UCA STUDENT SYLLABUS

NARYN CAMPUS

COURSE TITLE: Information Security

COURSE #: COMP 4031

Timing: 90-minute classes.

Number of Weeks: 16 weeks.

Course Faculty (and office number): Dr. Ayman ALJARBOUH, office 3.14.

Office Hours: Thursday from 15:00 to 17:00.

Contact information: ayman.aljarbouh@ucentralasia.org.

Prerequisites and/or Corequisites (if applicable): Operating Systems, Computer Networks, Fundamentals of Programming.

Last updated: January 19, 2023.

Course Description

This course introduces the core security concepts and skills needed to monitor, detect, analyze and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes the practical application of the skills needed to maintain and ensure security operational readiness of secure networked systems. This course aligns with the Cisco Certified CyberOps Associate certification. Students who successfully complete this course will acquire the knowledge and skills that are required to pass the certification.

Course Learning Outcomes

By the end of the course, students will be able to:

1. Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
2. Explain the role of the Cybersecurity Operations Analyst in the enterprise.
3. Explain the features and characteristics of the Linux Operating System.
4. Analyze the operation of network protocols and services.
5. Explain the operation of the network infrastructure.
6. Classify the various types of network attacks.
7. Use network monitoring tools to identify attacks against network protocols and services.
8. Explain how to prevent malicious access to computer networks, hosts, and data.
9. Explain the impacts of cryptography on network security monitoring.
10. Explain how to investigate endpoint vulnerabilities and attacks.
11. Evaluate network security alerts.
12. Analyze network intrusion data to identify compromised hosts and vulnerabilities.
13. Apply incident response models to manage network security incidents.

Course Organization

This course is designed for students who are seeking career-oriented, entry-level security analyst skills. Students in this course are exposed to all the foundational knowledge required to detect, analyze, and escalate basic cybersecurity threats using common open-source tools. This course contains numerous opportunities for practicing and assessing student skills through various types of assessments and labs. This course includes videos, labs, Packet Tracer activities, Quizzes, and Exams.

Equipment List

This course uses one of two virtual machines (VM) for many of the labs. Only one VM is required to be run at a time in any lab that uses a VM. The lab should meet the following requirements:

- Host computer using 64-bit processor with at least 8 GB of RAM and 40 GB of free disk space.
- Latest version of Oracle VirtualBox.
- Internet connection.

Core literacies

- Creative thinking (Network Security).
- Quantitative (Solving various algorithmic and encryption/decryption problems).
- Written communication (Lab reports).

- Inquiry and Analysis (Security System Analysis, Social Engineering, Digital Forensics).
- Problem Solving (Applying different attacks on Information infrastructure for Security evaluation).

Attendance Policy

The university views class attendance as your individual responsibility. You are expected to attend all classes, complete all assignments, and take all exams as scheduled. Instructors will take attendance every class. If you miss more than 10 % of class time, you may not be able to write the final exam or get credit for the course. Each absence from a class session or part of a class session must be justified in writing to the faculty member. If you are late for class, the instructor may mark you as absent. See UCA's Attendance Policy to understand all your rights and obligations.

Academic Integrity

You are reminded that plagiarism (representing another person's ideas, writings, etc., as one's own) is a serious academic offence; the penalty can be as severe as expulsion. Students must write their essays and assignments in their own words. Whenever students take an idea, or a passage from another author, they must acknowledge their debt both by using quotation marks where appropriate and by proper referencing such as footnotes or citations. Plagiarism is a major academic offence (see UCA's Academic Integrity Policy). All required papers may be subject to submission for textual similarity review to the commercial plagiarism detection software under license to the University for the detection of plagiarism. All papers submitted will be included as source documents in the reference database for the purpose of detecting plagiarism of papers subsequently submitted to the system. Use of the service is subject to the licensing agreement, currently between UCA and Turnitin.com. See UCA's Academic Integrity Policy to understand all your rights and obligations.

Required Resources/Textbook Readings

Resources: Library (for articles, readings), IT support (for Moodle – materials to be uploaded, Turnitin for plagiarism check).

Textbook: None.

Recommended books:

- Principles of Information Security, July 2021; Authors: Michael E. Whitman, Herbert J. Mattord. ISBN 9780357506493.
- Foundations of Information Security: A Straightforward Introduction by Jason Andress, October 7, 2019.
- Cyber Security: The Lifeline of Information and Communication Technology by Ramjee Prasad, October 17, 2019.

Course Assessments and Grading

Item	Weight
Attendance (weekly attendance)	12%
Quizzes (4 quizzes)	16%
Lab assignments (42 labs)	22%
Midterm exam (Assessments that assess content from multiple modules)	20%
Final exam (Assessments that assess content from multiple modules)	30%
Total	**100%**

Course Calendar

Week	Topic	Labs and Quizzes

1	• Course Introduction
	• Cybersecurity and the Security Operations Center:
	  ○ The Danger
	  ○ Fighters in the War Against Cybercrime
		• Lab 1 - Installing the Virtual Machines
		• Lab 2 - Learning the Details of Attacks
		• Lab 3 - Cybersecurity Case Studies
		• Lab 4 - Understand Vulnerabilities of Wireless and Other Common Technologies

2	• Linux Operating System
	  ○ Linux Overview (Linux Basics, Working in the Linux Shell, Linux Servers and Clients)
	  ○ Linux Administration (Basic Server Administration, The Linux File System)
	  ○ Linux Hosts (Working with the Linux GUI, Working on a Linux Host)
		• Lab 5 – Working with Text Files in the CLI
		• Lab 6 - Navigating the Linux Filesystem and Permission Settings
		• Lab 7 – Getting Familiar with the Linux Shell
		• Lab 8 - Linux Servers

3	• Network Protocols and Services
	  ○ Network Protocols
	  ○ Ethernet and Internet Protocol (IP)
		• Lab 9 – Tracing a Route
		• Lab 10 - Introduction to Wireshark
		• Quiz 1

4	• Network Protocols and Services
	  ○ Connectivity Verification
	  ○ Address Resolution Protocol
		• Lab 11 – Verify IPv4 and IPv6 Addressing
		• Lab 12 – Using Wireshark to Examine Ethernet Frames

5	• Network Protocols and Services
	  ○ The Transport Layer
	  ○ Network Services
		• Lab 13 – Using Wireshark to Observe the TCP 3-Way Handshake
		• Lab 14 - Using Wireshark to Examine a UDP DNS Capture

		• Lab 15 - Exploring Nmap • Lab 16 - Using Wireshark to Examine HTTP and HTTPS Traffic

6	• Network Infrastructure
	  ○ Network Representation and Security Infrastructure
	  ○ Network Communication Devices
		• Lab 17 - Identify Packet Flow
		• Lab 18 - ACL Demonstration
		• Quiz 2

7	• Principles of Network Security
	  ○ Attackers and Their Tools (Who is Attacking our Network?, Threat Actor Tools)
	  ○ Common Threats and Attacks (Malware, Common Network Attacks - Reconnaissance, Access, and Social Engineering, Network Attacks - Denial of Service, Buffer Overflows, and Evasion)
		• Lab 19 - Anatomy of Malware
		• Lab 20 – Social Engineering
		• Lab 21 - Explore Social Engineering Techniques

8	Midterm Exam	

9	• Network Attacks: A Deeper Look
	  ○ Network Monitoring and Tools
	  ○ Attacking the Foundation
	  ○ Attacking What We Do
		• Lab 22 - Logging Network Activity
		• Lab 23 - Attacking a mySQL Database
		• Lab 24 - Reading Server Logs

10	• Cryptography and the Public Key Infrastructure
	  ○ Cryptography (What is Cryptography?, Integrity and Authenticity, Confidentiality)
	  ○ Public Key Cryptography (Public Key Cryptography, Authorities and the PKI Trust System, Applications and Impacts of Cryptography)
		• Lab 25 - Creating Codes
		• Lab 26 - Hashing Things Out
		• Lab 27 - Encrypting and Decrypting Data Using OpenSSL
		• Lab 28 - Encrypting and Decrypting Data using a Hacker Tool
		• Lab 29 – Certificate Authority Stores

11	• Protecting the Network
	  ○ Understanding Defense
	  ○ Access Control
	  ○ Threat Intelligence
		• Lab 30 - Examining Telnet and SSH in Wireshark
		• Lab 31 - The Cybersecurity Cube Scatter Quizlet
		• Quiz 3

12	• Security Monitoring
	  ○ Technologies and Protocols
	  ○ Network Security Data
		• Lab 32 - Logging from Multiple Sources
		• Lab 33 - Explore a NetFlow Implementation

13	• Intrusion Data Analysis
	  ○ Evaluating Alerts
	  ○ Working with Network Security Data
		• Lab 34 - Snort and Firewall Rules
		• Lab 35 - Convert Data into a Universal Format
		• Lab 36 – Regular Expression Tutorial
		• Lab 37 – Extract an Executable from a PCAP

14	• Endpoint Security and Analysis
	  ○ Endpoint Protection (Antimalware Protection, Host-based Intrusion Prevention, Application Security)
	  ○ Endpoint Vulnerability Assessment (Network and Server Profiling, Common Vulnerability Scoring System (CVSS), Secure Device Management, Information Security Management Systems)
		• Lab 38 – Interpret HTTP and DNS Data to Isolate Threat Actor
		• Lab 39 – Isolate Compromised Host Using 5-Tuple
		• Lab 40 – Investigate a Malware Exploit
		• Quiz 4

15	• Digital Forensics and Incident Analysis and Response
	  ○ Evidence Handling and Attack Attribution
	  ○ The Cyber Kill Chain
	  ○ The Diamond Model of Intrusion Analysis
	  ○ Incident Response
		• Lab 41 - Incident Handling
		• Lab 42 – Investigating an Attack on a Windows Host

16	Final Exam	

Note that the schedule is subject to change as the course progresses.