Expert Hacker - SM (EHSM)

Training Syllabus

IL Hack Institute: Expert Hacker – SCADA Master (EHSM)
5 Days Training.

Day 1:

- Introduction to SCADA
  - SCADA in general
  - Regular security VS SCADA security
  - SCADA security approach
  - Best practice & Policies
  - Physical security

- DMZ
  - The different networks
  - The different access options
  - Remote access
  - Separation of applications
  - Common DMZ mistakes
  - How to manage SCADA DMZ's
  - Vendors access

- Day 1 Lab

Day 2:

- The AAA's of SCADA
  - Authentication
  - Roll / Location authentication
  - Authorization
  - Accounting

- AAA's and more
  - Application integration
  - Identification
  - Users and passwords management
  - Policies and enforcement
  - Standards of AAA in SCADA
  - Methodologies

- Day 2 Lab

Day 3:

- Protocols
  - SCADA proprietary protocols
  - The new age of SCADA protocols
  - SCADA networks
  - SCADA and Microsoft
- Protection by software
  - Anti Virus, IDS, IPS and more
  - Patch management

- Day 3 Lab

Day 4:

- Penetration test for SCADA
  - Fundamentals of penetration tests in SCADA
  - Vulnerability assessments
  - Tools of the trade
  - Spoofing in SCADA
  - Logs collection and analysis
  - Exceptions

- Exploits and Vulnerabilities
  - Fuzzing SCADA systems
  - Fuzzing SCADA protocols
  - Exploits for SCADA
  - Metasploit in SCADA

- Day 4 Lab

Day 5:

- Material wrap up
- Conclusive lab
- Preparation for the SCADA EHSM exam