Advanced ICS/SCADA Hacking Training

Applied Risk

Applied Risk OT Solution Snapshot

This Advanced ICS/SCADA Hacking Training teaches advanced security research methodologies and mitigation strategies to keep your Operations Technology (OT) systems cyber resilient.

During the course, participants will have the opportunity to engage in real-life attacks against key ICS/SCADA components. The course takes a deep dive into industrial protocols used within low-level ICS assets such as OPC, Profinet and Modbus in addition to discussing DNP3, Ethernet/IP, MMS, WirelessHART, ISA100.11a.

The training has been specifically designed for all staff responsible for securing ICS/SCADA systems and networks. Typically staff with functions like: Process Automation Managers/ Engineers, Control Systems Managers/Engineers, IT/OT Security Officers, Network Engineers, Penetration Testers, Forensic Researchers, System Developers as well as Auditing and Security Operations officers.

Key Takeaways

- **Methodologies through which security research may be performed against ICS/SCADA devices in order to identify zero-day vulnerabilities**
- **Real-life attack experience against key ICS/SCADA components and other Industrial Control Systems and protocols**
- **Knowledge covering how industrial hacking is executed. This will enable you to better protect your operations against hacking activities**

Course Content

The Advanced ICS/SCADA Hacking training consists of the following modules:

- Overview, trends and threats
- Securing Your ICS/SCADA
- Open Source Intelligence (OSINT)
- Attacking devices – Identify & exploit
- Hacking Windows-based systems
- Ransomware – Delivery & impacts
- Hacking SCADA Applications
- Hardening Legacy OPC applications
- Fuzzing & abusing industrial protocols
- Firmware Reverse Engineering
- Incident Response – Stages and tools

Get in touch.

info@applied-risk.com
www.applied-risk.com
+31 (0)20 833 4020

Teleportboulevard 110,
1043 EJ Amsterdam