



# **National CyberWatch Center Information Security Curricula**

---

**A Complete Solution for Higher  
Education Institutions**

A grayscale background image showing a close-up of hands typing on a laptop keyboard. Overlaid on this image are various digital graphics: a world map, a circular gauge showing '20%', and a percentage sign '%'. A blue vertical bar is positioned on the left side of the page, partially overlapping the white box containing the website address.

**NATIONALCYBERWATCH.ORG**

# About National CyberWatch



*In October 2016, the National Science Foundation (NSF) awarded Prince George’s Community College a \$4.8 million National Advanced Technological Education (ATE) Center continuation grant for its National CyberWatch Center project. The grant allows National CyberWatch to build on a 10+-year foundation of success, as evidenced by four successive NSF ATE grants since 2005.*

National CyberWatch has achieved major national impact in cybersecurity education by establishing and validating national and Federal education and training standards; creating an annual conference (Community College Cyber Summit) focused on cybersecurity education at the community college level; developing and validating cybersecurity skills using performance-based assessments, which are scalable across many industry certifications, curricula, job roles, and verticals; and building new cybersecurity curricula, the first to align instructional design, skill practice facilities, cybersecurity professional job performance standards, national workforce frameworks, and industry needs, which are desperately needed to guide responsible curriculum development for the new generation of Information Security specialists, to name just a few of the Center’s more notable successes.

The Center’s strategic and leadership role as the national ATE center for cybersecurity is to build, promote, and coordinate:

1. Programs and services designed to attract large numbers of diverse populations
2. Career readiness programs
3. Skills-based curricula
4. Collaboration among industry, government, and academia
5. Educational, training, and assessment standards for the burgeoning Information Security discipline, and
6. Capacity development

# Table of contents

ABOUT NATIONAL CYBERWATCH	02
THE CYBERWATCH DIFFERENCE	04
E-BOOKS	08
CLOUD BASED LAB SOLUTIONS	09
ABOUT THE 6 DEGREE PROGRAMS	10
ABOUT THE 10 CERTIFICATES	18
ABOUT THE 34 TECHNICAL COURSES	18



# The CyberWatch Difference

## Information Security Curriculum



*When CyberWatch started in 2005, quality Information Security curriculum was in short supply, so the development of new curriculum was a necessity.*

In 2006, CyberWatch, working in conjunction with Anne Arundel Community College, MD, developed model Information Assurance and Computer Forensics curricula, which supported the growth of cybersecurity education nationally, including complete courses and multiple degrees and certificates.

Building on its model curriculum base, the National CyberWatch Center expanded the reach of cybersecurity education curriculum in several other ways, including the sharing of stackable credential models. These specialization certificates allow students to earn multiple certificates while pursuing their degree and to earn industry credentials by sitting for industry certification exams.

# Curriculum Design Considerations

Answers to the following question drive our curriculum efforts: What does effective curriculum look like? It is:

- Relevant: to employers, students, and colleges/universities
- Designed with fundamentals in mind: yes, the field of Information Security is rapidly changing; but there are still fundamentals that can and should be taught. The National Security Agency’s Knowledge Units (KUs) are the start of this foundation and the first semblance of a Common Body of Knowledge for the cybersecurity discipline
- Aligned to job roles: backed by input from commercial and federal partners, as well as labor market demand sources
- Focused on skills validation: lab exercises aligned with industry recognized competencies, cybersecurity competitions, and faculty professional development courses
- Specifically named: while putting the *Cyber* label on anything and everything is en vogue, saying you have a Cybersecurity program is not helpful for students looking for training and education and employers looking to hire students from two- and four-year programs. Is your program focus on Secure Coding, Network Security, etc.? Name it.
- Agile: in regards to content development and maintenance/updates
- Consumable: in various digital formats
- Modular: schools can adopt the degrees/certificates en masse, or customize them based on their needs/goals/outcomes (e.g., replace the National CyberWatch Center Networking I and II courses with Cisco I and II)
- Mapped to federal and national standards (e.g., National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, National Security Agency (NSA) National Centers of Academic Excellence Knowledge Units)
- Compliant with the Sharable Content Object Reference Model (SCORM)
- All digital: each technical course comes with a myriad of instructional materials: textbook recommendation, hosted virtual environment with requisite virtual machines and lab exercises, syllabus, instructor guide, assessments, and lecture slides that can be purchased and plugged into various Learning Management Systems
- Capped at 60 credits: updated and new degree offerings do not exceed many state-mandated 60-credit Associate of Applied Science limits
- Preparation for professional certifications (e.g., CompTIA, Cisco, Microsoft, EC-Council)
- Articulated with four-year schools: so students wishing to continue their studies at a four-year university can

# Curriculum Standards Panel

The National CyberWatch Curriculum Standards Panel was established in 2016. The mission is to identify the learning objectives, concepts, procedures, situational judgments, and intellectual abilities required to successfully complete courses currently available as digital courseware from the National CyberWatch Center.

The first project of the National CyberWatch Center Curriculum Standards Panel was the **Cybersecurity Core Curriculum Mapping Project**. This project involved eight online working sessions with synchronous and asynchronous activities, with over 100 faculty, industry professionals, and government representatives completing various tasks to determine the requirements to successfully complete five National CyberWatch Center courses:



**Networking I:  
Networking Fundamentals**



**Linux Server I:  
Linux Fundamentals**



**Information Security  
Fundamentals**



**Scripting  
Fundamentals**



**Ethical Hacking  
& Systems Defense**

The produced standards will be the first to align instructional design, skill practice facilities, cybersecurity professional job performance standards, national workforce frameworks, and industry needs, which are desperately needed to guide responsible curriculum development for the new generation of Information Security specialists.

The Cybersecurity Core Curriculum Mapping Project will be the first of several planned initiatives from the National CyberWatch Center to produce formative credentialing solutions that increase the number of capable cybersecurity professionals protecting our nation from cyber incursion and increasing the reliability and effectiveness of the computing infrastructure critical to our national security and economic prosperity.

**Nominate yourself or someone else to participate - [info@nationalcyberwatch.org](mailto:info@nationalcyberwatch.org)**



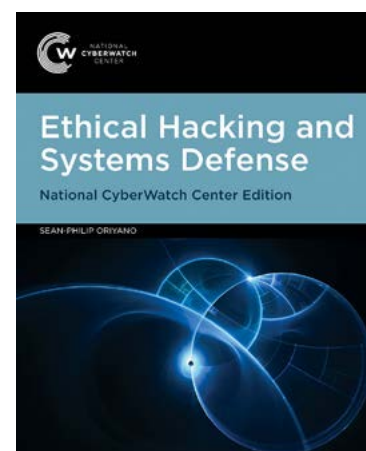
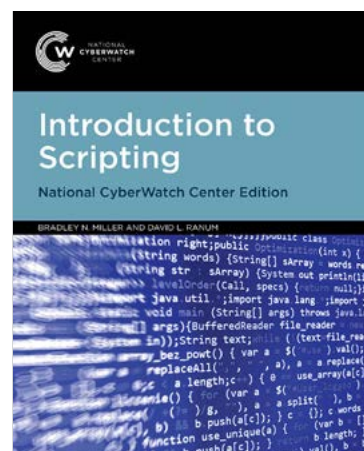
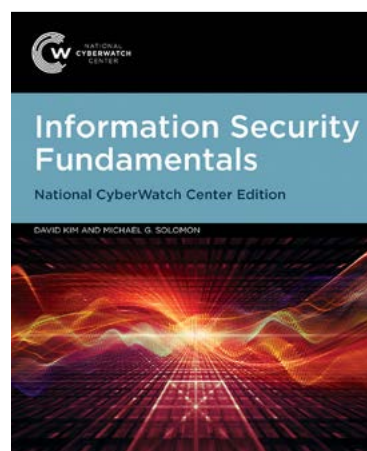
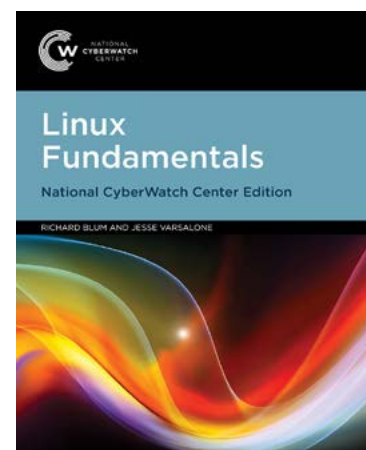
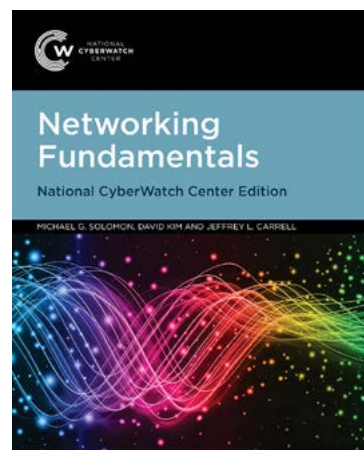
## e-Books

*The National CyberWatch Center, in conjunction with Jones & Bartlett Learning, have produced a series of e-Books. These e-Books support the various National CyberWatch technical courses.*

**ebooks.nationalcyberwatch.org**

e-Books Include:

- Syllabus
- Lecture Slides
- Testbank/Assessment Questions
- Project Answers
- Instructor's Guide



## Complete Cloud-Based Lab Solution

*A hands-on, scalable, and customizable virtual platform that proves skills are the cornerstone of any degree, certificate, training, or assessment program.*

This lab solution solves faculty and student needs in the following ways:



- Cloud-based infrastructure, allowing schools to begin using it immediately
- No up-front cost to the school, nor any on-going fees
- Hundreds of virtual labs mapped to many National CyberWatch courses, professional certifications, and various standards and frameworks
- Step-by-step lab tutorials with corresponding virtual machines
- Capture the Flag-type Challenge Labs with auto-scoring
- All HTML 5, no plugins needed
- Instructor analytics allowing faculty to see the activity of their students
- Learning Tools Integration (LTI) into the school's Learning Management System (LMS), allowing for single-sign-on capability
- Ability to update and distribute content seamlessly, without effort from the school
- Tech support: 7 days a week (8am - Midnight)

To see a complete list of labs, by National CyberWatch course, or to request a demo, see

**lab.nationalcyberwatch.org**





# About the 6 Degree Programs

DATA  
SEARCHING  
VERIFICATION  
CODING  
SENDING



Based on input from the National CyberWatch Curriculum Standards Panels, industry, labor market demand research, and over 10+ years of content development experience, the National CyberWatch degree programs help prepare students for the cutting-edge jobs of the knowledge economy. In addition, where appropriate, technical courses have been mapped to effective instructional design practices, skill practice facilities, the National Security Agency/Dept. of Homeland Security Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units (KUs), the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800-181), and industry competency and capability maturity models.

For more information:

[degrees.nationalcyberwatch.org](https://degrees.nationalcyberwatch.org)

## CYBER DEFENSE (A.A.S.)

The 11 technical courses in this degree combine both networking and systems administration fundamentals, with a focus on defensive strategies to securing networks and systems.

Cyber Defense A.A.S. Degree by Semester					
First Year			Second Year		
Fall	Spring	Summer	Fall	Spring	Summer
Gen Ed: Transitioning to College (1)	NCC 206: Windows Server I: Installing and Configuring Windows Server (3)	NCC 205: Linux Server II: System Administration (3)	NCC 207: Windows Server II: System Administration (4)	NCC 220: Network Security I: Network Security Fundamentals (4)	Gen Ed: Social & Behavioral Sciences (3)
Gen Ed: IT (3)	NCC 210: Information Security Fundamentals (3)	3 Credits	NCC 213: Intrusion Detection/Prevention Systems Fundamentals (4)	NCC 214: Ethical Hacking & Systems Defense (4)	Gen Ed: Fundamentals of Speech (3)
NCC 200: Networking I: Networking Fundamentals (3)	Gen Ed: Mathematics (3)		Gen Ed: College Composition (3)	Gen Ed: Arts and Humanities or Social/Behavioral Sciences (3)	6 Credits
NCC 201: Networking II: Switching and Routing Fundamentals (4)	NCC 212: Scripting Fundamentals (3)		10 Credits	Gen Ed: Biological & Physical Sciences (3)	
NCC 204: Linux Server I: Linux Fundamentals (3)	12 Credits			14 Credits	
14 Credits					
59 TOTAL CREDIT HOURS					



CYBER DEFENSE (A.A.S.) [CONT.]

Students completing this degree can apply for jobs as:

- Computer Network Defense Analyst
- Computer Network Defense Infrastructure Support
- Computer User Support
- Customer Service and Technical Support
- Intrusion Detection System (IDS) Technician
- Network Administrator
- Network Defense Technician
- Network Services
- Network Support
- Network Support Specialist
- Red Team Technician
- Systems Administrator

In addition, students can sit for the following industry certifications:

- CompTIA Network+
- CompTIA Linux+
- CompTIA Security+
- Cisco Certified Entry Networking Technician (CCENT)
- Microsoft Certified Professional (MCP)

NETWORK FORENSICS (A.A.S.)

The 11 technical courses in this degree program combines hardware, operating systems, Digital Forensics, and network fundamentals with the requisite security concepts required to detect and respond to system and network intrusions.

Network Forensics A.A.S. Degree by Semester					
First Year			Second Year		
Fall	Spring	Summer	Fall	Spring	Summer
Gen Ed: Transitioning to College (1)	NCC 217: Operating Systems Fundamentals (3)	NCC 212: Scripting Fundamentals (3)	NCC 215: Digital Forensics I: Digital Forensics Fundamentals (3)	ENCC 214: thical Hacking & Systems Defense (4)	Gen Ed: Social & Behavioral Sciences (3)
NCC 200: Networking I: Networking Fundamentals (3)	NCC 218: Hardware I: Hardware Fundamentals (4)	Gen Ed: Fundamentals of Speech (3)	NCC 216: Digital Forensics II: Advanced Digital Forensics (4)	Gen Ed: Arts and Humanities or Social/Behavioral Sciences (3)	Gen Ed: Biological & Physical Sciences (3)
NCC 204: Linux Server I: Linux Fundamentals (3)	Gen Ed: Mathematics (3)	6 Credits	NCC 213: Intrusion Detection/Prevention Systems Fundamentals (4)	NCC 219: Network Forensics & Incident Response (4)	6 Credits
Gen Ed: IT (3)	NCC 210: Information Security Fundamentals (3)		Gen Ed: College Composition (3)	11 Credits	
10 Credits	13 Credits		14 Credits		
60 TOTAL CREDIT HOURS					

NETWORK FORENSICS (A.A.S.) [CONT.]

