

Getting Started in ICS/OT Cyber Security

Lab Manual



Contents

Part 1: Course Introduction.....	4
Exercise 1.1: Setting Up VMware Workstation for Personal Use	4
Exercise 1.2 Installing Python on Windows	5
Exercise 1.3 Installing PIP	5
Part 2: ICS/OT Cyber Security Overview	7
Exercise 2.1: Top Critical Controls for ICS/OT Cyber Security.....	7
Part 3: Main Types of Control Systems & Protocols.....	9
Exercise 3.1: Installing a Modbus Server & Client.....	9
Exercise 3.2: Installing Wireshark.....	11
Exercise 3.3: Capturing Network Traffic with Wireshark.....	12
Exercise 3.4: Using Wireshark Statistics	15
Exercise 3.5: Inspecting TCP/IP Traffic in Wireshark	16
Exercise 3.6: Inspecting ICS/OT Protocols in Wireshark.....	17
Part 4: Secure Network Architecture	19
Exercise 4.1: The Expanded Purdue Model.....	19
Exercise 4.2: Reviewing IT/OT DMZ Access Control Lists (ACLs)	21
Part 5: Asset Registers and Control Systems Inventory.....	22
Exercise 5.1: Building an Asset Register with System Configs.....	22
Exercise 5.2: Building an Asset Register with Packet Captures	26
Part 6: Threat & Vulnerability Management.....	27
Exercise 6.1: Building an IT Host Scanning Target	27
Exercise 6.2: Active Scanning	27
Exercise 6.3: Scanning for IT Vulnerabilities.....	30
Part 7: OSINT for Control Systems.....	32
Exercise 7.1: Google Searches.....	32
Exercise 7.2: Using WHOIS for OSINT.....	35
Exercise 7.3: Using DNS for OSINT	36
Exercise 7.4: Using LinkedIn for OSINT.....	36
Exercise 7.5: Using Shodan for OSINT	37
Part 8: Incident Detection & Response	40
Exercise 8.1: Backdoors & Breaches (ICS OT Core Deck).....	40
Part 9: Industry Standards & Regulations	41

Part 10: Introduction to ICS/OT Penetration Testing.....	42
Appendix B: List of Resources (Books)	53