Industrial Control Systems Cybersecurity (301) Training

Student Guide

January 2016

Homeland Security

AGENDA
Industrial Control Systems Cyber Security (301) Training
Idaho Falls, Idaho
January 11 - 15, 2016

	Monday	Tuesday	Wednesday	Thursday	Friday
7:00 AM					
8:00-8:15 AM	Introductions	Active Discovery	Network Exploitation	8:00 AM - 12:00 Noon Red / Blue Exercise	Exercise Debrief
8:15-8:30 AM	DHS Overview	Vulnerability Scanner			
8:30-8:45 AM			Basic Web Hacking		
8:45-9:00 AM		Discovery Review			
9:00-9:15 AM	ICS 101	Metasploit	Man-in-the-Middle		
9:15-9:30 AM		Terminology - Vulnerabilities & Exploits			
9:30-9:45 AM			Password and Hashes		Break
9:45-10:00 AM					Exercise Debrief (cont)
10:00-10:15 AM	Break	Break			
10:15-10:30 AM	ICS Threat/Risks		Break		
10:30-10:45 AM		Basic Exploitation Process	Network Defense		
10:45-11:00 AM					
11:00-11:15 AM					
11:15-11:30 AM		Remote Exploits			
11:30-11:45 AM					11:30 AM - 12:00 Noon Lunch Round table perspectives; leave to catch plane if needed or discuss week with new contacts
11:45 AM - 12:00 Noon					
12:00 Noon - 12:15 PM	12:00 Noon - 12:30 PM Lunch	12:00 Noon - 12:30 PM Lunch	12:00 Noon - 12:30 PM Lunch	12:00 Noon - 12:30 PM Lunch	
12:15-12:30 PM					
12:30-12:45 PM	Working Lunch Presentation "Black Energy"	Working Lunch Presentation "ICS-CERT"	Working Lunch Presentation "AAL"	Blue Team All-Hands Meeting	End
12:45-1:00 PM					
1:00-1:15 PM	Exploit Demonstration	Metasploit - continued	Logging & Log Analysis	1:00 - 5:00 PM Red / Blue Exercise	
1:15-1:30 PM		Client Side Exploits			
1:30-1:45 PM					
1:45-2:00 PM		Payloads	Network Architecture		
2:00-2:15 PM	Network Discovery				
2:15-2:30 PM		Meterpreter			
2:30-2:45 PM			Network Flow Data		
2:45-3:00 PM	Basic Networking Topics	Pcap Forensics			
3:00-3:15 PM	Break				
3:15-3:30 PM	Passive Discovery	Break	Break		
3:30-3:45 PM	Host Discovery	Separate into Red & Blue			
3:45-4:00 PM		Initial Briefings			
4:00-4:15 PM	Active Discovery		Red Team / Blue Team Strategy Meetings		
4:15-4:30 PM	Nmap	Red Team / Blue Team Strategy Meetings			
4:30-4:45 PM					
4:45-5:00 PM					
5:00 PM	Optional–tcpdump & wireshark	Red Team / Blue Team Strategy Meetings (Optional)	Red Team / Blue Team Strategy Meetings (Optional)	Turn in Playbooks Exercise Results End	
6:00 PM	End	End	End		

Industrial Control Systems Cybersecurity (301) Training

Student Guide

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
U.S. Department of Homeland Security

Homeland Security

CONTENTS

Course Introduction 7

Session 1: Industrial Control Systems Overview 10
LO1: Describe basic industrial control systems 10
SCADA or DCS? 10
Embedded Systems 11
Embedded Systems Components 11
Embedded Systems used in ICS 11
ICS Basics 12
Field Controllers – Environmental 13
Field Controllers – Hardware 13
Field Controllers – Programs 14
Data Flow in ICSs 15
Network Models 16
Protocols (partial list) 16
OPC 17
Why is OPC Popular? 17
Modbus 18
RTU Modbus Messages 18
Protocol Vulnerabilities: Expediting Attack Success 19
Manipulation of the System 19
Manipulation of the System 20
Considerations 20
Basic ICS Review 20
LO2: Discuss cyber risks to industrial control systems 21
Threat Trends for Control Systems 21
The Risk Curve 22
Incidents of Suspected or Confirmed Cyber Attacks 23
Identify Vulnerable Components 24
Identify Threat Vectors 24
Identify Mitigations 25
Exposure 25
Cyber Risk Review 26
Review of Session 1 26

