aci LEARNING | CollegePro

2026

Lab Sets

Table of Contents

Programming

Introduction to Programming Using Python

25 Labs

Designed to build foundational Python skills through guided practice, the labs progress from core syntax and data handling to control flow, file operations, functions, and standard library usage—making them ideal for introductory programming, IT, cybersecurity, and data-focused pathways.

Working with Primitive Data Types
Create Python scripts that use variables and primitive data types to store, evaluate, and manipulate values, forming the foundation for accurate program logic.

Working with Multiple Assignment Statements
Apply multiple assignment statements to efficiently assign and manage multiple values within Python programs.

Converting Types in Python
Determine variable data types using the type() function and perform explicit data type conversions to ensure correct program behavior.

Creating Lists
Create Python lists and access individual elements to manage and reference collections of related data.

Modifying Lists
Modify list contents by updating values, appending new items, deleting existing elements, and identifying item positions using indexes.

Sorting and Reversing Lists
Control the order of list data by sorting and reversing list elements using Python's built-in list operations.

Slicing Lists
Extract and manipulate subsets of list data using slicing techniques, including negative indexing and partial list selection.

Working with Operators
Use arithmetic, comparison, and logical operators to construct expressions that evaluate conditions and perform calculations.

Determining Operator Precedence
Evaluate expressions accurately by applying identity and membership operators and understanding operator precedence rules.

Working with If Statements
Implement conditional logic using if, if-else, and nested if-else statements to control program execution paths.

Using Compound Conditional Expressions
Combine multiple conditions into compound conditional expressions to support more complex decision-making logic.

Working with For Loops
Use for loops with break and continue statements to iterate over data sets and control loop execution.

Working with While Loops
Implement while loops to repeatedly execute code based on dynamic conditions.

Introduction to Programming Using Python

Nesting For Loops
Use nested for loops to perform repeated operations across multiple dimensions of data.

Reading Files
Open, read, and close text files to retrieve persistent data within Python programs.

Copying Files
Copy data from one text file to another, enabling duplication and transfer of file contents through Python.

Merging Files
Combine multiple text files into a single output file to consolidate file-based data.

Reading Console Inputs and Formatting Outputs
Accept user input from the console and generate formatted output, including building a simple calculator application.

Reading Command Line Arguments
Access and process command-line arguments to control program behavior at runtime.

Defining Functions
Define reusable functions to structure Python programs and implement modular logic, including calculator functionality.

Using Default Arguments
Define functions with default argument values to support flexible and optional input parameters.

Using Keyword and Positional Arguments
Control function execution by passing arguments using positional and keyword syntax.

Handling Exceptions
Implement exception handling using try-except blocks to manage runtime errors and prevent program failure.

Using Math and Random Modules
Perform mathematical calculations using the math module and generate pseudo-random values using the random module, including seed configuration.

Displaying Datetime, Working Directory, and File Metadata
Retrieve and display date and time values, identify and manipulate the current working directory, and access file metadata such as creation and modification timestamps.

Scripting Fundamentals

15 Labs

Designed to build practical scripting skills through guided Python exercises, these labs progress from core data types and control structures to file parsing, secure coding, visualization, and basic machine learning concepts—making them ideal for introductory programming, automation, and IT-focused pathways.

Advanced Data Structure Usage
Apply advanced data structures to organize, store, and manipulate complex data within Python programs.

File I/O, String Parsing, and Data Structures
Read and write data to files, parse string content, and store processed information using appropriate data structures.

Tuples (Arrays), Error Handling, and Secure Programming
Use tuples for structured data storage, implement error handling to manage unexpected conditions, and apply secure programming practices to reduce risk.

Loops
Use loop constructs to repeat operations based on defined conditions and control execution flow within Python programs.

Math in Python
Perform mathematical operations using Python's built-in math capabilities to support calculations and program logic.

Getting Started with Python on Ubuntu – Running from the Command Line
Run Python programs from the Linux command line and navigate the Ubuntu environment to execute scripts.

Introduction to Control Structures and Data Types
Use core data types and control structures to store information and direct program execution.

Getting Started with Python on Ubuntu – Writing Your First Program
Create and execute a Python program within an Ubuntu environment.

Verifying a File Type with Its Extension
Determine file types by inspecting file extensions to support validation and processing logic.

Creating a Ping Scanner
Build a script that sends network ping requests and evaluates connectivity responses.

Data Visualization
Generate visual representations of data to support analysis and interpretation.

Pattern Matching
Identify and match patterns within text data using Python-based pattern matching techniques.

Extracting and Cleaning Data Using Python
Extract raw data and apply cleaning techniques to prepare it for analysis or processing.

Analysis with K-Means
Apply K-means clustering to group data based on similarity and analyze resulting clusters.

Inheritance
Implement inheritance to create class hierarchies that promote code reuse and structured object-oriented design.

Software Testing Fundamentals

13 Labs

Designed to build core software testing skills through guided practice, these labs progress from foundational programming and test planning to unit/integration testing, TDD, exploratory testing, defect management, and automation strategy—making them ideal for QA, development, and software delivery pathways.

Fundamentals of Software Programming
Identify and differentiate core programming concepts, including data types, compiled languages, and interpreted languages.

Unit and Integration Testing
Create and run unit tests, integrate program components, and perform integration testing to verify that code functions correctly as a whole.

Creating Use Case Diagrams
Create UML use case diagrams to model |system behavior and user interactions for a sample application.

Implementing Test-Driven Development
Apply test-driven development practices by writing tests first and developing code to meet defined test requirements.

Exploratory Testing
Conduct exploratory testing to identify defects by evaluating application behavior without predefined test cases.

Log Bugs
Submit and document software defects clearly and accurately within a bug-tracking system.

Define Test Automation Strategies
Define test automation strategies, analyze code coverage, and trace application execution using IntelliTrace data.

Implement Test Automation
Implement automated tests, including user interface testing, and execute automated test runs against applications.

Testing Methodologies
Apply common software testing methodologies to guide test planning, execution, and evaluation.

Manage Software Testing Projects
Manage software testing projects using Kanban workflows and review test plan reports to track progress and outcomes.

Manage Test Scripts
Organize, configure, and schedule test scripts to support repeatable and automated testing processes.

Detecting Software Defects
Identify and document software defects through systematic testing activities.

Manage Bugs
Review, triage, update, and manage bug status throughout the defect lifecycle using structured workflows.

Front End Web Development

10 Labs

Designed to build foundational front-end development skills through guided practice, these labs progress from HTML5 and CSS3 fundamentals to building and debugging websites with JavaScript—making them ideal for introductory web development and digital product pathways.

Website Development Basics
Understand the core components of a website and how HTML, CSS, and JavaScript work together to deliver web content.

HTML5 Basics I
Write HTML5 syntax, create the basic structure of a web page, and apply semantic elements to organize content.

HTML5 Basics II
Build on HTML5 fundamentals by structuring content using additional HTML elements and attributes.

HTML5 Basics III
Apply advanced HTML5 elements and techniques to create more complete and structured web pages.

CSS3 Basics I
Apply CSS3 rules to control layout, colors, fonts, and basic styling of web pages.

CSS3 Basics II
Use more advanced CSS3 techniques to refine layout, styling, and visual presentation.

Building a Website
Combine HTML5 and CSS3 to create a complete, multi-page website.

Introduction to JavaScript
Understand core JavaScript concepts and syntax used to add logic and interactivity to web pages.

JavaScript and HTML
Integrate JavaScript with HTML to manipulate page content and respond to user interactions.

Website Debugging
Identify and resolve common HTML, CSS, and JavaScript issues that prevent websites from functioning correctly.

IT Foundations

Digital Literacy

18 Labs

Designed to build essential digital workplace skills through guided practice, these labs progress from basic hardware, operating systems, and networking concepts to safe web use and core Microsoft Office productivity tools—making them ideal for entry-level IT readiness and workforce skills pathways.

Computer Hardware and Troubleshooting
Identify and resolve common hardware, printing, and device driver issues, and configure disk maintenance tools to support system performance.

Computer Software
Download, install, and use productivity and runtime software, including opening and editing documents and installing required system components.

Operating System Types and Features – Part 1
Compare operating system interfaces and select appropriate workstation operating systems based on user and organizational needs.

Operating System Types and Features – Part 2
Modify operating system interface settings and manage system options using configuration tabs and search tools.

Introduction to Networking – Part 1
Explain network types and benefits, describe the OSI model, and compare OSI and TCP/IP architectures.

Introduction to Networking – Part 2
Enable and verify network services by configuring web servers and confirming service availability across systems.

Online Communication
Use electronic communication tools effectively to support professional online interactions.

Web Browsing
Manage browser settings by importing bookmarks, viewing and clearing cache data, and enabling or disabling client-side scripting.

Internet Security
Configure browser and web server security settings, secure websites, and manage authentication to support safe internet usage.

Microsoft Word Fundamentals – Part 1
Search within documents, navigate to specific content, and display or hide formatting symbols.

Microsoft Word Fundamentals – Part 2
Apply and clear formatting, adjust spacing and indentation, and use built-in styles to format documents consistently.

Microsoft Word Fundamentals – Part 3
Create and modify tables, convert text to tables, and convert tables back to text within documents.

Microsoft Excel Fundamentals – Part 1
Create and navigate workbooks, adjust rows and columns, and print worksheets or entire workbooks.

Digital Literacy

Microsoft Excel Fundamentals – Part 2
Filter and manipulate data using find and replace, AutoFilter, complex criteria, and Paste Special options.

Microsoft PowerPoint Fundamentals – Part 1
Create, save, and organize presentations, including building blank and template-based slide decks.

Microsoft PowerPoint Fundamentals – Part 2
Apply themes, animations, transitions, and proofing tools to enhance presentation delivery.

Microsoft Outlook Fundamentals – Part 1
Navigate the Outlook interface, explore menus and panes, and search for specific messages.

Microsoft Outlook Fundamentals – Part 2
Create, manage, and share appointments and meetings, including recurring calendar events.

CompTIA Tech+ (FC0-U71)

17 Labs

Designed to build entry-level IT and tech support skills through guided practice, these labs progress from hardware and OS fundamentals to networking, virtualization, cloud concepts, basic programming and databases, and core security practices—making them ideal for early IT career, help desk, and foundational certification pathways.

Managing Units of Measure—Disks, Network Throughput, and Processor
Compare and apply common units of measure used for storage, network throughput, and processor performance to interpret system and network specifications.

Installation of Peripheral Devices
Install and configure common peripheral devices based on given scenarios, including input, output, and storage peripherals.

Introduction to Virtualization and Cloud Technologies
Compare virtualization and cloud technologies, including their characteristics, use cases, and operational differences.

Basic Networking Concepts
Identify foundational networking concepts, including network components, connection types, and basic communication principles.

Filesystem Management and Operating System Utilities
Identify core operating system components and use built-in utilities to manage filesystems and system resources.

Compare Different Operating Systems and Functionalities
Explain the purpose of operating systems and compare features and functionality across different OS platforms.

CompTIA Tech+ (FC0-U71)

Management of Business and Productivity Software
Install and use productivity and business software, configure an email client, and create a basic database using office productivity tools.

Web Browser Configuration and Settings – Part 1
Modify system and browser security settings, including user account control policies and client-side scripting options.

Web Browser Configuration and Settings – Part 2
Manage browser extensions and certificates across web browsers to support secure and functional web access.

Common Uses of Artificial Intelligence
Identify common applications of artificial intelligence and understand how AI is used across software and business environments.

Software Programming Fundamentals
Differentiate between compiled and interpreted programming languages and explain foundational software development concepts.

Python Programming Fundamentals
Use primitive data types, lists, and functions in Python to support basic program development.

Introduction to Database Concepts
Create database tables, define relationships, and use data definition and manipulation statements to manage structured data.

Securing and Administering Databases
Create database users and roles, assign permissions, and perform backup and restore operations using SQL tools.

Securing Workstations
Apply device security methods and best practices to protect workstations from common threats.

Implementing Password Policies
Explain and apply password best practices to support secure authentication and access control.

Introduction to Encryption
Identify common encryption use cases and explain how encryption protects data during storage and transmission.

CompTIA A+ (220-1201)

26 Simulations

Designed to build hands-on hardware and network troubleshooting skills through guided simulations, these labs progress through common device replacements, connectivity setup, tool usage, and real-world troubleshooting tasks—making them ideal for A+ Core 1 prep and job-ready technical support pathways.

Troubleshooting Network Connectivity
Diagnose and resolve common network connectivity issues using Windows and Linux graphical and command-line tools.

Replacing a Laptop SSD
Replace a laptop solid-state drive by preparing the workspace, removing and installing components correctly, reconnecting hardware, and verifying system functionality.

Replacing a Laptop Battery
Safely remove and replace a laptop battery using proper component handling and ESD procedures, and verify system operation after replacement.

Replacing a Laptop Keyboard
Identify keyboard components, perform a laptop keyboard replacement, and confirm proper installation and functionality.

Setting Up a Bluetooth Device
Configure and verify Bluetooth device connectivity, including resolving common pairing and configuration issues.

Installing a Network TAP
Install a network TAP by identifying appropriate slots, securing hardware connections, and confirming successful system recognition.

Connecting to Network-Based Devices
Connect systems to network-based devices, verify connectivity, and document configuration settings.

Configuring a Wi-Fi Network Connection
Configure wireless network connections, apply appropriate settings, verify connectivity, and resolve common connection issues.

Using Crimpers and Cable Testers
Use crimpers and cable testers to create, test, and diagnose network cables and interpret test results.

Using Punch Down Tools
Terminate network cables using punch down tools and verify correct connections based on test outcomes.

Using Toner Probes
Trace and identify network cables using toner probes and interpret diagnostic results to locate faults.

CMOS Battery Replacement
Replace a CMOS battery by identifying components, following ESD precautions, and verifying system settings post-replacement.

Verifying UEFI Settings
Inspect and verify UEFI settings, confirm system compatibility, and identify configuration issues.

Cooling a Desktop System
Install and configure cooling components, apply thermal paste correctly, manage airflow, and monitor system temperatures.

Changing Inkjet Cartridges
Replace inkjet cartridges, perform alignment and calibration, and verify print quality.

Installing a Desktop RAM Module
Install desktop memory modules, ensure proper seating and configuration, and verify system recognition.

CompTIA A+ (220-1201)

Configuring RAID
Configure RAID settings, verify connectivity, and troubleshoot common RAID configuration issues.

Installing a Desktop Expansion Card
Install expansion cards by aligning components correctly, securing hardware, and verifying system functionality.

Setting Up Two-Factor Authentication (2FA)
Configure two-factor authentication settings, validate security requirements, and troubleshoot configuration issues.

Synchronizing Microsoft 365
Configure Microsoft 365 synchronization settings, manage OneDrive preferences, and resolve synchronization issues.

Testing with a Loopback Plug
Use a loopback plug to test network and hardware ports, analyze results, and determine corrective actions.

Choosing Power Supply Units
Evaluate system power requirements, compare PSU specifications, and select appropriate power supplies based on system needs.

Configuring a Wi-Fi Network Router
Configure wireless routers, apply security settings, verify connectivity, and troubleshoot configuration problems.

Configuring Computer Accessories – Webcam
Install and configure webcam accessories, verify connectivity, and resolve common setup issues.

Inspecting Desktop Motherboards
Inspect desktop motherboards to identify components, assess condition, verify specifications, and recommend upgrades.

