Networking Career Development Program Lectureflow

IT Fundamentals ====>Module 1) IT Fundamentals	4

- What is Information Technology?
- What is hardware and Network?
- What are software, Applications, Enterprise Applications
- What is project management
- What is security and compliance in IT industry
- Roles in IT industry
- How Internet works?
- What is website? What are applications
- Different Computer Parts
- How computer works
- COmputer Architecture - bits, bytes, types of memory
- Computer network - Lan, wan, topology, IP address, firewall, hubs and switches
- Cable, Fiber optics, wireless internet
- What is software?
- What is Programming?
- What is a database?
- Different Programming languages
- Web Browser
- search engines
- MUST HAVE FOR Getting basic job skills - word, ppt, excel, computer storage, files access, windows explorer
- Folder settings
- file extensions
- Using clipboard
- searching for files
- compressed files
- Save work, screenhsot, editing photos, playing videos
- emailing multiple files, compress, outlook
- email usage, scheduling calendars, creating meeting invites
- Organizing tasks
- hide folder - unhide folder
- Gmail Label wise Arrangement, Searching Google Drive Sharing
- Google - SLIDE,DOC,SHEETS
- Contacts Group wise Mail
- Task Management
- MS OFFICE - excel
- sheets, calculator ,basic formulas, multiple tabs, merge cells search, match and replace,
- data tables, filtter freeze and split frame, resizing print area
- Invoice creation
- Word Writing a paragraph, formatting Elements, create your resume,

- insert table, add pic Text alignment with image
- Word to pdf convert, pdf to word convertor

Hardware - Module 2) Hardware and Components Basics Understanding of Hardware and its components	10

- Day 1: Overview of Hardware Components Theory (1 hour): Introduction to motherboards, CPUs, RAM, GPUs, storage (HDD, SSD). Importance of each component in a computer system. Assignment: Create a diagram of a PC with labeled hardware components.
- Day 2: Motherboard and CPU Theory (30 min): Types of motherboards and CPU socket compatibility. Functions of the CPU and chipset. Practical (30 min): Identify the motherboard slots and ports.
- Day 3: RAM and Storage Theory (30 min): Types of RAM (DDR3, DDR4, DDR5) and storage (HDD vs. SSD, NVMe). Practical (30 min): Remove and reinstall RAM and storage drives.
- Day 4: GPUs and Cooling Systems Theory (30 min): Basics of GPUs and cooling systems (air vs. liquid cooling). Practical (30 min): Identify a GPU and cooling system in a PC setup.
- Day 5: Assemble and Disassemble a PC Practical (1 hour): Full hands-on session: Assemble and disassemble a desktop PC. Task: Document the process with labeled steps.

Module 3) A+ - Peripherals and Power Supply	10

- Operating System Basics
- Day 1: Overview of Peripherals Theory (1 hour): Functions of printers, scanners, webcams, and their connection interfaces.
- Operating System Administration
- Day 2: Power Supply Systems Theory (30 min): Basics of SMPS and UPS systems. Practical (30 min): Identify power cables and connectors.
- Working with Windows 10/11
- Day 3: Peripheral Troubleshooting Theory (30 min): Common issues and solutions for peripherals. Practical (30 min): Troubleshoot a non-working printer.
- Working with Mac OS and Linux
- Day 4: Connecting and Testing Peripherals Practical (1 hour): Set up and test peripherals like printers and webcams. Task: Resolve connectivity issues for a given setup.
- Users, Groups & permissions
- Operating System information, windows, Linux, macOS installation and adjust OS settings
- Maintaining & optimizing operating systems
- Working with command line interfaces
- Securing Computers

Module 4) A+ - Understanding and maintenance of Networks	5

- Local area networking

- Day 1: Introduction to Networking Hardware Theory (1 hour): Overview of modems, routers, switches, access points, and network cables.
- Wireless networking
- Day 2: Routers and Switches Theory (30 min): Basic functions and differences between routers and switches. Practical (30 min): Identify ports and LEDs on a router and switch.
- The Internet
- Day 3: Configuring Basic Network Hardware Theory (30 min): IP addressing basics and network configuration. Practical (30 min): Set up a router with default settings.
- Virtualization
- Day 4: Network Cable Types and Tools Theory (30 min): Types of cables (Ethernet, fiber optics) and tools (RJ45 crimper). Practical (30 min): Create a straight-through Ethernet cable
- Day 5: Network Testing Practical (1 hour): Connect devices to a network and test connectivity (ping, traceroute). Task: Write a report on how to set up and test a basic network.

Module 5) A+ - Troubleshooting and Helpdesk	**5**

- Mobile Operating Systems and Connectivity
- Day 1: Tools for Troubleshooting Theory (1 hour): Overview of tools (multimeter, POST card, software diagnostics).
- Troubleshooting Theory, OSs, and Security
- Day 2: Diagnosing Hardware Failures Theory (30 min): Common hardware issues and their symptoms. Practical (30 min): Test components using a multimeter.
- Understanding Operational procedure
- Day 3: BIOS and POST Troubleshooting Theory (30 min): Understanding BIOS and POST errors. Practical (30 min): Analyze POST error codes on a given setup.
- Day 4: Component-Specific Troubleshooting Practical (1 hour): Identify and fix issues in faulty components (RAM, GPU, storage). Task: Create a checklist for diagnosing hardware issues.
- Day 5: Case Study Practical (1 hour): Work on a scenario involving multiple hardware issues.

