SDA.ACADEMY
Cybersecurity training

THINKCYBER

Syllabus

ICS/SCADA Penetration Testing

CYBERIUM ARENA

-SIMULATOR-

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 state's continual maintenance. 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.

The course helps prepare for the certification exams CSSA (INFOSEC) and GICSP (SANS).

Target Audience

The course targets participants with cybersecurity knowledge that want to master penetration knowledge in critical infrastructure.

Pre-requisites

Linux

Penetration

Objectives

- Hands-on with critical infrastructure protocols and vulnerabilities
- 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.

ICS Network

- Types of ICS Systems
- Human Machine Interface (HMI)
- Supervisory System
- Remote Terminal Units (RTUs)
- Programmable Logic Controller (PLCs)
- Basic Security Concepts
- Physical Security
- Digital Security
- ICS Lifecycle Challenges
- ICS Network Architectures
- Known ICS Protocols
- ICS Protocol Fuzzing

Module 2: ICS Attacks and Vulnerabilities

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

Security in ICS

- Encryption
- Firewalls with ICS
- DMZ Approach
- Access Control
- Intrusion Detection (IDS)
- Web Application Attacks

Metasploit

- ICS Exploitation using Metasploit
- Metasploit modules for SCADA
- Exploit with Metasploit
- Control with Metasploit
- ICS Attack Tools
- ICS Scanning Tools
- Denial of Service (DoS)
- Wi-Fi Security Issues
- Attacks on HMI

Module 3: ICS Penetration Testing

In this module, students will get familiar with 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

Vulnerabilities

- Checking for Vulnerabilities
- Analyzing Services and Ports
- Analyzing Communications
- Testing for Vulnerabilities on User Interfaces
- Searching for Web Applications Vulnerabilities
- Testing for Vulnerabilities on Network Protocols
- Protocol Analysis
- Using Network-Based Signatures
- Sniffing Network Traffic
- Testing for Vulnerabilities in Embedded devices
- Firmware Fuzzing
- Analyzing the Firmware
- Exploiting Firmware Vulnerabilities
- Security Assessment