OT Penetration Testing

Methodology for Industrial Security Assessments

OT Security Learning Series

Document 710 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

OT penetration testing evaluates the security of industrial control systems by simulating real-world attack scenarios. Unlike traditional IT pentesting, OT assessments require specialized knowledge, careful planning, and strict safety considerations to avoid disrupting critical processes.

Critical

OT penetration testing carries significant risk. Improper testing can cause equipment damage, safety incidents, production outages, or environmental harm. Always prioritize safety over thoroughness.

1.1 OT vs IT Pentesting

Aspect	IT Pentesting	OT Pentesting
Primary concern	Data confidentiality	Safety and availability
System tolerance	Resilient to testing	Fragile, crash-prone
Downtime impact	Business disruption	Physical/safety impact
Testing window	Often flexible	Maintenance windows only
Protocol knowledge	Standard (TCP/IP)	Industrial (Modbus, DNP3)
Recovery	Restore from backup	May require site visit

2 Planning and Scoping

2.1 Pre-Engagement Requirements

Key Point

Essential pre-engagement activities:

- Obtain written authorization from asset owner
- Identify all stakeholders (OT, IT, Safety, Operations)
- Define clear scope boundaries and exclusions
- Establish emergency contacts and rollback procedures
- Review safety documentation and process constraints
- Schedule during planned maintenance if possible

2.2 Scope Considerations

Element	Considerations
Network segments	Which zones are in scope (IT, DMZ, OT, Safety)?
System types	HMIs, PLCs, RTUs, historians, engineering workstations
Protocols	Which industrial protocols can be tested?
Active vs passive	Can active exploitation be performed?
Physical access	Is physical security testing included?
Time constraints	Testing windows, blackout periods

2.3 Risk Assessment

Before testing, assess potential impacts:

- **Safety risks:** Could testing trigger safety systems or cause harm?
- **Production risks:** What is the cost of unplanned downtime?
- **Equipment risks:** Could commands damage physical equipment?
- **Cascading effects:** Could actions affect connected systems?

3 Testing Phases

3.1 Phase 1: Passive Reconnaissance

Safe information gathering without active probing:

- **OSINT:** Public information about systems, vendors, employees
- **Network capture:** Passive traffic analysis (span/tap port)
- **Protocol identification:** Identify industrial protocols in use
- **Asset inventory:** Map devices from observed traffic
- **Credential discovery:** Monitor for cleartext authentication

Tip

Passive reconnaissance provides significant intelligence with minimal risk. Spend adequate time in this phase before any active testing.

3.2 Phase 2: Active Reconnaissance

Careful active discovery with OT-safe techniques:

- **Controlled scanning:** Slow, targeted port scans
- **Service identification:** Banner grabbing on known ports
- **Protocol enumeration:** Query devices using native protocols
- **Vulnerability scanning:** OT-aware scanners only

Warning

Standard IT vulnerability scanners can crash OT devices. Use only scanners designed for industrial environments or perform manual testing.

3.3 Phase 3: Vulnerability Assessment

Identify weaknesses without exploitation:

- Default and weak credentials
- Unpatched vulnerabilities
- Insecure protocol configurations
- Network segmentation gaps
- Unnecessary services and ports

3.4 Phase 4: Controlled Exploitation

If authorized and safe, validate vulnerabilities:

- **Test environment first:** Validate exploits on lab systems
- **Reversible actions only:** No destructive testing
- **Monitoring:** Continuous observation during exploitation
- **Immediate rollback:** Stop at first sign of issues

4 Testing Techniques

4.1 Network-Level Testing

Test	Purpose
Segmentation validation	Verify zone boundaries are enforced
Firewall rule analysis	Identify overly permissive rules
VLAN hopping	Test for layer 2 isolation bypasses
Traffic interception	Assess encryption and authentication
Wireless assessment	Identify rogue or insecure wireless

4.2 Protocol-Specific Testing

- **Modbus:** Read/write coils and registers, function code fuzzing
- **DNP3:** Command injection, authentication bypass
- **OPC:** Enumeration, unauthorized data access
- **EtherNet/IP:** Device discovery, configuration changes

4.3 Application Testing

- HMI web interface vulnerabilities
- Historian database security
- Engineering software weaknesses

- Remote access portal testing

5 Safety Guidelines

5.1 Absolute Rules

Critical

Never perform these actions without explicit approval:

- Write commands to PLCs or RTUs in production
- Modify safety system configurations
- Test during active production without operations present
- Use denial-of-service techniques on OT networks
- Exploit vulnerabilities that could cause physical impact

5.2 Safe Testing Practices

1. **Start passive:** Observation before interaction
2. **Test replicas first:** Use lab or staging environments
3. **Coordinate continuously:** Real-time communication with operations
4. **Monitor impacts:** Watch process variables during testing
5. **Document everything:** Detailed logs for incident response
6. **Have rollback plans:** Know how to undo any changes

6 Reporting

6.1 Report Structure

Information

OT pentest reports should include:

- Executive summary with business impact
- Methodology and scope description
- Findings with OT-specific risk ratings
- Attack path diagrams showing IT-to-OT routes
- Remediation recommendations prioritized by risk
- Compensating controls for unpatchable systems

6.2 Risk Rating Considerations

Traditional CVSS scores may not reflect OT risk. Consider:

- **Safety impact:** Could exploitation cause physical harm?
- **Production impact:** What is the cost of downtime?
- **Cascading effects:** Could compromise spread?
- **Recovery difficulty:** How hard is restoration?

7 Tools and Resources

7.1 OT-Specific Tools

Tool	Purpose
Wireshark + dissectors	Protocol analysis (Modbus, DNP3, S7)
PLCScan	PLC discovery and enumeration
Redpoint (Nmap scripts)	ICS device identification
mbtget/modbus-cli	Modbus protocol testing
GRASSMARLIN	Passive OT network mapping

8 Further Reading

Standards and Guidelines

- **IEC 62443-4-1** – Secure Product Development
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- **NIST SP 800-82 Rev. 3** – OT Security Guide
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA** – ICS Assessment Methodology
  https://www.cisa.gov/resources-tools/services/cisa-assessments

Books

- Pascal Ackerman – *Industrial Cybersecurity* (Packt)
- Clint Bodungen – *Hacking Exposed Industrial Control Systems* (McGraw-Hill)