Asquare Technologies
ISO 9001 : 2015 Certified Training Company

Certified Ethical Hacking -V12

Total Duration: 3 to 4 Months (Approx.)

Target Audience

- Ethical Hackers
- System Administrators
- Network Administrators
- Engineers
- Web Managers
- Auditors
- Security Professionals

Pre-Requisites

- Basic understanding of network essentials and core concepts, including server and network components

Module 01: Ethical Hacking: An Introduction (10Hours)

In this first module, you will learn the basics of ethical hacking that are essential for the CEH exam.

Overview of Information Security

1.1 Internet is an Integral Part of Business and Personal Life – What Happens Online in 60 Seconds

1.2 Essential Terminology

1.3 Elements of Information Security

1.4 The Security, Functionality, and Usability Triangle

Attack Vectors and Threats to Information Security

1.5 Motives, Goals, and Objectives of Information Security Attacks

1.6 Top Information Security Attack Vectors

1.7 Information Security Threat Categories

1.8 Types of Attacks on a System

1.9 Information Warfare

Basic Concepts of Hacking

1.10 What is Hacking?

1.11 Who is a Hacker?

1.12 Hacker Classes

1.13 Hacking Phases

Basic Concepts of Ethical Hacking

1.14 What is Ethical Hacking?

1.15 Why is Ethical Hacking Necessary?

1.16 Scope and Limitations of Ethical Hacking

1.17 Skills of an Ethical Hacker

Information Security Controls

1.18 Information Assurance (IA)

1.19 Information Security Management Program

1.20 Enterprise Information Security Architecture (EISA)

1.21 Network Security Zoning

Module 02: Basics of Reconnaissance and Footprinting(15 Hours)

Concepts of Footprinting

2.1 What is Footprinting?

2.2 Objectives of Footprinting

Footprinting Using Search Engines

2.3 Footprinting through Search Engines

2.4 Footprint Using Advanced Google Hacking Techniques

2.5 Information Gathering Using Google Advanced Search and Image Search

2.6 Google Hacking Database

2.7 VoIP and VPN Footprinting through Google Hacking Database

Footprinting Using Web Services

2.8 Finding Company's Top-Level Domains (TLDs) and Sub-Domains

2.9 Finding the Geographical Location of the Target

2.10 People Search on Social Networking Sites and People Search Services

2.11 Gathering Information from LinkedIn

2.12 Gathering Information from Financial Services

2.13 Footprinting through Job Sites

2.14 Monitoring Target Using Alerts

2.15 Information Gathering Using Groups, Forums, and Blogs

2.16 Determining the Operating System

2.17 VoIP and VPN Footprinting through SHODAN

Footprinting Using Social Networking Sites

2.18 Collecting Information through Social Engineering on Social Networking Sites

Footprinting of Websites

2.19 Website Footprinting

2.20 Website Footprinting using Web Spiders

2.21 Mirroring Entire Website

2.22 Extracting Website Information from https://archive.org

2.23 Extracting Metadata of Public Documents

2.24 Monitoring Web Pages for Updates and Changes

Footprinting of Emails

2.25 Tracking Email Communications

2.26 Collecting Information from Email Header

2.27 Email Tracking Tools

Competitive Intelligence

2.28 Competitive Intelligence Gathering

2.29 Competitive Intelligence – When When did this company begin? How did it develop?

2.30 Competitive Intelligence – What are the company's plans?

2.31 Competitive Intelligence – What do expert opinions say about the company?

2.32 Monitoring Website Traffic of Target Company

2.33 Tracking Online Reputation of the Target

Footprinting using Whois

2.34 Whois Lookup

2.35 Whois Lookup Result Analysis

2.36 Whois Lookup Tools

2.37 Finding IP Geolocation Information

DNS Footprinting

2.38 Extracting DNS Information

2.39 DNS Interrogation Tools

Network Footprinting

2.40 Locate the Network Range

2.41 Traceroute

2.42 Traceroute Analysis

2.43 Traceroute Tools

Footprinting by Social Engineering

2.44 Footprinting through Social Engineering

2.45 Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

Tools used for Footprinting

2.46 Maltego

2.47 Recon-ng

2.48 FOCA

2.49 Recon-Dog

2.50 OSRFramework

2.51 Additional Footprinting Tools

Countermeasures

2.52 Footprinting Countermeasures

Asquare Technologies
ISO 9001 : 2015 Certified Training Company

Module 03: Network Scanning(15Hours)

