ITSC 206 - Advanced Networking for Offensive and Defensive Environments

Course Description:
This advanced course provides a deeper examination of the implementation, strengths and weaknesses of both industrial protocols and business protocols. Topics include: networking security protocols, advanced routing and intrusion detection/prevention.

3 credits

Time Guidelines:
The standard instructional time for this course is 105 hours.

Effective Term:
Spring 2020

Prerequisite(s):

- ITSC 200 - Network Protocols and Security

Course Assessment:

Quizzes/Presentation	10%
Lab Completion	15%
Midterm Exam	35%
Final Exam	40%
Total:	100%

SAIT Policies and Procedures:
For information on the SAIT Grading Scale, please visit policy AC 3.1.1 Grading Progression Procedure: http://www.sait.ca/Documents/About SAIT/Administration/Policies and Procedures/AC.3.1.1 Grading and Progression Procedure.pdf

For information on SAIT Academic Policies, please visit: www.sait.ca/about-sait/administration/policies-and-procedures/academic-student

Course Learning Outcome(s):

1. Summarize the fundamentals of network security.

    Objectives:

        1.1 Define network security.

        1.2 Research common network security threats.

        1.3 Identify network security vulnerabilities.

        1.4 Describe the goals of network security.

        1.5 Discuss the measures of network security.

        1.6 Compare wired versus wireless LAN infrastructure.

        1.7 Compare and contrast internal and external vulnerabilities.

        1.8 Examine offense and defense security tools.

2. Secure the Local Area Network (LAN).

    Objectives:

        2.1 Explain switched data plan attack types.

        2.2 Configure the secure LAN environment.

        2.3 Introduce a security threat into the LAN environment.

        2.4 Analyze switched data plan security threats.

        2.5 Protect the LAN environment against potential threats.

3. Evaluate advanced routing protocols.

    Objectives:

        3.1 Define advanced routing protocols.

        3.2 List the types of routing protocols.

        3.3 Compare the advantages of the routing protocols.

        3.4 Configure advanced routing protocols.

        3.5 Analyze the behaviour of routing protocols.

4. Implement Identity-Based Networking Services (IBNS).

    Objectives:

        4.1 Discuss IBNS.

        4.2 List the components of IBNS.

        4.3 Configure the IBNS components.

        4.4 Analyze the IBNS components and data traffic.

5. Implement Network Address Translation (NAT).

    Objectives:

        5.1 Explain NAT.

5.2 List the types of NAT.

5.3 Compare the advantages and disadvantages of the different types of NAT technologies.

5.4 Select the appropriate NAT technology based on different technical environments.

5.5 Configure the NAT technologies.

5.6 Analyze NAT technologies and data traffic behaviour.

6. Implement security policies surrounding firewalls and perimeters.

Objectives:

6.1 Research the types of firewalls.

6.2 Discuss pros and cons of firewalls.

6.3 Decide on the appropriate placement of a firewall.

6.4 Configure different types of firewalls.

7. Deploy strategies for a network-based intrusion detection and prevention system.

Objectives:

7.1 Explain an Intrusion Detection System (IDS).

7.2 Explain an Intrusion Prevention System (IPS).

7.3 Compare and contrast IDS and IPS.

7.4 Evaluate IDS and IPS deployment strategies.

7.5 Configure IDS and IPS policies.

8. Implement secure connectivity technologies.

Objectives:

8.1 Research general deployment guidelines for Virtual Private Network (VPN) technologies.

8.2 Choose an appropriate VPN topology.

8.3 Choose appropriate VPN cryptographic.

8.4 Configure VPN technologies.
