Network Defense

Course Overview

This course covers different methods to monitor the network and how to evaluate security alerts. It delves into tools and techniques used to protect the network, including access control, firewalls, cloud security, and cryptography.

Benefits

The demand for security professionals continues to grow. Gain the intermediate knowledge used in the workplace as a Cybersecurity Technician.

- ✓ Builds a cybersecurity foundation
- ✓ Explores the many career possibilities in cybersecurity
- ✓ Develops skills to create a layered defense-in-depth cybersecurity strategy

Course Details

Target Audience: Secondary and 2-year college vocational students; Reskilling to find a job in cyber

Estimated Time to Completion: 27 hours

Recommended Preparation: Introduction to Cybersecurity and Endpoint Security

Course Delivery: Instructor-led or Self-paced

Learning Component Highlights:

- ✓ 11 modules
- ✓ 29 Labs and Cisco Packet Tracer activities
- ✓ 58 + interactive activities & quizzes
- ✓ 1 final exam

Course Recognitions: Digital badge

Certification Alignment: CCST Cybersecurity

Recommended Next Course: Cyber Threat Management

Requirements

- ASC Alignment: Recommended
- Instructor Training: Optional
- Physical Equipment: Not required

Network Defense

Scope and Sequence

Version 1.0

Contents

Target Audience

The Network Defense course is appropriate for learners with a high school reading proficiency, basic computer literacy, and interested in pursuing an entry-level job in the field of cybersecurity.

Prerequisites

There are no prerequisites for this course, although learners should have the following basic skills:

- Basic PC operating system navigation skills
- Knowledge of TCP/IP networking including network protocols, services, and processes

While not required, it is recommended that learners complete the following courses within the cybersecurity learning path:

- Introduction to Cybersecurity
- Network Essentials
- Endpoint Security

Certification Alignment

This course, from the Junior Cybersecurity Analyst Career Path, aligns with the CCST Cybersecurity Certification (formerly known as IT Specialist Cybersecurity certification from Certiport).

Course Description

Network Defense has many features to help learners understand network defense concepts. The course design includes:

- Eleven modules comprised of key topics.
- Modules emphasize critical thinking, problem solving, collaboration, and the practical application of skills.
- Each module contains practice and assessment activities such as a Check Your Understanding activity, a lab, or an activity using our network simulation tool, Cisco® Packet Tracer.
- Topic-level activities are designed to indicate a learner's mastery of course skills, enabling learners to gage understanding before taking a graded quiz or exam.
- Language describing concepts is designed to be easily understood by learners at a high school level.
- Assessments and practice activities focus on specific competencies are designed to increase retention and provide flexibility in the learning path.
- Multimedia learning tools, including videos and quizzes, address a variety of learning styles, stimulate learning, and promote knowledge retention.
- Labs and Packet Tracer simulation-based activities help learners develop critical thinking and complex problem-solving skills.
- Innovative assessments provide immediate feedback to support the evaluation of knowledge and skills.
- Technical concepts are explained using introductory-level language.

- Embedded interactive activities break-up reading of large content blocks and reinforce understanding.
- The course emphasizes applied skills and hands-on experiences, while encouraging learners to consider additional Information Technology (IT) education.

Course Objectives

Network Defense introduces important foundational concepts in cybersecurity such as system and network defense, access control, firewalls, cloud security, applications of cryptography, network security data, and evaluating security alerts. By the end of the course, learners can implement defensive measures and access control, configure a simulated firewall, use different types of network data, and evaluate security alerts.

The course material will assist you in developing learner skills, including:

- Explain approaches to network security defense
- Implement some of the various aspects of system and network defense
- Configure local and server-based access control
- Implement access control lists (ACLs) to filter traffic and mitigate network attacks
- Understand how firewalls are implemented to provide network security
- Implement Zone-Based Policy Firewall using the CLI
- Recommend cloud security requirements based on a given cloud scenario
- Determine the cryptographic techniques that are required to ensure confidentiality, integrity, and authenticity
- Explain how security technologies affect security monitoring
- Use different types of logs and records to store information regarding hosts and the network
- Explain the process of evaluating alerts

Equipment Requirements

Network Defense hands-on labs require equipment found in most home networks. Any lab that requires a more complex networking environment uses Packet Tracer, the network simulation tool.

Software

- Oracle Virtual Box
- Lab virtual machine OVA files
- Packet Tracer 8.0.1 or higher

Optional Lab Equipment

- Microsoft Windows host

Course Outline

Table 1 below details the modules and their associated competencies. Each module is an integrated unit of learning that consists of content, activities, and assessments that target a specific set of competencies. The size of the module depends on the depth of knowledge and skill needed to master the competency.

Table 1: Module Title and Objective

Module Title / Topic Title	Objective
Module 1: Understanding Defense	
1.0 Understanding Defense	Explain approaches to network security defense.
1.1 Defense-in-Depth	Explain how the defense-in-depth strategy is used to protect networks.
1.2 Cybersecurity Operations Management	Explain how an organization monitors cybersecurity threats.
1.3 Security Policies, Regulations, and Standards	Explain security policies, regulations, and standards.
Module 2: System and Network Defense	
2.0 System and Network Defense	Implement some of the various aspects of system and network defense.
2.1 Physical Security	Explain how physical security measures are implemented to protect network equipment.
2.2 Application Security	Explain how to apply application security measures.
2.3 Network Hardening: Services and Protocols	Explain how to harden network services and protocols.
2.4 Network Hardening: Segmentation	Explain how network segmentation can help you harden the network.
2.5 Hardening Wireless and Mobile Devices	Configure wireless router hardening and security.
2.6 Cybersecurity Resilience	Explain physical security with IoT devices.
2.7 Embedded and Specialized Systems	Implement physical security with IoT devices.
Module 3: Access Control	
3.0 Access Control	Configure local and server-based access control.
3.1 Access Controls	Configure secure access on a host.
3.2 Access Control Concepts	Explain how access control protects network data.
3.3 Account Management	Explain the need for account management and access control strategies.

Module 4: Access Control Lists	
4.1 Introduction to Access Control Lists	Describe standard and extended IPv4 ACLs.
4.2 Wildcard Masking	Explain how ACLs use wildcard masks.
4.3 Configure ACLs	Explain how to configure ACLs.
4.4 Named Standard IPv4 ACL Syntax	Use sequence numbers to edit existing standard IPv4 ACLs.
4.5 Implement ACLs	Implement ACLs.
4.6 Mitigate Attacks with ACLs	Use ACLs to mitigate common network attacks.
4.7 IPv6 ACLs	Configure IPv6 ACLs using the CLI.
4.1 Introduction to Access Control Lists	Describe standard and extended IPv4 ACLs.
Module 5: Firewall Technologies	
5.0 Firewall Technologies	Explain how firewalls are implemented to provide network security.
5.1 Secure Networks with Firewalls	Explain how firewalls are used to help secure networks.
5.2 Firewalls in Network Design	Explain design considerations for implementing firewall technologies.
Module 6: Zone-Based Policy Firewalls	
6.0 Zone-Based Policy Firewalls	Implement Zone-Based Policy Firewall using the CLI.
6.1 ZPF Overview	Explain how Zone-Based Policy Firewalls are used to help secure a network.
6.2 ZPF Operation	Explain the operation of a Zone-Based Policy Firewall.
Module 7: Cloud Security	
7.0 Cloud Security	Recommend cloud security requirements based on a given cloud scenario.
7.1 Virtualization and Cloud Computing	Describe ways to manage threats to the private and public cloud.
7.2 The Domains of Cloud Security	Explain the domains of cloud security.
7.3 Cloud Infrastructure Security	Explain mitigation of threats to the cloud platform infrastructure.
7.4 Cloud Application Security	Recommend cloud security applications.
7.5 Cloud Data Security	Explain how to secure cloud data.
7.6 Protecting VMs	Explain how to secure VM instances.

Module 8: Cryptography	
8.0 Cryptography	Determine the cryptographic techniques that are required to ensure confidentiality, integrity, and authenticity.
8.1 Confidentiality	Determine the encryption algorithm to use according to requirements.
8.2 Obscuring Data	Use a technique to obscure data.
8.3 Integrity and Authenticity	Explain the role of cryptography in ensuring the integrity and authenticity of data.
8.4 Hashing	Explain how to use hashing tools.
8.5 Public Key Cryptography	Use a digital signature.
8.6 Authorities and the PKI Trust System	Use hashing to detect network interception.
8.7 Applications and Impacts of Cryptography	Explain how the use of cryptography affects cybersecurity operations.
Module 9: Technologies and Protocols	
9.0 Technologies and Protocols	Explain how security technologies affect security monitoring.
9.1 Monitoring Common Protocols	Explain the behavior of common network protocols in the context of security monitoring.
9.2 Security Technologies	Explain how security technologies affect the ability to monitor common network protocols.
Module 10: Network Security Data	
10.0 Network Security Data	Use different types of logs and records to store information regarding hosts and the network.
10.1 Types of Security Data	Describe the types of data used in security monitoring.
10.2 End Device Logs	Describe the elements of an end device log file.
10.3 Network Logs	Use different types of services to gather network data.
Module 11: Evaluating Alerts	
11.0 Evaluating Alerts	Explain the process of evaluating alerts.
11.1 Source of Alerts	Identify the structure of alerts.
11.2 Overview of Alert Evaluation	Explain how alerts are classified.