Concepts Network Scanning

3.1 Overview of Network Scanning

3.2 TCP Communication Flags

3.3 TCP/IP Communication

3.4 Creating Custom Packet Using TCP Flags

3.5 Scanning in IPv6 Networks

Tools used for Scanning

3.6 Nmap

3.7 Hping2 / Hping3

3.8 Scanning Tools

3.9 Scanning Tools for Mobile

Techniques used for Scanning

3.10 Scanning Techniques

Scanning Beyond IDS and Firewall

3.11 IDS/Firewall Evasion Techniques

Banner Grabbing

3.12 Banner Grabbing

3.13 How to Identify Target System OS

3.14 Banner Grabbing Countermeasures

Network Diagrams

3.15 Drawing Network Diagrams

3.16 Network Discovery and Mapping Tools

3.17 Network Discovery Tools for Mobile

Scanning Pen Testing

Module 04: Basics of Enumeration(10 Hours)

Concepts of Enumeration

4.1 What is Enumeration?

4.2 Techniques for Enumeration

4.3 Services and Ports to Enumerate

NetBIOS Enumeration

4.4 NetBIOS Enumeration

4.5 NetBIOS Enumeration Tools

4.6 Enumerating User Accounts

4.7 Enumerating Shared Resources Using Net View

SNMP Enumeration

4.8 Simple Network Management Protocol (SNMP) Enumeration

4.9 Working of SNMP

4.10 Management Information Base (MIB)

4.11 SNMP Enumeration Tools

LDAP Enumeration

4.12 LDAP Enumeration

4.13 LDAP Enumeration Tools

NTP Enumeration

4.14 NTP Enumeration

4.15 NTP Enumeration Commands

4.16 NTP Enumeration Tools

SMTP and DNS Enumeration

4.17 SMTP Enumeration

4.18 SMTP Enumeration Tools

4.19 DNS Enumeration Using Zone Transfer

Module 05: Vulnerability Analysis(10Hours)

Concepts of Vulnerability Assessment

5.1 Vulnerability Research

5.2 Vulnerability Classification

5.3 What is Vulnerability Assessment?

5.4 Types of Vulnerability Assessment

5.5 Vulnerability-Management Life Cycle

Solutions for Vulnerability Assessment

5.6 Comparing Approaches to Vulnerability Assessment

5.7 Working of Vulnerability Scanning Solutions

5.8 Types of Vulnerability Assessment Tools

5.9 Characteristics of a Good Vulnerability Assessment Solution

5.10 Choosing a Vulnerability Assessment Tool

5.11 Criteria for Choosing a Vulnerability Assessment Tool

5.12 Best Practices for Selecting Vulnerability Assessment Tools

Vulnerability Scoring Systems

5.13 Common Vulnerability Scoring System (CVSS)

5.14 Common Vulnerabilities and Exposures (CVE)

5.15 National Vulnerability Database (NVD)

5.16 Resources for Vulnerability Research

Vulnerability Assessment Tools

5.17 Vulnerability Assessment Tools

5.18 Vulnerability Assessment Tools for Mobile

Module 06: basics of System Hacking(15Hours)

