing the use of the vSphere lab environment at Conestoga College; this must be done on vSphere – not on a local VMWare Workstation install

# Refer to the posted list of your assigned 10.x.x.x network

# Deliverables

* Install a pfSense firewall in your vSphere environment with the following specifications and functions:
  + An interface on your \_01 network as the WAN; pick an appropriate IP address from the subnet you were assigned
  + An interface on the \_02 network as your LAN; assign it an appropriate address on a /24 sized network from the RFC 1918 private address space that starts with “172”.
  + Configure your LAN and pfSense device to provide DHCP to devices on your LAN; ensure they get a correct IP address, default gateway, and use your pfSense device for DNS
  + Configure pfSense to run a DNS server on its WAN IP - DNS Forwarder to 8.8.8.8
* Deploy a Windows 10 Desktop to your \_02 network, name the machine “8590-id1234-desktop01”, for example, 8590-my1234-desktop01. Use your initials plus the last 4 digits of your student ID in the middle as the identifier. Ensure these names are visible in screenshots.
  1. Demonstrate it is working and using the pfSense device as its default router and DNS server
* Install the Suricata package on your pfSense device and show that it is enabled/configured
* Install the Snort package (after turning off Suricata) and show that it is enabled/configured
* Independently, working on your own, asking your faculty for help if needed, use a method to demonstrate that Suricata is detecting traffic patterns and alerting to potential issues. Hint: By default PfSense 2.5 does not enable rulesets by default; after turning on the IDS package you will need to enable the groups of rules that do the filtering.
* Show the configuration of PFBlockerNG-devel, and then test
  1. blocking outbound traffic based on geo location
  2. test any other filter ruleset you have enabled in PFBlocker
* 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.