Network Defense Essentials

(Version 1)

Course Outline

Module 01: Network Security Fundamentals

- **Understand Fundamentals of Network Security**
  - Essentials of Network Security
  - Goal of Network Defense
  - Information Assurance (IA) Principles
    - Confidentiality
    - Availability
    - Integrity
    - Non-repudiation
    - Authentication
  - Network Defense Benefits
  - Network Defense Challenges
  - Types of Network Defense Approaches
    - Preventive Approach
    - Reactive Approach
    - Retrospective Approach
    - Proactive Approach
  - Network Security Controls
    - Administrative Network Security Controls
    - Physical Network Security Controls

- Technical Network Security Controls

- **Discuss Essential Network Security Protocols**
  - Network Security Protocols
    - Remote Authentication Dial-in User Service (RADIUS)
    - Terminal Access Controller Access Control System Plus (TACACS+)
    - Kerberos
    - Pretty Good Service (PGP)
    - Secure/Multipurpose Internet Mail Extensions (S/MIME)
      - Difference between PGP and S/MIME
    - Secure Hypertext Transfer Protocol (S-HTTP)
    - Hypertext Transfer Protocol Secure (HTTPS)
    - Transport Layer Security (TLS)
    - Secure Sockets Layer (SSL)
    - Internet Protocol Security (IPsec)

Module 02: Identification, Authentication and Authorization

- **Discuss Access Control Principles, Terminologies, and Models**
  - Access Control
  - Access Control Terminologies
  - Access Control Principles
  - Access Control Models
    - Mandatory Access Control (MAC)
    - Discretionary Access Control (DAC)
    - Role-based Access Control (RBAC)
    - Rule-based access control (RB-RBAC)
  - Logical Implementation of DAC, MAC, and RBAC

Lab Exercise

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

- **Discuss Identity and Access Management (IAM) Concepts**
  - Identity and Access Management (IAM)
    - User Identity Management (IDM)
      - Identity Management
      - Identity Repository
  - User Access Management (AM)
    - Authentication
      - Types of Authentication
        - ✓ Password Authentication
        - ✓ Smart Card Authentication
        - ✓ Biometric Authentication
        - ✓ Two-factor Authentication
        - ✓ Single Sign-on (SSO) Authentication
    - Authorization
      - Types of Authorization
        - ✓ Centralized Authorization
        - ✓ Implicit Authorization
        - ✓ Decentralized Authorization
        - ✓ Explicit Authorization
    - Accounting

Module 03: Network Security Controls - Administrative Controls

- **Discuss Various Regulatory Frameworks, Laws, and Acts**
  - Regulatory Frameworks Compliance
    - Role of Regulatory Frameworks Compliance in an Organization's Administrative Security
  - Why Organizations Need Compliance
  - Identifying Which Regulatory Framework to Comply
  - Deciding on How to Comply to Regulatory Framework
  - Regulatory Frameworks, Laws, and Acts
    - Payment Card Industry Data Security Standard (PCI-DSS)

- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA)
- ISO Information Security Standards
- The Digital Millennium Copyright Act (DMCA)
- The Federal Information Security Management Act (FISMA)
- Other Information Security Acts and Laws
- Cyber Law in Different Countries

- **Learn to Design and Develop Security Policies**
  - What is Security Policy?
  - Need for a Security Policy
  - Advantages of Security Policies
  - Characteristics of a Good Security Policy
  - Key Elements of Security Policy
  - Contents of a Security Policy
  - Typical Policy Document Content
  - Types of Information Security Policies
    - 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
  - Password Policy

Lab Exercise

- Implementing Password Policies Using Windows Group Policy

- **Learn to Conduct Different Type of Security and Awareness Training**
  - Employee Awareness and Training
    - Security Policy
    - Physical Security
    - Social Engineering
    - Data Classification