Concepts of System Hacking

6.1 CEH Hacking Methodology (CHM)

6.2 System Hacking Goals

Cracking Passwords

6.3 Password Cracking

6.4 Types of Password Attacks

6.5 Password Recovery Tools

6.6 Microsoft Authentication

6.7 How Hash Passwords Are Stored in Windows SAM?

6.8 NTLM Authentication Process

6.9 Kerberos Authentication

6.10 Password Salting

6.11 Tools to Extract the Password Hashes

6.12 Password Cracking Tools

6.13 How to Defend against Password Cracking

6.14 How to Defend against LLMNR/NBT-NS Poisoning

Escalating Privileges

6.15 Privilege Escalation

6.16 Privilege Escalation Using DLL Hijacking

6.17 Privilege Escalation by Exploiting Vulnerabilities

6.18 Privilege Escalation Using Dylib Hijacking

6.19 Privilege Escalation using Spectre and Meltdown Vulnerabilities

6.20 Other Privilege Escalation Techniques

6.21 How to Defend Against Privilege Escalation

Executing Applications

6.22 Executing Applications

6.23 Keylogger

6.24 Spyware

6.25 How to Defend Against Keyloggers

6.26 How to Defend Against Spyware

Hiding Files

6.27 Rootkits

6.28 NTFS Data Stream

6.29 What is Steganography?

Covering Tracks

6.30 Covering Tracks

6.31 Disabling Auditing: Auditpol

6.32 Clearing Logs

6.33 Manually Clearing Event Logs

6.34 Ways to Clear Online Tracks

6.35 Covering BASH Shell Tracks

6.36 Covering Tracks on Network

6.37 Covering Tracks on OS

6.38 Covering Tracks Tools

Penetration Testing

6.39 Password Cracking

6.40 Privilege Escalation

6.41 Executing Applications

6.42 Hiding Files

6.43 Covering Tracks

Module 07: Threats from Malware(15 Hours)

7.1 Introduction to Malware

7.2 Different Ways Malware can Get into a System

7.3 Common Techniques Attackers Use to Distribute Malware on the Web

7.4 Components of Malware

Concepts of Trojans

7.5 What is a Trojan?

7.6 How Hackers Use Trojans

7.7 Common Ports Used by Trojans

7.8 How to Infect Systems Using a Trojan

7.9 Trojan Horse Construction Kit

7.10 Wrappers

7.12 How Attackers Deploy a Trojan

7.13 Exploit Kits

7.14 Evading Anti-Virus Techniques

7.15 Types of Trojans

Concepts of Viruses and Worms

7.16 Introduction to Viruses

7.17 Stages of Virus Life

7.18 Working of Viruses

7.19 Indications of Virus Attack

7.20 How does a Computer Get Infected by Viruses

7.21 Virus Hoaxes

7.22 Fake Antiviruses

7.23 Ransomware

7.24 Types of Viruses

7.25 Creating Virus

7.26 Computer Worms

7.27 Worm Makers

Malware Analysis

7.28 What is Sheep Dip Computer?

7.29 Anti-Virus Sensor Systems

7.30 Introduction to Malware Analysis

7.31 Malware Analysis Procedure: Preparing Testbed

7.32 Static Malware Analysis

7.33 Dynamic Malware Analysis

7.34 Virus Detection Methods

7.36 Virus Analysis: WannaCry

Countermeasures

7.37 Trojan Countermeasures

7.38 Backdoor Countermeasures

7.39 Virus and Worms Countermeasures

Module 08: Basics of Sniffing(15Hours)

Concepts of Sniffing

8.1 Network Sniffing

8.2 Types of Sniffing

8.3 How an Attacker Hacks the Network Using Sniffers

8.4 Protocols Vulnerable to Sniffing

8.5 Sniffing in the Data Link Layer of the OSI Model

8.6 Hardware Protocol Analyzers

8.7 SPAN Port

8.8 Wiretapping

8.9 Lawful Interception

Sniffing Technique: MAC Attacks

8.10 MAC Address/CAM Table

8.11 How CAM Works

8.12 What Happens When CAM Table Is Full?

8.13 MAC Flooding

8.14 Switch Port Stealing

8.15 How to Defend against MAC Attacks

Sniffing Technique: DHCP Attacks

8.16 How DHCP Works

8.17 DHCP Request/Reply Messages

8.18 DHCP Starvation Attack

8.19 Rogue DHCP Server Attack

8.20 How to Defend Against DHCP Starvation and Rogue Server Attack

Sniffing Technique: ARP Poisoning

8.21 What Is Address Resolution Protocol (ARP)?

8.22 ARP Spoofing Attack

8.23 Threats of ARP Poisoning

8.24 ARP Poisoning Tools

8.25 How to Defend Against ARP Poisoning

8.26 Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

8.27 ARP Spoofing Detection Tools

Sniffing Technique: Spoofing Attacks

8.28 MAC Spoofing/Duplicating

8.29 MAC Spoofing Technique: Windows

8.30 MAC Spoofing Tools

8.31 IRDP Spoofing

8.32 How to Defend Against MAC Spoofing

Sniffing Technique: DNS Poisoning

8.33 DNS Poisoning Techniques

8.34 How to Defend Against DNS Spoofing

Tools for Sniffing

8.35 Sniffing Tool: Wireshark

8.36 Display Filters in Wireshark

8.37 Additional Wireshark Filters

8.38 Sniffing Tools

8.39 Packet Sniffing Tools for Mobile

Countermeasures

8.40 How to Defend Against Sniffing

Module 09: Social Engineering(15 Hours)

