Revised 8/2023

NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 260 – NETWORK SECURITY BASICS (3CR.)

Course Description

Provides instruction in the basics of network security in depth. Includes security objectives, security architecture, security models and security layers, risk management, network security policy, and security training. Includes the give security keys, confidentiality integrity, availability, accountability, and auditability. Lecture 3 hours per week.

General Purpose

The purpose of this course is to instill the basics of network security (aka "information assurance") as well as also serve as a resource to help the student with pursuing CompTIA's Security+ certification. As such, textbooks are selected that map directly to the Security+ certification exam concepts. This course also includes content, as indicated below in parenthesis behind each learning objective that directly maps to DHS/NSA's Center of Academic Excellence – 2 Year (CAE2Y) criteria. Current information on NOVA's Cybersecurity Program is located at www.nvcc.edu/cybersecurity

Course Prerequisite/Corequisite

Prerequisites: ITN 100 or ITN 101 or networking/network protocols knowledge

Course Objectives

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

- Network security basics, security architecture and design, and security models.
- Network security planning, risk management and policy
- Network security technology and tools
- Network security organization
- Legal, privacy and ethical issues
- Application of Cryptography and PKI

Major topics to be Included

- Network security basics, threats, attacks, and vulnerabilities
- Network security planning, risk management and policy
- Network security technology and tools
- Network security organization
- Legal, privacy and ethical issues
- Application of Cryptography and PKI

Student Learning Outcomes

1.0 Network security basics, threats, attacks, and vulnerabilities (NBW, CSF, NDF, CTH, VLA, CCR)

- 1.1 Understand computer, network and information security, including information in its various states; processing, storage, and transmission.
- 1.2 Explain why network security is important
- 1.3 Explain network security prevention, detection and response.
- 1.4 Define and explain the concept of network confidentiality.
- 1.5 Define and explain the concept of information integrity.
- 1.6 Define and explain the concept of network availability.
- 1.7 Define and explain the concept of network auditability.
- 1.8 Define and explain the concept of non-repudiation.

1.9 Understand management's role in the development, implementation and maintenance of network security.
1.10 Understand the value of education, training and awareness programs to the organization.
1.11 Understand security architecture, it's principles, components and employment,
1.12 Understand the security design process and performance measures used to validate security architecture.
1.13 Understand basic attacks (i.e. password guessing/cracking, backdoors, viruses, ransomware, sniffing, session hijacking, DoS, DDoS, botnets, MAC and IP Spoofing, web app attacks, zero day exploits, and the vulnerabilities that enable them).
1.14 Social engineering (phishing, vishing, tailgating, impersonation, dumpster diving, shoulder surfing)
1.15 Understand the concept of Attack Timing and zero day attacks.
1.16 Understand insider threat to the organization.
1.17 Explain vulnerability scanning concepts

2.0 Network security planning, risk management and policy (NDF, NSA, ISC)
2.1 Define risk management and its role in security policy and security architecture.
2.2 Understand the relationship between risk, threats, vulnerabilities and countermeasures.
2.3 Identify and describe risk assessments and mitigation strategies.
2.4 Define and understand how to prepare a Security Plan.
2.5 Define and describe Disaster Recovery Plans
2.6 Define and describe an Incident Response Plan, include evidence collection and preservation procedures.
2.7 Define and describe a Business Continuity Plan.
2.8 Describe the various functions related to database security.
2.9 Describe and understand a feasibility study with respect to risk management.
2.10 Understand the need for constantly evaluating the status of security management.
2.11 Understand the difference between policies, procedures, standards and guidelines.
2.12 Describe the importance of backing up data and files to the importance of data integrity and recovery.
2.13 Describe the importance of Configuration Management
2.14 Demonstrate the ability to analyze trends and issues and their impact on security, including BYOD issues.

3.0 Network Security Technology and tools (NDF, NSA, CCO, VTT, CSP)
3.1 Understand the process of encryption and define the key cryptography terms.
3.2 Understand the difference between asymmetric and symmetric encryption.
3.3 Describe scanning and analysis tools.
3.4 Describe the various types of firewalls.
3.5 Describe the various types of Intrusion Detection Systems and Intrusion Prevention Systems.
3.6 Understand the difference between Host Based Intrusion Detection and Network Based Intrusion Detection.
3.7 Describe the operation of Virtual Private Networks.
3.8 Understand the difference between identification and authentication, the characteristics of a good password, and the importance of multifactor authentication.
3.9 Describe the various approaches to biometrics access control.
3.10 Describe the threats and controls to physical security, including equipment, environmental controls, building construction, cabling systems, and equipment/voice emanations.
3.11 Describe various approaches to securing media, media storage controls, secure off-site transport of media, and media destruction and sanitization methods.
3.12 List and describe various access control methods, including mandatory, discretionary and role-based access controls.
3.13 Explain the significance of concepts such as defense-in-depth, job rotation, separation of duties, mandatory vacation, and least privilege.

