

Certified Network Defense (CND) v2-Outline

1. INTRODUCTION

CNDv2 Module 01: Network Attacks and Defense Strategies

LO#01: Explain essential terminologies related to network security attacks

- Asset
- Threat
 - Threats Sources
 - Natural
 - Unintentional
 - Intentional
 - Internal
 - External
 - Threat Actors/Agents
 - Hacktivist
 - Cyber Terrorists
 - Suicide Hackers
 - State-Sponsored Hackers
 - Organized Hackers
 - Script Kiddies
 - Industrial Spies
 - Insider
- Vulnerability
 - Common Reasons behind the Existence of Vulnerability
 - Network Security Vulnerabilities: Technological
 - Network Security Vulnerabilities: Configuration
 - Network Security Vulnerabilities: Security Policy
- Risk
 - Risk Levels
 - Risk Matrix
- Attack
 - Intent-Motive-Goal

CND Outline

- Tactics-Techniques-Procedures (TTPs)

LO#02: Describe the various examples of network-level attack techniques

- Reconnaissance Attacks
- Network Scanning
- Port Scanning
- DNS Footprinting
- Network Sniffing
- Man-in-the-Middle Attack
- Password Attacks
 - Password Attack Techniques
 - Dictionary Attack
 - Brute Forcing Attacks
 - Hybrid Attack
 - Birthday Attack
 - Rainbow Table Attack
- Privilege Escalation
- DNS Poisoning
- DNS Cache Poisoning
- ARP Poisoning
- DHCP Starvation Attacks
- DHCP Spoofing Attack
- Switch Port Stealing
- MAC Spoofing/Duplicating
- Network-based Denial-of-Service Attack (DoS)
- Distributed Denial-of-Service Attack (DDoS)
- Malware Attacks
- Advanced Persistent Threats (APTs)

LO#03: Describe the various examples of application-level attack techniques

- SQL Injection Attacks
- Cross-site Scripting (XSS) Attacks
- Parameter Tampering
- Directory Traversal
- Cross-site Request Forgery (CSRF) Attack

CND Outline

- Application-level DoS Attack
- Session Attacks
 - Cookie Poisoning Attacks
 - Session Fixation

LO#04: Describe the various examples of social engineering attack techniques

- Impersonation
- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Piggybacking and Tailgating

LO#05: Describe the various examples of email attack techniques

- Malicious Email Attachments
- Malicious User Redirection
- Phishing
- Spoofing
- Spamming

LO#06: Describe the various examples of mobile device-specific attack techniques

- Untrusted APK's
- SMS
- Email
- Spying
- App Sandboxing Issue
- Rooting

LO#07: Describe the various examples of cloud-specific attack techniques

- Denial of Service (DoS)/Distributed Denial of Service (DDoS)
- Cloud malware injection attacks
- Cross-cloud attacks
- Side channel attack
- Insider attacks

LO#08: Describe the various examples of wireless network-specific attack techniques

- Packet Sniffing
- Wardriving
- Warshipping

CND Outline

- MAC Spoofing

LO#09: Describe Attacker's Hacking Methodologies and Frameworks

- EC-Council's- Hacking Methodology
- Lockheed Martin's - Cyber Kill Chain Methodology
- MITRE Attack Framework

LO#10: Understand fundamental goal, benefits, and challenges in network defense

- Goal of Network Defense
- Information Assurance (IA) Principles
 - Integrity
 - Confidentiality
 - Availability
 - Non-repudiation
 - Authentication
- Network Defense Benefits
- Network Defense Challenges

LO#11: Explain Continual/Adaptive security strategy

- What constitutes Computer Network Defense?
- Types of Network Defense Approaches
 - Preventive Approach
 - Reactive Approach
 - Retrospective Approach
 - Proactive Approach
- Continual/Adaptive Security Strategy
 - Protect
 - Detect
 - Respond
 - Predict
- Administrative Network Security
- Physical Network Security
- Technical Network Security
- Network Defense Elements
 - Technologies
 - Operations

CND Outline

- People

LO#12: Explain defense-in-depth security strategy

- Multi-Layered Security

Exercise 01: Understanding the Working of SQL Injection Attacks

Exercise 02: Understanding the Working of XSS Attacks

Exercise 03: Understanding the Working of Network Scanning Attacks

Exercise 04: Understanding the Working of Brute Force Attacks

2. PROTECT

CNDv2 Module 02 Administrative Network Security

LO#01: Learn to obtain compliance with regulatory framework and standards

- What constitutes regulatory frameworks Compliance
- Why Organizations need Compliance
- Identifying which Regulatory framework to Comply
- Deciding on how to Comply to Regulatory framework

LO#02: Discuss various 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)
- ISO Information Security Standards
- The Digital Millennium Copyright Act (DMCA)
- Federal Information Security Management Act (FISMA)
- Other Information Security Acts and Laws
- Cyber Law in Different Countries

LO#03: Learn to design and develop security policies

- 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

CND Outline

- 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)

CND Outline

- User Access Control Policy
- Switch Security Policy
- Intrusion Detection and Prevention (IDS/IPS) Policy
- Personal Device Usage Policy
- Encryption Policy
- Router Policy
- Policy Implementation Checklist

LO#04: Learn to conduct different type security and awareness training

- Employee Awareness and Training
 - Security Policy Training
 - Physical Security Training
 - Social Engineering Awareness
 - Data Classification Training

LO#05: Learn to implement other administrative security measures

- Managing the Staff Hiring and Leaving Process
- Employee Monitoring

Exercise 01: Implementing Password Policies Using Windows Group Policy

Exercise 02: Implementing Password Policies in Linux

Exercise 03: Monitoring User Activities on Remote User System

CNDv2 Module 03: Technical Network Security

LO#01: Discuss access control principles, terminologies, and models

- Access Control
 - Access Control Terminology
 - Access Control Principles
 - Types of Access Control
 - Discretionary Access Control (DAC)
 - Mandatory Access Control (MAC)
 - Role-based Access Control (RBAC)
 - Rule-based access control (RB-RBAC)
 - MAC Model Example
 - Bell-LaPadula Model (BLM)-Confidentiality Model
 - Biba integrity model-Integrity Model
 - DAC Model Example

CND Outline

- Access Control Matrix
- Logical Implementation of DAC, MAC, and RBAC
 - MAC Implementation- Windows User Account Control (UAC)
 - DAC Implementation- Windows File Permissions
 - RBAC Implementation- Just Enough Administration (JEA)
 - RBAC Implementation-Windows Admin Center (WAC)

LO#02: Redefine the Access Control in Today's Distributed and Mobile Computing World

- Castle-and-Moat Model
- Zero Trust Network Model
 - Principles of Zero Trust Model

LO#03: Discuss Identity and Access Management (IAM):

- Identity and Access Management (IAM)
 - User Identity Management (IDM)
 - Identity Management
 - Identity repository
 - User Access Management (AM)
 - User Authentication
 - Types of Authentication
 - Password Authentication
 - Two-factor Authentication
 - Biometrics
 - Smart Card Authentication
 - Single Sign-on (SSO)
 - User Authorization
 - Types of Authorization
 - Centralized Authorization
 - Implicit Authorization
 - Decentralized Authorization
 - Explicit Authorization
 - User Accounting

LO#04: Discuss cryptographic security techniques

- Cryptography
 - Encryption

CND Outline

- Symmetric Encryption
- Asymmetric Encryption
- Hashing: Data Integrity
- Digital Signatures
- Digital Certificates
- Public Key Infrastructure (PKI)

LO#05: Discuss various cryptographic algorithms

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- RC4, RC5, and RC6 Algorithms
- Digital Signature Algorithm (DSA) and Rivest Shamir Adleman (RSA)
- MD5
- Secure Hashing Algorithm (SHA)
- HMAC

LO#06: Discuss security benefits of network segmentation techniques

- Network Segmentation
- Network Segmentation Example: Demilitarized Zone (DMZ)

LO#07: Discuss various essential network security solutions

- Firewalls
 - How Does a Firewall Work?
 - Firewall Example: pFSense
- Intrusion Detection and Prevention System (IDS/IPS)
 - How does an IDS Work?
 - IDS Example: Snort
- Honeypot
 - Honeypot Example: KFSensor
- Proxy Server
 - Proxy Server Example: Squid Proxy
- Network Protocol Analyzer
 - Network Protocol Analyzer Example: Wireshark
- Web Content Filter
 - Web Content Filter Example: OpenDNS

CND Outline

- Load Balancer
- Unified Threat Management (UTM)
 - UTM Appliances Examples
- Security Information and Event Management (SIEM)
 - SIEM Example: Splunk
- Network Access Control (NAC)
 - NAC Examples
- Virtual Private Network (VPN)
 - VPN Example: OpenVPN

LO# 08: Discuss various essential network security protocols

- Network Security Protocols
 - RADIUS
 - TACACS+
 - Kerberos
 - 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)

Exercise 01: Implementing Role-Based Access Control using JEA

Exercise 02: Implementing Role-Based Access Control in Windows Admin Center (WAC)

