



Graduate Course Syllabus

IT 643: Network Assessment and Defense

Center: Online

Course Prerequisites

IT 549 and IT 640

Course Description

Explore a broad range of topics from secure network fundamentals, protocols, and analysis; threats and vulnerabilities; application, data, and host security; access control; and identity management. Examine defensive measures to secure an organization's network. Identify overall network security posture and the basic practices in vulnerability assessment.

Course Outcomes

- Interpret results of network and vulnerability scans for identifying security vulnerabilities
- Implement appropriate methods that protect against and address network threats and vulnerabilities using appropriate risk mitigation techniques
- Assess the severity of security incidents using industry best practices to determine the appropriate immediate response
- Recommend timely countermeasures that minimize the consequences of current security incidents
- Communicate response and mitigation strategies that align with an organization's strategic goals

Required Materials

Using your learning resources is critical to your success in this course. Please purchase directly through the [SNHU Online Bookstore](#) rather than any other vendor. Purchasing directly from the bookstore ensures that you will obtain the correct materials and that the IT Service Desk, your advisor, and the instructor can provide you with support if you have problems..

InfoSec

Your course uses virtual labs from InfoSec Learning. You will need to purchase an access code for InfoSec, a cloud-based lab environment.

- Go to the [InfoSec Learning Website](#) to register.
- When prompted, please use the course ID **PBIWDUKQSY** to complete your registration and gain access.

Diversity, Equity, and Inclusion

As indicated in our core values, SNHU is committed to “embrace diversity where we encourage and respect diverse identities, ideas, and perspectives by honoring difference, amplifying belonging, engaging civilly, and breaking down barriers to bring our mission to life.”

This may or will be reflected in SNHU’s curriculum as we embrace and practice diversity, equity, and inclusion (DEI) to provide the most transformative experience for our students, faculty, and staff. Because topics pertaining to DEI can be sensitive, please remember that embodying and practicing diversity, equity, and inclusion is one of our core values that you will encounter throughout the academic experience. In higher education, we are expected to think and engage critically. Use a growth mindset to embrace the diverse readings, course assignments, and experiences of your peers and faculty.

For more information about DEI at SNHU, please visit our website at the [Office of Diversity and Inclusion](#).

Instructor Availability and Response Time

Your class interaction with the instructor and your classmates will take place on a regular, ongoing basis. Your instructor will be actively engaged within the course throughout the week. You will normally communicate with your instructor in the weekly discussions or the General Questions discussion topic so that your questions and the instructor’s answers benefit the entire class. You should feel free, however, to communicate with your instructor via SNHU email at any time, particularly when you want to discuss something of a personal or sensitive nature. Your instructor will generally provide a response within 24 hours. Instructors will post grades and feedback (as applicable) within seven days of an assignment’s due date, or within seven days of a late submission.

Grade Distribution

Assignment Category	Number of Graded Items	Point Value per Item	Total Points
Discussions	9	20	180
InfoSec Labs	16	15	240
Training Manual Draft: Purpose	1	20	20
Training Manual Drafts	6	30	180
Final Project	1	380	380
			Total Course Points: 1,000

This course may also contain practice activities. The purpose of these non-graded activities is to assist you in mastering the learning outcomes in the graded activity items listed above.

University Grading System: Graduate

Grade	Numerical Equivalent	Points
A	93–100	4.00
A-	90–92	3.67
B+	87–89	3.33

Grade	Numerical Equivalent	Points
B	83–86	3.00
B-	80–82	2.67
C+	77–79	2.33
C	73–76	2.00
F	0–72	0.00
I	Incomplete	
IF	Incomplete/Failure *	
W	Withdrawn	

* Please refer to the [policy page](#) for information on the incomplete grade process.

Grading Guides

Specific activity directions, grading guides, posting requirements, and additional deadlines can be found in the Assignment Guidelines and Rubrics section of the course.

Weekly Assignment Schedule

All reading and assignment information can be found within each module of the course. Assignments and discussion posts during the first week of each term are due by 11:59 p.m. Eastern Time. Assignments and discussion posts for the remainder of the term are due by 11:59 p.m. of the student's local time zone.

In addition to the textbook readings that are listed, there may be additional required resources within each module.

Module	Topics and Assignments
1	Introduction to Traffic Analysis 1-1 Discussion: Traffic Analysis 1-2 Lab: TCP/IP Protocols - The Core Protocols: Networking Fundamentals 1-3 Lab: Capturing and Analyzing Network Traffic Using a Sniffer: Ethical Hacking and System Defense 1-4 Draft of Training Manual: Purpose 1-5 Final Project Review
2	Traffic Analysis Tools and Methodologies 2-1 Discussion: Traffic Analysis Scenario 2-2 Lab: Examining Wireless Networks 2-3 Lab: Deep Dive in Packet Analysis Using Wireshark and Network Miner: Information Security Fundamentals 2-4 Draft of Training Manual Section One: Traffic Analysis
3	Firewall Setup and Configuration 3-1 Discussion: Firewall Setup 3-2 Lab: Network Security - Firewalls: Network Fundamentals 3-3 Lab: Configuring a Windows Firewall to Allow Incoming Traffic: Network Fundamentals

