Packet Capture Using Wireshark

Summary

Wireshark is a powerful, free, and open-source program used by security professionals to monitor and inspect network traffic. Because of this it is important to understand the basics of Wireshark use and be able to filter out unnecessary data. The ability to use Wireshark to decode network traffic streams is also a valuable skill. Security professionals should understand how the default behavior of network devices restricts the monitoring of network traffic.

Learning Outcomes

- Discuss the purpose of packet capture software such as Wireshark.
- Use Wireshark to capture network data.
- Explain the different ways Wireshark can present and format captured data.
- Control the display and capture of network data using filters.
- Discuss various ways networks and network devices can be manipulated to allow the capture of network traffic.

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

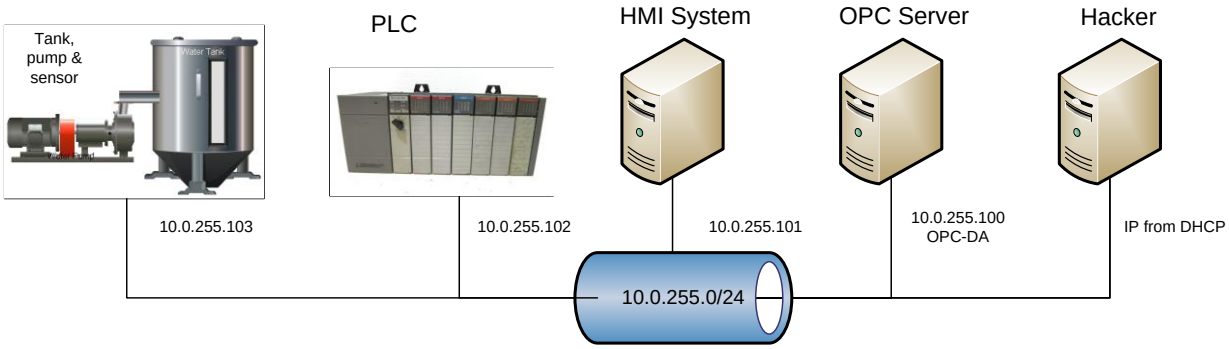
General Lab

Approximate time to complete – 1 Hour

Students will generate typical network traffic and use Wireshark to capture that network data. Students will learn the difference between Wireshark's packet list, packet details and packet bytes data display panels. They will implement filters to limit the amount of data shown which will enable easier analysis. Students will use Wireshark's protocol follow feature to decode and inspect captured network data. When doing the lab students will use Wireshark to observe the security implications of using either encrypted or unencrypted network traffic.

Setup and Deploy

Basic System and Network Diagram



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.

Wireshark – Go Deep. Wireshark website. https://www.wireshark.org/. Accessed July 13, 2021.

Wireshark. HackerSploit. May 16, 2022. Video, https://www.youtube.com/playlist?list=PLBf0hzazHTGPgyxeEj_9LBHiqjtNEjsgt.

References

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (April 2017). *ICS Advisory (ICSA-17-101-01) Schneider Electric Modicon Modbus Protocol*. Retrieved from https://www.us-cert.gov/ics/advisories/ICSA-17-101-01.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (February 2019). *ICS Advisory (ICSA-13-011-03) Rockwell Automation ControlLogix PLC Vulnerabilities*. Retrieved from https://www.us-cert.gov/ics/advisories/ICSA-13-011-03.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (April 2020). *ICS Advisory (ICSA-19-283-02) Siemens PROFINET Devices (Update E)*. Retrieved from https://www.us-cert.gov/ics/advisories/ICSA-13-011-03.

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.