Replacing a Laptop RAM Module
Replace laptop memory modules by safely removing and installing components and verifying system performance.

CompTIA A+ (220-1202)

30 Labs

Designed to build OS, security, and troubleshooting skills through guided practice, these labs progress from operating system installation and configuration to security controls, malware defense, mobile device support, operational procedures, and scripting concepts—making them ideal for A+ Core 2 prep and help desk technician pathways.

Operating System Types, Filesystems, and Lifecycle Compatibility
Compare operating system types, filesystems, and lifecycle considerations, including licensing models across platforms.

Operating System Installations and Upgrades
Perform clean installations, upgrades, and troubleshooting for modern operating systems including Windows 11 and Ubuntu Linux.

CompTIA A+ (220-1202)

Windows Edition Features and Comparison
Identify and compare Windows editions and select appropriate versions based on deployment requirements.

Windows Graphical and Command-Line Management Tools
Manage Windows systems using both graphical and command-line tools to perform administrative tasks and system configuration.

Windows Settings and Personalization
Configure Windows settings and personalization options to optimize usability and system performance.

Windows Security Controls
Configure Windows security features such as User Account Control and built-in protection tools to harden systems against threats.

Windows Networking Configuration
Configure IPv4 addressing, including static IP addresses, and verify network connectivity.

macOS and Linux Desktop Features and Utilities
Identify macOS and Linux desktop features and utilities, and perform operating system installations and upgrades.

Application and Cloud Service Deployment
Deploy applications and cloud services, including implementing automated deployment strategies.

Windows Local Security Controls
Apply local Windows security controls to protect systems and user accounts.

Windows Local Security Configuration
Configure local security settings to enforce system protection and access controls.

Wireless Security Protocols and Authentication
Configure wireless security protocols and authentication methods, and recognize indicators of wireless security breaches.

Malware Defense
Configure and update anti-malware tools, identify malware behavior, and respond to system infections.

Social Engineering Attacks
Identify social engineering techniques and understand how attackers exploit human behavior to compromise systems.

SOHO Malware Removal
Remove malware from small office and home office environments using proper remediation and system cleaning procedures.

System Hardening
Apply system hardening techniques to reduce attack surfaces and strengthen system security.

Mobile Device Security Configuration
Configure mobile device security settings and application permissions to protect user data and devices.

Data Destruction and Disposal Methods
Apply secure data destruction and disposal methods to protect sensitive information at end of life.

SOHO Networking
Configure SOHO networking components, including network segmentation and DMZ settings.

Browser Security Hardening
Harden browser security settings, including secure DNS configuration, to reduce exposure to web-based threats.

Windows OS Troubleshooting
Diagnose and resolve Windows operating system issues, including application crashes and compatibility problems.

Mobile OS and Application Troubleshooting
Troubleshoot mobile operating system and application issues, including safe mode and recovery procedures.

CompTIA A+ (220-1202)

Mobile Security Issue Troubleshooting
Identify and remediate mobile security incidents while preserving user data when possible.

Personal Computer Security Troubleshooting
Diagnose and resolve personal computer security issues, including corrupted or altered system files.

Documentation and Asset Management Best Practices
Create and maintain technical documentation and asset management standards to support consistent IT operations.

Change Management Process Implementation
Implement change management processes, including supporting Change Advisory Board (CAB) activities.

Backup and Recovery Strategies
Implement backup and recovery solutions to protect data and maintain business continuity.

Safety Procedures and Environmental Controls
Apply safety procedures and manage environmental controls such as temperature, humidity, and air quality in IT spaces.

Policy, Licensing, and Privacy Compliance
Apply organizational policies, licensing requirements, and privacy practices, including acceptable use policies.

Scripting and AI
Apply scripting, automation, and AI-enabled tools to improve efficiency and problem-solving in IT environments.

PC Maintenance and Repair

15 Labs

Designed to build practical PC support skills through guided practice, these labs progress from hardware, operating systems, and networking basics to troubleshooting, recovery, remote access, enterprise tools, and security—making them ideal for entry-level desktop support and repair-focused pathways.

Examining PC Hardware
Identify and examine core PC hardware components and understand their roles within a desktop or laptop system.

PC Operating Systems
Configure and manage Windows operating system settings based on common support and usage scenarios.

Networking Essentials
Identify foundational networking concepts and apply basic security and operating system networking configurations.

Printers
Install, configure, and troubleshoot printers and printing components in common workplace environments.

Security Practices
Manage and configure basic Windows security settings to protect systems from common threats.

Troubleshooting
Diagnose and resolve common hardware and network issues using a structured troubleshooting approach.

PC Maintenance and Repair

Disk Maintenance and Data Recovery
Perform disk maintenance tasks and implement workstation backup and recovery methods.

Command Prompt Tools
Use Windows command-line tools to perform system management and troubleshooting tasks.

Remote Access
Configure and use remote access tools to support systems and users from remote locations.

Control Panel
Navigate and use the Windows Control Panel to manage system settings and configurations.

Desktop Customization
Customize desktop settings to improve usability and align system configurations with user needs.

Using Active Directory in the Enterprise
Use Active Directory to manage users, resources, and permissions in an enterprise environment.

Data Backups in Windows, BSD, and Linux
Implement data backup strategies across Windows, BSD, and Linux systems to support system resilience.

Ubuntu Desktop Linux Installation
Install Ubuntu Linux using custom disk layouts, configure boot settings, and apply system updates.

Domain Security
Apply domain-level security controls and practices to protect systems and organizational resources.

Networking

Introduction to Networking Fundamentals

13 Labs

Designed to build foundational networking skills through guided practice, these labs progress from core network concepts and IP addressing to routing, DHCP, name resolution, VPN configuration, and TCP/IP troubleshooting tools—making them ideal for introductory networking and IT infrastructure pathways.

Understanding the Concepts of Internet, Intranet, and Extranet
Differentiate between internet, intranet, and extranet environments and explain how each is used within organizations.

Understanding Local Area Networks (LANs)
Explain how local area networks operate and configure IP addressing within a LAN environment.

Configuring Routing
Configure routing to control how data packets travel between interconnected networks.

Configuring a NAT Firewall
Configure Network Address Translation (NAT) firewalls and port forwarding to manage traffic flow and improve network security.

Understanding IPv4
Explain IPv4 addressing concepts and configure IPv4 network settings.

Understanding IPv6
Explain IPv6 addressing concepts and configure IPv6 network settings.

Understanding Name Resolution
Configure and test name resolution using hostnames, DNS servers, HOSTS files, and WINS services.

Managing DHCP Servers
Configure DHCP servers and clients, manage IP address leases, and support dynamic address assignment across networks.

Working with TCP/IP Command-Line Tools
Use TCP/IP command-line tools to test connectivity, troubleshoot network issues, and inspect network configurations.

Understanding Client-Server and Peer-to-Peer Networks
Differentiate between client-server and peer-to-peer network models, including domains, workgroups, and home groups.

Understanding Network Communications and Protocols
Explain core network communication concepts and protocols that enable data transmission across networks.

Install and Configure VPN Server
Install and configure a VPN server and adjust server properties to enable secure remote access.

Understanding IPSec
Configure IPSec connection security rules and prepare systems to monitor and secure network communications.

CompTIA Network+ (N10-009)

17 Labs

Designed to build Network+ aligned networking skills through guided practice, these labs progress from the OSI model and network architecture to addressing, routing and switching, monitoring, security concepts, and troubleshooting—making them ideal for Network+ preparation and core networking pathways.

Introduction to the OSI Model
Explain the seven layers of the OSI model, with emphasis on Layer 2 (Data Link) and Layer 3 (Network), including their roles in data transfer, addressing, and routing.

Networking Appliances and Functionality
Explain the purpose and functionality of common networking appliances, including VPN technologies used to securely connect remote users to private networks.

Cloud Networking Concepts
Explain cloud networking fundamentals, including virtualized network resources, scalability, and cost considerations compared to on-premises networking.

Networking Ports and Protocols
Identify common network ports and protocols and explain how protocols define communication rules between networked devices.

Networking Topologies and Architecture
Compare logical network topologies and architectures, including star, bus, ring, and mesh, and explain how devices communicate within each model.

IPv4 Network Addressing
Explain IPv4 addressing concepts, including address classes and subnetting fundamentals used in network configuration.

Software-Defined Networking Concepts
Explain software-defined networking (SDN), including the separation of control and data planes and the role of centralized controllers.

Routing Concepts
Configure and explain routing concepts, including static routing, NAT with port forwarding, and the use of subinterfaces.

Switching Concepts
Explain switching operations within a LAN, including frame forwarding and the role of MTU settings in efficient data transmission.

Network Monitoring Concepts
Explain network monitoring techniques, including packet capture, network discovery, and topology mapping to support performance and security.

Disaster Recovery Concepts
Explain disaster recovery and high availability concepts, including redundancy, failover, and strategies for business continuity.

Implementing IPv4 Network Services
Implement essential IPv4 network services and explain their role in supporting enterprise network operations.

Network Access and Management
Configure and differentiate secure and insecure network access methods, including SSH and other management connections.

Network Security Concepts
Explain core network security concepts, including full-disk and file-level encryption used to protect data in transit and at rest.

General Network Attacks
Identify common network attacks, including eavesdropping, session hijacking, phishing, and unauthorized access techniques.

CompTIA Network+ (N10-009)

Network Hardening Techniques
Apply network hardening techniques, including disabling unused ports, configuring access control lists (ACLs), and reducing attack surfaces.

Network Troubleshooting Tools and Techniques
Use network troubleshooting tools such as ping, tracert, and traceroute to diagnose connectivity and routing issues.

Cisco CCNA (200-301)

22 Labs

Designed to build CCNA-aligned networking skills through guided configuration practice, these labs progress from network fundamentals and IP addressing to VLANs, routing (including OSPF), NAT, DHCP, management services, security, QoS, and wireless—making them ideal for associate-level networking pathways.

Networking Concepts – Part One
Perform initial router configuration tasks and enable secure remote access using SSH.

Networking Concepts – Part Two
Identify and compare network cabling types, including UTP, STP, single-mode and multimode fiber, Ethernet media types, and Power over Ethernet (PoE).

IP Addressing and Virtualization Concepts
Calculate subnets, prepare IP addressing schemes, and verify network implementations.

Switching Fundamentals – Part One
Explain MAC address learning, adjust aging timers, and manage frame switching and flooding behavior.

Switching Fundamentals – Part Two
Configure trunk links, implement VTP, secure the native VLAN, and complete trunk configurations.

Configuring VLANs – Part One
Create and manage VLANs, secure the default VLAN, configure voice VLANs, and explain VTP behavior.

Configuring VLANs – Part Two
Identify and modify the spanning tree root bridge and adjust interface costs to influence path selection.

Static and Dynamic Routing Principles
View routing tables, implement and remove static routes, and configure loopback interfaces.

Configure OSPFv2
Configure OSPFv2 settings, manage router IDs, establish adjacencies, and configure passive interfaces.

FHRP Configuration and Verification
Configure and verify first-hop redundancy protocols, including HSRP and VRRP with object tracking.

Static NAT Configuration
Configure static NAT, dynamic NAT, and port address translation, and troubleshoot NAT behavior.

NTP Configuration
Configure routers as NTP servers and synchronize network devices using NTP services.

Cisco CCNA (200-301)

DHCP Concepts, Configuration, and Verification
Configure DHCP scopes, DNS settings, relay agents, and troubleshoot DHCP address assignment issues.

Network Traffic Management Using SNMP
Configure SNMP on network devices and verify network monitoring data using management software.

Configuring Syslog for Switching and Routing
Configure syslog servers, enable logging on routers, and set logging severity levels.

Remote Management Techniques
Configure console, AUX, HTTPS access, and apply management plane protection controls.

Using File Transfer Protocols on Routers
Back up and restore router configuration files using file transfer protocols.

Network Management Tools
Use network management tools, including Ansible, and interpret JSON-encoded network data.

Applying Security Protocols
Configure standard, extended, and named access control lists and enable secure remote access.

QoS for Routing Configuration Using PHB
Configure Quality of Service (QoS) classification, marking, queuing, and congestion management.

Security Mitigation Techniques
Identify threats, vulnerabilities, and exploits, and apply physical and logical security controls.

Wireless Architecture and Application
Compare wired and wireless networks, explain wireless communication principles, and configure wireless channels, including overlapping and non-overlapping designs.

Networking Fundamentals

16 Labs

Designed to build practical networking and network security skills through guided practice, these labs progress from core protocols and models to NAT, firewalls, policy implementation, remote access, troubleshooting, and resiliency concepts—making them ideal for infrastructure and security-aware networking pathways.

Configuring Port Redirection
Configure port redirection to control how incoming network traffic is forwarded to internal systems.

Implementing NAT and Allowing Remote Access
Configure Network Address Translation (NAT) and enable secure remote access to internal network resources.

IPv4 vs. IPv6 – Calculating, Configuring, and Testing
Compare IPv4 and IPv6 addressing, calculate address ranges, configure network settings, and test connectivity.

Network Management
Monitor and manage network operations, apply basic network security controls, and support troubleshooting activities.

Networking Fundamentals

Business Continuity – Disaster Recovery
Apply disaster recovery and business continuity concepts to protect network operations and reduce downtime.

Breaking WEP and WPA and Decrypting Traffic
Analyze wireless security weaknesses by examining WEP and WPA encryption and evaluating traffic decryption methods.

Closing Ports and Unnecessary Services
Reduce network attack surfaces by closing unused ports and disabling unnecessary services.

Implementing Security Policies on Windows and Linux
Apply security policies on Windows and Linux systems to support governance, risk management, and compliance.

Network Security – Firewalls
Configure firewall rules to filter network traffic and protect network infrastructure.

Network Troubleshooting
Diagnose and resolve network issues using structured troubleshooting techniques.

TCP/IP Utilities
Use TCP/IP utilities to test connectivity, analyze network behavior, and troubleshoot communication issues.

The OSI Model
Explain the OSI model and how its layers support network communication.

TCP/IP Protocols – The Core Protocols
Explain core TCP/IP protocols and their roles in network communication and operations.

TCP/IP Protocols – Other Key Protocols
Identify additional TCP/IP protocols and explain how they support network services.

Types of Networks
Compare different types of networks and explain their use cases and characteristics.

Introduction to Wireshark

8 Labs

Designed to build packet analysis skills through guided practice, these labs progress from Wireshark installation and configuration to capturing, filtering, and analyzing traffic and protocols—making them ideal for networking, troubleshooting, and security fundamentals pathways.

Understand Common Ports and Protocols
Identify common network ports and protocols, including HTTP (80), HTTPS (443), NetBIOS (139), and the differences between TCP and UDP.

Installing Wireshark
Download, install, and verify a functional Wireshark installation.

Wireshark Functionality
Navigate the Wireshark interface, understand packet processing, and use export features to manage captured data.

Customizing Wireshark
Customize Wireshark by creating profiles, marking packets, adjusting time displays, and modifying interface settings.

Introduction to Wireshark

Working with Captured Traffic
Capture network traffic and apply capture filters, display filters, and color rules to isolate relevant data.

Analyzing Captured Traffic
Analyze captured traffic using statistics, packet navigation, GeoIP mapping, and create firewall ACL rules based on findings.

Analyzing Protocols
Analyze protocol behavior by examining TCP/IP, HTTP, DNS, ARP, and IPv4 traffic within Wireshark.

Packet Sniffing with Wireshark
Identify security risks by examining packet captures for password brute-force attempts and insecure protocols such as Telnet.

