Pen Testing ICS and Other Highly Restricted Environments

Don C. Weber - @cutaway

Principal Consultant, Founder

Presented at SANS Pen Test HackFest Summit in Bethesda, MD on Nov. 19, 2019

Cutaway Security, LLC

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

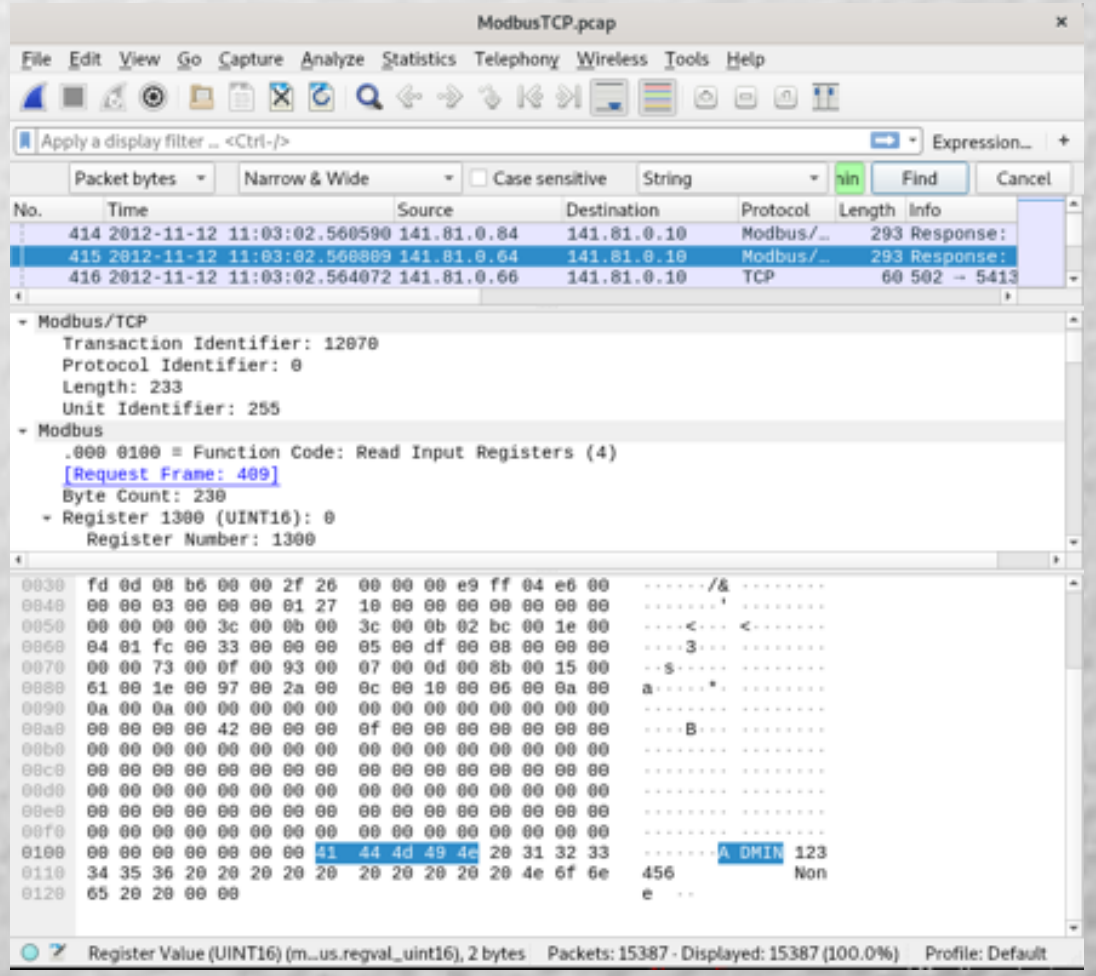
CUTAWAY SECURITY