Module 6) N+ - Network Fundamentals and building networks	**15**

- Introduction to Networks
- Day 1: Introduction to Networking and the OSI Model Theory (1 hour): What is Networking? Overview of the OSI Model: Layers and their functions. Practical (1 hour): Use a network sniffer (e.g., Wireshark) to observe traffic and identify layers. Task: Create a diagram of the OSI Model with examples for each layer.
- Network Topologies
- Day 2: TCP/IP Suite Theory (1 hour): What is the TCP/IP Suite? Layers of TCP/IP: Application, Transport, Internet, and Network Access. Practical (1 hour): Analyze packet headers to identify the TCP/IP layer using Wireshark. Task: Compare OSI and TCP/IP models with real-world examples.
- OSI Layer
- Day 3: Introduction to IP Addressing Theory (1 hour): IPv4 and IPv6: Differences, structure, and importance. Subnetting basics: CIDR, subnet masks. Practical (1 hour): Assign static IPs to devices and verify connectivity. Task: Solve subnetting exercises and calculate valid subnets.

- Network Cable and connectors
- Day 4: Hands-on Subnetting Practical (1 hour): Divide a network into subnets and assign IP addresses to devices. Task: Document the steps to create a subnet plan.
- Ethernet standard and specification
- Day 5: Network Testing Tools Theory (30 min): Tools for network testing: Ping, Traceroute, nslookup. Practical (30 min): Use these tools to test connectivity in a LAN. Task: Report on the tools used and results obtained.
- Network devices
- Day 6: Introduction to Network Devices Theory (1 hour): Overview of switches, routers, hubs, firewalls, and access points. Practical (1 hour): Identify ports and functions of network devices in a setup. Task: Create a table comparing network devices and their features.
- IP addressing & Subnetting
- Day 2: Network Topologies Theory (1 hour): Types of network topologies: Bus, Star, Ring, Mesh. Practical (1 hour): Simulate a star topology using Cisco Packet Tracer. Task: Draw a diagram of topologies with examples.
- Configure IPv6 Addressing
- Day 3: Switch and Router Configuration Basics Theory (1 hour): Intro to VLANs and static routing. Practical (1 hour): Create and configure VLANs on a switch. Task: Configure a static route between two routers in a simulation.
- IP routing and routing protocols
- Day 4: Firewall Basics Theory (1 hour): Firewall types and use cases (hardware and software firewalls). Practical (1 hour): Configure basic rules in a software firewall (e.g., Windows Defender). Task: Document how to block and allow specific traffic using a firewall.
- Switching and VLANS
- Day 5: Review and Practice Practical (1 hour): Create a physical network topology in Cisco Packet Tracer. Task: Document the steps for configuring a small network.
- Wireless Networking

Module 7) N+ - Network security, Maintenance and Troubleshooting procedures	**9**

- Build a SOHO network
- Day 1: Introduction to Network Protocols Theory (1 hour): Overview of DNS, DHCP, HTTP/HTTPS, FTP, and SNMP. Practical (1 hour): Observe DNS and HTTP traffic using Wireshark. Task: Write a report on the role of DNS and HTTP in web communication.
- Secure networks with firewalls NAT, port filtering, packet filtering, and other methods
- Day 2: DHCP Configuration Theory (30 min): DHCP process: Discover, Offer, Request, Acknowledge. Practical (30 min): Configure a DHCP server in Cisco Packet Tracer. Task: Create a diagram showing the DHCP process flow.
- Authentication and Access Control
- Day 3: DNS Server Configuration Theory (30 min): How DNS resolves domain names to IPs. Practical (30 min): Configure a DNS server and test domain resolution. Task: Document the configuration and troubleshooting steps.
- Network Threats and Mitigation & Physical Security and Risk

- Day 4: Other Protocols in Action Theory (30 min): Introduction to FTP and SNMP. Practical (30 min): Set up an FTP server and transfer files between devices. Task: Create a table comparing FTP and HTTP.
- Wide Area Networks
- Day 5: Troubleshooting Network Services Practical (1 hour): Troubleshoot DNS and DHCP issues in a simulated network. Task: Document solutions for common DNS and DHCP issues.
- Troubleshooting Tools
- Days 1-5: Build and Configure a Small Office Network Deliverable: Fully functional LAN with: Proper IP addressing and subnetting. Configured DHCP and DNS services. VLANs for network segmentation. Simulated internet access via a router. Troubleshooting documentation for common issues. Task: Submit a detailed report on the network setup and configurations performed.
- Software and Hardware Tools
- Network Troubleshooting, Management, Monitoring, and Optimization