Interconnecting Cisco Networking Devices (ICND1 v3.0)

19 Labs

Designed to build Cisco device configuration and troubleshooting skills through guided practice, these labs progress from initial device setup and addressing to VLANs, inter-VLAN routing, routing protocols, ACLs, NAT, device management, and maintenance tools—making them ideal for foundational Cisco networking pathways.

Performing Initial Device Configuration
Review physical and configuration characteristics of routers and switches and configure secure remote access.

Cloud Troubleshooting Methodologies
Apply structured troubleshooting models to diagnose and resolve cloud-related issues.

Configure, Verify, and Troubleshoot Port Security
Configure static and dynamic port security, manage err-disabled recovery, and troubleshoot port security violations.

Configure and Verify Switching Concepts
Configure and verify core switching concepts used in enterprise network environments.

Interface Configuration and Cabling
Configure network interfaces and apply correct cabling standards for reliable connectivity.

Configuring and Verifying VLANs
Create, configure, and verify VLANs to segment networks and control broadcast traffic.

Compare Static and Dynamic Routing
Compare static and dynamic routing methods and evaluate their use cases in network environments.

Configure and Verify RIPv2 for IPv4
Configure RIPv2 routing and verify IPv4 route propagation.

Configure and Verify DHCP and DNS
Configure DHCP and DNS services to support dynamic IP addressing and name resolution.

Configuring and Verifying NTP Operation
Configure NTP servers and clients and verify accurate time synchronization across network devices.

Interconnecting Cisco Networking Devices (ICND1 v3.0)

Configure and Verify Standard Access Lists
Configure and verify standard, extended, and named access control lists to restrict network traffic and remote access.

Configure and Verify IPv4 and IPv6 Access Lists for Traffic
Apply IPv4 and IPv6 access control lists to filter and manage network traffic.

Configure and Verify Device Management
Configure device management features, monitor devices, back up and restore configurations, and use discovery protocols.

Device Maintenance Procedures
Perform routine device maintenance procedures to support system stability and uptime.

Cisco IOS Troubleshooting Tools
Use Cisco IOS troubleshooting tools to diagnose and resolve network device issues.

Cybersecurity

Security Fundamentals

18 Labs

Designed to build foundational security knowledge through guided practice, these labs progress from authentication, permissions, and password policies to encryption, isolation, auditing, secure protocols, malware concepts, and common attack awareness—making them ideal for introductory cybersecurity pathways.

Understand Internet Security
Configure browser security settings, secure web services, and manage authentication for web applications.

Understand User Authentication
Configure user authentication methods, including VPN authentication, Network Policy Server settings, and multi-factor authentication.

Understand Permissions
Configure and modify file and folder permissions within Windows Server environments.

Understand Password Policies
Configure password policies to enforce strong authentication and account security requirements.

Understand Encryption
Apply encryption concepts and configure file-level encryption to protect data at rest.

Understand Network Isolation
Configure network isolation techniques, including IPsec, routing controls, server and domain isolation, and honeypot deployment.

Understand Audit Policies
Configure audit policies to monitor system activity and support security investigations.

Understand Network Access Protection
Configure Network Access Protection (NAP) servers and clients to enforce compliance-based network access.

Understand Protocol Security
Secure network communications by configuring tunneling and protocol-level security controls.

Implementing Client Protection
Configure client security controls, including User Account Control, offline file encryption, and application restriction policies.

Understand E-Mail Protection
Configure email security controls, including antivirus protection for mail systems.

Understand Server Protection
Configure server protection mechanisms, including update services, to maintain secure and reliable systems.

Manage IPv6 Connectivity
Test IPv6 connectivity and configure DHCPv6 services to support modern network environments.

Understand Secure Sockets Layer and Transport Layer Security
Explain and apply SSL/TLS concepts to secure data transmission.

Cisco CCNA (200-301)

Understand Malware
Identify malware behavior, test network services, and deploy malware protection mechanisms.

Understand Cryptography Tools
Identify and use cryptography tools to support secure communications and data protection.

Understand How Password Cracking Tools Work
Explain how password cracking tools operate and assess their impact on authentication security.

Understand Common Network Attacks
Identify common network attacks, including reconnaissance, packet sniffing, man-in-the-middle attacks, denial-of-service, and phishing techniques.

CompTIA Security+ (SY0-701)

18 Labs

Designed to build Security+ (SY0-701) aligned skills through guided practice, these labs progress from security concepts and cryptography to threat analysis, architecture and resilience, vulnerability management, monitoring, identity and access management, and automation/orchestration—making them ideal for Security+ preparation pathways.

Security Concept Fundamentals
Explain core security principles, including confidentiality, integrity, and availability (CIA), and how authentication and authorization support these concepts.

Cryptographic Solutions
Apply cryptographic concepts to protect data confidentiality, integrity, authenticity, and availability in secure communications and transactions.

Threat Vectors and Attack Surfaces
Identify common threat vectors and attack surfaces, including open ports, default credentials, and vulnerable applications, and apply mitigation strategies.

Identifying Security Vulnerabilities
Identify configuration and system vulnerabilities and understand how vulnerability assessments reduce organizational risk.

Analyze Malicious Activity
Recognize indicators of malicious activity, including brute-force attacks, command injection, and SYN flood attacks.

Security Architecture Models
Explain security architecture models, including virtualization and containerization, and deploy virtual machines and containers securely.

Securing Enterprise Infrastructures
Secure enterprise infrastructure by configuring encryption and remote access solutions, including VPN servers and clients using L2TP/IPsec.

CompTIA Security+ (SY0-701)

Data Protection Strategies
Apply data protection strategies such as encryption and hashing to protect data confidentiality, integrity, and availability and support compliance.

Resilience in Security Architecture
Implement resilient security architecture concepts that support incident response, system recovery, and continuity of operations.

Securing Computing Resources
Secure computing resources by establishing security baselines, managing vulnerabilities, and isolating untrusted workloads.

Asset Management Techniques
Apply asset management practices to track IT resources, support security controls, and ensure secure data destruction during deprovisioning.

Vulnerability Management
Detect and monitor vulnerabilities in devices and web applications to prioritize remediation efforts.

Monitoring Computing Resources
Monitor system resource utilization to identify performance and security issues.

Enhancing Enterprise Security
Apply server hardening techniques for Linux and Windows systems to reduce attack surfaces.

Implement Identity and Access Management
Provision and manage user accounts on Windows and Linux systems to enforce access control policies.

Implementation of Automation and Orchestration for Security Operations
Implement automation scripts to support security operations and improve response efficiency.

Investigative Data Sources
Analyze log files and investigative data sources to support security monitoring and incident investigations.

Mitigation Techniques
Apply mitigation techniques by hardening network devices, configuring access controls, enabling encryption, and implementing logging.

CompTIA PenTest+ (PT0-003)

11 Labs

Designed to build PenTest+ (PT0-003) aligned penetration testing skills through guided practice, these labs progress from reconnaissance and enumeration to vulnerability scanning, attack execution across domains, social engineering, scripting automation, and engagement management—making them ideal for penetration testing preparation pathways.

Penetration Testing Information Gathering Techniques
Perform passive and active reconnaissance to collect information about target systems, networks, and environments.

Enumeration Tools and Techniques
Enumerate network resources to identify users, services, shares, and system details that can be leveraged during an attack.

Vulnerability Scanning Techniques
Conduct vulnerability scans to identify weaknesses in systems, applications, and configurations.

Conducting Network Attacks
Exploit network services and resources, including compromising FTP servers and other exposed network components.

Conducting Authentication Attacks
Perform authentication attacks such as SMB and RDP brute-force attempts to evaluate credential security.

Conducting Host-Based Attacks
Exploit vulnerabilities on host systems to gain access and escalate privileges.

Conducting Web Application Attacks
Execute common web application attacks, including brute-force authentication attacks and SQL injection.

Performing a Social Engineering Attack
Conduct social engineering attacks to exploit human behavior and assess organizational security awareness.

Automating Attacks Using Scripts
Use scripts to automate attack techniques and streamline penetration testing activities.

Compromising a System and Maintaining Persistence
Compromise target systems and implement persistence mechanisms to maintain long-term access.

Penetration Testing Management Engagement
Apply penetration testing engagement processes, including scoping, authorization, execution, and reporting

CompTIA CySA+ (CS0-003)

12 Labs

Designed to build CySA+ (CS0-003) aligned analyst skills through guided practice, these labs progress from threat intelligence and detection to vulnerability analysis, prioritization, incident response workflows, reporting, and attack surface management—making them ideal for security analytics and SOC pathways.

System & Network Security Implementation
Implement security controls by collecting logs with SIEM tools, encrypting sensitive data, and enabling multi-factor authentication.

Threat Intelligence & Threat Gathering Concepts
Collect, analyze, and share threat intelligence using multiple sources to support threat hunting and security operations.

Techniques to Determine Malicious Activity
Monitor system and authentication events using Windows and Linux logs and automation scripts to identify suspicious activity.

Vulnerability Scanning Tools & Techniques
Detect network assets and identify vulnerabilities using scanning tools and assessment techniques.

Identifying & Analyzing Malicious Activity
Analyze system resource utilization and detect unauthorized privilege escalation.

Tools for Identifying Malicious Activity
Monitor network activity, analyze malicious files in a sandbox environment, and validate domains and IP addresses.

Attack Methodology Frameworks
Apply attack methodology frameworks, including OWASP, to understand adversary techniques and improve defensive strategies.

Vulnerability Data Analysis and Prioritization
Analyze vulnerability data using CVSS scoring and identify web application vulnerabilities to prioritize remediation.

Incident Response Management Techniques
Apply incident response processes to manage, contain, and recover from security incidents.

Incident Response Communication & Reporting
Coordinate incident response, communications and review required reports and breach impact assessments.

Vulnerability Reporting Concepts
Collect security data and create structured vulnerability reports using SIEM tools.

Vulnerability Patching & Attack Surface Management
Apply patch management techniques for Windows and Linux systems to reduce attack surfaces.

Certified Ethical Hacker (CEH v13)

16 Labs

Designed to build CEH v13 aligned ethical hacking skills through guided practice, these labs progress across the CEH domains while incorporating AI-assisted techniques for reconnaissance, vulnerability analysis, exploitation concepts, web attacks, cloud concepts, and cryptography—making them ideal for CEH-aligned pathways.

Introduction to AI in Ethical Hacking
Explain how artificial intelligence is applied to ethical hacking workflows and supports reconnaissance, analysis, and attack simulation.

Footprinting and Reconnaissance Techniques with AI
Use AI-assisted techniques to collect publicly available information about target organizations and systems.

Network Reconnaissance Techniques with AI
Apply AI-driven methods to identify network hosts, services, and exposed infrastructure.

Enumeration Reconnaissance Techniques with AI
Enumerate users, services, shares, and system details using AI-supported reconnaissance techniques.

Vulnerability Analysis Tools & Techniques with AI
Identify and analyze system and application vulnerabilities using AI-enhanced scanning and assessment techniques.

System Hacking Methodologies with AI
Apply AI-assisted system hacking techniques to gain access, escalate privileges, and maintain control of compromised systems.

Malware Threat Concepts with AI
Analyze malware behaviors and threat patterns using AI-supported detection and analysis techniques.

Network Sniffing Techniques with AI
Capture and analyze network traffic using AI-assisted sniffing techniques to identify sensitive data and insecure communications.

Social Engineering Techniques and Exploits with AI
Conduct AI-enhanced social engineering attacks to assess human vulnerabilities and organizational security awareness.

Denial-of-Service Attacks with AI
Analyze and execute AI-supported denial-of-service attack techniques to evaluate system resilience.

Session Hijacking Concepts with AI
Identify and exploit session management weaknesses using AI-assisted hijacking techniques.

Compromising Web Servers with AI
Exploit web server misconfigurations and vulnerabilities using AI-driven attack techniques.

Web Application Hacking with AI
Identify and exploit common web application vulnerabilities, including broken authentication and command injection, using AI-assisted analysis.

SQL Injection Methodologies with AI
Perform SQL injection attacks using AI-supported techniques to extract and manipulate database data.

Introduction to Cloud Computing with AI
Explain cloud computing concepts and identify how AI is applied to cloud-based attack and defense scenarios.

Cryptography Techniques with AI
Apply cryptographic concepts and evaluate encryption mechanisms using AI-assisted analysis techniques.

Digital Forensics

15 Labs

Designed to build GIAC-aligned digital forensics skills through guided practice, these labs progress from file systems and artifact locations to imaging, tool usage (including Autopsy), registry and log analysis, memory analysis, and a capstone case—making them ideal for forensics certification-aligned pathways.

Introduction to File Systems
Explain file system structures and how they store, organize, and manage digital evidence.

Common Locations of Windows Artifacts
Identify key Windows artifact locations, including host and application event logs, used in forensic investigations.

Hashing Data Sets
Generate and verify cryptographic hashes to ensure the integrity of digital evidence.

Drive Letter Assignments in Linux
Identify and interpret Linux drive and mount point assignments relevant to forensic analysis.

The Imaging Process
Create forensic images of storage media while preserving data integrity and evidentiary value.

Introduction to Single-Purpose Forensic Tools
Use single-purpose forensic tools to collect and analyze specific types of digital evidence.

Introduction to Autopsy Forensic Browser
Navigate the Autopsy forensic browser to examine file systems, artifacts, and timelines.

FAT File System
Analyze FAT file system structures to recover and interpret digital evidence.

The NTFS File System
Examine NTFS file system components, including metadata and file records, for forensic analysis.

Browser Artifact Analysis
Analyze browser artifacts and Windows Registry data to reconstruct user activity.

Communication Artifacts
Identify and analyze communication artifacts related to user messaging and communications.

User Profiles and the Windows Registry
Analyze Windows user profiles and Registry data to identify system and user activity.

Log Analysis
Analyze host and application logs to identify events relevant to forensic investigations.

Memory Analysis
Analyze system memory to identify running processes, network connections, and volatile artifacts.

Forensic Case Capstone
Conduct an end-to-end forensic investigation, including evidence acquisition, analysis, and reporting.

SOC Analyst

3 Labs

Designed to build SOC-relevant analyst skills through focused guided practice, these labs cover SIEM configuration and attack analysis, threat landscape tracking, and vulnerability management workflows—making them ideal for SOC readiness and security operations pathways.

SIEM Configuration and Attack Analysis
Configure a SIEM to collect, normalize, and analyze log data and identify indicators of attack activity.

Tracking the Threat Landscape
Correlate firewall and security events within a SIEM to track emerging threats and attacker behavior.

Vulnerability Management: Scan, Prioritize, Remediate
Analyze vulnerability scan results, prioritize risks, and develop documented remediation plans from a SOC analyst perspective.

Network Security Fundamentals

15 Labs

Designed to build practical network security skills through guided configuration practice, these labs progress from host and network firewall configuration to secure services, VPN setup, IDS with Snort, RADIUS, and closing common security gaps—making them ideal for security-focused networking and junior security pathways.

Configuring a Windows-Based Firewall to Allow Incoming Traffic
Configure Windows firewall rules to securely allow inbound network traffic.

Configuring a Linux-Based Firewall to Allow Incoming and Outgoing Traffic
Configure Linux firewall rules to control inbound and outbound network traffic.

Implementing Secure DHCP and DNS
Secure DHCP and DNS services to protect network address assignment and name resolution.

