Assessments in Active ICS Environments

Don C. Weber - @cutaway
Principal Consultant, Founder

© 2019 Cutaway Security, LLC. All Rights Reserved.
Cutaway Security, LLC

- Don C. Weber - Jack of All Trades
  - Security Management
  - Penetration Testing
  - Security Assessments
  - Security Researcher
  - Instructor / Presenter
  - Incident Response
Agenda

• Understanding ICS Environments
• Assessment Approach
• Reporting
• Recap
What are ICS Implementations?

- A process is a group of devices and servers that perform a specific function, typically combined with other processes.
- Plants are multiple processes that can be independent or mutually beneficial which can be centrally controlled.
- SCADA are processes and plants that are mutually dependent but spread over a wide region.

Image Source: https://potato-chips-machine.com/
What are ICS Concerns?

• Safety to personnel, environment, and process.
• Sustained operations, availability and integrity, of the process.
• Regulation, due to safety, environmental hazard, or public impact.
What are the states of ICS Environments?

• Each process control deployment is unique by industry, vendor, and company.
• Security may be built in, added on, or not considered.
• Regulations may have dictated security, lack of regulations may have dictated lack of security.
Expected Architecture – Purdue Model

Purdue Level 4 - Plant’s Business Network

- Enforcement between ICS DMZ and Business Networks (Business pulls from or pushes to iDMZ)
  - ICS DMZ - ICS to Business
  - ICS DMZ - Business to ICS
  - ICS DMZ - Cloud Access
  - ICS DMZ - Remote Access

- Enforcement between Control Networks and ICS DMZ (Control pulls from or pushes to iDMZ)

- Enforcement between Cell / Lines and Plant Supervisory (ACL on router / layer-3 switch or Firewall)

<table>
<thead>
<tr>
<th>Plant Networks</th>
<th>Control Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - Field Devices</td>
<td>0 - Field Devices</td>
</tr>
<tr>
<td>1 - Local Control</td>
<td>1 - Local Control</td>
</tr>
<tr>
<td>2 - Local Supervisory</td>
<td>2 - Local Supervisory</td>
</tr>
</tbody>
</table>

- Airgap / Enforcement Safety Systems

- Master Servers, Historian, and HMIs
- Workstations (per group/role)
- Testing/Staging (per system)
- Cyber Security Operations
- Jump Hosts (per vendor or group/role)

© 2019 Cutaway Security, LLC. All Rights Reserved.

Image Source: https://www.controlthings.io/ - Accessing and Exploiting Control Systems
What are Operational Technology (OT) Team's Concerns?

- Breaking devices and negatively impacting the processes.
- Causing delays because assessments conflict with important milestones.
- Do not know or understand goals of assessment.
- Showing how their baby is ugly…. err…. challenged.
- Making their jobs harder, less efficient.
• Make management comfortable
• Make process engineers and operators comfortable.
• Make IT personnel comfortable.

white-glove (wit’glöv’, hwîl’t-) adj.
1. Marked by extra attention or respect; special: clients who were given the white-glove treatment.
2. Scrupulous and thorough: a white-glove inspection.
3. Catering to or used by the wealthy; expensive or luxurious: “the city’s white-glove shopping boulevard” (John Freeman Gill).
IT / OT Team Approach

• Plan and scope assessment with sufficient lead time. ← organize
• Identify critical process times. ← avoid them
• Identify maintenance, upgrade, and testing windows. ← leverage them.
• Identify specific assessment goals with OT, IT, and Security Teams. ← test to those goals
• Define and work security requirements into Factory and Site Acceptance Testing (FAT / SAT) ← let the Quality Assurance / Control Team do their jobs
Assessment Approach

• Gather Information
• Process Interaction
• Reporting

Image Source: https://potato-chips-machine.com/
Gather Information

• Architecture Review
• Site Walk Thru
  • Physical Security
  • Engineer / Operator Actions in Process
• Interviews
  • Managers
  • Engineers / Operators / Programmers
  • IT Team
  • IT Security
• Threat Modeling
Process Interaction (1)

- Monitor network communications
  - Software: tcpdump, wireshark
  - Hardware: tap, switch with span port
• Configuration Hardening Assessment PowerShell Script (CHAPS) - https://github.com/cutaway/chaps
• Windows Exploit Suggester - Next Generation - [https://github.com/bitsadmin/wesng](https://github.com/bitsadmin/wesng)
Port scanning can crash legacy embedded systems if not careful! Here are the most likely causes:

- **OS Fingerprinting**
  - Don't use the -O or -A flags in Nmap
  - By far the most likely cause of crashed embedded systems
  - Can do ARP scans locally on each subnet and use MAC to ID devices
- **Scanning with SYN scans**
  - Default when using Nmap with sudo or running it as root
  - Not proper RFC behavior, so only mature ICP/IP stacks handles this properly
  - Always specify -sT in your scans to avoid this accident
- **Scanning too fast (yes, the defaults in Nmap are too fast)**
  - Use Nmap's -T2 setting sets this at 0.4 seconds
  - Or use Nmap's --scan-delay 0.1 or --max-parallelism 1 to scan 1 port at a time per host
- **Scanning UDP ports with null payloads** (can affect ICS software on Windows and Linux too!!!)
  - Don't use the -sU option in Nmap
- **Service fingerprinting usually safe, but can occasionally cause problems**
  - Use Nmap's -sV selectively on new subnets
  - Or use Nmap’s --script=banner

Source: ControlThings.io - Scanning Highly Sensitive Networks:
https://drive.google.com/file/d/1IMaDVTNRXNr0yEFr2dW7HuZYohaEpHmL/view

Image Source: https://nmap.org
Process Interaction (5)

- Escalate According to Goals
  - Active Directory Testing
  - Windows Shares Review
  - Interact with Field Level devices
  - Consider how to demonstrate evil appropriate with your skill level
  - Don't mess with production equipment
• What common penetration testing tools did I not mention?
• Typical Assessment Reporting
  • Executive Summary
  • Methodology
  • Findings with Remediations

• Systemic Issues
  • ICS Security Program aligned with NIST CyberSecurity Framework
  • Segmentation and Isolation
  • Vendor Access
Recap

• Understanding ICS Environments
• Assessment Approach
• Reporting
• Recap