THE CYBER SCHEME

IN PARTNERSHIP WITH

HACKTONICS

OPERATIONAL TECHNOLOGY SECURITY TRAINING

SYLLABUS

OT SECURITY TESTING: FOUNDATIONS

COURSE OVERVIEW

OT Security Testing: Foundations provides a practical introduction to operational technology (OT) security testing and industrial control systems (ICS). Participants are introduced to the technologies, protocols and vulnerabilities commonly encountered within operational environments before exploring asset discovery, security testing approaches and the operational impact of cyber attacks.

The course combines expert-led instruction, demonstrations and practical exercises using specialist OT training environments to develop an understanding of OT security concepts and testing methodologies.

WHO THE COURSE IS FOR

The course is intended for cyber security professionals who are familiar with IT security principles and technologies but are new to operational technology and industrial control systems.

ENTRY REQUIREMENTS

- Working knowledge of the Linux command line
- Some experience with Kali Linux is advantageous
- Working knowledge of Python
- Prior knowledge of operational technology is not required.

LEARNING OUTCOMES

On completion of the course, participants should be able to:

- Explain the purpose and function of operational technology and industrial control systems
- Identify common OT assets, protocols and associated vulnerabilities
- Explain key differences between IT and OT security
- Conduct OT asset discovery activities within a controlled environment
- Describe common attacks against industrial control systems and their operational impact
- Understand the principles of OT security testing and safe engagement practices.

FOUNDATION COURSE SYLLABUS

1. Introduction to ICS and OT

- Industrial control systems and operational technology fundamentals
- Components commonly found within OT environments
- OT and IT security differences
- OT cyber security case studies

2. Security Testing OT Systems

- Security testing principles
- Scope and rules of engagement
- Structuring OT security tests
- Common testing pitfalls and how to avoid them

3. Asset Discovery

- OT asset discovery methods
- Active and passive discovery techniques
- Tools used for OT asset discovery
- Practical asset discovery exercises

4. Vulnerabilities and their Impact

- OT protocol vulnerabilities
- Device vulnerabilities
- Human Machine Interface (HMI) vulnerabilities
- Operational impact and consequence analysis

INDICATIVE SCHEDULE

Subject to change

One Day Course

Time	Session
09:45	Arrival
10:00 - 11:00	Introduction
11:00 - 11:15	Security Testing OT Systems
11:15 - 11:30	Break
11:30 - 12:30	Asset Discovery
12:30 - 13:15	Lunch
13:15 - 14:00	Vulnerabilities and their Impact
14:00 - 14:15	Break
14:15 - 14:45	Vulnerabilities and their Impact, continued
14:45 - 15:00	Conclusion.

PENTESTING OPERATIONAL TECHNOLOGY SYSTEMS: PRACTITIONER

COURSE OVERVIEW

Pentesting Operational Technology Systems: Practitioner develops practical OT security testing capability through structured penetration testing exercises. Participants build on foundational OT knowledge to explore penetration testing methodologies, asset discovery, vulnerability assessment, security baseline evaluation and exploitation techniques within controlled industrial environments.

The course combines theory, demonstrations and extensive hands-on exercises to develop practical testing skills and an understanding of operational impact.

WHO THE COURSE IS FOR

The course is intended for participants who have completed OT Security Testing: Foundations or who can demonstrate equivalent knowledge and experience.

ENTRY REQUIREMENTS

- Completion of OT Security Testing: Foundations or equivalent experience
- Working knowledge of the Linux command line
- Some experience with Kali Linux is advantageous
- Working knowledge of Python.

LEARNING OUTCOMES

On completion of the course, participants should be able to:

- Explain the stages of an OT penetration test
- Conduct OT asset discovery and vulnerability assessment activities
- Evaluate OT security baselines and control effectiveness
- Investigate vulnerabilities in industrial protocols and devices
- Assess the operational impact of OT cyber attacks
- Recommend mitigating controls and security improvements.

PRACTITIONER COURSE SYLLABUS

1. Introduction and Foundations Review

- OT security testing fundamentals
- Asset discovery recap
- Vulnerabilities and operational impact.

2. Anatomy of an OT Penetration Test

- Planning and preparation
- Rules of engagement
- Testing methodologies
- Reporting and best practice.

3. Asset Discovery and Vulnerability Scanning

- Active and passive discovery methods
- Vulnerability scanning techniques
- Open-source intelligence sources
- Asset discovery and assessment activities.

4. Establishing a Security Baseline

- Security controls and baseline assessment
- Protocol, device and platform vulnerabilities
- Evaluation of defensive controls
- Security control effectiveness.

5. Exploiting Industrial Protocols

- Industrial protocol design and operation
- Protocol weaknesses and exploitation techniques
- Protocol attack demonstrations and exercises.

6. PLC Attacks

- PLC architectures
- PLC attack methodologies
- Logic manipulation and firmware attacks
- Practical PLC security testing exercises.

INDICATIVE SCHEDULE

Subject to change

Day One

Time	Session
08:45	Arrival
09:00 - 10:00	Introduction
10:00 - 10:15	Break
10:15 - 12:15	Anatomy of an OT Penetration Test
12:15 - 13:00	Lunch
13:00 - 15:00	Asset Discovery and Vulnerability Scanning
15:00 - 15:15	Break
15:15 - 17:00	Establishing a Security Baseline.

