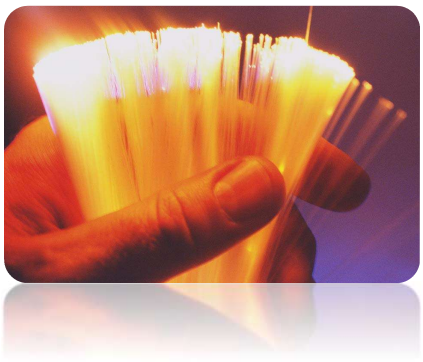
CS & ECE J444/544

Supervisory Control & Critical Infrastructures
Lecture 29
25 April 2024



1

Substation Vulnerability Assessment

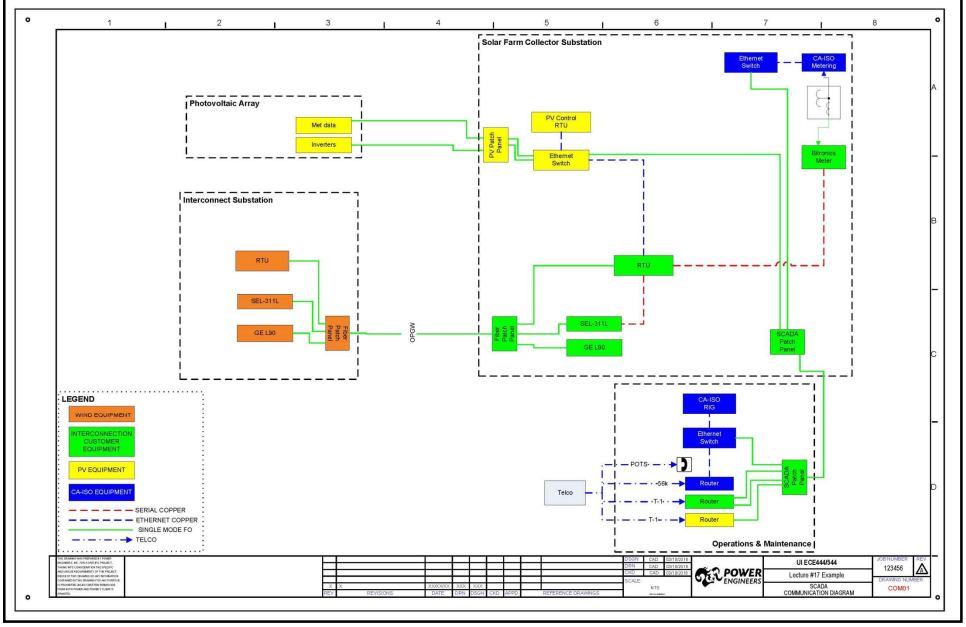
2

Step 1 - Preparation

- Location
- Tools
- Checklist
- Drawings and Diagrams
- Asset List
- Other Info

3

Step 2 – Scope



4

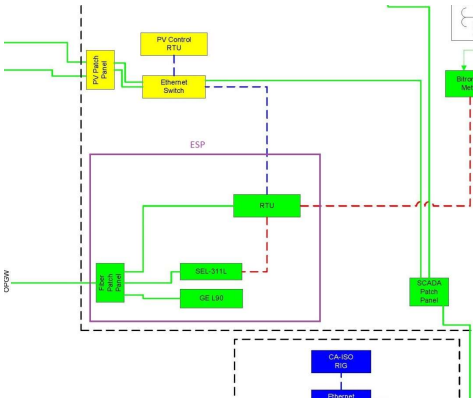
Step 3 – Physical Site

- Locks or PACS
- Vegetation
- Fencing
- Lighting
- Cameras
- Signage
- Other

5

Step 4 – ESP Access Control

- Determine Electronic Security Perimeter
  - Inventory devices
- Review Access Point
  - Accounts
  - Logs
  - Ports and Services
  - Firewall Rules



