Nmap Basics

Summary

Nmap is free, open-source software used by most technicians responsible for network functionality or network security. Nmap can be used for network discovery, security auditing, service mapping and more. A basic understanding and the ability to use this versatile tool is very important to anyone seeking to learn more about cybersecurity.

Learning Outcomes

- Describe TCP/IP Network Communications.
- Discuss Nmap Host Discovery.
- Discuss Nmap Port Mapping.
- Discuss Using Nmap to Identify Target Service and Operating System Data.
- Use Nmap to Perform Network Mapping.

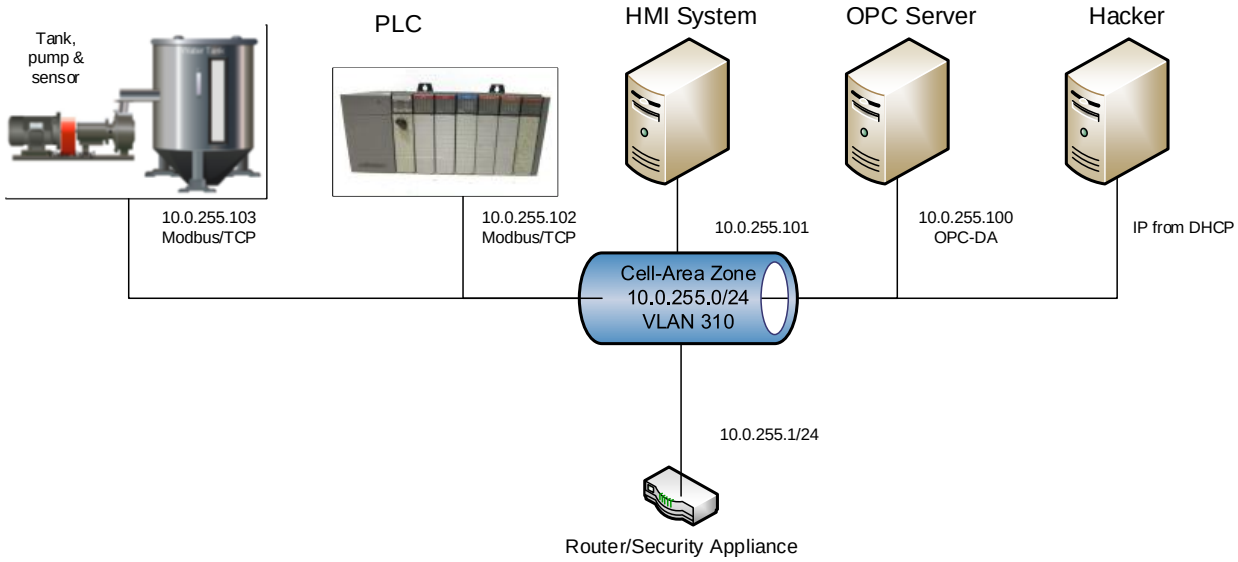
Systems

- Kali Linux – Hacker
    - Username: student; Password: Password01
- Industrial Control System
    - Windows XP – OPC Server
        - Username: student; Password: Password01
    - Windows XP – HMI
        - Username: student; Password: Password01
    - PLC/Pump/Sensors
        - Username: root; Password: Password01
- pfSense – Router/Firewall
    - Username: admin; Password: Password01

General Lab

In this lab students will use nmap to perform basic and advanced network scanning. Multiple methods for accessing common built-in nmap resources will be demonstrated. Students will learn to modify nmap's behavior using switches. Students will learn to use caution when using nmap by observing how it can disrupt system functionality.

Setup and Deploy



For Further Information

National Institute of Standards and Technology (NIST) (May 2015). *Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

Nmap Series. HackerSploit. January 11, 2021. Video, https://www.youtube.com/playlist?list=PLBf0hzazHTGM8V_3OEKhvCM9Xah3qDdIx.

The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.COM LLC. 2022. https://nmap.org/book/.