EET-4100: NETWORK SECURITY FOR MANUFACTURING

Cuyahoga Community College

Viewing: EET-4100 : Network Security for Manufacturing

Board of Trustees:

September 2023

Academic Term:

Fall 2024

Subject Code

EET - Electrical/Electronic Engineer

Course Number:

4100

Title:

Network Security for Manufacturing

Catalog Description:

The Network Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of manufacturing network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure. In this course, the student will learn the necessity of a comprehensive security policy and how it affects the strength of the network and to protect the industrial manufacturer’s data from theft, damage, or disruption. The student will also learn to perform basic tasks to secure a small industrial network. Students will be prepared to sit for a corresponding Cisco Badge.

Credit Hour(s):

4

Lecture Hour(s):

2

Lab Hour(s):

4

Requisites

Prerequisite and Corequisite

EET-3100 Manufacturing Networking Devices.

Outcomes

Course Outcome(s):

Evaluate key terms and concepts of network security for manufacturing.

Objective(s):

1. Assess mitigation methods for common network attacks.
2. Evaluate mitigation methods for Worm, Virus, and Trojan Horse attacks.
3. Evaluate the Cisco Self Defending Network architecture.
4. Evaluate processes used to mitigate threats to Cisco routers and networks using Access Control Lists (ACLs).
5. Evaluate types of physical security.
6. Evaluate and recommend types of application security.
7. Evaluate a Manufacturing Network Hardening.
8. Execute and recommend a Bootstrap the Cisco Adaptive Security Appliance (ASA) Firewall for use in a production network.
9. Explain and assess how a network can be compromised using freely available tools.
10. Explain and assess the behavior of common network protocols in the context of security monitoring.
11. Evaluate Authentication, Authorization, and Accounting (AAA) concepts and features using the local database as well as Cisco Secure ACS 5.2.

12. Evaluate the role of cryptography in ensuring authenticity of data.
13. Evaluate a virtual tunnel interface using GRE (Generic Routing Encapsulation) with IPSec.

Course Outcome(s):

Construct, evaluate, and implement network security for manufacturing infrastructure.

Objective(s):

1. Recommend and implement secure network management for reporting Mitigate common Layer 2 attacks.
2. Recommend and implement the Cisco IOS firewall features.
3. Recommend and implement the Cisco IOS IPS features.
4. Recommend and implement site-to-site VPNs on Cisco Routers.
5. Evaluate and construct the Cisco ASA Firewall for remote access SSL VPN.
6. Evaluate and construct a Cisco IOS zone-based firewall (ZBF) to perform basic security operations on a network.
7. Evaluate and construct site-to-site VPNs using Cisco IOS features.
8. Evaluate and construct security features on IOS switches to mitigate various Layer 2 attacks.
9. Implement line passwords, and enable passwords and secrets.
10. Construct packet filtering on the Perimeter Router.
11. Develop a Smart Manufacturing network security policy base to counter threats against information security.
12. Design, implement, and support security for Smart Manufacturing devices and data.
13. Design and implement configuration of industrial routers and switches with Cisco IOS Software security attributes.
14. Configure site-to-site VPNs using Cisco IOS.
15. Perform basic security operations on an industrial network by configuring a Cisco IOS zone-based firewall.
16. Configure an Intrusion Prevention System (IPS) on industrial network routers and switches.
17. Configure IPv6 ACL.

