Network Defense Essentials

Course Duration: 16 Hrs. **Course code: N|DE (112-51)**

Course Overview

The Network Defense Essentials (N|DE) course provides foundational knowledge in network security, equipping learners with skills to protect IT infrastructures from cyber threats, including network security fundamentals, authentication, access control, firewalls, and more.

What you'll learn?

In a Network Defense Essentials course, you'll learn fundamental cybersecurity concepts, network security protocols, identification/authentication/authorization, and how to defend against common threats, including wireless security, virtualization, cloud computing, and data security.

Target Audience

- Cybersecurity students seeking practical training.
- Network engineers aiming to enhance defense tactics.
- Cybersecurity consultants requiring knowledge update.

Pre-Requisites

- Basic Networking Knowledge
- Understanding of Operating Systems
- Cybersecurity Fundamentals
- Experience with Command-Line Interfaces (CLI)
- Familiarity with Network Security Tools

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Course content

Module 01: Network Security Fundamentals

A. Fundamentals of Network Security
B. Network Security Protocols

Module 02: Identification, Authentication and Authorization

A. Access Control Principles, Terminologies, and Models
B. Identity and Access Management (IAM) Concepts

Module 03: Network Security Controls - Administrative Controls

A. Regulatory Frameworks, Laws, and Acts
B. Design and Develop Security Policies
C. Conduct Different Types of Security and Awareness Training

Module 04: Network Security Controls - Physical Controls

A. Importance of Physical Security
B. Physical Security Controls
C. Workplace Security
D. Environmental Controls

Module 05: Network Security Controls - Technical Controls

A. Types of Network Segmentation
B. Types of Firewalls and their Role
C. Types of IDS/IPS and their Role
D. Types of Honeypots
E. Types of Proxy Servers and their Benefits
F. Fundamentals of VPN and its Importance in Network Security
G. Security Incident and Event Management (SIEM)
H. User Behavior Analytics (UBA)
I. Antivirus/Anti-Malware Software

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Module 06: Virtualization and Cloud Computing

A. Virtualization Essential Concepts and OS
B. Virtualization Security
C. Cloud Computing Fundamentals
D. Insights of Cloud Security and Best Practices

Module 07: Wireless Network Security

A. Wireless Network Fundamentals
B. Wireless Network Encryption Mechanisms
C. Types of Wireless Network Authentication Methods
D. Implement Wireless Network Security Measures

Module 08: Mobile Device Security

A. Mobile Device Connection Methods
B. Mobile Device Management Concepts
C. Common Mobile Usage Policies in Enterprises
D. Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies
E. Implement Enterprise-level Mobile Security Management Solutions
F. Implement General Security Guidelines and Best Practices on Mobile Platforms

Module 09: IoT Device Security

A. IoT Devices, Application Areas, and Communication Models
B. Security in IoT-enabled Environments

Module 10: Cryptography and PKI

A. Cryptographic Techniques
B. Cryptographic Algorithms
C. Cryptography Tools
D. Public Key Infrastructure (PKI)

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Module 11: Data Security

A. Data Security and its Importance
B. Security Controls for Data Encryption 8
C. Data Backup and Retention
D. Data Loss Prevention Concepts

Module 12: Network Traffic Monitoring

A. Need and Advantages of Network Traffic Monitoring
B. Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic
C. Perform Network Monitoring for Suspicious Traffic

Exam Preference

Exam Code	112-51
Number Of Questions	75
Length Of Test	120 Minutes
Passing Score	70%