The Case for Penetration Testing in ICS Environments

Krish Sridhar, P.E, GSEC, MBA
Sr. Business Manager – Industrial Cybersecurity
aeSolutions
krish.sridhar@aesolns.com

Abstract

Rising awareness of securing industrial control systems (ICS) and focus of organizations to roll out ICS cybersecurity programs have prompted a fresh look at the applicability and benefits of penetration (pen) testing. A well designed pen testing project in a controlled environment provides insights and in-depth findings that cannot be otherwise obtained from traditional risk assessments alone. It complements risk based assessment by taking a deeper look at critical zones and conduits that were identified during the assessment. The results and recommendations help generate cybersecurity requirements specifications and drive standardization of security measures across multiple plants within an organization. This paper highlights the benefits of pen testing in an ICS environment and offers guidelines to design and conduct a pen testing project.

Introduction

Industrial control systems (ICS) are a critical part of production operations. They have demanding requirements to run uninterrupted for several years, execute time-critical deterministic logic operations, detect drifting control loops, diagnose imminent failures of field devices, modify/add controller logic online, and prioritize control system tasks ensuring smooth and safe operations. Plant control systems are measured by their uptime and deterministic response. Therefore, traditional penetration (pen) testing is taboo within the ICS world for fear of potential intrusions to normal operations. However rising awareness and focus of organizations to roll out ICS cybersecurity programs have prompted a fresh look at the applicability and benefits of pen testing.

Pen Testing

Why pen testing? During traditional vulnerability and risk assessments extreme care is taken to conduct such assessments without causing intrusions to the running plant. Consequently, some attack scenarios and threat vectors cannot be tested to understand their implications to plant cybersecurity. Take for example assessing cybersecurity risks to a safety control system. A pen testing exercise in a controlled development environment can deploy invasive tools and procedures without regard for causing any interruptions to the control system. Consequently, the findings provide in-depth understanding of

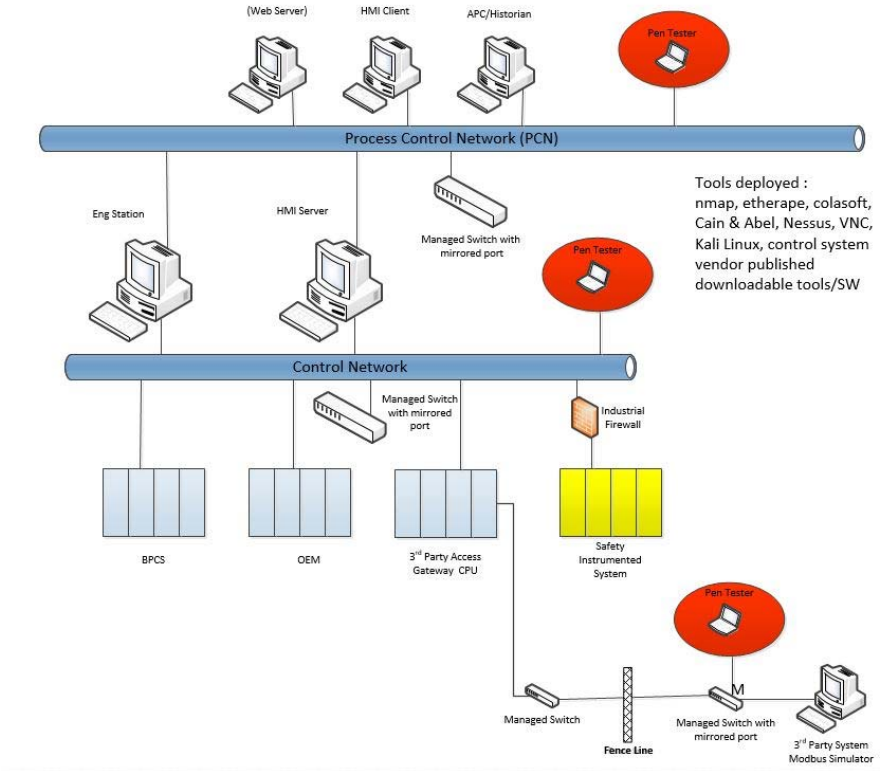
potential vulnerabilities, threat actions and impact to ICS operations. Results from pen testing can be used to develop cybersecurity requirement specifications and help drive standardization of security measures across multiple plants.

