Assessments in Active ICS Environments

Don C. Weber - @cutaway

Principal Consultant, Founder

Presented at SANS Orlando Fall – Orlando, FL on Oct. 29, 2019

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

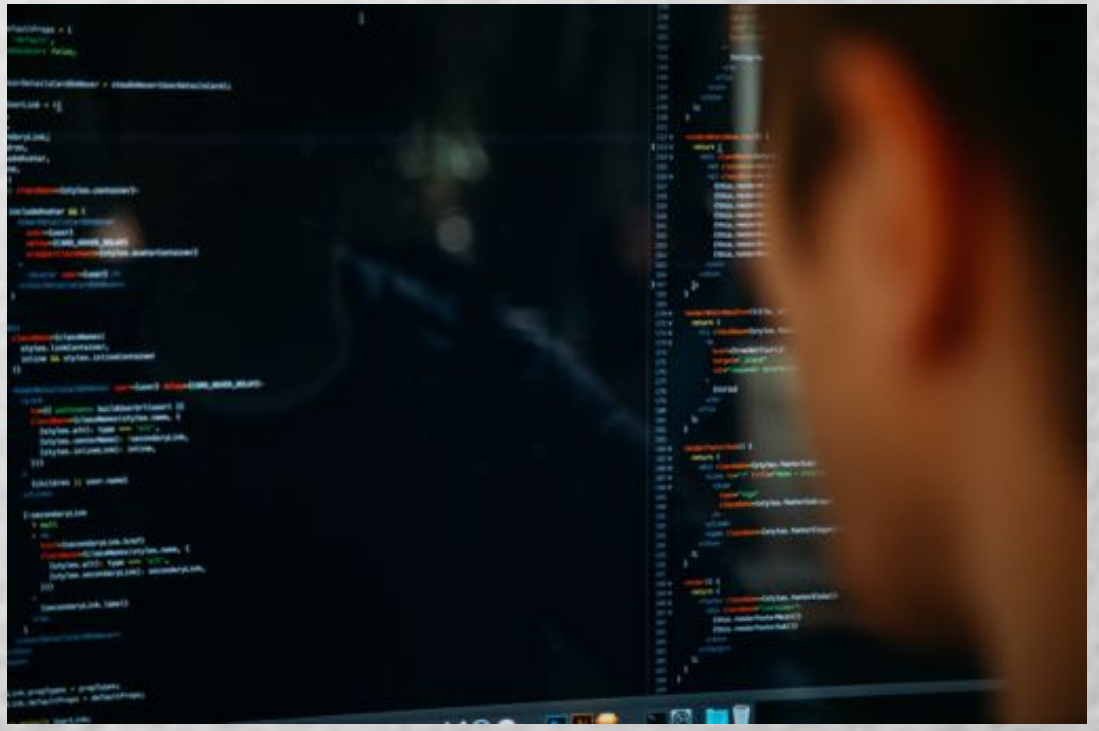


Image Source: https://unsplash.com/photos/pjAH2Ax4uWk

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: Google Maps

What is a process?

What are ICS Concerns?

Image Source: https://s3-us-west-1.amazonaws.com/umbrella-blog-uploads/wp-content/uploads/2015/08/Cannisters_After.jpg

- 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.