Exercise 03: Implementing Proxy Server Using Squid Proxy

Exercise 04: Establishing VPN Connection using OpenVPN

Exercise 05: Establishing VPN Connection using SoftEther VPN

Perimeter Security

CNDv2 Module 04 Network Perimeter Security

LO#01: Understand firewall security concerns, capabilities, and limitations

- Firewalls security Concerns
- Why Firewalls are Bypassed?
- Firewall Capabilities

CND Outline

- Firewall Limitations

LO#02: LO#02: Understand different types of firewall technologies and their usage

- Firewall Technologies
 - Packet Filtering Firewall
 - Circuit Level Gateway
 - Application Level Firewall
 - Stateful Multilayer Inspection Firewall
 - Multilayer Inspection Firewall
 - Application Proxy
 - Network Address Translation
 - Virtual Private Network
 - Next Generation Firewall (NGFW)

LO#03: Understand firewall topologies and their usage

- Firewall Topologies
 - Bastion host
 - Screened subnet
 - Multi-homed firewall
 - Choosing Right Firewall Topology

LO#04: Distinguish between hardware, software, host, network, internal, and external firewalls

- Hardware vs Software-based Firewalls
- Host vs Network-based Firewalls
- External vs Internal Firewalls

LO#05: Select firewalls based on its deep traffic inspection capability

- Full Data Traffic Normalization
- Data Stream-based Inspection
- Vulnerability-based Detection and Blocking

LO#06: Discuss firewall implementation and deployment process

- Firewall Implementation and Deployment Process
 - Planning
 - Assess the need of implementing firewall
 - Things to Consider Before Implementing Firewalls
 - Points of consideration while implementing firewall
 - Factors to Consider before Purchasing any Firewall Solution
 - Configuring

CND Outline

- Hardware and software installation
- Creating and Configuring Firewall policies
 - Steps involved in creating a firewall policy
 - Conduct Periodic Review of Firewall Policies
- Creating and Configuring Firewall rules
 - Firewall Rules
 - Build an Appropriate Firewall Ruleset
 - How Does a Firewall Rule Work?
 - Example: The Packet Filter Firewall Ruleset
 - Firewall Rule Tester: Firewalk
- Configuring logging and alerting
 - Example: Smoothwall firewall logging
 - Example: Pfsense firewall logging
- Integrating firewall into network architecture
- Testing
- Deploying
- Managing and Maintaining

LO#07: Discuss recommendations and best practices for secure firewall Implementation and deployment

- Secure Firewall Implementation: Best Practices
- Secure Firewall Implementation: Recommendations
- Secure Firewall Implementation: Do's and Don'ts

LO#08: Discuss firewall administration concepts

- Accessing Firewall Platform
- Build Operating System Platform for Firewall
- Firewall Failover Strategies
- Firewall Logging
- Firewall Backups
- Security Incidents
- Deny Unauthorized Public Network Access
- Deny Unauthorized Access Inside the Network
- Restricting Client's Access to External Host

CND Outline

LO#09: Understand role, capabilities, limitations, and concerns in IDS deployment

- Intrusion Detection and Prevention Systems (IDS/IPS)
- Role of an IDS in Network Defense
- IDS Capabilities
- IDS/IPS Limitations
- IDS/IPS Security Concerns
- Common Mistakes in IDS/IPS Configurations

LO#10: Discuss IDS classification

- IDS Classification
 - Approach-based IDS
 - Anomaly and Misuse Detection Systems
 - Behavior-based IDS
 - Protection-based IDS
 - Structure-based IDS
 - Analysis Timing based IDS
 - Source Data Analysis based IDS

LO#11: Discuss various components of ID

- IDS Components
 - Network Sensors
 - Command Console
 - Alert Systems
 - Response System
 - Attack Signature Database
- Collaboration of IDS components in Intrusion Detection

LO#12: Discuss effective deployment of network and host-based IDS

- Staged IDS Deployment
- Deploying Network-based IDS
- Deploying a Host-based IDS

LO#13: Learn to how to deal with false positive and false negative IDS/IPS alerts

- What is an Alert?
- Types of IDS Alerts
 - True Positive Alerts

CND Outline

- False Positive Alerts
- False Negative Alerts
- True Negative Alerts
- What Should Be the Acceptable Level of False Alarms
- Calculating False Positive and False Negative Rates
- Dealing with a False Positive Alerts
- Dealing with a False Negative Alerts

LO#14: Discuss the considerations for selection of an appropriate IDS/IPS solutions

- Characteristics of a Good IDS Solutions
- IDS Product Selection Criteria
 - General Requirements
 - Security Capability Requirements
 - Performance Requirements
 - Management Requirements
 - Life Cycle Costs

LO#15: Discuss various NIDS and HIDS Solutions with their intrusion detection capabilities

Snort

- Intrusion detection with Snort
- Intrusion detection with Bro IDS and ELK
- Intrusion detection with Suricata
- Intrusion detection with OSSEC
- Intrusion detection with Wazuh

LO#16: Discuss router and switch security measures, recommendations, and best practices

- Why Secure a Router?
- Router Security Measures
- Why Switch Security is Important
- Switch Security Measures

LO#17: Leverage Zero Trust Model Security using Software-Defined Perimeter (SDP)

- Why Software Defined Perimeter (SDP)
- Traditional Security Drawbacks
 - 01: Attacks Comes from the Outside World Only, So Authenticating Outsiders is Enough
 - 02: Traditional Firewalls are Static in Nature
 - 03: Traditional VPN Gives Wide Access to Network Resources
 - 04: Lacks Identity-Centric Security and Access Model

CND Outline

- 05: Fails to Prevent Lateral Movement
- 06: Traditional Network Connectivity Model is Less Effective
- What is SDP?
- SDP Applications
- SDP Deployment Models
- SDP Architecture and Components
- SDP Advantages Over Traditional Network Access Control
- SDP Tools / Solutions

Exercise 01: Implementing Network-Based Firewall Functionality: Blocking Unwanted Website access using pfSense Firewall

Exercise 02: Implementing Network-Based Firewall Functionality: Blocking Insecure Ports using pfSense Firewall

Exercise 03: Implementing Network-Based Firewall Functionality: Blocking Insecure Ports using pfSense Firewall

Exercise 04: Implementing host-based firewall functionality using Windows Firewall

Exercise 05: Implementing host-based firewall functionality using IPTable

Exercise 06: Implementing network-based IDS functionality using Snort IDS

Exercise 07: Implementing network-based IDS functionality using Suricata IDS

Exercise 08: Implementing network-based IDS functionality using Bro IDS

Exercise 09: Implementing Host-based IDS functionality using Wazuh HIDS

Endpoint Security

CNDv2 Module 05 Endpoint Security-Windows Systems

LO#01: Understand Window OS and Security Concerns

- Windows Operating System
- Windows Architecture
- Windows Security and Concerns
 - Example: CVE Details-Windows 10 Security Vulnerabilities

LO#02: Discuss Windows Security Components

- Windows Security Components
 - Security Reference Monitor (SRM)
 - Local Security Authority subsystem (LSASS)
 - Security Account Manager (SAM)
 - SAM Database
 - Active Directory (AD)

CND Outline

- Authentication Packages
- Interactive logon manager (Winlogon)
- Logon user interface (LogonUI)
- Credential providers (CPs)
- Network logon service (Netlogon)
- Kernel Security Device Driver (KSecDD)

LO#03: Discuss Various Windows Security Features

- Windows Object Protection
- Windows Access Checks
 - Security Identifier (SID)
 - Viewing SID of all users using Process Explorer
 - Viewing SID of all users using Command Prompt
 - Viewing SID of all users using PowerShell
 - Viewing SID of all users in Windows Registry
- Windows Integrity Control
 - Viewing integrity levels of processes using Process Explorer
- Virtual Service Accounts
- Secure File Sharing
 - Assigning right permissions
 - Enabling Password Protections
 - Granting access permissions to share folder using Command Prompt
 - Revoking access permissions to share folder for everyone using PowerShell
 - Granting access permissions to share folder using PowerShell
- Security Auditing
 - Viewing Security Audit Event using PowerShell

LO#04: Discuss Windows Security Baseline Configurations

- Windows Security Baseline Configurations
 - Checking Windows Security Baseline Configuration Using Security Compliance Toolkit (SCT) Baseline

LO#05: Discuss Windows User Account and Password Management

- User Account Management
 - Disable Guest Account

CND Outline

- Disabling Active Accounts using Command Prompt
- Disabling Active accounts using PowerShell
- Disable Unnecessary Accounts
 - Disable Unnecessary Local Administrator Accounts
 - Disabling unnecessary Administrator Account using PowerShell
 - Disabling unnecessary Administrator Account using Command Prompt
- Password Management
 - Enforce Password Policy
 - Enabling Domain Password Policy using PowerShell
 - Password Age
 - Setting Password Age for Domain Password Policy using PowerShell
 - Password Length
 - Setting password length for Domain Password Policy using PowerShell
- Password Protection using Credential Guard