INFOSEC CONSULTANTS

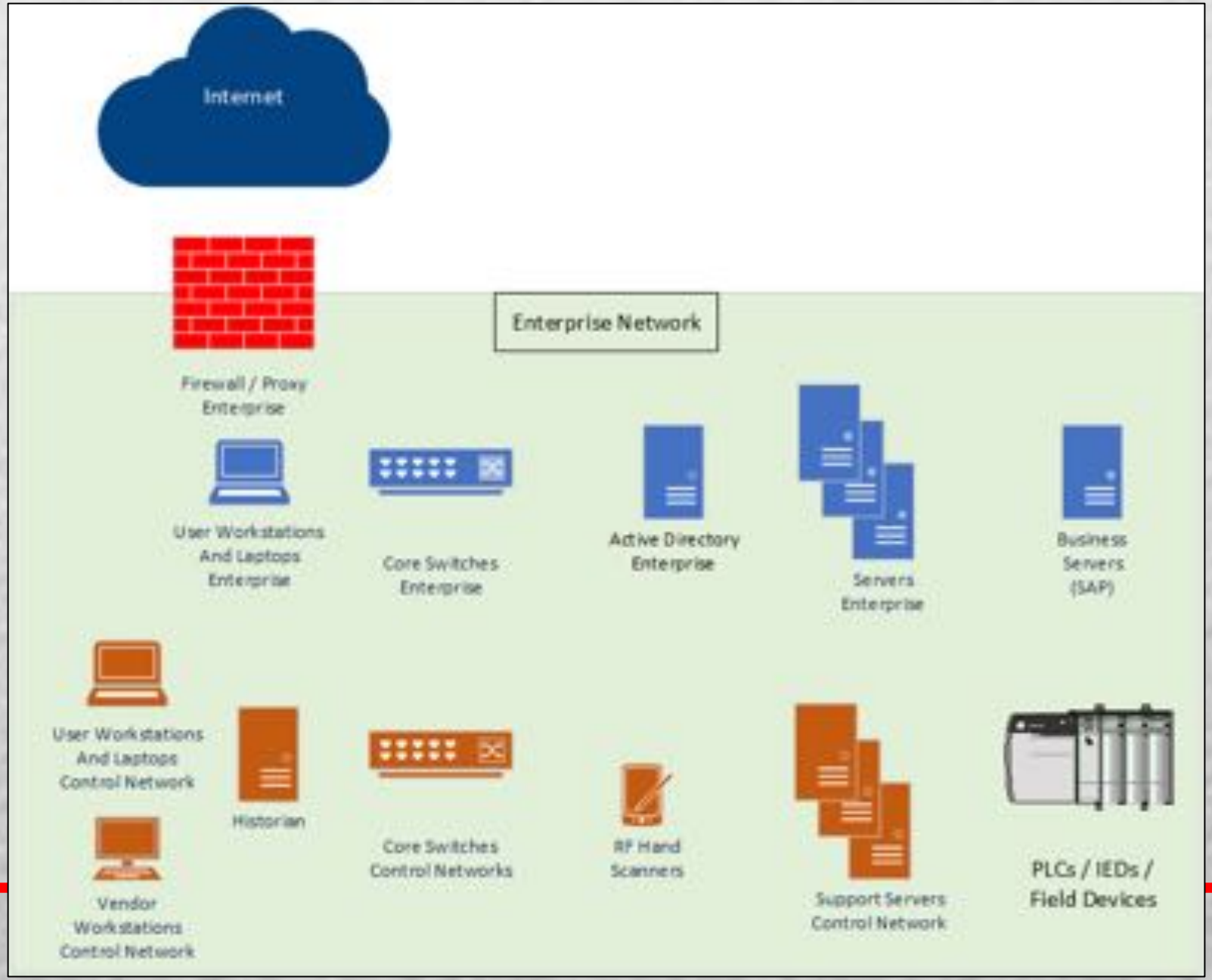
You don't know Infosec about ICS…

Things to get over…

- Clear Text Protocols
- Insecure Applications
- Vulnerable Firmware
- Brittle Services
- Legacy Software and Equipment



Worst Case Scenario



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.