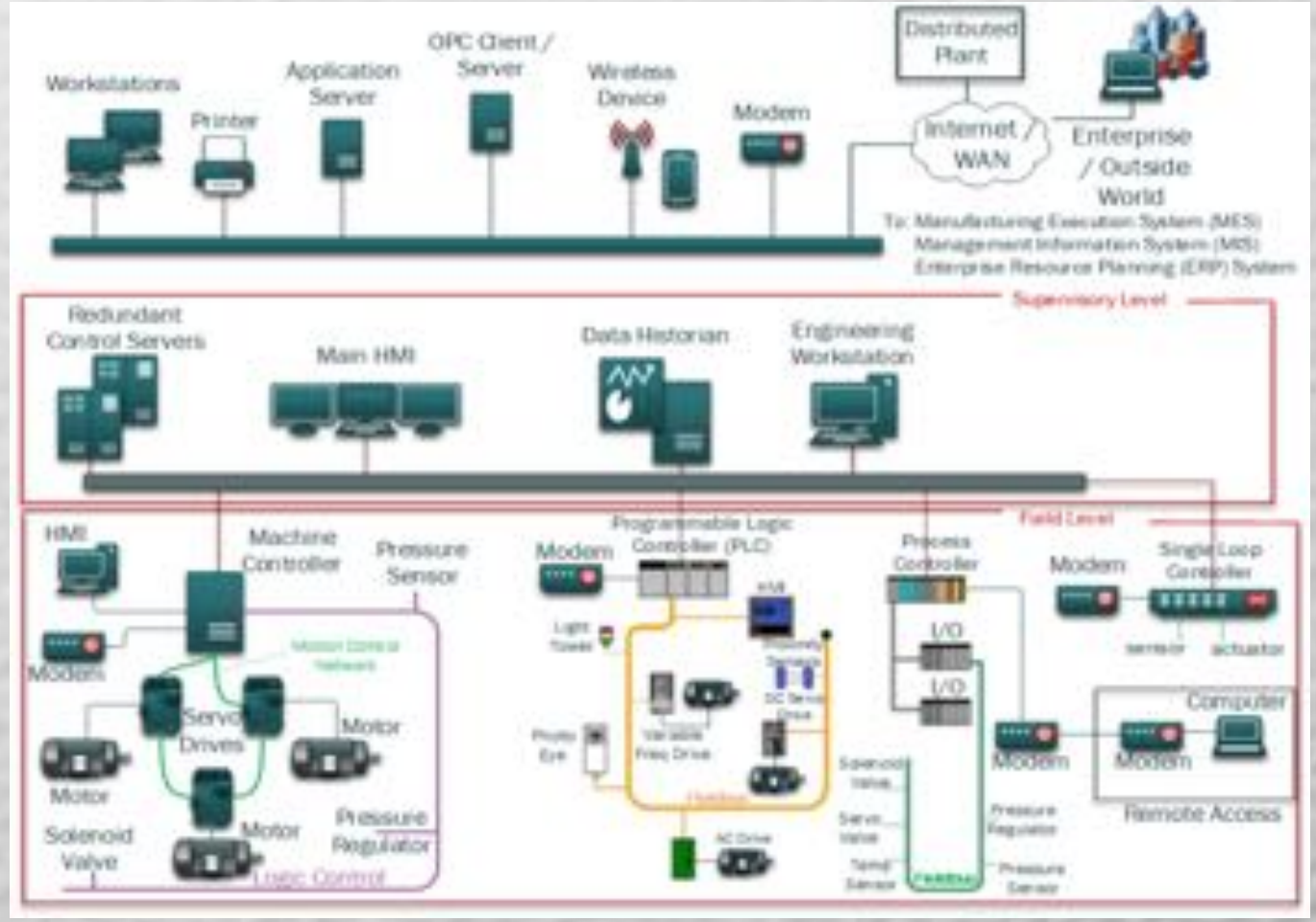


Image Source: https://www.controlthings.io/ - Accessing and Exploiting Control Systems