LO#06: Discuss Windows Patch Management

- Patch Management
 - Enable Automatic Updates
 - Enabling Automatic Updates using Windows Registry
 - Enabling Automatic Updates using PowerShell
 - Enabling Automatic Updates using Command Prompt
 - Disable Force System Restarts
 - Remote Patch Management
 - Remote Patch Management using BatchPatch
 - Remote Patch Management using ManageEngine Patch Manager Plus

LO#07: Discuss User Access Management

- Restricting Access to Files and Folders
 - Restricting access to folder using PowerShell
- Prevent Unauthorized Changes in System
 - Turn on User Account Control using PowerShell
- Disable Anonymous Security Identifiers Enumeration
- Moderating Access to Control Panel
- Control Access to Command Prompt

CND Outline

- Administrative Access Management using Just Enough Administration (JEA)

LO#08: Windows OS Security Hardening Techniques

- Set up BIOS Password
- Prevent Windows from Storing LAN Manager Hash
- Restrict Software Installations
- Disable Unwanted Services
 - Disabling Windows Service using PowerShell
- Install Antivirus Software
- Enable Windows Firewall
 - Viewing Firewall Status using PowerShell
 - Getting Firewall Rules using PowerShell
- Monitor Windows Registry
 - Viewing Registry key data using PowerShell

LO#09: Discuss Windows Active Directory Security Best Practices

- Cleaning Domain Admins Group
- Local Administrator Password Solution (LAPS)
- Disable NTLM and NTLMv2 Protocols
- Monitor Active Directory Events for Signs of Compromise
- PowerShell Cmdlets for Securing Active Directory
 - View Default Password Policy
 - View accounts having Password Set to Never Expire
 - Force user to change password at Next Login
 - Disable user account and list all disabled accounts
 - Search for Locked Out users
 - Search for Locked Out users and Unlock the locked users
 - View Users Login details
 - Disable Inactive accounts
- Active Directory Security Best Practices
 - General Recommendations
 - Protect Admin Credential
 - Protect Resources
 - Protect Service Account Credentials

CND Outline

- Protect Workstations and Servers
- Protect Domain Controllers
- Logging

LO#10: Discuss Windows Network Services and Protocol Security

- Secure PS Remoting Endpoints
 - Enable PowerShell Logging
 - Disable PowerShell V 2.0
 - Enforce Script Signing for PowerShell Scripts
 - Use ConstrainedLanguageMode of PowerShell
 - PS Remoting Security Recommendations
- Securing Remote Desktop Protocol (RDP)
 - Limit the Number of RDP Users
 - Scoping RDP Firewall Rule
 - Implementing RDP Gateways
 - Enabling Network Level Authentication (NLA) in RDP Server and Client
 - Enabling NLA using Windows PowerShell
 - Protecting Credentials Over RDP
- DNSSEC
 - Managing DNSSEC for your Domain Name
 - Securing DNS with DNSSEC
 - How does DNSSEC Protect Internet Users
 - Monitor DNS Logs for Security Threats
- Server Message Block (SMB) protocol
 - Disable SMB 1.0
 - Enable SMB Encryption
 - Enable SMB Encryption with Windows PowerShell

CND Outline

Exercise 01: Basic Network Administration and Troubleshooting Using Windows Command Line Utilities

Exercise 02: Analyzing Security Configuration Baseline Using Microsoft Security Compliance Toolkit

Exercise 03: Remote Patch Management using BatchPatch

Exercise 04: Remote Patch Management using ManageEngine Patch Manager Plus

Exercise 05: Delegating Admin Permission to User Using Delegation of Control Wizard

Exercise 06: Securing Local Administrator Password using LAPS

Exercise 07: Securing Windows File Share in Active Directory

CNDv2 Module 06 Endpoint Security-Linux Systems

LO#01: Understand Linux OS and security concerns

- Linux OS
- Linux Features
- Linux Security Concerns

LO#02: Discuss Linux Installation and Patching

- Enable Minimal Installation Option
- Password Protect BIOS and Bootloader
- Linux Patch Management
- Linux Hardening Checklist: System Installation and Patching

LO#03: Discuss Linux OS Hardening Techniques

- Disabling Unnecessary Services
- Remove or Uninstall Unnecessary Software's / Packages
- Install Antivirus
- Linux Hardening Checklist: OS Hardening

LO#04: Discuss Linux User Access and Password Management

- Enforce Strong Password Management
- Restrict User from Using Previous Passwords
- Ensure No Accounts Have Empty Passwords
- Disable Unnecessary Accounts
- Secure Shared Memory
- Delete X Window Systems (X11)
- Create Separate Disk Partitions for Linux System
- Enable Disk Quota for All Users
- Understanding and Checking Linux File Permissions
- Changing File Permissions

CND Outline

- Check and Verify Permissions for Sensitive Files and Directories
- Disable Unwanted SUID and SGID Binaries
- Remove or Rectify the permissions for World-Writable Files
- Disable USB Storage
- Linux Hardening Checklist: User Access and Passwords

LO#05: Discuss Linux Network Security and Remote Access

- Configure sysctl to Secure Linux Kernel
- Host-based Firewall Protection with Iptables
- TCP Wrappers
- Monitor Open Ports and Services
- Turn Off IPv6 if Not In Use
- Secure SSH Login Root Login
- Setup Chroot SFTP
- Linux Hardening Checklist: Network Security and Remote Access

LO#06: Discuss Various Linux Security Tools and Frameworks

- Security Auditing and System Hardening using Lynis
- Turn On AppArmor
- Turn on Security-Enhanced Linux (SELinux)
- Audit Linux System for Security Compliance using OpenSCAP
- Additional Linux Hardening Tools

Exercise 01: Implementing Linux security Best Practices

Exercise 02: Implementing Name-based Mandatory Access Controls Using AppArmor

Exercise 03: Linux Security Auditing and System Hardening Using Lynis

CNDv2 Module 07 Endpoint Security- Mobile Devices

LO#01: 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)

CND Outline

- COBO Policy Implementation

LO#02: 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

LO#04: Discuss and implement various enterprise-level mobile security management Solutions

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Mobile Threat Defense (MTD)
- Unified endpoint management (UEM)
- Mobile Email Management (MEM)
- Mobile Content Management (MCM)
- Enterprise Mobility Management (EMM)

LO#05: 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
- SMS Phishing Countermeasures

LO#06: Discuss Security guidelines and tools for Android devices

- Android Device Administration API
- Securing Android Devices
- Android Security Tool: Find My Device
- Android Security Tools
- Android Vulnerability Scanner
- Android Device Tracking Tools

LO#07: Discuss Security guidelines and tools for iOS devices

- Guidelines for Securing iOS Devices
- iOS Device Tracking Tools
- iOS Device Security Tools

CND Outline

Exercise 01: Implementing Enterprise Mobile Security Using Miradore MDM Solution

Exercise 02: Implementing Enterprise Mobile Security Using COMODO (ITarian) MDM Solution

CNDv2 Module 08 Endpoint Security-IoT Devices

LO#01: Understanding IoT Devices, their need and Application Areas

- What is IoT?
- Why Organization are Opting for IoT-enabled Environments
- IoT Application Areas and Devices

LO#02: Understanding IoT Ecosystem and Communication models

- IoT Architecture
- Layers of IoT Architecture
 - Device Layer
 - Communication Layer
 - Cloud Platform Layer
 - Process Layer
- IoT Communication Models
- IoT-Enabled IT Environment

LO#03: Understand Security Challenges and risks associated with IoT-enabled environments

- Security Challenges IoT Enabled Environments
- Inherent Security issues with IoT Devices
- IoT Threat Landscape and Impact
- Attack Vectors in IoT Architecture
- DDOS Attack From Hacked IoT Device
- OWASP TOP 10 IoT Vulnerabilities

LO#04: Discuss the security in IoT-enabled environments

- Understanding the Attack Scenario in IoT-enabled Environment
- Security in IoT- enabled Environments
- Stack-wise IoT Security Principles
 - Secure Device Layer
 - Secure Communication Layer
 - Secure Cloud Platform Layer
 - Secure Process Layer
- Securing Device Layer: Attacks and Respective Countermeasures

CND Outline

- Secure Communications Layer: Attacks and Respective Countermeasures
- Secure Cloud Layer: Attacks and Respective Countermeasures
- Secure Process Layer: Attacks and Respective Countermeasures