It's a network, why can't we pentest it?

ICS Pen Test Roadblocks

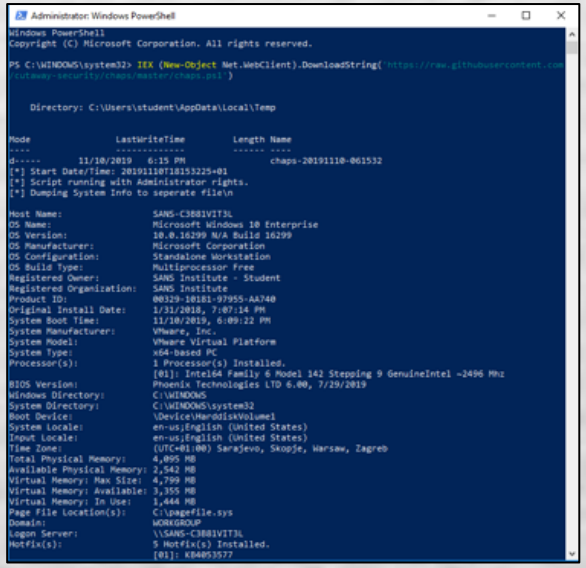
InfoSec Consultant: "… then we will do some simple scanning to discover services …"

IT Security Director: "No. You can't scan."

InfoSec Consultant: "Can I run an ARP scan to discover…?"

IT Security Director: "No. No scanning at all."

```
> sudo arp-scan 192.168.8.0/24
WARNING: Could not obtain IP address for interface eth0. Using 0.0.0.0 for
the source address, which is probably not what you want.
Either configure eth0 with an IP address, or manually specify the address
with the --arpspa option.
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.8.5     dc:89:19:38:a7:49       (Unknown)
192.168.8.6     dc:89:19:38:a6:75       (Unknown)
192.168.8.7     78:84:56:98:05:65       (Unknown)
192.168.8.8     d4:c9:ef:32:8f:ea       Hewlett Packard
192.168.8.4     00:1d:9c:97:68:9d       Rockwell
192.168.8.11    00:0c:29:83:fc:95       VMware, Inc.
192.168.8.12    08:00:06:ef:71:f2       Siemens AG
192.168.8.13    00:50:56:d4:e3:93       VMware, Inc.
192.168.8.16    d4:c9:ef:a2:8c:da       Hewlett Packard
192.168.8.17    00:0c:29:b4:5e:d9       VMware, Inc.
192.168.8.18    08:00:06:8f:e1:f3       Siemens AG
192.168.8.19    00:1d:9c:e7:d8:cd       Rockwell
```



InfoSec Consultant: "I'm going to run a PowerShell script that only check system settings and writes it to a file."

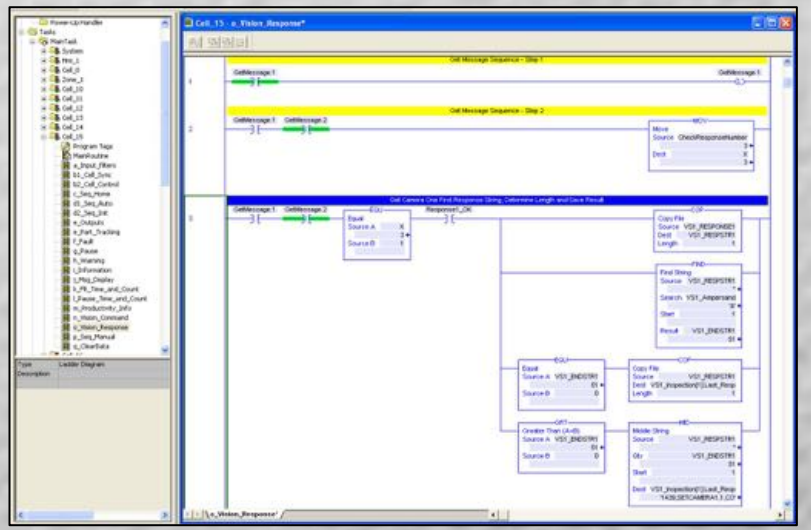
OT Lead: "But that means you are making changes to the system. "

InfoSec Consultant: "No changes, just creating one file with system configuration information."

