Network Security 2023-2024 Catal

[ARCHIVED CATALOG]

NETI 210 - Network Security

PREREQUISITES/COREQUISITE: NETI 119 Networking II

PROGRAM: Network Infrastructure
CREDIT HOURS MIN: 3
LECTURE HOURS MIN: 1.5
LAB HOURS MIN: 3
TOTAL CONTACT HOURS MIN: 4.5
DATE OF LAST REVISION: Fall 2022

CATALOG DESCRIPTION:

Network Security. This course provides an introduction to the core security concepts and skills needed for the installation, troubleshooting, and monitoring of network devices to maintain the integrity, confidentiality, and availability of data and devices. This course will provide associate-level knowledge and skills required to secure networks. With this Network Security course, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. This course helps students develop the skills needed for entry-level network security career opportunities.

MAJOR COURSE LEARNING OBJECTIVES: MAJOR COURSE LEARNING OBJECTIVE: Upon successful completion of this course the student will be expected to:

- Explain the various types of threats and attacks
- Explain the tools and procedures to mitigate the effects of malware and common network attacks
- Configure command authorization using privilege levels and role-based CLI
- Implement the secure management and monitoring of network devices
- Configure AAA to secure a network
- Implement ACLs to filter traffic and mitigate network attacks on a network
- Implement Zone-Based Policy Firewall using the CLI
- Explain how network-based Intrusion Prevention Systems are used to help secure a network
- Explain endpoint vulnerabilities and protection methods
- Implement security measures to mitigate Layer 2 attacks
- Explain how the types of encryption, hashes, and digital signatures work together to provide
- confidentiality, integrity, and authentication
- Explain how a public key infrastructure is used to ensure data confidentiality and provide authentication
- Configure a site-to-site IPsec VPN, with pre-shared key authentication, using the CLI
- Explain how the Next-Generation Firewalls (NGFWs) act as advanced stateful firewall
- Implement NGFW firewall configuration using a Cisco ASA or similar device
- Test network security

COURSE CONTENT: Topical areas of study include -

COURSE CONTENT: Topical areas of study include -

Network Security Concepts

Network Threats

Mitigation Technologies

Assigning Administrative Roles

Device Monitoring and Management

AAA

Access Control Lists

Firewall Technologies

Zone-Based Policy Firewalls

IDS/IPS Operation and Implementation

Endpoint Security

Layer 2 Security Considerations

Cryptographic Services

Basic Integrity and Authenticity

Public Key Cryptography

VPN Concepts

Implementing Site-to-Site VPNs

Network Security Testing