Expected Architecture – Purdue Model

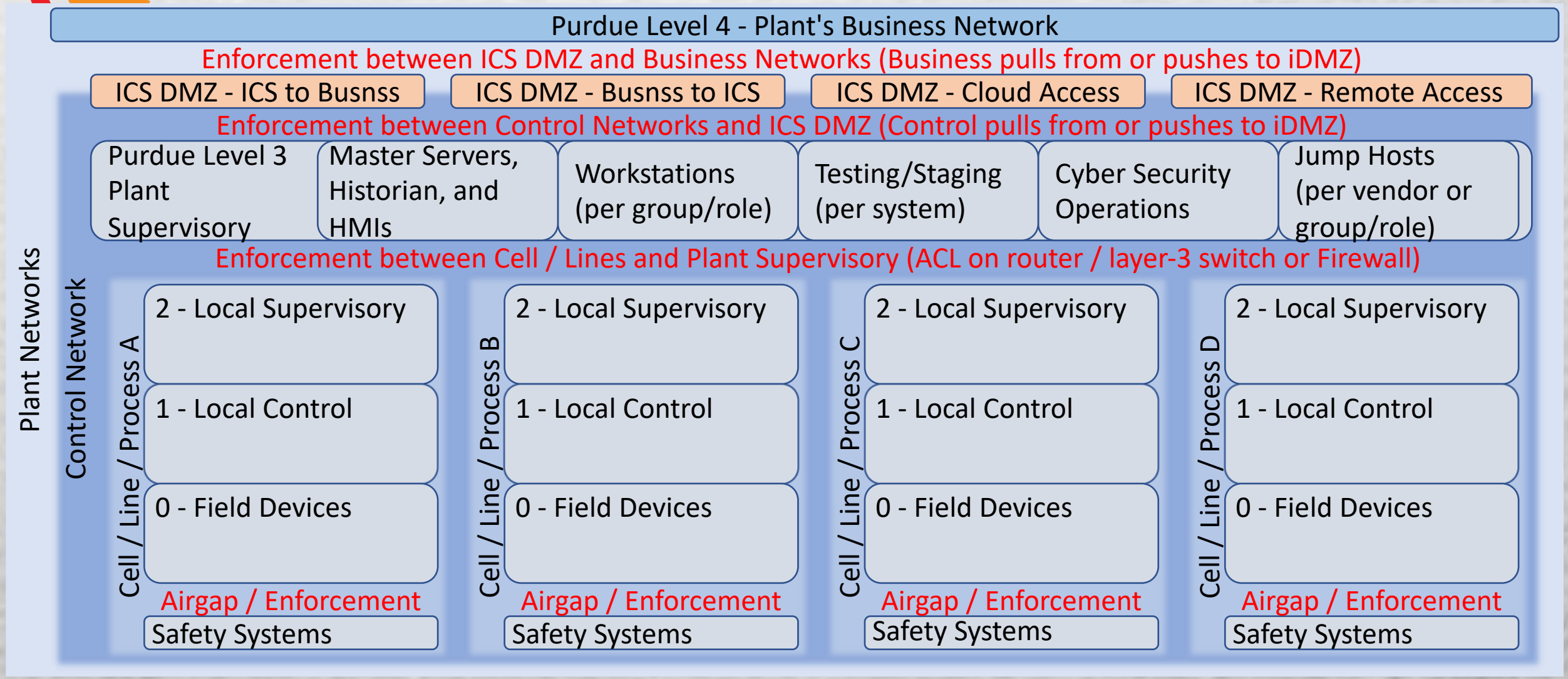


Image Source: https://www.controlthings.io/ - Accessing and Exploiting Control Systems

What are Operational Technology (OT) Team's Concerns?

Image Source: https://s3-us-west-1.amazonaws.com/umbrella-blog-uploads/wp-content/uploads/2015/08/Cannisters_After.jpg

- 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.

