# NET - NETWORK ENGINEERING

**NET 110 Network Communications**

This course prepares students to have an overall view of the way computers communicate and the basics of networking. Key topics include networking standards, the OSI model, network protocols, transmission media, topologies, hardware, software, WANs and remote connectivity, security, managing and upgrading a network, and TCP/IP.

*Upon successful completion of this course, students should be able to:*
*Describe and implement various network services and standards as related to the Open Systems Interconnection (OSI) model.*
*Demonstrate the ability to properly troubleshoot network connectivity problems.*
*Establish network security and various management practices.*
*Describe and install network connectivity devices and transmission media.*
*Define the topologies and how they work with each other.*
*Perform basic TCP/IP computations and perform troubleshooting utilizing various TCP/IP command line utilities.*
*Describe and implement common network protocols.*
*College Academic Learning Goal Designation: Information Technology (TC)*

Prerequisites: MAT 050 and ((ENG 050 and REA 050) or ENG 099* or REA 075). Successful College Placement Test Scores may be accepted. *(Courses may be taken concurrently.)

**3 Credits3 Weekly Lecture Hours**

**NET 115 Microsoft Windows**

This course is designed to introduce students to setup and manage the current field accepted and supported Microsoft Windows client operating system. Students will gain experience in installing, configuring, and troubleshooting this enterprise level workstation operating system along with gaining the knowledge and foundation related to Microsoft’s current vendor certification exams for this operating system.

*Upon successful completion of this course, students should be able to:*
*Understand the current Windows operating system features and requirements.*
*Perform installations and upgrades of current Windows client operating systems.*
*Configure and manage virtual hard disks.*
*Configure IP addresses and network settings.*
*Configure and manage NTFS permissions to shares, folders, and files.*
*Configure and monitor Windows system performance.*
*Configure User Account Controls and Local Policies.*
*Configure Windows Firewall.*
*Configure Windows backup and recovery options.*
*Configure Windows mobility and remote access controls.*

Prerequisite: NET 110.

**4 Credits3 Weekly Lecture Hours**
**2 Weekly Lab Hours**

**NET 116 Microsoft Hybrid Server: Core Infrastructure**

This course is designed to teach students how to implement the core components of the current Microsoft Server operating system. Students will learn how to enable Windows Server to integrate with Azure Cloud. Students will gain hands-on experience with configuring Active Directory and objects, group policies, file and storage services, DNS, virtualization and containers, and hybrid network connectivity. This course helps prepare students to sit for the Testout Hybrid Server Pro Core certification exam and the Microsoft AZ-800 certification exam.

*Upon successful completion of this course, students should be able to:*
*Plan and install the most recent Microsoft Windows Server operating system.*

*Install and configure the DNS server role.*
*Install and configure Active Directory.*
*Manage IP Addressing.*
*Implement and manage storage and file services.*
*Implement and manage virtualization and containers.*
*Plan and implement Group Policies.*

Prerequisite: NET 110.

**4 Credits4 Weekly Lecture Hours**

**NET 117 Microsoft Server: Networking**

This course is designed for students who plan to support Microsoft Server 2016 and its various domain environment and networking services. Students will learn how to manage and configure DNS and TCP/IP on a Microsoft Server, how to install and configure a DHCP server, how to install and configure the Routing and Remote Access policies and Network Access policies in a Microsoft Server environment, as well as configuring NIC teaming. This course is designed to help students prepare for the current, related, directly maps towards and is a first step in helping students prepare for the Microsoft Server 2016 Networking 70-741 certification exam.

*Upon successful completion of this course, students should be able to:*
*Manage and Configure DNS on a Microsoft Server.*
*Manage and Configure TCP/IP settings and addresses.*
*Install and Configure a Microsoft DHCP Server.*
*Install and Configure Routing and Remote Access on a Microsoft Server.*
*Implement and Manage Network Access Policies on a Microsoft Server.*
*Configure NIC Teaming on a Microsoft Server.*

Prerequisite: NET 110.

**4 Credits4 Weekly Lecture Hours**

**NET 125 Ethical Hacking**

This course is designed to teach students how to identify common cyber and network attacks. Students will utilize current cyber and network administration software utilities in order to perform penetration testing, vulnerability assessments, and analyze network traffic. Students will configure network devices that help to prevent common cyber threats and provide network system and data security. This course is intended to help prepare students for the EC Council's Certified Ethical Hacker Certification exam.

*Upon successful completion of this course, students should be able to:*
*Identify common penetration testing processes and types.*
*Identify current Social Engineering Techniques and Countermeasures.*
*Understand and perform vulnerability assessments.*
*Compare and contrast the various forms of Malware.*
*Analyze network traffic by utilizing current cyber and network administration tools.*
*Configure and manage Intrusion Detection systems.*
*Define and implement Wireless network device security.*
*Define and implement Cloud Security.*
*Define and implement Cryptography.*

Prerequisite: NET 110.

**4 Credits4 Weekly Lecture Hours**

**NET 142 Cyber and Network Security Concepts**

This course gives the student the skills necessary to apply and implement secure network administration procedures and policies. Students will be able to identify common network threats and vulnerabilities, understand networking compliance and operational security, implement application, data and host security, manage access control, and perform stable cryptography implementations. This course is intended to help prepare students for the CompTia Security+ certification exam.

