COMP-4722 Course Syllabus

1 Course Information

Course Name	COMP 4722: Network Security
Prerequisites	COMP-4621 Computer Networking
Required Textbook	No textbook required

2 Course Description

This course delves into arguably the most important security topic today; the security of the network. In this course, we cover primarily the defensive side of network security, and the tools and techniques used to secure, analyze and detect attacks in modern networks. Specific topics include:

- Firewalls, types and capabilities, software implementations, configuration and management
- Linux networking basics, setting up a virtual network environment for testing and implementation
- Common Unix/Linux tools for network management/configuration (ip, if, ss, netstat, route, ping, nc, etc.)
- Common networking setup for Linux environments (configuration files, DHCP/DNS/VLAN/VPN in test networks)
- Programming using OpenSSL libraries for key exchange and encryption/decryption
- Firewall configuration and implementation in Linux (netfilter, iptables, etc.)
- Intrusion detection basics, types and capabilities
- Intrusion detection (NIDS) deployment and usage (snort, bro, etc.)
- Automated vulnerability scanning and vulnerability management basics
- Vulnerability scanner/manager deployment using (Greenbone, Wazuh, ELK)
- Host-based vulnerability scanning, management, HIDS using Wazuh

- VPNs, overview, implementation and usage (openvpn, wireguard)
- Security auditing for real: SIEMs
- Wireless network security, attacks and threats (open wireless, Wifi pineapple, cracking network passwords and keys)

3 Textbook and Materials

For lectures, we will use the following textbook:

Cryptography and Network Security: Principles and Practice by W. Stallings; ISBN-13: 978-0134444284

You will need a good internet connection and a laptop that meets DU specifications. (See `https://www.du.edu/it/support/how-to/students/laptops`). For technical support in using Canvas, please go to `http://otl.du.edu/knowledgebase/canvas`

3.1 Other Stuff

- Reliable access to a computer and the Internet. If you are online you can turn your homework in from wherever in the world you are!
- Wireshark, which is freely available. You will need to install this and make sure it's working on your computer. I'm assuming as computer science or computer engineering majors, you will have the ability to download software and install it without the need for technical support. Seriously, if you can't get the software installed, you're not ready for this course, it's far more advanced than that!
- git: We will be using git, a source code version control system. You will be required to set up and use a git repository to turn in the programming assignments.
- Canvas: We will be using the Canvas platform for most of the course, including course material and communication. Be sure you are able to access Canvas.
- CLion/PyCharm: This is not a requirement, but I will generally be programming in-class examples in the CLion IDE from JetBrains OR the PyCharm IDE from JetBrains. I like the JetBrains IDEs and they are free for you to use if you sign up with your du.edu email address.

4 Course Learning Objectives

By the end of this course, you should be able to:

- Identify and classify network security threats, and develop a security model (and/or policies) to prevent, detect and recover from the attacks.

- Understand generic properties of secret keys, message digest, and well-known public key algorithms, and how each is used.
- Understand authentication handshakes and analyze their relative security and performance strengths.
- Obtain an overview of security standards used in practice, PKI standards, IPSec, and SSL.
- Understand attack payloads, intrusion detection, and the use of a firewall and its configuration to provide network access control.
- Familiarity with using the OpenSSL library high level interface to secure communications.
- Be able to configure network security software in modern *nix operating systems
- Capability to deploy and use vulnerability scanning, detection, and management software
- Know how NIDS/HIDS operate (and differ), and some common types of implementations (rule based, anomaly detection, thresholds, etc.)
- Be able to use and identify common attacker tools from a network perspective
- Be familiar with the MITRE ATT&CK framework and how it applies to network security
- Have a baseline understanding of what's involved with discovering and triaging a network intrusion

5 Course Outcomes

The high level objectives of this course are as follows:

1. Teach students the fundamentals of network security, so they can understand common network security vocabulary (SIEM, SOC, IDS/IPS, etc.).
2. Give students a theoretical understanding of how to protect networks and assets from attackers, and best practices for configuring security devices.
3. Provide hands-on experience with configuring network security software including firewalls, IDS, etc. as well as with monitoring and alerting on possible TTPs/IoCs.

6 Program Level Goals

Courses in the cyber security MS program, including this one, should contribute to overall program level outcomes for students. This course contributes to the following program level goals:

1. **Understand how modern operating systems work (with a leaning towards Unix style OSes).** Be familiar with their security components (identification, authentication, access controls, auditing) and how to configure them.

2. Demonstrate a **foundational understanding of** networking and **network security**. Networking concepts like the 5-layer Internet protocol stack and their components, and **network security concepts including the purposes of firewalls, IDSes and SIEMs are deeply understood.**

7 Knowledge Units

This course covers the following NSA cybersecurity Knowledge Units:

1. IT Systems Components (ISC, Foundational CDE)

2. Basic Networking (BNW, Core Technical CDE)

3. Network Defense (NDF, Core Technical CDE)

4. Advanced Network Technology and Protocols (ANT, Optional KU)

5. Systems Programming (SPG, Optional KU)

8 Attendance Policy

Regular attendance is expected. Students are responsible for all material covered in class, including announcements and handouts.

9 Academic Integrity

All work submitted for this course must be the student's own original work. Any instance of plagiarism or cheating will be dealt with according to the university's academic integrity policy. Refer to the Student Rights and Responsiblities, as well as the University of Denver Student Honor code, here: `https://studentaffairs.du.edu/student-rights-responsibilities`

10 Disability Services

If you have a disability that may affect your ability to complete the work for this course, please contact the Disability Services office at: `https://studentaffairs.du.edu/disability-services-progr`