Module 8) CCNA - Routing and switching	**17**

- host-to-host communication Model
- Day 1: Static Routing Concepts Theory : What is static routing? Advantages and disadvantages of static routes. Practical : Configure static routes between two routers in Cisco Packet Tracer.
- Cisco Internetwork Operating System software
- Introduction to Dynamic Routing Theory: What is dynamic routing? Comparison between static and dynamic routing. Practical - Observe RIP routing updates in a pre-configured network.
- Describe LANs and the role of switches within LANs
- Day 3: Configuring RIP Theory: RIP concepts: Hop count, updates, and convergence. Practical : Configure RIP on a multi-router network. Task: Capture RIP updates using simulation tools and analyze them.
- Describe Ethernet as the network access layer of TCP/IP
- Day 4: Introduction to OSPF Theory: How OSPF works: Areas, LSAs, and cost. Practical: Observe OSPF adjacency formation in Packet Tracer. Task: Write down steps to configure OSPF in a network.
- describe the operation of switches
- Day 5: Configuring OSPF Practical: Configure OSPF on a network with multiple areas. Task: Simulate a scenario where a router fails and observe OSPF reconvergence.
- Day-6 Wireless Standard & Configuration : Wireless Setup, Channel Selection & Avoiding Interference, Wireless Security, MAC Filtering & Access Control Lists
- Switching Basics Theory: Switch operation: MAC address table, frame forwarding. Practical: Observe MAC table population in a simulated network. Task: Explain the process of frame forwarding in switches.
- VLAN Concepts Theory: VLANs: Segmentation, benefits, and use cases. Practical : Create VLANs on a switch and assign ports. Task: Document VLAN configurations.
- VLAN Trunking and Access Ports Theory : Trunking protocols (802.1Q, ISL). Practical: Configure trunk ports on a switch. Task: Simulate communication between VLANs using trunk ports.
- Inter-VLAN Routing Basics Theory: Methods of inter-VLAN routing: Router-on-a-stick, Layer 3 switches. Practical: Configure router-on-a-stick for inter-VLAN communication. Task: Troubleshoot

inter-VLAN routing issues in a simulated scenario.
- Weekly Review and Practice Practical (2 hours): Create a network with multiple VLANs and configure inter-VLAN routing. Task: Submit a report on VLAN and inter-VLAN routing setup.

Module 9) CCNA - VLANs and Inter-VLAN Routing	13

- Install a switch and perform the initial configuration
- 1: Introduction to WAN Technologies Theory : WAN vs. LAN: Key differences and use cases. MPLS basics. Practical : Observe MPLS routing in a pre-configured network. Task: Document MPLS benefits over traditional routing.
- Describe the TCP/IP Internet layer, IPv4, its addressing scheme, and subnetting
- 2: Introduction to VPNs Theory : Types of VPNs: Site-to-site, remote access. Practical : Configure a basic site-to-site VPN in Packet Tracer. Task: Submit configuration steps for a VPN.
- Explain host-to-host communications across switches and routers
- 3: NAT and PAT Concepts Theory : What is NAT/PAT? Importance in IP address conservation. Practical : Configure NAT and PAT on a router. Task: Simulate external connectivity using NAT/PAT.
- Describe the operation, benefits, and limitations of static routing
- 4: Weekly Practice and Troubleshooting Practical: Simulate a WAN setup with VPN and NAT. Task: Troubleshoot connectivity issues in the setup. Checkpoint: Quiz: WAN technologies, VPNs, and NAT/PAT. Practical Evaluation: Configure and troubleshoot a WAN.
- Describe, implement, and verify Virtual Local Area Networks (VLANs) and trunks
- Inter-VLAN Routing Concepts ???? Theory: Why is Inter-VLAN Routing Needed? Problem: VLANs cannot communicate with each other Solution: Use a router or Layer 3 switch Methods of Inter-VLAN Routing: Router-on-a-Stick (RoS) (Single router interface for multiple VLANs) Layer 3 Switch Routing ???? Practical: Router-on-a-Stick Configuration ???? Hands-on Lab Enable router sub-interfaces for VLANss
- Describe the application and configuration of inter-VLAN routing
- Layer 3 Switch Inter-VLAN Routing ???? Theory: Using a Layer 3 Switch No need for a router Uses SVIs (Switch Virtual Interfaces) for routing Faster than Router-on-a-Stick ???? Practical: Configuring Inter-VLAN Routing on a Layer 3 Switch ???? Hands-on Lab Enable IP Routing
- Explain the basics of dynamic routing protocols
- Describe IPv6 addresses, and configure and verify basic IPv6 connectivity
- Describe the terms of Open Shortest Path First (OSPF)
- Configure link aggregation using EtherChannel
- Describe the purpose of Layer 3 redundancy protocols

Module 10) CCNA - WAN Technologies	9

- Introduction IP Services, NAT, Terms for NAT, Adv of NAT, Dis NAT, Types of NAT, Static NAT Configuration
- a.Introduction to WAN Technologies : Definition of WAN, Types of WAN Connections, WAN Devices: CSU/DSU, WAN Aggregators.
- Dynamic NAT, Dynamic NAT Configuration

- b.WAN Authentication Protocols: Authentication is Needed in WAN, WAN Authentication Protocols: HDLC, PPP Authentication (PAP, CHAP, MS-CHAP).
- Port Address Translation, PAT Configuration
- c.AAA (Authentication, Authorization, Accounting): Three core functions, AAA in Networking & Security, AAA Deployment Models..
- Explain vtp and configuring
- d.RADIUS & TACACS+ : TACACS+ & RADIUS Features, RADIUS Authentication Process, TACACS+ Use Cases, RADIUS vs. TACACS+
- Network Time Protocol, NTP Configuration
- Dynamic Host Configuration Protocol, DHCP Configuration
- e.Hybrid WAN (SD-WAN) : Introduction to SD-WAN, Key Benefits of SD-WAN
- Explain Syslog, Syslog Server Configuration
- Simple Network Management Protocol, SNMP-V3 Configuration.

Module 11) CCNA - Network Troubleshooting	**9**

- •Introduction to Password, Username & Password, Console, AUX, VTY, Enable Password, Enable Secret, SSH, AAA Server, Switch Port Security
- 1: Common Network Issues Theory : Common hardware and software issues. Practical : Identify faulty devices in a simulated network. Task: Create a troubleshooting checklist.
- •SSH Configure, Radius server configuration AAA server, DNS configure, HTTP configure
- 2: Using Ping and Traceroute Theory : How Ping and Traceroute work. Practical : Use Ping and Traceroute to test connectivity. Task: Report findings for a simulated connectivity issue.
- •Configure Switch Port Security, Protect Mode, Restrict Mode.
- 3: Using Advanced Tools Theory : Introduction to tools like Wireshark, Nmap. Practical : Use Wireshark to capture and analyze network traffic. Task: Document key findings from a packet capture.
- •Access Control List, Purpose of ACL, Types and Classification of ACL, Diff between Standard and Extended ACLs
- 4-5: Weekly Practice and Troubleshooting Practical (2 hours): Resolve connectivity issues in a complex network. Task: Submit troubleshooting steps and resolutions.
- •Numbered Access Control Lists, Standard ACL Configuration, Extended ACL Configuration
- •Named Access Control Lists, Name Standard ACL Configuration, Name Extended ACL Configuration
- •WAN Technologies, Fundamentals of WAN
- •2 WAN Device, DSL, Asymmetrical DSL, Symmetric DSL
- •Describe VPN Configuration with cisco practical’s
- Point-to-Point Protocol (PPP) PPP Configure, CHAP

Module 1) Windows Server Basics & Installation	**13**

- Installing Windows Server
- 1: Basics of Windows Server and Active Directory Theory : Overview of Windows Server and its roles. Introduction to Active Directory (AD): Concepts, architecture, and uses. Practical : Install

Windows Server and configure Active Directory Domain Services (AD DS). Task: Submit a document on the steps to install and configure AD DS.

- Basic Configuration
- 2: User Management in Active Directory Theory : Creating and managing users, groups, and OUs in AD. Best practices for user account management. Practical : Create user accounts, groups, and organizational units (OUs). Task: Submit a screenshot of the AD setup with user accounts and OUs.
- Dashboard in windows server
- 3: Group Policies Theory : What is Group Policy? Configuring Group Policy Objects (GPOs) to enforce security and administrative settings. Practical : Create and apply GPOs for password policies and desktop restrictions. Task: Document the GPO settings applied and their impact.
- Understanding Server Roles and Features
- 4: File Sharing in Windows Server Theory : Introduction to file sharing and permissions. NTFS vs. Share permissions. Practical : Configure a shared folder with specific permissions. Task: Simulate access scenarios with different user permissions.
- Introduction to Active Directory, Forests, Trees and OU's
- 5: Weekly Review and Practice Practical (2 hours): Set up a basic AD environment with user accounts, GPOs, and shared resources. Task: Submit a report summarizing the setup with screenshots and configurations. Checkpoint: Quiz: Active Directory concepts, GPOs, and file sharing. Practical Evaluation: Configure AD with GPOs and shared folders.
- Adding our First Roles - AD and DNS
- Domain Controllers
- Editions and Requirements
- Drivers and Services

Module 2) Windows Networking Services	**15**

- Shares and Permissions
- 1: DNS in Windows Server Theory : Introduction to DNS: Concepts, zones, and records. Configuring DNS in Windows Server. Practical : Set up DNS zones and create records. Task: Simulate a DNS resolution scenario and submit findings.
- GPO - Overview
- 2: DHCP in Windows Server Theory : How DHCP works: Scope, leases, and reservations. Configuring DHCP on a Windows Server. Practical : Set up a DHCP scope and allocate IP addresses. Task: Document the DHCP configuration with screenshots.
- DNS and DHCP or IPAM
- 3: File Server Role Theory : File server overview and use cases. Configuring shared folders with permissions. Practical : Set up shared folders and assign NTFS and share permissions. Task: Test file access from client systems and document results.
- Implement Core and Distributed Network Solutions
- Virtualiztion with Hyper-V
- 4: Print Server Role Theory : Overview of the Print Server role. Configuring printers and managing print queues. Practical : Configure a network printer and set up print permissions. Task: Submit a report on the print server setup and test results.

- 5: Weekly Review and Practice Practical (2 hours): Configure DNS, DHCP, and file/print servers in a simulated network. Task: Submit a report with all configurations and tests. Checkpoint: Quiz: DNS, DHCP, file server, and print server roles. Practical Evaluation: Configure and troubleshoot networking services in Windows Server.
- Print Server
- Web Services : IIS
- HYPER V
- Remote access and RDS
- RDS
- WSUS

Module 3) Windows Server Security and Maintenance	**13**

- Install and Configure Active Directory Domain Services (AD DS)
- Hardware and Storage
- •Install and Configure Active Directory Domain Services (AD DS)
- 1: Backup Strategies Theory : Types of backups (full, incremental, differential). Backup best practices for Windows Server. Practical : Configure Windows Server Backup and schedule regular backups. Task: Submit a report on backup configurations.
- Manage and Maintain AD DS
- RAID in Action
- •Hardware and Storage
- 2: Windows Defender Theory : Overview of Windows Defender: Features and functionalities. Configuring real-time protection and scheduled scans. Practical : Perform a full system scan and configure Defender policies. Task: Document threats detected (if any) and actions taken.
- Create and Manage Group Policy
- SAN and ISCSI
- •Manage and Maintain AD DS
- 3: Patch Management Theory : Importance of patch management. Using WSUS for patch deployment. Practical : Configure WSUS and deploy patches to client machines. Task: Create a patch report showing successful installations.
- Implement Active Directory Certificate Services (AD CS)
- Advanced AD Topics
- •RAID in Action
- 4: Security Policies Theory : Best practices for server security: Password policies, account lockout. Hardening a Windows Server. Practical : Configure security policies and audit logs. Task: Submit a report on the security policies implemented.
- Implement Identity Federation and Access Solutions
- FSMO Roles
- •Create and Manage Group Policy
- Active Directory Certificate Services (AD CS
- Implement of Server Maintenance
- •SAN and ISCSI

