2.15 INFORMATION COMMUNICATION TECHNOLOGIES – VULNERABILITY ASSESSMENT

IoT Security Technician Skill Zone – CSSIA.ORG

2. Information Communication Technologies

2.15 Vulnerability Assessment

1. Describe the purpose and use of vulnerability scanners and controls.
2. Identify the characteristics of well-known wireless and mobile device attacks.
3. Describe the security threats and vulnerabilities associated with IoT and industrial control systems.
4. Describe the penetration testing principles, tools, and techniques associated with IoT and industrial control systems.
5. Demonstrate the use of penetration testing tools, and techniques used to conduct vulnerability scanning associated with IoT and ICS.

Configuration Management

Vulnerability Assessment is the process of identifying and analyzing vulnerabilities within an organization's information management systems. Vulnerability assessment can include scanning for network, host, operating systems, applications and services vulnerabilities. The IoT security technician needs to be knowledgeable of resources like the National Vulnerability Exploit Database and resources published by specific vendors that detail vulnerabilities associated with their products.

The IoT security technician needs to be familiar with and able to use tools like vulnerability scanners, product hardening tools and application vulnerability analyzers. A common process used to identify vulnerabilities would be penetration testing. Pen testing can identify current vulnerabilities and enable the technician to analyze the risk posed by specific vulnerabilities.

2.15 INFORMATION COMMUNICATION TECHNOLOGIES – VULNERABILITY ASSESSMENT

Existing Course Cross Reference

Cisco Networking Academy Courses

Cisco Cybersecurity Essentials

CCNA Security

Cisco Partner Courses

Security+ (CSSIA.ORG)

Ethical Hacking and Penetration Testing (NDG/CSSIA)

Python Programming for Security Technicians (CSSIA.ORG)

IoT and ICS Security Controls (CSSIA.ORG)

ICS and SCADA Security (CSSIA.ORG)

CISSP (CSSIA.ORG)

Curriculum Resources

Videos

YouTube.com – Configuration Management

YouTube.com – Cisco Nessus Configuration Management

Web Links

Configuration Management: Best Practices White Paper

SANS Institute InfoSec Reading Room, Secure Configuration Management Demystified

NIST Special Publication 800-82 Section 6.2

Textbooks

Practical Internet of Things Security
Chapter 2, 3, 4, 7, 8

Internet of Things
Chapter 10, 11

NIST Special Publication 800-82 Revision 2
Guide to Industrial Control Systems (ICS) Security

Cyber-security of SCADA and Other Industrial Control Systems
Edward J. M. Colbert, Alexander Kott, 2016
ISBN 9783319321257

Assessment Resources

Labs

None

Quizzes/Exams

CSSIA CISSP Course

Security Operations – Chapter Exam

Quizlet.com

Configuration Management Flashcards

Configuration Planning and Management flashcards