



EC-Council Certified Network Defender (C|ND) v3 Course Outline



ERIC REED

CYBERSECURITY TRAINING

PASS ON THE FIRST ATTEMPT!™

COMPANY OVERVIEW

For over 25 years, Eric Reed Cybersecurity Training has been a trusted leader in cybersecurity education, equipping more than 60,000 professionals with the skills needed to defend against emerging cyber threats. Our mission is to empower individuals and organizations with comprehensive, hands-on training that translates directly to real-world success. Recognized with multiple industry awards—including an unprecedented 10-time EC Council Instructor of the Year and 7-time Circle of Excellence honoree—we combine innovative delivery methods with a passion for excellence to ensure our students achieve certification success on the first attempt

EC-COUNCIL C|ND

The Certified Network Defender (C|ND) certification focuses on network security and proactive defense strategies to protect organizations against cyber threats.

ONLINE LIVE
LEARNING

ON-DEMAND
LIVE LEARNING

ONLINE LIVE & ON-DEMAND LIVE

All the benefits of live, instructor-led training with the convenience of on-demand.

- **Online Live:** Attend our scheduled sessions in real time (Monday–Friday). Get immediate interaction with the instructor and fellow students.
- **On-Demand Live:** Access recordings of the most recent live sessions on your own schedule, while still having direct instructor support.
- **Flexible Scheduling:** Choose a structured approach—one-week bootcamp (M–F), two nights a week for five weeks, or every Saturday for five weeks. Need more wiggle room? Adjust any schedule to fit your lifestyle!

COURSE OBJECTIVES

- Implement secure network architecture and design principles.
- Detect and respond to network security threats and attacks.
- Configure and manage network security tools.
- Apply best practices in network monitoring and traffic analysis.
- Implement security policies and incident response plans.

SALARY RANGE

C|ND → \$75,000 - \$110,000

These figures are approximate and depend on location, experience, and job role. Higher salaries are usually seen in major tech hubs and with significant experience.

JOB ROLES

- **Network Security Analyst**



“It’s was a great class that covered all aspects of security. Most importantly, I appreciate the fact that you are giving up your own time to assist us and maintain a sharedrive with the latest security tools and informative papers even after the class is over. I was able to pass the test after one week of attending the training.”

-Shadi Ehalabi

Contact Us

- (707) 722-7333
- info@ericreedlive.com
- 1401 61st St S
Gulfport, FL 33707



EC-COUNCIL C|ND OVERVIEW

1 - Network Attacks and Defense Strategies

Explain essential terminologies related to network security attacks

Describe the various examples of network-level attack techniques

Describe the various examples of application-level attack techniques

Describe the various examples of social engineering attack technique

Describe the various examples of email attack techniques

Describe the various examples of mobile device-specific attack techniques

Describe the various examples of cloud-specific attack techniques

Describe the various examples of wireless network-specific attack techniques

Describe Attacker's Hacking Methodologies and Frameworks

Understand fundamental goal, benefits, and challenges in network defense

Explain Continual/Adaptive security strategy

Explain defense-in-depth security strategy



2 - Administrative Network Security

Learn to obtain compliance with regulatory framework and standards

Discuss various Regulatory Frameworks, Laws, and Acts

Learn to design and develop security policies

Learn to conduct different type security and awareness training

Learn to implement other administrative security measures



3 - Technical Network Security

Discuss access control principles, terminologies, and models

Redefine the Access Control in Today's Distributed and Mobile Computing World

Discuss Identity and Access Management (IAM)

Discuss cryptographic security techniques

Discuss various cryptographic algorithms

Discuss security benefits of network segmentation techniques

Discuss various essential network security solutions

Discuss various essential network security protocols



4 - Network Perimeter Security

Understand firewall security concerns, capabilities, and limitations

Understand different types of firewall technologies and their usage

Understand firewall topologies and their usage

Distinguish between hardware, software, host, network, internal, and external firewalls

Select firewalls based on its deep traffic inspection capability

Discuss firewall implementation and deployment process

Discuss recommendations and best practices for secure firewall Implementation and deployment

Discuss firewall administration concepts

Understand role, capabilities, limitations, and concerns in IDS deployment

Discuss IDS classification

Discuss various components of ID

Discuss effective deployment of network and host-based IDS

Learn to how to deal with false positive and false negative IDS/IPS alerts

Discuss the considerations for selection of an appropriate IDS/IPS solutions

Discuss various NIDS and HIDS Solutions with their intrusion detection capabilities

Snort

Discuss router and switch security measures, recommendations, and best practices

Leverage Zero Trust Model Security using Software-Defined Perimeter (SDP)