Configuring a Linux-Based Firewall to Allow Outgoing Traffic
Restrict and manage outbound network traffic using Linux firewall configurations.

Configuring Access Control Lists on Linux-Based Firewalls
Implement access control lists (ACLs) on Linux firewalls to enforce authorization policies.

Configuring a Virtual Private Network with PPTP
Configure a VPN using PPTP to enable secure remote connectivity.

Network Security Fundamentals

Configuring a Virtual Private Network with OpenVPN
Deploy and configure OpenVPN to provide encrypted remote access and secure communications.

Implementing RIP, RIPv2, and Securing RIP
Configure RIP and RIPv2 routing and apply security controls to protect routing updates.

Intrusion Detection Using Snort
Deploy and configure Snort to detect and analyze network intrusion attempts.

Writing Custom Rules
Create custom security rules to detect threats and support security assessment processes.

Host-Based Firewalls
Configure host-based firewalls to protect individual systems from unauthorized network access.

Configuring RADIUS
Configure RADIUS authentication to centralize network access control.

Domain Security
Apply domain-level security controls to protect authentication, authorization, and access services.

Configuring a Site-to-Branch Virtual Private Network
Configure site-to-branch VPN connections to securely connect remote networks.

Closing Security Holes
Identify and remediate network security gaps through configuration hardening and assessment.

Introduction to Network Security Tools

12 Labs

Designed to build foundational security tooling skills through guided practice, these labs progress from network discovery and scanning to protocol analysis, vulnerability awareness, and IDS/firewall evasion concepts—making them ideal for introductory security operations and tooling pathways.

Topology Discovery – Part 2
Use Nmap and Zenmap to perform OS fingerprinting, analyze scan output logs, and visualize network topology.

Scanning Networks – Part 1
Scan networks using tools such as Nmap, Advanced IP Scanner, and MyLanViewer to identify hosts and map network structures.

Understand Network Communications and Protocols
Analyze network communications by validating common ports and protocols, including HTTP, HTTPS, NetBIOS, TCP, and UDP.

Network Security – Protocol Analyzers
Analyze network traffic and investigate ARP cache tables using protocol analysis tools.

Introduction to Network Security Tools

Threats – Network Vulnerability
Identify network vulnerabilities through footprinting, packet sniffing, ARP spoofing, denial-of-service techniques, and phishing indicators.

Network Security – Routing Protocols
Analyze routing protocol security by sniffing routing traffic, injecting poisoned routes, and configuring authentication for RIP packets.

Network Security – Spam Filter
Configure email services and clients to implement spam filtering and reduce email-based threats.

Understanding IDS, Firewall Evasion, and Honeypots
Analyze intrusion detection systems, examine firewall evasion techniques, and deploy honeypots to detect malicious activity.

Cybersecurity Fundamentals

20 Labs

Designed to build practical cybersecurity readiness through guided practice, these labs progress from securing endpoints, mobile, and cloud environments to configuring browsers and firewalls, applying encryption, backup/recovery, and addressing common social and communication threats—making them ideal for entry-level cybersecurity and IT security pathways.

Introduction to Data Security
Explain data security principles, identify types of data and data threats, and assess the impact of data breaches on organizations.

Configuring Endpoint Security
Configure endpoint security controls on Windows systems, including antivirus and antispyware tools, and identify common malware symptoms.

Common Threats to a Wireless Network
Identify wireless network threats and apply techniques to secure and harden wireless network configurations.

Configuring a Web Browser
Configure security settings in web browsers, including Firefox, Chrome, and Edge, to support safe internet usage.

Email Security Concepts
Configure email clients and apply security practices to reduce phishing, malware, and email-based threats.

Securing Mobile Platforms
Apply security controls to mobile platforms to protect devices and user data.

Securing the Cloud
Explain cloud security concepts and apply basic controls to protect cloud-based resources.

Securing Network Connections
Configure and secure network connections using Windows networking features.

Using Data Destruction and Disposal Methods
Perform data destruction techniques, including formatting and secure data wiping, to prevent data recovery.

Cybersecurity Fundamentals

Configuring File System Security
Configure file system permissions, sharing settings, and effective access controls on Windows systems.

Administering User and Group Accounts
Manage local and domain user and group accounts to enforce access control policies.

Securing Windows
Apply security hardening techniques to protect Windows operating systems.

Configuring and Running Windows Update
Configure and manage Windows Update and server update services to maintain system security.

Configuring Firewall on Windows
Configure Windows firewall rules to control inbound and outbound network traffic.

Encryption
Configure disk encryption using BitLocker to protect data at rest.

Data Backup and Disaster Recovery
Create system backups, configure restore points, and use recovery tools to support data recovery.

Implementing Basic Disaster Prevention and Recovery Methods
Apply basic disaster prevention and recovery strategies to minimize data loss and downtime.

Managing System Maintenance Tools
Use system maintenance tools, including disk cleanup, DNS cache management, and disk defragmentation.

Social Networking Security
Identify social networking security risks and apply controls to reduce exposure.

Instant Messaging Security
Apply security controls and best practices to protect instant messaging platforms from threats.

Information Security Fundamentals

15 Labs

Designed to build applied information security skills through guided practice, these labs progress from firewall and protocol configuration to wireless assessment, policy implementation, incident response/forensics foundations, exploitation concepts, and encryption—making them ideal for intermediate security fundamentals pathways.

Securing the pfSense Firewall
Configure and secure a pfSense firewall to control network traffic and enforce security rules.

Implementing NAT and Allowing R emote Access
Configure Network Address Translation (NAT) and remote access to securely connect internal networks to external resources.

Information Security Fundamentals

Implementing Common Protocols and Services
Configure and secure common network protocols and services used in enterprise environments.

Examining Wireless Networks
Analyze wireless network configurations and identify security weaknesses in wireless deployments.

Implementing Security Policies on Windows and Linux
Apply security policies on Windows and Linux systems to enforce governance, risk, and compliance controls.

Data Backups in Windows, BSD, and Linux
Implement backup strategies across Windows, BSD, and Linux systems to support cybersecurity resilience.

Incident Response Procedures, Forensics, and Analysis
Apply incident response procedures, perform basic forensic analysis, and support security investigations.

Crafting and Deploying Malware Using a Remote Access Trojan
Analyze how remote access trojans are created and deployed to understand attacker techniques and improve defenses.

Social Engineering Using SET
Conduct social engineering attacks using the Social Engineering Toolkit (SET) to assess human-based security risks.

Breaking WEP and WPA and Decrypting Traffic
Analyze weaknesses in WEP and WPA wireless encryption by capturing and decrypting network traffic.

Deep Dive in Packet Analysis Using Wireshark
Perform detailed packet analysis using Wireshark to investigate network behavior and security incidents.

Remote and Local Exploitation
Analyze remote and local exploitation techniques to identify vulnerabilities and assess system risk.

Patching, Securing Systems, and Configuring Antivirus
Apply patch management, system hardening, and antivirus configuration to reduce attack surfaces.

Using Active Directory in the Enterprise
Configure and manage Active Directory components to support authentication, authorization, and security controls.

Using Public Key Encryption to Secure Messages
Apply public key encryption techniques to secure communications and protect data in transit.

Linux Based Security+

14 Labs

Designed to build Linux-focused defensive and offensive security skills through guided practice, these labs progress from VPN and proxy configuration to permissions, log analysis, vulnerability scanning, exploitation scenarios, encryption, and steganography—making them ideal for Linux security and applied cybersecurity pathways.

Configuring a VPN Tunnel Using pfSense
Configure a secure VPN tunnel using pfSense to protect network communications and enable secure remote access.

Comparing Clear Text and Encrypted Protocols
Analyze the risks of clear-text protocols and compare them to encrypted alternatives to understand secure data transmission.

Linux Attack and Response
Analyze common attacks against Linux systems and apply response techniques to detect and mitigate threats.

Log Analysis of Linux Systems with Grep and Gawk
Analyze Linux system logs using command-line tools to identify suspicious activity and support incident investigations.

Attacking and Defending Linux Systems
Simulate attacks against Linux systems and apply defensive controls to strengthen system security.

Cracking Passwords on Linux Systems
Analyze password cracking techniques to understand authentication weaknesses and improve password security policies.

Identifying and Analyzing Host Intrusion Detection Alerts
Analyze host-based intrusion detection system alerts to identify malicious activity on Linux systems.

Exploiting Shellshock
Examine the Shellshock vulnerability to understand command injection risks and apply mitigation strategies.

Vulnerability Scanning of a Linux Target
Perform vulnerability scans against Linux systems to identify weaknesses and prioritize remediation efforts.

Encrypting Data Using TrueCrypt
Implement data encryption using disk encryption tools and analyze methods used to attack encrypted data.

Injection Attacks Using WebGoat
Analyze common injection attacks against web applications to understand exploitation techniques and defenses.

Managing Permissions, Users, and Groups in Linux
Configure Linux permissions, users, and groups to enforce access control and system security.

Creating a Proxy Server and SSL Certificate Using pfSense
Configure a proxy server and deploy SSL certificates to secure network traffic and web communications.

Steganography
Analyze steganography techniques to understand how data can be hidden within files and detect covert data channels.

PenTesting and Understanding Vulnerabilities

30 Labs

Designed to build web application penetration testing skills through guided practice, these labs progress from provisioning a vulnerable environment to exploiting and mitigating common web vulnerabilities (SQLi, XSS, command injection), firewall concepts, and incident response—making them ideal for hands-on web security and pentesting pathways.

Provisioning a Web Server
Install and configure an Apache web server on Ubuntu, including virtual hosts, remote administration, and secure file transfer.

Exploring HTML
Analyze the structure of HTML to understand how web pages are built and how vulnerabilities can be introduced.

Provisioning a MySQL Database
Install and configure a MySQL database and create tables used for user authentication and data storage.

Provisioning PHP
Install and configure PHP on a web server and implement basic user authentication using HTML forms and PHP scripts.

Dissecting the Login Process
Analyze how user credentials are processed from form submission through database queries and server responses.

SQL Injection (SQLi)
Exploit SQL injection vulnerabilities to bypass authentication and understand how improper input handling leads to compromise.

SQLi Vulnerability and Pentesting Steps
Follow a structured penetration testing methodology to identify, exploit, and recommend controls for SQL injection vulnerabilities.

HTML Injection (HTMLi)
Exploit HTML injection vulnerabilities to understand how attackers manipulate web page content.

HTML Injection Vulnerability and Mitigation
Apply security controls to mitigate HTML injection vulnerabilities and reduce attack surface.

Reflected Cross-Site Scripting (XSS)
Execute reflected XSS attacks to demonstrate how malicious scripts are injected and executed in user browsers.

Reflected XSS Mitigation and URL Encoding
Apply filtering and encoding techniques to mitigate reflected XSS attacks and understand their limitations.

PHP Sessions and Cookies
Analyze how PHP sessions and cookies maintain state and how attackers can exploit weak session management.

Additional Script Elements
Explore alternative script elements attackers use to bypass filtering and execute malicious code.

Session Stealing via Remote Reflected XSS
Use phishing techniques and browser tools to steal session identifiers through remote reflected XSS attacks.

Remote Reflected XSS Mitigation and Encoding
Apply advanced input validation and encoding techniques to reduce remote reflected XSS risks.

Vulnerable Forum
Deploy a vulnerable forum application to simulate real-world attack surfaces and user interaction risks.

PenTesting and Understanding Vulnerabilities

Pentesting the Forum
Identify and exploit stored XSS vulnerabilities within a forum application and apply mitigation controls.

Session Stealing via Stored XSS
Exploit stored XSS vulnerabilities to hijack active user sessions and extract session identifiers.

Command Injection
Exploit command injection vulnerabilities to execute operating system commands through vulnerable web applications.

Stateless Firewall Configuration
Configure a stateless firewall and test its ability to defend against denial-of-service attacks.

Abusing a Stateless Firewall
Bypass stateless firewall protections using crafted DoS attacks and packet manipulation techniques.

Stateful Firewall Configuration
Configure a stateful firewall and evaluate its effectiveness against network-based attacks.

Abusing a Stateful Firewall
Demonstrate how certain attacks can bypass stateful firewall protections, including SYN-based DoS attacks.

IDS, Syslog, and NTP
Configure intrusion detection, centralized logging, and time synchronization to improve security visibility.

Signature Detection and Alerting
Create custom SNORT signatures to detect malicious traffic and alert administrators.

IPS, Syslog, and NTP
Deploy intrusion prevention systems and logging infrastructure to detect and block active threats.

Signature Detection and Remote Shell Prevention
Detect and prevent remote shell activity using custom intrusion detection signatures.

Remote Shell: Embedding Client-Side Code
Analyze how malicious client-side code can be embedded into software packages to establish remote shells.

Remote Shell Data Extraction
Use exploitation frameworks to extract data from compromised systems via remote shells.

Incident Response Procedures and Forensic Analysis
Apply incident response and forensic analysis techniques to investigate attacks and preserve evidence.

Cybersecurity Attack and Defend

18 Labs

Designed to build practical blue-team and investigation skills through guided practice, these labs progress from identifying malicious indicators and monitoring to host hardening, malware analysis, forensics across platforms, encryption, secure transfer, and integrity validation—making them ideal for defensive security and incident response pathways.

Creating and Securing User Accounts
Manage and secure user accounts across Linux and Windows systems using command-line and graphical tools to reduce account-based risk.

Network Exploitation
Exploit a vulnerable system using Metasploit to understand how unpatched systems are compromised and how timely patching prevents attacks.

Finding Malicious Indicators
Identify indicators of compromise by analyzing system artifacts using command-line and GUI tools on a compromised Windows Server.

Static and Dynamic Malware Analysis
Analyze malware using static techniques such as hashing and dynamic execution to observe real-world malicious behavior.

Local Operating System Exploitation
Exploit local operating system vulnerabilities to understand post-compromise attack techniques and escalation paths.

Investigating a Network Compromise
Analyze a compromised network environment to identify attacker entry points, lateral movement, and persistence mechanisms.

Log Analysis in Linux and Splunk
Analyze logs using Linux tools and Splunk to detect indicators of compromise, attacker behavior, and post-exploitation activity.

Network and System Monitoring
Capture and analyze network traffic using tcpdump in a SPAN-port environment to monitor suspicious activity.

Hardening Windows
Apply best practices for securing Microsoft Windows systems through updates, configuration hardening, and defensive controls.

Hardening Linux
Secure Linux systems by applying hardening techniques commonly used in enterprise and cloud environments.

Windows Registry Analysis
Analyze the Windows Registry using recovery tools to identify system changes and potential malicious modifications.

Forensic Analysis of Windows Server
Conduct forensic analysis on a Windows Server using Autopsy, including examination of IIS logs to identify intrusion activity.

Forensic Analysis of a Windows Client
Use forensic tools to analyze Windows client systems and identify evidence of compromise and user activity.

Forensic Analysis of a Linux System
Perform forensic analysis on a Linux system using Autopsy to investigate system artifacts and attacker behavior.

Using Encrypting File System (EFS)
Protect sensitive files and folders using Windows Encrypting File System (EFS) and enforce access controls.

Using Disk Encryption
Apply full-disk encryption to protect data at rest and prevent unauthorized access.

Cybersecurity Attack and Defend

Using SSH and SCP
Securely transfer files and remotely manage systems using encrypted SSH and SCP connections.

Using Hash Functions to Validate Data Integrity
Verify file integrity using hashing algorithms such as MD5, SHA-1, and SHA-512 to ensure data has not been altered.

