SECURITY SPECIALIST BUNDLE

This Bundle includes,

1. **BASICS OF NETWORKING**
2. **CCNA -> CCNP**

3. **FIREWALLS – 4**
4. **CERTIFIED ETHICAL HACKING**
5. **BACK TRACK BASIC**

6. **KALI LINUX BASIC**

1. **BASICS OF NETWORKING:**

Networking Basics: What You Need to Know. A network connects computers, mobile phones, peripherals, and even IoT devices. Switches, routers, and wireless access points are the essential networking basics. Through them, devices connected to your network can communicate with one another and with other networks, like the Internet.

Topics related to the mentioned will be discussed in details

2. **KALI LINUX BASIC:** Kali Linux is a Debian based distribution for Ethical Hackers, Penetration Testers, Security Researchers and Enthusiasts. It is stable, updated, enterprise ready, open source and well maintained distribution by Offensive Security. Kali Linux default desktop environment is GNOME but it also offers a variety of other desktop environments including KDE, MATE, LXDE and others. It can be installed on various type of systems including laptops, Servers, ARM devices (raspberry pi etc.) and Cloud. It also has a portable version for android devices called NetHunter which can be used within android operating system and comes with pre-installed tools and scripts that offer portability while doing security auditing or penetration testing.
   Why You Should Use Kali Linux? Kali Linux is mainly used by Penetration Testers, Security Auditors, Forensics Investigators and Researchers. It has almost every tool or script pre-installed that can be used for any of the above purposes. You can use Kali Linux to crack Wi-Fi networks, to run Open Source Intelligence (OSINT) on someone, to hack websites and networks and many more.

CISCO CERTIFIED NETWORK ASSOCIATE

(200-301 CCNA)

COURSE DURATION: 30 HOURS   **FEE -1300 AED**

What is CCNA?

CCNA (Cisco Certified Network Associate) is an information technology (IT) certification from Cisco Systems. CCNA certification is an associate-level Cisco Career certification.

Why should you become a CCNA?

As a networking professional, you will cultivate industry-supported skills and credentials that you will be able to transfer to future employment opportunities. With your CCNA certification, you will be able to demonstrate and promote the fact that you have the necessary skills to do your job effectively and you are certified by the leader in Network Technologies.

Requirements for the certification
To become Cisco Certified Network Associate, you are required to pass one exam (exam #200-125 CCNA). The exam duration is 90 minutes and there are 50 to 60 questions. This exam is developed with the input of professionals in the industry and reflects how Cisco products are used in organizations throughout the world. The exam is administered by Pearson Vue™, an independent testing organization with locations worldwide. Computer Institute is an authorized testing center.

The following table shows the exam percentages for exam sections:

1. Network Fundamentals	**15%**
2. LAN Switching Technologies	**21%**
3. Routing Technologies	**23%**
4. WAN Technologies	**10%**
5. Infrastructure Services	**10%**
6. Infrastructure Security	**11%**
7. Infrastructure Management	**10%**

Contents in Detail

1. Network Fundamentals

2. LAN Switching Technologies

3. Router and Switches configuration

4. Routing Configuration – Static – RIP – RIPv2

5. IGRP, EIGRP, OSPF

6. ACL and Extended ACL

7. NAT, PAT

8. Switch Configuration

9. VLAN, VTP Domain

10. Password recovery

11. TFTP Setup

12. Wireless basics

CISCO CERTIFIED NETWORK PROFESSIONAL

300-101 ROUTE- Implementing Cisco IP Routing (ROUTE)

300-115 SWITCH- Implementing Cisco IP Switched Networks (SWITCH)

300-135 TSHOOT - Troubleshooting and Maintaining Cisco IP Networks (TSHOOT) ISCO CERTIFIED NETWORK PROFESSIONAL

 DURATION -30 HOURS   **FEE: 3500 AED**

What is CCNP?

Cisco Certified Network Professional (CCNP) is an intermediate-level certification in the Cisco certified professional program. This certification is aimed at full-time network or system administrators, or those who work with local and/or wide-area network (LAN/WAN) infrastructure**.**

Why should you become a CCNP?