Students completing this degree can apply for jobs as:

- Computer Forensic Analyst
- Computer Network Defense Analyst
- Computer Network Defense Forensic Analyst
- Computer Network Defense Infrastructure Support
- Computer Network Support Specialist
- Computer User Support
- Customer Service and Technical Support
- Digital Forensics Analyst
- Digital Media Collector
- Forensic Analyst
- Forensic Technician
- Incident Handler
- Incident Responder
- Intrusion Analyst
- Intrusion Detection System (IDS) Technician
- Network Administrator
- Red Team Technician
- Systems Administrator

In addition, students can sit for the following industry certifications:

- CompTIA A+
- CompTIA Network+
- CompTIA Security+

**NETWORK SECURITY ADMINISTRATION (A.A.S)**

The 11 technical courses in this degree program combines networking fundamentals with the requisite network security concepts and effective practices required to implement and administer secure network environments.

Network Security Administration A.A.S. Degree by Semester					
First Year			Second Year		
Fall	Spring	Summer	Fall	Spring	Summer
Gen Ed: Transitioning to College (1)	NCC 210: Information Security Fundamentals (3)	Gen Ed: Mathematics (3)	NCC 213: Intrusion Detection/Prevention Systems Fundamentals (4)	NCC 214: Ethical Hacking & Systems Defense (4)	Gen Ed: Social & Behavioral Sciences (3)
Gen Ed: IT (3)	NCC 206: Windows Server I: Installing and Configuring Windows Server (3)	NCC 212: Scripting Fundamentals (3)	NCC 220: Network Security I: Network Security Fundamentals (4)	NCC 219: Network Forensics & Incident Response (4)	3 Credits
NCC 200: Networking I: Networking Fundamentals (3)	NCC 204: Linux Server I: Linux Fundamentals (3)	6 Credits	Gen Ed: Biological & Physical Sciences (3)	Gen Ed: Arts and Humanities or Social/Behavioral Sciences (3)	
NCC 201: Networking II: Switching and Routing Fundamentals (4)	9 Credits		Gen Ed: College Composition (3)	Gen Ed: Fundamentals of Speech (3)	
NCC 211: TCP/IP Fundamentals (3)			14 Credits	14 Credits	
14 Credits					
60 TOTAL CREDIT HOURS					

Students completing this degree can apply for jobs as:

- Computer Network Defense Analyst
- Computer Network Defense Infrastructure Support
- Computer Network Support Specialist
- Customer Service and Technical Support
- Computer User Support
- Intrusion Detection System (IDS) Technician
- Network Administrator
- Network Analyst
- Network Defense Technician
- Network Services
- Network Support
- Network Systems and Data Communications Analyst
- Red Team Technician
- Systems Administrator

In addition, students can sit for the following industry certifications:

- CompTIA Network+
- CompTIA Security+
- Cisco Certified Entry Networking Technician (CCENT)

**SECURE SOFTWARE DEVELOPMENT (A.S.)**

The 5 technical courses in this degree combines Computer Science fundamentals with secure coding concepts. It is also designed as a transfer degree into baccalaureate programs of study in Computer Science.

Secure Software Development A.S. Degree			
First Year		Second Year	
Fall	Spring	Fall	Spring
Gen Ed: Transitioning to College (1)	Gen Ed: Arts and Humanities (3)	NCC 222: Computer Science I (4)	NCC 224: Computer Architecture & Organization (4)
Gen Ed: IT (3) (e.g., Secure Mobile App Development OR Secure Operating Systems)	Gen Ed: Social and Behavioral Sciences (3)	Gen Ed: Fundamentals of Speech (3)	Gen Ed: Biological and Physical Sciences with a Lab (4)
Calculus I (4)	Discrete Math (4)	NCC 223: Computer Science II (4)	Gen Ed: Social and Behavioral Sciences (3)
NCC 210: Information Security Principles (3)	Gen Ed: College Composition II (3)	Probability & Statistics OR Linear Algebra (4)	Gen Ed: Biological and Physical Sciences (4)
Gen Ed: College Composition I (3)	NCC 221: Intro. to Secure Programming Logic (3)	15 Credits	15 Credits
14 Credits	16 Credits		
TOTAL CREDIT HOURS: 60			

Students completing this degree can apply for jobs as:

- Developer
- Programmer
- Coder
- Computer Programmer
- Application Developer
- Software Developer



SECURE SOFTWARE DEVELOPMENT (A.A.S.)

The 12 technical courses in this degree combines computer programming, software assurance, and database development fundamentals and is intended to provide students with fundamental skills in software assurance.

Secure Software Development A.A.S. Degree					
First Year			Second Year		
Gen Ed: Transitioning to College (1)	NCC 225: Intro. to Relational Databases (3)	Gen Ed: Mathematics (3)	NCC 228: C# Programming (3)	NCC 231: Mobile Application Programming (3)	Gen Ed: Social & Behavioral Sciences (3)
Gen Ed: IT (3)	NCC 226: Secure Coding (3)	3 Credits	NCC 229: Structured Query Language (3)	NCC 232: Database Administration (3)	Gen Ed: Fundamentals of Speech (3)
NCC 222: Computer Science I (4)	NCC 227: Computer Science III (3)		NCC 230: Intro. to Assured Software Engineering (3)	NCC 233: Structured System Analysis (3)	6 Credits
NCC 210: Information Security Fundamentals (3)	9 Credits		Gen Ed: College Composition (3)	Gen Ed: Arts and Humanities or Social/Behavioral Sciences (3)	
NCC 223: Computer Science II (4)			12 Credits	Gen Ed: Biological & Physical Sciences (3)	
15 Credits				15 Credits	
60 TOTAL CREDIT HOURS					

Students completing this degree can apply for jobs as:

- Developer
- Programmer
- Coder
- Computer Programmer
- Application Developer
- Software Developer

SYSTEMS SECURITY ADMINISTRATION (A.A.S.)

The 11 technical courses in this degree program combines systems administration fundamentals with the requisite security concepts and effective practices required to implement, administer, and harden operating systems.

Systems Security Administration A.A.S. Degree by Semester					
First Year			Second Year		
Fall	Spring	Summer	Fall	Spring	Summer
Gen Ed: Transitioning to College (1)	NCC 210: Information Security Fundamentals (3)	Gen Ed: Mathematics (3)	NCC 205: Linux Server II: System Administration (3)	NCC 208: Windows Server III: Advanced System Administration (4)	Gen Ed: Social & Behavioral Sciences (3)
Gen Ed: IT (3)	NCC 218: Hardware I: Hardware Fundamentals (4)	NCC 212: Scripting Fundamentals (3)	NCC 206: Windows Server I: Installing and Configuring Windows Server (3)	Gen Ed: Fundamentals of Speech (3)	NCC 209: Secure Server Services (4)
Gen Ed: Arts and Humanities or Social/Behavioral Sciences (3)	NCC 204: Linux Server I: Linux Fundamentals (3)	6 Credits	NCC 207: Windows Server II: System Administration (3)	Gen Ed: Biological & Physical Sciences (3)	7 Credits
NCC 200: Networking I: Networking Fundamentals (3)	10 Credits		Gen Ed: College Composition (3)	10 Credits	
NCC 217: Operating Systems Fundamentals (3)			12 Credits		
13 Credits					
58 TOTAL CREDIT HOURS					

Students completing this degree can apply for jobs as:

- Customer Service and Technical Support
- Computer Support Specialist
- Computer User Support
- Systems Administrator
- Systems Analyst

In addition, upon completion of this degree, students can sit for the following professional certifications:

- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Linux+ Powered by LPI
- Microsoft Certified Professional (MCP)
- Microsoft Certified Solutions Associate (MCSA)

# About the 10 Certificates

*These specialized certificates prepare students for industry-recognized certification exams and cutting-edge jobs of the knowledge economy.*

Students can also earn credits, which can be applied towards an Associate’s degree. In addition, certificates can be stacked on top of each other, providing a pathway toward more advanced study and other certificates.

More information:

[certificates.nationalcyberwatch.org](https://certificates.nationalcyberwatch.org)

## CYBER DEFENSE

The 11 technical courses in this certificate combine both networking and systems administration fundamentals, with a focus on defensive strategies to securing networks and systems.

Cyber Defense Certificate	
Technical Courses	Credits
NCC 200: Networking I: Networking Fundamentals	3
NCC 201: Networking II: Switching and Routing Fundamentals	4
NCC 204: Linux Server I: Linux Fundamentals	3
NCC 205: Linux Server II: System Administration	3
NCC 206: Windows Server I: Installing and Configuring Windows Server	3
NCC 207: Windows Server II: System Administration	3
NCC 210: Information Security Fundamentals	3
NCC 212: Scripting Fundamentals	3
NCC 213: Intrusion Detection/Prevention Systems Fundamentals	4
NCC 220: Network Security I: Network Security Fundamentals	4
NCC 214: Ethical Hacking & Systems Defense	4
Total Program Requirement Credits	37

Students completing this certificate can apply for jobs as:

- Computer Network Defense Analyst
- Computer Network Defense Infrastructure Support
- Computer User Support
- Customer Service and Technical Support
- Intrusion Detection System (IDS) Technician
- Network Administrator
- Network Defense Technician
- Network Services
- Network Support
- Network Support Specialist
- Red Team Technician
- Systems Administrator

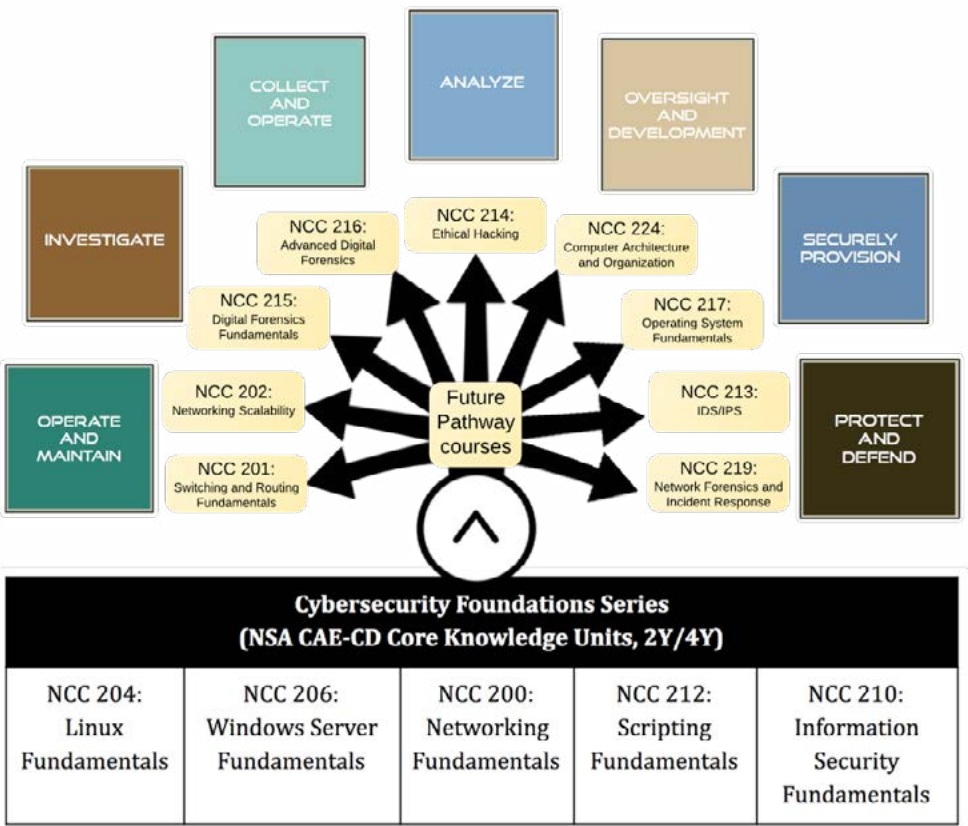
## CYBER DEFENSE (CONT.)

In addition, students can sit for the following industry certifications:

- CompTIA Network+
- CompTIA Linux+
- CompTIA Security+
- Cisco Certified Entry Networking Technician (CCENT)
- Microsoft Certified Professional (MCP)

## CYBER FOUNDATIONS

The 5 technical courses in this certificate provide the IT foundation to branch into any number of Information Security specializations. These courses also align with the core Knowledge Units (KUs) necessary for the two- and four-year National Security Agency/Dept. of Homeland Security Center of Academic Excellence in Cyber Defense (CAE-CD) designation.



NETWORK FORENSICS

The 11 technical courses in this certificate program combines hardware, operating systems, Digital Forensics, and network fundamentals with the requisite security concepts required to detect and respond to system and network intrusions.

Network Forensics Certificate	
Technical Courses	Credits
NCC 200: Networking I: Networking Fundamentals	3
NCC 204: Linux Server I: Linux Fundamentals	3
NCC 217: Operating Systems Fundamentals	3
NCC 218: Hardware I: Hardware Fundamentals	4
NCC 210: Information Security Fundamentals	3
NCC 212: Scripting Fundamentals	3
NCC 215: Digital Forensics I: Digital Forensics Fundamentals	3
NCC 216: Digital Forensics II: Advanced Digital Forensics	4
NCC 213: Intrusion Detection/Prevention Systems Fundamentals	4
NCC 214: Ethical Hacking & Systems Defense	4
NCC 219: Network Forensics & Incident Response	4
Total Program Requirement Credits	38

Students completing this degree can apply for jobs as:

- Computer Forensic Analyst
- Computer Network Defense Analyst
- Computer Network Defense Forensic Analyst
- Computer Network Defense Infrastructure Support
- Computer Network Support Specialist
- Computer User Support
- Customer Service and Technical Support
- Digital Forensics Analyst
- Digital Media Collector
- Forensic Analyst
- Forensic Technician
- Incident Handler
- Incident Responder
- Intrusion Analyst
- Intrusion Detection System (IDS) Technician
- Network Administrator
- Red Team Technician
- Systems Administrator

In addition, students can sit for the following industry certifications:

- CompTIA A+
- CompTIA Network+
- CompTIA Security+

NETWORK SECURITY ADMINISTRATION

The 11 technical courses in this certificate program combines networking fundamentals with the requisite network security concepts and effective practices required to implement and administer secure network environments. There are 3 Network Security Administration certificates that can be stacked on top of each other, and also provide the foundation for other certificates (e.g., Systems Security Administration).

Network Security Administration Certificate	
Technical Courses	Credits
NCC 200: Networking I: Networking Fundamentals	3
NCC 201: Networking II: Switching and Routing Fundamentals	4
NCC 211: TCP/IP Fundamentals	3
NCC 210: Information Security Fundamentals	3
NCC 212: Scripting Fundamentals	3
NCC 204: Linux Server I: Linux Fundamentals	3
NCC 206: Windows Server I: Installing and Configuring Windows Server	3
NCC 213: Intrusion Detection/Prevention Systems Fundamentals	4
NCC 220: Network Security I: Network Security Fundamentals	4
NCC 214: Ethical Hacking & Systems Defense	4
NCC 219: Network Forensics & Incident Response	4
Total Program Requirement Credits	38

Students completing this degree can apply for jobs as:

- Computer Network Defense Analyst
- Computer Network Defense Infrastructure Support
- Computer Network Support Specialist
- Customer Service and Technical Support
- Computer User Support
- Intrusion Detection System (IDS) Technician
- Network Administrator
- Network Analyst
- Network Defense Technician
- Network Services
- Network Support
- Network Systems and Data Communications Analyst
- Red Team Technician
- Systems Administrator

In addition, students can sit for the following industry certifications:

- CompTIA Network+
- CompTIA Security+
- Cisco Certified Entry Networking Technician (CCENT)



SECURE SOFTWARE DEVELOPMENT

The 12 technical courses in this certificate program combines computer programming, software assurance, and database development fundamentals and is intended to provide students with fundamental skills in software assurance.

Secure Software Development Certificate	
Technical Courses	Credits
NCC 222: Computer Science I	4
NCC 210: Information Security Fundamentals	3
NCC 223: Computer Science II	4
NCC 225: Intro. to Relational Databases	3
NCC 226: Secure Coding	3
NCC 227: Computer Science III	3
NCC 228: C# Programming	3
NCC 229: Structured Query Language	3
NCC 230: Intro. To Assured Software Engineering	3
NCC 231: Mobile Application Programming	3
NCC 232: Database Administration	3
NCC 233: Structured System Analysis	3
Total Program Requirement Credits	38

Students completing this degree can apply for jobs as:

- Developer
- Programmer
- Coder
- Computer Programmer
- Application Developer
- Software Developer

SYSTEMS SECURITY ADMINISTRATION

The 11 technical courses in this certificate program combines systems administration fundamentals with the requisite security concepts and effective practices required to implement, administer, and harden operating systems. There are 3 Systems Security Administration certificates that can be stacked on top of each other, and also provide the foundation for other certificates (e.g., Network Security Administration).

Systems Security Administration Certificate	
Technical Courses	Credits
NCC 200: Networking I: Networking Fundamentals	3
NCC 210: Information Security Fundamentals	3
NCC 217: Operating Systems Fundamentals	3
NCC 212: Scripting Fundamentals	3
NCC 218: Hardware I: Hardware Fundamentals	4
NCC 204: Linux Server I: Linux Fundamentals	3
NCC 205: Linux Server II: System Administration	3
NCC 206: Windows Server I: Installing and Configuring Windows Server	3
NCC 207: Windows Server II: System Administration	3
NCC 208: Windows Server III: Advanced System Administration	4
NCC 209: Secure Server Services	4
Total Program Requirement Credits	36

Students completing this degree can apply for jobs as:

- Customer Service and Technical Support
- Computer Support Specialist
- Computer User Support
- Systems Administrator
- Systems Analyst

In addition, upon completion of this degree, students can sit for the following professional certifications:

- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Linux+ Powered by LPI
- Microsoft Certified Professional (MCP)
- Microsoft Certified Solutions Associate (MCSA)

# Curriculum Specialists

*Let our knowledgeable staff help you craft a program or course that meets the needs of your local advisory board, faculty knowledge and skills, employers, and the students coming through your institutions.*

Consulting services include:

- Degree and Certificate program creation, adoption, adaptation
- Technical course creation, adoption, adaptation
- Articulation agreement models
- Faculty professional development programs
- Mapping services to various national and federal standards, job roles, and certifications
- ...and more

Contact us: [info@nationalcyberwatch.org](mailto:info@nationalcyberwatch.org)

# Mapping, Mapping Oh My!

*Our degree, certificate, and technical course learning objectives and topic areas have been mapped to the following, ensuring your students are prepared for the cutting-edge jobs of the knowledge economy:*

- Professional certifications
- Job Roles
- National Security Agency Knowledge Units (KUs)
- National Institute of Standards & Technology (NIST) Cybersecurity Workforce Framework Knowledge, Skills & Abilities (KSAs)
- Cybersecurity professional job performance standards
- Industry needs



# ABOUT THE 34 TECHNICAL COURSES

[courses.nationalcyberwatch.org](https://courses.nationalcyberwatch.org)


# Networking I

## NCC 200: Networking I: Networking Fundamentals

3 credit/unit hours – Three hours of lecture weekly; one term

This course explores converging computer and communications technologies, such as transmission concepts, network hardware and software, protocols, and standards. It is also designed to serve the needs of those interested in understanding the field of computer networking and how it relates to other areas of Information Technology (IT). The material covered in this class provides the broad-based knowledge necessary to prepare students for further study in specialized networking fields, or may be used by those interested in an introduction to the field.

It also helps prepare individuals seeking to pass the Cisco Certified Network Associate (CCNA) or Cisco Certified Entry Networking Technician (CCENT) certification exams.

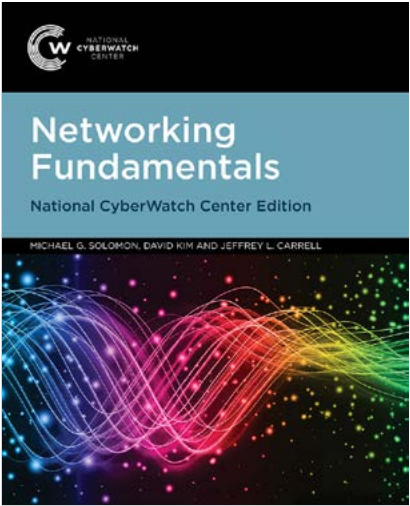


**PREREQUISITE:** General Education IT course  
(can be taken concurrently)

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Describe the devices and services used to support communications in data networks and the Internet;
- Describe the role of protocol layers in data networks;
- Design, calculate and implement various IPv4 and IPv6 addressing and naming schemes;
- Describe fundamental Ethernet concepts (e.g., media, services, and operations);
- Build simple Local Area Networks (LANs);
- Utilize common network utilities to verify and troubleshoot small networks;
- Analyze network and data traffic; and
- Utilize network diagrams



# Networking I (cont.)

### MAIN TOPICS

#### 1.0 Exploring the Network:

- Globally Connected
- LANs, WANs, and the Internet
- The Network as a Platform
- The Changing Network Environment

#### 2.0 Configuring a Network Operating System:

- Internetworking Operating System (IOS)
- Getting Basic
- Addressing Schemes

#### 3.0 Network Protocols and Communications:

- Rules of Communication
- Network Protocols and Standards
- Moving Data

#### 4.0 Network Access:

- Physical Layer Protocols
- Network Media
- Data Link Layer Protocols
- Media Access Control

#### 5.0 Ethernet:

- Ethernet Protocol
- Address Resolution Protocol (ARP)
- Local Area Network (LAN) Switches

#### 6.0 Network Layer:

- Network Layer Protocols
- Routing
- Routers
- Configuring a Router

#### 7.0 Transport Layer:

- Transport Layer Protocols
- Transmission Control Protocol (TCP)

- User Datagram Protocol (UDP)

#### 8.0 Internet Protocol (IP) Addressing:

- IPv4 addresses
- IPv6 addresses
- Connectivity Verification

#### 9.0 Subnetting Internet Protocol (IP) Networks:

- Subnetting an IPv4 Network
- Addressing Schemes
- Design Considerations for IPv6

#### 10.0 Application Layer:

- Application Layer Protocols and Services

#### 11.0 Putting It All Together:

- Create and Grow
- Network Security
- Basic Network Performance
- Managing IOS Configuration Files

### RECOMMENDED TEXTBOOK

TITLE: Networking Fundamentals: National CyberWatch Center Edition (1st Edition)

AUTHOR: Solomon, Kim & Carrell (2017)

PUBLISHER: Jones & Bartlett Learning

PRINT ISBN: 9781284108064, 1284108066

eTEXT ISBN (VitalSource): 9781284108064



# Networking II

**NCC 201: Networking II:  
Switching and Routing Fundamentals**

4 credit/unit hours – Four hours of lecture weekly; one term

This course introduces the student to the architecture, components, and operation of switches and routers, as well as the fundamentals of switching, routing, and the primary routing protocols. The course is designed to help students prepare for professional careers in the information and communication technology (ICT) field. It also helps prepare individuals seeking to pass the Cisco Certified Network Associate (CCNA) or Cisco Certified Entry Networking Technician (CCENT) certification exams.



**PREREQUISITE:** NCC 200: Networking I:  
Networking Fundamentals

LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Describe basic switching concepts;
- Discuss the purpose, nature, and operations of a router, routing tables, and the route lookup process;
- Describe and implement Virtual Local Area Networks (VLANs) to create logically separate networks and how routing occurs between them;
- Configure and troubleshoot static and dynamic routing protocols, distance vector routing protocols, and link-state routing protocols;
- Implement, and troubleshoot Access Control Lists (ACLs) for IPv4 and IPv6 networks;
- Configure and troubleshoot Dynamic Host Configuration Protocol (DHCP) for IPv4 and IPv6 networks;
- Implement and troubleshoot Network Address Translation (NAT);
- Utilize network diagrams

# Networking II (cont.)

MAIN TOPICS

1.0 Introduction to Switched Networks:

- LAN Design
- The Switched LAN Environment

2.0 Basic Switching Concepts and Configuration:

- Basic Switch Configuration
- Switch Security: Management and Implementation
- Troubleshooting Security Implementations

3.0 Virtual Local Area Networks (VLANs):

- VLAN Segmentation
- VLAN Implementation
- VLAN Security and Design
- Troubleshooting VLAN Issues

4.0 Routing Concepts:

- Initial Configuration of a Router
- Routing Decisions
- Router Operation
- Troubleshooting Router Issues

5.0 Inter-VLAN Routing:

- Inter-VLAN Routing Configuration
- Troubleshooting Inter-VLAN Routing
- Layer 3 Switching

6.0 Static Routing:

- Static Routing Implementation
- Configure Static and Default Routes
- Review of Classless Inter-Domain Routing (CIDR) and Variable-Length Subnet Mask (VLSM)
- Configure Summary and Floating Static Routes
- Troubleshoot Static and Default Route Issues

7.0 Dynamic Routing:

- Dynamic Routing Protocols

- Distance Vector Routing Protocols
- Routing Information Protocol (RIP) and RIPv6 Routing
- Link-State Dynamic Routing
- Routing Table
- Troubleshooting Dynamic Routing Implementations

8.0 Single-Area Open Shortest Path First (OSPF):

- Characteristics of OSPF
- Configuring Single-Area OSPF v2
- Configuring Single-Area OSPF v3
- Troubleshooting OSPF Implementations

9.0 Access Control Lists (ACLs):

- Internet Protocol (IP) ACL Operations
- Standard and Extended IPv4 ACLs
- IPv6 ACLs
- Troubleshooting ACLs

10.0 Dynamic Host Configuration Protocol (DHCP):

- Implementing DHCP v4 and DHCP v6
- Troubleshooting DHCP Implementations

11.0 Network Address Translation (NAT):

- NAT Operation for IPv4
- Configuring NAT
- Troubleshooting NAT

RECOMMENDED TEXTBOOK

TITLE: Routing and Switching Essentials v6 Companion Guide

PUBLISHER: Cisco Press (2016)

ISBN-10: 1-58713-428-4


ISBN-13: 978-1-58713-428-9

# Networking III

## NCC 202: Networking III: Network Scalability

4 credit/unit hours – Four hours of lecture weekly; one term

This course introduces the student to advanced switching and routing architectures, components, and operations. The course is designed to help students prepare for professional careers in the information and communication technology (ICT) field. It also helps prepare individuals seeking to pass the Cisco Certified Network Associate (CCNA) certification exam.



**PREREQUISITE:** NCC 201: Networking II:  
Switching and Routing Fundamentals

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Configure and troubleshoot enhanced switching technologies such as Virtual Local Area Networks (VLANs), Rapid Spanning Tree Protocol (RSTP), Per VLAN Spanning Tree Plus Protocol (PVST+), and EtherChannel;
- Configure and troubleshoot first hop redundancy protocols (HSRP) in a switched network;
- Configure and troubleshoot wireless routers and wireless clients;
- Configure and troubleshoot routers in a complex routed IPv4 or IPv6 network using single-area Open Shortest Path First (OSPF), multiarea OSPF, and Enhanced Interior Gateway Routing Protocol (EIGRP); and
- Utilize network diagrams

# Networking III (cont.)

### MAIN TOPICS

**1.0 Introduction to Scaling Networks:**

- Implementing a Network Design
- Selecting Network Devices

**2.0 LAN Redundancy:**

- Spanning Tree Concepts
- Varieties of Spanning Tree Protocols
- Spanning Tree Configuration and Troubleshooting
- First Hop Redundancy Protocols

**3.0 Link Aggregation:**

- Link Aggregation Concepts
- Link Aggregation Configuration and Troubleshooting

**4.0 Wireless LANs:**

- Wireless LAN Concepts
- Wireless LAN Operations
- Wireless LAN Security
- Wireless LAN Configuration and Troubleshooting

**5.0 Adjust and Troubleshoot Single-Area OSPF:**

- Advanced Single-Area OSPF Configurations
- Troubleshooting Single-Area OSPF Implementations

**6.0 Multiarea OSPF:**

- Multiarea OSPF Operation
- Configuring Multiarea OSPF

**7.0 EIGRP:**

- Characteristics of EIGRP
- Operation of EIGRP
- Configuring EIGRP for IPv4
- Configuring EIGRP for IPv6

**8.0 EIGRP Advanced Config. and Troubleshooting:**

- Advanced EIGRP Configurations

- Troubleshooting EIGRP Implementations

**9.0 Access Control Lists (ACLs):**

- Internet Protocol (IP) ACL Operations
- Standard and Extended IPv4 ACLs
- IPv6 ACLs
- Troubleshooting ACLs

**10.0 Dynamic Host Configuration Protocol (DHCP):**

- Implementing DHCP v4 and DHCP v6
- Troubleshooting DHCP Implementations

**11.0 Network Address Translation (NAT):**

- NAT Operation for IPv4
- Configuring NAT
- Troubleshooting NAT

**RECOMMENDED TEXTBOOK**

TITLE: Scaling Networks v6 Companion Guide

PUBLISHER: Cisco Press (2017)

ISBN-10: 1-58713-434-9

ISBN-13: 978-1-58713-434-0

# Networking IV

**NCC 203: Networking IV:  
Network Connectivity**

**4 credit/unit hours – Four hours of lecture weekly; one term**

This course introduces the student to Wide Area Network (WAN) technologies and network services required by converged applications in a complex network. The course enables students to understand the selection criteria of network devices and WAN technologies to meet network requirements. Students learn how to configure and troubleshoot network devices and resolve common issues with data link protocols. Students will also develop the knowledge and skills needed to implement virtual private network (VPN) operations in a complex network.