Concepts of Social Engineering

9.1 What is Social Engineering?

9.2 Phases of a Social Engineering Attack

Techniques of Social Engineering

9.3 Types of Social Engineering

9.4 Human-based Social Engineering

9.5 Computer-based Social Engineering

9.6 Mobile-based Social Engineering

Insider Threats

9.7 Insider Threat / Insider Attack

9.8 Type of Insider Threats

Impersonation on Social Networking Sites

9.9 Social Engineering Through Impersonation on Social Networking Sites

9.10 Impersonation on Facebook

9.11 Social Networking Threats to Corporate Networks

Identity Theft

9.12 Identity Theft

Countermeasures

9.13 Social Engineering Countermeasures

9.14 Insider Threats Countermeasures

9.15 Identity Theft Countermeasures

9.16 How to Detect Phishing Emails?

9.17 Anti-Phishing Toolbar

9.18 Common Social Engineering Targets and Defense Strategies

Social Engineering Pen-Testing

9.19 Social Engineering Pen-Testing

9.20 Social Engineering Pen-Testing Tools

Asquare Technologies
ISO 9001 : 2015 Certified Training Company

Module 10: Denial-of-Service Attack(10Hours)

DoS/DDoS Concepts

10.1 What is a Denial-of-Service Attack?

10.2 What is Distributed Denial-of-Service Attack?

Techniques used for DoS/DDoS Attacks

10.3 Basic Categories of DoS/DDoS Attack Vectors

10.4 UDP Flood Attack

10.5 ICMP Flood Attack

10.6 Ping of Death and Smurf Attack

10.7 SYN Flood Attack

10.8 Fragmentation Attack

10.9 HTTP GET/POST and Slowloris Attacks

10.10 Multi-Vector Attack

10.11 Peer-to-Peer Attacks

10.12 Permanent Denial-of-Service Attack

10.13 Distributed Reflection Denial-of-Service (DRDoS)

Botnets

10.14 Organized Cyber Crime: Organizational Chart

10.15 Botnet

10.16 A Typical Botnet Setup

10.17 Botnet Ecosystem

10.18 Scanning Methods for Finding Vulnerable Machines

10.19 How Malicious Code Propagates?

10.20 Botnet Trojans

DDoS Case Study

10.21 DDoS Attack

10.22 Hackers Advertise Links to Download Botnet

10.23 Use of Mobile Devices as Botnets for Launching DDoS Attacks

10.24 DDoS Case Study: Dyn DDoS Attack

Tools used for DoS/DDoS Attack

10.25 DoS/DDoS Attack Tools

10.26 DoS and DDoS Attack Tool for Mobile

Countermeasures

10.27 Detection Techniques

10.28 DoS/DDoS Countermeasure Strategies

10.29 DDoS Attack Countermeasures

10.30 Techniques to Defend against Botnets

10.31 DoS/DDoS Countermeasures

10.32 DoS/DDoS Protection at ISP Level

10.33 Enabling TCP Intercept on Cisco IOS Software

Tools used for DoS/DDoS Protection

10.34 Advanced DDoS Protection Appliances

10.35 DoS/DDoS Protection Tools

Module 11: Session Hijacking(15 Hours)

Concepts of Session Hijacking

11.1 What is Session Hijacking?

11.2 Why Session Hijacking is Successful?

11.3 Session Hijacking Process

11.4 Packet Analysis of a Local Session Hijack

11.5 Types of Session Hijacking

11.6 Session Hijacking in OSI Model

11.7 Spoofing vs. Hijacking

Application Level Session Hijacking

11.8 Application Level Session Hijacking

11.9 Compromising Session IDs using Sniffing and Predicting Session Token

11.10 Compromising Session IDs Using Man-in-the-Middle Attack

11.11 Compromising Session IDs Using Man-in-the-Browser Attack

11.12 Compromising Session IDs Using Client-side Attacks

11.13 Compromising Session IDs Using Client-side Attacks: Cross-site Script Attack

11.14 Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery Attack

11.15 Compromising Session IDs Using Session Replay Attack

11.16 Compromising Session IDs Using Session Fixation

11.17 Session Hijacking Using Proxy Servers

Network Level Session Hijacking

11.20 TCP/IP Hijacking

11.21 IP Spoofing: Source Routed Packets

11.22 RST Hijacking

11.23 Blind Hijacking

11.24 UDP Hijacking

11.25 MiTM Attack Using Forged ICMP and ARP Spoofing

Session Hijacking Tools

11.26 Session Hijacking Tools

11.27 Session Hijacking Tools for Mobile

Countermeasures

11.28 Session Hijacking Detection Methods

11.29 Protecting against Session Hijacking

11.30 Methods to Prevent Session Hijacking: To be Followed by Web Developers

Module 12: How to Evade IDS, Firewalls, and Honeypots(10 Hours)

