Miami Dade College

Course Description

CTS2670 | Check Point Security Administration | 4.00 credits

This course, designed for students specializing in network security, prepares students for the Check Point Certified Security Administrator (CCSA) certification exam. Students will learn how to install security gateways; configure rules on servers; create a rule base; assign user permissions; schedule backups and upgrades; monitor and troubleshoot common network traffic. Prerequisite: CTS1134, CTS1120.

Course Competencies:

Competency 1: The student will demonstrate an understanding of security technology by:

1. Describing the key elements of a security network architecture
2. Describing the security required at each level of the OSI model
3. Describing firewall technologies used to deny or permit network traffic (e.g., packet filtering Stateful Inspection, Application Intelligence)
4. Describing network topologies and their associated deployment considerations
5. Conducting a feasibility study to determine network security requirements
6. Designing a distributed environment based on recommendations derived from a feasibility study
7. Selecting appropriate topologies given an organization's requirements
8. Using a console dashboard to manage users

Competency 2: The student will demonstrate understanding of deployment platforms by:

1. Performing backups and restores
2. Identifying critical files needed to perform administrative functions, including purge, backup, importing and exporting users and groups, adding and deleting administrators
3. Deploying gateways
4. Selecting appropriate bundles to address targeted specific threats
5. Selecting appropriate platforms to meet targeted operational security needs
6. Monitoring the operating system

Competency 3: The student will demonstrate understanding of security policy by:

1. Creating and configuring a secure network using rules
2. Creating and implementing rules to manage user rights, access, etc
3. Creating and managing objects in the rule database
4. Evaluating existing policies and optimizing the rules based on current organization requirements
5. Maintaining Security Management Server (SMS) with scheduled backups and policy versions to ensure seamless upgrades and minimal downtime
6. Using a dashboard to monitor rules Managing version control. Configuring multicast access control

Competency 4: The student will demonstrate an understanding of how to monitor traffic and connections by:

1. Identifying tools to use to monitor network traffic and troubleshoot events using packet data
2. Interpreting alerts and log data
3. Generating reports
4. Troubleshooting system and security issues
5. Ensuring network functionality
6. Configuring alerts and traffic counters
7. Monitoring suspicious activity
8. Analyzing tunnel activity
9. Monitoring remote user access

Competency 5: The student will demonstrate an understanding of Network Address Translation (NAT) by:

1. Explaining the function of NAT on networks
2. Describing the differences between public and private IP addresses and their respective advantages and disadvantages
3. Distinguishing between Hide NAT and Static NAT
4. Discussing the benefits and liabilities of Automatic NAT and manual NAT respectively
5. Discussing Global Properties and how to modify them to adjust Automatic NAT rules
6. Configuring NATs

Competency 6: The student will demonstrate an understanding of centralized policy management across enterprise- wide deployments by:

1. Monitoring remote gateways to evaluate the need for upgrades, new installations, and license modifications
2. Applying upgrade packages to single or multiple VPN- gateways
3. Monitoring, upgrading and attaching product licenses remotely
4. Monitoring, upgrading and managing licenses remotely

Competency 7: The student will demonstrate an understanding of user management and authentication by:

1. Creating users and groups
2. Applying different levels of user authentication (e.g., user, session, client)
3. Applying authentication schemes to identify valid users
4. Configuring the authentication method for remote users
5. Configuring user, session and client authentications
6. Tracking successful and unsuccessful authentication attempts
7. Managing Lightweight Directory Access Protocol (LDAP) servers

Competency 8: The student will demonstrate an understanding of identify awareness by:

1. Defining identifies awareness
2. Distinguishing between endpoint and terminal server identify agents
3. Using Identify Awareness to provide granular level access to network resources
4. Acquiring user information to control access
5. Defining access roles for use in an Identify Awareness rule
6. Implementing Identify Awareness in the Firewall Rule Base
7. Explaining how to establish browser-based authentication using Captive Portal and Transparent Kerberos authentication

Competency 9: The student will demonstrate an understanding of virtual private networking (VPN) by:

1. Describing the types and uses of VPNs
2. Comparing and contrasting VPN topologies
3. Discussing considerations and issues involved in VPN deployments
4. Selecting an appropriate VPN topology given an organization's requirement
5. Configuring a certificate-based site-to-site VPN
6. Discussing the role of tunneling in VPN implementation
7. Configuring remote access to corporate resources using tunneling protocol

Learning Outcomes:

- Solve problems using critical and creative thinking and scientific reasoning
- Formulate strategies to locate, evaluate, and apply information
- Use computer and emerging technologies effectively