The course is designed to help students prepare for professional careers in the information and communication technology (ICT) field. It also helps prepare individuals seeking to pass the Cisco Certified Network Associate (CCNA) certification exam.

 **PREREQUISITE:** NCC 202: Networking III:  
Network Scalability

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to:

- Describe different WAN technologies and their benefits;
- Discuss the operations and benefits of virtual private networks (VPNs) and tunneling;
- Configure and troubleshoot serial connections;
- Configure and troubleshoot broadband connections;
- Configure and troubleshoot tunneling operations;
- Configure and troubleshoot Network Address Translation (NAT) operations;
- Monitor and troubleshoot network operations using syslog, Simple Network Management Protocol (SNMP), and NetFlow;
- Describe network architectures (e.g., Borderless networks, Data centers and virtualization, Collaboration technology and solutions); and
- Utilize network diagrams

# Networking IV (cont.)

**MAIN TOPICS**

**1.0 Hierarchical Network Design:**

- Hierarchical Network Design Overview
- Evolving Network Architectures

**2.0 Connecting to the WAN:**

- WAN Technologies Overview
- Selecting a WAN Topology

**3.0 Point-to-Point (PPP) Connections:**

- Serial Point-to-Point Overview
- PPP Operation
- Configure PPP
- Troubleshooting WAN Connectivity

**4.0 Frame Relay:**

- Introduction to Frame Relay
- Configuration and Troubleshooting Frame Relay

**5.0 Network Address Translation (NAT) for IPv4:**

- NAT Operation
- Configuration and Troubleshooting NAT

**6.0 Broadband Solutions:**

- Teleworking
- Comparing Broadband Solutions
- Configuring xDSL Connectivity

**7.0 Securing Site-to-Site Connectivity:**

- VPNs
- Site-to-site Generic Routing Encapsulation (GRE) Tunnels
- Introducing IP Security (IPSec)
- Remote Access

**8.0 Monitoring the Network:**

- Syslog

- SNMP
- Netflow

**9.0 Troubleshooting the Network:**

- Troubleshooting with a Systematic Approach
- Network Troubleshooting

**RECOMMENDED TEXTBOOK**

TITLE: Connecting Networks v6 Companion Guide

PUBLISHER: Cisco Press (2017)

ISBN-10: 1-58713-432-2

ISBN-13: 978-1-58713-432-6




# Linux Server I

## NCC 204: Linux Server I: Linux Fundamentals

3 credit/unit hours – Three hours of lecture weekly; one term

This course will provide students with the fundamental concepts of Linux/UNIX operating systems. The course covers such topics as the Linux/UNIX file system, commands, utilities, text editing, shell programming, and text processing utilities. Students will learn command line syntax and features of the popular Linux/UNIX shells, including filename generation, redirection, pipes, and quoting mechanisms.

The course is designed to help students prepare for professional careers in the information and communication technology (ICT) field. It also helps prepare individuals seeking to pass the CompTIA Linux+ (powered by the Linux Professional Institute (LPI)) certification exam (LX0-103).

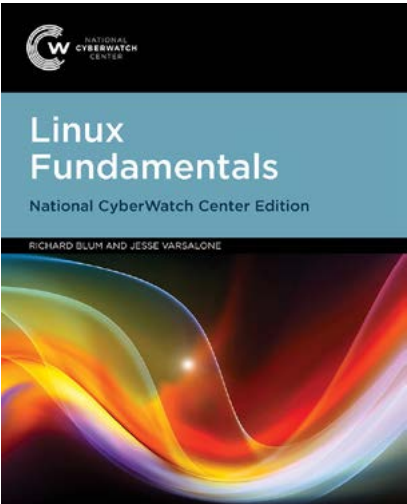


**PREREQUISITE:** General Education IT Course  
(can be taken concurrently)

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Customize and utilize both GUI (Graphical User Interface) and CLI (Command Line Interface);
- Set general and advance permissions on files and directories;
- Use filename generation standards and best practices;
- Use pipes and redirection along with input output helper commands;
- Control processes locally and remote via network;
- Customize basic and advanced networking and software management; and
- Utilize command line search, utilities, file system management, and configuration modification



# Linux Server I (cont.)

## MAIN TOPICS

### 1.0 System Architecture:

#### 1.1 Determine and Configure hardware settings:

- Enable and disable integrated peripherals
- Configure systems with or without external peripherals such as keyboards
- Differentiate between the various types of mass storage devices Weakest Link in the Security of an IT Infrastructure
- Describe the differences between coldplug and hotplug devices
- Determine hardware resources for devices
- Tools and utilities to list various hardware information (e.g. lsusb, lspci, etc.)
- Tools and utilities to manipulate USB devices
- Conceptual understanding of sysfs, udev, dbus

#### 1.2 Boot the System:

- Provide common commands to the boot loader and options to the kernel at boot time
- Demonstrate knowledge of the boot sequence from BIOS to boot completion
- Describe SysVinit and system
- Discuss Upstart
- Check boot events in the log file

#### 1.3 Change runlevels / boot targets and shutdown or reboot system:

- Set the default runlevel or boot target
- Change between runlevels / boot targets including single user mode
- Shutdown and reboot from the command line
- Alert users before switching runlevels / boot targets or other major system events
- Properly terminate processes

### 2.0 Linux Installation and Package Management:

#### 2.1 Design hard disk layout:

- Allocate filesystems and swap space to separate partitions or disks
- Tailor the design to the intended use of the system
- Ensure the /boot partition conforms to the hardware architecture requirements for booting
- Knowledge of basic features of Logical Volume Manager (LVM)

#### 2.2 Install a boot manager:

- Providing alternative boot locations and backup boot options
- Install and configure a boot loader such as GRUB Legacy
- Perform basic configuration changes for GRUB 2
- Interact with the boot loader

#### 2.3 Manage shared libraries:

- Identify shared libraries
- Identify the typical locations of system libraries
- Load shared libraries

#### 2.4 Use Debian package management:

- Install, upgrade and uninstall Debian binary packages
- Find packages containing specific files or libraries which may or may not be installed
- Obtain package information like version, content, dependencies, package integrity, and installation status (whether or not the package is installed)

#### 2.5 Use RPM and YUM package management:

- Install, re-install, upgrade and remove packages using RPM and YUM

# Linux Server I (cont.)

MAIN TOPICS

- Obtain information on RPM packages such as version, status, dependencies, integrity and signatures
- Determine what files a package provides, as well as find which package a specific file comes from

3.0 GNU and Unix Commands:

3.1 Work on the command line:

- Use single shell commands and one line command sequences to perform basic tasks on the command line
- Use and modify the shell environment including defining, referencing and exporting environment variables
- Use and edit command history
- Invoke commands inside and outside the defined path

3.2 Process text streams using filters:

- Send text files and output streams through text utility filters to modify the output using standard UNIX commands found in the GNU textutils package

3.3 Perform basic file management:

- Copy, move and remove files and directories individually
- Copy multiple files and directories recursively
- Remove files and directories recursively
- Use simple and advanced wildcard specifications in commands
- Using find to locate and act on files based on type, size, or time
- Usage of tar, cpio, and dd

3.4 Use streams, pipes and redirects:

- Redirecting standard input, standard output and standard error
- Pipe the output of one command to the input of another command
- Use the output of one command as arguments to another command
- Send output to both stdout and a file

3.5 Create, monitor and kill processes:

- Run jobs in the foreground and background
- Signal a program to continue running after logout
- Monitor active processes
- Select and sort processes for display
- Send signals to processes

3.6 Modify process execution priorities:

- Know the default priority of a job that is created
- Run a program with higher or lower priority than the default
- Change the priority of a running process

3.7 Search text files using regular expressions:

- Create simple regular expressions containing several notational elements
- Use regular expression tools to perform searches through a filesystem or file content

3.8 Perform basic file editing operations using vi:

- Navigate a document using vi
- Use basic vi modes (e.g., insert, edit, delete, copy and find text)

# Linux Server I (cont.)

MAIN TOPICS

4.0 Devices, Linux Filesystems, Filesystem Hierarchy Standard:

4.1 Create partitions and filesystems:

- Manage MBR partition tables
- Use various mkfs commands to create various filesystems (e.g., ext2/ext3/ext4, XFS, VFAT)
- Awareness of ReiserFS and Btrfs
- Basic knowledge of gdisk and parted with GPT

4.2 Maintain the integrity of filesystems:

- Verify the integrity of filesystems
- Monitor free space and inodes
- Repair simple filesystem problems

4.3 Control mounting and unmounting of filesystems:

- Manually mount and unmount filesystems
- Configure filesystem mounting on bootup
- Configure user mountable removeable filesystems

4.4 Manage disk quotas:

- Set up a disk quota for a filesystem
- Edit, check and generate user quota reports

4.5 Manage file permissions and ownership:

- Manage access permissions on regular and special files as well as directories
- Use access modes such as suid, sgid and the sticky bit to maintain security
- Demonstrate how to change the file creation mask
- Use the group field to grant file access to group members

4.6 Create and change hard and symbolic links:

- Create links
- Identify hard and/or soft links
- Copying versus linking files

- Use links to support system administration tasks

4.7 Find system files and place files in the correct location:

- Understand the correct locations of files under the FHS
- Find files and commands on a Linux system
- Describe the location and propose of important file and directories as defined in the FHS

RECOMMENDED TEXTBOOK

TITLE: Linux Fundamentals: National CyberWatch Center Edition (1st Edition)

AUTHOR: Richard Blum & Jesse Varsalone (2017)

PUBLISHER: Jones & Bartlett Learning


eText ISBN (VitalSource): 9-781-28410-805-7

# Linux Server II

**NCC 205: Linux Server II:  
System Administration**

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course introduces the student to the fundamentals of system administration using Linux operating systems. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized security fields. It is also intended to serve the needs of individuals seeking to pass the Computing Technology Industry Association’s (CompTIA) Linux + certification exam (LX0-104).



**PREREQUISITE:** NCC 204: Linux Server I:  
Linux Fundamentals

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to:

- Work at the Linux command line;
- Managing user accounts and groups;
- Maintain system time and logging;
- Manage server services (e.g., SMTP);
- Manage printers and printing;
- Work with shells, manage data, and implement basic shell scripts;
- Automate system administration tasks by scheduling jobs;
- Install and configure a workstation (including X) and connect it to a LAN;
- Work with Internet protocols;
- Setup host security;
- Secure data using encryption; and
- Demonstrate appropriate and ethical behavior and good work habits



# Linux Server II (cont.)

**MAIN TOPICS**

**1.0 Shells, Scripting and Data Management:**

**1.1 Customize and use the shell environment:**

- Set environment variables (e.g. PATH) at login or when spawning a new shell
- Write BASH functions for frequently used sequences of commands
- Maintain skeleton directories for new user accounts
- Set command search path with the proper directory

**1.2 Customize or write simple scripts:**

- Use standard sh syntax (loops, tests)
- Use command substitution
- Test return values for success or failure or other information provided by a command
- Perform conditional mailing to the superuser
- Correctly select the script interpreter through the shebang (!) line
- Manage the location, ownership, execution and suid-rights of scripts

**1.3 SQL data management:**

- Use of basic SQL commands
- Perform basic data manipulation

**2.0 User Interfaces and Desktops:**

**2.1 Install and configure X11:**

- Verify that the video card and monitor are supported by an X server
- Awareness of the X font server
- Basic understanding and knowledge of the X Window configuration file

**2.2 Setup a display manager:**

- Basic configuration of LightDM
- Turn the display manager on or off

- Change the display manager greeting
- Awareness of XDM, KDM and GDM

**2.3 Accessibility:**

- Basic knowledge of keyboard accessibility settings (AccessX)
- Basic knowledge of visual settings and themes
- Basic knowledge of assistive technology (ATs)

**3.0 Administrative Tasks:**

**3.1 Manage user and group accounts and related system files:**

- Add, modify and remove users and groups
- Manage user/group info in password/group databases
- Create and manage special purpose and limited accounts

**3.2 Automate system administration tasks by scheduling jobs:**

- Manage cron and at jobs
- Configure user access to cron and at services
- Configure anacron

**3.3 Localisation and internationalization:**

- Configure locale settings and environment variables
- Configure timezone settings and environment variables

**4.0 Essential System Services:**

**4.1 Maintain system time:**

- Set the system date and time
- Set the hardware clock to the correct time in UTC
- Configure the correct timezone



