Metasploit Basics

Summary

Metasploit is a powerful, free, and open-source penetration testing tool used by both hackers and security professionals to probe and exploit security weaknesses. Because of this it is important to understand the basics of Metasploit and be able to use it to test for security vulnerabilities. In this scenario, students will learn basic Metasploit concepts and usage.

Learning Outcomes

- Explain Metasploit's Purpose.
- Define Metasploit Terminology.
- Discuss Basic Metasploit Usage.
- Demonstrate Basic Metasploit Usage.

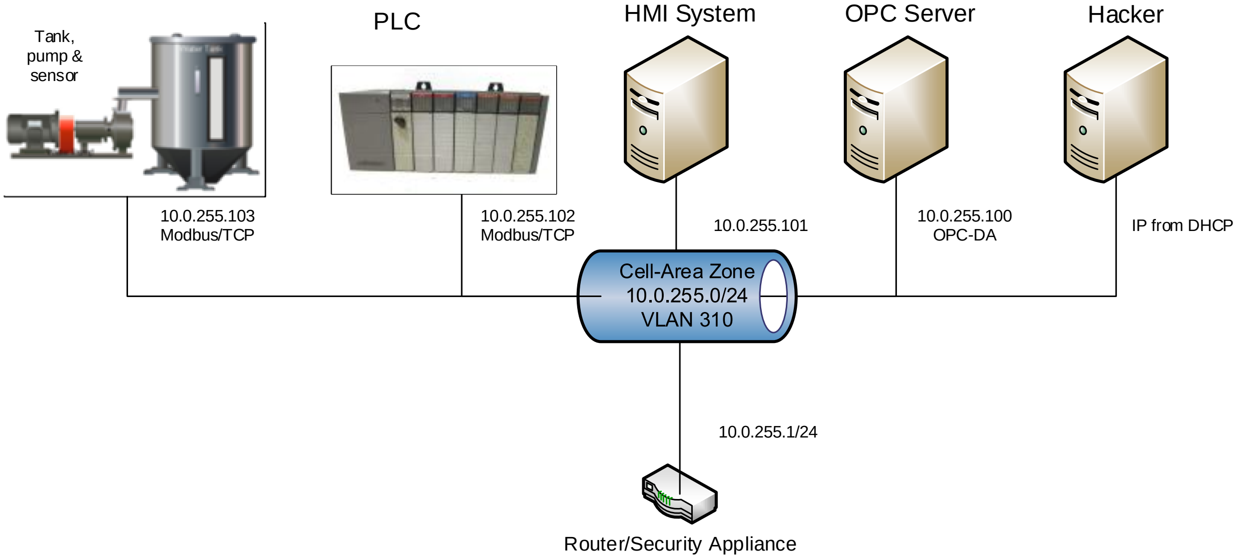
Systems

- 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 Metasploit to create a network map, confirm a system vulnerability then use that vulnerability to exploit a system. While doing this, students will learn to perform basic module and payload searches in Metasploit and how to use the built-in help functionality. Students will also learn how to configure and use a database to store Metasploit data.

Setup and Deploy



For Further Information

Metasploit Unleashed | Offensive Security (2019). OffSec. Accessed 2019. https://www.offensive-security.com/metasploit-unleashed/.