Discipline: Computer Information Systems

Originator: James Cregg

RIVERSIDE COMMUNITY COLLEGE DISTRICT
INTEGRATED COURSE OUTLINE OF RECORD

COMPUTER INFORMATION SYSTEMS 26F

CIS-26F : Cisco Networking Security

College: RIV
Lecture Hours: 72.000
Units: 4.00
Letter Grade

Course Description

Prerequisite: None

Advisory: CIS-26B, CIS-26C and CIS-27 or CSC-27

Course Credit Recommendation: Degree Credit

Provides students with in-depth network security education and a comprehensive understanding of network security concepts. Instruction includes, but is not limited to, installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data, skills needed to develop a security infrastructure, recognize vulnerabilities to networks, and mitigate potential security threats. Course is designed to prepare students for CCNA Security Certification (IINS 640-553 exam). 72 hours lecture.

Short Description for Class Schedule

Principles of Cisco network security.

Entrance Skills:

Before entering the course, students should be able to demonstrate the following skills:

1. **CCNA-level knowledge and skills strongly recommended.**
   - **CIS-26C -** Demonstrate an understanding of switching concepts and LANdesign.
2. **Core routing and switching configuration skills recommended.**
   - **CIS-26C** - Demonstrate an understanding of switching concepts and LANdesign.
   - **CIS-26C -** Define and understanding the use of Virtual LANs.
   - **CIS-26C -** Define and describe the Spanning Tree Protocol and its benefits.
   - **CIS-26C -** Demonstrate an understanding of virtual LAN trunking protocol.
   - **CIS-26C -** Demonstrate an understanding of virtual LAN trunking protocol.

Student Learning Outcomes:

Upon successful completion of the course, students should be able to demonstrate the following skills:

1. **Demonstrate the use of security intrusion prevention systems and configure routers to watch for attacks.**
2. **Analyze and understand firewall interface configuration, encryption, and using zone-based firewalls.**
3. **Analyze and understand AAA Radius configuration,authentication, authorization and accounting components.**
4. **Design basic security policy development and implementation using VPN.**

Course Content:

1. Fundamental Principles of Secure Networks
   a. Evolution of network Security
   b. Drivers for Network Security
   c. Network Security Organizations
   d. Domains of Network Security
   e. Network Security Policies
   f. Viruses, Worms, and Trojan Horses
   g. Attack Methodologies

2. Securing Network Devices
    a. Securing Device Access
    b. Securing the Edge Router
    c. Configuring Secure Administrative Access
    d. Configuring Enhances Security for Virtual Logins
    e. Configure SSH
    f. Configuring Privilege Levels
    g. Configuring Role-Based CLI Access
    h. Monitoring and Managing Devices
    i. Using Automated Security Features
3. Authentication, Authorization, and Accounting
    a. Configuring Local AAA Authentication with CLI
    b. AAA Authentication with SDM
    c. Troubleshooting Local AAA Authentication
    d. Server-Based AAA Communication Protocols
    e. Cisco Secure ACS
    f. Cisco Secure ACS Users and Groups
    g. Configuring Server-Based AAA Authorization
4. Implementing Firewall Technologies
    a. Configuring Standard and Extended IP ACLs
    b. Topology and Flow for Access Control Lists
    c. Configuring Dynamic ACLs / Configuring Time-Based ACLs
    d. Mitigating Attacks with ACLs
    e. Securing Networks with Firewalls
    f. Firewalls in Network Design
    g. Context-Based Access Control
    h. Zone-Based Policy Firewall Operations
    i. Configuring Zone-Based Policy Firewall
5. Implementing Intrusion Prevention
    a. Host-Based IPS Implementations
    b. Network-Based Intrusion Implementations
    c. IPS Signature Characteristics
    d. Turning IPS Signature Actions and Alarms
    e. Configuring Cisco IOS IPS with CLI and SDM
    f. Verifying Cisco IOS IPS
6. Securing the Local Area Network
    a. Endpoint Security with Network Admission Control
    b. MAC Address Spoofing Attacks
    c. MAC Address Manipulation Attacks
    d. LAN Storm Attack
    e. Configuring Port Security
    f. Configuring Storm Control
    g. Configuring VLAN Trunk Security
    h. Wireless Security Considerations
    i. VoIP Security Solutions
7. Cryptographic Systems
    a. Securing Communications
    b. Cryptography
    c. Cryptanalysis
    d. Cryptology
    e. Cryptographic Hashes
    f. Integrity with MD5 and SHA-1
    g. Key Management
    h. Data Encryption Standard
    i. Advanced Encryption Standard and Algorithms
    j. Symmetric Versus Asymmetric Encryption
    k. Digital Signatures
    l. Public key Infrastructure
    m. Certificate Authorities
8. Implementing Virtual Private Networks
    a. VPN Topologies
    b. VPN Solutions
    c. Configuring a Site-to-Site GRE Tunnel
    d. IPsec VPN Components and Operation
    e. IPsec Security Protocols
    f. Internet Key Exchange
    g. Implementing Site-to-Site IPsec VPNs with CLI
    h. Configure Compatible ACLs
    i. Configure the Crypto ACLs
    j. Implementing Site-to-Site IPsec VPNs with SDM
    k. Implementing Remote-Access VPNs
    l. SSL VPNs

