ITSC 200 - Network Protocols and Security

Course Description:

This introductory course provides students a grounding in basic switching, routing and general protocols. These are analyzed and implemented from both a functionality and vulnerability viewpoint. The configuration of defensive and offensive tools is practiced in the lab environment.

3 credits

Time Guidelines:

The standard instructional time for this course is 135 hours.

Effective Term:

Fall 2017/2018

Course Assessment:

Quizzes	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. Explain the fundamentals of networking and operating systems.

Objectives:

1.1 Identify the characteristics and types of networking.

1.2 Explain fundamental operating system concepts.

1.3 Review network standards and standards organizations.

1.4 Discuss network performance issues and related concepts.

1.5 Analyze network traffic to separate multiple simultaneous conversation.

1.6 Identify the common characteristics of all operating systems.

1.7 Use basic operating systems commands to perform common operating system tasks.

1.8 Use basic functions of Wireshark to examine network traffic.

2. Analyze the interconnection of network architecture.

Objectives:

2.1 Outline Open System Interconnection (OSI) reference model layers.

2.2 Analyze OSI reference model issues and concepts.

2.3 Describe TCP/IP protocol suite in reference to the OSI model.

2.4 Explain how operating systems use drivers to support multiple protocols.

2.5 Apply the OSI model to captured traffic.

3. Explain how operating systems interact over LAN’s.

Objectives:

3.1 Describe the basic components of Ethernet technology.

3.2 Explain the structure of Media Access Control (MAC) addresses.

3.3 Differentiate logical and physical network addressing.

3.4 Examine the Ethernet framing process and structure.

3.5 Analyze Address Resolution Protocol (ARP).

3.6 Analyze the Content-Addressable Memory (CAM) table.

3.7 Define Broadcast and Collision domains.

3.8 Identify devices used to create and mitigate collision and broadcast domains.

3.9 Explain Spanning-Tree Protocol (STP).

4. Implement Network and internet layer connection technology.

Objectives:

4.1 Define Network and internet layer connection protocols.

4.2 Explain how protocol stacks work to support upper layer protocols.

4.3 Outline key routing protocol concepts.

4.4 Configure IP routing protocols.

4.5 Analyze the process of routing.

4.6 Explain the structure of IPv4.

4.7 Apply the IP Subnet addressing concepts.

4.8 Explain the structure of IPv6.

4.9 Compare the characteristics of IPv4 and IPv6.

4.10 Recognize basic network protocols found on Ethernet networks.

4.11 Analyze Network layer data packets using network sniffing tools.

4.12 Analyze ICMP protocols.

4.13 Explain IP related concepts such as IPsec and NAT.

5. Implement Transport Layer technology.

Objectives:

5.1 Compare Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocols.

5.2 Contrast and compare TCP and UDP Sockets.

5.3 Explain why some operating system protocols use TCP while others use UDP.

5.4 Differentiate how a TCP session is initiated and torn down with a UDP connection.

5.5 Identify the aspects of TCP operation including TCP Reliability and Flow Control used in Denial of Service.

5.6 Identify the components of UDP protocol operation including UDP unreliability features.

5.7 Explain network traffic security concerns with TCP and UDP.

5.8 Explain how applications like Port-Knocking can increase security of a network.

5.9 Use NMAP to perform port scans and capture with Wireshark.

6. Implement Application Layer protocols.

Objectives:

6.1 Define the Application layer protocols such as DNS, DHCP and HTTP.

6.2 Compare and contrast the characteristics of the different Application protocols.

6.3 Analyze Application layer protocols, functions and characteristics.

6.4 Identify common Application layer protocols, security concerns and mitigations.

6.5 Implement HTTP and HTTPS services.

6.6 Implement DNS services.

6.7 Implement DHCP services.