Certified Network Defense (CND) Outline

Module 01: Computer Network and Defense Fundamentals

- Network Fundamentals
    - Computer Network
    - Types of Network
    - Major Network Topologies
- Network Components
    - Network Interface Card (NIC)
    - Repeater
    - Hub
    - Switches
    - Router
    - Bridges
    - Gateways
- TCP/IP Networking Basics
    - Standard Network Models: OSI Model
    - Standard Network Models: TCP/IP Model
    - Comparing OSI and TCP/IP
- TCP/IP Protocol Stack
    - Domain Name System (DNS)
    - DNS Packet Format
    - Transmission Control Protocol (TCP)
        - TCP Header Format
        - TCP Services
        - TCP Operation
        - Three-way handshake
    - User Datagram Protocol (UDP)
        - UDP Operation
    - IP Header
        - IP Header: Protocol Field
        - What is Internet Protocol v6 (IPv6)?
        - IPv6 Header
    - Internet Control Message Protocol (ICMP)
        - Format of an ICMP Message
    - Address Resolution Protocol (ARP)
        - ARP Packet Format

        - Ethernet
        - Fiber Distributed Data Interface (FDDI)
        - Token Ring
    - IP Addressing
        - Classful IP Addressing
        - Address Classes
        - Reserved IP Address
        - Subnet Masking
            - Subnetting
            - Supernetting
        - IPv6 Addressing
            - Difference between IPv4 and IPv6
            - IPv4 compatible IPv6 Address
    - Computer Network Defense (CND)
        - Computer Fundamental Attributes
        - What CND is NOT
        - CND Layers
            - CND Layer 1: Technologies
            - CND Layer 2: Operations
            - CND Layer 3: People
        - Blue Teaming
        - Network Defense-In-Depth
        - Typical Secure Network Design
    - CND Triad
    - CND Process
    - CND Actions
    - CND Approaches

Module 02: Network Security Threats, Vulnerabilities, and Attacks

- Essential Terminologies
    - Threats
    - Vulnerabilities
    - Attacks
- Network Security Concerns
    - Why Network Security Concern Arises?
    - Fundamental Network Security Threats

    - Types of Network Security Threats
    - Where they arises from?
    - How does network security breach affects business continuity?
- Network Security Vulnerabilities
    - Types of Network Security Vulnerabilities
    - Technological Vulnerabilities
    - Configuration Vulnerabilities
    - Security policy Vulnerabilities
    - Types of Network Security Attacks
- Network Reconnaissance Attacks
    - Reconnaissance Attacks
        - Reconnaissance Attacks: ICMP Scanning
        - Reconnaissance Attacks: Ping Sweep
        - Reconnaissance Attacks: DNS Footprinting
        - Reconnaissance Attacks: Network Range Discovery
        - Reconnaissance Attacks: Network Topology Identification
        - Reconnaissance Attacks: Network Information Extraction using Nmap Scan
        - Reconnaissance Attacks: Port Scanning
        - Reconnaissance Attacks : Network Sniffing
        - How an Attacker Hacks the Network Using Sniffers
        - Reconnaissance Attacks : Social Engineering Attacks
- Network Access Attacks
    - Password Attacks
    - Password Attack Techniques
        - Dictionary Attack
        - Brute Forcing Attacks
        - Hybrid Attack
        - Birthday Attack
        - Rainbow Table Attack
    - Man-in-the-Middle Attack
    - Replay Attack
    - Smurf Attack
    - Spam and Spim
    - Xmas Attack
    - Pharming
    - Privilege Escalation

    - DNS Poisoning
    - DNS Cache Poisoning
    - ARP Poisoning
    - DHCP Attacks: DHCP Starvation Attacks
        - DHCP Attacks: DHCP Spoofing Attack
    - Switch Port Stealing
    - Spoofing Attacks
        - MAC Spoofing/Duplicating
- Denial of Service (DoS) Attacks
- Distributed Denial-of-Service Attack (DDoS)
- Malware Attacks
    - Malware
        - Types of Malware: Trojan
        - Types of Malware: Virus and Armored Virus
    - Malware Attacks
        - Adware
        - Spyware
        - Rootkits
        - Backdoors
        - Logic Bomb
        - Botnets
        - Ransomware
        - Polymorphic malware

Module 03: Network Security Controls, Protocols, and Devices

- Fundamental Elements of Network Security
    - Network Security Controls
    - Network Security Protocols
    - Network Security Perimeter Appliances
- Network Security Controls
    - Access Control
        - Access Control Terminology
        - Access Control Principles
        - Access Control System: Administrative Access Control
        - Access Control System: Physical Access Controls
        - Access Control System: Technical Access Controls
    - Types of Access Control

        - Discretionary Access Control (DAC)
        - Mandatory Access Control (MAC)
        - Role-based Access
    - Network Access Control (NAC)
    - NAC Solutions
- User Identification, Authentication, Authorization and Accounting
    - Types of Authentication :Password Authentication
    - Types of Authentication: Two-factor Authentication
    - Types of Authentication : Biometrics
    - Types of Authentication : Smart Card Authentication
    - Types of Authentication: Single Sign-on (SSO)
- Types of Authorization Systems
    - Centralized Authorization
    - Implicit Authorization
    - Decentralized Authorization
    - Explicit Authorization
- Authorization Principles
    - Least privilege
    - Separation of duties
- Cryptography
    - Encryption
        - Symmetric Encryption
        - Asymmetric Encryption
    - Hashing: Data Integrity
    - Digital Signatures
    - Digital Certificates
    - Public Key Infrastructure (PKI)

- Security Policy
    - Network Security Policy
    - Key Consideration for Network Security Policy
    - Types of Network Security Policies
- Network Security Devices
    - Firewalls
    - DMZ
    - Virtual Private Network (VPN)
    - Proxy Server

        - Advantages Of using Proxy Servers
        - Proxy Tools
    - Honeypot
        - Advantages of using Honeypots
        - Honeypot Tools
    - Intrusion Detection System (IDS)
    - Intrusion Prevention System (IPS)
    - IDS/IPS Solutions
    - Network Protocol Analyzer
        - How it Works
        - Advantages of using Network Protocol Analyzer
        - Network Protocol Analyzer Tools
    - Internet Content Filter
        - Advantages of using Internet Content Filters
        - Internet Content Filters
    - Integrated Network Security Hardware
- Network Security Protocols
        - Transport Layer
        - Network Layer
        - Application Layer
        - Data Link Layer
    - RADIUS
    - TACACS+
    - Kerbros
    - Pretty Good Service (PGP) Protocol
    - S/MIME Protocol
        - How it Works
        - Difference between PGP and S/MIME
    - Secure HTTP
    - Hyper Text Transfer Protocol Secure (HTTPS)
    - Transport Layer Security (TLS)
    - Internet Protocol Security (IPsec)

Module 04: Network Security Policy Design and Implementation

- What is Security Policy?
    - Hierarchy of Security Policy
    - Characteristics of a Good Security Policy

  - Contents of Security Policy
  - Typical Policy Content
  - Policy Statements
  - Steps to Create and Implement Security Policies
  - Considerations Before Designing a Security Policy
  - Design of Security Policy
  - Policy Implementation Checklist
  - Types of Information Security Policy
    - Enterprise information security policy(EISP
    - Issue specific security policy(ISSP)
    - System specific security policy (SSSP)
- Internet Access Policies
  - Promiscuous Policy
  - Permissive Policy
  - Paranoid Policy
  - Prudent Policy
- Acceptable-Use Policy
- User-Account Policy
- Remote-Access Policy
- Information-Protection Policy
- Firewall-Management Policy
- Special-Access Policy
- Network-Connection Policy
- Business-Partner Policy
- Email Security Policy
- Passwords Policy
- Physical Security Policy
- Information System Security Policy
- Bring Your Own Devices (BYOD) Policy
- Software/Application Security Policy
- Data Backup Policy
- Confidential Data Policy
- Data Classification Policy
- Internet Usage Policies
- Server Policy
- Wireless Network Policy
- Incidence Response Plan (IRP)
- User Access Control Policy

