NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 263 - INTERNET/INTRANET FIREWALLS AND E-COMMERCE SYSTEMS (4 CR.)

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

Course Description

Gives an in-depth exploration of firewall, Web security, and e-commerce security. Explores firewall concepts, types, topology and the firewall's relationship to the TCP/IP protocol. Includes client/server architecture, the Web server, HTML and HTTP in relation to Web Security, and digital certification, D.509, and public key infrastructure (PKI). Lecture 4 hours per week.

General Course Purpose

The purpose of this course is to allow the student to develop additional knowledge and skills on perimeter network defenses, including firewalls and intrusion detection systems, that provide protection to our corporate data assets. 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 or Corequisites

Prerequisite: ITN 260

Course Objectives

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

A. Firewall concepts, principles, and types
B. Firewall selection, configuration, and employment
C. Securing a Web Server
D. Securing e-Commerce
E. HIDS concepts and principles
F. IDS/IPS concepts and principles
G. Incident Response
H. Forensics Analysis

Course Content

- Firewalls
- Intrusion Detection Systems
- E-Commerce
- Incident Response
- Forensic Analysis

Student Learning Outcomes

1. **Firewalls (NDF)**
   1.1. Specify the main consideration associated with selecting a firewall by organization, and operating systems.
   1.2. Specify the main consideration associated with selecting a firewall by type and firewall.
   1.3. Define the firewall terms and identify the firewall strategies.
   1.4. Explain packet-filtering firewalls.
   1.5. Explain application gateway firewalls
   1.6. Explain circuit level gateway firewalls.
   1.7. Explain stateful inspection firewalls.
   1.8. Explain the different firewall architectures.
   1.9. Explain Network Address Translation (NAT).
   1.10. Specify the firewall security policy tradeoffs.
   1.11. Identify the various sections of a firewall security policy.
   1.12. Given specific protocols, specify generic firewall rules for configuring a firewall.
   1.13. Explain port security

2. **Intrusion Detection Systems (IDS)**
   2.1. Define the intrusion detection terms and their relationship to the security management model.
   2.2. Differentiate between host based intrusion detection system and a network based intrusion detection system.
   2.3. Differentiate between the two primary classes of host based intrusion detection systems.
   2.4. Describe the operation of a host based intrusion detection system.
   2.5. Describe the operation of a network based intrusion detection system.
   2.6. Describe intrusion detection analysis

2.7. Identify and describe the two main approaches to intrusion detection analysis.
2.8. Describe the various automated responses to intrusion detection.

3. E-Commerce (WAS)
3.1. Explain the rational for the concerns regarding electronic commerce.
3.2. Differentiate between the two major e-Commerce models.
3.3. Identify the major goals associated with e-commerce.
3.4. Describe the various functions related to client side security.
3.5. Describe the various functions related to server side security.
3.6. Describe the various functions of application security.
3.7. Describe the various functions related to database security.
3.8. Describe the various elements of a typical E-commerce architecture.
3.9. Define E-commerce security zones and their rational.

4. Incident Response (CPM, SRA)
4.1. Identify the incident response goals.
4.2. Describe the Incident response process.
4.3. Describe the various factors to be considered when preparing for an incident.
4.4. Describe the phases of the risk management process.
4.5. Explain the various functions required to prepare a host for an incident.
4.6. Explain the various functions required to prepare a network for an incident.
4.7. Describe the various considerations related to incident response policies and investigative steps.
4.8. Identify the hardware and software tools required to investigate an incident.
4.9. Explain the composition of a typical incident response team and their functions.
4.10. Describe the various functions related to the initial response to an incident.
4.11. Describe the various functions relating to investigating and assessing an incident.
4.12. Explain the function of restoring a system after an incident.
4.13. Describe the various concerns in evaluating an incident.

5. Forensic Analysis (DVF, HOF, NWF, PLE)
5.1. Explain the typical guidelines related to forensics analysis.
5.2. Describe the hardware and software tools required to conduct a forensics analysis.
5.3. Define the various terms related to forensics analysis.
5.4. Explain the rational for evidence chain of custody.
5.5. Describe the need for trusted binaries in conducting an investigation into a computer incident.
5.6. Describe the most common Unix forensics utilities.
5.7. Describe the most common Windows forensics utilities.
5.8. Explain the process, tools and techniques for recovering Unix volatile data.
5.9. Explain the process, tools and techniques for recovering Windows volatile data.
5.10. Explain the process, tools and techniques for conducting an offline Windows analysis.
5.11. Describe the various consideration related to conducting a network analysis
5.12. Be able to track and identify the packets involved in a simple TCP connection using Wireshark.

CAE2Y Knowledge Unit Domain Index

KU Category	Course Content KU Mapping	CAE2Y KU Name	Description
Core Technical CDE Knowledge Units	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	CPM	Cybersecurity Planning and Management	Provide students with the ability to develop plans and processes for a holistic approach to

			cybersecurity for an organization.
	PLE	Policy, Legal, Ethics, and Compliance	Provide students with and understanding of information assurance in context and the rules and guidelines that control them.
	SRA	Security Risk Analysis	Provide students with sufficient understanding of risk assessment models, methodologies and processes such that they can perform a risk assessment of a particular systems and recommend mitigations to identified risks.
Optional Knowledge Units	DVF	Device Forensics	Provide students with the ability to apply forensics techniques to investigate and analyze a device.
	HOF	Host Forensics	Provide students with the ability to apply forensics techniques to investigate and analyze a host in a network.
	IDS	Intrusion Detection Systems	Provide students with knowledge and skills related to detecting and analyzing vulnerabilities and threats and taking steps to mitigate associated risks.
	NWF	Network Forensics	Provide students with the ability apply forensics techniques to investigate and analyze network traffic.
	WAS	Web Application Security	Provide students with an understanding of technology, tools, and practices associated with web applications.

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 263 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 60 student-contact-hours per semester for a four credit course. (This includes 15 weeks of instruction and does not include the final exam week so 15* 4 = 60 hours. Sections of the course that are given in alternative formats from the standard 16 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
Firewalls	16	27%
Intrusion Detection Systems	16	27%
E-Commerce	1	2%
Incident Response	3	5%
Forensic Analysis	6	10%
Exams, Quizzes	8	13%
Other Optional Content	10	17%
Total	60	100%