Day Two

Time	Session
08:45	Arrival
09:00 - 09:15	Recap of Day 1
09:15 - 11:15	Exploiting Industrial Protocols
11:15 - 11:30	Break
11:30 - 12:30	Exploiting Industrial Protocols, continued
12:30 - 13:15	Lunch
13:15 - 14:15	PLC Attacks
14:15 - 14:30	Break
14:30 - 16:15	PLC Attacks, continued
16:15 - 16:45	Wrap-up and conclusion.

OPERATIONAL TECHNOLOGY SECURITY TESTING: ADVANCED

COURSE OVERVIEW

Operational Technology Security Testing: Advanced provides an in-depth examination of industrial control system security testing. Participants explore advanced protocol analysis, PLC and HMI security assessment, end-to-end attack scenarios, operational impacts and security architecture principles within complex OT environments.

The course is designed for experienced practitioners seeking to develop advanced technical capability in OT and ICS security assessment.

WHO THE COURSE IS FOR

The course is intended for experienced OT security practitioners who have completed Pentesting Operational Technology Systems: Practitioner or who possess equivalent knowledge and experience.

ENTRY REQUIREMENTS

- Completion of Pentesting Operational Technology Systems: Practitioner or equivalent experience
- Practical experience of OT asset discovery and vulnerability assessment
- Working knowledge of LINICS and associated testing tools
- Working knowledge of Python.

LEARNING OUTCOMES

On completion of the course, participants should be able to:

- Analyse security weaknesses in OT protocols and devices
- Assess PLC and HMI security within operational environments
- Conduct advanced OT security testing activities
- Evaluate operational and safety impacts arising from cyber attacks
- Assess OT security architectures and their effectiveness
- Recommend architectural improvements to strengthen resilience.

ADVANCED COURSE SYLLABUS

1. Refresher: OT Security Testing

- Asset discovery and vulnerability assessment
- OT penetration testing methodologies
- Security baseline assessment.

2. OT Protocols: A Deep Dive

- Protocol design weaknesses
- Industrial protocol analysis
- Advanced protocol assessment techniques
- Protocol exploitation exercises.

3. PLCs: A Deep Dive

- PLC architecture analysis
- Vendor implementation differences
- Advanced PLC attack techniques
- PLC security assessment exercises.

4. HMIs: A Deep Dive

- HMI architectures
- HMI security vulnerabilities
- HMI assessment methodologies
- Practical security testing exercises.

5. Anatomy of OT Attacks: A Deep Dive

- Operational impact categories
- Safety and reliability impacts
- End-to-end attack scenarios
- Impact analysis techniques.

6. Security Architectures

- Regulatory and governance considerations
- Security frameworks and standards
- Industrial security architecture principles
- Secure design and re-architecture exercises.

INDICATIVE SCHEDULE

Subject to change

Day One

Time	Session
08:45	Arrival
09:00 - 10:00	Refresher
10:00 - 10:15	Break
10:15 - 12:15	OT Protocols
12:15 - 13:00	Lunch
13:00 - 15:00	OT Protocols, continued
15:00 - 15:15	Break
15:15 - 17:00	OT Protocols, continued.

Day Two

Time	Session
08:45	Arrival
09:00 – 09:15	Recap Day 1
09:15 – 11:15	PLCs
11:15 – 11:30	Break
11:30 – 12:30	PLCs, continued
12:30 – 13:15	Lunch
13:15 – 15:00	PLCs, continued
15:00 – 15:15	Break
15:15 – 17:00	HMIs.

INDICATIVE SCHEDULE

Subject to change

Day Three

Time	Session
08:45	Arrival
09:00 – 09:15	Recap Day 2
09:15 – 11:15	Anatomy of OT Attacks
11:15 – 11:30	Break
11:30 – 12:30	Anatomy of OT Attacks, continued
12:30 – 13:15	Lunch
13:15 – 14:15	Security architectures
14:15 – 14:30	Break
14:30 – 16:15	Security architectures, continued
16:15 – 16:45	Wrap-Up and Conclusion.

COURSE DELIVERY

All courses combine expert-led instruction with practical learning activities designed to develop real-world operational technology security capability.

DELIVERY METHODS

- Expert-led instruction
- Technical demonstrations
- Guided practical exercises
- Hands-on laboratory activities
- Individual and group-based learning activities
- Realistic industrial control system scenarios
- Question-and-answer sessions throughout the course

TRAINING ENVIRONMENT

Training is delivered using specialist operational technology learning environments designed to replicate technologies, protocols and devices commonly encountered within industrial environments.

Training environments may include:

- Hacktonics ICS training boxes
- LINICS operational technology security platform
- Industrial control system training environments
- Programmable Logic Controllers (PLCs)
- Human Machine Interfaces (HMIs)
- Industrial communications protocols
- Specialist OT security assessment tools
- Simulated operational technology attack scenarios

Training exercises are designed to help participants understand the relationship between technical vulnerabilities, operational processes and organisational risk.

DELEGATE REQUIREMENTS

Equipment

No specialist equipment is required.

Laptop

Training laptops are provided for all delegates.

Software

All software required for practical exercises is pre-installed on the provided equipment.

Prior Knowledge

Participants should review the entry requirements for the course level they intend to attend.

Accessibility

Reasonable adjustments can be discussed and arranged in advance where required.

No formal assessment is required for successful completion of these courses.

Certificate of attendance will be issued by The Cyber Scheme on successful completion.

For current course dates, pricing, bookings and accessibility enquiries, please visit https://thecyberscheme.org/ot-training/ or contact info@thecyberscheme.org