Red Team and Blue Team Fundamentals

21 Labs

Designed to build foundational red-team and blue-team skills through guided practice, these labs progress from core protocols and tools (Kali, Nmap, Wireshark, Metasploit) to monitoring, firewalling, credential attacks, exploitation scenarios, and cyber range fundamentals—making them ideal for introductory adversarial and defensive security pathways.

Introduction to Red Team and Blue Team Fundamentals
Understand the roles, responsibilities, and objectives of Red Team (offensive) and Blue Team (defensive) operations within modern cybersecurity environments.

Protocols and Ports Used for Exploits
Identify open ports and active services on Windows and Linux systems to understand how attackers discover and exploit network weaknesses.

IP Addressing and Virtualization Concepts
Plan and implement IP addressing schemes, perform subnetting, and verify network configurations to support secure infrastructure design.

Red Team: Introduction to Kali Linux
Install and configure Kali Linux as an attack platform for Red Team operations and penetration testing activities.

Server Operating Systems Installation Methods
Install and configure Windows Server to support enterprise environments and security testing scenarios.

Wireshark Essentials
Capture and analyze network traffic using Wireshark to identify suspicious activity and validate network behavior.

Blue Team: Network Monitoring Tools
Monitor system and network performance using Windows and Linux tools to detect anomalies and potential security incidents.

Red Team: Nmap Network Scanning Techniques
Discover hosts and open services using Nmap and Zenmap to map attack surfaces and identify exploitable targets.

Blue Team: Server Firewall Configuration
Configure and manage server-based firewalls to protect systems from unauthorized access and network-based threats.

Red Team and Blue Team Fundamentals

Red Team: Man-in-the-Middle Exploits
Conduct Man-in-the-Middle (MITM) attacks using ARP spoofing techniques to intercept and manipulate network traffic.

Blue Team: Malware and Antivirus Protection
Deploy and test malware protection controls on Windows and Linux systems to detect and mitigate malicious software.

Red Team: Introduction to Metasploit
Use the Metasploit Framework to develop exploits, manage payloads, and conduct controlled attacks on vulnerable systems.

Blue Team: Patch Management and Software Updates
Identify system vulnerabilities and apply patches and updates to reduce exposure to known exploits.

Red Team: Credential Harvesting Tools
Harvest and crack credentials using tools such as Metasploit, Responder, and John the Ripper to demonstrate credential-based attacks.

Blue Team: Securing Servers with Policies
Implement security policies, password standards, and Group Policy controls to harden enterprise systems.

Denial-of-Service Attack and Mitigation
Launch and analyze Denial-of-Service attacks and apply defensive techniques to reduce service disruption.

Exploiting Telnet Vulnerabilities
Exploit insecure Telnet services and implement IPSec policies to protect against interception and misuse.

SMB Exploitation with Responder
Exploit SMB file sharing weaknesses and analyze credential interception attacks using Responder.

Brute Force Password Attacks
Conduct brute force attacks against authentication services and apply hardening techniques to mitigate credential abuse.

Exploiting Windows with Metasploit (EternalBlue)
Exploit unpatched Windows systems using EternalBlue to understand the impact of critical vulnerabilities.

Introduction to Cyber Ranges
Apply Red Team and Blue Team techniques within cyber range environments designed to simulate real-world attack and defense scenarios.

CompTIA SecurityX (CAS-005)

15 Labs

Designed to build CASP+/SecurityX (CAS-005) aligned advanced security skills through guided practice, these labs progress from governance and resilient architecture to secure cloud solutions, automation, SIEM implementation, threat-hunting resources, and malware analysis—making them ideal for advanced security operations and security engineering pathways.

Governance, Risk, and Compliance (GRC)
Apply governance frameworks, risk management practices, and compliance controls to align security strategy with business objectives and regulatory requirements.

Resilient System Architecture Design
Design and implement resilient architectures that maintain availability, fault tolerance, and recovery capabilities across enterprise environments.

Automated Software Deployment
Deploy automated software delivery solutions to improve consistency, reduce configuration drift, and support secure DevOps and enterprise operations.

Vulnerability Management Implementation
Build and operate a vulnerability management program that identifies, prioritizes, and remediates security weaknesses across enterprise systems.

Secure Access Control Solutions
Implement identity, authentication, and authorization controls to enforce least privilege and protect sensitive enterprise resources.

Secure Cloud Storage Deployment
Deploy and secure cloud-based storage solutions with encryption, access controls, and compliance considerations for enterprise workloads.

Authentication and Authorization Troubleshooting
Detect, analyze, and resolve authentication and authorization failures that impact user access, system security, and operational continuity.

Secure System Architecture Implementation
Apply security controls and design principles to harden enterprise systems against modern threats and attack vectors.

Network Infrastructure Troubleshooting and Remediation
Diagnose and remediate complex network infrastructure issues affecting performance, security, and availability.

Automated Security Monitoring
Implement automated monitoring solutions to detect threats, anomalies, and security events across enterprise environments.

Cryptographic Solution Deployment
Deploy cryptographic solutions to protect data confidentiality, integrity, and availability in transit and at rest.

Enterprise SIEM Implementation
Design and implement an enterprise SIEM solution to centralize logging, correlate security events, and support incident response.

Enterprise Vulnerability Detection
Identify and assess vulnerabilities across enterprise infrastructure to reduce attack surface and improve security posture.

Threat Hunting and Intelligence Resources
Leverage threat-hunting tools and intelligence sources to proactively identify adversary activity and emerging threats.

Malware Detection and Analysis
Detect, analyze, and respond to malware infections to minimize impact and strengthen enterprise defenses.

Ethical Hacking & Systems Defense

15 Labs

Designed to build applied ethical hacking and defense skills through guided practice, these labs progress from reconnaissance and scanning to exploitation, traffic analysis, social engineering, wireless attacks, web attacks, and secure communications—making them ideal for hands-on security and ethical hacking pathways.

Reconnaissance from the WAN
Conduct external reconnaissance to identify exposed services, attack surfaces, and security weaknesses from an adversary's perspective.

LAN Network Scanning
Scan internal networks to discover hosts, services, and vulnerabilities that could be leveraged during lateral movement or escalation.

Host Enumeration with Wireshark, Windows, and Linux
Enumerate systems using packet analysis and native command-line tools to uncover network relationships, services, and misconfigurations.

Remote and Local Exploitation
Exploit vulnerable systems locally and remotely to demonstrate how attackers gain access, escalate privileges, and persist within environments.

Malware Deployment with Remote Access Trojans (RATs)
Craft and deploy malware to establish command-and-control access, while analyzing detection and mitigation strategies.

Network Traffic Capture and Analysis
Capture and analyze network traffic to identify sensitive data exposure, insecure protocols, and attacker activity.

Social Engineering Attacks Using SET
Execute social engineering attacks to exploit human vulnerabilities and understand how attackers bypass technical controls.

Denial-of-Service Attacks from the WAN
Launch and analyze denial-of-service attacks to understand their impact on availability and how defenses can mitigate them.

Browser-Based Exploitation
Exploit browser vulnerabilities to compromise endpoints and demonstrate the risks of client-side attacks.

Web Server Attacks from the WAN
Attack exposed web servers to identify configuration flaws, vulnerable services, and insecure deployments.

Exploiting Vulnerable Web Applications
Identify and exploit web application vulnerabilities to demonstrate real-world attack paths against business applications.

SQL Injection Attacks
Perform SQL injection attacks to manipulate databases, extract data, and understand defensive coding practices.

Wireless Security Attacks (WEP/WPA)
Break weak wireless encryption to capture and decrypt traffic, highlighting the risks of outdated security protocols.

Firewall Evasion and Data Exfiltration
Attack firewalls and exfiltrate data over encrypted channels to demonstrate advanced evasion techniques.

Public Key Encryption for Secure Communications
Apply public key encryption to secure communications and understand how cryptography protects data from interception.

Applications of Cybersecurity Using ChatGPT

8 Labs

Designed to build practical cybersecurity workflows using generative AI through guided practice, these labs progress from ChatGPT fundamentals to phishing simulation planning, threat intelligence support, policy creation, secure coding review, automation scripting, and security awareness content—making them ideal for modern security operations and AI-assisted security pathways.

Introduction to ChatGPT and Generative AI
Build foundational knowledge of ChatGPT and generative AI, including how large language models work, their strengths, limitations, and responsible use in cybersecurity contexts.

Planning and Executing a Phishing Simulation with ChatGPT
Use ChatGPT to design realistic phishing simulations, including campaign planning, messaging analysis, and risk assessment—while reinforcing ethical and defensive objectives.

Social Media Threat Intelligence with ChatGPT
Leverage ChatGPT to analyze social media data for threat intelligence, identifying trends, indicators of compromise, and emerging social engineering techniques.

Creating an Incident Response Policy Using ChatGPT
Develop a structured incident response policy using ChatGPT to support detection, containment, eradication, recovery, and post-incident analysis.

Detecting and Mitigating Security Vulnerabilities with ChatGPT
Use ChatGPT to review Python code, identify security vulnerabilities, and recommend secure coding practices and remediation strategies.

Cybersecurity Automation with ChatGPT
Write automation scripts using ChatGPT to streamline security tasks such as log analysis, alert triage, configuration validation, and response workflows.

Writing Organizational Security Policies with ChatGPT
Apply ChatGPT to draft clear, structured security policies aligned with organizational needs, regulatory requirements, and best practices.

Developing Social Engineering Awareness Training with ChatGPT
Create effective security awareness and social engineering training materials using ChatGPT to improve user resilience against human-focused attacks.

AI/ML in Cybersecurity (Cybersecurity Analytics)

12 Labs

Designed to build AI-driven cybersecurity analytics skills through guided practice, these labs progress from prompt engineering to using generative AI with malware analysis, deepfake detection, web app testing, automation, and text/image generation—making them ideal for security analytics and emerging-technology pathways.

Analyzing Malware with ChatGPT and YARA
Use ChatGPT alongside YARA rules to analyze malware samples, identify behavioral patterns, and support detection and classification workflows.

Combating Social Engineering with AI/ML
Apply ChatGPT and machine learning techniques to identify, analyze, and mitigate social engineering attacks such as phishing and pretexting.

Web Application Security Testing with ChatGPT and OWASP ZAP
Leverage ChatGPT to plan, execute, and interpret web application security testing using OWASP ZAP, supporting vulnerability identification and remediation.

Detecting Deepfakes with AI/ML
Analyze media artifacts using AI/ML techniques to identify deepfake content and assess authenticity risks in security investigations.

Robotic Process Automation (RPA) with ChatGPT and Python
Build AI-assisted automation workflows using ChatGPT and Python to streamline repetitive cybersecurity and operational tasks.

Planning and Executing Phishing Simulations with ChatGPT
Design and evaluate phishing simulations using ChatGPT to improve organizational readiness and user awareness.

Detecting and Mitigating Code Vulnerabilities with ChatGPT
Use ChatGPT to review Python code, identify security flaws, and recommend secure coding and remediation strategies.

Malware Analysis with ChatGPT and Cuckoo Sandbox
Combine ChatGPT with dynamic analysis from Cuckoo Sandbox to investigate malware behavior and support incident response.

Fundamentals of Prompt Engineering
Develop effective prompts to guide AI systems for cybersecurity analysis, automation, and investigative workflows.

Intermediate and Advanced Prompt Engineering
Refine prompt design techniques to improve accuracy, consistency, and analytical depth in AI-assisted security tasks.

Generative AI for Text Analysis and Reporting
Use generative AI to produce structured security reports, summaries, and analytical narratives from technical data.

Generative AI for Image Analysis and Creation
Apply generative AI to image-based workflows, including security visualization, threat illustration, and analysis support.

Network & Cybersecurity Automation with Ansible

11 Labs

Designed to build automation skills for network and security operations through guided practice, these labs progress from Ansible basics to playbooks, inventory management, device hardening, firewall automation, log collection, vulnerability scanning workflows, and automated deployments—making them ideal for DevSecOps and security automation pathways.

Introduction to Ansible with ChatGPT
Build foundational knowledge of Ansible concepts and architecture while using ChatGPT to assist with playbook creation, troubleshooting, and learning reinforcement.

Working with Control Structures in Ansible Using ChatGPT
Use ChatGPT to design and implement Ansible control structures such as conditionals and loops, enabling scalable and dynamic automation workflows.

Hardening Network Devices with Ansible and ChatGPT
Apply security baselines and hardening configurations across networked systems using Ansible playbooks supported by ChatGPT-guided development.

Automated Inventory Management with Ansible and ChatGPT
Automate the discovery, organization, and management of infrastructure inventory using Ansible, with ChatGPT assisting in playbook logic and optimization.

Automating Vulnerability Scanning with Nessus, Ansible, and ChatGPT
Integrate Nessus scanning into automated workflows using Ansible, with ChatGPT supporting scan orchestration, execution, and result interpretation.

Managing Tasks in Ansible Playbooks with ChatGPT
Design, organize, and execute Ansible tasks efficiently, using ChatGPT to improve readability, structure, and maintainability of playbooks.

Automating System Administration Tasks with Ansible and ChatGPT
Streamline routine system administration activities—such as updates, service management, and configuration enforcement—through AI-assisted automation.

Automating LAMP Stack Deployment with Ansible and ChatGPT
Deploy a complete LAMP environment using Ansible automation, following best practices for installation, configuration, and validation with ChatGPT support.

Automating Firewall Configuration with Ansible and ChatGPT
Implement consistent, repeatable firewall configurations across systems using Ansible, with ChatGPT assisting in rule design, validation, and troubleshooting.

Automated Log Collection with Ansible and ChatGPT
Centralize and automate log collection processes using Ansible playbooks, ensuring visibility and consistency across enterprise systems.

Automating Application Installation with Ansible and ChatGPT
Create reliable, repeatable application deployment workflows using Ansible, with ChatGPT aiding in dependency handling, sequencing, and verification.

LogRhythm – Analyst Fundamentals (v7)

7 Labs

Designed to build LogRhythm SIEM analyst skills through guided practice, these labs progress from platform familiarization to use-case execution, ransomware and botnet detection, outage response, and policy-driven investigations—making them ideal for SIEM onboarding and SOC analyst pathways.

LogRhythm SIEM Familiarization
Build foundational proficiency with the LogRhythm platform by exploring core SIEM concepts, analyst workflows, and interface navigation. Learners review key sections of the LogRhythm Analyst Fundamentals guide to understand how data is collected, normalized, and analyzed to support security operations.

Analyst Use Case Walkthrough
Develop hands-on experience with real-world security use cases by walking through a complete analyst workflow. Learners examine detection logic, alerts, and investigative steps outlined in LogRhythm Analyst Fundamentals Chapter 4, reinforcing how SIEM data supports actionable decision-making.

Complete Use Case Investigation
Apply security analytics concepts to a full end-to-end use case. Students analyze events, correlate data, and validate findings using methodologies from the LogRhythm Security Analytics guide, strengthening investigative and analytical skills required in a SOC environment.

Ransomware Injection Detection and Analysis
Gain practical experience detecting and analyzing ransomware activity within LogRhythm. Learners use guided scenarios to understand attack indicators, log patterns, and response considerations based on LogRhythm Security Analytics Chapter 4.

Botnet Detection and Threat Identification
Analyze botnet-related activity using LogRhythm security analytics. Students investigate malicious command-and-control behavior, network indicators, and alert patterns, reinforcing detection strategies described in LogRhythm Security Analytics Chapter 5.

