Diploma in

Computer Operating Systems & Network Technology

Course Summary Security

Program of Study: Diploma, Computer Operating Systems & Network Technology

Course Rubric/Title: CNT-3016 Security Fundamentals

Clock hours: 193

Prerequisite Course: Completion of 1st and 2nd Trimester

Industry Certification:

CompTIA Security+ Certification

Course Description:

This course is designed to educate students about various computer attacks; including, worms, Trojans, spoofing attacks to name a few. In addition to learning the various types, students are taught how to combat and protect against the attacks or rid a computer of infected items.

Course Competencies:

1. Understand network security; including, security threat trends and their ramification, the goals, and the factors involved in a secure network strategy.
2. Explain denial-of-service (DOS) attacks, the major components used in DOS attacks and how they are installed.
3. Explain and discuss ping-of-death, man-in-the-middle, replay, and TCP session hijacking attacks.
4. Understand the major types of spoofing attacks.
5. Detail three types of social-engineering attacks.
6. List the major types of attacks used against encrypted data.
7. List the major types of malicious software and identify a countermeasure for each one.
8. Understand the implications of IEEE 802.1x and how it is used.
9. Understand VPN technology and its uses for securing remote access to networks.

10. Understand how RADIUS authentication works.
11. Understand how TACACS+ operates.
12. Understand how PPTP, L2TP, SSH, and IPSec work and when they are used.
13. Understand the vulnerabilities associated with telecommuting.
14. Understand the need for secure email, email vulnerabilities, and how to safeguard against them.
15. Outline the benefits of PGP and S/MIME.
16. Understand SSL/TLS protocols and their implementation on the Internet and the HTTPS protocol as it relates to SSL.
17. Understand the vulnerabilities of JavaScript, buffer overflow, ActiveX, cookies, CGI, applets, SMTP relay, and how they are commonly exploited.
18. Identify the vulnerabilities of the FTP method of exchanging data then discuss the alternative to FTP, S/FTP in order to better secure your network infrastructure.
19. Understand security issues related to wireless data transfer; including the 802.11x standards, Wireless Application Protocol (WAP), Wireless Transport Layer Security (WTLS) protocol, and Wired Equivalent Privacy (WEP.
20. Understand the purpose of a network firewall.
21. Understand the role of routers, switches, or other networking hardware in security.