ICS Penetration Testing

Index: **RT431**
Duration: **40 hours**

Description

The ICS Penetration Testing program was constructed primarily for the security industry and was meant to equip participants with advanced techniques and information warfare. Energy companies, telecommunications, transportation, healthcare, and many other such industries are perceived as critical infrastructure for the continual maintenance of the state. SCADA (Supervisory Control and Data Acquisition) systems are considered the "weak link" in the defense chain, for reasons you will discover throughout the training. This training covers possible attack methods by hostile entities and the security challenges that naturally follow. Cyberwarfare is one of the most fascinating and advanced disciplines in the Cyber Security world.

Target Audience

- OT
- Incident responders
- Cyber forensics investigators

Pre-requisites

- ThinkCyber Level-2 Courses

Objectives

- Various aspects of cyber-warfare on the defensive side
- Expand ICS knowledge in both methodologies and required techniques

Module 1: ICS overview

During this module, students will learn cybersecurity in the environment of Industrial Control Systems. Students will learn how a control system can be attacked from the internet and perform hands-on practice sessions on network discovery techniques.

- IT vs. OT
- Types of ICS Systems
  - DCS vs. SCADA
- SCADA components
  - Human Machine Interface (HMI)
  - Supervisory System
  - Remote Terminal Units (RTUs)
  - Programmable Logic Controller (PLCs)
- ICS security overview
  - Basic Security Concepts
  - Physical Security
  - Digital Security
  - ICS Lifecycle Challenges
- ICS Network Architectures
- Known ICS Protocols
  - Modbus
  - DNP3
  - How to Approach Protocols Research
  - ICS Protocol Fuzzing

Module 2: ICS Attacks & Vulnerabilities

During this module, students will be trained on network discovery using Metasploit and practicing in hands-on Red Team exercises. In this module, we will cover the ways to attack the SCADA environment. Students will develop a broader understanding of where these specific attack vectors exist, as well as the tools that are used to discover vulnerabilities.

- Security in ICS
    - Encryption
    - Firewalls with ICS
    - DMZ Approach
    - Access Control
    - Intrusion Detection (IDS)
- Web Application Attacks
    - Brute Force
    - Extracting Data
    - SQL Injection
- ICS Exploitation using Metasploit
    - Metasploit modules for SCADA
    - Exploit with Metasploit
    - Control with Metasploit
- ICS Attack Tools
    - Modscan
    - SMOD
- Network attacks
    - Flooding
    - MiTM
    - Denial of Service (DoS)
    - Jamming
    - Wi-Fi Security Issues
- Attacks on HMI
    - ICS Security Framework
    - Brute Force

Module 3: ICS Penetration Testing

In this module, we will present students' ways to plan, design, and implement an effective program to protect SCADA systems using Penetration Testing methods. Students will gain knowledge of conducting these tests on the "Test-environment" using advanced techniques.

- Preparing for Penetration Testing
    - Setting up a Virtual Machine for Penetration Testing
    - Creating your VM Network
    - Architectures Overview
- Testing your Network
    - Gathering Information Passively
    - Port Scanning
    - System Fingerprinting
    - Passwords Complexity Testing
    - Administrator Privileges Escalation Testing
- Testing for Vulnerabilities on Master Servers
    - Checking for Vulnerabilities
    - Analyzing Services and Ports
    - Analyzing Communications
- Testing for Vulnerabilities on User Interfaces
    - Web Applications
        - Identifying Attacks
        - Exploiting Vulnerabilities
        - PHP Vulnerabilities
    - Terminal Interfaces
    - Traditional Applications
- Testing for Vulnerabilities on Network Protocols
    - Breaking Open Network Protocols
    - Protocol Analysis
    - Using Network-Based Signatures
    - Radio Frequency Capture
    - Sniffing Network Traffic
    - Extracting Network Traffic
- Testing for Vulnerabilities in Embedded devices
    - Firmware Fuzzing
    - Analyzing the Firmware
    - Exploiting Firmware Vulnerabilities
- Security Assessment
- Writing a Penetration Testing Report