- Switch Security Policy
- Intrusion Detection and Prevention (IDS/IPS) Policy
- Personal Device Usage Policy
- Encryption Policy
- Router Policy
- Security Policy Training and Awareness
- ISO Information Security Standards
    - ISO/IEC 27001:2013: Information technology — Security Techniques — Information security Management Systems — Requirements
    - ISO/IEC 27033:Information technology -- Security techniques -- Network security
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Information Security Acts: Sarbanes Oxley Act (SOX)
- Information Security Acts: Gramm-Leach-Bliley Act (GLBA)
- Information Security Acts: The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)
- Other Information Security Acts and Laws
    - Cyber Law in Different Countries

Module 05: Physical Security

- Physical Security
    - Need for Physical Security
    - Factors Affecting Physical Security
    - Physical Security Controls
        - Administrative Controls
        - Physical Controls
        - Technical Controls
    - Physical Security Controls: Location and Architecture Considerations
    - Physical Security Controls: Fire Fighting Systems
    - Physical Security Controls: Physical Barriers
    - Physical Security Controls: Security Personnel
- Access Control Authentication Techniques
    - Authentication Techniques: Knowledge Factors
    - Authentication Techniques: Ownership Factors
    - Authentication Techniques: Biometric Factors
- Physical Security Controls
    - Physical Locks

    - Mechanical locks:
    - Digital locks:
    - Combination locks:
    - Electronic /Electric /Electromagnetic locks:
    - Concealed Weapon/Contraband Detection Devices
    - Mantrap
    - Security Labels and Warning Signs
    - Alarm System
    - Video Surveillance
    - Physical Security Policies and Procedures
- Other Physical Security Measures
    - Lighting System
    - Power Supply
- Workplace Security
    - Reception Area
    - Server/ Backup Device Security
    - Critical Assets and Removable Devices
    - Securing Network Cables
    - Securing Portable Mobile Devices
- Personnel Security: Managing Staff Hiring and Leaving Process
- Laptop Security Tool: EXO5
    - Laptop Tracking Tools
- Environmental Controls
    - Heating, Ventilation and Air Conditioning
    - Electromagnetic Interference (EMI) Shielding
    - Hot and Cold Aisles
- Physical Security: Awareness /Training
- Physical Security Checklists

Module 06: Host Security

- Host Security
    - Common Threats Specific to Host Security
    - Where do they come from?
    - Why Host Security?
    - Before Configuring Host Security: Identify purpose of each Host
    - Host Security Baselining
- OS Security
    - Operating System Security Baselining

- Common OS Security Configurations
- Windows Security
    - Windows Security Baselining: Example
    - Microsoft Baseline Security Analyzer (MBSA)
    - Setting up BIOS Password
    - Auditing Windows Registry
    - User and Password Management
    - Disabling Unnecessary User Accounts
    - Configuring user authentication
- Patch Management
    - Configuring an update method for Installing Patches
    - Patch Management Tools
- Disabling Unused System Services
- Set Appropriate Local Security Policy Settings
- Configuring Windows Firewall
- Protecting from Viruses
    - Antivirus Software
- Protecting from Spywares
    - Antispywares
- Email Security: AntiSpammers
    - Spam Filtering Software
- Enabling Pop-up Blockers
- Windows Logs Review and Audit
    - Log Review Recommendations
    - Event IDs in Windows Event log
- Configuring Host-based IDS/IPS
    - Host based IDS: OSSEC
    - AlienVault Unified Security Management (USM)
    - Tripwire
    - Additional Host Based IDSes
- File System Security: Setting Access Controls and Permission to Files and Folders
    - Creating and Securing a Windows file share
- File and File System Encryption
    - EFS Limitations
    - Data encryption Recommendations
    - DATA Encryption Tools

- Linux Security
    - Linux Baseline Security Checker: buck-security