Lab 8 – Fundamental Linux Security

Overview

This lab will review fundamental practices for security on Linux-based machines. You may do this lab on either a CentOS 8 or a Ubuntu 18.x or 20.x virtual machine.

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 previous labs.

Preparation

- Familiarity with the 8580-vSphere environment and assignment network addresses.

Deliverables

- On a new or existing Linux machine, demonstrate the appropriate method to patch your chosen Linux machine to see if it is up to date.
- How do you use iptables to configure the rules for the Linux Firewall?

Screenshots

- Appropriate screenshots that show the work was completed.

Reflection

- What are the considerations in not rebooting after updating? Why would or wouldn't you, and what could be the impact? Does it matter more or less if a kernel update is done?
- What happens if you make a firewall update, but do not reload the firewall?