I. Course Title: Networking and Security Laboratory

II. Course Prefix/Number: CSCI 216

III. Credit Hours: 2.0

IV. Prerequisite(s):
CSCI 215 minimum grade of C- or concurrent enrollment in CSCI 215 or CSCI 345 minimum grade of C- or concurrent enrollment in CSCI 345.

V. Catalog Description:
Students will implement secure network services. Students will also practice various types of hacking attacks and study defenses against them. Virtual machines will be used to simulate networks.

VI. Curricular Relationships:
CSCI 216 is required of students working toward the Associate of Science Degree with an emphasis in Internet Computing and Security. CSCI 216 can be used together with CSCI 215 to satisfy the networking requirement for the Bachelor of Science Degree in Mathematics with a Computer Science Emphasis.

VII. Student Learning Outcomes:

- Students will be able to effectively use network tools such as ping, nslookup, arp, tracert, netstat, and ssh.
- Students will be able to analyze the Windows and Linux routing tables.
- Students will be able to view active TCP and UDP ports.
- Students will be able to install and use network defense tools such as Snort and Windows Network Monitor.
- Students will be able to monitor network traffic.
- Students will be able to encrypt a file system.
• Students will be able to detect errors in IPSec performance statistics.

• Students will be able to use a network sniffer such as Wireshark to examine and analyze network traffic at all layers of the protocol stack.

• Students will be able to use a port scanning tool such as NMAP to subvert firewalls and intrusion detection systems, perform penetration testing, detect rogue wireless access points, and quash network worm outbreaks.

• Students will be able to install a simple network with two clients and a single server using standard host configuration software tools such as DHCP.

• Students will be able to set-up and configure basic routing and protocols including static routing, RIP2, OSPF, and EIGRP.

• Students will be able to generate and distribute a PGP key pair and use the PGP package to send an encrypted e-mail message.

• Students will be able to implement secure remote access using RADIUS, TACACS+, PPTP, L2TP, SSH, and IPSec.

• Students will be able to implement secure enterprise directory management using LDAP.

• Students will be able to implement S/FTP to secure file transfer through the internet.

• Students will be able to implement security through ACLs on routers, switches and other networking hardware.

• Students will be able to set up an encrypted tunnel between two hosts.

VIII. Content Outline:

The content will consist of laboratory exercises and activities designed around the learning outcomes of the course. The laboratories may vary. Example labs include:

• Introduction to Networking Lab
  o Connecting two virtual machines so that both computers are capable of pinging each other.
  o Include a second network and a third virtual machine that is part of both networks.
  o Use iptables to configure static routing on the third virtual machine.
  o Add one computer to each of the two networks. Set up a simple networking service such as DNS.
  o Send a ping between the two networks. Use Wireshark to capture the packets and analyze the contents.

• Buffer Overflow Vulnerabilities, Intrusion Detection, and Access Control List Lab
  o A server is set up with a buffer overflow vulnerability.
Students install Nessus, a penetration testing tool to find the vulnerable server.

Students use Nessus to gain control of the victim machine.

Snort is used on the defensive side to detect the intrusion attempt.

The tool Advanced Intrusion Detection Environment (AIDE) is used to determine if any changes have been made to the system.

Students then implement an access control list on the vulnerable machine to prevent future attacks on the buffer overflow vulnerability.

- **Falsifying Identity on a Network**
  - Students first practice spoofing MAC and IP addresses, DNS spoofing using the tool DNSspoof, and dsniff to kill a tcp session.
  - Students practice using netstat to detect a hostile IP address.
  - Next students explore the use of defensive measures to help detect spoofing attacks such as arpwatch.

- **Implementing IPSec**
  - Students will produce a Secure Sever IPSec Policy GPO that is linked to an OU.
  - Students will produce a Client Respond IPSec Policy GPO linked to the new OU.

- **Implementing a Virtual Private Network**
  - Students will initialize and configure a VPN server.
  - Students will connect the server to a LAN behind a firewall that implements a NAT server.
  - Students will configure the firewall to forward all inbound connections to an internal VPN server.

**IX. Course Procedures/Policies/Grading Scale:**

1. Course will consist of laboratory assignments and activities that will comprise a large part of the course grade.

2. At least one laboratory exam will be given during each semester.

3. A final laboratory exam will be given at the end of the semester.

**X. Required/Recommended Readings:**

Depending on instructor preference, a text book may be required or the instructor may use his/her own laboratory materials with the course. Reference books may be useful such as:


XI. Issues Unique to Course: The course will consist of two 2-hour laboratories per week.

XII. Additional Departmental Issues: None.