Methods of Evaluation:

1. Homework
2. Laboratory experiments and reports
3. Midterm examination
4. Final examination

Course Content Outline:

1. Networking Security Concepts
    a. Foundation Topics
    b. Understanding Network and Information Security Basics 6
        i. Network Security Objectives
        ii. Confidentiality, Integrity, and Availability
        iii. Cost-Benefit Analysis of Security
        iv. Classifying Assets
        v. Classifying Vulnerabilities
        vi. Classifying Countermeasures
        vii. What Do We Do with the Risk?
    c. Recognizing Current Network Threats
        i. Potential Attackers
        ii. Attack Methods
        iii. Attack Vectors
        iv. Man-in-the-Middle Attacks
        v. Other Miscellaneous Attack Methods
    d. Applying Fundamental Security Principles to Network Design
        i. Guidelines
        ii. Network Topologies
        iii. Network Security for a Virtual Environment
        iv. How It All Fits Together
2. Common Security Threats

- a. Foundation Topics
- b. Network Security Threat Landscape
- c. Distributed Denial-of-Service Attacks
- d. Social Engineering Methods
    - i. Social Engineering Tactics
    - ii. Defenses Against Social Engineering
- e. Malware Identification Tools
    - i. Methods Available for Malware Identification
- f. Data Loss and Exfiltration Methods

3. Implementing AAA in Cisco IOS
    - a. Foundation Topics
    - b. Cisco Secure ACS, RADIUS, and TACACS
        - i. Why Use Cisco ACS?
        - ii. On What Platform Does ACS Run?
        - iii. What Is ISE?
        - iv. Protocols Used Between the ACS and the Router
        - v. Protocol Choices Between the ACS Server and the Client (the Router)
    - c. Configuring Routers to Interoperate with an ACS Server
    - d. Configuring the ACS Server to Interoperate with a Router
    - e. Verifying and Troubleshooting Router-to-ACS Server Interactions
4. Bring Your Own Device (BYOD)
    - a. Foundation Topics
    - b. Bring Your Own Device Fundamentals
    - c. BYOD Architecture Framework
        - i. BYOD Solution Components
    - d. Mobile Device Management
        - i. MDM Deployment Options
        - ii. On-Premise MDM Deployment
        - iii. Cloud-Based MDM Deployment
5. Fundamentals of VPN (Virtual Private Network) Technology and Cryptography
    - a. Foundation Topics
    - b. Understanding VPNs and Why We Use Them
        - i. What Is a VPN?
        - ii. Types of VPNs
        - iii. Two Main Types of VPNs
        - iv. Main Benefits of VPNs
        - v. Confidentiality
        - vi. Data Integrity
        - vii. Authentication
        - viii. Antireplay Protection
    - c. Cryptography Basic Components
        - i. Ciphers and Keys
        - ii. Ciphers
        - iii. Keys
        - iv. Block and Stream Ciphers
        - v. Block Ciphers
        - vi. Stream Ciphers
        - vii. Symmetric and Asymmetric Algorithms
        - viii. Symmetric
        - ix. Asymmetric
        - x. Hashes
        - xi. Hashed Message Authentication Code
        - xii. Digital Signatures
        - xiii. Digital Signatures in Action
        - xiv. Key Management
        - xv. Next-Generation Encryption Protocols
        - xvi. IPsec and SSL

   d. Implementing and Verifying an IPsec Site-to-Site VPN in Cisco
      i. Troubleshooting IPsec Site-to-Site VPNs in Cisco ASA

8. Implementing SSL VPNs Using Cisco ASA
   a. Foundation Topics
   b. Functions and Use of SSL for VPNs
      i. Is IPsec Out of the Picture? 206
      ii. SSL and TLS Protocol Framework 207
      iii. The Play by Play of SSL for VPNs 207
      iv. SSL VPN Flavors 208
   c. Configuring Clientless SSL VPNs on ASA
      i. Using the SSL VPN Wizard
      ii. Digital Certificates
      iii. Accessing the Connection Profile
      iv. Authenticating Users
      v. Logging In
      vi. Seeing the VPN Activity from the Server
   d. Using the Cisco AnyConnect Secure Mobility Client
      i. Types of SSL VPNs
      ii. Configuring the Cisco ASA to Terminate the Cisco AnyConnect Secure Mobility Client Connections
      iii. Groups, Connection Profiles, and Defaults
      iv. One Item with Three Different Names
      v. Split Tunneling
   e. Troubleshooting SSL VPN
      i. Troubleshooting SSL Negotiations
      ii. Troubleshooting AnyConnect Client Issues
      iii. Initial Connectivity Issues
      iv. Traffic-Specific Issues