OT Lead: "You are changing the system."

InfoSec Consultant: "We are here to understand how the PLC accepts user input and determine…"

OT PLC Programmer: "Why don't you just go away and let us do our jobs."



How did this happen?

Situation 0: Nessus scan, in 2016, of an OT subnet took over a week to fix the process.

Situation 1: Changes to systems can trigger rigorous and expensive testing. They can also void maintenance agreements.

Situation 2: IT security team and OT had different operational goals.

Image Source: https://media.giphy.com/media/C9PXSH5ZASgkU/giphy.gif

How do we overcome this mentality?

White-Glove Treatment

white-glove (wīt'glōv', 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.

#1 Recommendation from ICS IT/ OT Teams

ICS Security Team needs to spend time with the OT Team to understand the people, processes, and operations.

Image Source: Boyd Animation https://boydanimation.com/

How do we test?

Expected Architecture – ICS410 Reference Model

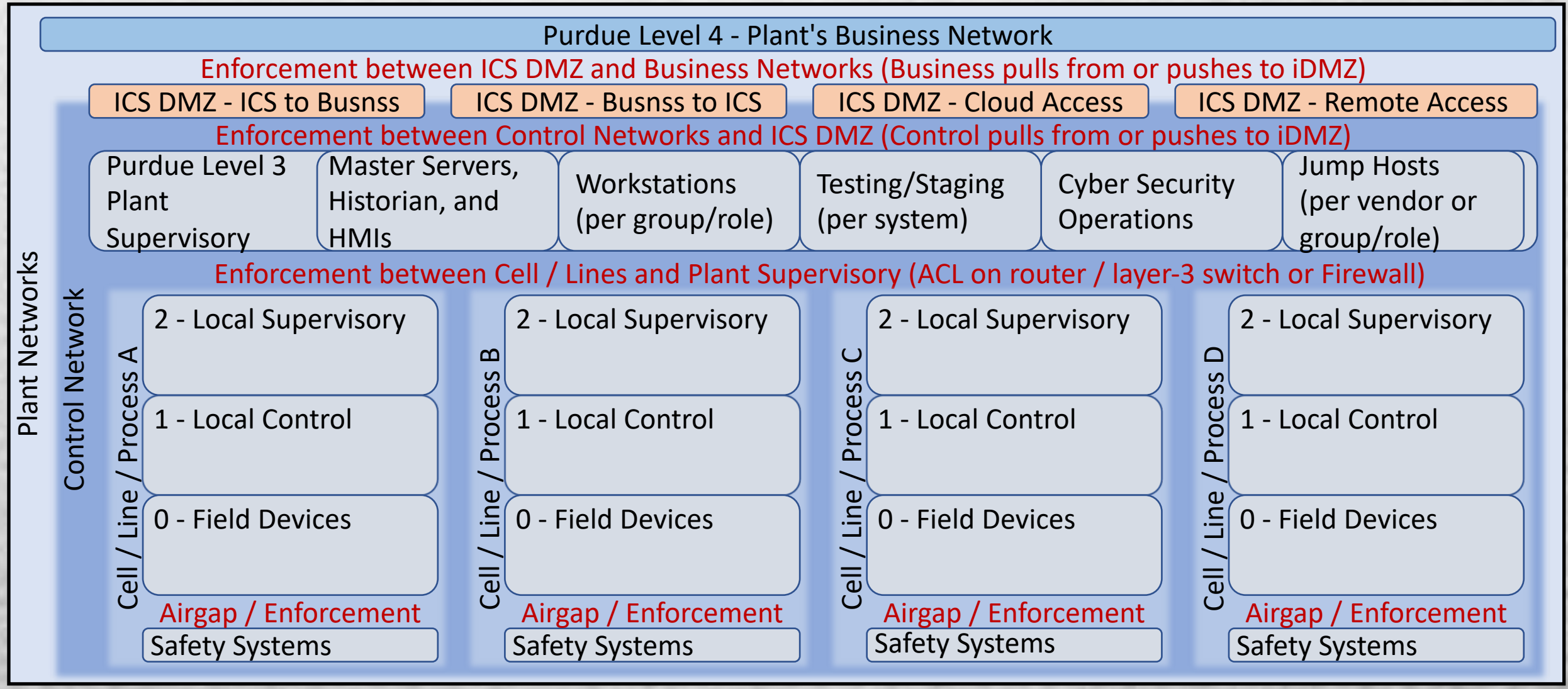
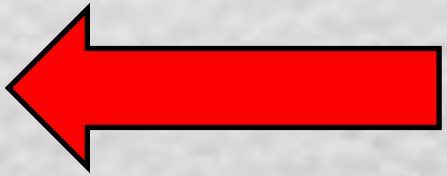