- 5: Weekly Review and Practice Practical (2 hours): Implement security policies and set up a backup and monitoring system. Task: Submit a report on server security and maintenance configurations. Checkpoint: Quiz: Backup strategies, Windows Defender, and security policies. Practical Evaluation: Implement server security and backup configurations.
- Implement of Server Updates
- •Implement Active Directory Certificate Services (AD CS)
- Checkpoint Project: Deploy a Windows Server for a Small Business 1-5: Project Execution Deliverable: A fully functional Windows Server setup, including: Active Directory with user accounts and GPOs. Networking services (DNS, DHCP). Shared resources (file and print servers). Security policies, backups, and documentation. Final Checkpoint: Evaluation: Review the server setup, configurations, and functionality. Assess documentation quality and ability to troubleshoot.
- Implement of Troubleshooting Methodology
- •Advanced AD Topics
- •Implement Identity Federation and Access Solutions
- •FSMO Roles
- •Implement of Server Maintenance
- •Implement of Server Updates
- Implement of Troubleshooting Methodology13

Module 1) Linux server - Linux Basics and Networking	**13**

- •Accessing the Command Line
- History & Evolution of Linux ? Linux Distributions (Ubuntu, CentOS, Debian, RHEL) ? Understanding CLI vs GUI
- •Managing Files from the Command Line
- 2. Basic Commands
- •getting Help in Red Hat Enterprise Linux
- Installing Linux (Ubuntu Server / CentOS) on VirtualBox / VMware ? Basic System Configuration (Hostname, Static IP, SSH Setup) ? Managing Users & Groups
- •Creating, Viewing, and Editing Text Files
- Understanding File System Structure (/, /var, /etc, /home) ? File & Directory Permissions (chmod, chown, chgrp) ? Symbolic & Hard Links
- 5. Logical Volume Management (LVM)
- •Controlling Access to Files with Linux File System Permissions
- 6. RHEL 8 LVM based Installation
- •Monitoring and Managing Linux Processes
- Managing Users, Groups, and Sudo Privileges ? SSH Security & Key-Based Authentication ? Understanding SELinux & AppArmor
- 8. Controlling Access to the Files
- 9. Enhanced User Security with SUDO
- Configuring Network Interfaces (ifconfig, ip, nmcli) ? Understanding DNS, DHCP, and Static IP Configuration ? Firewall Management (iptables, firewalld, ufw)
- 11.Booting Procedure of RHEL7/8 and Troubleshooting

Module 2) Linux server - Linux Services and Permissions	13

- •Configuring and Securing OpenSSH Service
- Introduction to Linux Services Theory (1 hour): Understanding services in Linux: Systemd, init.d. Introduction to Apache and Nginx web servers. Practical (1 hour): Install Apache and start/stop services using systemctl. Task: Verify the web server is running by accessing it in a browser.
- •Analyzing and Storing Logs
- Hosting a Static Website Theory (1 hour): Overview of web hosting with Apache/Nginx. File placement and basic configurations for static sites. Practical (1 hour): Host a simple HTML page on the web server. Task: Customize and host a static webpage.
- •Managing Red Hat Enterprise Linux Networking (IPv4 and IPv6)
- Linux Permissions and Security Theory (1 hour): File and directory permissions in Linux: chmod, chown. Users, groups, and access control. Practical (1 hour): Set up user-specific access to files. Task: Demonstrate restricted access to a directory for specific users.
- •Archiving and Copying Files Between Systems
- Combining Services and Permissions Theory (1 hour): Integrating permissions with web hosting for secure access. Practical (1 hour): Secure access to a hosted site using permissions. Task: Test and document restricted access to web resources.
- •Installing and Updating Software Packages
- Managing SELinux (Basics)
- •Accessing Linux File Systems
- 12. Manage Installed Services
- •Using Virtualized Systems
- 13. Introduction to Firewalld
- •Comprehensive Review Use Boolean settings to modify system SELinux settings
- 14. Backup and Restore (tar&gzip)
- Diagnose and address routine SELinux policy violations
- 15. Job Automation with Cronjobs
- 16. Software Management
- 17. Managing Processes
- MariaDB

Module 3) Linux server - Server Security and Automation	13

- •Improving Command-line Productivity
- Secure Shell (SSH) Theory (1 hour): Importance of SSH for secure communication. Configuring and securing SSH. Practical (1 hour): Configure SSH with key-based authentication. Task: Disable password login and document the configuration.
- •Scheduling Future Tasks
- Firewall Configurations Theory (1 hour): Basics of firewalls and ufw/iptables in Linux. Creating rules for inbound and outbound traffic. Practical (1 hour): Configure ufw to allow SSH and block other services. Task: Document the configured firewall rules.
- •Tuning System Performance

- Automation with Crontab Theory (1 hour): Scheduling tasks using crontab. Use cases for automation in Linux. Practical (1 hour): Automate backups of critical directories. Task: Submit a backup configuration and log output.
- •Controlling Access to Files with ACLs
- SELinux Basics Theory (1 hour): Introduction to SELinux and its role in server security. Understanding SELinux modes and contexts. Practical (1 hour): Enable SELinux and troubleshoot access denials. Task: Document an SELinux configuration with resolved issues.
- •Managing SELinux Security
- Implement SSH, firewall, automation, and SELinux on a Linux server. Task: Submit a comprehensive report on server security configurations.
- Server web server with other services
- 17. Administrating Remote System
- 18. NFS (Network File System) Server
- 19. Samba Server
- 20. DNS (Domain Name System) Server
- 21. Web Server (Apache)
- setting up a kick start server

Module 8) Introduction to Cloud Computing	**5**

- Contrasting Cloud Services
- Theory (1 hour): Overview of Cloud Computing Definition and benefits of cloud computing. Key characteristics: On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Practical (2 hours): Navigate the AWS or Azure Management Console. Identify key services offered by the platform.
- Contrasting Cloud Delivery Models
- Theory (1 hour): Cloud Service Models (IaaS, PaaS, SaaS) Examples of each model (e.g., AWS EC2 for IaaS, Google App Engine for PaaS, Office 365 for SaaS). Practical (2 hours): Set up an EC2 instance on AWS or a similar virtual machine on Azure.
- Cloud Characteristics and Terms
- Theory (1 hour): Cloud Deployment Models (Public, Private, Hybrid, Community) Use cases and pros/cons of each deployment model. Practical (2 hours): Explore and compare deployment models through case studies.
- Object Storage Concepts
- Theory (1 hour): Shared Responsibility Model in Cloud Computing Understanding roles and responsibilities between cloud providers and users. Practical (2 hours): Configure user permissions and policies in the cloud environment.
- Task: Compare deployment models for a given use case. Students choose a use case (e.g., hosting a website) and evaluate the suitability of public, private, and hybrid clouds. Review (2 hours): Present and discuss findings.

Module 9) Cloud Networking	**5**

- Theory (1 hour): Introduction to Cloud Networking Virtual Private Cloud (VPC) basics and components. Practical (2 hours): Create a basic VPC on AWS with a public and private subnet.
- Theory (1 hour): Load Balancers Types of load balancers (application, network, classic). Importance in high availability and fault tolerance. Practical (2 hours): Set up and configure a load balancer in AWS.
- Theory (1 hour): Auto-scaling Concepts How auto-scaling works to handle varying workloads. Practical (2 hours): Configure auto-scaling groups based on traffic metrics.
- Theory (1 hour): Security in Cloud Networking Firewalls, security groups, and network ACLs. Practical (2 hours): Set up security groups to allow and block specific traffic.
- Task: Design a scalable cloud architecture. Students propose and document a scalable and secure architecture for a sample application. Review (2 hours): Present and critique architecture designs.

Module 10) Storage in the Cloud	**5**

- Policies and Procedures in a Cloud Environment
- Theory (1 hour): Introduction to Cloud Storage Services Overview of AWS S3, EBS, and Glacier. Practical (2 hours): Create and configure an S3 bucket on AWS.
- Diagnose Remediate, and Optimize Physical Host Performance
- Theory (1 hour): Storage Security Bucket policies, encryption, and access management. Practical (2 hours): Apply bucket policies and enable server-side encryption.
- Host and Guest Performance Concepts
- Theory (1 hour): Lifecycle Policies and Cost Optimization Managing data lifecycle with automated transitions. Practical (2 hours): Implement lifecycle policies to move objects from S3 to Glacier.
- Implement Appropriate Testing Techniques when Deploying Cloud Services
- Theory (1 hour): EBS vs. S3: Choosing the Right Storage Option Key differences and use cases. Practical (2 hours): Attach and manage EBS volumes for an EC2 instance.
- Accessing AWS, Azure and Google cloud Platforms
- Task: Implement lifecycle policies for storage objects. Students configure lifecycle policies and monitor transitions. Review (2 hours): Discuss storage strategies and cost implications.

Module 11) Security in the Cloud	**5**

- Resource Monitoring Techniques
- Theory (1 hour): Introduction to IAM Overview of IAM and its importance in cloud security. Key concepts: Users, Groups, Roles, and Policies. Practical (2 hours): Navigate the IAM dashboard in AWS or Azure. Create users and groups.
- Best Practice for Appropriate Allocation of Physical & Virtual Host Resources
- Theory (1 hour): Policies and Permissions Types of policies: Inline and managed. JSON-based policy syntax. Practical (2 hours): Write and attach custom policies to users and groups.
- Appropriate Remote Access Tools
- Theory (1 hour): Multi-Factor Authentication (MFA) Importance of MFA in securing cloud accounts. Configuring MFA in AWS or Azure. Practical (2 hours): Enable MFA for a cloud account. Test access scenarios with and without MFA.
- Network & Storage Security Concepts, Tools and Best Practices

- Theory (1 hour): Best Practices in IAM Implementing least privilege access. Regularly reviewing IAM policies. Practical (2 hours): Analyze an existing IAM configuration and optimize it using best practices.
- Encryption Technologies and Methods
- Task: Implement least privilege access for a cloud account. Students audit a cloud account and configure roles and policies for least privilege access. Review (2 hours): Present configurations and discuss improvements.
- Identifying Access Control Methods
- Implementing Guest and Host Hardening Techniques