White-Glove Treatment

white-glove (wīt'glŏv', hwīt'-)

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).*

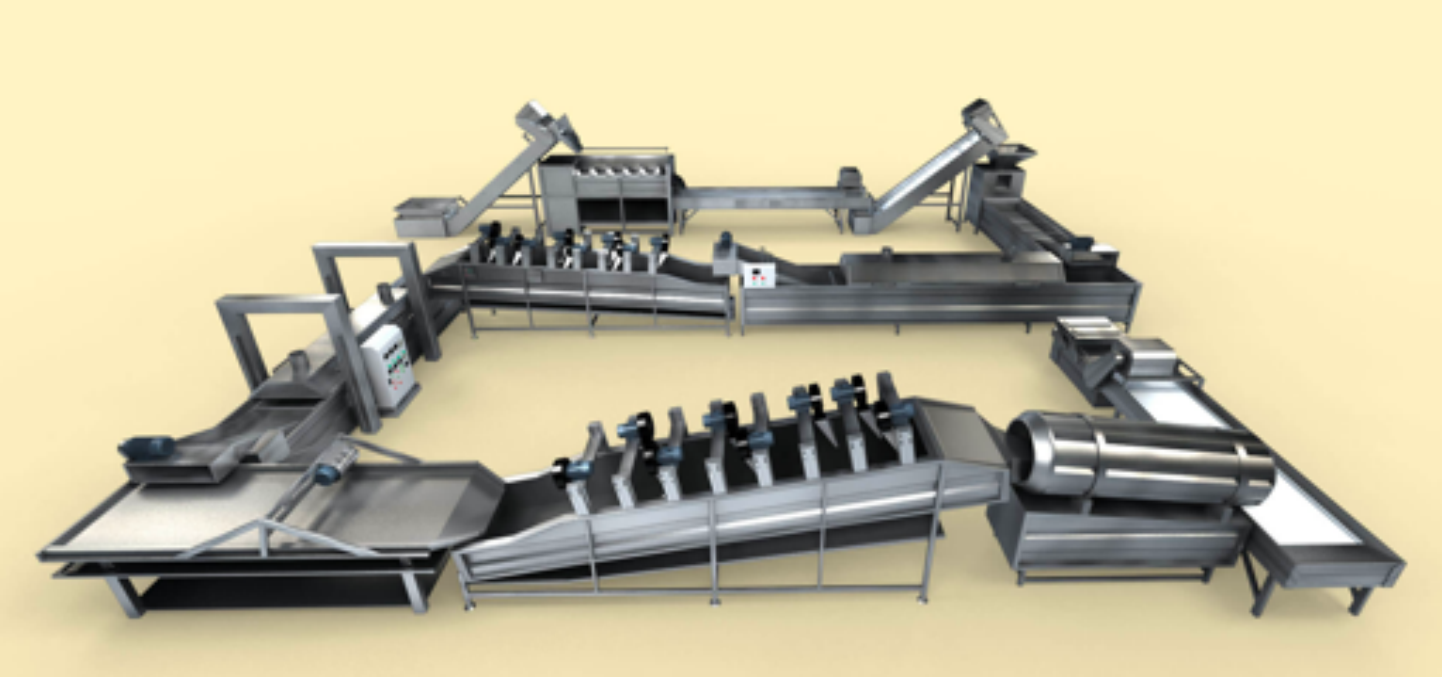
- Make management comfortable
- Make process engineers and operators comfortable.
- Make IT personnel comfortable.

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

Image Source: https://pixabay.com/en/result-excuse-me-failure-3236280/

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

Image Source: https://www.controlthings.io/ - Accessing and Exploiting Control Systems

