CIS 284 : CISCO CCNA SECURITY

Transcript title

Cisco CCNA Security

Credits

4

Grading mode

Standard letter grades

Total contact hours

50

Lecture hours

30

Other hours

20

Prerequisites

CIS 154C or CCNA certification.

Course Description

Introduces security related issues and provides essential skills network administrators need in order to provide security for a computer network. Covers protective security technologies including TCP packet analysis, network device hardening, advanced firewall techniques, cryptography, intrusion prevention systems, LAN security, virtual private networks, network attacks and mitigation techniques, andsecurity policy planning.

Course learning outcomes

1. Identify network threats, mitigation techniques, and the basics of securing a network.
2. Secure administrative access on Cisco routers.
3. Secure administrative access with authentication, authorization, and accounting.
4. Implement firewall technologies to secure the network perimeter.
5. Configure an intrusion prevention system to mitigate attacks on the network.
6. Describe LAN security considerations and implement endpoint and layer 2 security features.
7. Describe methods for implementing data confidentiality and integrity related to cryptography.
8. Implement secure virtual private networks.
9. Given the security needs of an enterprise, identify the necessary components required to implement a comprehensive security policy.
10. Implement firewall technologies using an adaptive security appliance to secure the network perimeter.
11. Analyze TCP/IP packets for security purposes.