Minnesota State College Southeast

NWAT 2685: Wireless Security

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 a basic to intermediate approach to secure home and business wireless networks. Students will learn how wireless networks are installed and implemented in various networking environments and topologies. Emphasis will be placed on understanding security features found on most wireless routers. Students will have an opportunity to install, configure and implement a secure wireless network. Additional emphasis will be given to third party security software solutions. (Prerequisites: NWAT1609, NWAT1642, NWAT1650) (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 wireless LAN 802.11 technology
2. Compare 802.11a verses 802.11b security issues
3. Identify various security attacks
4. Identify antenna security issues
5. Define major security risks to 802.11b
6. Define war-driving
7. Explain insertion attacks
8. Describe plug-in unauthorized clients
9. Identify various wireless sniffers
10. Install various wireless sniffers
11. Configure various wireless sniffers
12. Analyze various wireless sniffer data
13. Define ARP spoofing
14. Define MAC spoofing
15. Define Access Point
16. Install Access Point
17. Configure Access Points
18. Define server set ID (SSID)
19. Describe brute force base station SSID
20. Explain WEP
21. Identify attacks against WEP
22. Define WEP keys
23. Install WEP keys
24. Configure WEP keys
25. Define SNMP community works
26. Identify SNMP vulnerabilities
27. Define client side security risks
28. Define installation risks
29. Define jamming
30. Describe client to client attacks
31. Describe file sharing attacks
32. Define parasitic grids
33. Define hotspots
34. Identify hotspot security issues
35. Explain base station configuration
36. Explain MAC address filtering
37. Configure base station
38. Configure MAC address filtering
39. Define base station discovery
40. Display workplace professionalism
41. Define FakeAP
42. Explain honeypots
43. Identify base station security assessments
44. Explain wireless client protection

45. Configure personal firewall
46. Configure wireless VPN
47. Explain wireless intrusion detection
48. Configure wireless intrusion detection software
49. Display interpersonal communication
50. Describe 802.11 gateway infrastructure
51. Display common sense approach
52. Define BlueSocket
53. Define EcuTel
54. Identify security analysis tools
55. Install security analysis tools
56. Configure security analysis tools
57. Define vulnerability scanning
58. Describe third party security solutions
59. Explain wireless encryption techniques

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

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted