Revised 8/2023

NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 266 – NETWORK SECURITY LAYERS (3 CR.)

Current information on NOVA's Cybersecurity Program is located at www.nvcc.edu/cybersecurity

Course Description

Provides an in-depth exploration of various security layers needed to protect the network. Explores Network Security from the viewpoint of the environment in which the network operates and the necessity to secure that environment to lower the security risk to the network. Includes physical security, personnel security, operating system security, software security and database security. Lecture 3 hours per week.

General Course Purpose

The purpose of this course is to introduce the student to the tools and concepts used at different layers to protect our network assets. Students will be expected to understand how to install and “harden” Windows servers and Linux servers through the application of patches, removing unnecessary services and accounts, and using vulnerability scanners (i.e. Nessus, GFI LanGuard) to identify and remediate vulnerabilities within the O/S or application. This course also includes content, as indicated below in parenthesis behind each learning objective, which directly maps to DHS/NSA’s Center of Academic Excellence – 2 Year (CAE2Y) criteria.

Course Prerequisites/Corequisites

Prerequisite: ITN 260

Course Objectives

Upon completion of this course, the student will have a working knowledge of:

A. The danger to the network presented by trusted employees
B. The concept and principles of in-depth security
C. Physical and personnel security
D. Operating system, application software, and database security

Course Content

1.0 Physical Security
2.0 Personnel Security
3.0 Computer System Security
4.0 Local Area Network Security
5.0 Application Software Security
6.0 Communication Security
7.0 Database Security

Student Learning Outcomes

1.0 Physical Security (CSF)

1.1 Understand the operating environment of the network and the need for physical security.
1.2 Identify the threats to security that are unique to physicals security.
1.3 Identify and explain the access controls necessary to physically secure a network facility.
1.4 Understand the necessity for a fire safety program in securing the physical facility.
1.5 Identify and describe the components of fire detection and response.
1.6 Understand the necessity to secure the supporting facilities such as heating, air conditioning, temperature, humidity, etc.
1.7 Understand the technical details associated with Uninterruptible Power Supplies (UPS) and their ability to increase availability.
1.8 Understand and explain the countermeasures to the physical theft of computer or network devices.
1.9 Understand the necessity to maintain an accurate physical inventory of all computer and network devices.

2.0 Personnel Security (CPM) (CSP)

2.1 Understand how the organization’s employment policies support organizational security.

2.2. Understand the need for the separation of duties.
2.3 Understand the relationship and interaction between the employee job description, performance evaluation, the standards manual and security.
2.4 Understand the relationship between reference checks, background investigations, interviews.
2.5 Understand the impact of employee education, employee relationships and management and supervisory practices upon security.
2.6 Understand how continuous employee observation, job rotations, access control and adherence to standards impact security.
2.7 Understand how terminations due to events such as promotion, resignation, death, retirement, layoff and firing (hostile terminations) should be handled and their potential impact upon security.

3.0 Computer System Security (OSC, OSA, OSH)
3.1 Identify and explain the key Linux security components.
3.2 Identify and explain the Linux file systems controls.
3.3 Identify and explain the Linux files used to manage network functions.
3.4 Identify and explain Linux network running process and networking commands.
3.5 Describe the various techniques for hardening Linux operating system applications.
3.6 Identify and explain the key Windows server security components.
3.7 Identify and explain the value of the Active Directory and its role in security.
3.8 Identify and explain Windows server authentication methods.
3.9 Identify and explain Windows server user and group security methodologies.
3.10 Understand the Windows server security configuration tools, file and folder security, EFS, NAT, and IPSec
3.11 Understand the importance of patching and maintaining O/S updates and vulnerability windows.
3.12 Demonstrate the application of cyber defense methods to prepare a Linux or Windows system to repel attacks.

4.0 Local Area Network Security (ANT, BNW, NDF, IDS)
4.1 Understand the design of the network and its impact upon network security.
4.2 Understand and explain the components relating to end user access.
4.3 Describe the value associated with policy based security management of the network.
4.4 Understand the impact on network security of IP address assignment.
4.5 Understand the different network media types, their threats and how best to secure them.
4.6 Explain the impact of cable installation on security particularly with regard to plenum cables and risers.
4.7 Understand the threats against routers, hubs and switches and how best to secure them.
4.8 Understand the employment of firewalls, IDS and auditing in securing the network.

5.0 Application Software Security (SPP, ISC)
5.1 Understand and explain the software development life cycle and its relation to security.
5.2 Understand and explain software quality assurance and its relation to security.
5.3 Understand and explain software configuration management and its relation to security.
5.4 Understand and explain software testing and its relation to security.
5.5 Identify and explain the various type of malicious code.
5.6 Understand the buffer overflow problem and the threat it poses to security.
5.7 Understand the importance of maintaining application patches and updates.
5.8 Understand the importance of hardening applications and resources available (i.e. DISA STIGs).

6.0 Communication Security (BCY, NDF)
6.1 Understand the OSI seven layer communication model and the TCP model.
6.2 Identify and explain the threats various attacks against the communication systems and their countermeasures.
6.3 Discuss the process of encryption and its key terms.
6.4 Understand the difference between symmetric and asymmetric encryption.
6.5 Understand digital signatures and Public key Encryption (PKE).

6.6 Understand IPSec and Virtual Private Networks (VPN).

6.7 Understand and explain the issues surrounding email security and privacy.

7.0 Database Security (DBA, DAT)

7.1 Understand the concept of a database and the database terms (including aggregation, polyinstantiation, data mining, inference, etc.).

7.2 Understand the different type database and the components that compose database.

7.3 Understand the issues associated with physical database integrity, logical database integrity, element integrity, auditability, access control, user authentication and availability.

7.4 Understand and explain the issue of two-phase, data redundancy and internal consistency.

7.5 Understand the issue associated with indirect attacks against databases that report only statistical data.

7.6 Understand the security issues associated with multilevel database.

7.7 Understand the importance of hardening a database and resources available (i.e. DISA STIGs).

CAE2Y Knowledge Unit Domain Index

KU Category	Course Content KU Mapping	CAE2Y KU Name	Description
Foundational CDE Knowledge Units	CSF	Cybersecurity Foundations	Provide students with a basic understanding of the fundamental concepts behind cybersecurity. This is a high level introduction or familiarization of the Topics, not a deep dive into specifics.
	CSP	Cybersecurity Principles	Provide students with basic security design fundamentals that help create systems that are worthy of being trusted.
	ISC	IT Systems Components	Provide students with a basic understanding of the components in an information technology system and their roles in system operation. This is a high level introduction or familiarization of the Topics, not a deep dive into specifics.
Core Technical CDE Knowledge Units	BCY	Basic Cryptography	Provide students with a basic ability to understand where and how cryptography is

			used.
	BNW	Basic Networking	Provide students with basic understanding of how networks are built and operate, and to give students some experience with basic network analysis tools. Students are exposed to the concept of potential vulnerabilities in a network.
	NDF	Network Defense	Provide students with knowledge of the concepts used in defending a network, and the basic tools and techniques that can be taken to protect a network and communication assets from cyber threats.
	OSC	Operating Systems Concepts	Provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.
Core Non-Technical CDE Knowledge	CPM	Cybersecurity Planning and Management	Provide students with the ability to develop plans and processes for a holistic approach to cybersecurity for an organization.
Optional Knowledge Units	ANT	Advanced Network Technology and Protocols	Provide students with an understanding of advanced networking concepts, including the latest network technologies and more complex security issues involved in network communications.

			Examples may include (but are not limited to): software defined networking, converged voice/data networking.
	DAT	Database	Teach students how database systems are used, managed, and issues associated with protecting the associated data assets.
	DBA	Data Administration	provide students with methods to protect the confidentiality, integrity, and availability of data throughout the data life cycle.
	IDS	Intrusion Detection/Prevention Systems	Provide students with knowledge and skills related to detecting and analyzing vulnerabilities and threats and taking steps to mitigate associated risks.
	OSA	Operating Systems Administration	Provide students with skill to perform basic operations involved in system administration of operating systems.
	OSH	Operating Systems Hardening	Provide students with the ability to apply methods such as managing applications, services, and network ports to improve the robustness of operating systems.
	SPP	Secure Programming Practices	Provide students with an understanding of the characteristics of secure programs and the ability to implement programs that are free from vulnerabilities.

NOTE: the course content KU mapping represents the KU Domain topic as shown in the Center of Academic Excellence (CAE) KU mapping matrix (Excel file).

Required Time Allocation per Topic

In order to standardize the core topics of ITN 266 so that a course taught at one campus is equivalent to the same course taught at another campus, the following student contact hours per topic are required. Each syllabus should be created to adhere as closely as possible to these allocations. Of course, the topics cannot be followed sequentially. Many topics are taught best as an integrated whole, often revisiting the topic several times, each time at a higher level. There are normally 42 student-contact-hours per semester for a three credit course. (This includes 14 weeks of instruction and does not include the final exam week so 14* 3 = 42 hours. Sections of the course that are given in alternative formats from the standard 15 week section still meet for the same number of contact hours.) The final exam time is not included in the time table. The category, Other Optional Content, leaves ample time for an instructor to tailor the course to special needs or resources.

Topic	Time in Hours	Percentages
Physical Security	3	7%
Personnel Security	3	7%
Computer System Security	7	17%
Local Area Network Security	7	17%
Application Software Security	6	14%
Communication Security	3	7%
Database Security	3	7%
Exams, Quizzes, Exercises	7	17%
Other Optional Content	3	7%
Total	42	100%