# Linux Server II (cont.)

MAIN TOPICS

- Basic NTP configuration
  - Knowledge of using the pool.ntp.org service
  - Awareness of the ntpq command
- 4.2 System logging:**
- Configuration of the syslog daemon
  - Understanding of standard facilities, priorities and actions
  - Configuration of logrotate
  - Awareness of rsyslog and syslog-ng
- 4.3 Mail Transfer Agent (MTA) basics:**
- Create e-mail aliases
  - Configure e-mail forwarding
  - Knowledge of commonly available MTA programs (postfix, sendmail, qmail, exim) (no configuration)
- 4.4 Manage printers and printing:**
- Basic CUPS configuration (for local and remote printers)
  - Manage user print queues
  - Troubleshoot general printing problems
  - Add and remove jobs from configured printer queues
- 5.0 Networking Fundamentals:**
- 5.1 Fundamentals of Internet protocols:**
- Demonstrate an understanding network masks and CIDR notation
  - Knowledge of the differences between private and public “dotted quad” IP addresses
  - Knowledge about common TCP and UDP ports (e.g., 20, 21, 22, 23, 25, 53, 80)
  - Knowledge about the differences and major features of UDP, TCP and ICMP
- Knowledge of the major differences between IPv4 and IPv6
  - Knowledge of the basic features of IPv6
- 5.2 Basic network configuration:**
- Manually and automatically configure network interfaces
  - Basic TCP/IP host configuration
  - Setting a default route
- 5.3 Basic network troubleshooting:**
- Manually and automatically configure network interfaces and routing tables to include adding, starting, stopping, restarting, deleting or reconfiguring network interfaces
  - Change, view or configure the routing table and correct an improperly set default route manually
  - Debug problems associated with the network configuration
- 5.4 Configure client side DNS:**
- Query remote DNS servers
  - Configure local name resolution and use remote DNS servers
  - Modify the order in which name resolution is done
- 6.0 Security:**
- 6.1 Perform security administration tasks:**
- Audit a system to find files with the suid/sgid bit set
  - Set or change user passwords and password aging information
  - Being able to use nmap and netstat to discover open ports on a system
  - Set up limits on user logins, processes and memory usage

# Linux Server II (cont.)

MAIN TOPICS

- Determine which users have logged in to the system or are currently logged in
  - Basic sudo configuration and usage
- 6.2 Setup host security:**
- Awareness of shadow passwords and how they work
  - Turn off network services not in use
  - Understand the role of TCP wrappers
- 6.3 Securing data with encryption:**
- Perform basic OpenSSH 2 client configuration and usage
  - Understand the role of OpenSSH 2 server host keys
  - Perform basic GnuPG configuration, usage, and revocation
  - Understand SSH port tunnels (including X11 tunnels)

RECOMMENDED TEXTBOOK

TITLE: Security Strategies in Linux Platforms and Applications, Second Edition  
AUTHOR: Jang & Messier (2017)  
PUBLISHER: Jones & Bartlett Learning  
ISBN: 978-1-284-09065-9

# Windows Server I

**NCC 206: Windows Server I:  
Installing and Configuring Windows Server**

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course offers in-depth coverage of core services such as Active Directory and networking services and provides validation of skills necessary to implement a core Windows Server 2012 Infrastructure into an existing enterprise environment. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized Information Technology and security fields. It is also intended to serve the needs of individuals seeking to pass the Microsoft certification exam (70-410).



**PREREQUISITE:** NCC 200: Networking I: Networking Fundamentals &  
NCC 204: Linux Server I: Linux Fundamentals

**LEARNING OBJECTIVES**

- Upon completion of this course the student will be able to:
- Implement and administer Active Directory Domain Services;
  - Implement Local Storage;
  - Implement File and Print Services;
  - Setup and manage Group Policy;
  - Implement and administer Server Virtualization with Hyper-V; and
  - Demonstrate appropriate and ethical behavior and good work habits

**MAIN TOPICS**

- 1.0 Installing Servers*
- 2.0 Configuring Servers*
- 3.0 Configuring Local Storage*
- 4.0 Configuring File and Sharing Access*
- 5.0 Configuring Print and Document Services*
- 6.0 Configuring Servers for Remote Management*
- 7.0 Creating and Configuring Virtual Machine Settings*

# Windows Server I (cont.)

- 8.0 Creating and Configuring Virtual Machine Storage*
- 9.0 Creating and Configuring Virtual Networks*
- 10.0 Configuring IPv4 and IPv6 Addressing*
- 11.0 Deploying and Configuring the DHCP Service*
- 12.0 Deploying and Configuring the DNS Service*
- 13.0 Installing Domain Controllers*
- 14.0 Installing Domain Controllers*
- 15.0 Creating and Managing Active Directory Groups and Organizational Units*
- 16.0 Creating Group Policy Objects*
- 17.0 Configuring Security Policies*
- 18.0 Configuring Application Restriction Policies*
- 19.0 Configuring Windows Firewall*

**RECOMMENDED TEXTBOOK**


TITLE: 70-410 Installing & Configuring Windows Server 2012 R2  
AUTHOR: Craig Zacker (2014)  
PUBLISHER: John Wiley & Sons  
ISBN: 978-1-118-88231-3

# Windows Server II

**NCC 207: Windows Server II:  
System Administration**

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course builds on Windows Server I: Installing and Configuring Windows Server by continuing to provide validation of skills necessary to implement a core Windows Server 2012 Infrastructure into an existing enterprise environment. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized Information Technology and security fields. It is also intended to serve the needs of individuals seeking to pass the Microsoft certification exam (70-411).



**PREREQUISITE:** NCC 206: Windows Server I: Installing and Configuring Windows Server

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to:

- Implement a Group Policy Infrastructure;
- Manage user and service accounts;
- Maintain Active Directory Domain Services
- Configure and troubleshoot DNS;
- Configure and troubleshoot Remote Access;
- Install, configure, and troubleshoot the Network Policy Server Role;
- Optimize file services;
- Increase file system security;
- Implement Update Management; and
- Demonstrate appropriate and ethical behavior and good work habits

**MAIN TOPICS**

- 1.0 Deploying and Managing Server Images*
- 2.0 Implementing Patch Management*
- 3.0 Monitoring Servers*

# Windows Server II (cont.)

- 4.0 Configuring Distributed File System (DFS)*
- 5.0 Configuring File Server Resource Manager (FSRM)*
- 6.0 Configuring File Services and Disk Encryption*
- 7.0 Configuring Advanced Audit Policies*
- 8.0 Configuring DNS Zones*
- 9.0 Configuring DNS Records*
- 10.0 Configuring VPN and Routing*
- 11.0 Configuring Direct Access*
- 12.0 Configuring a Network Policy Server (NPS)*
- 13.0 Configuring Network Policy Server Policies*
- 14.0 Configuring Network Access Protection (NAP)*
- 15.0 Configuring Server Authentication*
- 16.0 Configuring Domain Controllers*
- 17.0 Maintaining Active Directory*
- 18.0 Configuring Account Policies*
- 19.0 Configuring Group Policy Processing*
- 20.0 Configuring Group Policy Settings*
- 21.0 Managing Group Policy Objects*
- 22.0 Configuring Group Policy Preferences*

**RECOMMENDED TEXTBOOK**

TITLE: 70-411 Administering Windows Server 2012 R2  
AUTHOR: Patrick Regan (2014)  
PUBLISHER: John Wiley & Sons  
ISBN: 978-1-118-88283-2



# Windows Server III

## NCC 208: Windows Server III: Advanced System Administration

4 credit/unit hours – Four hours of lecture weekly; one term

This course validates the skills and knowledge necessary for implementing, managing, maintaining and provisioning services and infrastructure in a Windows Server 2012 environment. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized Information Technology and security fields. It is also intended to serve the needs of individuals seeking to pass the Microsoft certification exam (70-412).



**PREREQUISITE:** NCC 207: Windows Server II: System Administration

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Configure advanced network services;
- Implement advanced file services;
- Configure dynamic access control;
- Implement network load balancing;
- Configure failover clustering;
- Implementing disaster recovery;
- Install and maintain Active Directory Certificate Services (AD CS);
- Configure and administer Active Directory Federation Services (AD FS); and
- Demonstrate appropriate and ethical behavior and good work habits

### MAIN TOPICS

- 1.0 Configuring Network Load Balancing*
- 2.0 Configuring Failover Clustering*
- 3.0 Managing Failover Clustering Roles*

# Windows Server III (cont.)

- 4.0 Managing Virtual Machine Movement*
- 5.0 Configuring Advanced File Services*
- 6.0 Implementing Dynamic Access Control*
- 7.0 Configuring and Optimizing Storage*
- 8.0 Configuring and Managing Backups*
- 9.0 Recovering Servers*
- 10.0 Configuring Site-Level Fault Tolerance*
- 11.0 Implementing an Advanced DHCP Solution*
- 12.0 Implementing an Advanced DNS Solution*
- 13.0 Deploying and Managing IPAM*
- 14.0 Configuring a Domain and Forest*
- 15.0 Configuring Trusts*
- 16.0 Configuring Sites*
- 17.0 Managing Active Directory and SYSVOL Replication*
- 18.0 Implementing Active Directory Federation Services*
- 19.0 Installing and Configuring Active Directory Certificate Services (AD CS)*
- 20.0 Managing Certificates*
- 21.0 Installing and Configuring Active Directory Rights Management Services*

### RECOMMENDED TEXTBOOK


TITLE: 70-412 Configuring Advanced Windows Server 2012 R2  
AUTHOR: Patrick Regan (2014)  
PUBLISHER: John Wiley & Sons  
ISBN: 978-1-118-88299-3

# Secure Server Services

## NCC 209: Secure Server Services

4 credit/unit hours – Four hours of lecture weekly; one term

This course introduces the student to the design, installation, and secure administration of popular server services, such as web and mail. Students will also demonstrate how to secure these services to ensure their confidentiality, integrity, and availability.



**PREREQUISITE:** NCC 205: Linux Server II: System Administration &  
NCC 208: Windows Server III: Advanced System Administration

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to design, install, and securely administer the following services:

- Domain Name System;
- Hypertext Transfer Protocol (HTTP/HTTPS);
- File Transfer Protocol (FTP/SFTP/FTPS);
- Secure Shell (SSH)
- Sendmail;
- Exchange;
- Database services (e.g., MySQL); and
- Demonstrate appropriate and ethical behavior and good work habits

**MAIN TOPICS**

- 1.0 Hypertext Transfer Protocol (HTTP/HTTPS)
- 2.0 File Transfer Protocol (FTP/SFTP/FTPS)
- 3.0 Secure Shell (SSH)
- 4.0 Mail Services
- 5.0 Database Services

# Information Security Fundamentals

## NCC 210: Information Security Fundamentals

3 credit/unit hours – Three hours of lecture weekly; one term

This course offers in-depth coverage of the current risks and threats to an organization’s data, combined with a structured way of addressing the safeguarding of these critical electronic assets. The course provides a foundation for those new to Information Security as well as those responsible for protecting network services, devices, traffic, and data. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized security fields. It is also intended to serve the needs of individuals seeking to pass the Computing Technology Industry Association’s (CompTIA) Security + certification exam (SY0-401).

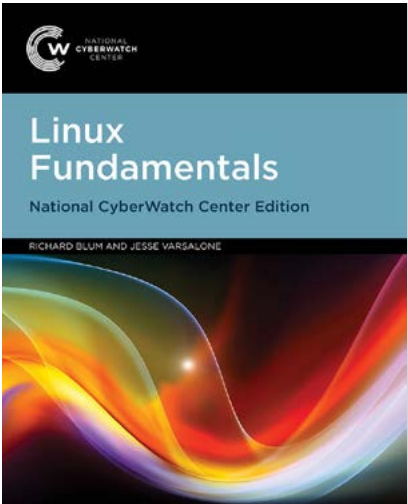


**PREREQUISITE:** NCC 200: Networking 1:  
Networking Fundamentals

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to:

- Describe why information security is essential in today’s IT environment;
- Identify the goals of information security;
- Describe common security threats and their ramifications;
- Determine the factors involved in developing a secure information security strategy;
- Identify common attacks and describe how to safeguard against them;
- Describe communications, E-mail, Web, remote access, and wireless security issues;
- Evaluate various network devices and media and how best to secure them;
- Describe the basics of cryptography;
- Differentiate between physical security, disaster recovery, and business continuity;
- Utilize network diagrams; and
- Demonstrate appropriate and ethical behavior and good work habits



# Information Security Fundamentals (cont.)

MAIN TOPICS

1.0 Information Security:

- Information Security
- Tenets of Information Security
- The Seven Domains of a Typical IT Infrastructure
- Weakest Link in the Security of an IT Infrastructure
- IT Security Policy Framework

2.0 Changing How People and Business Communicate:

- Evolution of Voice Communications
- VoIP and SIP Risks, Threats, and Vulnerabilities
- Converting to a TCP/IP World
- Multimodal Communications
- Evolution from Brick-and-Mortar to E-Commerce
- Why Businesses Need an Internet Marketing Strategy
- IP Mobility

3.0 The Drivers of the Information Security Business:

- Defining Risk Management
- Implementing a BIA, a BCP, and a DRP
- Assessing Risk, Threats, and Vulnerabilities
- Closing the Information Security Gap
- Adhering to Compliance Guidelines and Laws
- Keeping Private Data Confidential

4.0 Access Controls:

- The Four Parts of Access Control
- The Two Types of Access Control
- Defining an Authorization Policy
- Identification Methods and Guidelines
- Authentication Processes and Requirements
- Accountability Policies and Procedures
- Formal Methods of Access Control
- Threats to Access Controls
- Effects of Access Control Violations
- Centralized and Decentralized Access Control

5.0 Security Operations and Administration:

- Security Administration
- Compliance
- Professional Ethics
- The Infrastructure for an IT Security Policy
- Data Classification Standards
- Configuration Management
- The Change Management Process
- The System Life Cycle (SLC) and Systems Development Life Cycle (SDLC)
- Software Development and Security

6.0 Auditing, Testing, and Monitoring:

- Security Auditing and Analysis
- Defining Your Audit Plan
- Auditing Benchmarks
- Audit Data - Collection Methods
- Post-Audit Activities
- Security Monitoring
- Types of Log Information to Capture
- How to Verify Security Controls
- Monitoring and Testing Security Systems

7.0 Risk, Response, and Recovery:

- Risk Management and Information Security
- The Process of Risk Management
- Risk Analysis
- Two Approaches: Quantitative and Qualitative
- Developing a Strategy for Dealing with Risk
- Evaluating Countermeasures
- Controls and Their Place in the Security Life Cycle
- Planning to Survive
- Backing Up Data and Applications
- Steps to Take in Handling an Incident
- Recovery From a Disaster

# Information Security Fundamentals (cont.)

MAIN TOPICS

8.0 Cryptography:

- What is Cryptography?
- Business and Security Requirements for Cryptography
- Cryptographic Applications and Uses in Information Security
- Cryptographic Principles, Concepts, and Terminology
- Cryptographic Applications, Tools, and Resources
- Principles of Certificates and Key Management

9.0 Networks and Telecommunications:

- The Open Systems Interconnection Reference Model
- The Two Types of Networks
- TCP/IP and How It Works
- Network Security Risks
- Basic Network Security Defense
- Wireless Networks

10.0 Malicious Attacks, Threats, and Vulnerabilities:

- Malicious Activity on the Rise
- What Are You Trying to Protect?
- Whom Are You Trying to Catch?
- What is a Security Breach?
- What are Risks, Threats, and Vulnerabilities
- What is Malicious Software?
- Characteristics, Architecture, and Operations of Malicious Software
- Main Types of Malicious Software
- A Brief History of Malicious Software
- Threats to Organizations
- What is a Malicious Attack?
- Attack Tools
- Anatomy of an Attack

- Attack Prevention Tools and Techniques
- Incident Detection Tools and Techniques

11.0 Information Security Standards:

- Standards Organizations
- ISO 17799
- ISO/IEC 27002
- PCI DSS

12.0 Information Security Professional Certifications:

- U.S. DoD/Military - 8570.01 Standard
- Vendor-Neutral Professional Certifications
- Vendor-Specific Professional Certifications

13.0 U.S. Compliance Guidelines & Laws:

- Compliance is the Law
- The Federal Information Security Management Act (FISMA)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Gramm-Leach Bliley Act
- The Sarbanes-Oxley Act
- The Family Educational Rights and Privacy Act
- The Children’s Internet Protection Act
- Making Sense of Laws for Information Security Compliance

RECOMMENDED TEXTBOOK

TITLE: Information Security Fundamentals: National CyberWatch Center Edition (1st Edition)  
AUTHOR: Kim & Solomon (2016)  
PUBLISHER: Jones & Bartlett Learning  
eText ISBN (VitalSource): 9-781-28423-964-5




# TCP/IP Fundamentals

## NCC 211: TCP/IP Fundamentals

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course offers an in-depth look at the various TCP/IP protocols that comprise today’s converging communication technologies and state-of the-art networks. This course is intended for students wishing to understand how communication and network protocols operate: programmers writing network applications, system administrators responsible for maintaining systems and networks utilizing the various protocols, and users who deal with network applications on a daily basis.



