SPRINGFIELD TECHNICAL COMMUNITY COLLEGE

ACADEMIC AFFAIRS

Course Number: CSO-175 Class/Lect. Hours: 3 Lab Hours: 0 Credits: 3 Dept.: TCOM

Course Title: Cisco CCNA Security Semester: Spring Year: 2017

Course Description, Prerequisite, Corequisite:

CSO-175 - Cisco CCNA Security

This is the security course offered through Cisco CCNA curriculum. Students will be expected to have completed and passed CSO-105/105L and CSO-155/155L or have an active CCENT certification. Topics include, but are not limited to, common network threats, configuring and securing cisco devices, local and server based AAA, zone-based policy firewalls (ZBF), intrusion prevention systems (IPS), layer 2 attacks and prevention, cryptographic services, virtual private networks (VPN), Cisco Adaptive Security Appliances (ASA) and the Cisco Adaptive Security Device Manager (ASDM). By the end of this course, students will be able to configure and troubleshoot Integrated Service Routers (ISR), Intrusion Prevention Systems, firewalls and Cisco ASA's using both he CLI and the ASDM. This class aligns with the CCNA Security certification using the Cisco Netacademy courseware.**

Note: Certification is not guaranteed after the completion of this course, students will need to purchase additional test prep material and invest additional time for test preparation.

Prerequisite(s): CSO-155 or permission of instructor.

Corequisite(s): CSO 175L

OBJECTIVES/COMPETENCIES

Course Objectives	Competencies
Upon successful completion of this course, the student should be able to: - Understand common network threats - Understand cisco administrative roles - Understand monitoring and managing devices - Understand the control plane - Understand AAA (authentication, authorization, accounting) - Understand local and server AAA - Understand cisco firewall technologies - Understand access control lists (ACL) and zone-based policy firewalls (ZBF) - Understand cisco intrusion prevention systems (IPS) - Understand endpoint threats and protection - Understand layer 2 attacks and prevention methods - Understand spanning tree protocol (STP) - Understand basic cryptographic services - Understand hashing as it pertains to authentication and integrity - Understand symmetric and asymmetric encryption - Understand public key infrastructure (PKI) - Understand virtual private networks (VPN) - Understand the cisco adaptive security appliance (Cisco ASA) command line interface - Understand the Cisco ASA graphical user interface tool adaptive security device manager (ASDM) software - Understand VPN setup on a Cisco ASA using ASDM - Understand network testing tools - Understand the development of a security policy	Upon successful completion of this course, the student should be able to perform tasks related to the following: - Describe the nature of common network threats - Explain techniques for mitigating common network threats - Configure secure access to cisco devices in the form of SSH and login controls - Configure privilege levels for user and develop role-based command line interface (CLI) controls for user accounts - Describe in-band and out-of-band management device management techniques - Configure and secure syslog server/network time protocol (NTP)/simple network management protocol (SNMPv3) on cisco devices - Configure routing protocol authentication - Describe control plan policing (COPP) and control plan protection (CPPr) - Describe the aspects of AAA (authentication, authorization, accounting) - Describe the use of local AAA - Configure local AAA - Describe the use of server based AAA - Configure server AAA using a RADIUS server - Describe the operation of 802.1X port based authentication - Describe to the operation of access control lists (ACL's) - Describe the difference between standard and extended ACL's - Configure IPv4 standard and extended ACL's - Configure IPv6 ACL's - Describe firewall operation in depth with regards to classic and zone based policy firewalls (ZBF)

Course Objectives	Competencies
	- Configure ZBF's on cisco routers - Describe the differences between network intrusion prevention systems (NIPS) and host-based intrusion prevention systems (HIPS) - Describe port mirroring and cisco switchport analyzer (SPAN) as it pertains to implementation of a intrusion detection systems (IDS) - Describe intrusion prevention systems (IPS) signatures types, attributes, and engines - Configure IPS using the cisco internetwork operating system (IOS) - Configure IPS signatures using the cisco IOS - Describe the functions and use cases for advanced malware protection (AMP), email security appliance (ESA) and web security appliance (WSA) - Describe to function of network access control (NAC) and the various NAC components - Describe layer 2 security threats such as content addressable memory (CAM) table attacks, virtual local area network (VLAN) attacks, dynamic host configuration protocol (DHCP) attacks, address resolution protocol (ARP) attacks, and spanning tree protocol (STP) attacks - Configure defenses against CAM, VLAN, DHCP, and ARP attacks - Describe IPSec technologies and protocols - Describe phase 1 and phase 2 of the internet key exchange (IKE) - Configure a site-to-site VPN between routers using cisco IOS - Describe the common Cisco ASA solutions and features - Describe to the outside features of an Cisco ASA - Describe objects on a Cisco ASA - Describe the configuration of a Cisco ASA via command line

Course Objectives	Competencies
	- Configure basic setup, objects, ACL's, network address translation (NAT), AAA and IPS service policies on a Cisco ASA via the command line interface - Describe the use and function of the Cisco ASA adaptive security device manager (ASDM) software - Configure the Cisco ASA to use the ASDM - Describe the layout and navigation of the ASDM - Configure the basic setup, objects, ACL's, NAT, AAA and IPS functions on the Cisco ASA using the ASDM - Configure site-to-site, remote-access, clientless ssl, and Cisco AnyConnect VPN's on the Cisco ASA using the ASDM - Describe various network scanning and penetration testing techniques and software - Describe the structure of a security policy and the various standards guidelines and procedures