Image Source: ControlThings.io Accessing and Exploiting Control Systems

IT / OT Security Effort Prioritization

- Separate policies for IT and OT environments
- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery



Tactical ICS Security Starts Here

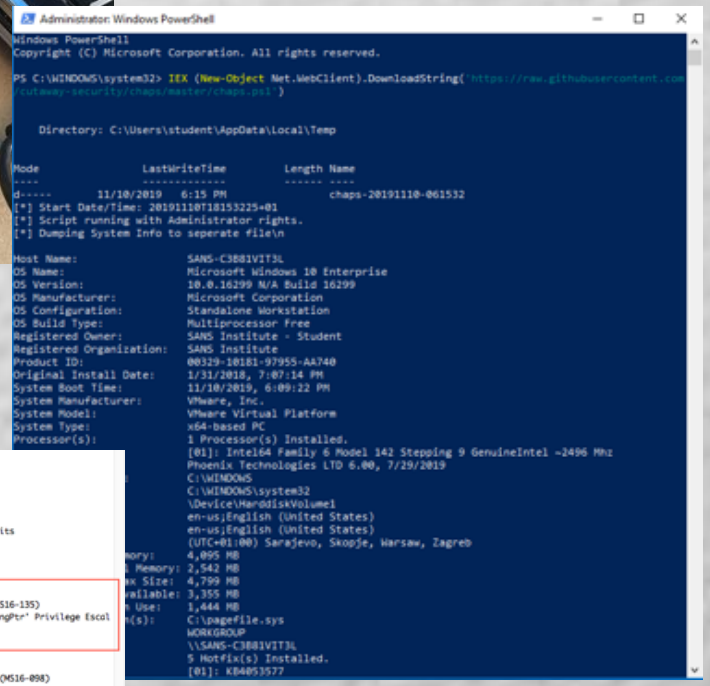
Process Familiarization

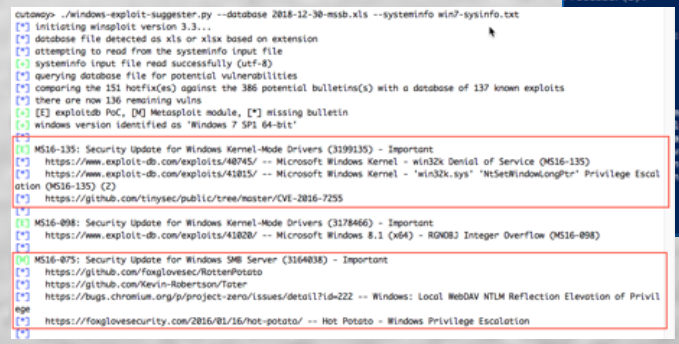
- Architecture Review
- Site Walk Thru
  - Physical Security
  - Engineer / Operator Actions in Process
- Interviews
  - Managers
  - Engineers / Operators / Programmers
  - IT Team
  - IT Security
- Threat Modeling
- Configuration Analysis
- Source Code Analysis

