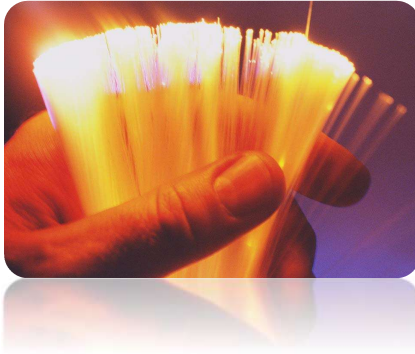


CS & ECE J444/544

Supervisory Control & Critical Infrastructures

Lecture 29

25 April 2024



1

Substation Vulnerability Assessment



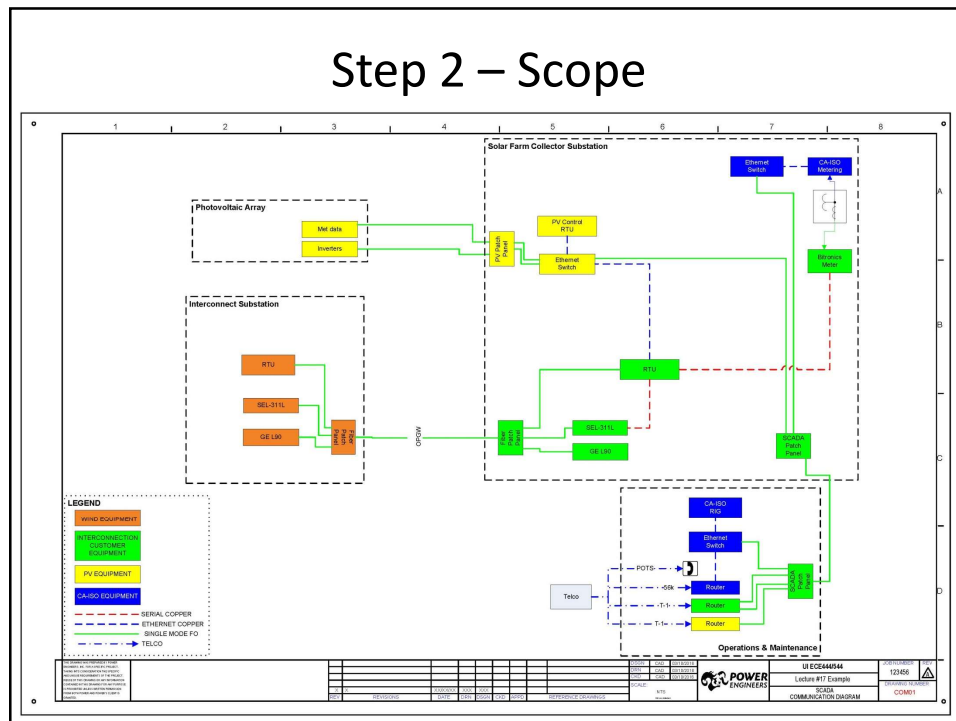
2

Step 1 - Preparation

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

3

Step 2 – Scope



4

Step 3 – Physical Site

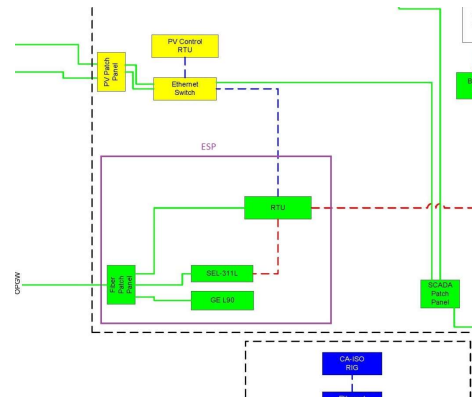
- Locks or PACS
- Vegetation
- Fencing
- Lighting
- Cameras
- Signage
- Other



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)

```

Administrator: C:\WINDOWS\system32\cmd.exe
C:\Users\njpack> nmap -T4 -v 192.168.1.1
Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-23 08:08 Mountain Standard Time
Initiating ARP Ping Scan at 08:08
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 08:08, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:08
Completed Parallel DNS resolution of 1 host. at 08:08, 16.57s elapsed
Initiating SYN Stealth Scan at 08:08
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Completed SYN Stealth Scan at 08:08, 4.34s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:15:FF:18:F2:3B (Novatel Wireless)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 22.97 seconds
Raw packets sent: 1056 (46.448KB) | Rcvd: 1005 (40.200KB)

C:\Users\njpack>
    
```

11

Scanning Tools

- Nessus – vulnerability scanner

The screenshot displays the Nessus interface with several panels:

- Configuration Check Results:** Shows compliance checks with a progress bar. Pass/Low is 84%, Fail/High is 13%, and Couldn't Execute / Medium is 3%.
- Web Server Plugins and Patch Audit Results:** A table showing the number of vulnerabilities found for different severities.
- Configuration Check Result Details - Fails and Couldn't Execute:** A list of failed checks with their severity and NetBIOS names.
- Patch Audit Detail Results:** A table listing specific vulnerabilities with their IDs, names, severities, and NetBIOS names.
- Web Server Plugin Details - High and Medium Risk:** A table listing high and medium risk plugins with their IDs, names, severities, ports, and NetBIOS names.

Severity	Web Server Plugins	Patch Audit Results
High Severity	0	24
Medium Severity	6	12
Low Severity	18	3

Plugin ID	Plugin Name	Severity	NetBIOS
42109	MS09-053: Vulnerabilities in FTP Service for Internet Info...	High	ITSDEPTW1
53385	MS11-028: Vulnerability in .NET Framework Could Allow ...	High	ITSDEPTW1
55119	MS11-039: Vulnerability in .NET Framework and Microso...	High	ITSDEPTW1
55124	MS11-044: Vulnerability in .NET Framework Could Allow ...	High	ITSDEPTW1
56449	MS11-075: Vulnerability in Microsoft Active Accessibility ...	High	ITSDEPTW1

Plugin ID	Plugin Name	Severity	Port	NetBIOS
24244	Microsoft .NET Custom Errors Not Set	Medium	80	ITSDEPTW1
24244	Microsoft .NET Custom Errors Not Set	Medium	443	ITSDEPTW1
24244	Microsoft .NET Custom Errors Not Set	Medium	80	ITSDEPTW2
24244	Microsoft .NET Custom Errors Not Set	Medium	443	ITSDEPTW2
24244	Microsoft .NET Custom Errors Not Set	Medium	80	ITSDEPTW3

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

