Nmap

NIST Standards and other best practices.

NIST 800-115 – 4 – Target Identification and Analysis

The main topic covered by this scenario is network mapping which allows an administrator or penetration tester to identify and analysis systems on a network.

NIST 800-82r3 – E.2.3. – Active Scanning

When doing the lab, the students are intentionally instructed to perform a scan which will cause the PLC in the industrial control system to crash. This allows them to verify that caution should be used when using Nmap in a production environment.