

**LAB**

**LINUX SYSTEM ADMINISTRATION**

**Copyright © (2022-2023) All Rights Reserved**

**Dr. Matthew Kisow**

VERSION 3

20-JUN-2023

**LAB:** LAB22-01

**OBJECTIVE**: The objective of this lab is to learn how to use the IPTables firewall to block and unblock traffic.

**INSTRUCTIONS**: These labs will test your ability to actively research how to perform a required action on a Linux operating system. All questions asked (below) should be included in a lab report. This lab report should be written in Microsoft Word and include a numbered list corresponding to the task (below). This list must include a clear screenshot of the command and its output. Please follow the instructions for submitting this assignment on Blackboard.

* You should be logged in as ***labuser1*** with the password ‘P@$$w0rd’
* You must be in the /labs/CH22 folder to complete this lab.

**IPTABLES**

1. Open a terminal window (cmd prompt – Windows) or (terminal – macOS) and send a continuous ping to your Linux server’s IP address.
2. From the Linux server, add an ***iptables*** rule to drop all ICMP packets[[1]](#footnote-2).
   1. What happened to the ping running in the other window?
3. Remove this rule from iptables[[2]](#footnote-3).

**EXTRA CREDIT**

1. From the Linux server, add an ***iptables*** rule to drop SSH communication.

1. You will have to use the ***sudo*** command for these steps. [↑](#footnote-ref-2)
2. You will have to use the ***sudo*** command for these steps. [↑](#footnote-ref-3)