Minnesota State College Southeast

NWAT 2687: LAN/WAN Network 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 the identification and implementation of router security in current network environments. The student will learn basic and intermediate techniques to secure network traffic and protocols refining router configurations. This course covers the advanced concepts of perimeter security in current networking environments. The student will learn how to plan, design, install and implement firewall security appliances to protect private enterprise networks from high security risk public networks. Additional emphasis will be placed on how to configure a Cisco PIX firewall to specific security guidelines in various networking scenarios. (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 network security
2. Identify legal issues and privacy concerns
3. Identify/describe security perimeter
4. Explain security policy basics
5. Describe dedicated firewalls
6. Describe server-based firewalls
7. Describe personal firewalls
8. Explain general router security defaults
9. Configure router privilege levels
10. Configure router user accounts
11. Configure routing protocol security
12. Explain router perimeter security
13. Configure traffic filtering
14. Explain router management
15. Explain remote management using SSH
16. Configure SSH
17. Explain ACL (access control list)
18. Configure standard ACLs
19. Configure extend ACLs
20. Configure reflexive ACLs
21. Explain Content-Based Access Control
22. Configure CBAC inspection rules
23. Explain CBAC inspection rules
24. Explain AAA (authentication, authorization, accounting)
25. Describe Syslog
26. Explain tunneling protocols
27. Explain IPSec
28. Configure IPSec
29. Configure VPNs
30. Describe router remote access
31. Describe firewall appliance technology
32. Describe packet filtering technology
33. Describe Cisco PIX Security Appliance
34. Describe cut-through proxy operation
35. Identify PIX features
36. Identify basic PIX configuration commands
37. Explain PIX dynamic host control configuration
38. Identify PIX transport protocols
39. Explain NAT
40. Configure PIX-related NAT
41. Explain PIX related ACLs
42. Identify various PIX-related ACLs
43. Configure various PIX-related ACLs
44. Describe malicious applet filtering

45. Describe object grouping
46. Configure PIX authentication
47. Describe PPPoE security
48. Explain PIX advanced protocols
49. Configure PIX Advanced Intrusion Detection
50. Describe FTP Fixup configuration
51. Describe PIX multimedia support
52. Describe attack guards
53. Identify various PIX-related attacks
54. Explain PIX signatures
55. Explain PIX Failover
56. Display interpersonal communication
57. Display workplace professionalism
58. Display common sense approach
59. Configure PIX VPN
60. Configure PIX VPN IKE
61. Configure PIX IPSec
62. Configure PIX management tools
63. Configure PIX Device Manager

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

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted