NDE – Network Defense Essentials (e-Learning)

EC-Council

Com certificação

- **Nível:**
- **Duração:** 14h

Sobre o curso

Spring Deals: Cursos EC-Council com 5% de desconto até 30 de abril

The **Network Defense Essentials (NDE)** covers the fundamental concepts of information security and network defense, providing a holistic overview of identification, authentication, authorization, visualization, and more. No IT/Cybersecurity experience required for this course.

Test your skills with CTF-based Capstone Project and validate these newly acquired skills in proctored exams. With 12 modules, 14+ hours of premium self-paced video training, and 11 interactive labs, the series enables you to add formal recognition to your resume, demonstrating your skills and expertise to employers.

Key Features:

- 14+ hours of premium self-paced video training
- 11 hands-on lab activities in a simulated lab environment
- 750+ pages of e-courseware
- Capstone project
- 1-year access to courseware and 6-month access to labs
- Proctored exam voucher with 1-year validity
- Globally recognized EC-Council certification
- Increased value in the job market to advance your career

What skills you'll learn:

- Key issues plaguing network security.
- Essential network security protocols.
- Identification, authentication, and authorization concepts.
- Network security controls:
    - Administrative controls (frameworks, laws, acts, and security policies).
    - Physical controls (physical security controls, workplace security, and environmental controls).
    - Technical controls (network segmentation, firewall, IDS/IPS, honeypot, proxy server, VPN, SIEM, UBA, and anti-malware).
- Fundamentals of virtualization, cloud computing, and cloud security.

- Wireless network fundamentals, wireless encryption, and security measures.
- Fundamentals of mobile and IoT devices and their security measures.
- Cryptography and PKI concepts.
- Data security, data encryption, and data backup and data loss prevention techniques.
- Network traffic monitoring for suspicious traffic.

Destinatários

Who is NDE for?

- High School/ College/University students
- Teams and organizations
- Career starters
- Working professionals

Pré-requisitos

No prior cybersecurity knowledge or IT work experience required.

Metodologia

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.

Exam Details:

- Exam Code: 112-51
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice

Programa

- Network Security Fundamentals
- Identification, Authentication and Authorization
- Network Security Controls – Administrative Controls
- Network Security Controls – Physical Controls
- Network Security Controls – Technical Controls
- Virtualization and Cloud Computing
- Wireless Network Security
- Mobile Device Security
- IoT Device Security

- Cryptography and PKI
- Data Security
- Network Traffic Monitoring

Network Security Fundamentals

- Fundamentals of Network Security
- Network Security Protocols

Identification, Authentication and Authorization

- Access Control Principles, Terminologies, and Models
- Identity and Access Management (IAM) Concepts

Lab Exercise:

- Implementing Access Controls in Windows Machine
- Managing Access Controls in Linux Machine
- Implementing Role-Based Access Control in Windows Admin Center (WAC)

Network Security Controls – Administrative Controls

- Regulatory Frameworks, Laws, and Acts
- Design and Develop Security Policies
- Conduct Different Types of Security and Awareness Training

Lab Exercise:

- Implementing Password Policies Using Windows Group Policy

Network Security Controls – Physical Controls

- Importance of Physical Security
- Physical Security Controls
- Workplace Security
- Environmental Controls

Network Security Controls – Technical Controls

- Types of Network Segmentation
- Types of Firewalls and their Role
- Types of IDS/IPS and their Role
- Types of Honeypots
- Types of Proxy Servers and their Benefits
- Fundamentals of VPN and its importance in Network Security
- Security Incident and Event Management (SIEM)
- User Behavior Analytics (UBA)
- Antivirus/Anti-malware Software

Lab Exercise:

- Implementing Host-Based Firewall Protection with iptables
- Implementing Host-Based Firewall Functionality Using Windows Firewall
- Implementing Network-Based Firewall Functionality: Blocking Unwanted Website access using pfSense Firewall
- Implementing Network-Based Firewall Functionality: Blocking Insecure Ports using pfSense Firewall
- Implementing Host-Based IDS functionality using Wazuh HIDS
- Implementing Network-based IDS Functionality Using Suricata IDS
- Detect Malicious Network Traffic using HoneyBOT
- Establishing Virtual Private Network Connection using SoftEther VPN

Virtualization and Cloud Computing

- Virtualization Essential Concepts and OS
- Virtualization Security
- Cloud Computing Fundamentals
- Insights of Cloud Security and Best Practices

Lab Exercise:

- Auditing Docker Host Security Using Docker-Bench-Security Tool
- Implementing AWS Identity and Access Management
- Securing Amazon Web Services Storage

Wireless Network Security

- Wireless Network Fundamentals
- Wireless Network Encryption Mechanisms
- Types of Wireless Network Authentication Methods
- Implement Wireless Network Security Measures

Lab Exercise:

- Configuring Security on a Wireless Router

Mobile Device Security

- Mobile Device Connection Methods
- Mobile Device Management Concepts
- Common Mobile Usage Policies in Enterprises
- Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies
- Implement Enterprise-level Mobile Security Management Solutions
- Implement General Security Guidelines and Best Practices on Mobile Platforms

Lab Exercise:

- Implementing Enterprise Mobile Security Using Miradore MDM Solution

IoT Device Security

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

Lab Exercise:

- Securing IoT Device Communication Using TLS/SSL

Cryptography and PKI

- Cryptographic Techniques
- Cryptographic Algorithms
- Cryptography Tools
- Public Key Infrastructure (PKI)

Lab Exercise:

- Calculate One-way Hashes using HashCalc
- Calculate MD5 Hashes using HashMyFiles
- Create a Self-signed Certificate

Data Security

- Data Security and its Importance
- Security Controls for Data Encryption
- Data Backup and Retention
- Data Loss Prevention Concepts

Lab Exercise:

- Perform Disk Encryption using VeraCrypt
- File Recovery Using EaseUS Data Recovery Wizard
- Backing Up and Restoring Data in Windows

Network Traffic Monitoring

- Need and Advantages of Network Traffic Monitoring
- Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic
- Perform Network Monitoring for Suspicious Traffic

Lab Exercise:

- Capturing Network Traffic using Wireshark
- Applying Various Filters in Wireshark
- Analyzing and Examining Various Network Packet Headers in Linux using tcpdump