System Hardening Basics

Summary

Even the most secure operating system or software can be hacked if poor security practices are followed. Conversely, even old, inherently insecure software can be made much more secure if basic security hardening principles are applied. A basic understanding of system hardening will help mitigate many security risks.

Learning Outcomes

- Examine Good Password Hygiene.
- Demonstrate the Importance of Applying Software Patches.
- Disable Unnecessary System Services.
- Discuss and Enable Local System Security Software.

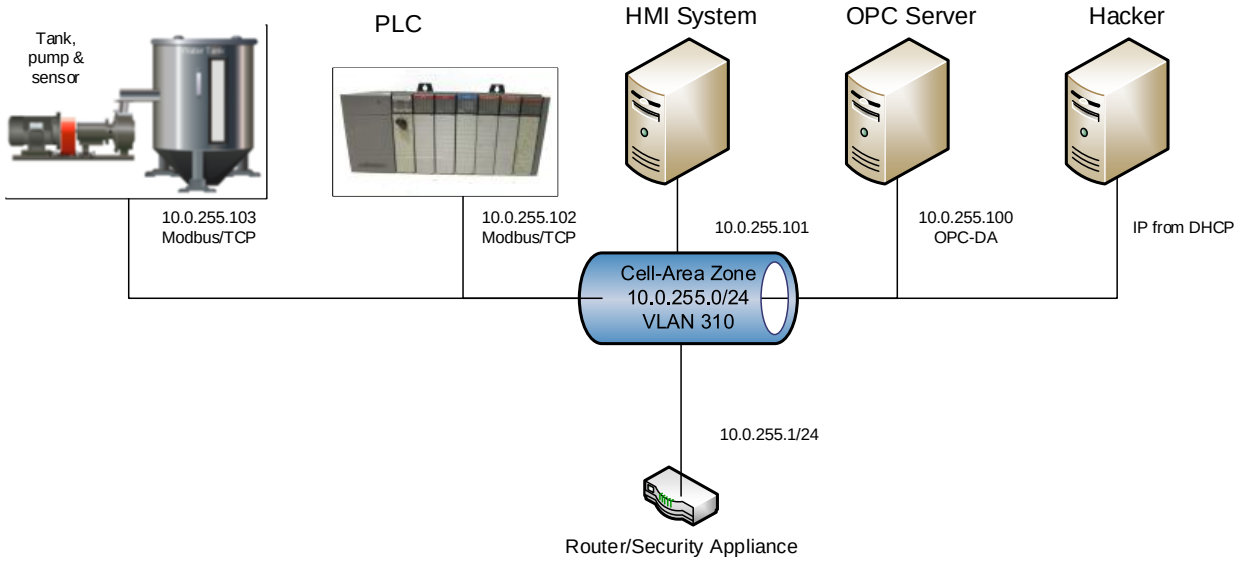
Systems

- 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 start work with a network where basic security hardening principles have not been followed. Specifically, they will demonstrate how effectively poor password hygiene, unpatched software, unnecessary services enabled, and disabled system security software can be exploited. Students will then follow system hardening best practices and observe how the network and its hosts are much more secure as a result.

Setup and Deploy



For Further Information

National Institute of Standards and Technology (NIST) (Oct 2023). *Digital Identity Guidelines, NIST Special Publication 800-63 Revision 3*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

National Institute of Standards and Technology (NIST) (Apr 2022). *Guide to Enterprise Patch Management Planning, NIST Special Publication 800-40 Revision 4*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf.

National Institute of Standards and Technology (NIST) (Jul 2008). *Guide to General Server Security, NIST Special Publication 800-123*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf.

National Institute of Standards and Technology (NIST) (Sep 2020). *Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.