9. Securing Layer 2 Technologies
   a. Foundation Topics
   b. VLAN and Trunking Fundamentals
      i. What Is a VLAN?
      ii. Trunking with 802.1Q
      iii. Following the Frame, Step by Step
      iv. The Native VLAN on a Trunk
      v. So, What Do You Want to Be? (Asks the Port)
      vi. Inter-VLAN Routing
      vii. The Challenge of Using Physical Interfaces Only
      viii. Using Virtual Sub Interfaces
   c. Spanning-Tree Fundamentals
      i. Loops in Networks Are Usually Bad
      ii. The Life of a Loop
      iii. The Solution to the Layer 2 Loop
      iv. STP Is Wary of New Ports
      v. Improving the Time Until Forwarding
   d. Common Layer 2 Threats and How to Mitigate Them 246
      i. Disrupt the Bottom of the Wall, and the Top Is Disrupted, Too 246
      ii. Layer 2 Best Practices 246
      iii. Do Not Allow Negotiations 247
      iv. Layer 2 Security Toolkit 248
      v. Specific Layer 2 Mitigation for CCNA Security
      vi. BPDU Guard
      vii. Root Guard
      viii. Port Security
   e. CDP and LLDP
   f. DHCP Snooping
   g. Dynamic ARP Inspection

10. Network Foundation Protection
   a. Foundation Topics 264
   b. Using Network Foundation Protection to Secure Networks 264

        i. The Importance of the Network Infrastructure
        ii. The Network Foundation Protection Framework
        iii. Interdependence
        iv. Implementing NFP 265
    c. Understanding the Management Plane
        i. First Things First
        ii. Best Practices for Securing the Management Plane
    d. Understanding the Control Plane
        i. Best Practices for Securing the Control Plane
    e. Understanding the Data Plane
        i. Best Practices for Protecting the Data Plane
        ii. Additional Data Plane Protection Mechanisms

11. Securing the Management Plane on Cisco IOS Devices 275
    a. Foundation Topics 278
    b. Securing Management Traffic 278
        i. What Is Management Traffic and the Management Plane?
        ii. Beyond the Blue Rollover Cable
        iii. Management Plane Best Practices
        iv. Password Recommendations
        v. Using AAA to Verify Users
        vi. AAA Components
        vii. Options for Storing Usernames, Passwords, and Access Rules
        viii. Authorizing VPN Users
        ix. Router Access Authentication
        x. The AAA Method List
        xi. Role-Based Access Control
        xii. Custom Privilege Levels
        xiii. Limiting the Administrator by Assigning a View
        xiv. Encrypted Management Protocols
        xv. Using Logging Files
        xvi. Understanding NTP
        xvii. Protecting Cisco IOS Files
    c. Implementing Security Measures to Protect the Management Plane
        i. Implementing Strong Passwords
        ii. User Authentication with AAA
        iii. Using the CLI to Troubleshoot AAA for Cisco Routers
        iv. RBAC Privilege Level/Parser View
        v. Implementing Parser Views
        vi. SSH and HTTPS
        vii. Implementing Logging Features
        viii. Configuring Syslog Support
        ix. SNMP Features
        x. Configuring NTP
        xi. Secure Copy Protocol
        xii. Securing the Cisco IOS Image and Configuration Files

12. Securing the Data Plane in IPv6
    a. Foundation Topics
    b. Understanding and Configuring IPv6
        i. Why IPv6?
        ii. The Format of an IPv6 Address
        iii. Understanding the Shortcuts
        iv. Did We Get an Extra Address?
        v. IPv6 Address Types
    c. Configuring IPv6 Routing
        i. Moving to IPv6
    d. Developing a Security Plan for IPv6
        i. Best Practices Common to Both IPv4 and IPv6
        ii. Threats Common to Both IPv4 and IPv6

        iii. The Focus on IPv6 Security
        iv. New Potential Risks with IPv6
        v. IPv6 Best Practices
        vi. IPv6 Access Control Lists