Reducing Downtime Caused by a Security Outage
Learn how LogRhythm analytics can be used to identify, investigate, and mitigate incidents that cause operational downtime. This lab emphasizes incident response efficiency, root-cause analysis, and continuity considerations using scenarios from Chapter 6.

Acceptable Use Policy Compliance Monitoring
Develop skills in monitoring and enforcing acceptable use policies through LogRhythm SIEM analytics. Learners analyze user behavior, identify policy violations, and support compliance objectives using investigative techniques from Chapter 7.

Cyber Challenge Range

19 Labs

Designed to build applied cyber range skills through scenario-based guided challenges, these labs progress from reconnaissance and initial access to persistence, forensics, malware analysis, reverse engineering, evidence recovery, and debugging code—making them ideal for capstone experiences and skills validation pathways.

Challenge – Reconnaissance
Develop foundational reconnaissance skills by identifying perimeter defenses and externally exposed services. Learners locate the organization's outer firewall and perform active scanning to identify potential vulnerabilities, building essential pre-exploitation awareness.

Challenge – Cracking the Perimeter
Apply exploitation techniques to bypass perimeter defenses and gain access to the demilitarized zone (DMZ). This challenge reinforces firewall evasion, service exploitation, and lateral movement concepts used in real-world penetration testing.

Challenge – Infiltration
Advance from initial foothold to internal network access by pivoting from the development (DEV) network into the user network. Learners practice network traversal, credential use, and access escalation techniques.

Challenge – Situational Awareness
Leverage previously discovered credentials to infiltrate the administrative network. Learners assess the environment, identify high-value targets, and make informed attack decisions based on network awareness and privilege context.

Challenge – Kerberoasting
Execute a Kerberoasting attack to obtain privileged credentials and generate a Golden Ticket for domain persistence. This challenge emphasizes Active Directory exploitation, credential abuse, and long-term access techniques.

Challenge – Locating the Crown Jewels
Identify and access the organization's most critical assets—specifically sensitive financial systems. Learners analyze implant behavior, command-and-control callbacks, and target prioritization strategies.

Challenge – Exfiltrating Data
Demonstrate controlled data exfiltration techniques by extracting sensitive financial data from a mainframe system. This challenge highlights stealth, data handling, and operational security considerations.

Challenge – Covering Your Tracks
Simulate post-engagement cleanup by removing indicators of compromise, creating fallback access mechanisms, and maintaining covert persistence. Learners explore attacker tradecraft used to evade detection.

Challenge – Maintaining Persistence
Establish and manage persistent access through backdoors and implants. Learners analyze callback behavior and persistence mechanisms commonly used in advanced threat campaigns.

Challenge – Carving Disk Images
Recover critical information from backup disk images to obtain local administrative access. Learners practice forensic image analysis and data recovery techniques used in incident response and investigations.

Challenge – Host-Based Forensics
Conduct a full forensic analysis of a compromised system to answer investigative challenge questions. This lab reinforces evidence collection, timeline reconstruction, and artifact analysis.

Cyber Challenge Range

Challenge – Mobile Forensics
Perform a basic forensic examination of a mobile device. Learners analyze artifacts, recover data, and build familiarity with mobile forensic workflows.

Challenge – Malware Analysis in Windows
Analyze malware samples to understand execution flow, behavior, and components. Learners perform rapid static and dynamic analysis to identify malicious intent and functionality.

Challenge – Reverse Engineering in Linux
Disassemble and reverse engineer Linux binaries to understand program logic and behavior. This challenge builds low-level analysis skills critical for malware researchers and exploit developers.

Challenge – Binary Exploitation
Develop a working exploit that leverages a race condition to gain unauthorized access to protected files. Learners combine debugging, exploitation, and privilege escalation techniques.

Challenge – Searching Through Evidence
Analyze forensic evidence to uncover hidden data, including encoded cryptocurrency wallet information. Learners use Kali Linux forensic tools to identify steganography and obfuscation techniques.

Challenge – File Recovery
Recover corrupted or deleted files using forensic tools in the FLARE VM. This challenge emphasizes data restoration and investigative problem-solving.

Challenge – Recreating an Attack
Reconstruct an attack scenario from forensic evidence. Learners identify the vulnerability, reproduce the exploit, and validate findings—mirroring real-world incident reconstruction tasks.

Challenge – Debugging Existing Python Code
Debug and repair existing Python scripts in a penetration testing context. Learners improve scripting proficiency, problem-solving skills, and tool customization capabilities.

Computer Forensics and Investigations

15 Labs

Designed to build foundational digital forensics and investigations skills through guided practice, these labs progress from acquisition and scene handling to analysis across systems, mobile, cloud, reporting, and courtroom readiness—making them ideal for forensics and investigative pathways.

Understanding the Digital Forensics Profession and Investigations
Explore the role of the digital forensic examiner, investigative workflows, legal considerations, and professional responsibilities within criminal, civil, and corporate investigations.

Processing Crime and Incident Scenes (Lab ID-3528)
Apply proper procedures for identifying, preserving, and documenting digital evidence at crime scenes and incident locations to maintain chain of custody and evidentiary integrity.

Computer Forensics and Investigations

Data Acquisition
Perform forensic data acquisition using Linux-based tools, including preparing target drives and capturing disk images with dd while preserving evidentiary integrity.

Virtual Machine Forensics, Live Acquisitions, and Network Forensics
Conduct live acquisitions, analyze virtual machine artifacts, and collect network evidence to support active incident investigations.

Working with Windows and CLI Systems
Analyze disk partitions, deleted NTFS files, and Windows Registry artifacts using both GUI and command-line techniques.

Linux and Macintosh File Systems
Examine Linux and macOS file systems using Sleuth Kit and Autopsy to recover files and analyze file system structures.

Recovering Graphics Files
Recover and analyze image files from forensic media, reinforcing file carving and artifact recovery techniques.

Current Digital Forensics Tools
Evaluate and apply modern digital forensics tools to analyze evidence across multiple investigative scenarios.

Digital Forensics Analysis and Validation
Analyze digital evidence and validate findings to ensure accuracy, repeatability, and admissibility.

E-mail and Social Media Investigations
Investigate email and social media artifacts to identify communication patterns, timelines, and relevant evidence.

Mobile Device Forensics
Extract and analyze data from mobile devices, including call logs, messages, application data, and metadata.

Cloud Forensics
Investigate cloud-based environments by identifying, collecting, and analyzing artifacts from cloud services and platforms.

Reporting, Legal Process & Courtroom Readiness

Report Writing for High-Tech Investigations
Develop clear, defensible forensic reports that accurately document findings, methods, and conclusions.

Expert Testimony in Digital Investigations
Prepare to present forensic findings in legal proceedings, including courtroom procedures and expert witness responsibilities.

Ethics for the Expert Witness
Examine ethical standards and professional conduct requirements for forensic investigators serving as expert witnesses.

CISSP (Certified Information Systems Security Professional)

24 Labs

Designed to build CISSP-aligned security knowledge through guided practice, these labs progress across risk management, cryptography, access control, secure network and system administration, vulnerability scanning, incident response concepts, and secure infrastructure configuration—making them ideal for advanced security and CISSP preparation pathways.

Introduction to CISSP
Explore the CISSP certification structure, exam domains, and real-world application of CISSP principles. Learners contextualize how CISSP knowledge is applied across enterprise security roles.

Security and Risk Management
Apply governance, risk, and compliance principles through hands-on scenarios that reinforce risk assessment, policy alignment, and organizational security strategy.

Encryption and Hashing
Compare encryption and hashing techniques, evaluate hash algorithms, and analyze integrity verification mechanisms foundational to asset protection.

Implement OpenPGP
Deploy OpenPGP for secure communication, including key generation, certificate distribution, message signing, verification, and decryption.

BitLocker on Portable Media
Protect data at rest by implementing encryption controls for removable media in enterprise environments.

SCCM Configuration Items and Baselines
Implement configuration baselines to enforce security standards and ensure consistent system hardening.

Implement SSL VPN using ASA Device Manager
Deploy clientless and AnyConnect SSL VPNs to secure remote access using enterprise-grade network security controls.

Configuring IPtables
Apply firewall rules and traffic filtering using Linux IPtables to enforce network segmentation and secure communication paths.

Configure and Verify IPv4 and IPv6 Access Lists
Design, implement, and verify access control lists for IPv4 and IPv6 traffic filtering in secure network architectures.

Two-Factor Authentication with SSH
Strengthen authentication mechanisms by implementing multi-factor authentication for secure remote access.

Manage Role-Based Security
Design and manage role-based access controls, including administrative scopes and privilege boundaries.

Managing Remote Desktop
Secure remote administration services through configuration and access control best practices.

Administering and Deploying Endpoint Protection
Deploy endpoint protection solutions to defend against malware and endpoint-based threats.

Windows Command Line Tools
Use command-line tools to support secure system administration and operational security tasks.

Installing Kali
Deploy Kali Linux to support security operations, testing, and analysis activities.

Implement Backup and Recovery
Design and execute backup and recovery strategies to support availability and resilience requirements.

CISSP (Certified Information Systems Security Professional)

Installation and Verification of Snort
Install and configure intrusion detection systems to monitor and detect malicious activity.

Upgrading and Securing SSH Connections
Harden SSH services by upgrading configurations, regenerating keys, mitigating MITM risks, and enforcing secure access policies.

Configuring and Securing IIS
Secure web servers by applying hardening techniques, configuration best practices, and access controls.

Configuring MBSA Scanner
Identify system vulnerabilities using automated scanning tools to support continuous security assessment.

Compliance Patching
Implement patch management using WSUS, including certificate configuration, group policies, and compliance validation.

Passive Topology Discovery
Analyze network topology using packet capture and traffic analysis to support asset discovery and threat assessment.

Scanning and Remediating Vulnerabilities with OpenVAS
Perform vulnerability scanning and remediation to reduce enterprise attack surfaces.

DVWA – Manual SQL Injection and Password Cracking
Analyze insecure application behavior by performing SQL injection attacks and password cracking, reinforcing secure coding and application defense concepts.

Cloud Computing

CompTIA Cloud+ (CV0-004)

18 Labs

Designed to build Cloud+ (004) aligned skills through guided practice, these labs progress from service models and storage to virtualization, deployment automation, resource provisioning, logging, security controls, backup, vulnerability management, and DevOps fundamentals—making them ideal for cloud operations and certification-aligned pathways.

Cloud Service Models
This lab introduces cloud service models, including shared responsibility, service delivery models, and advanced cloud services. Learners explore how cloud responsibilities are divided between providers and customers through structured, real-world scenarios.

Service Availability Concepts
Learners examine service availability concepts by configuring high availability and scalability within a private cloud environment. The lab focuses on maintaining uptime and ensuring resilient cloud services.

Introduction to Cloud Networking Concepts
This lab covers foundational cloud networking concepts, including network segmentation, cloud network services, and security protocols used to protect cloud traffic.

Cloud Storage Concepts
Learners work with cloud storage services by provisioning an Amazon S3 bucket and an Azure Storage account, gaining hands-on experience with object storage resources.

Introduction to Virtualization
This lab explores virtualization concepts, including virtual machine provisioning and hypervisor types. Learners examine Type 1 and Type 2 hypervisors and their roles in private cloud environments.

Cloud Database Concepts
Learners explore cloud database services, including relational databases such as Amazon RDS and SQL Server, as well as non-relational databases like Amazon DynamoDB.

Cloud Deployment Models
This lab examines cloud deployment models by exploring public cloud providers and private cloud environments through guided exercises.

Code-based Cloud Deployment and Configuration
Learners deploy and configure cloud resources using code-based methods, working with services such as Amazon EC2 and Amazon S3 to implement cloud infrastructure.

Provisioning Cloud Resources
This lab focuses on provisioning cloud resources, including selecting and deploying Amazon EC2 instance types and configuring AWS Auto Scaling.

Configuring Logging in the Cloud
Learners configure cloud logging by examining dashboards, reporting features, and log data used to monitor cloud environments.

Implementing Cloud Security Controls
This lab covers the implementation of cloud security controls within AWS, including identity and access management, network security, encryption, and threat detection services.

CompTIA Cloud+ (CV0-004)

Cloud Security Monitoring Techniques
Learners monitor cloud security by observing and analyzing a virtual machine in Microsoft Azure using built-in monitoring tools.

Implementing Cloud Backup Solutions
This lab focuses on implementing cloud backup solutions, including performing backup and restoration operations for a virtual machine.

Cloud Vulnerability Management
Learners perform cloud vulnerability management tasks, including log collection and analysis using Splunk to identify and prioritize security issues.

Cloud Resource Access Management
This lab explores cloud resource access management concepts through hands-on configuration of access controls in a cloud environment.

Cloud Security Best Practices
Learners apply cloud security best practices by creating and configuring a secure cloud storage solution.

Cloud DevOps Fundamentals
This lab introduces Cloud DevOps concepts by guiding learners through creating and configuring application settings in a cloud environment.

AWS Cloud Practitioner (CLF-C01)

9 Labs

Designed to build CLF-C01 aligned AWS foundational knowledge through guided practice, these labs progress from core cloud concepts to security/compliance, deployment models, global infrastructure, and primary compute, storage, networking, and database services—making them ideal for AWS Cloud Practitioner preparation pathways.

Security Concept Fundamentals
Explore core security principles including confidentiality, integrity, and availability (CIA). Examine how authentication and authorization support these principles and how security controls are implemented using common tools and configurations.

AWS Security & Compliance Concepts
Review AWS security and compliance capabilities by exploring AWS Artifact and understanding how AWS supports regulatory and compliance requirements. Examine logging services used to track, monitor, and audit activity within AWS environments.

AWS Security Services
Work with AWS-native security services to understand how cloud environments are protected. Identify key AWS security services and examine how they integrate with third-party security tools.

AWS Deployment Methods
Examine AWS deployment methods and commonly used services such as EC2, RDS, and S3. Understand how different deployment approaches support application delivery, scalability, and operational needs.

AWS Cloud Practitioner (CLF-C01)

AWS Global Infrastructure
Explore the AWS global infrastructure, including regions and availability zones. Understand how AWS delivers high availability, fault tolerance, and global scalability.

AWS Computing Services
Examine AWS computing services used to run applications and workloads in the cloud. Understand how compute options support different performance, scaling, and cost requirements.

AWS Storage Services
Explore AWS storage services including Amazon S3, EBS, Glacier, Snowball, EFS, Storage Gateway, RDS, DynamoDB, and Redshift. Understand how each service supports different data storage, access, and durability needs.

AWS Networking Services
Explore AWS networking services with a focus on Virtual Private Cloud (VPC) components and IP address management. Understand how networking services are used to design secure and scalable cloud environments.

AWS Database Services
Explore AWS database services and create databases within AWS-managed environments. Understand how relational and non-relational databases are deployed and used in cloud architectures.

AWS Cloud Practitioner (CLF-C02)

12 Labs

Designed to build CLF-C02 aligned AWS foundational knowledge through guided practice, these labs progress from identifying services and IAM to monitoring/logging, security services, infrastructure, core service categories, and billing/support—making them ideal for AWS Cloud Practitioner preparation pathways.

Introduction to AWS Cloud
This lab introduces Amazon Web Services (AWS) and its core cloud services. Learners explore foundational AWS concepts, including cloud computing basics and networking services such as Amazon Virtual Private Cloud (VPC).

