

LAST REVIEW:

(i.e. 2003-2004)

NEXT REVIEW: 2014-15

(i.e. 2008-2009)

STATUS: A

(A, I, D)

COURSE TITLE: Cisco CCNA Security

COMMON COURSE NUMBER: CET2660C

CREDIT HOURS: 4

CONTACT HOUR BREAKDOWN

(per 16 week term)

CLOCK HOURS:

(Voc. Course ONLY)

Lecture: **48**

Lab: **16**

Clinic:

Other:

PREREQUISITE(S): CET1620C (with a grade of C or higher)

COREQUISITE(S):

PRE/COREQUISITE(S):

COURSE DESCRIPTION *(750 characters, maximum)*: CCNA Security equips students with the knowledge and skills needed to prepare for entry-level security specialist careers. It provides a hands-on introduction to network security.

General Education Requirements – Associate of Arts Degree (AA), meets Area(s): Area
General Education Requirements – Associate in Science Degree (AS), meets Area(s): Area
General Education Requirements – Associate in Applied Science Degree (AAS), meets Area(s): Area

UNIT TITLES

1. Modern Network Security Threats
2. Securing Network Devices
3. Authentication, Authorization and Accounting
4. Implementing Firewall Technologies
5. Implementing Intrusion Prevention
6. Securing the Local Area Network
7. Cryptography
8. Implementing Virtual Private Networks
9. Managing a Secure Network

EVALUATION:

Please provide a brief description (250 characters maximum) that details how students will be evaluated on the course outcomes.

Evaluation instruments will include written and/or skills-based examinations and individual in-class and/or take-home assignments. Evaluation methods may also include group in-class and/or take-home assignments.

Common Course Number: CET2660C

UNITS

Unit 1 Modern Network Security Threats

General Outcome:

- 1.0 The student shall: Explain network threats, mitigation techniques, and the basics of securing a network**

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 1.1** Describe the fundamental principles of securing a network
- 1.2** Describe the characteristics of worms, viruses, and Trojan horses and mitigation methods
- 1.3** Describe common network attack methodologies and mitigation techniques such as Reconnaissance, Access, Denial of Service, and DDoS

Common Course Number: CET2660C

Unit 2 Securing Network Devices

General Outcome:

2.0 The student shall: Secure administrative access on Cisco routers

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 2.1** Configure secure administrative access and router resiliency
- 2.2** Configure command authorization using privilege levels and role-based CLI
- 2.3** Configure network devices for monitoring
- 2.4** Secure IOS-based routers using automated features

Common Course Number: CET2660C

Unit 3 Authentication, Authorization and Accounting

General Outcome:

3.0 The student shall: Secure administrative access with AAA

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 3.1** Describe the purpose of AAA and the various implementation techniques
- 3.2** Implement AAA using the local database
- 3.3** Implement AAA using TACACS+ and RADIUS protocols

Common Course Number: CET2660C

Unit 4 Implementing Firewall Technologies

General Outcome:

- 4.0 The student shall: Implement firewall technologies to secure the network perimeter**

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 4.1 Implement ACLs**
- 4.2 Describe the purpose and operation of firewall technologies**
- 4.3 Implement CBAC**
- 4.4 Implement Zone-based policy Firewall using SDM and CLI**

Common Course Number: CET2660C

Unit 5 Implementing Intrusion Prevention

General Outcome:

5.0 The student shall: Configure IPS to mitigate attacks on the network

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 5.1 Describe the purpose and operation of network-based and host-based Intrusion Prevention Systems**
- 5.2 Implement Cisco IOS IPS operations using SDM and CLI**

Unit 6 Securing the Local Area Network

General Outcome:

- 6.0 The student shall: Describe LAN security considerations and implement endpoint and Layer 2 security features**

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 6.1 Describe endpoint vulnerabilities and protection methods**
- 6.2 Describe basic Catalyst switch vulnerabilities such as VLAN attacks, STP manipulation, CAM table overflow attacks, and MAC address spoofing attacks**
- 6.3 Describe the fundamentals of Wireless, VoIP and SANs, and the associated security considerations**
- 6.4 Configure and verify switch security features, including port security and storm control**
- 6.5 Describe Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN)**

Common Course Number: CET2660C

Unit 7 Cryptography

General Outcome:

- 7.0 The student shall: Describe methods for implementing data confidentiality and integrity**

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 7.1** Describe how different types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and non-repudiation
- 7.2** Describe the mechanisms to ensure data integrity
- 7.3** Describe the mechanisms used to ensure data confidentiality

Common Course Number: CET2660C

Unit 8 Implementing Virtual Private Networks

General Outcome:

8.0 The student shall: Implement secure virtual private networks

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 8.1** Describe the purpose and operation of VPN types
- 8.2** Describe the components and operations of IPSec VPNs
- 8.3** Configure and verify a site-to-site IPSec VPN with pre-shared key authentication using SDM and CLI
- 8.4** Configure and verify a remote access VPN
- 8.5** Configure and verify SSL VPNs

Common Course Number: CET2660C

Unit 9 Managing a Secure Network

General Outcome:

9.0 The student shall: Given the security needs of an enterprise, create and implement a comprehensive security policy

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 9.1** Describe the secure network lifecycle
- 9.2** Describe the components of a self-defending network and business continuity plans
- 9.3** Establish a comprehensive security policy to meet the security needs of a given enterprise