Module 04: Network Security Controls - Physical Controls

- **Understand the Importance of Physical Security**
  - Need for Physical Security
  - Physical Security Attack Vectors
    - Natural/Environmental Threats
    - Man-made Threats
- **Discuss Various Physical Security Controls**
  - Types of Physical Security Controls
  - Location Considerations
  - Site Architecture Considerations
  - Fire Fighting Systems
  - Physical Barriers
  - Security Personnel
  - Physical Locks
    - Mechanical locks
    - Digital locks
    - Combination locks
    - Electronic /Electric /Electromagnetic locks
  - Concealed Weapon/Contraband Detection Devices
  - Mantrap
  - Warning Signs
  - Alarm System
  - Video Surveillance
  - Lighting System

- Power Supply

- **Describe Workplace Security**
  - Reception Area
  - Server/ Backup Device Security
  - Critical Assets and Removable Devices
  - Securing Network Cables
  - Securing Portable Mobile Devices
  - Physical Security Policy
- **Describe Various Environmental Controls**
  - Heating, Ventilation and Air Conditioning
  - Electromagnetic Interference (EMI) Shielding
  - Hot and Cold Aisles
  - Physical Security Checklists

Module 05: Network Security Controls - Technical Controls

- **Understand Different Types of Network Segmentation**
  - What is Network Segmentation?
  - Types of Network Segmentation
    - Physical Segmentation
    - Logical Segmentation
    - Network Virtualization
  - Introduction to Bastion Host
  - Need for Bastion Host
  - Positioning the Bastion Host
  - Types of Bastion Hosts
    - Single-homed
    - Multi-homed
    - Internal Bastion Host
    - Non-routing Dual-homed Hosts
    - External Services Hosts
    - Victim Machines

- One-box Firewalls

- What is Demilitarized Zone (DMZ)?
  - Different Ways to Create a DMZ
    - Single Firewall DMZ
    - Dual Firewall DMZ

- **Understand Different Types of Firewalls and their Role**
  - What is a Firewall?
  - Types of Firewalls
    - Hardware Firewalls
    - Software Firewalls
    - Host-based Firewalls
    - Network-based Firewalls
  - Firewall Technologies
    - Packet Filtering Firewall
    - Circuit-Level Gateways
    - Application-Level Gateways
    - Stateful Multilayer Inspection Firewall
    - Application Proxy
    - Network Address Translation (NAT)
    - Virtual Private Network
    - Next Generation Firewall (NGFW)
  - Firewall Capabilities
  - Firewall Limitations
  - Firewall Implementation and Deployment Process
  - Host-based Firewall Protection with Iptables
  - Secure Firewall Implementation
    - Best Practices
    - Recommendations
    - Do's and Don'ts

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

- **Understand Different Types of IDS/IPS and their Role**
  - Intrusion Detection and Prevention Systems (IDS/IPS)
  - How does an IDS Work?
  - Role of an IDS in Network Defense
  - How an IDS Detects an Intrusion?
  - IDS Capabilities
  - IDS/IPS Limitations: What an IDS/IPS is NOT?
  - IDS/IPS Security Concerns
    - Common Mistakes in IDS/IPS Configurations
  - General Indications of Intrusions
    - File System Intrusions
    - Network Intrusions
    - System Intrusions
  - IDS Classification
    - Approach-based IDS
      - Signature-Based Detection
      - Anomaly-based Detection
    - Anomaly and Misuse Detection Systems
    - Behavior-based IDS
    - Protection-based IDS
    - Structure-based IDS
    - Analysis Timing-based IDS
    - Source Data Analysis-based IDS
  - IDS Components
    - Network Sensors

- Command Console
- Alert Systems
- Response System
- Attack Signature Database

- Collaboration of IDS Components in Intrusion Detection
- Deployment of Network and Host-based IDS
  - Staged IDS Deployment
  - Deploying Network-based IDS
  - Deploying a Host-based IDS
- What is an IDS Alert?
- Types of IDS Alerts
  - True Positive Alerts
  - False Positive Alerts
  - False Negative Alerts
  - True Negative Alerts
- Characteristics of Good IDS Solutions
- Selection of an Appropriate IDS/IPS Solutions
- Intrusion Detection with Snort
- Intrusion Detection Tools