Module 12) Cloud Security Essentials	**5**

- Disaster Recovery Methods and Concepts
- Theory (1 hour): Encryption in the Cloud Overview of encryption methods: Symmetric and asymmetric. Server-side vs. client-side encryption. Practical (2 hours): Implement server-side encryption for an S3 bucket or equivalent.
- Deploying Solutions to Meet Availability Requirements
- Theory (1 hour): Key Management Systems (KMS) Creating and managing keys in AWS KMS or Azure Key Vault. Key rotation policies. Practical (2 hours): Configure a KMS key and enable automatic key rotation.
- Theory (1 hour): Threat Detection in the Cloud Tools like AWS GuardDuty, Azure Security Center. How threat detection works in real-time. Practical (2 hours): Enable and monitor a threat detection tool for a cloud environment.
- Theory (1 hour): Security Best Practices Protecting data in transit and at rest. Regular security audits. Practical (2 hours): Conduct a basic vulnerability scan for a cloud environment using open-source tools or native features.
- Task: Conduct a vulnerability scan for a cloud environment. Students document vulnerabilities and propose mitigation strategies. Review (2 hours): Share findings and discuss solutions.

Module 13) - Compliance And Monitoring	**5**

- Theory (1 hour): Introduction to Cloud Compliance Standards Overview of GDPR, HIPAA, and other major standards. Cloud providers' role in compliance. Practical (2 hours): Identify compliance features in AWS or Azure.
- Theory (1 hour): Setting Up Monitoring Systems Importance of monitoring in cloud environments. Tools: AWS CloudWatch, Azure Monitor. Practical (2 hours): Set up basic monitoring for resources like VMs or storage.
- Theory (1 hour): Logging and Auditing Tools like AWS CloudTrail for tracking user activities. Importance of audit trails for compliance. Practical (2 hours): Enable and analyze logs using CloudTrail or Azure Activity Logs.
- Theory (1 hour): Creating Alerts and Notifications Setting thresholds for resource usage. Integration with email or SMS alerts. Practical (2 hours): Configure alerts for CPU utilization and storage limits.
- Task: Create an alerting system for resource usage. Students configure alert rules and test notifications. Review (2 hours): Discuss alert configurations and enhancements.

Module 14) Secure and Monitor a Cloud Infrastructure	5

- Theory (1 hour): Designing a Secure Cloud Infrastructure Key considerations for security and monitoring. Practical (2 hours): Plan the architecture for a secure and monitored cloud environment.
- Project Work: Tasks: Implement IAM roles and least privilege access. Configure server-side encryption and key rotation. Enable monitoring and logging tools. Set up an alerting system for critical resources.
- Presentation and Evaluation (3 hours): Students present their secured and monitored cloud infrastructure. Peer and trainer feedback on implementation.

Module 10) Introduction to Cybersecurity	5

- •Basic computer hardware
- Theory (1 hour): Overview of Cybersecurity Importance of cybersecurity in modern enterprises. Key terms and concepts: Cybersecurity, threats, vulnerabilities, and risks. Practical (2 hours): Explore cybersecurity dashboards and tools. Demonstration of a basic simulated phishing attack setup using email templates.
- •Types of Operating System
- Theory (1 hour): Threat Landscape Types of cyber threats: Phishing, ransomware, insider threats, etc. Practical (2 hours): Simulate a phishing attack in a controlled environment using open-source tools (e.g., SET toolkit). Demonstrate email spoofing and prevention techniques.
- •Operating system installation
- Theory (1 hour): Security Frameworks Overview of NIST, ISO 27001, and CIS Controls. Practical (2 hours): Map security measures to a given framework.
- •Linux Essentials
- •Windows security
- •Networking technologies
- •IP addressing
- •OSI & Network protocols
- •Routers/modems/switches
- •Wireless Technology
- Data Backup & recovery

Module 9) Cyber Security - Virtualization and Cloud Basics	5

- •Hackers & Hacking Methodologies
- Theory (1 hour): Introduction to Virtualization What is virtualization, types, and benefits? Overview of hypervisors: Type 1 (bare-metal) and Type 2 (hosted). Practical (2 hours): Install and configure a hypervisor (VirtualBox or VMware Workstation). Create a virtual machine (VM).
- •Types of hackers
- Theory (1 hour): Cloud Computing Basics Definition, types (IaaS, PaaS, SaaS), and use cases. Comparison of AWS, Azure, and Google Cloud. Practical (2 hours): Explore AWS free tier: Set up an account and navigate the console. Launch a basic virtual server (EC2 instance) on AWS.
- •Cyber Security threats

- Theory (1 hour/day): Key cloud concepts: Storage, databases, and networking. Security in cloud environments: Identity and Access Management (IAM). Practical (2 hours/day): Set up storage on AWS (S3 bucket). Configure IAM roles for access control.
- •Methods of Foot printing
- •Google Hacking Technique
- •Google Advance Search Operators
- •Scanning network
- •Check Live system, open ports, Services
- •Vulnerability Scanning
- •Describing VAPT and VAPT Reports Writing
- •Describing VAPT tools (Burp Suite, OWASP)
- Proxy servers