Concepts of IDSs, Firewalls, and Honeypots

12.1 Intrusion Detection System (IDS)

12.2 Firewall

12.3 Honeypot

IDS, Firewall, and Honeypot Solutions

12.4 Intrusion Detection Tool

12.5 Firewalls

12.6 Honeypot Tools

IDS Evasion

12.7 IDS Evasion Techniques

Tools for IDS/Firewall Evasion

12.9 IDS/Firewall Evasion Tools

12.10 Packet Fragment Generator Tools

Detecting Honeypots

12.11 Detecting Honeypots

12.12 Detecting and Defeating Honeypots

12.13 Honeypot Detection Tool: Send-Safe Honeypot Hunter

IDS/Firewall Evasion Countermeasures

12.14 How to Defend Against IDS Evasion

12.15 How to Defend Against Firewall Evasion

Penetration Testing

12.16 Firewall/IDS Penetration Testing

Module 13: Basics of Hacking Web Servers(10 Hours)

Web Server Concepts

13.1 Web Server Operations

13.2 Open Source Web Server Architecture

13.3 IIS Web Server Architecture

13.4 Web Server Security Issue

13.5 Why Web Servers Get Compromised?

13.6 Impact of Web Server Attacks

Attacks of Web Servers

13.7 DoS/DDoS Attacks

13.8 DNS Server Hijacking

13.9 DNS Amplification Attack

13.10 Directory Traversal Attacks

13.11 Man-in-the-Middle/Sniffing Attack

13.12 Phishing Attacks

13.13 Website Defacement

13.14 Web Server Misconfiguration

13.15 HTTP Response Splitting Attack

13.16 Web Cache Poisoning Attack

13.17 SSH Brute Force Attack

13.18 Web Server Password Cracking

Methodology of Web Server Attacks

13.20 Information Gathering

13.21 Web Server Footprinting/Banner Grabbing

13.22 Website Mirroring

Tools of Web Server Attacks

13.27 Metasploit

13.28 Web Server Attack Tools

Countermeasures

13.29 Place Web Servers in Separate Secure Server Security Segment on Network

13.30 Countermeasures

Module 14: Web Application Hacking(10 Hours)

Web App Concepts

14.1 Introduction to Web Applications

14.2 Web Application Architecture

14.3 Web 2.0 Applications

14.4 Vulnerability Stack

Threats to Web App

14.5 OWASP Top 10 Application Security Risks – 2017

14.6 Other Web Application Threats

Hacking Methodology

14.7 Web App Hacking Methodology

14.8 Footprint Web Infrastructure

14.9 Attack Web Servers

14.10 Analyze Web Applications

14.11 Bypass Client-Side Controls

14.12 Attack Authentication Mechanism

14.13 Attack Authorization Schemes

14.14 Attack Access Controls

Web App Hacking Tools

14.21 Web Application Hacking Tools

Countermeasures

14.22 Web Application Fuzz Testing

14.23 Source Code Review

14.24 Encoding Schemes

Module 15: Basics of SQL Injection(15 Hours)

SQL Injection Concepts

15.1 What is SQL Injection?

15.2 SQL Injection and Server-side Technologies

15.3 Understanding HTTP POST Request

15.4 Understanding Normal SQL Query

15.5 Understanding an SQL Injection Query

Types of SQL Injection

15.10 Types of SQL Injection

SQL Injection Methodology

15.11 SQL Injection Methodology

SQL Injection Tools

15.12 SQL Injection Tools

15.13 SQL Injection Tools

15.14 SQL Injection Tools for Mobile

Countermeasures

15.17 How to Defend Against SQL Injection Attacks

15.18 SQL Injection Detection Tools

Module 16: Wireless Network Hacking(10 Hours)

Wireless Concepts

16.1 Wireless Terminologies

16.2 Wireless Networks

16.3 Wireless Standards

16.4 Service Set Identifier (SSID)

16.5 Wi-Fi Authentication Modes

Wireless Encryption

16.8 Types of Wireless Encryption

16.9 WEP vs. WPA vs. WPA2

Wireless Threats

16.12 Wireless Threats

Wireless Hacking Methodology

16.13 Wireless Hacking Methodology

Tools for Wireless Hacking

16.14 WEP/WPA Cracking Tools

16.15 WEP/WPA Cracking Tool for Mobile

16.16 Wi-Fi Sniffer

Countermeasures

16.24 Wireless Security Layers

16.25 How to Defend Against WPA/WPA2 Cracking

16.26 How to Defend Against KRACK Attacks

16.27 How to Detect and Block Rogue AP

16.28 How to Defend Against Wireless Attacks

16.29 How to Defend Against Bluetooth Hacking

Tools Wireless Security

16.30 Wireless Intrusion Prevention Systems

16.31 Wireless IPS Deployment

Asquare Technologies
ISO 9001 : 2015 Certified Training Company

Module 17: Hacking Mobile Platforms(15 Hours)

Mobile Platform Attack Vectors

17.1 Vulnerable Areas in Mobile Business Environment

17.2 OWASP Top 10 Mobile Risks – 2016

17.3 Anatomy of a Mobile Attack

17.4 How a Hacker Can Profit from Mobile when Successfully Compromised

17.5 Mobile Attack Vectors and Mobile Platform Vulnerabilities

Hacking Android OS

17.11 Android OS

17.12 Android Rooting

17.13 Blocking Wi-Fi Access using NetCut

17.14 Hacking with zANTI

17.15 Hacking Networks Using Network Spoofer

17.16 Launching DoS Attack using Low Orbit Ion Cannon (LOIC)

17.17 Performing Session Hijacking Using DroidSheep

Mobile Spyware

17.32 Mobile Spyware

17.33 Mobile Spyware: mSpy

17.34 Mobile Spywares

Mobile Device Management

17.35 Mobile Device Management (MDM)

17.36 Mobile Device Management Solutions

17.37 Bring Your Own Device (BYOD)

Mobile Security Guidelines and Tools

17.38 General Guidelines for Mobile Platform Security

17.39 Mobile Device Security Guidelines for Administrator

Mobile Pen Testing

17.43 Android Phone Pen Testing

Module 18: Basics of IoT Hacking (10 Hours)

IoT Concepts

18.1 What is IoT

18.2 How IoT Works

18.3 IoT Architecture

18.4 IoT Application Areas and Devices

Attacks on IoT

18.9 IoT Security Problems

18.10 OWASP Top 10 IoT Vulnerabilities and Obstacles

18.11 IoT Attack Surface Areas

18.12 IoT Threats

Methodology used for IoT Hacking

18.17 What is IoT Device Hacking?

18.18 IoT Hacking Methodology

Tools used for IoT Hacking

18.19 Information Gathering Tools

18.20 Sniffing Tools

18.21 Vulnerability Scanning Tools

Countermeasures

18.23 How to Defend Against IoT Hacking

18.24 General Guidelines for IoT Device Manufacturing Companies

Module 19: Basics of Cloud Computing(10 Hours)

19.1 Introduction to Cloud Computing

19.2 Separation of Responsibilities in Cloud

19.3 Cloud Deployment Models

Cloud Computing Threats

19.7 Cloud Computing Threats

Cloud Computing Attacks

19.8 Service Hijacking using Social Engineering Attacks

19.9 Service Hijacking using Network Sniffing

19.10 Session Hijacking using XSS Attack

19.11 Session Hijacking using Session Riding

19.12 Domain Name System (DNS) Attacks

19.23 Best Practices for Securing Cloud

19.24 NIST Recommendations for Cloud Security

19.25 Organization/Provider Cloud Security Compliance Checklist

19.26 Cloud Security Tools

Module 20: Basics of Cryptography(5 Hours)