Lab Exercise

- Implementing Host-based IDS functionality using Wazuh HIDS
- Implementing Network-based IDS Functionality Using Suricata IDS

▪ **Understand Different Types of Honeypot**

- Honeypot
- Types of Honeypots
  - Classification of Honeypots based on their design criteria
  - Classification of honeypots based on their deployment strategy
  - Classification of honeypots based on their deception technology
- Honeypot Tools

Lab Exercise

- Detect Malicious Network Traffic using HoneyBOT

- **Understand Different Types of Proxy Servers and their Benefits**
  - What are Proxy Servers?
  - Benefits of Proxy Server
  - Functioning of a Proxy Server
  - Proxy Servers vs Packet Filters
  - Types of Proxy Servers
    - Transparent Proxy
    - Non-transparent Proxy
    - SOCKS Proxy
    - Anonymous Proxy
    - Reverse Proxy
  - How to Configure Proxy Server
    - Configuring Automatic Proxy Setup in Windows 10
    - Configuring Manual Proxy Setup in Windows 10
    - Configuring Proxy Setup in Google Chrome
    - Configuring Proxy Setup in Microsoft Edge
  - Limitations of Proxy Server
    - Example of a Proxy Server: Squid Proxy
  - List of Proxy Tools
- **Discuss Fundamentals of VPN and its importance in Network Security**
  - What is a VPN?
  - How VPN Works?
  - Why Establish VPN?
  - VPN Components
  - VPN Concentrators
    - Functions of a VPN Concentrator
  - VPN Types and Categories
    - Client-to-site (Remote-access) VPNs
    - Site-to-Site VPNs

- Hardware VPNs
  - Hardware VPN Products
- Software VPNs
  - Software VPN Products

- Selecting an Appropriate VPN
- VPN Core Functionality
  - Encapsulation
  - Encryption
  - Authentication
- VPN Technologies
  - Trusted VPNs
  - Secure VPNs
  - Hybrid VPNs
- VPN Topologies
  - Hub-and-Spoke VPN Topology
  - Point-to-Point VPN Topology
  - Full Mesh VPN Topology
  - Star Topology
- Example of a VPN: OpenVPN
- VPN Security Risks
- VPN Security
  - Firewalls
  - IPsec Server
  - AAA Server
  - Remote Access Dial-In User Service
  - Connection to VPN
    - SSH and PPP
    - SSL and PPP
    - Concentrator

Lab Exercise

- Establishing Virtual Private Network Connection using SoftEther VPN

- **Discuss Security Incident and Event Management (SIEM)**
  - Security Incident and Event Management (SIEM)
  - SIEM Architecture
  - SIEM Functions
  - SIEM Solutions
- **Discuss User Behavior Analytics (UBA)**
  - User Behavior Analytics (UBA)
  - Why User Behavior Analytics is Effective?
  - UBA/UEBA Tools
- **Understand Various Antivirus/Anti-malware Software**
  - Anti-Trojan Software
  - Antivirus Software

Module 06: Virtualization and Cloud Computing

- **Understand Virtualization Essential Concepts and OS Virtualization Security**
  - Virtualization
    - Virtualization Approaches
    - Levels of Virtualization
    - Types of Virtualization
  - Virtualization Components
  - Virtualization Enablers
    - Network Virtualization (NV)
    - Software Defined Network (SDN)
    - Network Function Virtualization (NFV)
  - Common Virtualization Vendors
  - OS Virtualization Security and Concerns
    - Container
    - Container Technology Architecture
    - Types of Containers
    - Containers Vs Virtual Machine

- Docker
- Docker Networking
- Kubernetes
- Container Security Challenges
- Container Security Threats
- Docker Security Threats
- Kubernetes Security Challenges and Threats

o OS Virtualization Security Best Practices

- Best Practices for Container Security
- Best Practices for Docker Security
- Best Practices for Kubernetes Security
- Docker Security Tools