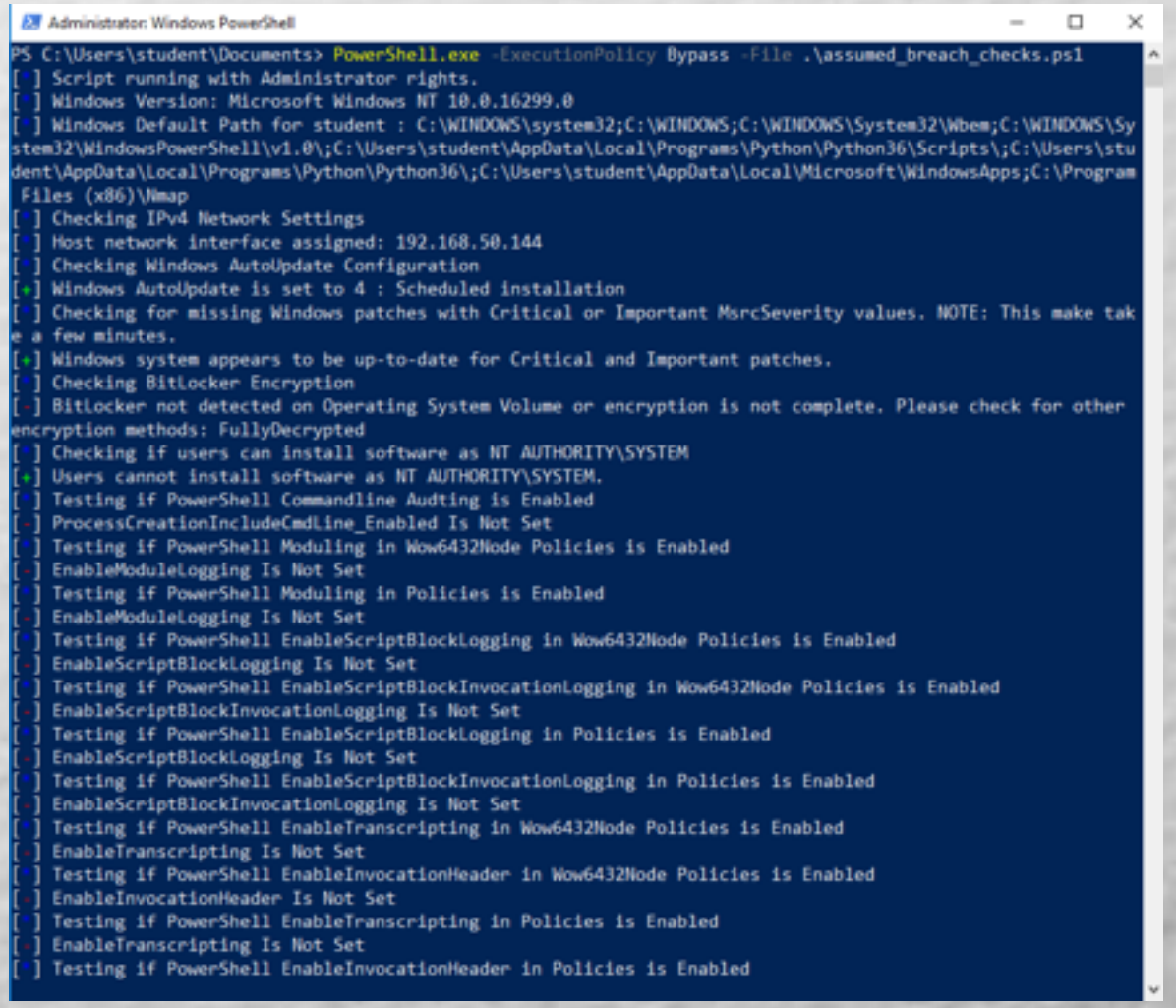
Image Source: https://gratisography.com/photo/gorilla-on-computer/

Process Interaction (1)

- Monitor network communications
  - Software: tcpdump, wireshark
  - Hardware: tap, switch with span port

Process Interaction (2)

- Configuration Hardening Assessment PowerShell Script (CHAPS) - https://github.com/cutaway/chaps



Process Interaction (3)

- Windows Exploit Suggester - Next Generation - https://github.com/bitsadmin/wesng

```
cutaway> ./windows-exploit-suggester.py --database 2018-12-30-mssb.xls --systeminfo win7-sysinfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 151 hotfix(es) against the 386 potential bulletins(s) with a database of 137 known exploits
[*] there are now 136 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 SP1 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escal
ation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privil
ege
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
```

Process Interaction (4)