LO#05: Discuss Security Measures for IoT enabled IT Environments

- Have Complete Visibility on IoT Devices
- Create IoT Assets Map
- Monitor Behavior of IoT Device
- Ensure Security at IoT Ecosystem Interfaces
- Use Proper Network Segmentation to Isolate IoT Devices
- Place IoT Device on Segmented Network
- Create Virtual LAN pipe dynamically to connect to IoT device
- Limit Access to IoT Devices
- Always Look out for latest Malware and Ransomware on IoT
- Understand the Threat Landscape of IoT devices
- Scan the IoT Device for Known Vulnerabilities
- Update Your IoT device Firmware with latest Patches and Upgrades
- Deploy End-to-End Encryption on IoT devices
- Implement End to End Security and Identity Management
- Enforce Strong Authentication
- Close Insecure Network services
- Ensure Chip-Level Security of IoT Device
- Ensure Hardware Security
- Secure IoT Gateways
- Secure IoT Control Servers
- Secure Remote Administration of IoT Devices
- Secure Router of IoT Connected Devices
- Isolate IoT Devices when Connected to Wi-Fi
- Isolate IoT Devices when Connected to Ethernet
- Control Internet Access for IoT device
- Monitor Network Activity of IoT Device
- Monitor Bandwidth Consumption of IoT device
- Centralize Access Logs of IoT devices
- Manage Risk from Shadow IoT Devices

CND Outline

LO#06: Discuss IoT Security Tools and Best Practices

- IoT Security Best Practices
- IoT Security Tools

LO#07: Discuss and refer various standards, Initiatives and Efforts for IoT Security

- AIOTI WG03: IoT Standardisation
- Internet of Things Cybersecurity Improvement Act of 2019
- NIST Security Feature Recommendations for IoT Devices
- US DHS Strategic Principles for Securing IoT
- GSMA IoT Security Guidelines and Assessment
- Standards for Potential IoT Attacks and Vulnerabilities
- Additional Standards, Initiatives and Efforts for IoT Security

Exercise 01: Securing IoT Device Communication Using TLS\SSL

Application Security

CNDv2 Module 09 Administrative Application Security

- Application Security Administration
- Application Security Administration Practices

LO#01: Discuss and implement Application Whitelisting and Blacklisting

- Application Whitelisting
- Application Blacklisting
- Using Software Restriction Policies (SRP) for Application Whitelisting
- Using AppLocker for Application Whitelisting
- Using McAfee Application Control for Application Whitelisting
- Using ManageEngine Desktop Central for Application Blacklisting
- Using Windows PUA (Potentially Unwanted Applications) Protection Feature
- Using Group policies for Blocking Software Installation from Users
- Using Registry for Blocking Certain Apps
- Application Whitelisting Tools

LO#02: Discuss and implement application Sandboxing

- Application Sandboxing
 - Application Sandbox Examples
- Run Applications in Windows Sandbox
- Sandboxing in Linux: Firejail
- Sandboxing Approaches in Linux

CND Outline

- Sandboxing Tool: Sandboxie
- Windows Defender Application Guard: Microsoft Edge

LO#03: Discuss and implement Application Patch Management

- Application Patch Management
- Software Patch Management for third-party software using Patch Manager
- Application Patch Management Solutions and Tools

LO#04: Discuss and implement Web Application Firewall (WAF)

- Web Application Firewall (WAF)
 - Benefits of WAF
 - WAF Limitations
- Configuring URLScan to setup as WAF For IIS Server
- Open Source WAFs for Web Application Security

Exercise 01: Implementing Application whitelisting using AppLocker

Exercise 02: Implementing Application whitelisting using SRP

Exercise 03: Implementing Application Security Using Firejail Sandbox

Exercise 04: Deploying and implementing URLscan as WAF

Data Security

CNDv2 Module 10: Data Security

LO#1: 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

LO##2: Discuss the implementation of data access controls

- Logical Implementation of Access Controls
- Access Controls List (ACL)
 - Setting Access Controls and Permission to Files and Folders in Windows
 - Setting Access Controls and Permission to Files and Folders in Linux
- Group Policy
- Passwords /Access Token

CND Outline

- Account Restrictions
 - Restricting Logon Hours for Linux Users

LO#03: Discuss the implementation of Encryption of Data at rest

- Encrypting “Data-at-Rest”
- Disk Encryption
 - Implementing Built-in Disk Encryption for Windows
 - Implementing Built-in Disk Encryption for MacOS
 - Implementing Built-in Disk Encryption in Linux
 - Implementing Built-in Disk Encryption in Android Devices
 - Implementing Built-in Disk Encryption in iOS devices
 - Third Party Disk Encryption Tools
- File Level Encryption
 - Implementing Built-in File System-level Encryption on Windows
 - Third-Party Windows File Encryption Tools
 - Implementing Built-in File System-level Encryption on MacOS
 - Third-Party Linux File Encryption Tools
- Removable Media Encryption
 - Implementing Removable Media Encryption in Windows
 - Implementing Removable Media Encryption in Mac
 - Implementing Removable Media Encryption in Linux
- Database Encryption
 - MS SQL Server
 - Implementation of Transparent Database Encryption in MS SQL Server
 - Encryption: Implementation of Column-level Encryption in MS SQL Server
 - Implementation of Always Encrypted in MS SQL Server
 - Oracle
 - Implementation of Transparent Data Encryption in Oracle

LO#04: Discuss the implementation of Encryption of “Data at transit”

LO#4.1: Discuss the implementation of Encryption of “Data at transit” between browser and web server

- Secure HTTP Connection using Digital Certificate
- Viewing a Digital Certificate
 - Version 1 Fields

CND Outline

- Extensions
- Certificate Path
- Root Certificate
- Install and Configure SSL Certificate on Windows Server
- Backing Up and Exporting Digital Certificate in Windows Server
- Renew Certificate
- Revoke Certificate

LO#4.2: Discuss the implementation of Encryption of “Data at transit” between database server and web server

- Enabling Encrypted connections for an instance of the SQL Server Database Engine
- Enabling SSL/TLS encryption in Oracle Server

LO#4.3: Discuss the implementation of Encryption of “Data at transit” in Email Delivery

- Email Encryption
 - MS Outlook
 - Gmail

LO#05: Discuss Data Masking Concepts

- Data Masking
- Implementing Dynamic Data Masking in SQL Server
- Implementing Data Masking in Oracle Database
- Data Masking Tools

LO#06: Discuss data backup and retention

- Introduction to Data Backup
- Data Backup Strategy/Plan
- Identify Critical Business Data
- Selecting the Backup Media
- Examples of Data Backup Media Devices
- RAID (Redundant Array Of Independent Disks) Technology
 - Advantages/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

CND Outline

- RAID Level 10: Blocks Striped and Mirrored
- RAID Level 50: Mirroring and Striping across Multiple RAID Levels
- Selecting Appropriate RAID Levels
- Hardware and Software RAIDs
- Using RAID Best Practices
- Storage Area Network (SAN)
 - SAN Advantages
 - SAN Backup Best Practices
 - SAN Data Storage and Backup Management Tools
- Network Attached Storage (NAS)
 - NAS Implementation Types: Integrated NAS System
 - Examples of Integrated NAS System
 - NAS Implementation Types: Gateway NAS System
 - Gateway NAS System: FreeNAS
- Selecting an Appropriate Backup Method
- Choosing the Backup Location
- Types of Backup
- Backup Types: Advantages and Disadvantages
- Windows Data Backup: Disk, file and folders Backup
- Third-Party Windows Data Backup Tools
- Linux Data Backup: Disk, file and folders Backup
- Third-Party Linux Data Backup Tools
- Mac OS Data Backup: Disk, file and folders Backup
- Third-party MAC OS Data Backup Tools
- Database Backup: MS SQL Server
- Database Backup: Oracle
- Email Backup: Outlook
- Email Backup : Gmail
- Email Backup Tools
- Web Server Configuration Backup: IIS
- Website Back Up
- Data Backup Retention
- Data Retention Policy Best practices

CND Outline

LO#07: Discuss Data Destruction Concepts

- Data Destruction
- Data Destruction Policy
- Data Destruction Techniques
- Disk Wipe: Windows Diskpart Utility
- Data Destruction Tools
- Data Destruction Best Practices

LO#08: Data Loss Prevention Concepts

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

Exercise 01: Encrypting data at rest using VeraCrypt

Exercise 01: Implementing Encryption on SQL Server Database using Transparent Database Encryption (TDE) Method

Exercise 01: Implementing Always Encrypted feature in SQL Server

Exercise 02: Encrypting data in transit using SSL

Exercise 03: Ensuring Secure Email Communication using PGP

Exercise 04: Performing Data Backup Using AOMEI Backupper Standard

Exercise 05: File Recovery Using EaseUS Data Recovery Wizard

Exercise 05: File recovery using quick recovery tool

Exercise 06: Partition Recovery Using MiniTool Power Data Recovery Tool

Security in Modern Network Technologies

CNDv2 Module 11: Enterprise Virtual Network Security

LO#01: Discuss the evolution of network and security management concept in modern Virtualized IT Environments

- Evolution of Network Management in Modern IT Environment
- Security Management in Evolved Network Management

LO#02: Understand Virtualization Essential Concepts

- Virtualization Concept
- Virtualization Components
- Virtualization Enablers

CND Outline

- Network Virtualization (NV)
- Software Defined Network (SDN)
- Network Function Virtualization (NFV)

