CAE-2Y Accredited

Computer and Network Security Certification Apprenticeship Program

(*All Courses Online Only)*

Certificate of Completion
36 credit hours

This program meets the CAE2Y knowledge units designation and is specifically designed to prepare students as *Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011* provide current Information Systems professionals with an Information Systems security certification to meet the needs of current and future employer requirements. Upon completion of this program students will be receive a university certification of completion and the Industry Certification - CompTIA A+, CompTIA Network +, and CompTIA Security+. Note, the labs use the INFOSEC virtual labs for hands-on training and the National Cyber League (NCL) Competitions.

IS 101 – IT Essentials I: PC Hardware, Software, and Practical Applications (4) ****
IS 121 - IT Essentials II: Network Operating Systems (3) ****
CS 123/L Programming Fundamentals (4) Credits ****
IS 131 COMPUTER AND SECURITY FUNDAMENTALS. (3) Credits
IS 257 ETHICAL HACKING, COMPUTER AND NETWORK DEFENSE AND COUNTER MEASURES (4) Credits
IS 297 Cyber Security Technician Apprenticeship (18) Credits

****SUN Online Courses and/or ENMU-Ruidoso.

The objectives of the program include:

- Students are capable of plan, analyze, develop, implement, maintain, and enhancing information systems security programs, policies, procedures, and tools to ensure the confidentiality, integrity, and availability of systems, networks, and data.
- Students will have the knowledge to implement higher-level security requirements; integrate security programs across disciplines; define security plans and policies; assess new system design methodologies to improve software quality; and institute measures to ensure awareness and compliance.

- Students will have the knowledge to assess new security technologies and/or threats and recommend changes; review and evaluate security incident response policies; and develop long-range plans for IT security systems.
- Students will have understanding and knowledge to resolve integration issues related to the implementation of new systems with the existing infrastructure.

Course Descriptions

IS 101 – IT Essentials I: PC Hardware, Software, and Practical (SUN Online) Applications (4)

Course Description:

Covers the fundamentals of computer hardware and software as well as advanced concepts. The basics of computer hardware and Network Operating Systems (NOS) technologies are introduced in a lab-oriented environment.

Course Objectives:

1. Identify, test and install PC-compatible computer and operating system components;
2. Install, configure and test PC-compatible hardware, equipment and applications software
3. Upgrade and change hardware and software components;
   Use the appropriate operation systems tools to manage the computer systems
4. Install and configure disk storage systems and multimedia, and customize systems and/or user interfaces
5. Configure PCs for installation on peer-to-peer and local area networks
6. Perform hardware and system diagnostics
7. Manage data storage and backup, and implement PC and data security
8. Provide basic setup and support to laptops, PDAs, printers and scanners

IS 121 - IT Essentials II: Network Operating Systems (3) (SUN Online

This course covers the installation and administration of Network Operating Systems including Microsoft Windows and Linux. Students will be instructed in both lecture and hands-on labs, including server setup, server configuration, basic administration of common networking services and security administration with an emphasis on network communication protocols.

Course Objectives:

1. Configure network services, including basic network security and troubleshooting
2. Use fundamental command-line features of the Linux environment including file system navigation, file permissions, the vi text editor, command shells, and basic network use
3. Explore GUI features including Applications Manager, Text Editor, printing, and mail
4. Understand administrative tasks and network services with Microsoft Windows, UNIX and Linux.
5. Hardware installation under different operating system, configuration of network services, including network security and troubleshooting.

6. Perform network administration including backups, drive mapping, partition and process management, monitoring resources, analyzing and optimizing network Performance.

CS 123/L Programming Fundamentals (4) Credits

Course Description:

Concepts and programming techniques fundamentals using JAVA/Python to the practice and theory of Computer Science: I/O, operators and expressions, control structures, functions and arrays. Lab provides students hands on programming using JAVA NETBEANS environment. This allows students to gain hands on experience of developing, testing, debugging and production programming processes. *Prerequisite: MATH 104.*

Course Objectives:

1. Understand and application of the basic fundamentals of programming structure.
2. Understand and application of modules, hierarchy charts, and documentation.
3. Understand and application of making decisions, looping, control breaks, and arrays.
4. Understand and application of designing and writing a complete program.
5. Skills and ability to test and debug programs.

IS 131 COMPUTER AND SECURITY FUNDAMENTALS. (3) Credits

Course Description:

A comprehensive overview of network security concepts that include: remote access, e-mail, the Web, directory and file transfer, wireless data, common network attacks, cryptography, operational/organizational security, disaster recovery, business continuity, and Cyber Ethics. Students are prepared and take the CompTIA Security + Exam

Course Objectives:

1. Differentiate and distinguish between the different network design elements, components, ports and protocols, their respective threats and mitigation techniques.
2. Identify and apply industry best practices for access control methods.
3. Deploy various authentication models and identify the components of each.
4. Conduct periodic audits of system security settings and discuss how to improve analysis by auditing network security procedures and carry out vulnerability assessments using common tools.
5. Use monitoring tools on systems and networks and direct security-related anomalies.
6. Determine the appropriate use of network security tools to facilitate network security.
7. Summarize the various authentication models and identify the components of each.

IS 257 ETHICAL HACKING, COMPUTER AND NETWORK DEFENSE AND COUNTER MEASURES (4) Credits

Course Description:

This course examines the tools, techniques and technologies used in the technical securing of information assets. Students will receive in-depth information about the

software and hardware components of Information Security and Assurance. The students will experience an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council ANSI accredited Certified Ethical Hacker exam 312-50 PREREQUISITE: IS 131

Course Objectives:

1. Describe the goals of and threats to network security and understanding of the background of ethical hacking
2. Explain the Common Vulnerabilities and Exposures (CVE) standard and demonstrate ability of analysis and assessment of cybersecurity
3. Describe router security controls and demonstrate understanding and use of IT tools, systems and programs
4. Describe security solutions for wireless networking and demonstrate understanding of security and how to apply to IT
5. Identify the components of an intrusion detection and prevention system and demonstrate knowledge and application of procedures and methodology
6. Explain basic VPN concepts and demonstrate knowledge and application of regulation, policy and ethics
7. Strengthen network control by managing security events and demonstrate ability to compete in the NCL Cybersecurity Competitions

IS 297 Cyber Security Technician Apprenticeship (18) Credits

Course Description:

(On the Job Training (OJT) apprenticeship component is facilitated by the CNM NMITAP program; however, students have the opportunity of completing this requirement at a variety of locations throughout the state of New Mexico. The one-year apprenticeship follows the National Initiative In Cyber Education (NICE) Framework covering the following Job Functions/Course Objectives:

Job Functions/Course Objectives:

JOB FUNCTION 1: Assist in developing security policies and protocols: assist in enforcing company compliance with network security policies and protocols

JOB FUNCTION 2: Provide technical support to users or customers

JOB FUNCTION 3: Install, configure, test, operate, maintain and manage networks and their firewalls including hardware and software that permit sharing and transition of information.

JOB FUNCTION 4: Installs, configures, troubleshoots and maintains server configurations to ensure their confidentiality, integrity and availability; also manages accounts, firewalls, configuration, patch and vulnerability management. Responsible for access control, security configuration and administration.

JOB FUNCTION 5: Configure tools and technologies to detect, mitigate and

prevent potential threats.

JOB FUNCTION 6: Assess and mitigate system, network, business continuity and related security risks and vulnerabilities

JOB FUNCTION 7: Review network utilization data to identify unusual patterns, suspicious activity or signs of potential threats.

JOB FUNCTION 8: Respond to cyber intrusions, attacks and provide defensive strategies