Source: ControlThings.io - Scanning Highly Sensitive Networks: https://drive.google.com/file/d/1lMaDVTNRXNr0yEfr2dW7HuZYohaEpHmL/view

- 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

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

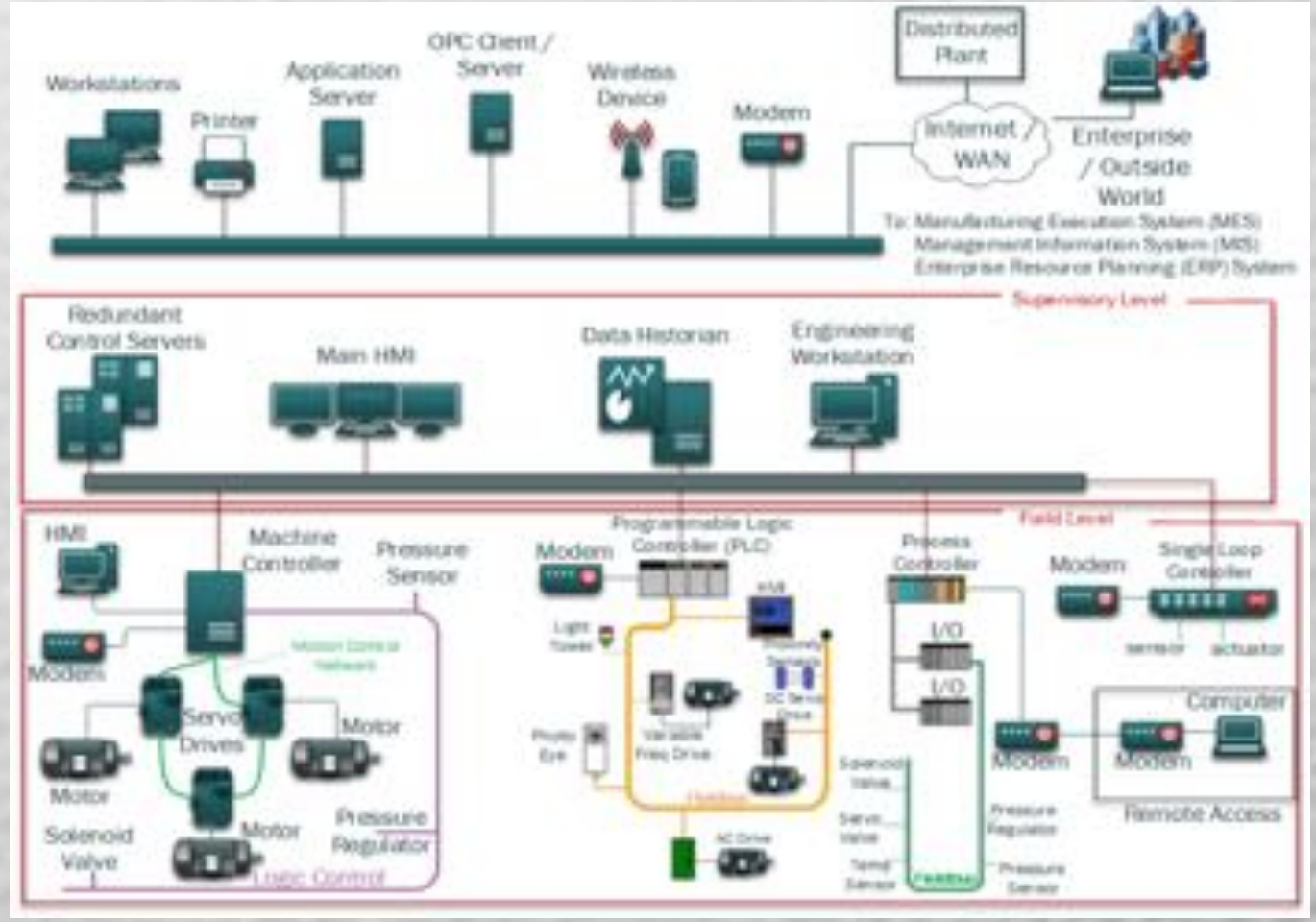


Image Source: https://www.controlthings.io/ - Accessing and Exploiting Control Systems

Process Interaction (6)

- What common penetration testing tools did I not mention?