Session 2: Process Control Attack Demonstration 28
LO3: Discuss the process control exploit demonstration 28
Demo Exploit Path 30
Attack Stage 1 – Internet to Corporate 30
Attack Stage #2 – Reconnaissance 31
Attack Stage #2 – Corporate to DMZ 31

Attack Stage #3 – Reconnaissance 32
Attack Stage #3 – DMZ to Control LAN 32
Attack Stage #3 – Pretty Pictures (HMI) 33
Attack Sends Commands to PLC 33
Demo Exploit Path 34
Demo System Vulnerabilities 34
ICS: Traditional Isolation 35
ICS: Modern Connectivity 36
Inherent Vulnerabilities 37
Review of Session 2 39

Session 3: Network Discovery and Mapping 41
LO4: Explain basic networking concepts necessary for active and passive network discovery 41
Basic Networking 41
Basic Networking Components 41
Basic Packet Traversal 42
LO5: Discuss passive discovery 46
Passive Discovery 46
Network Layout 55
IP Address 55
Tools – Kali 56
Basic Linux Shell Commands 58
Passive Discovery Hands-on Exercise 59
More Passive Discovery 64
Tcpdump and Wireshark Hands-on Exercise 74
Passive Discovery Review 81
LO6: Discuss active discovery 82
Active Discovery 82
Active Discovery: Nmap Hands-on Exercise 93
Active Discovery: Nessus and OpenVAS Hands-on Exercise 99
Review of Session 3 100

Session 4: The Exploitation Process & Using Metasploit 101
LO7: Discuss the three main stages of an attack 101
Target Development (TD) 102
Exploitation and Pivoting 104
Attacker's Trifecta 104
Types of Vulnerabilities 104
Software Vulnerabilities and Exploits – A Brief History 105
History & Exploitability: Language 106
Typical Program Flow 107
Exploitability Example 1 (C-Style) 107

Attacker Controlled Program Flow 107
Vulnerability Severity 109
Exploits Types 110
Exploitation Process 112
Attack Operations 114
Bypass Network Controls 114
Command and Control 115
Persistent and/or Remote Access 116
Summary 117
LO8: Describe Metasploit 118
MS Framework 118
Terminology 118
The Basic Exploit Process 119
MSF: Useful Commands 119
MSF Payloads Overview 119
MSF Payloads: OS Targets 120
MSF Payloads: Actions 120
MSF Payloads: Modifiers 120
Meterpreter: Useful Commands 120
Meterpreter Routing 121
LO9: Use the Metasploit framework 122
Class Customizations to Metasploit and Kali Hands-on Exercise 122
Exercise #5: Armitage 139

Session 5: Network Attacks and Exploits 143
LO10: Discuss the basic web hacking techniques 143
What is the web? 143
HTML 143
JavaScript 143
XSS (Cross-Site Scripting) 144
XSS Demonstration 144
XSS Defenses 144
PHP 144
SQL 144
SQLi 145
Web Injection Demonstration 145
SQLi Defenses 145
LO11: Describe password security 146
Passwords and Hashes 146
Password Crackers 146
Password Cracking: Brute Force 146
Password Cracking: Rainbow Tables 147

John the Ripper 147
Salting Passwords 147
Using Salted Passwords 147
LO12: Discuss wireless attacks and exploits 149
WEP Cracking 149
Basic Web Hacking Exercise 149
Review of Session 5 167

Session 6: Network Defense, Detection, and Analysis 169
LO13: Describe the components for defense in depth. 170
Defense-in-Depth Security 171
Network Architecture 172
Firewall Implementation 174
Data Diodes 176
Proxy Servers 180
Intrusion Detection/Prevention Systems 182
Intrusion Prevention Systems (IPSs) vs. Intrusion Detection Systems (IDSs) 183
Potential Complications 183
Intrusion Detection Systems 183
Host Intrusion Detection System (HIDS) 184
Network Intrusion Detection System (NIDS) 184
IDS Sensor Placement 185
NIDS: Tapping the Network 186
Logging Architecture 187
Network Architecture Exercise 189
LO14: Describe detection in depth – perimeter network 192
Firewall and VPN Logs 192
Proxy Logs 193
Netflow Anomaly Detection 195
Intrusion Detection/Prevention Systems - Perimeter 196
Expectations for All IDS 197
Signature vs. Anomaly Detection 197
Snort Rule Dissection 197
Snort Rule Headers 198
Snort Rule Metadata Options 199
Payload Options 200
This rule alerts ONLY for those packets containing the string "cmd.exe." 202
DNP3 Preprocessor Rule Options 202
DNP3 Preprocessor 203
Modbus Preprocessor Rule Options 203
Snort Output Plugins 204
Resources for ICS Vulnerability and IDS Signature Information 205

