SDA.ACADEMY
Cybersecurity training

THINKCYBER

Syllabus

ICS/SCADA Forensics

CYBERIUM ARENA

-SIMULATOR-

Description

Organizations, both civilian and government, are trying to build security teams to protect the ICS/SCADA environment. The program was designed comprehensively and professionally to impart the skills and knowledge required to integrate into the information security world's key positions, both in defense and attack teams. Participants will learn about the security threats that are unique to ICS/SCADA systems and the inherent weaknesses and vulnerabilities in Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) through the use of real-world examples, the frameworks and standards available to help develop an effective ICS/SCADA cyber-security strategy.

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 the forensics knowledge in the critical infrastructure.

Pre-requisites

Linux

Forensics

Objectives

- Understand ICS networks on a deep level
- Monitor user and system activities on the ICS network to recognize patterns of typical attacks
- Analyze abnormal activity patterns
- Using tools for intrusion detection
- Analyze log files and log data

Module 1: ICS Risk Assessment

During this module, students will learn the world of 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

- Known ICS Protocols
- Modbus
- DNP3
- How to Approach Protocols Research
- ICS Protocol Fuzzing
- Host Configuration Overview
- Wireless Access Overview
- Remote Access Overview
- Cyber-Security for ICS
- Passive Discovery
- Active Discovery
- Passive Enumeration
- Using CSET
- Ladder Logic Overview
- Using Metasploit Framework
- Web Hacking Techniques

Module 2: Security Methods and Products

This module will present students' ways to plan, design, and implement an effective program to protect SCADA systems. Students will understand common Industrial Control Systems (ICS) threats, vulnerabilities, and risks.

ICS Protection Concepts

- Endpoint Defenses
- Passive Solutions
- Agents
- Update and Patching
- Hardening Configuration
- Auditing Log Management

Network Fundamentals

- TCP/IP Protocol Suite
- ICS Protocols over TCP/IP
- Firewalls
- Building an ICS/SCADA Honeypots

Module 3: ICS Network Analysis

ICS network analysis evolves around the extraction, analysis, and identification of a user's online activities; the findings include artifacts such as logs and history files, cookies, cached content, and any remnants of the information left inthecomputer's volatile memory. During this module, participants will identify different user-behavior patterns. Upon completion of this stage, they will perform a detailed forensic analysis of the network traffic.

Wireshark Analysis

- Wireshark Tool Inspection
- Using Display Filters
- Advanced Usage
- Extracting Files from PCAP Files
- Reading Encrypted Data with Wireshark
- Attack Analysis

Advanced Packet Analysis

- Bro
- Bro-Cut
- Open-Source Tools

Identifying Attacks

- Dump Memory from Devices
- Network Scanning
- MiTM
- Brute-Force
- Injections
- Web Server Attacks
- Extracting Network Traffic from Memory
- Firewall Findings