LO#03: Discuss Network Virtualization (NV) Security

- Network Virtualization (NV)
- Virtual Networks
- Virtual Network Categories: Internal Virtual Network
 - Hypervisor Products
 - Internal Virtual Network Example: Internal Virtual Network using VMware ESX Server 3
- Virtual Network Categories: External Virtual Network
 - Layer 3 intelligent/managed switches Vendors
 - External Virtual Network Example: VLANs
- Vulnerabilities in Hypervisor/VMM
- Vulnerabilities in Virtual Networks
 - VLAN Attacks
- Hypervisor Security
 - Hyper-V Security
 - Time Synchronization
 - Set Privilege Access to the Users
 - Disable Unnecessary Services
 - Isolated User Mode (IUM)
 - Enable Server Message Block (SMB) 3.0
 - VM Ware Security
 - Time Synchronization
 - Restrict User Access
 - Encrypting Guest Virtual Machines
 - Virtual Box Security
 - Disable Nested Paging
 - Disable Hyperthreading
 - Flush level 1 cache data
 - Additional Hypervisor Security guidelines, Recommendation, and Best Practices
 - Virtual Network Security Recommendations

CND Outline

- VLAN Security
 - VLAN Security Best Practices

LO#04: Discuss SDN Security

- Software Defined Network (SDN)
- SDN Benefits
- SDN Limitations
- SDN Security Limitations
- SDN-Specific Vulnerabilities and Attacks
- SDN Security Principles
- SDN Security Measures
 - Application Plane
 - Control Plane
 - Data Plane
 - SDN Layer
- SDN Attack- Specific Countermeasures

LO#05: Discuss Network Function Virtualization (NFV) Security

- Network Function Virtualization (NFV)
- NFV Vulnerabilities
- NFV Infrastructure Security
 - Protect Operational Interface
 - Protect against Resource Freeing Attacks (RFA) and Resource Consumption Attacks
 - Protect Outsourcing workload to a third party
 - Protect Live Migration (Relocating VNFs without service interruption)
 - Prevent Noisy neighbor
 - Prevent Side-channel Attacks
 - Protect the scaling and elasticity of VNF
- NFV Security Best Practices

LO#06: Discuss OS Virtualization Security

- Container
- Container Technology Architecture
- Containers Vs Virtual Machine
- Docker
- Docker Networking

CND Outline

- Kubernetes
- Container Security Challenges
- Container Security Threats
- Docker Security Threats
- Kubernetes Security Threats

LO#07: Discuss Security Guidelines, Recommendations and Best Practices for Containers

- Container Security
 - Container Hardening
 - Securing Container Image
 - Managing Container Secrets
 - Container Runtime Security
- NIST Recommendations to Secure Containers
- Container Security Best Practices

LO#08: Discuss Security Guidelines, Recommendations and Best practices for Dockers

- Docker Security Features
- Docker Security
 - Enable Docker Content Trust
 - Set Resource Limits for Containers
 - Select Third-Party Tools Carefully
 - Use Third-Party Security Tool
- Docker Image Security Best Practices

LO#09: Discuss Security Guidelines, Recommendations and Best Practices for Kubernetes

- Know the Base Image When Building Containers
- Use Namespaces to Create Security Boundaries
- Restrict Linux Capabilities
- Enable RBAC with Least Privilege, Disable ABAC
- Ensure communication over TLS
- Audit Logs
- Implement Network policies
- Secure Kubernetes Cluster With Pod Security Policies
- Use Kubernetes Secrets
- Kubernetes Security Tools
- Compliance and Auditing: CIS Benchmark

CND Outline

Exercise 01: Auditing Docker Host Security Using Docker-Bench-Security Tool

Exercise 02: Securing SDN communication between Switch and SDN Controller using SSL

CNDv2 Module 12: Enterprise Cloud Security

LO#01: Understand Cloud Computing Fundamentals

- Cloud Computing
- Cloud Computing Benefits
- Types of Cloud Service Modules
- Customer vs CSP Shared Responsibilities in IaaS, PaaS, and SaaS
- Cloud Deployment Models
- NIST Cloud Deployment Reference Architecture

LO#02: Understanding the Insights of Cloud Security

- Cloud Security: Shared Responsibility
- Elements of Cloud Security: Consumers Vs Providers
 - Identity and Access Management (IAM)
 - Data Storage Security
 - Network Security
 - Monitoring
 - Logging
 - Compliance

LO#03: Evaluate CSP for Security before Consuming Cloud Service

- Major Cloud Service Providers
- Evaluate the CSP
- Security Features Provided By AWS, Azure, and GCP
- On-premises vs 3rd Party Security Controls Provided by Major CSP

LO#04: Discuss security in Amazon Cloud (AWS)

- AWS Security: Understand AWS Shared Responsibility Model
 - Shared Responsibility Model: Infrastructure Services
 - Shared Responsibility Model: Container Services
 - Shared Responsibility Model: Abstract Services
- AWS Identity and Access Management
 - Lock Away Your AWS Account Root User Access Keys
 - Create Individual IAM Users
 - Use Groups to Assign Permissions to IAM Users

CND Outline

- Grant Least Privilege
- Use AWS Managed Policies
- Use Customer Managed Policies Instead of Inline Policies
- Use Access Levels to Review IAM Permissions
- Configure a Strong Password Policy for Users
- Enabling MFA for Privileged Users
- Use Roles for Amazon EC2 Instances
- Rotate Security Credentials Regularly
- Use Roles to Delegate Permissions and Do not Share Access Keys
- Remove Unnecessary Credentials
- Monitor Activity of AWS Account
- AWS Encryption
 - Encrypting Data at Rest
 - Amazon S3
 - Cloud HSM
 - Data in Transit
- AWS Network Security
 - VPC and Other AWS Network Security Measures
 - Strengthening AWS Network Security
- AWS Storage Security
 - Amazon S3
 - Amazon EBS
 - Data Identification and Classification
- AWS Monitoring and Logging
 - AWS Inspector
- AWS Secured Solution Design
- AWS Security Checklist

LO#05: Discuss security in Microsoft Azure Cloud

- Azure Security: Understand Azure Shared Responsibility Model
- Azure IAM security
 - Centralize Identity Management
 - Implementing password hash synchronization with Azure AD Connect sync

CND Outline

- Enabling Single-Sign-on (SSO)
- Turn on Conditional Access
- Enabling password management
- Enforce multi-factor authentication (MFA) for users: Azure Multi-Factor Authentication
- Enforce multi-factor authentication (MFA) for users: cloud-based Multi-Factor Authentication
- Enforce multi-factor authentication (MFA) for users: Azure AD Identity Protection
- Implementing role based access control (RBAC)
- Restrict Exposure of privileged accounts
- Azure Encryption and Key Management
 - Azure: Encryption Data at Rest
 - Azure: Encryption Data in transit
- Azure Network security
 - Secure Inbound Internet communications to VMs using SSL
 - Configure endpoint access control list (ACL)
 - Disabling RDP/SSH Access to virtual machines
 - Optimize uptime and performance: Load balancing
 - Deploy perimeter networks for security zones
 - Logically segment subnets
- Azure storage security
 - Active geo-replication
- AZURE Monitoring, Logging, and Compliance
 - Azure Security Center
 - Azure Management Portal
 - Activity Log
 - Network Watcher
- Azure Secured Solution Design
- Azure Security Checklist

LO#06: Discuss security in Google Cloud Platform (GCP)

- Understand Google Cloud Shared Responsibility Model
- GCP IAM
 - Grant Least Privileges
 - Avoid Primitive Roles

CND Outline

- Grant Pre-defined Roles
- Create separate service account
- Check Granted Policy on Each Resource
- Restrict who act as service accounts
- Restrict access to create and manage service accounts
- Grant Pre-defined Roles
- Service accounts and service account keys
 - Use Logging Roles for log Auditing
- GCP Encryption
 - Cloud KMS
 - Create Key Ring and Encryption Key
- GCP Network security
- Defense-in-depth Network Security Principles
 - Use VPC to define your network
 - Centralize Network Control
 - Manage Traffic with Firewall Rules
 - Use Routes
- GCP Monitoring, logging and compliance
 - GCP Console
 - Cloud Audit Logs
 - Stackdriver
 - GCP Compliance
- GCP Secured Solution Design
- Google Security Checklist

LO#07: Discuss general security best practices and tools for cloud security

- Best Practices for Securing Cloud
- NIST Recommendations for Cloud Security
- Organization/Provider Cloud Security Compliance Checklist
- Cloud Security Tools
 - Qualys Cloud Platform
 - CloudPassage Halo
 - Scout Suite
 - Core CloudInspect

