Miami Dade College

Course Description

CTS2671 | Check Point Security Engineering | 4.00 credits

This course is for students specializing in network security, prepares students for the Check Point Certified Security Expert (CCSE) certification examination. Students learn how to configure, build, modify, deploy and troubleshoot a secure network utilizing firewall technologies. Topics include clustering, software acceleration, advanced VPN concepts and implementation, and monitoring and reporting tools. Prerequisite: CTS1120, CTS1134, CTS2670.

Course Competencies:

Competency 1: The student will demonstrate an understanding of system upgrading by:

1. Differentiating between snapshots, backups and upgrades
2. Creating schedules for snapshots, backups, and upgrades
3. Performing snapshots, backups, and upgrades

Competency 2: The student will demonstrate an understanding of advanced firewall practices by:

1. Explaining the elements and functions of the firewall kernel structure
2. Describing the function of Network Address Translation (NAT) in the context of a firewall
3. Identifying the functionality of key Firewall configuration files
4. Installing a firewall to specifications
5. Configuring a security server

Competency 3: The student will demonstrate an understanding of clustering and acceleration by:

1. Comparing and contrasting virtual routing redundancy protocol (VRRP) and Cluster XL protocol
2. Building, testing and troubleshooting a load sharing deployment on an enterprise network
3. Building, testing and troubleshooting a high availability (HA) deployment on an enterprise network
4. Building, testing and troubleshooting management HA deployment on an enterprise network
5. Building, testing and troubleshooting VRRP deployment on an enterprise network
6. Configuring, maintaining and troubleshooting acceleration solutions to ensure performance enhancements on the firewall
7. Optimizing secure server performance

Competency 4: The student will demonstrate an understanding of advanced user management by:

1. Configuring a network user authentication directory using an external user database
2. Managing internal and external user access to resources for remote access or across a VPN
3. Troubleshooting and resolving user authentication and user access issues
4. Using tools to configure identity and resource management

Competency 5: The student will demonstrate an understanding of virtual private network (VPN) advanced Internet Protocol Security (IPSec) and remote access by:

1. Troubleshooting site-to-site or certificate- based VPN's on a corporate gateway
2. Optimizing VPN performance and availability
3. Managing and testing corporate VPN tunnels for monitoring and scalability
4. Creating a VPN tunnel utilizing the Internet Key Exchange (IKE) process
5. Initiating connections between the gateway and remote users
6. Configuring and managing multiple-entry- point (MEP) VPNs

Competency 6: The student will demonstrate an understanding of auditing and reporting by:

1. Generating reports on specific network traffic
2. Troubleshooting report generation given command-line tools and debug-file information
3. Identifying and discussing the audit policies requirements for information technology (IT) compliance checking mandated by the Sarbanes-Oxley Act
4. Configuring and deploying management threat monitoring solutions
5. Generating threat reports

Competency 7: The student will demonstrate an understanding of how to maintain a security operating system by:

1. Adding and deleting licenses
2. Configuring image management
3. Configuring hardware health monitoring functions
4. Configuring backup and restore functions
5. Configuring emergency password restore
6. Performing system recovery
7. Erasing a hard disk

Learning Outcomes:

- Solve problems using critical and creative thinking and scientific reasoning