NWAT 2689: Forensic Investigation

A. COURSE DESCRIPTION

Credits: 3
Lecture Hours/Week: 2
Lab Hours/Week: 2
OJT Hours/Week:NW
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: NWAT1601, NWAT1602, NWAT1641, NWAT2681) (Prerequisite or concurrent: NWAT1649) (3 credits: 2 lecture/1 lab)

B. COURSE EFFECTIVE DATES: 08/27/2007 - 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. Compare 802.11b verses 802.11g security issues 
4. Identify various security attacks 
5. Identify various security issues 
6. Define major security risks to 802.11b 
7. Define war-driving 
8. Explain insertion attacks 
9. Describe plug-in unauthorized clients 
10. Identify various wireless sniffers 
11. Install various wireless sniffers 
12. Configure various wireless sniffers 
13. Analyze various wireless sniffer data 
14. Define ARP spoofing 
15. Define MAC spoofing 
16. Define Access Point 
17. Install Access Point 
18. Configure Access Point 
19. Define server set ID (SSID) 
20. Describe brute force base station SSID 
21. Explain WEP 
22. Identify attacks against WEP 
23. Define WEP keys 
24. Install WEP keys 
25. Configure WEP keys 
26. Define SNMP community works 
27. Identify SNMP vulnerabilities 
28. Define client side security risks 
29. Define installation risks 
30. Define jamming 
31. Describe client to client attacks 
32. Describe file sharing attacks 
33. Define parasitic grids 
34. Define hotspots 
35. Define hotspots security issues 
36. Explain base station configuration 
37. Explain MAC address filtering 
38. Configure base station 
39. Configure MAC address filtering 
40. Define base station discovery 
41. Display workplace professionalism 
42. Define FakeAP 
43. Explain honeypots 
44. Identify base station security assessments
45. Explain wireless client protection
46. Configure personal firewall
47. Configure wireless VPN
48. Explain wireless intrusion detection
49. Configure wireless intrusion detection software
50. Display interpersonal communication
51. Describe 802.11 gateway infrastructure
52. Display common sense approach
53. Define BlueSocket
54. Define EcuTel
55. Identify security analysis tools
56. Install security analysis tools
57. Configure security analysis tools
58. Define vulnerability scanning
59. Describe third party security solutions
60. 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