13. Securing Routing Protocols and the Control Plane
    a. Foundation Topics
    b. Securing the Control Plane
        i. Minimizing the Impact of Control Plane Traffic on the CPU
    c. Control Plane Policing
        i. Control Plane Protection
    d. Securing Routing Protocols
        i. Implement Routing Update Authentication on OSPF
        ii. Implement Routing Update Authentication on EIGRP
        iii. Implement Routing Update Authentication on RIP
        iv. Implement Routing Update Authentication on BGP
14. Understanding Firewall Fundamentals
    a. Foundation Topics
    b. Firewall Concepts and Technologies
        i. Firewall Technologies
        ii. Objectives of a Good Firewall
        iii. Firewall Justifications
        iv. The Defense-in-Depth Approach
        v. Firewall Methodologies
        vi. Static Packet Filtering
        vii. Application Layer Gateway
        viii. Stateful Packet Filtering
        ix. Application Inspection
        x. Transparent Firewalls
        xi. Next-Generation Firewalls
    c. Using Network Address Translation
        i. NAT Is About Hiding or Changing the Truth About Source Addresses
        ii. Inside, Outside, Local, Global
        iii. Port Address Translation
        iv. NAT Options
    d. Creating and Deploying Firewalls
        i. Firewall Technologies
        ii. Firewall Design Considerations
        iii. Firewall Access Rules
        iv. Packet-Filtering Access Rule Structure
        v. Firewall Rule Design Guidelines
        vi. Rule Implementation Consistency
15. Implementing Cisco IOS Zone-Based Firewalls
    a. Foundation Topics
    b. Cisco IOS Zone-Based Firewalls
        i. How Zone-Based Firewall Operates
        ii. Specific Features of Zone-Based Firewalls
        iii. Zones and Why We Need Pairs of Them
        iv. Putting the Pieces Together
        v. Service Policies
        vi. The Self Zone
    c. Configuring and Verifying Cisco IOS Zone-Based Firewalls
        i. First Things First
        ii. Using CCP to Configure the Firewall
        iii. Verifying the Firewall
        iv. Verifying the Configuration from the Command Line
        v. Implementing NAT in Addition to ZBF
        vi. Verifying Whether NAT Is Working
16. Configuring Basic Firewall Policies on Cisco ASA 413

   a. Foundation Topics
   b. The ASA Appliance Family and Features
      i. Meet the ASA Family
      ii. ASA Features and Services
   c. ASA Firewall Fundamentals
      i. ASA Security Levels
      ii. The Default Flow of Traffic
      iii. Tools to Manage the ASA
      iv. Initial Access
      v. Packet Filtering on the ASA
      vi. Implementing a Packet-Filtering ACL
      vii. Modular Policy Framework
      viii. Where to Apply a Policy
   d. Configuring the ASA
      i. Beginning the Configuration
      ii. Getting to the ASDM GUI
      iii. Configuring the Interfaces
      iv. IP Addresses for Clients
      v. Basic Routing to the Internet
      vi. NAT and PAT
      vii. Permitting Additional Access Through the Firewall
      viii. Using Packet Tracer to Verify Which Packets Are Allowed
      ix. Verifying the Policy of No Telnet

Resources

Omar Santos, John Stuppi. *CCNA Security 210-260*. 1st . Hoboken NJ: Pearson Education, 2023.

Dirk Schaefer, Lane Thames. *Cybersecurity for Industry 4.0*. NY, NY: Springer International Publishing, 2021.

Pascal Ackerman. *Industrial Cybersecurity*. Birmingham UK: Packt Publishing, 2020.

Top of page

Key: 5118