**PREREQUISITE:** NCC 200: Networking 1: Networking Fundamentals  
(can be taken concurrently)

**LEARNING OBJECTIVES**

- Upon completion of this course the student will be able to:
- Use a packet sniffer to capture traffic on a network;
  - Analyze captured network/application traffic;
  - Describe how various TCP/IP suite protocols function (e.g., DNS, TCP);
  - Explain how the encapsulation of various TCP/IP suite protocols works;
  - Describe the various TCP/IP suite protocol fields and differentiate between them; and
  - Discuss what normal TCP/IP suite protocol behavior looks like

**MAIN TOPICS**


<i>1.0 Capturing Network Traffic</i>	<i>9.0 User Datagram Protocol (UDP)</i>
<i>2.0 Trace File Analysis</i>	<i>10.0 Domain Name System (DNS)</i>
<i>3.0 Wireshark Functionality and Fundamentals</i>	
<i>4.0 Working with TCP/IP utilities</i>	<b>RECOMMENDED TEXTBOOK</b>
<i>5.0 Address Resolution Protocol (ARP)</i>	TITLE: TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition)
<i>6.0 Internet Protocol (IP) v4 and v6</i>	AUTHOR: Fall & Stevens (2012)
<i>7.0 Internet Control Message Protocol v4 and v6</i>	PUBLISHER: Pearson
<i>8.0 Transmission Control Protocol (TCP)</i>	ISBN: 978-0-321-33631-6

# Scripting Fundamentals

## NCC 212: Scripting Fundamentals

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course offers an in-depth introduction to scripting languages including basic data types, control structures, regular expressions, input/output, and textual analysis.



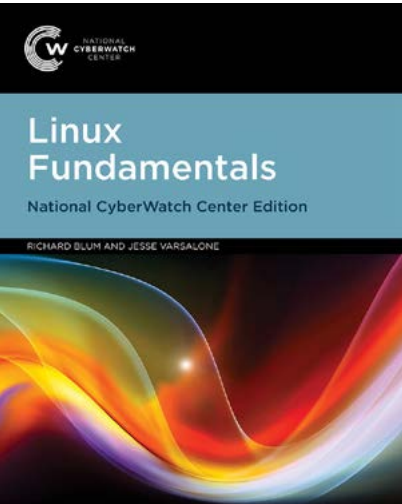
**PREREQUISITE:** NCC 204: Linux Server 1: Linux Fundamentals

**LEARNING OBJECTIVES**

- Upon completion of this course the student will be able to:
- Provide a foundation for learning to program;
  - Write, run, and debug a program;
  - Construct logical conditions and choose appropriate control statements;
  - Understand the software development cycle and program debugging;
  - Design and implement simple programs from user requirements

**MAIN TOPICS**

<i>1.0 Introduction to Scripting</i>	<i>9.0 Accessing Databases</i>
<i>2.0 Scripts, Variables, and Data Types</i>	<i>10.0 Network Programming</i>
<i>3.0 Decisions and Loops</i>	<i>11.0 Web Applications</i>
<i>4.0 Functions</i>	
<i>5.0 Objects and Classes</i>	<b>RECOMMENDED TEXTBOOK</b>
<i>6.0 Modules</i>	TITLE: Introduction to Scripting: National CyberWatch Center Edition (1st Edition)
<i>7.0 File Access</i>	AUTHOR: Miller & Ranum (2017)
<i>8.0 Text Processing and Regular Expressions</i>	Print ISBN: 9781284108071, 1284108074
	eText ISBN: 9781284108071



# Intrusion Detection/Prevention Systems Fundamentals

## NCC 213: Intrusion Detection/Prevention Systems Fundamentals

4 credit/unit hours – Four hours of lecture weekly; one term

Intrusion Detection/Prevention Systems are critical components of well-designed network architectures. These systems act as a line of defense, helping protect company assets from attacks.

In this course, students gain a thorough grounding in the design, implementation, and administration of IDSes/IPSes, as well as practical, hands-on experience working with these systems. In addition, students analyze various attack signatures and the network traffic these systems collect.



**PREREQUISITE:**

- **Cyber Defense degree/certificate:**
  - NCC 201: Networking II: Switching & Routing Fundamentals & NCC 210: Information Security Fundamentals. NOTE: NCC 211: TCP/IP Fundamentals is recommended, but not required in this degree/certificate
- **Network Security Administration degree and Network Security Administration III certificate:**
  - NCC 201: Networking II: Switching & Routing Fundamentals & NCC 211: TCP/IP Fundamentals & NCC 210: Information Security Fundamentals
- **Network Forensics degree:**
  - NCC 201: Networking II: Switching & Routing Fundamentals & NCC 210: Information Security Fundamentals. NOTE: NCC 211: TCP/IP Fundamentals is recommended, but not required in this degree/certificate

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to:

- Differentiate between host-based and network-based IDS solutions;
- Setup and administer an IDS in a working network;
- Dissect and analyze various types of normal and unusual traffic;
- Identify false positives and false negatives; and
- Demonstrate appropriate and ethical behavior and good work habits

# Intrusion Detection/Prevention Systems Fundamentals (cont.)

**MAIN TOPICS**

- 1.0 Network- and Host-Based IDS/IPS Solutions*
- 2.0 Fundamentals of Traffic Analysis*
- 3.0 Advanced Traffic Analysis*
- 4.0 Working with Filters/Rules for Network Monitoring*
- 5.0 Introduction to Network Security Monitoring*
- 6.0 Analyzing and Deconstructing Attack Signatures*

**RECOMMENDED TEXTBOOK**

TITLE: Managing Security with Snort & IDS Tools  
AUTHOR: Cox & Gerg (2004)  
PUBLISHER: O’Reilly Media  
ISBN: 978-0-596-00661-7

# Ethical Hacking

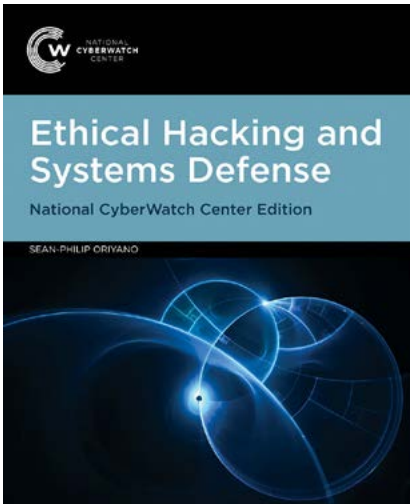
## NCC 214: Ethical Hacking and Systems Defense

**4 credit/unit hours – Four hours of lecture weekly; one term**

The course combines an ethical hacking methodology with the hands-on application of security tools to better help students secure their systems. Students are introduced to common countermeasures that effectively reduce and/or mitigate attacks.



- PREREQUISITE:**
- **Cyber Defense degree/certificate:**
    - All preceding Technical Courses in degree/certificate
  - **Network Security Administration degree and Network Security Administration III certificate:**
    - NCC 220: Network Security I: Network Security Fundamentals & NCC 204: Linux Server I: Linux Fundamentals & NCC 206: Windows Server I: Installing & Configuring Windows Server
  - **Network Forensics degree:**
    - NCC 213: Intrusion Detection/Prevention Systems Fundamentals



### LEARNING OBJECTIVES

- Upon completion of this course the student will be able to:
- Utilize various information security tools given different target systems in different environments;
  - Discuss how the tools interrelate with each other in an overall penetration testing process;
  - Implement countermeasures for various types of attacks;
  - Apply a common ethical hacking methodology to carry out a penetration test;
  - Analyze how penetration testing and ethical hacking fit into a comprehensive enterprise information security program; and
  - Demonstrate ethical behavior appropriate to security-related technologies

# Ethical Hacking (cont.)

### MAIN TOPICS

- 1.0 *Introduction to Ethical Hacking*
- 2.0 *Penetration testing professional certifications*
- 3.0 *Reconnaissance/Open Source Intelligence Gathering*
- 4.0 *Scanning*
- 5.0 *Enumeration*
- 6.0 *Exploitation*
- 7.0 *Post-Exploitation*

### RECOMMENDED TEXTBOOK

TITLE: Ethical Hacking and Systems Defense: National CyberWatch Center Edition (1st Edition)  
AUTHOR: Sean-Philip Oriyano (2016)  
PUBLISHER: Jones & Bartlett Learning  
eText ISBN: 9-781-28423-965-2




# Digital Forensics I

## NCC 215: Digital Forensics I: Digital Forensics Fundamentals

3 credit/unit hours – Three hours of lecture weekly; one term

This course introduces the student to the legal and technical aspects of Digital Forensics, including general forensic processes, imaging, hashing, file recovery, file system basics, identifying mismatched file types, reporting, and laws regarding computer evidence.



**PREREQUISITE:** NCC 204: Linux Server I: Linux Fundamentals

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Describe the standard digital forensic processes;
- Create a forensic copy of a piece of digital media;
- Verify a forensic copy;
- Identify structures of the FAT file system;
- Recover deleted files manually; and
- Discuss laws related to computer evidence



### MAIN TOPICS

- 1.0 Introduction to Digital Forensics
- 2.0 Overview of Forensic Sciences
- 3.0 Criminal and Civil Procedure
- 4.0 Courtroom Testimony
- 5.0 Evidence Law
- 6.0 Intellectual Property
- 7.0 Report Writing
- 8.0 Seizing and Imaging

# Digital Forensics I (cont.)

### MAIN TOPICS

- 9.0 Hierarchy of Access
- 10.0 File Systems
- 11.0 Physical Analysis
- 12.0 Forensic Tool Validation
- 13.0 Drives
- 14.0 Date and Time Stamps
- 15.0 Logical Analysis
- 16.0 Commercial Tools
- 17.0 Windows Registry Analysis
- 18.0 Internet and Email Forensics
- 19.0 Ethics

### RECOMMENDED TEXTBOOK

TITLE: System Forensics, Investigation and Response (2nd Edition)  
AUTHOR: Easttom (2014)  
PUBLISHER: Jones & Bartlett Learning  
ISBN: 978-1-284-03105-8

# Digital Forensics II

## NCC 216: Digital Forensics II: Advanced Digital Forensics

4 credit/unit hours – Four hours of lecture weekly; one term

This course introduces the student to the theory of forensic procedures, review of identification, imaging, and authentication, review of FAT, NTFS, EXT3, and HFS Plus file systems, ethics, RAM capture, honeypots, Window’s registry analysis, mobile device forensics, and Email and web history analysis.



**PREREQUISITE:** NCC 215: Digital Forensics I: Digital Forensics Fundamentals

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Identify and create a forensic copy of media, and authenticate digital evidence;
- Employ Linux and Windows-based digital forensics tools for a particular forensic task;
- Identify key components of various file systems;
- Perform a forensic analysis using Windows registry;
- Perform an analysis of Email and web history;
- Demonstrate an understanding of data hiding techniques

### MAIN TOPICS

1.0 Introduction to Digital Forensics

2.0 Introduction to Cyberforensics

3.0 Imaging and Verification

4.0 FAT File System

5.0 Forensic Tools

6.0 NTFS

7.0 EXT File System

8.0 HFS Plus, Macintosh and Linux Boot Processes

9.0 Windows Registry Analysis

10.0 Capturing and Analyzing RAM and Swap

11.0 Honeypots

12.0 Mobile Device Forensics

13.0 Forensics on Solid State Drives

14.0 Ethics

### RECOMMENDED TEXTBOOK

TITLE: File System Forensic Analysis

AUTHOR: Carrier (2005)

PUBLISHER: Pearson

ISBN: 978-0-321-26817-4

# Operating Systems Fundamentals

## NCC 217: Operating Systems Fundamentals

3 credit/unit hours – Three hours of lecture weekly; one term

This course is designed to provide an introduction to and basic technical understanding of the function and operation of Microsoft Windows operating systems. The course will focus on microcomputer operating system features, broad concepts, and diagnostic tools that allow the student to rapidly determine the condition of a PC system and how best to rectify a fault. This course also introduces the student to mobile operating systems.

This course is also intended for those preparing for the Computing Technology Industry Association’s (CompTIA) A+ certification exam (220-802).



