**CSCI 3500 – Fall 2025 Lab Template**

**Ethan Walton**

**27 August 2025**

**Instructor: Ms. Emond**

**Introduction to Kali Linux**

## **Lab Purpose (In Your Own Words)**

This lab is intended to teach students the basics of Kali Linux software and commands.

## **Tools & Resources Required**

* VMWare Workstation
* Kali Linux prebuilt machine

## **Lab Procedures (Minimum of 1 Page)**

* Install Kali Linux on virtual machine
* Run and log into Kali Linux
* Open the terminal and run Wireshark
* Close Wireshark and run ifconfig to find the local IP
* Nmap the local ip with various options
* Find and run Metasploit framework
* Run host and nmap commands to locate and select machines
* View the exploits for the host machines and search through them
* I was scared so I didn’t run an exploit, but exploits were available through “show exploits” and “run exploit”



## **Observations (Minimum of ½ a Page)**

In this lab, I learned how to install and use Kali Linux’s various tools. I noticed Wireshark detects network activity. After continuing to mess around with it, after pinging different IPs, I noticed it flagged all the pings and can create documents of them. I also messed around with Metasploit, a software used to exploit and test servers and networks. I noticed it has a lot of prebuilt exploits, such as fizzers and scanners. However, I was too scared to run them. A company based on network security, or any company that has someone trained to use Kali and its associated software, will benefit from it. The software is easy to use, and there is a ton of documentation online.