Lab Exercise

o Auditing Docker Host Security Using Docker-Bench-Security Tool

▪ **Understand Cloud Computing Fundamentals**

o Introduction to Cloud Computing

o Cloud Computing Benefits

o Types of Cloud Computing Services

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)
- Identity-as-a-Service (IDaaS)
- Security-as-a-Service (SECaaS)
- Container-as-a-Service (CaaS)
- Function-as-a-Service (FaaS)
- Anything-as-a-Service (XaaS)

o Customer vs CSP Shared Responsibilities in IaaS, PaaS, and SaaS

o Cloud Deployment Models

- Public Cloud
- Private Cloud

- Community Cloud
- Hybrid Cloud
- Multi Cloud

- On-premise vs. Hosted vs. Cloud
- NIST Cloud Deployment Reference Architecture
- Cloud Storage Architecture
- Cloud Service Providers

- **Discuss the Insights of Cloud Security and Best Practices**
  - Cloud Security: Shared Responsibility
  - Elements of Cloud Security
    - Consumers Vs Providers
    - Identity and Access Management (IAM)
    - Compliance
    - Data Storage Security
    - Monitoring
    - Network Security
    - Logging
  - AWS Identity and Access Management
    - Lock Your AWS Account Root User Access Keys
    - Create Individual IAM Users
    - Use Groups to Assign Permissions to IAM Users
    - Grant Least Privilege
    - Use AWS-managed Policies
  - Best Practices for Securing the Cloud
  - NIST Recommendations for Cloud Security
  - Organization/Provider Cloud Security Compliance Checklist
  - Cloud Security Tools

Lab Exercise

- Implementing AWS Identity and Access Management
- Securing Amazon Web Services Storage

Module 07: Wireless Network Security

- **Understand Wireless Network Fundamentals**
  - Wireless Terminologies
  - Wireless Networks
  - Wireless Technologies
  - Wired vs. Wireless Networks
  - Wireless Standards
  - Wireless Network Topologies
    - Ad-hoc Standalone Network Architecture (Independent Basic Service Set (IBSS))
    - Infrastructure Network Topology (Centrally Coordinated Architecture/ Basic Service Set (BSS))
  - Classification of Wireless Networks
    - Wireless Networks Based on the Connection
      - Extension to a Wired Network
      - Multiple Access Points
      - LAN-to-LAN Wireless Network
      - 4G Hotspot
    - Wireless Network Based on the Geographic Area Coverage
      - WLAN
      - WWAN
      - WPAN
      - WMAN
  - Components of Wireless Network
    - Access Point
    - Wireless Cards (NIC)
    - Wireless Modem
    - Wireless Bridge
    - Wireless Repeater
    - Wireless Router

- Wireless Gateways
- Wireless USB Adapter
- Antenna
  - Directional Antenna
  - Parabolic Grid Antenna
  - Dipole Antenna
  - Omnidirectional Antenna
  - Yagi Antenna
  - Reflector Antennas

- **Understand Wireless Network Encryption Mechanisms**
  - Types of Wireless Encryption
    - Wired Equivalent Privacy (WEP) Encryption
    - Wi-Fi Protected Access (WPA) Encryption
    - WPA2 Encryption
    - WPA3 Encryption
  - Comparison of WEP, WPA, WPA2, and WPA3
  - Issues in WEP, WPA, and WPA2
- **Discuss Different Types of Wireless Network Authentication Methods**
  - Wi-Fi Authentication Method
    - Open System Authentication
    - Shared Key Authentication
  - Wi-Fi Authentication Process Using a Centralized Authentication Server
- **Discuss and Implement Wireless Network Security Measures**
  - Wireless Network Security Measures
    - Creating an Inventory of Wireless Devices
    - Placement of a Wireless AP
    - Placement of a Wireless Antenna
    - Disable SSID Broadcasting
    - Selecting a Strong Wireless Encryption Mode
    - Defending Against WPA Cracking

- Detecting Rogue Access Points
  - Wireless Scanning
  - Wired Network Scanning
  - Simple Network Management Protocol (SNMP) Polling
- Wireless Security Tools
- Configuring the Administrative Security on Wireless Routers