Module	Topics and Assignments
4	Adapting Firewall Rules 4-1 Discussion: Firewall Configuration 4-2 Lab: Configuring a Linux-Based Firewall to Allow Ingoing and Outgoing Traffic: Information Security Fundamentals 4-3 Lab: Securing the pfSense Firewall: Information Security Fundamentals 4-4 Draft of Training Manual Section Two: Firewall Configuration
5	Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) 5-1 Discussion: Network Access Control Scenario 5-2 Lab: Intrusion Detection Using Snort: Network Security Fundamentals 5-3 Lab: Writing Custom Rules: Network Security Fundamentals 5-4 Draft of Training Manual Section Three: Intrusion Detection
6	Vulnerability Scanning 6-1 Discussion: Detecting Vulnerabilities in a Network 6-2 Lab: Vulnerability Scanning of a Linux Server: Linux Based Security+ 6-3 Lab: Perform Reconnaissance from the WAN: Ethical Hacking and System Defense 6-4 Draft of Training Manual Section Four: Vulnerability Assessment
7	Network Assessment 7-1 Discussion: Detecting Rogue Devices and Malicious Connections 7-2 Lab: Signature Detection and Alerting an Admin: Pen-Testing and Understanding Vulnerabilities 7-3 Lab: Scanning the Network on the LAN: Ethical Hacking and System Defense 7-4 Draft of Training Manual Section Five: Network Scanning
8	Auditing and Log Completion 8-1 Discussion: Audit Log Components 8-2 Lab: Log Analysis of Linux Systems with GREP and GAWK: Linux Based Security+ 8-3 Lab: IPS, SYSLOG, and NTP: Pen-Testing and Understanding Vulnerabilities 8-4 Draft of Training Manual Section Six: Auditing and Log Collection
9	Network Security Training Manual Compilation 9-1 Final Project: Executive Overview 9-2 Final Project Submission: Network Security Training Manual
10	Incident Reporting 10-1 Discussion: Incident Reporting Process

Course Participation

Course participation is required within the first week of the term for all online courses. *Participation* in this context is defined as completing one graded assignment during the first week of the course. Otherwise, students will be administratively removed for nonparticipation. Students who do not participate during the first week may forfeit their rights to be reinstated into the course. Students who stop attending a course after the first week and who do not officially withdraw will receive a grade calculated based on all submitted and missed graded assignments for the course. Missed assignments will earn a grade of zero. See the [course withdrawal policy](#) and the [full attendance policy](#) for further information.

Late Assignments

Students who need extra time may submit assignments (excluding discussion board postings) up to one week after the assignment due date. Discussion board submissions will not be accepted for credit after the deadline except in extenuating circumstances.

- A penalty of 10 percent of the total value of the assignment will be applied to the grade achieved on the late assignment regardless of the day of the week on which the work is submitted.
- Students who submit assignments more than one week late will receive a grade of zero on the assignment unless they have made prior arrangements with the instructor.

Students must submit all assignments no later than 11:59 p.m. (in their own time zone) on the last day of the term. No assignments are accepted after the last day of the term unless an incomplete has been submitted. See the [incomplete grades policy](#).

There may be times an instructor makes an exception to the late assignment policy. Instructors may accept late work, including discussion board posts, with or without prior arrangement.

- Exceptions to the late policy on these grounds are left to the instructor's discretion, including whether the late penalty is applied or waived. Students should not assume that they will be allowed to submit assignments after the due dates.
- If an instructor finds that they are unable to determine whether an exception to the late policy would be appropriate without documentation, the collection and review of student documentation should be handled through the Dispute Resolution team in order to protect the student's privacy. In these cases, students should file a [Student Concern Dispute form](#) to have the circumstances reviewed.

If a student is experiencing (or knows they will experience) a circumstance, including pregnancy, that is protected under the Americans with Disabilities Act or Title IX, they are encouraged to contact the [Online Accessibility Center \(OAC\)](#) as soon as possible to explore what academic accommodations might be offered. Instructors must honor all deadlines established through the OAC.

Student Handbook

Review the [student handbook](#).

ADA/504 Compliance Statement

Southern New Hampshire University (SNHU) is dedicated to providing equal access to individuals with disabilities in accordance with Section 504 of the Rehabilitation Act of 1973 and with Title III of the Americans with Disabilities Act (ADA) of 1990, as amended by the Americans with Disabilities Act Amendments Act (ADAAA) of 2008.

SNHU prohibits unlawful discrimination on the basis of disability and takes action to prevent such discrimination by providing reasonable accommodations to eligible individuals with disabilities. The university has adopted the [ADA/504 Grievances Policy](#) (version 1.2 effective October 16, 2017), providing for prompt and equitable resolution of complaints regarding any action prohibited by Section 504 or the ADA.

For further information on accessibility support and services, visit the [Disability and Accessibility Services](#) webpage.

Academic Integrity Policy

Southern New Hampshire University requires all students to adhere to high standards of integrity in their academic work. Activities such as plagiarism and cheating are not condoned by the university. Review the [full academic integrity policy](#).

Copyright Policy

Southern New Hampshire University abides by the provisions of United States Copyright Act (Title 17 of the United States Code). Any person who infringes the copyright law is liable. Review the [full copyright policy](#).

Withdrawal Policy

Review the [full withdrawal policy](#).

Southern New Hampshire University Policies

More information about SNHU policies can be found on the [policy page](#).