m. Configure VPN Client

9. Managing a Secure Network
    a. Principles of Secure Network Design
    b. Ensuring a Network is Secure
    c. Threat Identification and Risk Analysis
    d. Risk Management and Risk Avoidance
    e. Cisco Self-Defending Network
    f. Operations Security
    g. Network Security testing
    h. Business Continuity Planning and Disaster Recovery
    i. System Development Life Cycle
    j. Developing a Comprehensive Security Policy
    k. Standards, Guidelines, and Procedures
    l. Security Awareness and Training

Methods of Instruction:

Methods of instruction used to achieve student learning outcomes may include, but are not limited to, the following activities:

- Presentation of class lectures/discussions/ demonstrations in order to clarify encryption methods, Intrusion Prevention Systems (IPS), zone-based firewalls.
- Presentation of class lectures/discussions/ demonstrations in order to clarify the principles of remote access VPN server and client.
- Web-based/web-enhanced/online/distance learning tasks/activities to reinforce understanding of concepts related to Cisco security, firewalls, securing layer 2 devices.
- Laboratory activities and application assignments using NetLab and Packet tracer to develop and secure network operations.
- Projects in order to facilitate and demonstrate the acquisition of skills required to create secure networks.
- Collaborative projects/cooperative learning tasks in order to encourage students to develop and apply computer logic and team work skills.

Methods of Evaluation:

Students will be evaluated for progress in and/or mastery of student learning outcomes using methods of evaluation which may include, but are not limited to, the following activities:

- Security configurations designed to demonstrate centralized authentication, configure a ZBF firewall, Intrusion Prevention System (IPS) using Cisco IOS and SDM.
- Quizzes/examinations designed to measure students' degree of mastery of fundamental Cisco security concepts and terminology.
- Collaborative projects designed to demonstrate successful understanding and application of zone-based firewalls, securing layer 2 switches, exploring encryption methods, and configuring site-to-site IPsec VPNs.
- Computer Laboratory assignments/projects using NetLab and Packet Tracer to design and develop, security configurations.
- Final examination designed to evaluate students' overall achievement of course objectives in Cisco security concepts.

Sample Assignments:

Outside-of-Class Reading Assignments

- Students read and interact with the Cisco on-line curriculum, CCNA security text, and the CCNA lab manual.
- The lab manual provides the hands-on practice to master the skills needed to prepare for entry-level security specialist careers.
- These items must be read and understood to analyze and develop your in-depth understanding of network security principles.

Outside-of-Class Writing Assignments

- Students read and interact with the Cisco on-line curriculum, CCNA security text, and the CCNA lab manual.
- The lab manual provides the hands-on practice to master the skills needed to prepare for entry-level security specialist careers.
- Students will be tasked with written security plans, developing security training regimens and developing a cost trade-off analysis scheme to implement network security at business sites.

Other Outside-of-Class Assignments

- Students must research various network attacks that have actually occurred and select one of these and describe how the attack was perpetrated and how extensive the network outage or damage was.

Course Materials:

All materials used in this course will be periodically reviewed to ensure that they are appropriate for college level instruction. Possible texts include the following:

Paul Boger. *CCNA Security Course Booklet.* Version 1.0 Cisco Press, 2009.
Paul Boger. *CCNA Security Lab Manual* Cisco Press. 08-01-2009

Codes/Dates:

CB05 MOV Transfer Status: Transfers to Both UC/CSU (A)
CB05 NOR Transfer Status: Transfers to Both UC/CSU (A)
CB05 RIV Transfer Status: Transfers to Both UC/CSU (A)

Board of Trustees Approval Date: 01/24/2012
COR Rev Date: 01/24/2012