SYLLABUS

DIVISION: Business and Engineering Technology **REVISED:** FALL 2015

CURRICULA IN WHICH COURSE IS TAUGHT: IST, Information Systems Technology

COURSE NUMBER AND TITLE: ITN 262 – Cisco CCNA Security

CREDIT HOURS: 4 **HOURS/WK LEC:** 4 **HOURS/WK LAB:** 0 **LEC/LAB COMB:** 4

I. CATALOG DESCRIPTION: ITN 262 - Covers an in-depth exploration of various communications protocols with a concentration on TCP/IP. Explores communication protocols from the point of view of the hacker in order to highlight protocol weaknesses. Includes Internet architecture, routing, addressing, topology, fragmentation and protocol analysis, and the use of various utilities to explore TCP/IP.

II. RELATIONSHIP OF THE COURSE TO CURRICULA OBJECTIVES:

- Demonstrate proficiency in the fundamental Information Technology skills required to provide user support in business.
- Implement and maintain computer based information systems to support the decision-making function of management.
- Apply analytical and problem solving skills for typical computer system designs, planning, implementation and support.
- Design, code, test, debug, and document code for programs and other software needed for computer system implementation and maintenance.
- Apply current industry standards, protocols, and techniques; and keep up with evolving technology to maintain professional proficiency.
- User vendor supplied instructions material and testing tools leading towards certification.

Please Note: The overall Learner Outcomes from all of the course requirements for the A.A.S. Degrees in IT are more in-depth than those of the Career Studies Certificates. However, the IT courses that are the same in both the A.A.S. Degrees and the Certificate Programs carry the same Learner Outcomes and are identical in content. Please review the DCC Catalog or visit the DCC Web Site for more details.

III. REQUIRED BACKGROUND: None

IV. COURSE CONTENT:

- Modern Security Threats
- Securing Network Devices
- Authentication, Authorization and Accounting (AAA)
- Implementing Firewall Technologies

- Implementing Intrusion Prevention
- Securing the Local Area Network (LAN)
- Cryptographic Systems
- Implementing Virtual Private Circuits
- Managing a Secure Network

V. THE FOLLOWING GENERAL EDUCATION OBJECTIVES WILL BE ADDRESSED IN THIS COURSE. STUDENTS WILL:

___X___Communications
________Learning Skills

___X__Critical Thinking
________Interpersonal Skills and
Human Relations

___X__Computational and Computer Skills
________Understanding Culture and Society

___X___Understanding Science and Technology
________Wellness

VI. LEARNER OUTCOMES VII. EVALUATION

Modern Security Threats • Describe the Evolution of Network Security • Identify the Drivers for Network Security • Understand the issues with Network Security Organizations • Identify Domains of Network Security • Configure Network Security Policies • CUnderstand the difference in Viruses, Worms, and Trojan Horses • Mitigate Viruses, Worms, and Trojan Horses • Understand Attack Methodologies such as Reconnaissance Attacks, Access Attacks, Denial of Service Attacks, and Network Attacks	Lab exercises Online test
Securing Network Devices • Secure the Edge Router	Lab exercises In class assignments

• Configure Secure Administrative Access • Configure Enhanced Security for Virtual Logins • Configure SSH • Assign Administrative Roles • Configure Privilege Levels • Configure Role-Based CLI Access • Monitor and Manage Networking Devices including Securing the Cisco IOS Image and Configuration Files as well as Secure Management and Reporting • Utilize Syslog for Network Security • Utilize SNMP and NTP Technologies • CPerform Automated Security Features including Locking Down a Router using AutoSecure and SDM	Online test
Authentication, Authorization and Accounting (AAA) • Identify the purpose and characteristics of AAA • Configure Local AAA Authentication with CLI and SDM • Troubleshooting Local AAA Authentication • Identify Server-Based AAA including characteristics and Protocols • Configure Server-Based AAA Authentication using the CLI and SDM Methods • Troubleshoot Server-Based AAA Authentication	Lab exercises In class assignments Online test
Implementing Firewall Technologies • Configure and use Standard and Extended Access Lists	Lab exercises In class assignments Online test

• Understand the Topology and Flow for Access Control Lists • Configure Standard and Extended Access Lists using SDM • Configure TCP Established and Reflexive Access Control Lists • Configure Dynamic and Time-Based Access Control Lists • CTroubleshoot Complex Access Control Lists • Mitigate Attacks with Access Control Lists • Define he types of Firewalls and Secure Network Resources • Define the Characteristics, Operation, and Configuration of CBAC • Troubleshoot CBAC • Define and Configure Zone-Based Firewalls • Configure Secure Administrative Access	
Implementing Intrusion Prevention • Define IDS and IPS Characteristics • Define Host-Based IPS Implementations • Define Network-Based IPS • Define IPS Signature Characteristics • Configure and Tune IPS Alarms • Be Manage and Monitor IPS Traffic • Configure and Modify Cisco IOS IPS with CLI and SDM • Verify and Monitor IPS Traffic	Lab exercises In class assignments Online test
Securing the Local Area Network • Define Endpoint Security including	Lab exercises

IronPort, Network Admission Control and Security Agent • Define Layer 2 Security Considerations including Spoofing, OverFlow, Manipulation, Storm, and VLAN Attacks • Configure and Verify Port Security • Configure BPDU Guard, Root Guard, Storm Control, VLAN Trunk Security • Configure Cisco Switched Analyzer including Remote Access • Configure Wireless, VoIP, and SAN Security	In class assignments Online test
Cryptographic Systems • Define Cryptography, Cryptanalysis, and Cryptology • Create Integrity with MD5 and SHA-1 including Authenticity with HMAC and Key Management Systems • Configure Encryption using Standard, Advanced, Alternate, and Diffie-Hellman Key Exchange Options • Define and Configure Digital Signatures including Certificate Authorities	Lab exercises In class assignments Online test
Implementing Virtual Private Networks • Define VPN Topologies and Solutions • Configure Site-to-Site GRE Tunnels • Define and Configure IPSec as it relates to Securing VPN Traffic • Verify and Troubleshoot IPSec Configurations • Implement a Site-to-Site IPSec VPN with SDM using the Defined Wizard • Implement Remote Access VPNs	Lab exercises In class assignments Online test

• Configure a VPN using Cisco Easy VPN and SDM including the VPN Client	
Managing a Secure Network • Ensure a Network is Secure including Threat Identification, Risk Analysis, Risk Management, and Risk Avoidance • Define Cisco Self-Defending Network including Solutions for SDN • Define the Principles of Operations Security • Implement Network Security Testing • Implement a Disaster Recovery Plan including Continuity Planning, Disruptions and Backups • Develop a Security Policy including Standards, Guidelines, and Procedures • Develop Security Awareness and Training including details on the Laws and Ethics and Responding to a Security Breach	Lab exercises In class assignments Online test