Example Rules 205
Network Defense, Detection, and Analysis Hands-on Exercises 207
LO15: Describe detection in depth – mid-layer 212
Web and System Logs 212
Log Sources 212
Windows System Logs 212
Linux System Logs (Syslog) 213
Honey Pot – A Decoy System 216
Antivirus, Host Based IDS (HIDS) 218
LO16: Describe the components of change detection. 219
Application Logs 219
Application IDS/IPS/Firewall 220
Web Application Firewall 221
Integrity Checking 222
Application Whitelisting 223
LO17: Describe the components of cybersecurity management. 225
Security Controls 225
Security Risk Management 225
Mitigation Strategies 226
Operations Security (OPSEC) 227
What are you telling the world? 228
Supply Chain Considerations 228
Fault Trees and Attack Trees 229
Fault Tree Analysis 229
Attack Tree Analysis – INL Demo 231
Cost without Defense 231
Cost with Defense 232
Attackers Expertise – No Defense 232
Attackers Expertise with Defense 233
Incident Response 233
Cybersecurity Incident First Aid 234
Incident Response gone WRONG! 235
Review of Session 6 236
Review and Exercise Preparation 237
Appendix A: Further Reading/Resources 240
Appendix B: Opensource Pcap Compatible Tools 248
Appendix C: Understanding the Hacker's Mind 250
Appendix D: More Tshark and TCPdump 263
Appendix E: Industry-based Information Sharing and Analysis Centers (ISACs) 268
Appendix F: WHO TO CONTACT 274
Appendix G: ACRONYM LIST 275

Course Introduction

Welcome to the Industrial Control Systems Cybersecurity (301) Training course. This course provides intensive hands-on training on protecting and securing industrial control systems from cyber attacks including a Red Team / Blue Team exercise that will be conducted within an actual control systems environment.

In order to understand how best to defend a system, participants will learn about common vulnerabilities. Knowing the weaknesses of a system will enable participants to provide the fixes and institute the policies and programs that will provide defense in depth needed to ensure more secure industrial control systems in their work environments.

The course is split into the following six sessions, followed by the Red Team/Blue Team hands-on exercise.

1. Industrial Control System Overview
2. Process Control Attack Demonstration
3. Network Discovery and Mapping
4. The Exploitation Process and Using Metasploit
5. Network Attacks and Exploits
6. Network Defense, Detection, and Analysis

In addition, working lunch presentations will provide focus on common vulnerabilities, the ICS-CERT Program, and the Cyber Security Evaluation Tool (CSET®).

Course Objectives:

At the end of this course, attendees will be able to:

Session 1: Industrial Control System Overview

- Describe basic industrial control systems
- Discuss cyber risks to industrial control systems

Session 2: Process Control Attack Demonstration

- Discuss the process control exploit demonstration

Session 3: Network Discovery and Mapping

- Explain basic networking concepts necessary for active and passive network discovery
- Discuss passive discovery
- Discuss active discovery

Session 4: The Exploitation Process and Using Metasploit

- Discuss the three main stages of an attack
- Describe Metasploit
- Use the Metasploit framework

Session 5: Network Attacks and Exploits

- Discuss basic web hacking techniques
- Describe password security
- Discuss wireless attacks and exploits

Session 6: Network Defense, Detection, and Analysis

- Describe the components for defense in depth
- Describe detection in depth - perimeter network
- Describe detection in depth - mid-layer
- Describe the components of change detection
- Describe the components of cybersecurity management

Disclaimer

References made herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof.

The attacks and exploits shown in the demonstration are not specific to any vendor technology.

Use the described security tools and techniques at "your own risk," i.e., carefully evaluate any tool prior to using it in a production network.