Identifying AWS Services
Learners identify and explore core AWS services, including compute services like Amazon Elastic Compute Cloud (EC2), through guided exercises.

AWS Monitoring and Logging Services
This lab explores AWS monitoring and logging services, including Amazon CloudWatch, AWS Shield, and AWS Artifact. Learners work with metrics, logs, alarms, and monitoring dashboards.

AWS Identity and Access Management
Learners work with AWS Identity and Access Management (IAM) to improve account security, including managing users, permissions, and API keys.

AWS Cloud Practitioner (CLF-C02)

AWS Security Services
This lab introduces AWS security services and tools used to enhance cloud security. Learners explore built-in AWS security services and their integration within the AWS environment.

AWS Deployment Models
Learners examine AWS deployment and service models, including Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), along with connectivity options that support different business needs.

AWS Global Infrastructure
This lab explores the AWS global infrastructure, including regions, availability zones, and edge locations, and how they support scalability and availability.

AWS Computing Services
Learners explore AWS computing services used for a variety of cloud-based workloads and applications.

AWS Database Services
This lab introduces AWS database services. Learners explore database options and create a database within the AWS environment.

AWS Networking Services
Learners work with AWS networking services, exploring core networking components within a pre-configured AWS environment.

AWS Storage Services
This lab explores AWS storage services, including Amazon S3, Elastic Block Store (EBS), S3 Glacier, Elastic File System (EFS), Storage Gateway, and data transfer solutions.

AWS Billing and Support Services
Learners explore AWS billing and support services, including cost estimation using the AWS Pricing Calculator and reviewing available AWS support plans.

MS Azure Fundamentals

5 Labs

Designed to build Azure platform basics through guided practice, these labs introduce essential cloud concepts, the Azure platform, resource groups, networking fundamentals, and virtual machines—making them ideal for Azure beginner pathways.

Cloud Essential Concepts
This lab introduces foundational cloud computing concepts. Learners explore cloud service providers, cloud computing models, cloud service types, and the benefits of cloud infrastructure.

The Azure Platform
Learners explore the Microsoft Azure platform and its role as Microsoft's cloud solution. The lab focuses on navigating Azure and understanding how cloud resources and infrastructures are created and managed.

Azure Resource Groups
This lab focuses on Azure Resource Groups. Learners navigate the Azure portal and identify, organize, and manage resources using resource groups.

Azure Networking Concepts
Learners explore core Azure networking components and concepts, gaining familiarity with how networking is implemented and managed within Azure.

MS Azure Fundamentals

Azure Virtual Machines
This lab introduces Azure Virtual Machines. Learners create and scale virtual machines using the Azure portal and explore Infrastructure as a Service (IaaS) concepts within Azure.

Cloud Essentials

10 Labs

Designed to build foundational cloud OS and security skills through guided practice, these labs progress from configuring cloud Linux instances to SSH access, network configuration, services, logging, hashing, IoT concepts, and cloud hardening—making them ideal for introductory cloud and cloud-security pathways.

Installing Kali Cloud Linux
This lab introduces the installation of Kali Linux in a cloud environment, focusing on deploying a cloud-based operating system for security and testing purposes.

Updating Ubuntu Cloud Edition
Learners update and manage an Ubuntu Cloud Edition system, focusing on maintaining a secure and up-to-date cloud operating system.

Configuring SSH Keys on a Cloud OS
This lab focuses on configuring SSH key-based authentication within a cloud operating system to enable secure remote access.

Configuring TCP/IP in Your Cloud Environment
Learners configure TCP/IP settings in a cloud environment, focusing on network addressing, connectivity, and basic cloud networking concepts.

Adding Services to a Cloud Operating System
This lab explores installing and managing additional services on a cloud-based operating system.

Using Hashing Functions on Your Cloud OS
Learners use hashing functions within a cloud operating system to verify data integrity and understand basic cryptographic operations.

Configuring an IoT Cloud Device
This lab focuses on configuring an Internet of Things (IoT) device within a cloud environment.

Viewing the Logs of a Cloud System
Learners examine system logs within a cloud environment to understand logging, monitoring, and basic troubleshooting.

Pentesting a Cloud Operating System
This lab introduces penetration testing techniques applied to a cloud-based operating system.

Implementing a Secure Cloud OS
Learners implement security controls and hardening techniques on a cloud operating system.

AWS Fundamentals

5 Labs

Designed to build basic AWS platform familiarity through guided practice, these labs introduce AWS concepts, the management console, core networking components, storage/database basics, and virtual machine concepts—making them ideal for first-time AWS learners.

Cloud Networking Concepts
Cloud networking concepts are explored within a cloud environment, focusing on virtualized networking resources, connectivity, and how cloud networking differs from traditional on-premises architectures in terms of scalability and cost efficiency.

AWS Management Console
The AWS Management Console is used to explore and manage cloud services, including commonly used offerings such as Amazon EC2, Amazon RDS, and Amazon S3, while navigating the AWS cloud platform.

AWS Virtual Networking Components
AWS virtual networking components are examined through the AWS Management Console, including networking and content delivery services used to build and manage cloud-based network architectures.

AWS Database and Storage Concepts
AWS database and storage services are explored, covering core offerings such as Amazon S3, EBS, Glacier, EFS, Storage Gateway, RDS, DynamoDB, and Redshift.

AWS Virtual Machine Concepts
Virtual machine concepts in AWS are examined within an Infrastructure as a Service (IaaS) model, focusing on how cloud service providers manage physical infrastructure while enabling users to deploy and manage virtual devices.

MS Azure Concepts (Storage, Management, Security)

10 Labs

Designed to build practical Azure administration skills through guided practice, these labs progress from management and monitoring tools to storage services, databases, Key Vault, and network security—making them ideal for Azure operations and fundamentals-plus pathways.

Network Management Tools
Work with network management tools to interpret JSON-encoded data and automate configuration tasks using Ansible. Explore how automation supports consistent, repeatable network operations in cloud and hybrid environments.

Analyzing Output from Network Security Monitoring Tools
Analyze security monitoring data to identify indicators of compromise and assess system activity. Apply basic digital forensics techniques to investigate events and support security incident analysis.

MS Azure Concepts (Storage, Management, Security)

The Azure Marketplace
Explore the Azure Marketplace to identify certified solutions optimized for Azure environments. Review offerings ranging from web applications to AI and machine learning services, including free and paid solutions.

Azure Storage Services
Create and manage Azure storage accounts, file shares, and uploaded data. Examine how Azure storage services support scalability, availability, and enterprise data needs.

Working with Blobs
Configure Azure Blob Storage by creating storage accounts, containers, and uploading files. Explore how blob storage supports unstructured data storage for applications and services.

Azure SQL Databases
Provision Azure SQL databases and database servers. Examine how managed database services support both proprietary and open-source engines for modern application development.

Azure Cosmos Databases
Create and configure Azure Cosmos DB. Explore how this fully managed NoSQL database supports globally distributed, high-performance application workloads.

Using Azure Key Vault
Enable and configure Azure Key Vault to manage cryptographic keys, secrets, and certificates. Explore how hardware security modules (HSMs) and centralized key management enhance cloud security.

Admin Tools
Explore administrative and security tools available in the Azure portal and Azure Windows Admin Center. Examine built-in security assessment tools used to manage and secure Azure environments.

Network Security – Firewalls
Configure and examine firewall rules and network traffic filtering. Explore how firewalls and NAT support secure network design and protect infrastructure from unauthorized access.

Servers

CompTIA Server+ (SK0-005)

18 Labs

Designed to build Server+ (SK0-005) aligned server administration skills through guided practice, these labs progress from OS installation and infrastructure configuration to storage, backup, virtualization, hardening, physical security, licensing, and troubleshooting—making them ideal for server operations and certification pathways.

Server Operating Systems Installation Methods
Perform a local installation of Windows Server 2022 while exploring deployment options, initial configuration, and key considerations for enterprise server environments.

Server Network Infrastructure Configuration
Configure server networking to support applications and business needs, including firewall rules, port management, and security-related connectivity settings.

Installing and Configuring Server Roles and Features
Install and configure server roles and features that support client/server environments and deliver essential network services.

Server Identity and Access Management
Implement identity and access controls by configuring policies that manage permissions, auditing, and secure access to network resources.

Deploying and Managing Server Storage
Configure and manage server storage across Windows and Linux systems, including local and shared storage solutions.

Implementing a Backup and Restore Solution
Implement backup solutions and perform system restores to support data protection and business continuity.

Automation of Server Administration using Scripts
Automate administrative tasks using scripts on Windows and Linux systems to reduce manual effort and improve efficiency.

Server Virtualization Concepts
Install Hyper-V, configure virtual networking, and create virtual machines to deploy Windows Server and support cloud computing models.

Configuring Server High Availability
Improve availability by configuring network load balancing, NIC teaming, and redundant networking to minimize downtime.

Server and Application Hardening Techniques
Strengthen security by hardening services, applying updates, configuring firewalls, and securing hosts and applications.

Server Hardware Components
Examine server hardware components, including CPUs, memory, storage, networking, power, and rack-based infrastructure.

MS Azure Concepts (Storage, Management, Security)

Securing a Physical Server Infrastructure
Apply physical security controls such as access restrictions, surveillance, and environmental safeguards to protect server facilities.

Server Hardware Maintenance
Maintain server hardware using local and remote tools, manage firmware updates, and support hot-swappable components.

Server Licensing Concepts
Review common server licensing models, including physical and virtual licensing, subscriptions, and compatibility considerations.

Data Security Concepts
Protect data using secure boot controls, encryption, and effective storage practices while evaluating business risk.

Troubleshooting Server Storage–Related Issues
Diagnose and resolve storage issues using built-in tools to address disk errors, performance problems, and access failures.

Server Operating Systems Troubleshooting Techniques
Resolve OS issues by managing services, firewall rules, permissions, and recovery tools to restore system stability.

Troubleshooting Network Connectivity Issues
Troubleshoot network issues by configuring adapters, IPv4/IPv6 settings, DHCP services, and using command-line tools on Windows and Linux.

Introduction to Windows Server 2019 Administration

21 Labs

Designed to build practical Windows Server 2019 administration skills through guided practice, these labs progress from installation and domain setup to storage, backup, file services, centralized logging, virtualization management, WSUS, and core Active Directory and Group Policy tasks—making them ideal for Windows server administration pathways.

Installing Windows Server 2019
Install Windows Server 2019, perform initial configuration, and manage server roles and features to prepare the system for enterprise use.

Installing Server Core
Install and configure Windows Server Core. Compare Server Core and Desktop Experience installations and manage the server using command-line and remote tools.

Configuring Server Domain Infrastructure
Configure domain infrastructure components, including DNS forwarders, to support Active Directory environments and internal name resolution.

Working with Microsoft Assessment and Planning (MAP) Toolkit
Collect and analyze operating system and infrastructure data using the Microsoft Assessment and Planning Toolkit to support deployment and migration planning.

Introduction to Windows Server 2019 Administration

Managing Local Storage and Virtual Hard Disks
Configure local storage and manage virtual hard disks to support server workloads and data requirements.

Backup and Restore with Server 2019
Configure Windows Server Backup, protect system state data, and perform authoritative restore operations.

Configuring SMB and NFS File Shares
Set up and manage SMB and NFS file shares to support file access across Windows and mixed operating system environments.

Implementing Centralized Event Logs
Configure centralized event logging by adding event collector systems, creating subscriptions, and managing log collection.

Managing Virtual Machine Networks
Configure Hyper-V virtual switches, implement network isolation, and optimize network performance for virtual machines.

Managing Virtual Machine Settings
Configure virtual machine settings including Dynamic Memory, Smart Paging, Guest Integration Services, and Generation 2 virtual machines.

Managing Virtual Machine Storage
Create and manage VHD and VHDX files, modify virtual disks, and support virtual machine storage requirements.

Managing Server Performance
Monitor and analyze server performance using Performance Monitor to identify resource usage and performance issues.

Implementing Windows Server Update Services
Install and configure WSUS, create computer groups, and manage centralized update deployment.

Manage Group Policy Objects – Part One
Prepare a central Group Policy store, import Group Policy Objects, and delegate Group Policy management.

Manage Group Policy Objects – Part Two
Configure and manage Group Policy settings to enforce system and user configuration requirements.

Manage Group Policy Objects – Part Three
Implement Group Policy Preferences and deploy software using Group Policy.

Deploy and Manage Domain Controllers
Install Active Directory Domain Services on Server Core and deploy domain controllers to support directory services.

Manage Active Directory Accounts – Part One
Configure delegated administration to control user and administrative access within Active Directory.

Manage Active Directory Accounts – Part Two
Create and manage Active Directory user accounts to support organizational access requirements.

Administer Active Directory Groups and OUs
Prepare environments for group nesting, implement group nesting strategies, and manage group membership restrictions.

Maintain Active Directory
Back up and restore Active Directory using Windows Server Backup to support directory service recovery and continuity.

Linux Fundamentals

10 Labs

Designed to build core Linux administration skills through guided practice, these labs progress from installation and shell basics to file management, users, storage, services, software installation, and patching—making them ideal for introductory Linux and IT operations pathways.

Introduction to Linux
Explore what Linux is, navigate the file system, and identify common applications used in Linux environments.

Different Linux Flavors
Compare major Linux distributions by exploring Ubuntu and CentOS and understanding where each is commonly used.

Installation of Linux OS
Create a virtual machine and install the CentOS operating system to establish a working Linux environment.

Introduction to Bash
Navigate the Linux command line and execute basic Bash commands used for system interaction and administration.

Administering Files in Linux
Create, edit, and delete files while managing file content using standard Linux tools and commands.

User Creation and Management
Create and manage user accounts, assign permissions, and control access within a Linux system.

Managing Storage in Linux
Create and manage disk partitions, mount and unmount storage, identify file system formats, and remove partitions.

Application Installation in Linux
Install and remove applications using both command-line and graphical tools, and manage application status across CentOS and Ubuntu.

Service Management in Linux
Start, stop, and restart services in Ubuntu and CentOS to control system processes and background services.

Managing Software Updates and Patches
Check kernel versions, apply system updates, and manage repositories to keep Linux systems secure and up to date.

Linux Server I: Linux Fundamentals

16 Labs

Designed to build server-focused Linux skills through guided practice, these labs progress through installation, package management, partitions, quotas, boot processes, Bash fundamentals, process monitoring, and file/text management—making them ideal for Linux server foundations pathways.

CentOS Server Linux Installation
Install CentOS Server and configure the base operating system for use in a server environment.

Ubuntu Desktop Linux Installation 12.04
Install Ubuntu Desktop and configure core operating system components used in Linux workstations and servers.

Installing Packages and Shared Libraries on CentOS and Ubuntu
Install, update, and manage software packages and shared libraries across CentOS and Ubuntu systems.

Displaying Hardware
Identify and display system hardware details using Linux utilities to assess system configuration and resources.

Adding a New Partition
Create and configure disk partitions to expand storage capacity on a Linux system.

Managing Filesystem Quotas
Configure and manage filesystem quotas to control disk usage for users and groups.

Using the BASH Shell – 1
Execute essential Bash commands and navigate the Linux shell for system interaction and administration.

Booting and Restarting the System
Control system startup, shutdown, and reboot processes using Linux commands and configuration tools.

Using the BASH Shell – 2
Use advanced Bash features and scripting techniques to automate common administrative tasks.

Using the BASH Shell – 3
Apply Bash commands and shell techniques to support system security tasks and controls.