**PREREQUISITE:** NCC 200: Networking I: Networking Fundamentals  
(can be taken concurrently)

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Compare and contrast the features and requirements of Microsoft Operating systems;
- Install and configure the operating system using the most appropriate method;
- Implement appropriate command line tools;
- Setup and configure Windows networking on a client/desktop;
- Perform preventive maintenance procedures using appropriate tools;
- Implement security best practices to secure a workstation;
- Explain the basic features of mobile operating systems;
- Compare and contrast methods for securing mobile devices; and
- Implement and configure mobile device synchronization

### MAIN TOPICS:

1.0 Introduction to Operating Systems

2.0 Introducing How Hardware and Software Work

3.0 Install, Maintain, and Troubleshoot Windows OS

4.0 Working with the Command Line

5.0 Maintaining and Troubleshooting Fundamentals

6.0 Implementing and Configuring Security Best Practices to Harden a Workstation

7.0 Introduction to Mobile Devices


# Hardware I

## NCC 218: Hardware I: Hardware Fundamentals

4 credit/unit hours – Four hours of lecture weekly; one term

This course explores the inter-relationships between hardware and software at the system level. Topics covered include: processors and chipsets, motherboards, memory, storage devices, and multimedia devices. Diagnostic software is used to identify and isolate faulty devices and sub-systems.

This course is also intended for those preparing for the Computing Technology Industry Association’s (CompTIA) A+ certification exam (220-801).



PREREQUISITE: NCC 217: Operating Systems Fundamentals

LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Identify the basic components of a microcomputer;
- Distinguish between the popular CPU chips in terms of their basic characteristics;
- Identify basic procedures for disk management;
- Identify and install various memory types;
- Identify proper procedures for installing and configuring peripheral devices;
- Identify hardware methods of upgrading system performance, procedures for replacing basic subsystem components, unique components and when to use them;
- Identify common symptoms and problems associated with each subsystem and how to troubleshoot and isolate the problem;
- Discuss the fundamental workings of multimedia technology;
- Describe the basics of how computers communicate with each other; and
- Identify the major components of a printer

MAIN TOPICS

- 1.0 PC Hardware
- 2.0 All About Motherboards
- 3.0 Supporting Processors and Upgrading Memory

# Hardware I (cont.)

MAIN TOPICS

- 4.0 Supporting Hard Drives
- 5.0 Supporting I/O and Storage Devices
- 6.0 Networking
- 7.0 Laptops
- 8.0 Printers
- 9.0 Troubleshooting Hardware Problems

RECOMMENDED TEXTBOOK


TITLE: A+ Guide to Managing & Maintaining Your PC, 8th Edition  
AUTHOR: Andrews (2014)  
PUBLISHER: Cengage Learning  
ISBN: 978-1-133-13508-1



# Network Forensics

## NCC 219: Network Forensics and Incident Response

**4 credit/unit hours – Four hours of lecture weekly; one term**  
This course explores security incidents and intrusions, including identifying and categorizing incidents, responding to incidents, log analysis, network traffic analysis, various tools, and creating an incident response team.



**PREREQUISITE:** NCC 214: Ethical Hacking and Systems Defense

**LEARNING OBJECTIVES**

- Upon completion of this course the student will be able to:
- Detect and characterize various types of computer and network incidents;
  - Demonstrate a practical understanding of the analysis of artifacts left on a compromised system;
  - Demonstrate an understanding of how to effectively respond to privileged and major event incidents;
  - Demonstrate an understanding of advisories, alerts, and management briefings;
  - Demonstrate the ability to communicate incident response findings to technical and non- technical personnel

**MAIN TOPICS**

- 1.0

Overview of Incident Response
- 2.0

Malware Analysis
- 3.0

Working Over a Network
- 4.0

Network Forensics
- 5.0

Intelligence Gathering
- 6.0

Host-Based Intrusion Detection Systems (IDSes)
- 7.0

Honeypots
- 8.0


Identifying Indicators of an Intrusion
- 9.0

Ethics in Digital Forensics

# Network Security I

## NCC 220: Network Security I: Network Security Fundamentals

**4 credit/unit hours – Four hours of lecture weekly; one term**  
This course prepares students for entry-level security specialist careers by developing an in-depth understanding of network security principles and the tools and configurations needed to secure a network.



**PREREQUISITE:** NCC 213: Intrusion Detection/Prevention Systems Fundamentals (can be taken concurrently)

**LEARNING OBJECTIVES**

- Upon completion of this course the student will be able to:
- Describe the security threats facing modern network infrastructures;
  - Secure routers;
  - Implement Authentication, Authorization, and Accounting (AAA);
  - Mitigate threats to routers and networks using Access Control Lists (ACLs);
  - Implement secure network design, management, and reporting;
  - Mitigate common Layer 2 attacks;
  - Implement and administer a firewall;
  - Implement a site-to-site VPN; and
  - Implement a remote access VPN

**MAIN TOPICS:**

- 1.0

Modern Network Security Threats
- 2.0

Securing Network Devices
- 3.0

Authentication, Authorization, and Accounting
- 4.0

Implementing Firewall Technologies
- 5.0

Securing the Local-Area Network (LAN)
- 6.0

Cryptographic Systems
- 7.0

Implementing Virtual Private Networks (VPNs)
- 8.0

Managing a Secure Network



# Programming Logic

## NCC 221: Introduction to Secure Programming Logic

**3 credit/unit hours - Three hours of lecture weekly; one term**

This is an introductory course in structured programming logic. Students will learn to analyze problems; define data using simple data types and arrays; and create algorithmic solutions using basic control structures (sequence, selections, loops) and functions.

Students learn to systematically break down a problem into manageable parts; plan and design logical solutions; and write effective, structured, and well-documented instructions. Emphasis will be on problem-solving approaches (algorithms) and the fundamental concepts and programming techniques common to modern computer languages including variable assignment, expressions, input/output statements, loops, if-then-else and case constructs, functions, arrays, etc. The concepts learned in this course are applicable to multiple modern programming languages.



**PREREQUISITE:** General Education IT course (can be taken concurrently)

### LEARNING OBJECTIVES

- Upon completion of this course the student will be able to:
- Describe the software development life cycle;
  - Describe how security has to be a consideration from the point of initial design and throughout the lifecycle of a product;
  - Analyze problems and design structured solutions;
  - Create and apply simple data types and arrays;
  - Identify common coding errors (e.g., buffer overflow and integer errors) that lead to insecure programs;
  - Create algorithmic solutions using basic control structures (sequence, decisions, loops) and functions;
  - Discuss the importance of input validation and write correct input validation code;
  - Compile, execute, and run simple programs;
  - Describe the importance of secure and responsible programming; and
  - Conduct a personal code review (focused on common coding errors) on a program component using a provided checklist

# Programming Logic (cont.)

### MAIN TOPICS

- 1.0 Overview of Computers and Logic*
- 2.0 Comparison of Programming Languages*
- 3.0 Number Systems/ASCII (American Standard Code for Information Interchange)*
- 4.0 Program Structure*
- 5.0 Modules, Hierarchy Charts, and Documentation*
- 6.0 Writing a Complete Program*
- 7.0 Looping*
- 8.0 Arrays/Lists*
- 9.0 Validating Input*
- 10.0 Modularization Techniques*
- 11.0 Object-Oriented Programming Concepts*
- 12.0 Programming Graphical User Interfaces (GUIs)*
- 13.0 Software Development Life Cycle*
- 14.0 Ethics and Intellectual Property*
- 15.0 Globalization and Collaboration*

### RECOMMENDED TEXTBOOK

TITLE: Programming and Problem Solving with C++: Brief, Sixth Edition  
AUTHOR: Dale & Weems (2014)  
PUBLISHER: Jones & Bartlett Learning  
ISBN: 978-1-284-02864-5

# Computer Science I

## NCC 222: Computer Science I

4 credit/unit hours – Four hours of lecture weekly; one term

This course teaches problem-solving skills using accepted programming practices. Discussions and hands-on labs focus on algorithms, data structures, fundamental syntax of an object-oriented language, data types, control structures, file I/O, classes, objects, methods, and arrays.



**PREREQUISITE:** NCC 221: Introduction to Secure Programming

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Use an object-oriented programming language for problem solving;
- Design algorithms and translate them into working solutions;
- Demonstrate the importance of testing and validating the solution;
- Identify the data types and variable naming conventions;
- Demonstrate how to do calculations;
- Demonstrate inputting and outputting of data;
- Identify techniques for formatting data;
- Construct programs using the three control structures: sequence, selection, and repetition;
- Write programs using arrays;
- Identify, explain, and discuss data organization; and
- Develop basic GUI (Graphical User Interfaces) using various programming components

### MAIN TOPICS

#### 1.0 Role of Different Programming Languages:

- 1.1 Procedural
- 1.2 Event-Driven
- 1.3 Object-Oriented

#### 2.0 Introduction to a Structured Language:

- 2.1 Logic diagrams
- 2.2 Use of Integrated Development Environment

# Computer Science I (cont.)

### MAIN TOPICS

#### 3.0 Program Development Cycle:

- 3.1 Design the solution
- 3.2 Code
- 3.3 Test
- 3.4 Document

#### 4.0 Data Types

#### 5.0 Arithmetic Expressions

#### 6.0 Input and Output:

- 6.1 Accepting data from the keyboard
- 6.2 Formatting output

#### 7.0 Selection:

- 7.1 Simple If
- 7.2 Nested If
- 7.3 Switch

#### 8.0 Repetition:

- 8.1 while loop
- 8.2 do loop
- 8.3 for loop

#### 9.0 Methods and Classes

#### 10.0 Data Files:

- 10.1 Data vocabulary
- 10.2 Sequential files
- 10.3 Text files

#### 11.0 Arrays

#### 12.0 Debugging Techniques:

- 12.1 Use of loop invariants
- 12.2 Use of method preconditions and post-conditions
- 12.3 Use of stubs and drivers
- 12.4 Program tracing, testing, documentation and verification

#### 13.0 Graphical User Interfaces:

- 13.1 Components used in developing a GUI window
- 13.2 Complex GUI using layouts
- 13.3 ActionListener

### RECOMMENDED TEXTBOOK

TITLE: Java Illuminated, Fourth Edition

AUTHOR: Anderson & Franceschi (2016)

PUBLISHER: Jones & Bartlett Learning


ISBN: 978-1-284-04531-4

# Computer Science II

## NCC 223: Computer Science II

4 credit/unit hours – Four hours of lecture weekly; one term

This course teaches skills for solving complex problems. Discussions and hands-on labs focus on advanced data structures and algorithms for recursion, pointer variables, linked lists, stacks, queues, hash tables, collections, sorting and searching, and trees.



**PREREQUISITE:** NCC 222: Computer Science I

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Analyze problems to determine most appropriate data structure;
- Use an object-oriented or structured programming language for complex problem solving;
- Develop well-written, secure, and documented programs that use recursion, dynamic memory allocation, and abstract data types;
- Evaluate mathematical efficiency of algorithms and sorting and searching techniques;
- Discuss the advantages and disadvantages of object-oriented languages compared to procedural programming languages;
- Apply abstract data types to applications;
- Use recursion to solve looping problems;
- Discuss advantages of encapsulation and inheritance; and
- Work in teams to develop large, complex programs

### MAIN TOPICS

- 1.0 Introduction to Abstract Data Types (ADTs):

1.1 Definition of ADT

1.2 Use of Specification and Implementation Files

1.3 Collections
- 2.0 Recursion:

2.1 Static Versus Dynamic Storage Allocation

2.2 Recursive Versus Iterative Solutions

# Computer Science II (cont.)

### MAIN TOPICS

- 3.0 Databases:

3.1 Basic Table and Data Commands

3.2 Connecting to a Database
- 4.0 Abstract Data Types:

4.1 Linked Lists

4.2 Stacks

4.3 Queues

4.4 Binary Search Trees

4.5 Various Tree Traversals

4.6 Heaps

4.7 Collections
- 5.0 Big-O Notation and Efficiency of Algorithms:

5.1 Definition

5.2 Examples
- 6.0 Sorting Algorithms:

6.1 O(N<sup>2</sup>) Algorithms

6.2 O(N\*logN) Algorithms
- 7.0 Searching Algorithms:

7.1 Sequential Search

7.2 Binary Search

7.3 Hashing
- 8.0 Object-Oriented Programming Topics:

8.1 Encapsulation

8.2 Inheritance

8.3 Polymorphism and Dynamic Binding

8.4 Operations in Derived Classes

8.5 Constructors in Derived Classes
- 9.0 Advanced Sorting/Searching Techniques:

9.1 Binary Sort

9.2 Shell Sort

9.3 2-3 Trees
- 10.0 Advanced Graphical User Interfaces (GUIs):

10.1 Timers

10.2 Mouse Interface Features

**RECOMMENDED TEXTBOOK**

TITLE: Object-Oriented Data Structures Using Java, Fourth Edition

AUTHOR: Dale, Joyce & Weems (2018)

PUBLISHER: Jones & Bartlett Learning

ISBN: 9-781-28408-909-7



# Computer Architecture

## NCC 224: Computer Architecture

4 credit/unit hours – Four hours of lecture weekly; one term

This course is an introduction to the organization and operation of a computer system. The focus of the course is on machine representation of instructions and data through the study of a low-level, machine-oriented assembly language.



**PREREQUISITE:** NCC 223: Computer Science II

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Describe the operational components of a Von Neumann Machine and explain how they work together to as a modern computer;
- Design higher-level language program control constructs using a lower-level (assembly-level) language;
- Model higher-level language data structures such as arrays, queues and stacks, using a lower-level language;
- Solve arithmetic problems when numbers are represented in bases other than decimal (e.g., binary, octal and hexadecimal); and
- Locate and identify data and instructions represented in memory dumps

### MAIN TOPICS

- 1.0 The 7 Layer Model of the Modern Computer
- 2.0 Program Control Structures
- 3.0 Data representation Systems
- 4.0 Von Neumann’s Machine and Machine Cycle
- 5.0 Review of Boolean Operations
- 6.0 Higher Level Language Program Constructs
- 7.0 Data Modeling
- 8.0 Array Representation and Implementation

- 9.0 Basic Theorems of Boolean Algebra, Truth Tables and Logic Circuits
- 10.0 Digital Logic

### RECOMMENDED TEXTBOOK

TITLE: Essentials of Computer Organization and Architecture, Enhanced Fourth Edition  
AUTHOR: Null & Lobur (2015)  
PUBLISHER: Jones & Bartlett Learning  
ISBN: 978-1-284-07448-2

# Relational Databases

## NCC 225: Introduction to Relational Databases

3 credit/unit hours – Three hours of lecture weekly; one term

This course introduces elementary relational database concepts, including but not limited to database modeling and Structured Query Language (SQL).



