Lab 06 – Vulnerability Analysis

# Overview

We’ll take scanning to a deeper level this week and look at what is running on the ports. This time you’ll be dropped into a Kali machine that is connected to a network that you haven’t seen before and have no OSINT for. Your rules of engagement for this operation do not allow you to scan anything outside of the target network. Pay close attention to the subnet mask of the network and do not operate outside of the rules of engagement. If you would like to use nmap to complement the below scripts you may also do that.

**Target Network: 10.10.15.0/24**

DO NOT EXPLOIT OR MODIFY ANY OF THE TARGETS

# Task 1

Configure and run Openvas vulnerability scanner on the target network

# Task 2

Find and run at least 2 nmap NSE scripts against likely targets of compromise.

# Task 3

Once you have run the previous scans, run Nikto and report the results

Summarize your results and present the most significant findings with OS’s, ports open, and vulnerabilities.