5 - Endpoint Security-Windows Systems

Understand Window OS and Security Concerns

Discuss Windows Security Components

Discuss Various Windows Security Features

Discuss Windows Security Baseline Configurations

Discuss Windows User Account and Password Management

Discuss Windows Patch Management

Discuss User Access Management

Windows OS Security Hardening Techniques

Discuss Windows Active Directory Security Best Practices

Discuss Windows Network Services and Protocol Security



6 - Endpoint Security-Linux Systems

Understand Linux OS and security concerns

Discuss Linux Installation and Patching

Discuss Linux OS Hardening Techniques

Discuss Linux User Access and Password Management

Discuss Linux Network Security and Remote Access

Discuss Various Linux Security Tools and Frameworks



7 - Endpoint Security- Mobile Devices

Common Mobile Usage Policies in Enterprises

Discuss Security Risk and Guidelines associated with Enterprises mobile usage policies

Discuss and implement various enterprise-level mobile security management Solutions

Discuss and implement general security guidelines and best practices on Mobile platforms

Discuss Security guidelines and tools for Android devices

Discuss Security guidelines and tools for iOS device



8 - Endpoint Security-IoT Devices

Understanding IoT Devices, their need and Application Areas

Understanding IoT Ecosystem and Communication models

Understand Security Challenges and risks associated with IoT-enabled environments

Discuss the security in IoT-enabled environments

Discuss Security Measures for IoT enabled IT Environments

Discuss IoT Security Tools and Best Practices

Discuss and refer various standards, Initiatives and Efforts for IoT Security



9 - Administrative Application Security

Discuss and implement Application Whitelisting and Blacklisting

Discuss and implement application Sandboxing

Discuss and implement Application Patch Management

Discuss and implement Web Application Firewall (WAF)



10 - Data Security

Understand data security and its importance

Discuss the implementation of data access controls

Discuss the implementation of Encryption of Data at rest

Discuss the implementation of Encryption of “Data at transit”

Discuss Data Masking Concepts

Discuss data backup and retention

Discuss Data Destruction Concepts

Data Loss Prevention Concepts



11 - Enterprise Virtual Network Security

Discuss the evolution of network and security management concept in modern Virtualized IT Environments

Understand Virtualization Essential Concepts

Discuss Network Virtualization (NV) Security

Discuss SDN Security

Discuss Network Function Virtualization (NFV) Security

Discuss OS Virtualization Security

Discuss Security Guidelines, Recommendations and Best Practices for Containers

Discuss Security Guidelines, Recommendations and Best practices for Dockers

Discuss Security Guidelines, Recommendations and Best Practices for Kubernetes



12 - Enterprise Cloud Security

- Understand Cloud Computing Fundamentals
- Understanding the Insights of Cloud Security
- Evaluate CSP for Security before Consuming Cloud Service
- Discuss security in Amazon Cloud (AWS)
- Discuss security in Microsoft Azure Cloud
- Discuss security in Google Cloud Platform (GCP)
- Discuss general security best practices and tools for cloud security



13 - Wireless Network Security

- Understand wireless network fundamentals
- Understand wireless network encryption mechanisms
- Understand wireless network authentication methods
- Discuss and implement wireless network security measures



14 - Network Traffic Monitoring and Analysis

- Understand the need and advantages of network traffic monitoring
- Setting up the environment for network monitoring
- Determine baseline traffic signatures for normal and suspicious network traffic
- Perform network monitoring and analysis for suspicious traffic using Wireshark
- Discuss network performance and bandwidth monitoring tools and techniques



15 - Network Logs Monitoring and Analysis

- Understand logging concepts
- Discuss log monitoring and analysis on Windows systems
- Discuss log monitoring and analysis on Linux
- Discuss log monitoring and analysis on Mac
- Discuss log monitoring and analysis in Firewall
- Discuss log monitoring and analysis in Routers
- Discuss log monitoring and analysis on Web Servers
- Discuss centralized log monitoring and analysis



16 - Incident Response and Forensic Investigation

- Understand incident response concept
- Understand the role of first responder in incident response
- Discuss Do's and Don't in first response
- Describe incident handling and response process
- Describe forensics investigation process



17 - Business Continuity and Disaster Recovery

- Introduction to Business Continuity (BC) and Disaster Recovery (DR) concepts
- Discuss BC/DR Activities
- Explain Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
- Discuss BC/DR Standards



18 - Discuss BC/DR Standards

Understand risk management concepts

Learn to manage risk through risk management program

Learn different Risk Management Frameworks (RMF)

Learn to manage vulnerabilities through vulnerability management program

Learn vulnerability Assessment and Scanning



19 - Threat Assessment with Attack Surface Analysis

Understand the attack surface concepts

Learn to understand and visualize your attack surface

Learn to identify Indicators of Exposures (IoE)

Learn to perform attack simulation

Learn to reduce the attack surface

Discuss attack surface analysis specific to Cloud and IoT



20 - Threat Prediction with Cyber Threat Intelligence

Understand role of cyber threat intelligence in network defense

Understand the types of threat Intelligence

Understand the Indicators of Threat Intelligence: Indicators of Compromise (IoCs) and Indicators of Attack (IoA)

Understand the layers of Threat Intelligence

Learn to leverage/consume threat intelligence for proactive defense