**PREREQUISITE:** NCC 222: Computer Science I

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Understand the purpose, philosophy, and motivation behind databases;
- Understand the capabilities of relational databases;
- Perform data modeling;
- Consider special database designs;
- Implement a database design;
- Perform basic database administrator functions; and
- Demonstrate appropriate and ethical behavior and good work habits

### MAIN TOPICS:

- 1.0 Introduction to databases
- 2.0 Data modeling
- 3.0 Database design
- 4.0 Database implementation with the relational model - SQL
- 5.0 Multi-user databases
- 6.0 Enterprise databases

# Secure Coding

## NCC 226: Secure Coding

**3 credit/unit hours – Three hours of lecture weekly; one term**  
This course covers security vulnerabilities of programming in weakly typed languages like C and in more modern languages like Java. Common weaknesses exploited by attackers are discussed, as well as mitigation strategies to prevent those weaknesses. Students practice programming and analysis of software systems through testing and static analysis.



**PREREQUISITE:** NCC 223: Computer Science II

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Differentiate between types of security vulnerabilities;
- Describe various exploitations and risks in software;
- Use security assurance techniques in their coding to mitigate vulnerabilities;
- Testing and analyze software to provide security assurance; and
- Demonstrate appropriate and ethical behavior and good work habits

### MAIN TOPICS

- 1.0 Overview of security vulnerabilities and risks in software:**
  - 1.1 Common Weakness Enumeration(CWE)**
  - 1.2 Open Web Application Security Project (OWASP) Top 10**
- 2.0 Data Protection:**
  - 2.1 Methods for preventing unauthorized access or manipulation of data**
- 3.0 Input validation and user authentication**
- 4.0 Memory Management:**
  - 4.1 Buffer overflows**
  - 4.2 Memory corruption**
  - 4.3 Privilege violations**

# Secure Coding (cont.)

### MAIN TOPICS

- 5.0 Integer overflow and misuse of strings and pointers**
- 6.0 Communication Vulnerabilities:**
  - 6.1 Concurrency**
  - 6.2 Secure inter-process communication and authorization**
  - 6.3 Authentication and networking protocols**
- 7.0 Unit Testing for Security Vulnerabilities:**
  - 7.1 Fuzzing,**
  - 7.2 Abuse Cases**
- 8.0 Code Review:**
  - 8.1 Formal inspections**
  - 8.2 Static analysis**
- 9.0 Vulnerabilities in Modern Languages:**
  - 9.1 Insecurities in Java and hypertext preprocessor (PHP)**
- 10.0 Standard Risk Mitigation Strategies and Resources:**
  - 10.1 Coding standards**
  - 10.2 Enterprise Security API (ESAPI)**

# Computer Science III

## NCC 227: Computer Science III

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course covers design and implementation of large-scale problems; abstract data types; data structures (files, sets, pointers, lists, stacks, queues, trees, graphs); algorithmic analysis; software engineering principles; software and information assurance; and an introduction to searching and sorting algorithms.



**PREREQUISITE:** NCC 223: Computer Science II

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Design, implement and formally test for the elimination of common software security vulnerabilities in a medium-sized software application, utilizing super-classes, subclasses, abstract classes, and interfaces;
- Implement and utilize exception-handling techniques;
- Design, construct, and assess appropriateness of solutions using a variety of basic recursive techniques;
- Design, implement, and utilize data structures including arrays, linked lists, stacks, queues, trees, sets, hashing, maps and graphs;
- Understand time and space efficiency analysis of searching and sorting algorithms; and
- Practice the tenets of ethical and professional behavior promoted by professional societies and accept the professional responsibilities and liabilities associated with software development

### MAIN TOPICS

- 1.0 Design, implementation and use of the basic classes and object-oriented programs including encapsulation, inheritance, polymorphisms, dynamic binding, abstract classes and interface*
- 2.0 Implementation and use of exception handling in writing Java programs*
- 3.0 Principles and use of recursive techniques in writing Java programs*
- 4.0 Implementation of various searching and sorting algorithms, and the analysis of algorithm complexity and program verification*

# Computer Science II (cont.)

### MAIN TOPICS

- 5.0 Design, implementation and use of singly-linked lists and doubly-linked lists*
- 6.0 Design, implementation and use of stacks and queues*
- 7.0 Design, implement and use of sets, hashing, maps, trees and graphs*
- 8.0 Implementation and use of generic programming*
- 9.0 Tenets of ethical and professional behavior of programmers*
- 10.0 Security awareness and assurance through secure design and formal testing*

### RECOMMENDED TEXTBOOK


TITLE: Introduction to Java Programming - Comprehensive Version, 10th Edition  
AUTHOR: Daniel Y. Laing (2014)  
PUBLISHER: Upper Saddle River: Pearson Publishing  
ISBN-13: 978-0133761313  
ISBN-10: 0133761312

# C# Programming

## NCC 228: C# Programming

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course introduces a current Object Oriented Programmer to the C# programming language, a part of the Microsoft.NET platform. All programming elements of the language are presented in a rapid survey of the language. Emphasis is placed on interfacing with databases and class design. The skills needed to write console applications, Windows applications, and beginning Internet applications are presented.



**PREREQUISITE:** NGen Ed: Math and NCC 222: Computer Science I

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Create graphical Windows applications that use the standard graphical objects of the Windows platform;
- Interface with databases and perform routine database queries via the C# application;
- Make effective use of Object Oriented Class Design, including inheritance, and to make use of the advanced features of the language;
- Write console applications as well as beginning Internet applications; and
- Demonstrate appropriate and ethical behavior and good work habits

### MAIN TOPICS

- 1.0 Developing C# programs that run in a console window, in a graphical windows environment, and in deployment on a website*
- 2.0 Presenting the key features of the language, including language elements, class design, and inheritance*
- 3.0 Handling C# exceptions to avoid program crashes*
- 4.0 Using C# arrays, strings, and properties*
- 5.0 Coding C# indexers and enumerators*
- 6.0 Utilizing the C# interfaces, delegates, and event handlers*
- 7.0 Effective utilization of the C# container classes*

# C# Programming (cont.)

### MAIN TOPICS

- 8.0 Writing applications that use a Windows user interface*
- 9.0 Writing beginning Internet applications*

### RECOMMENDED TEXTBOOK

TITLE: Starting out with Visual C# 2012 (with CD-ROM), 3rd Edition  
AUTHOR: Tony Gaddis (2014)  
PUBLISHER: Addison-Wesley  
ISBN-13: 978-0133129458  
ISBN-10: 0133129454




# Structured Query Language

## NCC 229: Structured Query Language

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course covers programming in the Structured Query Language. Students are taught to create and maintain database objects and to store, retrieve, and manipulate data. In addition, students learn to create blocks of application code that can be shared by multiple forms, reports, and data management applications. Students also learn how to write and apply triggers, procedures, and packages. Demonstrations and hands-on practice reinforce the fundamental concepts.



**PREREQUISITE:** NCC 225: Introduction to Relational Databases

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to:

- Use SQL commands to create, maintain, and query a relational database;
- Write SQL scripts that create, maintain, and query relational databases;
- Develop, maintain, and use triggers, procedures, and packages within a relational database; and
- Demonstrate appropriate and ethical behavior and good work habits

**MAIN TOPICS**

- 1.0 Query commands
- 2.0 Joining multiple tables
- 3.0 Single row and group functions
- 4.0 Subqueries
- 5.0 Creating and managing tables
- 6.0 Constraints
- 7.0 Data manipulation
- 8.0 Views
- 9.0 Other objects: sequences, indexes
- 10.0 Creating and managing users
- 11.0 Formatting output
- 12.0 PL/SQL blocks
- 13.0 Procedures

- 14.0 Functions
- 15.0 Packages
- 16.0 Triggers
- 17.0 Performance tuning

**RECOMMENDED TEXTBOOK**


TITLE: Microsoft SQL Server 2008: T-SQL Fundamentals (1st Edition) & Inside Microsoft SQL Server 2008  
AUTHOR: Itzik Ben-Gan (2008 & 2009)  
PUBLISHER: Microsoft Press  
ISBN-13: 978-0735626010/ISBN-10: 0735626014 &  
ISBN-13: 978-0735626027  
ISBN-10: 0735626022

# Assured Software Engineering

## NCC 230: Assured Software Engineering

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course covers the basic principles and concepts of assured software engineering; system requirements; secure programming in the large; modeling and testing; object-oriented analysis and design using the Unified Modeling Language (UML); design patterns; frameworks and Application Programming Interfaces (APIs); client-server architecture; user interface technology; and the analysis, design and programming of software systems.



**PREREQUISITE:** NCC 227: Computer Science III

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to:

- Discuss software project management and security process models;
- Describe the role of assured software engineering;
- Apply analysis skills to assure functionality and quality requirements;
- Describe software architecture, architectural patterns, and client-server computing;
- Discuss misuse cases;
- Describe design patterns: composite, player-role, singleton, etc.;
- Develop and review core UML diagrams;
- Describe domain modeling;
- Discuss reusable technologies;
- Assure correct software behavior under all conditions;
- Verify and validate software including acceptance testing; and
- Demonstrate appropriate and ethical behavior and good work habits

**MAIN TOPICS:**


- 1.0 Evaluating the assurance and performance of various simple software designs
- 2.0 Addition of features, including assurance features, to existing systems
- 3.0 Testing a system to verify conformance to test cases including assurance
- 4.0 Building a graphical user interface (GUI) for an application
- 5.0 Building and reading core subset of UML
- 6.0 Developing and presenting a simple set of assured software requirements
- 7.0 Implementing and using the above using reusable technology, while understanding risks of reuse

# Mobile Application Programming

## NCC 231: Mobile Application Programming

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course covers the fundamental programming principles for mobile devices. The software architecture and user experience considerations underlying handheld software applications and their development environments will be investigated. Concepts will be reinforced by hands--on programming assignments, which will be run on a current mobile platform.



**PREREQUISITE:** NCC 223: Computer Science II

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to:

- Understand the meaning and uses of mobile computing;
- Understand of one or more major mobile operating systems;
- Describe the basic structures and objects of mobile programming;
- Understand how businesses use mobile applications;
- Plan, develop, and code mobile applications;
- Have a firm basis for further training in mobile application development; and
- Demonstrate appropriate and ethical behavior and good work habits

**MAIN TOPICS**

- 1.0 Introduction to Mobile Operating System

2.0 Mobile Application Market/Business Issues

3.0 Introduction to Applications

4.0 Classes, Objects, Methods

5.0 Variables/Constants and Assignment

6.0 Data Types

7.0 Control Structures

8.0 Decision/Selection

9.0 Iteration/Repetition

10.0 Arrays

**RECOMMENDED TEXTBOOK**

TITLE: Android: How to Program, 2nd Edition

AUTHOR: Paul Deital, Harvey Deital, Abbey Deital (2014)

PUBLISHER: Pearson

ISBN-13: 978-0133764031


ISBN-10: 0133764036

# Database Administration

## NCC 232: Database Administration

**3 credit/unit hours – Three hours of lecture weekly; one term**

This course is designed to give the database administrator (DBA) a firm foundation in basic administrative tasks and provide the necessary knowledge and skills to set up, maintain, and troubleshoot a relational database. Students learn to use an administration tool to startup and shutdown a database, create a database, manage file and database storage, and manage users and their privileges. In addition, students learn to organize the database and to move data into and between databases under different environments. Hands-on practices help to reinforce key concepts.



**PREREQUISITE:** NCC 229: Structure Query Language

**LEARNING OBJECTIVES**

Upon completion of this course the student will be able to:

- Manage database files;
- Manage tablespaces, segments, extents, and blocks;
- Manage users, privileges, and resources;
- Start up and shut down an instance and database;
- Use National Language Support Features (NLSF); and
- Demonstrate appropriate and ethical behavior and good work habits

**MAIN TOPICS:**

- 1.0 DBMS installation

2.0 SQL\*Plus, Import, SQL\*Loader, and other DBA tools, including the new wizards

3.0 DBMS account management

4.0 DBMS performance tuning, including the use of rules-based or cost-based optimizer, SQL statement tuning, and instance tuning

5.0 Advanced topics from PL/SQL programming and the enhanced resource management tools to auditing and partitioning

6.0 Internet functionality using Portal, the HTML server, Java, etc.

7.0 Syntax references for SQL, PL/SQL built-in functions, and SQL\*Plus

# Structured System Analysis

## NCC 233: Structured System Analysis

3 credit/unit hours – Three hours of lecture weekly; one term

This course presents the System Development Life Cycle (SDLC), as the basis for the development of computer systems. Various analysis tools are taught to aid students in the preparation of all aspects of system development.



**PREREQUISITE:** NCC 227: Computer Science III

### LEARNING OBJECTIVES

Upon completion of this course the student will be able to:

- Develop the ability to analyze present information flow;
- Use data flow diagrams for system specification;
- Write process specifications;
- Building data dictionaries;
- Describe the use of CASE tools;
- Test systems;
- Design input, output, and user interfaces; and
- Demonstrate appropriate and ethical behavior and good work habits

### MAIN TOPICS

#### 1.0 Introduction:

- 1.1 The system life cycle
- 1.2 CASE tools
- 1.3 Organizational styles
- 1.4 Feasibility studies

#### 2.0 The use of structured methodologies:

- 2.1 Sampling
- 2.2 Interviewing
- 2.3 Questionnaires
- 2.4 Observation
- 2.5 Prototyping

# Structured System Analysis (cont.)

#### 3.0 The analysis process:

- 3.1 Data flow diagrams
- 3.2 Data dictionaries
- 3.3 Process specifications
- 3.4 Decision support system
- 3.5 The systems proposal

#### 4.0 Elements of design:

- 4.1 Output
- 4.2 Input
- 4.3 Database and files
- 4.4 User interfaces
- 4.5 Data entry

#### 5.0 Quality assurance:

- 5.1 Concepts
- 5.2 Training users
- 5.3 Testing systems

### RECOMMENDED TEXTBOOK

TITLE: Systems Analysis and Design, 10th Edition

AUTHOR: Harry Rosenblatt (2013)

PUBLISHER: Cengage Learning

ISBN-13: 978-1285192482

ISBN-10: 1285192486



*Transforming lives.*

PRINCE GEORGE'S  
COMMUNITY COLLEGE



NATIONAL  
CYBERWATCH  
CENTER

**NATIONALCYBERWATCH.ORG**