Minnesota State College Southeast

NWAT 2683: Security Threats & Countermeasures

A. COURSE DESCRIPTION

Credits: 3

Lecture Hours/Week: 2

Lab Hours/Week: 2

OJT Hours/Week: *.*

Prerequisites: None

Corequisites: None

MnTC Goals: None

This course covers the concepts and familiarity of the tools and techniques used by malicious network intruders. The student will learn to recognize security threats and vulnerabilities that exist in present networking environments. Additional emphasis will be placed on recognizing and mitigating responsive measures to lessen the negative effectiveness of security breaches. (Prerequisites: NWAT1641 and NWAT 2681) (Prerequisite or concurrent: NWAT1649) (3 credits: 2 lecture/1 lab)

B. COURSE EFFECTIVE DATES: 10/10/2005 - Present

C. OUTLINE OF MAJOR CONTENT AREAS

D. LEARNING OUTCOMES (General)

1. Explain the security triangle concept
2. Explain hacktivism
3. Identify skill levels of hackers
4. Identify computer crimes
5. Explain malicious hacking
6. Describe reconnaissance
7. Describe scanning
8. Explain footprinting
9. Explain enumeration
10. Explain system hacking
11. Explain trojans and backdoors
12. Describe sniffers
13. Install sniffers
14. Configure sniffers
15. Analyze sniffer data
16. Explain denial of services
17. Explain social engineering
18. Explain session hijacking
19. Explain web server hijacking
20. Describe web application vulnerabilities
21. Identify web-based password cracking techniques
22. Explain SQL injection
23. Explain wireless hacking
24. Identify viruses
25. Explain physical security
26. Describe multi-platform hacking
27. Explain IDS (intrusion detection systems)
28. Install IDS
29. Configure IDS
30. Analyze IDS data
31. Explain honeypots
32. Install honeypots
33. Configure honeypots
34. Analyze honeypot data
35. Explain buffer overflows
36. Explain cryptography
37. Explain penetration testing
38. Describe penetration testing utilities
39. Install penetration testing utilities
40. Configure penetration testing utilities
41. Display workplace professionalism
42. Identify footprinting utilities
43. Identify scanning tools
44. Identify enumeration

45. Identify system hacking tools
46. Identify web server hacking tools
47. Identify wireless hacking tools
48. Explain preventative measures
49. Explain firewall protection
50. Display interpersonal communication
51. Install firewall protection utilities
52. Display common sense approach
53. Configure firewall protection utilities
54. Explain virtual private networks
55. Install virtual private network
56. Configure virtual private network
57. Display ethical standards
58. Identify common network intrusions
59. Describe US Federal Law pertaining to computer crimes
60. Describe Section 1029 of US Federal Law governing computer crimes
61. Describe Section 1030 of US Federal Law governing computer crimes

E. Minnesota Transfer Curriculum Goal Area(s) and Competencies

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted