OT-TTT/P1M1:
Cybersecurity Industrial Control Systems Engineer (CSIE+)
4 Days Workshop

Agenda

Day 1 (2 November 2021)

Overview of Cyber Physical Systems (CPS)

Basic CPS

- Overview of CPS: Industrial Control Systems (ICS) with communication network
- ICS basics including data flow and protocol
- Hands-on exercise

Cyber Risk and Security Vulnerabilities in CPS

- Cyber risks to ICS
- Threat trends for control systems
- Security Topics: Information Technology (IT) vs Operational Technology (OT)
- Common vulnerabilities for control systems
- Case studies: Real-life cyber-attacks
- Demonstration

Process Control Exploitation

- Overview of SWaT architecture and demonstration network layout
- Static multiple point attacker paths and model
- Demonstration

IT and OT Networks Discovery

Basic Networking Concepts

- IP address and basic networking
- NEY and IANA
- OSI 7-layer model
- Address Resolution Protocol (ARP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP)
- Protocol characteristics and relevant threats

Passive Discovery

- Passive discovery vs active discovery
- Intelligence gathering tools
- Tools and techniques for passive discovery
- Hands-on exercise

Day 2 (3 November 2021)

IT and OT Networks Discovery

Active Discovery

- Nmap
- Host Discovery in IT and OT
- Port scanning and states in IT and OT
- ICS challenges
- Introduction to Nessus (vulnerability scanner)
- Introduction to OpenCAS (Open Vulnerability Assessment System)
- Exercise

CPS and Network Attacks and Exploits

Discuss the different stages of attacks

- Attacker profiles, attack stages, tasks and consideration
- System vulnerabilities and software vulnerability
- National vulnerability database CVSS
- Exploit types
- Attack operations
- Bypass network controls
- Hands-on exercise

CPS Attack Surface

- Metasploit framework
- Basic exploit process
- Meterpreter: Useful commands
- Hands-on exercise

Day 3 (5 November 2021)

Network Defence and Incident Response

CPS Attack Surface

- Hands-on exercise: Armitage on IT and OT Networks

Security Monitoring and Incident Response

- Understanding defence-in-depth
- Intrusion detection / protection system
- Signature vs anomaly detection
- Intrusion prevention systems (IPSs) vs Intrusion Detection Systems (IDSs)
- Incident response plan for CPS
- Hands-on exercise

Assessment

Instructor will brief participant on assessment to complete for the course

Day 4 (8 November 2021)

Participants ("blue team") are grouped into various technical teams such as network and SOC and execute various defence and remediation techniques against mocked attacks launched by the instructor ("red team") in a operational and realistic OT cyber range.

Workshop Overview:

Through this Cyber Exercise, participants will learn:

- To describe Cyber Physical System (CPS) defence techniques through mocked Cyber Exercise
- To understand actual versus perceived capabilities of people and defence mechanisms
- Where to invest budgets in potential gaps and pitfalls
- To strengthen and foster security teams to smoothen processes and responses against actual attacks in a cyber range
- Improve morale and team building
- Build up capabilities towards meeting regulatory and organisational requirements

9:30am – 9:45am	**:**	Cyber Exercise Briefing
9:45am – 10:00am	**:**	Familiarisation of Monitoring Tools and Various Networks
10:00am – 10:45am	**:**	**Break**
10:45am – 12:30pm	**:**	Hands-On Cyber Exercise
12:30pm – 1:30pm	**:**	**Lunch Break**
1:30pm – 4:00pm	**:**	Hands-On Cyber Exercise
4:00pm – 4:15pm	**:**	**Break**
4:15pm – 5:00pm	**:**	Hands-On Exercise
5:00pm – 5:45pm	**:**	Debrief / Round-Table Discussion

- Instructor will brief participants on the assessment to be completed for the workshop
- Lunch is not provided for this workshop

All information is correct at the time of printing