Step 1: IT Essentials & Computer Networks

IT Essentials = Topics Covered

Introduction to Computers

- Overview of IT and computing
- Types of computers and their uses
- Hardware vs. Software
- Computer boot process (POST)

Hardware Components

- Motherboard, CPU, RAM, storage devices
- Power supplies, cooling systems, input/output devices
- Hardware interaction = how CPU, RAM, and storage work

Operating Systems Installation

- OS types and basics
- Assembling a PC: identifying and connecting components
- Installing and preparing an OS (updates, drivers, configuration)

Virtualization Technologies

- OS and network virtualization
- Containerized and virtualized environments
- Cloud computing technologies

Partitioning & File Systems

- File system types and partitioning schemes
- RAID technologies and redundancy mechanisms

Enterprise Domain Management

- Domain controller fundamentals
- Installing and deploying Active Directory (AD)
- Joining a PC to a domain Troubleshooting in enterprise environments

Troubleshooting

- Hardware and software troubleshooting methods
- Practical troubleshooting in organizations

Computer Network Introduction

- Basic network concepts
- Network types: LAN, WAN, MAN, PAN
- Network topologies: Star, Mesh, Bus, Ring, Hybrid

End-of-topic exam

Step 2: Computer Networks = Topics Covered

Introduction to Computer Networks

- Basic networking concepts
- Network types (LAN, WAN, MAN, PAN)
- OSI and TCP/IP models = principles and functionality
- Understanding network layers and data flow
- (Note: “Moodboard” here seems to refer to visual network mapping examples.)

IP Addressing and Subnetting

- Binary, decimal, and hexadecimal conversion
- IPv4/IPv6 address classes
- Public vs. private IP addresses
- Subnetting and supernetting concepts
- Practical subnetting exercises

Network Hardware and Cabling

- NICs and MAC addresses
- Devices: Router, Switch, Firewall, Modem, Hub
- Ethernet standards (CAT5e, CAT6, Fiber Optic)
- Cable assembly and testing

Network Protocols and Services

- TCP vs UDP Common ports and protocols
- DHCP (DORA process) and DNS = how they work
- Mail protocols: SMTP, IMAP, POP3
- Remote access: Telnet and SSH NTP = time synchronization
- FTP and SFTP file transfers
- LDAP = directory access protocol

Switching Concepts and Mechanisms

- Role of switches
- MAC address table and switching logic
- Ethernet frame structure
- Collision and broadcast domains
- VLANs, port modes (access, trunk)
- Layer 2 and Layer 3 switching (Inter-VLAN routing, Router-on-a-Stick)

Switching Security and Redundancy

- Link aggregation concepts
- Configuring and verifying EtherChannel (LACP, PAgP)
- Spanning Tree Protocol(STP) concepts
- Port security configurations
- DHCP snooping and Dynamic ARP inspection

Routing Concepts

- Role of routers
- Difference between routers and switches
- Routing process and packet forwarding
- Default gateway and routing logic
- Router-on-a-Stick configuration

IP Routing Fundamentals

- Routing tables and how they work
- Static and dynamic routing
- Administrative distance and metrics
- Default and floating routes (backup routes)
- Directly connected, static, and dynamic routes
- Configuring and verifying static routes

Dynamic Routing Overview

- Advantages of dynamic routing
- Interior (IGP) vs Exterior (EGP) protocols
- Distance Vector vs Link-State protocols
- OSPF and EIGRP basics
- Configuring and troubleshooting OSPF/EIGRP

Network Security Basics

- Firewalls and Intrusion Detection Systems (IDS) AAA:
- Authentication, Authorization, Accounting (RADIUS, TACACS+)
- Secure communication (SSL/TLS, IPsec) How HTTPS works
- Common security threats (Phishing, DoS, DDoS, MITM)
- Web Application Firewall (WAF)
- Privileged Access Management (PIM/PAM)
- Data Loss Prevention (DLP)
- Mail SecurityConcepts

End-of-topic exam

Step 3: Blue Team (Defensive Security Training)

- SOC Fundamentals and Operations
- Threat Detection and Analysis
- Incident Response and Threat Intelligence
- SIEM (e.g., Splunk, QRadar, Wazuh)
- Malware, Network, Application, and Email Security
- Encryption, Access Control, PKI, and VPNs
- Windows and Web Security Hardening
- Final Project: Threat Detection & Defense Strategies

Outcome after completing the course: Graduates become Junior Cybersecurity(BlueTeam) Specialist , skilled in:

- Network and system defence
- Threat detection and mitigation
- SIEM monitoring and rule creation
- Vulnerability analysis and security protocols
- Hans-on use of tools like (Wireshark, Nmap, Splunk, QRadar and Wazuh