Having a Cisco Certified Network Professional (CCNP) certification validates your ability to implement and troubleshoot both LAN and WAN networks. In addition,

you will be recognized as a person who can collaborate with specialists on issues related to voice, wireless, advanced security and video solutions.

REQUIREMENTS FOR CERTIFICATION:

Any CCNA or CCIE with at least one year of networking experience can become a **CCNP** by successfully passing 3 exams: ROUTE, SWITCH and TSHOOT.

300-101 ROUTE- Implementing Cisco IP Routing (ROUTE)

Prerequisites

The knowledge and skills that a learner must have before attending this Curriculum are as follows:

- Describing network fundamentals
- Establishing Internet and WAN connectivity (IPv4 and IPv6)
- Managing network device security
- Operating a medium-sized LAN with multiple switches, supporting VLANs, trunking, and spanning tree
- Troubleshooting IP connectivity (IPv4 and IPv6)
- Configuring and troubleshooting EIGRP and OSPF (IPv4 and IPv6)
- Configuring devices for SNMP, Syslog, and NetFlow access
- Managing Cisco device configurations, Cisco IOS images, and licenses
- It is highly recommended that this course be taken after the following Cisco courses:
- Interconnecting Cisco Networking Devices v2.0, Part 1 (ICND1 v2.0) and Part 2 (ICND2 v2.0)
- Interconnecting Cisco Networking Devices: Accelerated version 2.0 (CCNAX v2.0)

MACOB IT SOLUTIONS LLC

BMI Building 703, Bank Street
Burdubai, Dubai. Tel: + 97143274113
Email: info@macobit.ae

Course Objectives

- Upon completing this course, the learner will be able to meet these overall objectives:
- Describe routing protocols, different remote connectivity options and their impact on routing and implement RIPng
- Configure EIGRP in IPv4 and IPv6 environment
- Configure OSPF in IPv4 and IPv6 environment
- Implement route redistribution using filtering mechanisms
- Implement path control using policy based routing and IP SLA
- Implement enterprise Internet connectivity
- Secure Cisco routers according to best practices and configure authentication for routing protocols

Course Outline

Module 1: Basic Network and Routing Concepts

Module 2: EIGRP Implementation

Module 3: OSPF Implementation

Module 4: Configuration of Redistribution

Module 5: Path Control Implementation

Module 6: Enterprise Internet Connectivity

Module 7: Routers and Routing Protocol Hardening

300-115 SWITCH- Implementing Cisco IP Switched Networks (SWITCH)

Prerequisites

The knowledge and skills that a learner must have before attending this Curriculum are as follows:

- Describing network fundamentals
- Establishing Internet and WAN connectivity (IPv4 and IPv6)
- Managing network device security
- Operating a medium-sized LAN with multiple switches, supporting VLANs, trunking, and spanning tree
- Troubleshooting IP connectivity (IPv4 and IPv6)
- Configuring and troubleshooting EIGRP and OSPF (IPv4 and IPv6)
- Configuring devices for SNMP, Syslog, and NetFlow access
- Managing Cisco device configurations, Cisco IOS images, and licenses

MACOB IT SOLUTIONS LLC

BMI Building 703, Bank Street
Burdubai, Dubai. Tel: +97143274113
Email: info@macobit.ae

It is highly recommended that this course be taken after the following Cisco courses:

1. Interconnecting Cisco Networking Devices v2.0, Part 1 (ICND1 v2.0) and Part 2 (ICND2 v2.0)
2. Interconnecting Cisco Networking Devices: Accelerated version 2.0 (CCNAX v2.0)

Course Objectives

- Upon completing this course, the learner will be able to meet these overall objectives:
- Describe the hierarchical campus structure, basic switch operation, use of SDM templates, PoE, and LLDP
- Implement VLANs, trunks, explain VTP, implement DHCP in IPv4 and IPv6 environment, and configure port aggregation
- Implement and optimize STP mechanism that best suits your network - PVSTP+, RPVSTP+, or MSTP
- Configure routing on a multilayer switch
- Configure NTP, SNMP, IP SLA, port mirroring, and verify Stack Wise and VSS operation
- Implement First Hop redundancy in IPv4 and IPv6 environments
- Secure campus network according to recommended practices

Course Outline

Module 1: Basic Concepts and Network Design

Module 2: Campus Network Architecture

Module 3: Spanning Tree Implementation

Module 4: Configuring Inter-VLAN Routing

Module 5: Implementing High Availability Networks

Module 6: First Hop Redundancy Implementation

Module 7: Campus Network Security.

300-135 TSHOOT - Troubleshooting and Maintaining Cisco IP Networks (TSHOOT) ISCO CERTIFIED NETWORK PROFESSIONAL

Prerequisites

Prior to attending this course student should have the knowledge of and experience with the implementation and verification of enterprise routing and switching technologies as offered by the Implementing Cisco Switched Networks (SWITCH) v2.0 and Implementing Cisco IP Routing (ROUTE) v2.0 courses or equivalent skills and knowledge. This includes knowledge and experience of the following technologies:

- Layer 2 switching
- VLANs, VLAN access control lists, port security
- Switch security issues
- Link aggregation protocols
- Spanning Tree Protocol (STP)
- Inter-VLAN routing solutions
- First Hop Redundancy Protocols (FHRPs) - HSRP, VRRP, and GLBP
- Branch office operations
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Layer 3 path control
- Redistribution
- Internal and External Border Gateway Protocol (BGP)
- IPv6 Networking

Course Objectives

Upon completing this course, the learner will be able to meet these overall objectives:

- Describe the troubleshooting tools and methodologies that are used to identify and resolve issues in complex enterprise networks
- Isolate and fix the network issues that your company, SECHNIK Networking Ltd., is facing
- Isolate and fix the network issues that your customer, TINC Garbage Disposal Ltd., is facing
- Isolate and fix the network issues that your customer, PILE Forensic Accounting Ltd., is facing
- Isolate and fix the network issues that your customer, Bank of POLONA Ltd., is facing
- Isolate and fix the network issues that your customer, RADULKO Transport Ltd., is facing

Course Outline

Module 1: Tools and Methodologies of Troubleshooting

Module 2: Troubleshooting at SECHNIK Networking Ltd

Module 3: Troubleshooting at TINC Garbage Disposal Ltd.

Module 4: Troubleshooting at PILE Forensic Accounting Ltd

Module 5: Troubleshooting at Bank of POLONA Ltd

Module 6: Troubleshooting at RADULKO Transport Ltd

FIREWALLS

COURSE DURATION: 30 HOURS   **FEE- 4000AED**

WHAT IS FIREWALL?

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

TYPES OF FIREWALL

There are three basic types of firewalls that are used by companies to protect their data & devices to keep destructive elements out of network, viz. Packet Filters, Stateful Inspection and Proxy Server Firewalls.

CONTENTS

- Firewall Planning and Design
- Developing a Security Policy
- Firewall Configuration Strategies
- Packet Filtering
- Working with Proxies and Application - Level Firewalls
- Authenticating Users
- Encryption and Firewalls
- Choosing a Bastion Host
- Setting Up a Virtual Private Network
- Building Your Own Firewall
- Ongoing Administration

MACOB IT SOLUTIONS LLC

BMI Building 703, Bank Street
Burdubai, Dubai. Tel: + 97143274113
Email: info@macobit.ae

CERTIFIED ETHICAL HACKER

COURSE DURATION -30 HOURS   FEE-3500 AED

EXAM CODE: 312-50 (ECC EXAM), 312-50 (VUE)

WHAT IS CERTIFIED ETHICAL HACKING?

Certified Ethical Hacker (CEH) is a qualification obtained by demonstrating knowledge of assessing the security of computer systems by looking for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system. This knowledge is assessed by answering multiple choice questions regarding various ethical hacking techniques and tools. The code for the C|EH exam is 312-50. This certification has now been made a baseline with a progression to the C|EH (Practical), launched in March 2018, a test of penetration testing skills in a lab environment where the candidate must demonstrate the ability to apply techniques and use penetration testing tools to compromise various simulated systems within a virtual environment.

COURSE DESCRIPTION

 The Certified Ethical Hacker (C|EH v10) program is a trusted and respected ethical hacking training Program that any information security professional will need. Since its inception in 2003, the Certified Ethical Hacker has been the absolute choice of the industry globally.

It is a respected certification in the industry and is listed as a baseline certification on the United States Department of Defense Directive 8570. The C|EH exam is ANSI 17024 compliant adding credibility and value to credential members. C|EH is used as a hiring standard and is a core sought after certification by many of the Fortune 500 organizations, governments, cyber security practices, and a cyber-staple in education across many of the most prominent degree programs in top Universities around the globe. Hundreds of Thousands of InfoSec Professionals as well as Career Starters have challenged the exam and

BMI Building 703, Bank Street
Burdubai, Dubai. Tel: + 97143274113
Email: info@macobit.ae

for those who passed, nearly all are gainfully employed with successful careers, but the landscape is changing.

Cyber Security as a profession is evolving, the barrier to entry is rising, the demand for Skilled Cyber professionals continues to grow, but it is being refined, demanding a higher level of skill and ability. EC-Council raises the bar again for ethical hacking training and certification programs with the all new C|EH v10! This course in its 10th iteration, is updated to provide you with the tools and techniques used by hackers and information security professionals alike to break into any computer system.

 This course will immerse you into a "Hacker Mindset" in order to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver's seat with a hands-on training environment employing a systematic ethical hacking process. You are constantly exposed to creative techniques of achieving optimal information security posture in the target organization; by hacking it! You will learn how to scan, test, hack and secure target systems. The course covers the Five Phases of Ethical Hacking, diving into Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks. The tools and techniques in each of these five phases are provided in detail in an encyclopedic approach and absolutely no other program offers you the breadth of learning resources, labs, tools and techniques than the C|EH v10 program.

Contents in brief:

1. Key issues plaguing the information security world, incident management process, and penetration testing.
2. Various types of foot printing, foot printing tools, and countermeasures
3. Network scanning techniques and scanning countermeasures.
4. Enumeration techniques and enumeration countermeasures.
5. System hacking methodology, steganography, steganalysis attacks, and covering tracks.
6. Different types of Trojans, Trojan analysis, and Trojan countermeasures
7. Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.
8. Packet sniffing techniques and how to defend against sniffing.
9. Social Engineering techniques, identify theft, and social engineering countermeasures
10. DoS/DDoS attack techniques, botnets
11. Session hijacking techniques and countermeasures.
12. Different types of webserver attacks, attack methodology, and countermeasures.

13. Different types of web application attacks, web application hacking methodology, and countermeasures.
14. SQL injection attacks and injection detection tools.
15. Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi- security tools.
16. Mobile platform attack vector, android vulnerabilities, jail breaking IOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools.
17. Firewall, IDS and honeypot evasion techniques, evasion tools, and Countermeasures.
18. Various cloud computing concepts, threats, attacks, and security techniques and tools.
19. Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.
20. Various types of penetration testing, security audit, vulnerability Assessment, and penetration testing roadmap.

What is New in the CEHV9 COURSE?

This is the worlds most advanced ethical hacking course with 18 of the most current security domains any ethical hacker will ever want to know when they are planning to beef up the information security posture of their organization. In 18 comprehensive modules, the course covers over 270 attack technologies, commonly used by hackers.

What we have?

- All trainers are certified – Practical oriented approach
- Live/ Real-time server administration training
- 24/7 phone support for technical issues resolution
- Flexible timings – Each candidate get personalized training
- Gets hand on experience in server side issue resolution
- Chance to visit live data centers
- Special training materials with screen shots, easy to learn
- 100 % pass assured exam assistance.