CND Outline

Exercise 01: Implementing AWS Identity and Access Management

Exercise 02: Implementing Key Management Services

Exercise 03: Securing AWS Storage

CNDv2 Module 13: Wireless Network Security

LO#01: Understand wireless network fundamentals

- Wireless Terminologies
- Wireless Networks
 - Advantages of Wireless Networks
 - Disadvantages of Wireless Networks
- Wireless Standard
- Wireless Topologies
 - Ad-hoc Standalone Network Architecture (IBSS - Independent Basic Service Set)
 - Infrastructure Network Topology (Centrally Coordinated Architecture/ BSS - Basic Service Set)
- Typical Use of Wireless Networks
 - Extension to a Wired Network
 - Multiple Access Points
 - LAN-to-LAN Wireless Network
 - 4G Hotspot
- 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

CND Outline

- Yagi Antenna
- Reflector Antennas

LO#02: Understand wireless network encryption mechanisms

- WEP (Wired Equivalent Privacy) Encryption
- WPA (Wi-Fi Protected Access) Encryption
- WPA2 Encryption
- WEP vs. WPA vs. WPA2

LO#03: Understand wireless network authentication methods

- Wi-Fi Authentication Method
 - Open System Authentication
 - Shared Key Authentication
- Wi-Fi Authentication Process Using a Centralized Authentication Server

LO#04: Discuss and implement wireless network security measures

- Wireless Network Security
 - Creating Inventory of Wireless Devices
 - Placement of Wireless AP
 - Placement of Wireless Antenna
 - Disabling SSID Broadcasting
 - Selecting Stronger Wireless Encryption Mode
 - Implementing MAC Address Filtering
 - Monitoring Wireless Network Traffic
 - Defending Against WPA Cracking
 - Passphrases
 - Client Settings
 - Passphrase Complexity
 - Additional Controls
 - Detecting Rogue Access Points
 - Wireless Scanning:
 - Wired-side Network Scanning
 - SNMP Polling
- Wi-Fi Discovery Tools
 - inSSIDer and NetSurveyor
 - Vistumbler and NetStumbler

CND Outline

- Locating Rogue Access points
- Protecting from Denial-of-Service Attacks: Interference
- Assessing Wireless Network Security
- Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer
- WPA Security Assessment Tool
 - Elcomsoft Wireless Security Auditor
 - Cain & Abel
- Wi-Fi Vulnerability Scanning Tools
- Deploying Wireless IDS (WIDS) and Wireless IPS (WIPS)
 - Typical Wireless IDS/IPS Deployment
- WIPS Tool
 - Adaptive Wireless IPS
 - AirDefense
- Configuring Security on Wireless Routers
- Additional Wireless Network Security Guidelines

Exercise 1: Configuring Security on Wireless Router

3. DETECT

CNDv2 Module 14: Network Traffic Monitoring and Analysis

LO#01: Understand the need and advantages of network traffic monitoring

- Network Traffic Monitoring
- Need of Network Monitoring
- Advantages of Network Monitoring

LO#02: Setting up the environment for network monitoring

- Network Sniffers for Network Monitoring
- How Do Network Sniffers Work?
- Positioning your Machine at the Appropriate Location
- Connecting Your Machine to a Managed Switch

LO#03: Determine baseline traffic signatures for normal and suspicious network traffic

- Network Traffic Signatures
 - Normal Traffic Signature
 - Attack Signatures
- Baseline Normal Traffic Signatures

CND Outline

- 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

LO#04: Perform network monitoring and analysis for suspicious traffic using Wireshark

- Wireshark
- Understanding Wireshark Components
- Monitoring and Analyzing FTP Traffic
- Monitoring and Analyzing TELNET Traffic
- Monitoring and Analyzing HTTP Traffic
- Detecting OS Fingerprinting Attempts
 - Detecting Passive OS Fingerprinting Attempts
 - Detecting Active OS Fingerprinting Attempts
 - Detecting ICMP Based OS Fingerprinting
 - Detecting TCP Based OS Fingerprinting
 - Examine Nmap Process for OS Fingerprinting
- Detecting PING Sweep Attempt
- Detecting ARP Sweep/ ARP Scan Attempt
- Detecting TCP Scan Attempt
 - TCP Half Open/ Stealth Scan Attempt
 - TCP Full Connect Scan
 - TCP Null Scan Attempt
 - TCP Xmas Scan Attempt
- Detecting SYN/FIN DDOS Attempt
- Detecting UDP Scan Attempt
- Detecting Password Cracking Attempts

CND Outline

- Detecting FTP Password Cracking Attempts
- Detecting Sniffing (MITM) Attempts
- Detecting the Mac Flooding Attempt
- Detecting the ARP Poisoning Attempt
- Monitoring and Analyzing Traffic for SQL Injection Attempt

LO#06: Discuss network performance and bandwidth monitoring tools and techniques

- Network Performance Monitoring (NPM)
- Network Performance Monitoring and Analysis using the PRTG Network Monitor
- Bandwidth Monitoring
- Bandwidth Monitoring - Best Practices

Exercise 01: Capturing Network Traffic using Wireshark

Exercise 02: Analyzing and Examining Various Network Packet Headers using Wireshark

Exercise 03: Analyzing and Examining Various Network Packet Headers in Linux using tcpdump

Exercise 04: Applying Various Filters in Wireshark

Exercise 05: Detecting Clear-Text Traffic using Wireshark

Exercise 06: Monitoring and Detecting Network Reconnaissance, Access, and DoS/DDoS Attempts

Exercise 07: Detecting Brute Force Attempt using Wireshark

Exercise 08: Detecting SQL Injection Attack using Wireshark

Exercise 09: Network Traffic Monitoring using PRTG

Exercise 10: Network Traffic Analysis Using Capsa

Exercise 11: Network Traffic Bandwidth Monitoring using NTOP

CNDv2 Module 15: Network Logs Monitoring and Analysis

LO#01: Understand logging concepts

- Logs
- Typical Log Sources
- Need of Log
- Logging Requirements
- Typical Log Format
- Logging Approaches
 - Local Logging
 - Centralized Logging

LO#02: Discuss log monitoring and analysis on Windows systems

- Windows Logs

CND Outline

- Windows Log
- Windows Event Log Types and Entries
- Event Types
- Monitoring and Analysis of Windows Logs
 - Finding Events in a Log
 - Examining Event Log Entries

LO#03: Discuss log monitoring and analysis on Linux

- Linux Log
 - Different Linux Log Files
 - Linux Log Format
 - Severity Level and Value of Linux Logs
 - Monitoring and Analysis of Linux Logs

LO#04: Discuss log monitoring and analysis on Mac

- Mac Logs
 - Mac Logs
 - Types of Logs in Mac
 - Mac Log Files
 - Log Format in Mac System
 - Monitoring and Analysis of Mac Logs

LO#05: Discuss log monitoring and analysis in Firewall

- Firewall Logs
 - Firewall Logging
 - Monitoring and Analysis of Firewall Logs
 - Monitoring and Analysis of Windows Firewall Log
 - Monitoring and Analysis of IP Tables logs
 - Monitoring and Analysis of Firewall Log in Mac
 - Monitoring and Analyzing Cisco ASA Firewall Logs
 - Monitoring and Analyzing CheckPoint Firewall Logs

LO#06: Discuss log monitoring and analysis on Routers

- Cisco Router Log
- Monitoring and Analysis of Router Logs

CND Outline

LO#07: Discuss log monitoring and analysis on Web Servers

- Internet Information Services (IIS) Logs
- Monitoring and Analyzing Log Files in IIS
- Apache Logs
- Monitoring and Analysis of Apache Log

LO#08: Discuss centralized log monitoring and analysis

- Centralized Logging
 - Why Centralized Logging?
 - Centralized Logging
 - Centralized Logging Infrastructure
 - Centralized Logging, Monitoring, and Analysis Process
 - Log Collection
 - Log Transmission
 - Example: Syslog Log Transport Mechanism
 - Syslog Tools
 - Log Storage
 - Log Normalization
 - Log Correlation
 - Micro-level Correlation
 - Macro-level Correlation
 - Log Analysis
 - Log Analysis Approaches
 - Manual Log Analysis
 - Automated Log Analysis
 - Log Analysis Best Practices
 - Alerting and Reporting
 - Centralized Logging Best Practices
 - Centralized Logging/Log Management Tools
 - Centralized Logging Challenges

CND Outline

Exercise 01: Configuring, Viewing and Analyzing Windows Event Logs

Exercise 02: Configuring, Viewing and Analyzing IIS Logs

Exercise 03: Configuring, Viewing and Analyzing Logs in Centralized Location Using Splunk

Exercise 04: Identifying Suspicious Activities Using Log Monitoring and Analysis

4. RESPOND

CNDv2 Module 16 Incident Response and Forensic Investigation

LO#01: Understand incident response concept

- Incident Handling and Response
- Incident Response Team Members: Roles and Responsibilities

LO#02: Understand the role of first responder in incident response

- First Responder
 - Network Administrators as First Responder
 - What Should You Know?

LO#03: Discuss Do's and Don't in first response

- Avoid Fear, Uncertainty and Doubt (FUD)
- Make an Initial Incident Assessment
- Determining Severity Levels
- Communicate the Incident
- Contain the Damage: Avoid Further Harm
- Control Access to Suspected Devices
- Collect and Prepare Information about Suspected Device
- Record Your Actions
- Restrict Yourself from Doing Investigation
- Do Not Change the State of Suspected Device
- Disabling Virus Protection

LO#04: Describe incident handling and response process

- Incident Handling and Response Process
- Overview of IH&R Process Flow
 - Preparation for Incident Handling and Response
 - Detection and Analysis
 - Classification and Prioritization
 - Incident Prioritization

CND Outline

- Notification and Planning
- Containment
 - Guidelines for Incident Containment
- Eradication and Recovery
 - Countermeasures
 - Systems Recovery
- Post-incident Activities
 - Incident Documentation
 - Incident Damage and Cost Assessment
 - Review and Update the Response Policies
- Training and Awareness

LO#05: Describe forensics investigation process

- Forensic Investigation
- Network Forensics Investigation
- People Involved in Forensics Investigation
- Typical Forensics Investigation Methodology

Exercise 1: Working with Incident Tickets in OSSIM

CNDv2 Module 17 Business Continuity and Disaster Recovery

LO#01: Introduction to Business Continuity (BC) and Disaster Recovery (DR) concepts

- Business Continuity (BC)
 - Objectives of Business Continuity
- Disaster Recovery (DR)
 - Objectives of Disaster Recovery
- Business Continuity Management (BCM)
 - BCM Goals
- Business Impact Analysis (BIA)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)

LO#02: Discuss BC/DR Activities

- BC/DR Activities
 - Prevention
 - Response
 - Resumption

CND Outline

- Recovery
- Restoration

LO#03: Explain Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

- Business Continuity Plan (BCP)
 - BCP Goals
- Disaster Recovery Plan (DRP)
 - DRP Goals

LO#04: Discuss BC/DR Standards

- ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2012 Societal security — Business continuity management systems — Guidance
- ISO/IEC 27031:2011/ISO/IEC 27031:2011 (Information Technology-Security Techniques— Guidelines for Information and Communication Technology Readiness for Business Continuity)

Exercise 1: Implementing Business Continuity and Disaster Recovery Using Network Load Balancing (NLB)

5. PREDICT

CNDv2 Module 18 Risk Anticipation with Risk Management

LO#01: Understand risk management concepts

- Risk Management
 - Risk Management Benefits
 - Key Roles and Responsibilities in Risk management
- Key Risk Indicators(KRI)

LO#02: Learn to manage risk through risk management program

- Risk Management Phase
 - Risk Identification
 - Establishing Context
 - Quantifying Risks
 - Risk Assessment
 - Risk Analysis
 - Risk Prioritization
 - Risk Treatment
 - Risk Treatment Steps
 - Risk Tracking & Review

CND Outline

LO#03: Learn different Risk Management Frameworks (RMF)

- Enterprise Network Risk Management
 - Enterprise Risk Management Framework (ERM)
 - Goals of ERM Framework
 - NIST Risk Management Framework
 - COSO ERM Framework
 - COBIT Framework
 - Risk Management Information Systems (RMIS)
 - Tools for RMIS
 - Enterprise Network Risk Management Policy
 - Best Practices for Effective Implementation of Risk Management

LO#04: Learn to manage vulnerabilities through vulnerability management program

- Vulnerability Management
 - Discovery
 - Asset Prioritization
 - Assessment
 - Advantages of Vulnerability Assessment
 - Requirements for Effective Network Vulnerability Assessment
 - Types of Vulnerability Assessment
 - Steps for Effective External Vulnerability Assessment
 - Vulnerability Assessment Phases
 - Network Vulnerability Assessment Tools
 - Choosing a Vulnerability Assessment Tool
 - Choosing a Vulnerability Assessment Tool: Deployment Practices and Precautions
 - Reporting
 - Sample Vulnerability Management Reports
 - Remediation
 - Remediation Steps
 - Remediation Plan
 - Verification

LO#05: Learn vulnerability Assessment and Scanning

- External Network Vulnerability Assessment

CND Outline

- Internal Network Vulnerability Assessment
- Web Vulnerability Assessment

Exercise 01: Vulnerability Management using OSSIM

Exercise 02: Vulnerability Analysis Using the Nessus

Exercise 03: Network Vulnerabilities Scanning Using GFI LanGuard

Exercise 04: Auditing the Network Security with Nsauditor

Exercise 05: Application Vulnerability Scanning using OWASP ZAP

CNDv2 Module 19 Threat Assessment with Attack Surface Analysis

LO#01: Understand the attack surface concepts

- Attack Surface
- Attack Surfaces Categories
 - System Attack Surface
 - Network Attack Surface
 - Software Attack surface
 - Physical Attack Surface
 - Human Attack Surface

LO#02: Learn to understand and visualize your attack surface

- Attack Surface Analysis Steps
 - Step 1 Understand and visualize the attack surface
 - Attack Surface Visualization
 - Attack Path Visualization using ThreatPath
 - Attack Path Visualization using securiCAD
 - Attack Path Visualization using Skybox

LO#03: Learn to identify Indicators of Exposures (IoE)

- Step 2: Identify the Indicators of Exposures
 - Indicators of Exposure(IoE)
 - Identification of Indicators of Exposures
 - System Attack Surface
 - Identifying IoEs using Attack Surface Analyzer
 - Identifying IoEs using Windows Sandbox Attack Surface Analysis Tool
 - Application Attack Surface
 - Identifying IoEs using OWASP Attack Surface Detector
 - Identifying IoEs using ThreatModeler

CND Outline

- Network Attack Surface
 - Identifying IoEs using AttackSurfaceMapper
 - Identifying IoEs using amass — Automated Attack Surface Mapping
- Human Attack Surface: Identifying IoEs using Phishing Framework

LO#04: Learn to perform attack simulation

- Step 3: Simulate the attack
 - Attack Simulation
 - Attack Simulation using Breach and Attack Simulation (BAS)
 - Attack simulation using Infection Monkey
 - Attack simulation using Cymulate
 - Additional Breach and Attack Simulation (BAS) Vendors

LO#05: Learn to reduce the attack surface

- Step 4: Reduce the attack surface
 - Attack Surface reduction
 - Reducing system attack surface
 - Reducing Application attack surface
 - Reducing Network attack surface
 - Reducing Human attack surface
 - Reducing physical attack surface

LO#06: Discuss attack surface analysis specific to Cloud and IoT

- Cloud Attack Surface
- Attack Surface of IoT

Exercise 01: Performing attack surface analysis using Attack Surface Analyzer

Exercise 02: Analyzing Web Application Attack Surface using OWASP Attack Surface Detector (ZAP Plugin)

Exercise 02: Attack Surface Mapping and Visualizing using Amass

CNDv2 Module 20 Threat Prediction with Cyber Threat Intelligence

LO#01: Understand role of cyber threat intelligence in network defense

- Cyber Threat Intelligence (CTI)
- Objectives of Threat Intelligence
- How Threat Intelligence Can Help Organizations

LO#02: Understand the types of threat Intelligence

- Types of threat Intelligence

CND Outline

- Strategic Threat Intelligence
- Tactical Threat Intelligence
- Operational Intelligence

LO#03: Understand the Indicators of Threat Intelligence: Indicators of Compromise (IoCs) and Indicators of Attack (IoA)

- Indicators of Compromise (IoCs)
 - Example of IoC
- Indicators of Attack (IoA)
 - Examples of IOA

LO#04: Understand the layers of Threat Intelligence

- Layers of Threat Intelligence
 - Threat Intelligence Sources
 - Example: Gaining Knowledge of Attacker's TTPs Through Hacking Forums
 - Threat Intelligence Feeds
 - Focus area of TI Feeds
 - Example: Free and Open Source TI Providers
 - Example: Government TI Providers
 - Additional List of TI Feeds Providers
 - Threat Intelligence Platforms (TIP)
 - Threat Intelligence Platform: TC Complete™
 - Additional Threat Intelligence Platforms
 - Threat intelligence Professional services

LO#05: Learn to leverage/consume threat intelligence for proactive defense

- Threat Intelligence Leverage for Proactive Defense
 - Before consuming Threat Intelligence
 - Proactive defense with Consumption of TI Feeds
 - Ways of consuming TI feeds
 - Integrating TI feeds with Security Tools
 - Integrating TI feeds with Next Generation Firewalls: Cisco Firepower NGFW and NGIPS
 - Integrating of TI Feeds into SIEM
 - Integrating TI feeds with SIEM: OSSIM
 - Manual review

CND Outline

Exercise 1: Integrating OTX Threat Data in OSSIM

APPENDICES (Self-Study):

APPENDIX A: Computer Network Fundamentals

LO#01: Understand various network fundamental concepts

- Computer Network Fundamentals
 - Computer Network
 - TCP/IP Model
 - Comparing OSI and TCP/IP
 - Types of Networks
 - Local Area Network (LAN)
 - Wide Area Network (WAN)
 - Metropolitan Area Network (MAN)
 - Personal Area Network (PAN)
 - Campus Area Network (CAN)
 - Global Area Network (GAN)
 - Wireless Networks(WLAN)
 - Advantages
 - Disadvantages
 - Network Topologies
 - Physical Topology
 - Bus Topology
 - Ring Topology
 - Tree Topology
 - Star Topology
 - Mesh Topology
 - Hybrid Topology
 - Logical Topology
 - Network Hardware Components
 - Types of LAN Technology
 - Ethernet
 - Fast Ethernet
 - Gigabit Ethernet

CND Outline

- 10 Gigabit Ethernet
- Asynchronous Transfer Mode (ATM)
- Power over Ethernet (PoE)
- Specifications of LAN Technology
- Types of cables
 - Fiber Optic Cable
 - Coaxial Cable
 - CAT 3 and CAT 4
 - CAT 5
 - CAT 5e and CAT 6
 - 10/100/1000BaseT (UTP Ethernet)

LO#02: Understand the working of different protocols in TCP/IP protocol suite

- TCP/IP protocol suite
 - Application Layer Protocols
 - Dynamic Host Configuration Protocol (DHCP)
 - DHCP Packet Format
 - DHCP Packet Analysis
 - Domain Name System (DNS)
 - DNS Packet Format
 - DNS Packet Analysis
 - DNSSEC
 - How DNSSEC Works?
 - Managing DNSSEC for Your Domain Name
 - What is a DS Record?
 - How Does DNSSEC Protect Internet Users?
 - Non-DNSSEC-Aware Lookups
 - DNSSEC-Aware Lookups
 - Operation of DNSSEC
 - Hypertext Transfer Protocol (HTTP)
 - File Transfer Protocol (FTP)
 - How FTP Works?
 - Hardening FTP Servers
 - FTP Anonymous Access and its Risk

CND Outline

- Trivial File Transfer Protocol (TFTP)
- Simple Mail Transfer Protocol (SMTP)
 - Sendmail
 - Mail Relaying
- Telnet
 - Cisco Reverse Telnet
- SSH
- SOAP (Simple Object Access Protocol)
- Simple Network Management Protocol (SNMP)
- NTP (Network Time Protocol)
- RPC (Remote Procedure Call)
- Server Message Block (SMB) Protocol
- Session Initiation Protocol (SIP)
- Routing Information Protocol (RIP)
- OSPF (Open Shortest Path First)
- Transport Layer Protocols
 - Transmission Control Protocol (TCP)
 - TCP Header Format
 - TCP Services
 - Simplex
 - Half-duplex
 - Full-duplex
 - User Datagram Protocol (UDP)
 - UDP Operation
- Internet Layer Protocols
 - Internet Protocol (IP)
 - IP Header: Protocol Field
 - What is Internet Protocol v6 (IPv6)?
 - IPv6 Header
 - IPv4/IPv6 Transition Mechanisms
 - IPv6 Security Issues
 - IPv6 Infrastructure Security Issues
 - DNS Issues

CND Outline

- Mobile IP
- IPv4 vs. IPv6
- Internet Control Message Protocol (ICMP)
 - Error Reporting and Correction
 - ICMP Message Delivery
 - Format of an ICMP Message
 - Unreachable Networks
 - Destination Unreachable Message
 - ICMP Echo (Request) and Echo Reply
 - Time Exceeded Message
 - IP Parameter Problem
 - ICMP Control Messages
 - ICMP Redirects
- Address Resolution Protocol (ARP)
 - ARP Packet Format
 - ARP Packet Encapsulation
 - ARP Packet Analysis
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- Link Layer Protocols
 - Fiber Distributed Data Interface (FDDI)
 - Token Ring
 - TKIP
 - EAP (Extensible Authentication Protocol)
 - How EAP Works?
 - Understanding LEAP / PEAP
 - CDP (Cisco Discovery Protocol)
 - HSRP (Hot Standby Router Protocol)
 - Virtual Router Redundancy Protocol (VRRP)
 - VLAN Trunking Protocol (VTP)
 - STP (Spanning Tree Protocol)

LO#03: Understand the concepts of IP Addressing and port numbers

- IP Addressing and port numbers

CND Outline

- Internet Assigned Numbers Authority (IANA)
- IP Addressing
- Classful IP Addressing
- Address Classes
- Subnet Masking
- Subnetting
- Supernetting
- IPv6 Addressing
- Difference between IPv4 and IPv6
- Port Numbers

LO#04: Understand other network related terminologies

- Network Terminology
 - Routing
 - Static Routing
 - Dynamic Routing
 - Network Address Translation (NAT)
 - Benefits of NAT
 - Port Address Translation (PAT)
 - VLAN
 - Advantages
 - Disadvantages
 - Security implications of VLANs
 - Shared Media Network
 - Advantages
 - Disadvantages
 - Switched Media Network
 - Advantages
 - Disadvantages

LO#05: Learn to troubleshoot basic network issues with network troubleshooting utilities

- Troubleshooting
 - Network Troubleshooting Flow chart
 - Basic Network Issues

CND Outline

- Steps for Network Troubleshooting
 - Troubleshooting IP Problems
 - Troubleshooting Local Connectivity Issues
 - Troubleshooting Physical Connectivity Issues
 - Troubleshooting Routing Problems
 - Troubleshooting Upper-layer Faults
 - Troubleshooting Wireless Network Connection Issue
- Network Troubleshooting Tools
 - Ping
 - Tracert/traceroute
 - Ipconfig/ifconfig
 - NSlookup
 - Netstat
 - PuTTY/Tera Term
 - Subnet and IP Calculator
 - Speedtest.net
 - Pathping/mtr
 - Route

APPENDIX B: Physical Network Security

LO#01: Understand the importance of physical security

- Physical Security
 - Need for Physical Security
 - Physical Security Attack Vectors

LO#02: Describe various physical security controls

- Physical Security Controls
 - Location and Architecture Considerations
 - Fire Fighting Systems
 - Physical Barriers
 - Security Personnel
 - Physical Locks
 - Mechanical locks

CND Outline

- 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
- Lighting System
- Power Supply

LO#03: Describe Workplace Security

- Workplace Security
 - Reception Area
 - Server/ Backup Device Security
 - Critical Assets and Removable Devices
 - Securing Network Cables
 - Securing Portable Mobile Devices

LO#04: Describe various Environmental Controls

- Environmental Controls
 - Heating, Ventilation and Air Conditioning
 - Electromagnetic Interference (EMI) Shielding
 - Hot and Cold Aisles
- Physical Security Checklists

APPENDIX C: Virtual Private Network (VPN) Security

LO#01: Understand the working of VPN

- Virtual Private Network (VPN)
- How VPN works?
- Why to Establish VPN ?

LO#02: Understand the VPN Components

- VPN Components
 - VPN Client
 - Tunnel Terminating Device
 - Network Access Server (NAS)
 - VPN Protocol

CND Outline

- VPN Concentrators
 - Functions of VPN Concentrator

LO#03: Explain different VPN types and categories

- Types of VPN
 - Client-to-site (Remote-access) VPNs
 - Site-to-Site VPNs
 - Establishing Connections with VPN
- VPN Categories
 - Hardware VPNs
 - Hardware VPN Products
 - Software VPNs
 - Software VPN Products
- Selecting Appropriate VPN

LO#04: Explain the core functions, technologies, and topologies of VPN

- VPN Core Functions
 - Encapsulation
 - Encryption
 - Authentication
- VPN Technologies
- VPN Topologies
 - Hub-and-Spoke VPN Topology
 - Point-to-Point VPN Topology
 - Full Mesh VPN Topology
 - Star Topology

LO#05: Explain VPN security risks

- Common VPN Flaws
 - VPN Fingerprinting
 - Insecure Storage of Authentication Credentials by VPN Clients
 - Username Enumeration Vulnerabilities
 - Offline Password Cracking
 - Man-in-the-Middle Attacks
 - Lack of Account Lockout
 - Poor Default Configurations
 - Poor Guidance and Documentation

CND Outline

LO#06: Explain VPN security

- VPN Security
 - Firewalls
 - VPN Encryption and Security Protocols
 - Symmetric Encryption
 - Asymmetric Encryption
 - Authentication for VPN Access
 - VPN Security: IPsec Server
 - AAA Server
 - Connection to VPN: SSH and PPP
 - Connection to VPN: Concentrator
 - VPN Security – Radius

LO#06: Discuss Deployment, Quality Of Service and Performance in VPNs

- Improving VPN Speed
- Quality of Service (QOS) in VPNs
- SSL VPN Deployment Considerations
 - Client security
 - Client integrity scanning
 - Sandbox
 - Secure logoff and credential wiping
 - Timeouts and re-authentication
 - Virus, malicious code and worm activity
 - Audit and Activity awareness
 - Internal Network Security Failings
- SLAs for VPN
- IP VPN Service Level Management
- VPN Service Providers
- Auditing and Testing the VPN
 - Testing VPN File Transfer
- Best Security Practices for VPN Configuration
 - Recommendations for VPN Connection