Network Enumeration

**Lesson Description:** In this learning module, the teachers will learn what it means to enumerate a wireless network. The teachers will use the security testing features of the Kali (Linux based) O/S on the Raspberry Pi to enumerate a wireless network.

**Prerequisite Knowledge:** Basic understanding of the Raspberry Pi hardware and operating system.

**Length of Completion**: 60 minutes

**Level of Instruction:** High School or Middle school introductory level.

**Applicable First Principles &/or Concepts:**

**GenCyber First Principles**

Domain Separation Abstraction

Process Isolation Data Hiding

Resource Encapsulation Layering

Modularity Simplicity

Least Privilege Minimization

**GenCyber Cybersecurity Concepts**

Defense in Depth Availability

Confidentiality **Think Like an Adversary**

Integrity Keep it Simple

**Resources that are Needed:** A new Raspberry Pi kit, external monitor (HDMI input), external keyboard, and external mouse (USB connectors), and a webcam. A PC computer is also required. Multiple portable devices.

**Accommodations Needed:** May need someone to read items that are on the screens if there is a visually impaired participant.

# learning outcomes

LEsson learning oUTCOMES

* Define network enumeration
* Explain the importance of network enumeration
* Demonstrate how to enumerate a network
* Explain the basic NMAP command and common switches
  + Nmap 192.168.1.10 -p0-65535
  + Nmap -sV 192.168.1.10

# Lesson Details

**Interconnection:** Lays out foundations of staying safe on the computer which will be built upon further in lesson

**Assessment:** Post exercise discussions, Observations, Walk around.

**Extension Activities:** None

**Differentiated Learning Opportunities:** None

# lesson 2.5

**Lesson 2.5 Details:**

**Warm Up:** Instructor can talk about different movie scenes that involve network enumeration. If possible, instructor can show a few clips of network enumeration in movies.

**Lesson:**

There will be several servers available with MetaSploitable running. Teachers will connect their Pi to a switch and set the IP address on the Pi. Teachers will then run nmap scans against the MetaSploitable server IP address.

10 minutes for warm up, 20 minutes for lecture and slides, 5 minutes to demonstrate how to enumerate a network, 15 minutes for exercise, 10 minutes to troubleshoot exercise and questions. The following topics will be discussed:

1. Network Enumeration

2. Kali

3. NMAP

a. Basic commands

b. Basic switches to use with commands

4. MetaSploitable

a. Premade system with exploits

b. Safety when using MetaSploitable

Acknowledgement: Lesson developed by Mike Kwiatkowski & Roger Spears.