Pen Testing Design

It is common practice within many plants to have some sort of development control system. These could vary between a full blown “shadow” system, a “laboratory” scale development system, operator training/simulation system and similar test systems. These type of systems are prime candidates for designing a pen testing project.

One of the most important design criteria is to identify the perimeter network boundaries and system under consideration (SUC) for testing. The goal of a typical pen testing project is to test a subset of the overall control system architecture that is deemed relatively critical. Typically the system beneath the perimeter DMZ - this is Purdue control hierarchy model level 2 and below, is often the focus of study. Depending on the plant’s critical security zones and conduits that were previously identified by a risk based assessment, the SUC is defined. A conceptual pen testing system environment is shown in Figure 1.

Figure 1: A typical SUC for Pen Testing in a controlled environment



Testing Requirements

Once the SUC is defined, the next step is to develop a framework for the system configuration and testing locations. Some questions that arise are:

- What control system assets are essential part of the testing? What baseline configuration of these assets is a representative test?
- Where in the network should the pen testers be allowed access and with what privileges?
- What threat vectors are under consideration for testing? 3rd party access? Disgruntled employee? Other Insider threats – approved contractors, vendors? Accidental misconfigurations?

Based on these considerations the pen testing environment is configured and pen testers granted access to select locations in the network to launch simulated attacks. As shown in Figure 1, pen testers access various points in the networks to expose the vulnerabilities an attacker can find and exploit.

Another key requirement is for the pen testers to only deploy publicly available/downloadable tools and software for simulating the attack scenarios. These include any control system related tools and software available for download or purchase. Proprietary tools and custom software used by the plant are excluded from this list.

Testing scenarios are typically based on deliberate tampering type attacks. These include network sniffing and harvesting cryptographic hashes and user credentials, injecting packet floods to cause Denial of Service (DoS), introducing malformed packets, spoofing IP and MAC addresses to defeat firewall rules, compromising engineering and safety configuration stations to download malicious logic and similar attacks.

Interpreting the Results

The findings and results from the pen testing must be carefully reviewed within the context of normal plant operating procedures and practices. The following are examples of findings from a typical pen testing project:

- How cryptographic hashes can be stolen and user credentials compromised?
- How common network tools can be used to access communication modules on a PLC rack and launch a pivoted attack?
- How firewall rules can be defeated by address/protocol spoofing?
- How configuration stations if compromised can lead to safety incidents?
- How the system responds to DoS attacks? Is the PLC I/O scan impacted?
- What risk adjusted protection does industrial firewalls with deep packet inspection offer?
- What are the risks associated with insider threats and the current risk posture of the plant?

Each finding is analyzed in terms of skill level, resources necessary to exploit the vulnerability and consequences to plant operations.

Cybersecurity Requirements Specifications

The results are prioritized in the form of recommendations and transformed into requirements specifications. The requirements specifications focus on learnings from the pen testing project and typically address the following topics:

- Performance related requirements for industrial firewalls such as deep packet inspection of industrial protocols, diagnostics, configuration backup, options to phase in deployment of firewall rules without impacting operation, etc.
- Failure modes of network devices and appliances when malfunction occurs.
- Operational requirements for deploying host based intrusion detection systems such as application whitelisting.
- Role based access and monitoring requirements for critical assets such as engineering work stations addressing both operating system and applications level access control.
- Security event log monitoring requirements from various control system assets and consolidation of logs into a central location.

The project team uses the specifications to research and evaluate appropriate products and services in the market.

Conclusions

Pen testing can serve as a valuable tool within the framework of a corporate ICS cybersecurity program. It provides insights and in-depth findings that cannot be otherwise obtained from traditional risk assessments alone. It complements risk based assessment by taking a deeper look at critical zones and conduits that were identified during the assessment. Pen testing results must be carefully reviewed and contextualized against the plant's operating procedures and practices in order to derive meaningful results. The results and recommendations help generate cybersecurity requirements specifications and drive standardization of security measures across multiple plants within an organization.