Using IDS/IPS to Identify or Prevent Industrial Network Attacks

Summary

Monitoring network traffic flowing to and from industrial devices is one method of detecting and preventing hacking attempts on those devices. This monitoring can be automated using Intrusion Detection/Prevention Systems (IDS/IPS). In this training scenario students will learn the difference between different types of monitoring software and when each type should be implemented. Students will configure an IDS/IPS and see firsthand how these can be used in an industrial environment.

Learning Outcomes

- Explain the difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS).
- Discuss the usage cases that would make the use of an IDS more appropriate than the use of an IPS.
- Describe how host and network-based IDS/IPS differ in functionality.
- Describe how signature based and anomaly-based IDS/IPS differ in functionality.
- Describe the difference between a false negative and a false positive.
- Demonstrate how an IDS/IPS can be used to protect industrial devices such as PLCs or OPC servers.

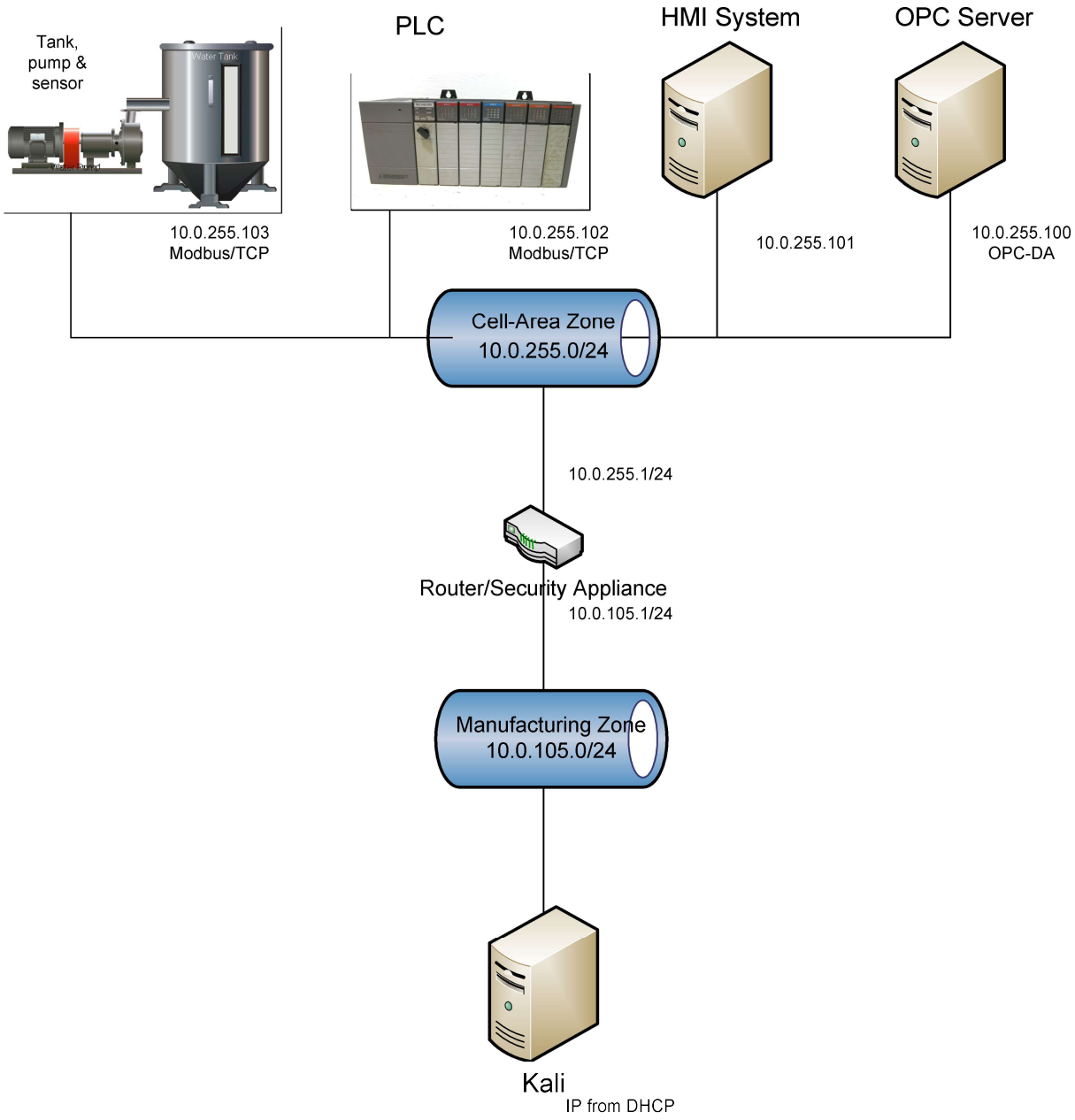
Systems

- 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

Students will start up and perform basic system configuration on an Intrusion Detection System (IDS). Students will use common security tools to attack systems on an Industrial Control System network and view the alerts captured on the IDS. Students will then modify the IDS so that it acts as an Intrusion Prevention System (IPS). They will perform the attack on the ICS an second time and observe that, unlike an IDS, the IPS prevents the attack from succeeding.

Setup and Deploy



For Further Information

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (September 2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. Retrieved from https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

National Institute of Standards and Technology (NIST) (July 2012). *Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94 Revision 1 Draft*. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf.

National Institute of Standards and Technology (NIST) (April 2013). *Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

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.