Module 11) Malware and Threat Detection	**5**

- •Types of Password Attacks
- Theory (1 hour): Types of Malwares Viruses, worms, ransomware, Trojans, spyware, adware. Practical (2 hours): Analyse a sample malicious file using VirusTotal. Demonstrate the effects of malware in a sandboxed environment. ,
- •Key logger and Anti Keyloggers
- Theory (1 hour): Indicators of Compromise (IoCs) How to identify IoCs in systems and networks. Practical (2 hours): Use Splunk or ELK Stack to monitor logs and detect anomalies.
- •Offline attack using live boot OS
- Theory (1 hour): Malware Analysis Basics Steps in static and dynamic malware analysis. Practical (2 hours): Use tools like Any.Run or Cuckoo Sandbox to analyze malware behavior.
- •System Hacking with Kali Linux
- Theory (1 hour): Threat Intelligence Platforms Introduction to tools like MISP and Open Threat Exchange (OTX). Practical (2 hours): Collect and analyze threat intelligence data for a specific domain.
- •Spyware and Antispyware
- Task: Create a detailed report of a malware analysis performed in class. Include IoCs, impact, and mitigation recommendations. Review and Q&A (3 hours): Present reports and discuss findings.
- •Steganography Techniques Clearing Logs
- •Trojans /Backdoors, Viruses, Worms
- •Create Virus and Worms
- Anti-Virus

Module 12) Penetration Testing Basics	**5**

- •Session Hijacking Process
- Theory (1 hour): Phases of Penetration Testing Planning, reconnaissance, scanning, exploitation, reporting. Practical (2 hours): Use tools like Nmap to perform a basic network scan.
- •Cross-Site Scripting XSS Attacks

- Theory (1 hour): Vulnerability Scanning Basics Common vulnerabilities and scanning tools (Nessus, OpenVAS). Practical (2 hours): Install and configure Nessus to scan a target system.
- •Web Application Denial-of-Service DoS Attack
- Theory (1 hour): Exploitation Basics Common techniques and tools (Metasploit Framework). Practical (2 hours): Exploit a simulated vulnerable system in a controlled lab.
- •Buffer Overflow Attacks
- Theory (1 hour): Reporting and Recommendations How to create an effective vulnerability assessment report. Practical (2 hours): Prepare a sample report based on the scan conducted earlier.
- •Cookie/Session Poisoning
- Task: Complete a full vulnerability assessment on a provided system. Submit a detailed report with prioritized recommendations. Review and Q&A (3 hours): Present and defend vulnerability assessment reports.
- •Hacking Web Servers
- SQL Injection Attacks

Module 13) Advanced Cybersecurity Concepts	**15**

- •wireless Threats
- Secure Network Architecture Day 1 Theory (1 hour): Introduction to Secure Network Architecture Importance of securing network infrastructure. Key concepts: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Practical (2 hours): Install Snort on a virtual machine. Configure Snort to monitor a simple network.
- •wireless Hacking Methodology
- Theory (1 hour): Zero Trust Security Model Principles of Zero Trust: "Never Trust, Always Verify." Implementation strategies: Micro-segmentation, least privilege access. Practical (2 hours): Create a Zero Trust policy for a sample network using simulated tools.
- •Mobile platform attack vector
- Theory (1 hour): Network Segmentation Benefits of segmentation: Improved security, limited attack surface. Methods: VLANs, subnets, and firewalls. Practical (2 hours): Use a virtual lab to set up VLANs and implement network segmentation.
- •Mobile Hacking Tools
- Theory (1 hour): Advanced IDS/IPS Concepts Analysing traffic patterns and detecting anomalies. Practical (2 hours): Use Snort to simulate and detect a specific type of attack (e.g., SQL injection).
- •Android Phone hacking
- Task: Secure a given network topology. Students design a segmented network with IDS/IPS implementation. Review and Q&A (3 hours): Evaluate student designs and discuss improvements.
- Android vulnerabilities hash calC
- Cryptography Basics Day 1 Theory (1 hour): Introduction to Cryptography Importance of cryptography in cybersecurity. Key differences between symmetric and asymmetric encryption. Practical (2 hours): Demonstrate AES (Advanced Encryption Standard) and RSA encryption using online tools.
- Theory (1 hour): SSL/TLS Protocols How SSL/TLS ensures secure communication over the internet. The role of digital certificates. Practical (2 hours): Set up an HTTPS website on a local server. Install

and configure SSL certificates using Let's Encrypt.

- Theory (1 hour): Hashing and Digital Signatures Explanation of hashing algorithms (SHA-256, MD5). Role of digital signatures in verifying authenticity. Practical (2 hours): Demonstrate hashing using tools like OpenSSL.
- Theory (1 hour): Real-World Cryptography Use Cases Encryption in messaging apps, VPNs, and file storage. Practical (2 hours): Encrypt and decrypt files using GPG (GNU Privacy Guard).
- Cloud Security Day 1 Theory (1 hour): Introduction to Cloud Security Principles Key principles: Data confidentiality, availability, and integrity. Common cloud security threats and mitigation strategies. Practical (2 hours): Explore AWS or Azure Management Console.
- Theory (1 hour): Shared Responsibility Model Differentiating user and cloud provider responsibilities. Practical (2 hours): Configure Identity and Access Management (IAM) roles and policies in AWS.
- Theory (1 hour): Securing Cloud Data and Applications Methods: Encryption, backup, and monitoring. Practical (2 hours): Enable and configure cloud monitoring tools (e.g., AWS CloudWatch).
- Theory (1 hour): Cloud Security Compliance Overview of standards like GDPR, HIPAA, and PCI DSS. Practical (2 hours): Perform a compliance audit using AWS Trusted Advisor.
- Cyber Security Architecture Day 1–2 Theory (1 hour/day): Designing Secure Architectures Combining secure network and cloud principles into an integrated system. Practical (2 hours/day): Design a secure architecture using VLANs, IDS/IPS, IAM policies, and cloud security tools.
- Ethical Hacking and Forensics Theory: Ethical Hacking Framework, Digital Forensics Basics. Practical: Perform a forensic analysis of a compromised system.