Certified Network Defender (CND) - Exam Topics (with Details)

Network Attacks and Defense Strategies

- Types of network attacks (DoS, DDoS, MITM, spoofing)
- Defensive strategies and layered security approaches

Administrative Network Security

- Security policies and procedures
- User management and access controls

Technical Network Security

- Network protocols and secure configurations
- Hardening routers, switches, and servers

Network Perimeter Security

- Firewalls, IDS/IPS configuration
- DMZ design and best practices

Endpoint Security - Windows Systems

- Windows security settings
- Patch management and antivirus tools

Endpoint Security - Linux Systems

- Linux hardening techniques
- Security monitoring tools for Linux

Endpoint Security - Mobile Devices

- Mobile Device Management (MDM)
- BYOD security policies

Endpoint Security - IoT Devices

- IoT vulnerabilities and risks
- IoT security controls

Administrative Application Security

- Secure application policies
- Application patch management

Data Security

- Encryption techniques and standards
- Data backup and recovery strategies

Enterprise Virtual, Cloud, and Wireless Security

- Securing virtualization platforms
- Cloud security models (IaaS, PaaS, SaaS)
- Wireless security protocols (WPA3, WPA2)

Network Traffic Monitoring and Analysis

- Traffic capture and analysis tools (Wireshark, tcpdump)
- Detecting abnormal traffic patterns

Network Logs Monitoring and Analysis

- Log collection and SIEM integration
- Incident detection through log analysis

Incident Response and Forensics

- Incident handling process
- Digital forensics basics and evidence handling

Business Continuity and Disaster Recovery

- BCP and DRP planning
- Redundancy and failover strategies

Risk Assessment and Vulnerability Management

- Risk management frameworks (NIST, ISO)
- Vulnerability scanning and patching

Threat Intelligence and Hunting

- Threat intelligence sources and feeds
- Proactive threat hunting techniques

Policy and Governance in Network Defense

- Security policy frameworks
- Regulatory compliance (GDPR, HIPAA, PCI-DSS)

Network Security Controls and Countermeasures

- Access controls and authentication methods
- Security baselines and monitoring

Operational Security for Networks

- Day-to-day security operations
- Change management and auditing