Cryptography Concepts

20.1 Cryptography

20.2 Government Access to Keys (GAK)

Encryption Algorithms

20.3 Ciphers

20.4 Data Encryption Standard (DES)

20.5 Advanced Encryption Standard (AES)

Cryptography Tools

20.12 MD5 Hash Calculators

20.13 Hash Calculators for Mobile

20.14 Cryptography Tools

Email Encryption

20.17 Digital Signature

20.18 Secure Sockets Layer (SSL)

20.19 Transport Layer Security (TLS)

Countermeasures

20.29 How to Defend Against Cryptographic Attacks

Asquare Technologies
ISO 9001 : 2015 Certified Training Company

Duration : 2 Months (Approx)

Network Fundamentals (15Hours)

- Explaining the roles and functions of components like routers, switches, access points, servers, endpoints, firewalls, IPS, and controllers
- Describing the properties of network architecture including 2-tier, 3-tier, spine-leaf, WAN, SOHO, cloud and on-premises topology
- Comparing types of cables - copper, single-mode, fibre, multimode fibre, etc. Physical interface comparison with respect to point-to-point and ethernet shared media connections. PoE Concepts are also discussed in this chapter
- Identifying interface and cable problems such as errors, collisions, speed, and mismatch duplex
- Comparing UDP to TCP
- Configuring and verifying IPv4 addresses and subnetting
- Demonstrating the importance of private IPv4 address
- Configuring and verifying of IPv6 prefix and address
- Comparing IPv6 address types, including link local, unique local, global unicast, anycast, multicast, modified EUI 64
- Describing wireless principles including WiFi channels (non-overlapping), SSID, RF, and encryption
- Explaining virtual machines
- Describing switching concepts, frame switching, frame flooding, MAC learning, ageing, and MAC address table

Network Access(15 Hours)

- VLAN verification and configuration comprising multiple switches, including details on default VLAN, connectivity, and access ports

- Verifying and configuring interswitch connectivity with respect to native VLAN, 802.1Q, and trunk ports
- LLDP and Cisco Discovery Protocol's configuration and verification
- LACP and Layer2/3 configuration and verification
-
- Describing AP and access connections such as HTTPS, HTTP, Telnet, SSH, and console, Radius/TACACS+
- Configuring WLAN access for client connectivity through WLAN creation, OoS profiles, advanced WLAN configuration, and security settings

IP Services (10hours)

- Configuring and verifying NAT through pools and static
- Configuring and verifying NTP in a client and server setting
- Explaining the function of DNS and DHCP
- Syslog features such as levels and facilities description
- Configuring and verifying relay and DHCP Client
-
- SSH method for configuring network devices
- Explaining TFTP/FTP capabilities and roles through SSH

Security Fundamentals (10 hours)

- Describing the impact of automation on network management
- Comparing networks using controller-based networking
- Describing software defined architectures using underlay, overlay, and fabric and explaining controller-based architecture
- Utilising Cisco DNA Centre enabled device management for comparing traditional campus device management
- Explaining properties of Rest-based APIs such as data encoding, CRUD, and HTTP verbs
- Recognizing the abilities of Ansible, Chef, and Puppet related to configuration management mechanisms
- Interpreting ISON encoded dat

Asquare Technologies
ISO 9001 : 2015 Certified Training Company

Linux Course Curriculum (40 Hours)

- ## Introduction to Linux

- **Topics:**
- Need for Linux OS
- What is Linux
- History of Linux
- Relationship Between Unix And Linux
- Features of Linux
- False myths around Linux
- Where Linux is used?
- Components of a Linux OS
- The architecture of Linux OS
- Types of Kernel
- Shell

- Programming in Linux
- Linux Distribution
- Miscellaneous Linux Concepts
- Software Licencing
- Installation and initialisation of Linux
- Shell Scripting
- Practical Uses of Shell Scripting

- **Linux Course Curriculum (40 Hours)**

- ## Introduction to Linux

- **Topics:**
- Need for Linux OS
- What is Linux
- History of Linux
- Relationship Between Unix And Linux
- Features of Linux
- False myths around Linux
- Where Linux is used?
- Components of a Linux OS
- The architecture of Linux OS
- Types of Kernel
- Shell

- Programming in Linux
- Linux Distribution
- Miscellaneous Linux Concepts
- Software Licencing
- Installation and initialisation of Linux
- Shell Scripting
- Practical Uses of Shell Scripting

- **Initialization of Linux**
- **User Administration**
- **Boot and Package Management**
- **Networking**
- **Linux Overview and Scripting**
- **Linux for software development**
- **Security Administration, Shell Script and Virtualization**