Lab 7 – Fundamental Windows Security

Overview

In this lab we will practice implementing fundamental practices in Windows security on a Windows 10 desktop behind one of our pfSense firewalls in the vSphere 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 sharean 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 vSphere and pfSense
- Have an existing pfSense firewall up and running providing DNS, DHCP, and internet access to an internal network

Deliverables

- Configure a Windows 10 desktop on your internal network (use the template) that has the following characteristics
    - Actual hostname (system name) in Windows set to match the name given for the machine in vSphere
    - Windows 10 machine to get all settings using DHCP, and uses DNS running on your pfSense machine
    - Ensure all patches (Windows updates) are applied and all dependencies
    - Ensure antivirus/malware signatures are up to date
    - Ensure that folder protection is enabled such that this system is less susceptible to damage from cryptographic or file damaging virus/malware payloads
        - Create a directory called C:\Code and ensure it is also protected
    - Configure the firewall to allow for pings (ICMP Echo Requests) from other machines also on a network designated as a “private” network

Screenshots

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

Reflection

- Record any of your own observations, solutions, or comments about the work you did. What problems did you have, what was not clear, what did you take away that you value? Explain yourconfiguration choices. This is mandatory. You may refer back to your observations section of your lab book in answering this question.
- Look into another practice that can be done that will also limit the damage that can be done by cryptographic and file damaging viruses – explain in your own words and share any citations if involved.