Image Source: https://gratisography.com/photo/gorilla-on-computer/

Reporting

- Typical Assessment Reporting
  - Executive Summary
  - Methodology
  - Findings with Remediations
- Systemic Issues
  - ICS Security Program aligned with NIST CyberSecurity Framework
  - Segmentation and Isolation
  - Vendor Access

Image Source: https://unsplash.com/photos/G3yLB3Fasow

Recap

- Understanding ICS Environments
- Assessment Approach
- Reporting
- Recap

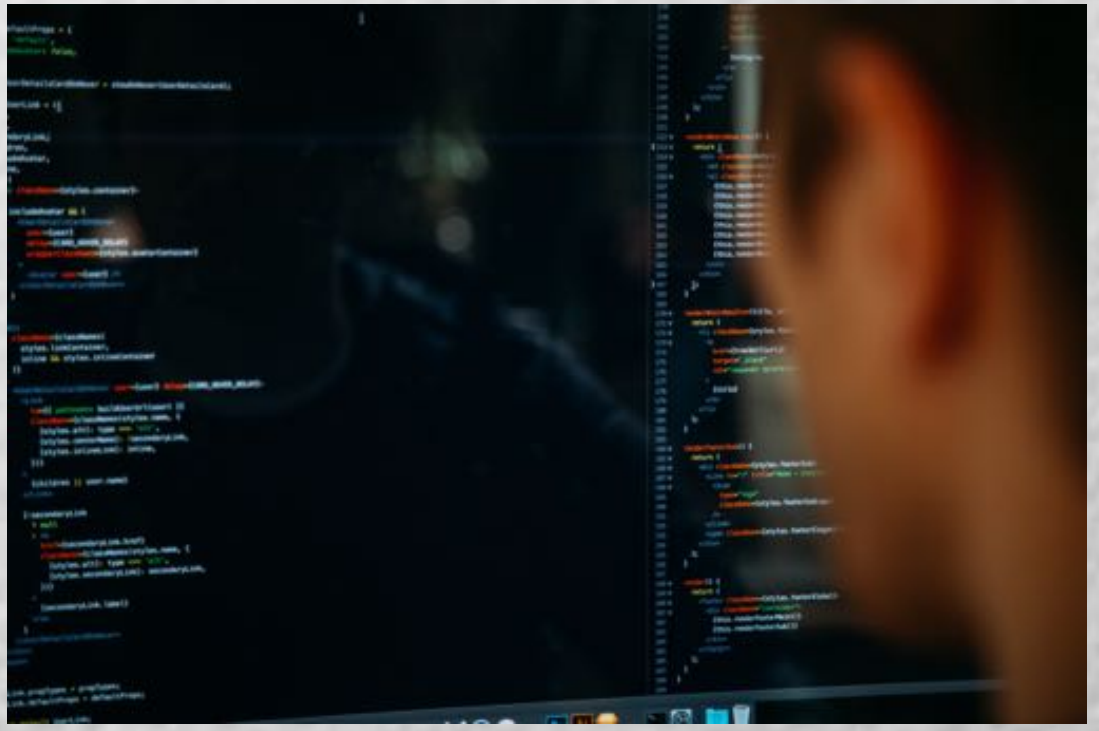


Image Source: https://unsplash.com/photos/pjAH2Ax4uWk

CUTAWAY SECURITY

INFOSEC CONSULTANTS

Don C. Weber - @cutaway

Principal Consultant, Founder

http://www.cutawaysecurity.com

http://linkedin.com/in/cutaway

https://www.sans.org/instructors/don-c-weber