Lab Exercise

- Configuring Security on a Wireless Router

Module 08: Mobile Device Security

- **Understand Various Mobile Device Connection Methods**
  - Near-field Communication (NFC)
  - Satellite Communication (Satcom)
  - Cellular Communication
  - ANT
  - Universal Serial Bus (USB)
  - Global Positioning System (GPS)
  - Infrared (IR)
  - Wi-Fi
  - Bluetooth
  - 5G Cellular (Mobile) Communication
  - Point-to-point (P2P) Connection
  - Point-to-multipoint Connection
  - Radio-frequency Identification (RFID)
- **Discuss Mobile Device Management Concepts**
  - Mobile Application Management
  - Mobile Content Management
  - Context-aware Authentication
  - Mobile Email Management
  - Enterprise Mobility Management
  - Mobile Security Management

- Remote Wipe
- Screen Lock
- Passwords and PINs
- Biometrics
- Push Notification Services
- Geolocation
- Geofencing
- Full Device Encryption
- Containerization

- **Discuss Common Mobile Usage Policies in Enterprises**
  - Mobile Use Approaches in Enterprise
  - Bring Your Own Device (BYOD)
    - BYOD Policy Implementation
  - Choose Your Own Device (CYOD)
    - CYOD Policy Implementation
  - Corporate Owned, Personally Enabled (COPE)
    - COPE Policy Implementation
  - Company Owned, Business Only (COBO)
    - COBO Policy Implementation
- **Discuss Security Risk and Guidelines Associated with Enterprises Mobile Usage Policies**
  - Enterprise Mobile Device Security Risks and Challenges
  - Risk Associated with BYOD, CYOD, COPE, and COBO
  - Security Guidelines for BYOD, CYOD, COPE, and COBO
- **Discuss and Implement Enterprise-level Mobile Security Management Solutions**
  - Mobile Device Management Solutions
  - Mobile Application Management Solutions
  - Mobile Content Management Solutions
  - Mobile Threat Defense Solutions
  - Mobile Email Management Solutions
  - Enterprise Mobility Management Solutions

- Unified Endpoint Management Solutions

- **Discuss and Implement General Security Guidelines and Best Practices on Mobile Platforms**
  - Mobile Application Security Best Practices
  - Mobile Data Security Best Practices
  - Mobile Network Security Guidelines
  - General Guidelines for Mobile Platform Security
  - Android Security Tools
  - iOS Device Security Tools

Lab Exercise

- Implementing Enterprise Mobile Security Using Miradore MDM Solution

Module 09: IoT Device Security

- **Understand IoT Devices, Application Areas, and Communication Models**
  - What is the IoT?
  - Why Organization are Opting for IoT-enabled Environments
  - IoT Application Areas and Devices
  - IoT Architecture
  - Layers of IoT Architecture
    - Device Layer
    - Communication Layer
    - Cloud Platform Layer
    - Process Layer
  - IoT Communication Models
  - IoT-Enabled IT Environment
- **Discuss the Security in IoT-enabled Environments**
  - Security in IoT- enabled Environments
  - IoT System Management
  - Stack-wise IoT Security Principles
    - Secure Device Layer
    - Secure Communication Layer

- Secure Cloud Platform Layer
- Secure Process Layer

- IoT Framework Security Considerations
- IoT Device Management
- IoT Security Best Practices
- IoT Security Tools

Lab Exercise

- Securing IoT Device Communication Using TLS/SSL

Module 10: Cryptography and PKI

- **Discuss Cryptographic Techniques**
  - Cryptography
  - Encryption
    - Symmetric Encryption
    - Asymmetric Encryption
  - Government Access to Keys (GAK)
- **Discuss Various Cryptographic Algorithms**
  - Ciphers
    - Data Encryption Standard (DES)
    - Advanced Encryption Standard (AES)
    - RC4, RC5, and RC6 Algorithms
    - Digital Signature Algorithm (DSA) and Rivest Shamir Adleman (RSA)
    - MD5 and MD6
    - Secure Hashing Algorithm (SHA)
    - HMAC
- **Discuss Various Cryptography Tools**
  - MD5 and MD6 Hash Calculators
  - Hash Calculators for Mobile
  - Cryptography Tools

Lab Exercise

- Calculate One-way Hashes using HashCalc
- Calculate MD5 Hashes using HashMyFiles

- **Discuss Public Key Infrastructure (PKI)**
  - Digital Signature
  - Digital Certificates
  - Public Key Infrastructure (PKI)
    - Certification Authorities

Lab Exercise

- Create a Self-signed Certificate

Module 11: Data Security

- **Understand Data Security and its Importance**
  - What is Business Critical Data?
    - Examples of Critical Data
  - The Need of Data Security
  - Data Security
  - Example: Data At Rest vs Data in Use vs Data in Transit
  - Data Security Technologies
- **Discuss Various Security Controls for Data Encryption**
  - Disk Encryption Techniques
    - Disk Encryption: Implementing Built-in Disk Encryption for Windows
      - Disk Encryption Tools
    - File Level Encryption: Implementing Built-in File System-level Encryption on Windows
      - File Encryption Tools
    - Removable Media Encryption: Implementing Removable Media Encryption in Windows
      - Removable Media Encryption Tools

Lab Exercise

- Perform Disk Encryption using VeraCrypt

- **Discuss Data Backup and Retention**

- Introduction to Data Backup
- Data Backup Strategy/Plan
- Selecting the Backup Media
- Examples of Data Backup Media Devices
- RAID (Redundant Array Of Independent Disks) Technology
  - Advantages and Disadvantages of RAID Systems
  - RAID Storage Architecture
  - RAID Level 0: Disk Striping
  - RAID Level 1: Disk Mirroring
  - RAID Level 3: Disk Striping with Parity
  - RAID Level 5: Block Interleaved Distributed Parity
  - RAID Level 10: Blocks Striped and Mirrored
  - RAID Level 50: Mirroring and Striping across Multiple RAID Levels
- Storage Area Network (SAN)
  - Advantages of SAN
- Network Attached Storage (NAS)
- Selecting Appropriate Backup Method
  - Hot Backup (Online)
  - Cold Backup (Offline)
  - Warm Backup (Nearline)
- Choosing the Backup Location
  - Onsite Data Backup
  - Offsite Data Backup
  - Cloud Data Backup
- Types of Backup
  - Full/Normal Data Backup
  - Differential Data Backup
  - Incremental Data Backup
  - Advantages and Disadvantages
- Data Backup Tools

- Data Backup Retention
- Data Retention Policy Best practices
- Data Recovery Tools

Lab Exercise

- File Recovery Using EaseUS Data Recovery Wizard
- Backing Up and Restoring Data in Windows

- **Discuss Data Loss Prevention Concepts**
  - What is Data Loss Prevention?
  - Types of Data Loss Prevention (DLP) Solutions
  - DLP Solution: Windows Information Protection (WIP)
    - DLP Solutions
  - Best Practices for a Successful DLP Implementation

Module 12: Network Traffic Monitoring

- **Understand the Need and Advantages of Network Traffic Monitoring**
  - Network Traffic Monitoring
  - Need for Network Monitoring
  - Advantages of Network Monitoring
- **Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic**
  - Network Traffic Signatures
    - Normal Traffic Signature
    - Attack Signatures
  - Baselining Normal Traffic Signatures
  - Categories of Suspicious Traffic Signatures
    - Informational
    - Reconnaissance
    - Unauthorized Access
    - Denial of Service
  - Attack Signature Analysis Techniques
    - Content-based Signatures Analysis

- Context-based Signatures Analysis
- Atomic Signatures-based Analysis
- Composite Signatures-based Analysis

▪ **Perform Network Monitoring for Suspicious Traffic**

- Wireshark
  - Follow TCP Stream in Wireshark
  - Display Filters in Wireshark
  - Additional Wireshark Filters
- Monitoring and Analyzing FTP Traffic
- Monitoring and Analyzing Telnet Traffic
- Monitoring and Analyzing HTTP Traffic
- Network Sniffers for Network Monitoring
- Network Monitoring Tools

Lab Exercise

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