*Upon successful completion of this course, students should be able to:*
*Explain the security function and purpose of network devices and technologies.*
*Apply and implement secure network administration principles.*
*Implement and use common protocols and default network ports.*
*Execute disaster recovery plans and procedures.*
*Analyze and differentiate among types of malware.*
*Analyze and differentiate among types of social engineering, wireless, and application attacks.*
*Analyze and differentiate among types of mitigation and deterrent techniques.*
*Implement assessment tools and techniques to discover security threats and vulnerabilities.*
*Explain the fundamental concepts and best practices related to authentication, authorization and access control.*
*Implement appropriate security controls when performing account management.*
*Use and apply appropriate cryptographic tools and products.*
*Implement Private Key Infrastructure, certificate management and associated components.*

Prerequisite: NET 110.

**4 Credits4 Weekly Lecture Hours**

**NET 200 Digital Forensics**

This course is designed to teach the students the methods of digital computer forensics and investigation. Students will learn how to properly conduct a digital forensics investigation by navigating through each phase of the digital forensics analysis methodology. Computer forensics lab requirements will be introduced along with the practical aspects of identification, seizure, and transportation of gathered evidence. Anti-forensics techniques and how they may negatively affect the forensic investigation process are discussed. The main elements of a digital forensics investigative report are also discussed. Additional topics include acquiring digital evidence, analyzing digital evidence, Windows forensics analysis, web browser and e-mail forensics, and open source intelligence.

*Upon successful completion of this course, students should be able to:*
*Differentiate digital forensics from other cyber security domains.*
*Research the characteristics and components of a physical forensics lab to determine implementation strategies and necessary costs.*
*Implement utilities to capture computer memory images.*
*Identify the nature of Anti-forensics techniques.*
*Explain the main elements of a final digital forensics investigative report.*

Prerequisite: CS 100.

**3 Credits3 Weekly Lecture Hours**

**NET 210 CCNA CISCO Network Support**

In this course, students will learn how to select, configure, and troubleshoot Cisco networking devices. The course will also provide the student with fundamental knowledge of computer networking topics including Internetworking essentials, the OSI Model, and various networking protocols including TCP\IP. This course also helps to prepare students for the current CISCO Routing and Switching certification exams.

*Upon successful completion of this course, students should be able to:*
*Explain the OSI Model and the concept of Layered Communications.*
*Analyze the fundamentals of bridging, switching, and wireless networks.*
*Analyze the fundamentals of security prevention and detection.*
*Describe Cisco network basics and the Cisco IOS.*
*Identify features and characteristics of various WAN protocols.*
*Apply commonly used Cisco automation tools.*
*Perform basic configuration tasks of Cisco routers and switches.*

Prerequisite: NET 110.

**6 Credits6 Weekly Lecture Hours**

**NET 230 Linux Operating Systems I**

This course is designed to provide students the needed information and abilities to understand and support popular Linux operating systems. Major concepts included are Linux operating system installation, user and group management, Linux file systems and file system security, network connectivity, process and task management, and Linux software and package management. Additionally, this course directly relates to, and helps students prepare for, the current CompTIA Linux + certification exam.

*Upon successful completion of this course, students should be able to:*
*Understand components of current Linux operating systems.*
*Implement a logical, organized, and secure file system.*
*Implement Linux console commands, services, and processes.*
*Perform Linux operating system installation.*
*Configure Linux operating system and software package updates.*

Prerequisite: NET 110.

**4 Credits4 Weekly Lecture Hours**

**NET 231 Microsoft Hybrid Server II**

This course is designed to teach students how to implement the advanced components of the current Microsoft Server operating system. Students will learn how to further enable Windows Server to integrate with Azure Cloud. Students will gain hands-on experience with installing and configuring advanced Windows Server on-premises and hybrid infrastructures, managing failover clusters, performing server backups and recovery, migrating servers to Azure, and troubleshooting hybrid networking connectivity and virtual machines. This course helps prepare students to sit for the Testout Hybrid Server Pro Advanced certificate exam and the Microsoft AZ-801 certification exam.

*Upon successful completion of this course, students should be able to:*
*Implement secure Windows Server on-premises and hybrid infrastructures.*
*Implement and manage Windows Server high availability.*
*Implement disaster recovery.*
*Migrate servers and workloads.*
*Monitor and troubleshoot Windows Server environments.*

Prerequisite: NET 115.

**4 Credits4 Weekly Lecture Hours**

**NET 236 Cyber Security Defense and Analysis**

This course provides students with the advanced knowledge and skills to apply behavioral analytics to networks and devices in order to prevent, detect, and combat cybersecurity threats through continuous security monitoring. Major topics students will learn are threat and vulnerability management, software and systems security, cybersecurity compliance and assessment, cybersecurity operations and monitoring, and incident response. Additionally, this course helps prepare students for the current CompTIA Cybersecurity Analyst (CySA+) certification exam.

*Upon successful completion of this course, students should be able to:*
*Apply proactive threat detection techniques.*
*Identify network vulnerabilities.*
*Explain software and hardware assurance best practices.*
*Apply security concepts in support of organizational risk mitigation.*
*Analyze and interpret network traffic and data.*
*Understand advanced electronic messaging concepts.*
*Understand advanced network security concepts.*
*Implement network configuration policies, procedures, and controls to improve security.*
*Apply appropriate incident response procedures.*

Prerequisite: NET 142.

**4 Credits4 Weekly Lecture Hours**