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

Passive Information Gathering

- Monitor network communications
  - Hardware: tap, switch with span port
  - Software: tcpdump, dumpcap, wireshark, zeek
- Scripts and Offline Analysis
  - Configuration Hardening Assessment PowerShell Script (CHAPS) - https://github.com/cutaway-security/chaps
  - Windows Exploit Suggester - Next Generation - https://github.com/bitsadmin/wesng





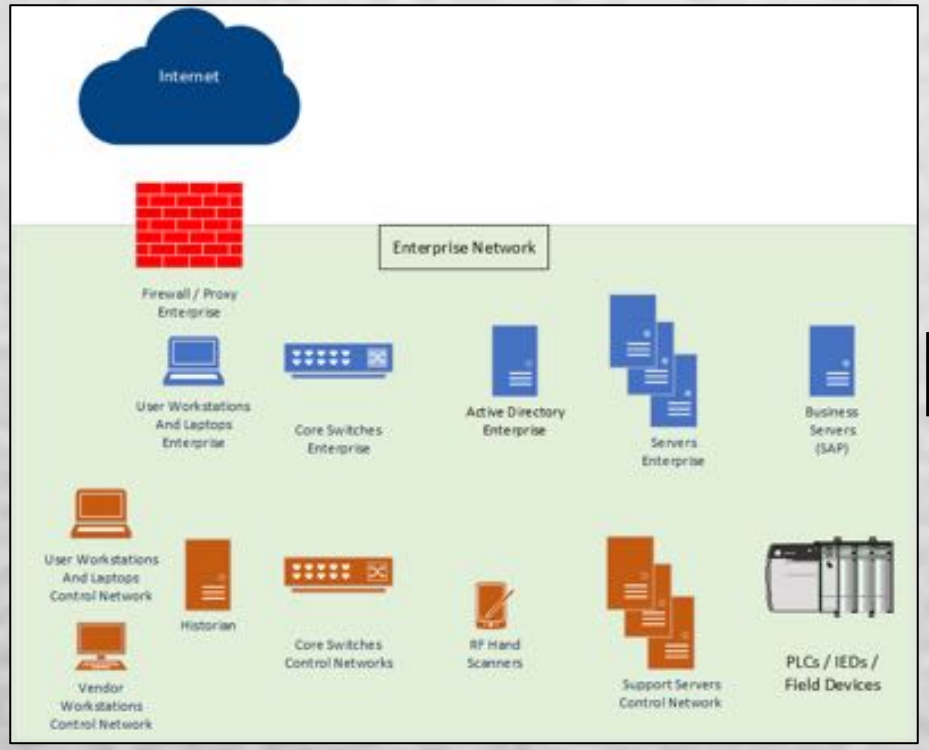
Active Testing

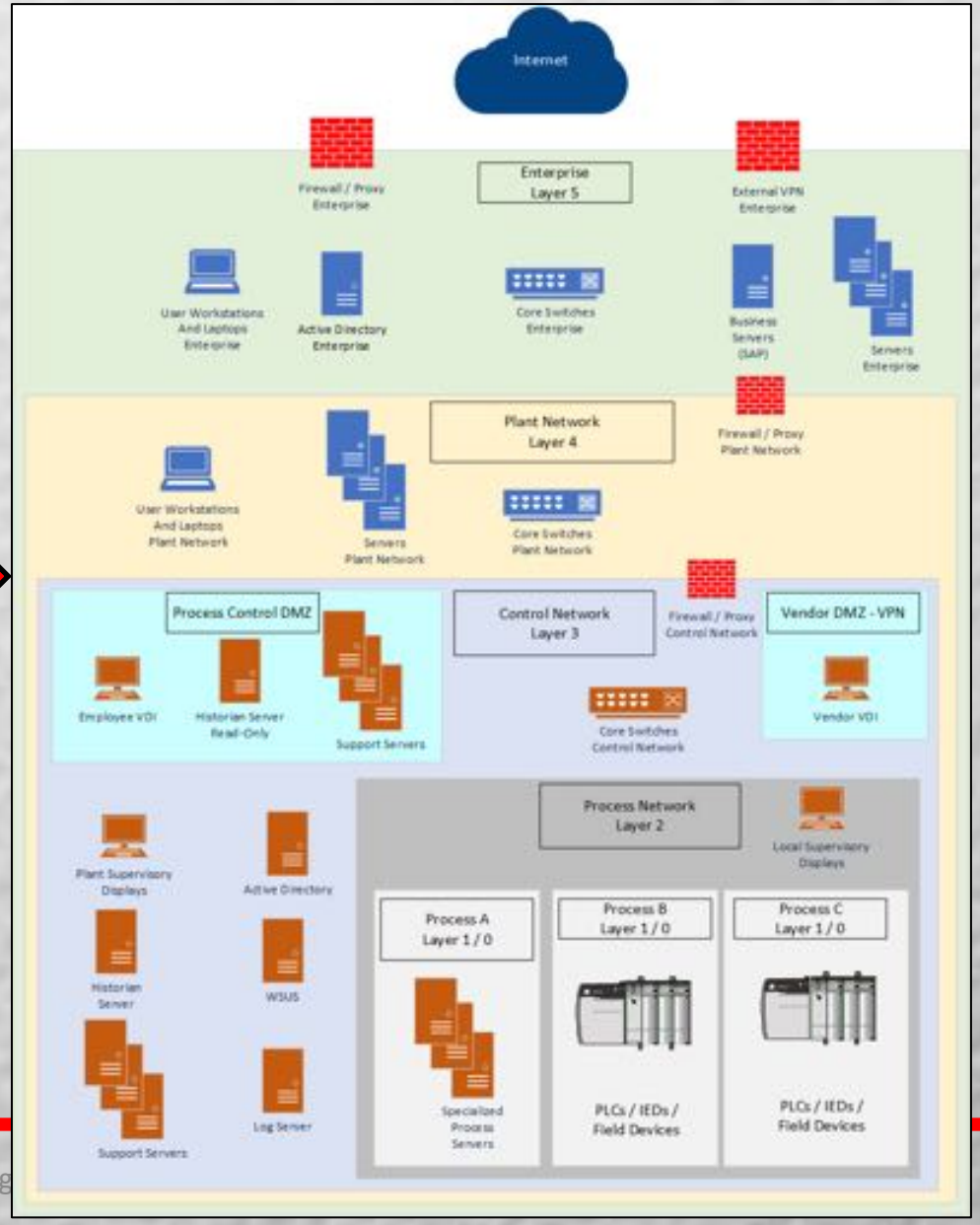
- Understand the consequences of active testing could impact safety.
- Know how to rate limit at both the network and application levels.
- Select individual targets: hosts and services.
- Know your tool configurations and double check with a partner.
- Remember assessment goals and test to them.

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

In Conclusion

Controlled Migration to Mature ICS Environment





ICS Pen Testing is a Different Kind of Sexy

- Slow your roll and check your attitude.
- OT environment cannot live up to IT policies and best practices.
- Get to know the OT teams and the processes.
- Start testing passively and escalate safely.
- Help identify issues and help the defenders protect the process.

CUTAWAY SECURITY

INFOSEC CONSULTANTS

Don C. Weber - @cutaway

Principal Consultant, Founder

http://linkedin.com/in/cutaway

https://github.com/cutaway

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

Cutaway Security, LLC

http://www.cutawaysecurity.com

http://linkedin.com/company/cutaway-security-llc

https://github.com/cutaway-security