BLACKBIRD FOR TRAINING

Certified Network Defender (CND)

Certified Network Defender (CND)

Introduction

Welcome to the Certified Network Defender CND training course! This comprehensive program is designed to equip network administrators with the knowledge and skills necessary to protect their networks from modern cyber threats. Participants will gain a deep understanding of network security concepts, including protection, detection, and response techniques against network attacks.

Through a combination of theoretical knowledge and hands-on practice, this course covers network defense fundamentals, secure protocol configuration, firewall and VPN management, traffic monitoring, and incident response strategies. By the end of the course, participants will be fully prepared to design, implement, and manage robust network security policies and achieve the Certified Network Defender CND certification.

Course Objectives

By the end of this course, participants will:

- Understand the core concepts and techniques of network defense.
- Implement and manage secure network protocols, firewalls, IDS/IPS, and VPNs.
- Gain hands-on experience in monitoring and analyzing network traffic to detect threats.
- Learn to conduct incident response and forensic investigations.
- Develop comprehensive network security policies and strategies.
- Prepare for the Certified Network Defender CND certification exam.

Course Outlines

Day 1: Introduction to Network Security

- Fundamentals of Network Security: Importance, types of threats, and challenges.
- Network Defense Essentials:
  - Defense-in-depth strategies.
  - Layered security architecture.
- Security Threats and Vulnerabilities:
  - Common vulnerabilities and attack vectors.
  - Risk assessment and management.
- Network Security Controls:
  - Physical, technical, and administrative controls.
- Introduction to Network Security Tools: Overview of tools and defense technologies.

Day 2: Secure Network Protocols and Configuration

- Secure Network Protocols:
  - Fundamentals of TCP/IP security.
  - Encryption protocols SSL/TLS, SSH.
  - VPN configurations and technologies.
- Firewall Management:
  - Types of firewalls and their architecture.
  - Configuring firewall rules and policies.
- Intrusion Detection/Prevention Systems IDS/IPS:
  - Deployment and configuration.
  - Managing IDS/IPS for proactive security.
- Network Segmentation and Secure Design:
  - Isolating and securing network zones.

Day 3: Network Traffic Monitoring and Analysis

- Traffic Monitoring Essentials:
  - Importance and tools for network traffic monitoring.
- Packet Analysis:
  - Capturing and analyzing packets to detect anomalies.
- Log Management:
  - Collecting and analyzing logs for threat detection.
- Network Performance Monitoring:
  - Identifying bottlenecks and maintaining efficiency.
- Anomaly Detection:
  - Identifying deviations from normal activity.

Day 4: Incident Response and Forensics

- Incident Response Fundamentals:
  - Life cycle of incident response.
  - Roles and responsibilities in incident handling.
- Detection and Analysis:
  - Analyzing incidents to determine root causes.
- Incident Containment and Recovery:
  - Strategies to contain and eradicate threats.
  - Best practices for recovery and restoration.
- Digital Forensics:
  - Evidence collection, preservation, and analysis.
- Incident Response Planning:
  - Developing response plans and conducting drills.

Day 5: Security Policies and Risk Management

- Network Security Policy Development:
  - Creating and enforcing comprehensive security policies.
- Risk Management:
  - Conducting risk assessments and implementing mitigation strategies.
- Business Continuity and Disaster Recovery:
  - Planning for resilience and quick recovery from disruptions.
- Security Awareness and Training:
  - Educating teams on best practices in network security.
- Continuous Improvement:
  - Monitoring, updating, and improving security measures.

Why Attend this Course: Wins & Losses!

- Advanced Skills: Master the latest tools and techniques for network defense.
- Practical Knowledge: Gain hands-on experience in managing secure networks.
- Industry Recognition: Prepare for the Certified Network Defender CND certification.
- Preparedness: Learn to proactively protect against and respond to cyber threats.

Conclusion

The Certified Network Defender CND course provides the essential skills and knowledge required to secure networks in today's cyber landscape. With a focus on both theoretical and practical training, this program ensures participants are well-prepared to defend against threats and maintain robust network security.

Join us to gain an in-depth understanding of network defense techniques, prepare for the CND certification, and advance your career as a network security professional.