



# Network Defense and Security

**Commitment:**  
**4 weeks of study**  
**10-20 hours/week**



## Network Security Principles

Learn the fundamentals of network security, focusing on defense-in-depth strategies. This includes understanding how multiple layers of security measures protect networks, providing a solid base for advanced topics.



## Access Control and Policies

Explore techniques for controlling and monitoring network access. Develop skills in implementing security policies, crucial for managing and defending a network. Emphasis is on practical applications and policy development.



## Endpoint Protection and Recovery

Understand the importance of securing network endpoints and effective disaster recovery planning. This includes cryptography's role in secure communications and essential practices in security administration.

## About the Course

In this course, you'll immerse yourself in the world of network defense and security, understanding the comprehensive strategies required to protect modern networks. We begin with the principles of network security, focusing on defense-in-depth strategies that layer multiple security measures for robust protection. This foundational knowledge is crucial in today's increasingly complex cybersecurity landscape.

Next, we explore the practical aspects of controlling and monitoring access to networks. You'll learn about the development and implementation of effective security policies, understanding their critical role in network defense. This includes hands-on experience with tools and techniques for safeguarding network access points.

The course culminates with a focus on endpoint protection and the importance of physical security measures. You'll delve into the role of cryptography in securing network communications and the key practices of security administration. The course also covers disaster recovery planning, ensuring you're prepared to respond effectively to security breaches and maintain operational continuity.

## At the end, you will be able to

1. Apply defense-in-depth strategies for comprehensive network security.
2. Develop and implement effective network security policies and access controls.
3. Protect network endpoints and understand the role of physical security measures.
4. Use cryptography for secure communications and master disaster recovery planning techniques.

## WEEK 1

# Network Security Foundations

This week, you'll dive into network security principles. We'll explore defense-in-depth strategies, understanding how multiple layers of security can protect a network.

You'll learn about the various threats that networks face and the importance of a comprehensive security approach. This foundational knowledge is crucial for building a robust defense against cyber threats.

---

## WEEK 2

# Access Control and Policy Implementation

Focus on techniques for controlling and monitoring access to networks. You'll learn about developing and implementing security policies, which are essential for effective network defense.

This week emphasizes practical skills in managing network access and safeguarding data.

---

## WEEK 3

# Endpoint Security and Physical Measures

Learn about the importance of securing network endpoints and implementing physical security measures. We'll cover strategies for protecting individual devices that access the network, a key

aspect of overall network security.

Understanding these concepts is vital for defending against attacks that target network endpoints.

---

## WEEK 4

# Cryptography, Security Administration and Exam

Delve into the role of cryptography in securing network communications. You'll also learn about security administration practices and the importance of disaster recovery planning.

This week is about consolidating your understanding and preparing you for the Nucamp CyDefSec exam, ensuring you're equipped with comprehensive network security knowledge.