3.14 Describe administrative controls, including securing documentation and logs.
3.15 Describe the security issues and controls of using dial up versus dedicated transmission lines, including end-to end access control, privileges (class, nodes), public versus private, covert channels, and traffic analysis.
3.16 Identify the mechanisms for securing data in its various states (in transmission, at rest, and in processing).
3.17 Describe the characteristics of various Security Models such as Bell La-Padula, Biba, and Clark-Wilson.
3.18 Describe basic hardware components of a system, their roles in system operation, and hardening recommendations (to include workstations, network storage devices, routers, gateways, firewalls, switches, mobile devices, and other peripheral devices).
3.19 Describe virtualization platforms and cloud services (SaaS, PaaS, DaaS, IaaS)

4.0 Network Security Organization (NDF)

4.1 Understand the position of the network security element within the organization and the significance of assurance to the concept of trust.
4.2 Understand the skills required to staff the network security element.
4.3 Describe the functional elements associated with network security as mechanisms to implement trust.
4.4 Understand the relationship between an organizations employment practices and policies and the network security function.
4.5 Understand the position of the CIRT element within the security function.
4.6 Explain the various credentials that can be acquired by the security professional and their value.
4.7 Discuss the various roles of organizational personnel, including the audit office, security custodians, security and telecom managers, information managers, executives, purchasing officers, end users, and other organizational roles impacting network security.
4.8 Understand the role of US-CERT and other threat information sources.
4.9 Understand the importance of audits to security.

5.0 Legal, Privacy and Ethical Issues (PLE)

5.1 Identify and explain the major laws, regulations, and standards relating to network security, such as HIPAA, FERPA, Computer Security Act, Sarbanes Oxley, PCI DSS, Gramm-Leach Bliley, State, US, and International Standards/Jurisdictions, Laws and Authorities, US Patriot Act, and Americans with Disabilities Act, Section 508.
5.2 Understand the issue of privacy, privacy laws such as COPPA, and the impact of privacy upon the network security function.
5.3 Understand the issue of ethics and its relationship to the security function.
5.4 Understand the necessity for a code of ethics.
5.5 Understand the potential for organizational liability with regard to network security.
5.6 Understand and describe the tradeoffs security, privacy and operations
5.7 Discuss the organizations and agencies assigned to investigate computer crimes.

6.0 Application of Cryptographic and PKI (BCY)

6.1 Identify the elements of a cryptographic system
6.2 Describe the difference between symmetric and asymmetric algorithms
6.3 Describe common cryptographic protocols
6.3 Understand security functions (data protection, data integrity, authentication, non-repudiation)
6.4 Understand Publik Key Cryptography (RSA, ECC, ElGamal, DSA, Difie-Hellman)
6.5 Understand Certificates

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.
Core Non-Technical CDE Knowledge	CTH	Cybersecurity Planning and Management	Provide students with basic information about the threats that may be present in the cyber realm.
	PLE	Policy, Legal, Ethics, and Compliance	Provide students with and understanding of information assurance in context and the rules and guidelines that control them.
Optional Knowledge Units	CCR	Cyber Crime	Provide students with an understanding of Cyber Crimes and other abuses arising in a cyber environment.
	CCO	Cloud Computing	provide students with a basic understanding of the technologies and services that enable cloud computing, different types of cloud computing models and the security and legal issues associated with cloud computing.
	VLA	Vulnerability Analysis	provide students with a thorough understanding of system vulnerabilities, to include what they are, how they can be found/identified, the different types of vulnerabilities, how to determine the root cause of a vulnerability, and how to mitigate their

			effect on an operational system.
	VTT	Virtualization Technology	provide students with an understanding of how modern host virtualization is implemented, deployed, and used. Students will understand the interfaces between major components of virtualized systems, and the implications these interfaces have for security.

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 260 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 15 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.