6

Step 5 – ESP Device Access Control

- Sample 10% of devices at large sites
- Determine
  - Accounts
  - Authorized Users
  - Logs
  - Ports and Services (if any)

7

Step 6 – Patching and Configuration Management

- Access Point and sample 10% of devices
- Determine
  - Patch levels (based on device type)
  - Configuration Management
    - OS or Firmware
    - Application software (commercial or open-source)
    - Network ports
  - Passwords and Accounts
    - Change defaults

8

Step 7 – Incident Response & Backup and Recovery

- Review Incident Response Plan
  - Check date of last exercise
  - Check applicability and inclusion of substation
  - Review incorporation of lessons learned
- Review Backup and Recovery Plan
  - Check date of last test or exercise
  - Check applicability and inclusion of substation
  - Review incorporation of lessons learned

9

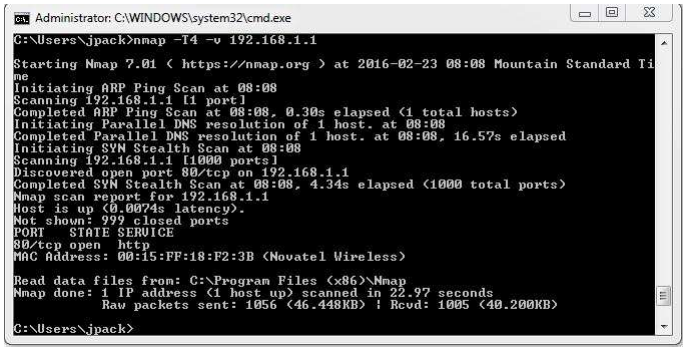
Step 8 – Perform Vulnerability Scan

- Ensure substation is out of service (during outage)
- Scan each Ethernet connected device the full range of TCP and UDP ports
- Where applicable, screenshot of running services
- Compare to previous scan or baseline configuration

10

Scanning Tools

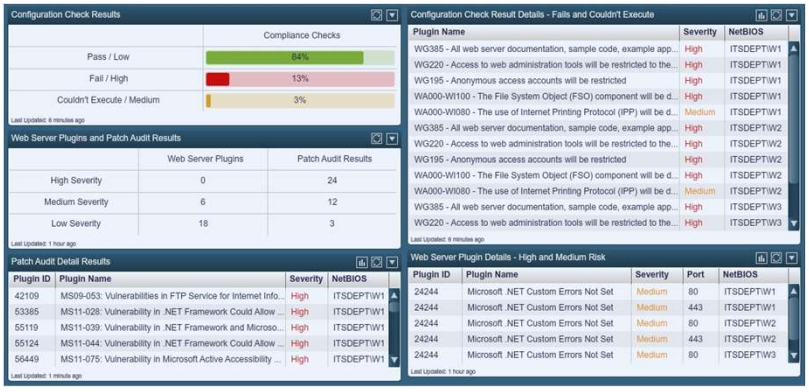
- Nmap – port scanner (and a few other things)



11

Scanning Tools

- Nessus – vulnerability scanner



12

Step 9 - Report

- Describe process
- Compare to earlier assessment results
- Compare to CM baseline
- List actions resulting from assessment
- Summarize assessment

13

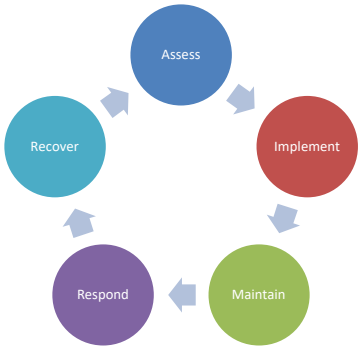
Future Trends

- AI
  - Vulnerability detection becoming more automated
- World of Software
  - End devices are becoming general purpose hardware
  - Software is what makes the difference
- Edge devices becoming more intelligent
  - Let's give them some defensive capabilities
- More intelligence – more complexity
  - Harder to secure for overall risk reduction

14

Summary

- Security is a fundamental part of control systems
- No longer bolted on – needs designed in



15