Using the BASH Shell – 4
Combine Bash commands and scripting concepts to support ongoing system operations and maintenance.

Monitoring Processes
Monitor, manage, and troubleshoot running processes using Linux system utilities.

Working with Files
Create, copy, move, and manage files and directories using Linux command-line tools.

Managing Text Files – 1
View and edit text files using standard Linux text-processing commands.

Managing Text Files – 2
Search, filter, and manipulate text file content using stream and text-processing utilities.

Managing Text Files – 3
Combine multiple text-processing tools to analyze and modify system files efficiently.

Linux Server II: System Administration

17 Labs

Designed to build intermediate Linux system administration skills through guided practice, these labs progress through user/group management, scheduling, localization, email basics, networking, security administration, encryption, Bash features and scripting, and database interaction—making them ideal for Linux admin and operations pathways.

Configuring X Windows in CentOS and Fedora Desktop
Configure and manage the X Window System on CentOS and Fedora desktop environments.

Accessibility Technologies
Enable and configure accessibility features to support diverse user needs in Linux environments.

User and Group Accounts
Create, modify, and manage user and group accounts to enforce access control and security policies.

System Administration Tasks – 1
Perform core system administration tasks related to hardware and system configuration.

System Administration Tasks – 2
Apply security-focused administrative tasks to protect system resources and configurations.

System Administration Tasks – 3
Execute operational and maintenance tasks to support stable and reliable Linux systems.

crontab and at
Schedule and manage automated tasks using cron, crontab, and at.

Configuring Locale and Time Zone Settings
Configure system locale, language, and time zone settings to ensure accurate regional and time-based operations.

Working with Email – 1
Configure and manage basic email services on a Linux system.

Working with Email – 2
Extend email configuration and administration to support messaging operations and troubleshooting.

Basic Network Configuration
Configure network interfaces, IP addressing, and connectivity on Linux systems.

Basic Security Administration
Implement access control, authentication, and authorization mechanisms to secure Linux systems.

Securing Data with Encryption on a Linux System
Encrypt data at rest and in transit using Linux encryption tools and security utilities.

Host Security
Harden Linux hosts by configuring security controls and mitigating common threats.

BASH Shell Features
Use advanced Bash shell features to streamline administration and system operations.

BASH Scripting
Create and execute Bash scripts to automate administrative and operational tasks.

Working with a SQL Database
Install, configure, and interact with a SQL database within a Linux environment.

CompTIA Linux+ (XK0-005)

24 Labs

Designed to build Linux+ (XK0-005) aligned skills through guided practice, these labs progress from core file and access management to processes, services, storage (including LVM), scripting, containers, Git, networking, and Linux security controls—making them ideal for Linux+ preparation and sysadmin pathways.

Introduction to Linux
Work with core Linux concepts, system architecture, and command-line navigation used across enterprise servers, cloud environments, and embedded systems.

File and Directory Management in Linux
Navigate the Linux file system, create and manage files and directories, and use links to organize and control data efficiently.

Editing Files in Linux
Edit and maintain configuration and text files using Vi/Vim and Nano, supporting system configuration and troubleshooting tasks.

Access Control Utilities
Apply standard and advanced permissions to secure files and directories while enforcing proper access controls.

Linux Backup and File Compression Concepts
Create file-level and disk-level backups using tar and dd, and compress data to support recovery and storage efficiency.

Package Management and Updating Linux Devices
Install, update, and manage software packages using dnf and apt to keep systems stable and secure.

Linux Identity Management
Create and manage users and groups to support authentication, authorization, and role-based access.

Elevated User Privilege Management
Configure and manage elevated privileges, authentication settings, and secure administrative access.

Remote Connectivity Management
Install, configure, and harden SSH servers and clients to enable secure remote administration.

Managing Processes in Linux
Monitor system processes, identify runaway tasks, and take corrective action to maintain system performance.

Managing & Configuring Linux System Services
Control system services, manage locales, and interact with kernel components to support stable operations.

Storage Management Concepts
Partition disks, create filesystems, and mount storage to support system and application requirements.

Logical Volume Manager Commands
Configure flexible storage using LVM, including volume creation, formatting, mounting, and removal.

Managing Linux Shared Storage
Build and manage RAID arrays, create filesystems, and configure persistent shared storage.

Linux Scripting Techniques
Develop shell scripts to automate routine administrative tasks and streamline system operations.

Container Creation & Management
Run and automate containers in Linux environments to support modern application deployment.

CompTIA Linux+ (XK0-005)

Version Control using Git
Create repositories and manage source code changes using Git for version control and collaboration.

Configuring Networking in Linux
Configure network adapters and connectivity on AlmaLinux and Ubuntu systems to support enterprise networking.

Name Resolution Concepts & Tools
Configure DNS and name resolution services to ensure reliable system communication.

Remote Access Tools
Implement secure remote access solutions for administering Linux systems.

Securing Linux Devices
Harden Linux systems by applying security controls, configurations, and best practices.

Configuring Linux Firewalls
Configure firewall services and rules to control network traffic and reduce attack surface.

Certificate Configuration & Management
Implement certificate-based authentication and manage SSH keys and certificates securely.

Authentication Methods
Configure multi-factor authentication and integrate Linux systems with Microsoft Active Directory.

Windows Server Administration Fundamentals

35 Labs

Designed to build broad Windows Server administration skills through guided practice, these labs progress from installation options and network deployment to AD/GPO administration, storage and security configuration, logging/auditing, backup/restore, and core server roles and services—making them ideal for Windows server fundamentals pathways.

Install and Configure Nano Server
Create and deploy a Nano Server image, configure networking and Active Directory integration, manage the server remotely, and deploy a basic IIS web page.

Install and Configure Server Core
Create and configure a Windows Server Core environment by deploying a virtual machine, installing Windows Server 2016 Standard, assigning static network settings, joining Active Directory, enabling WinRM for remote management, and installing DNS with a secondary zone.

Configure Network Installation of Windows
Prepare and configure Windows Deployment Services (WDS) to deploy Windows 10 over the network, verify successful remote installations, and troubleshoot deployment prerequisites.

Manage Windows Services
Configure and manage Windows services, adjust service properties, assign service accounts, and manage IIS-related services to support enterprise workloads.

Working with Mail Servers
Create mailbox-enabled user accounts, test internal email delivery, and manage junk email to control unsolicited messages from unknown senders.

Windows Server Administration Fundamentals

Configure Remote Assistance and Remote Server Admin Tools
Enable and configure Remote Assistance on Windows Server and Windows 10, install Remote Server Administration Tools (RSAT), and manage servers remotely.

Manage Remote Access with VPN
Configure VPN-based remote access to securely connect users to internal network resources.

Configure Application Virtualization
Package and publish applications using Microsoft App-V, manage App-V server components, and verify application streaming to Windows clients.

Manage Active Directory Infrastructure – Part 1
Deploy additional domain controllers, create a new Active Directory forest, configure forest trust relationships, and verify inter-domain trust functionality.

Manage Active Directory Infrastructure – Part 2
Create and manage Active Directory sites, associate subnets, and schedule replication between sites within the same domain.

Manage Active Directory Infrastructure – Part 3
Install additional domain controllers and transfer Flexible Single Master Operations (FSMO) roles to maintain directory health and availability.

Manage Virtual Hard Disks with Hyper-V
Manage virtual hard disks for Hyper-V guest machines, configure checkpoints, and maintain virtual machine storage configurations.

Enable Nested Virtualization
Use Windows PowerShell to enable nested virtualization, allowing virtual machines to host additional virtual workloads.

Manage Shared Storage Using iSCSI
Configure shared storage using iSCSI to support centralized and scalable server storage solutions.

Manage Updates with Windows Server Update Services
Install and configure WSUS, synchronize updates, organize computer groups, and manage update deployment across the network.

Configure Group Policy Settings
Create and manage local, site, domain, and organizational unit Group Policy Objects, verify policy application, and configure firewall rules for WMI.

Configure Disk Types
Create and manage basic, dynamic, primary, extended, and logical disks to support flexible storage requirements.

Configure Distributed File System
Install and configure Distributed File System (DFS) to organize shared folders across multiple servers.

Manage Disk Redundancy
Configure software RAID using RAID 0, RAID 1, and RAID 5 to improve data availability and fault tolerance.

Manage File System Security
Configure shared folders, assign NTFS permissions, evaluate effective permissions, map network drives, and secure file access.

Manage Windows Event Logs
Configure and manage Windows Event Logs to support monitoring, troubleshooting, and system auditing.

Configure Audit Policies
Enable and manage audit policies, locate audit data, and secure audit logs to support compliance and forensic investigations.

Windows Server Administration Fundamentals

Administer Organizational Units and Containers
Delegate administrative control over Active Directory objects and verify delegated permissions.

Administer User and Group Accounts
Create and manage Active Directory users and groups using PowerShell, configure home folders, templates, and perform bulk account operations.

Implement Group Nesting
Design and implement group nesting strategies using AGDLP and AGUDLP models across parent and child domains.

Backup and Restore Active Directory
Install Windows Server Backup, perform system state backups, and restore Active Directory data, including authoritative restores to recover critical directory services.

Install and Configure a Database Server
Install SQL Server Express, configure basic security, create service accounts, manage logins and roles, and attach databases using SQL Server Management Studio.

Install and Configure a Failover Cluster
Prepare servers for failover clustering, configure shared storage with iSCSI, install the Failover Clustering feature and File Server role, and validate high availability by testing clustered file share failover.

Configure User Profiles
Manage local and roaming user profiles to support consistent user environments and centralized profile management.

Implement Performance Monitor
Collect and analyze performance metrics using Performance Monitor, Data Collector Sets, and Resource Monitor.

Install and Configure Web Services
Install and configure IIS and FTP using PowerShell, deploy web services, and configure certificates for secure access.

Install and Configure Threat Management Software
Install and configure Threat Management Gateway (TMG) to control network traffic and enhance perimeter security.

Manage Remote Desktop Services
Install and configure Remote Desktop Services, RD Gateway, and session-based desktops for centralized access.

Working with Collaboration Software
Configure and manage calendar sharing and public folders in an Exchange Server 2016 environment.

Implement Folder Redirection
Configure Group Policy to redirect user folders to network shares, centralizing data storage and improving backup and recovery.

Windows Server 2019: Administration Concepts

13 Labs

Designed to build Windows Server 2019 administration concepts through guided practice, these labs cover installation, domain configuration, storage/VHD management, backup/restore, file sharing, centralized event logs, virtualization basics, performance monitoring, and WSUS—making them ideal for introductory server administration pathways.

Installing Windows Server 2019
Install Windows Server 2019, configure core system settings, and manage server roles and features to establish a stable foundation for enterprise server environments.

Installing Server Core
Deploy Windows Server 2019 Server Core, manage configuration tasks using PowerShell, and operate a minimal-attack-surface server optimized for performance and security.

Configuring Server Domain Infrastructure
Install and configure DNS forwarders to support name resolution across domains and networks, enabling reliable directory and application services.

Working with Microsoft Assessment and Planning (MAP) Toolkit
Collect and analyze operating system and infrastructure data using the MAP Toolkit to support capacity planning, migration, and upgrade decisions.

Managing Local Storage and Virtual Hard Disks
Configure local storage and virtual hard disks to support flexible, scalable storage solutions for physical and virtualized workloads.

Backup and Restore with Server 2019
Prepare Windows Server Backup, perform system state backups, and execute authoritative restores to recover critical directory and server data.

Configuring SMB and NFS File Shares
Set up and manage SMB and NFS file share infrastructure to provide secure, cross-platform access to shared resources.

Implementing Centralized Event Logs
Configure centralized event log collection by deploying an event collector, creating subscriptions, and enabling centralized monitoring and troubleshooting.

Managing Virtual Machine Networks
Configure Hyper-V virtual switches, implement network isolation, and optimize virtual machine network performance.

Managing Virtual Machine Settings
Configure virtual machine memory settings, enable smart paging, manage guest integration services, and deploy Generation 2 virtual machines.

Managing Virtual Machine Storage
Create and manage VHD and VHDX files, modify virtual disk configurations, and support scalable virtual storage environments.

Managing Server Performance
Monitor and analyze system performance using Performance Monitor tools to identify bottlenecks and maintain server reliability.

Implementing Windows Server Update Services
Install and configure WSUS, organize computer groups, and manage update deployment to maintain patch compliance across the environment.

MS Endpoint Administrator

12 Labs

Designed to build Microsoft endpoint administration skills through guided practice, these labs progress from setting up Microsoft 365 and Autopilot to Intune-based identity, compliance, configuration, monitoring, updates, endpoint protection, and app deployment—making them ideal for modern workplace and endpoint management pathways.

Create and Configure a Microsoft 365 Account
Create and configure a Microsoft 365 tenant using Microsoft Entra ID and Intune trial subscriptions, establishing the identity and management foundation required for endpoint administration.

Deploy a Windows Client Using Autopilot
Configure a Microsoft 365 tenant for Windows Autopilot, register devices, and deploy Windows clients using zero-touch provisioning for streamlined enterprise onboarding.

Configure Remote Management
Enable and configure Windows Admin Center and Intune Remote Help to support secure remote administration, troubleshooting, and end-user assistance.

Manage Identities
Register devices in Microsoft Entra ID and manage identity integration to support secure access, device trust, and conditional access enforcement.

Implement Intune Compliance Policies
Create, deploy, and validate Intune compliance policies to enforce security baselines and ensure devices meet organizational requirements.

Manage Device Lifecycle Using Intune
Configure Windows enrollment settings and manage device onboarding, lifecycle states, and retirement using Microsoft Intune.

Manage Device Configuration Using Intune
Deploy configuration profiles and manage Windows device settings through Intune to enforce standards and maintain consistent endpoint configurations.

Monitoring Devices Using Intune
Monitor Entra-joined devices using Intune reporting and device insights to track compliance, health, and operational status.

Managing Device Updates Using Intune
Create and deploy Windows Update policies through Intune to control update rings, feature updates, and patch compliance across endpoints.

Implement Endpoint Protection for Devices
Configure and deploy endpoint protection policies to secure Windows devices against malware, threats, and unauthorized access.

Deploy and Update Apps for Devices
Deploy, manage, and update applications using Intune app management to ensure devices remain functional and secure.

Implement App Protection and Configuration Policies
Create and deploy app protection and app configuration policies to secure corporate data on managed and unmanaged devices while supporting modern authentication requirements.

Information Management and Data

Microsoft Excel 2019

30 Labs

Designed to build practical Excel skills through guided practice, these labs progress from workbook navigation and formatting to importing and manipulating data, formulas and functions, tables, charts, inspection, and print/output configuration—making them ideal for productivity, business, and data literacy pathways.

Worksheet and Workbook Navigation
Create and manage workbooks, move efficiently between cells and ranges, use Go To navigation, and work with named ranges to move quickly through large worksheets.

Formatting Worksheets and Workbooks
Adjust row heights and column widths, configure page setup options, and customize headers and footers to prepare worksheets for professional presentation and printing.

Customizing the Quick Access Toolbar
Add, remove, and organize commands on the Quick Access Toolbar, then export toolbar customizations for reuse across systems.

Importing Data from Text Files and CSV Files
Create and import tab-delimited and CSV files into Excel, ensuring external data is properly structured and usable within worksheets.

Manipulating Data in Worksheets—Part 1
Paste data using Paste Special options, use AutoFill to populate series, and apply foundational data manipulation techniques to improve efficiency.

Manipulating Data in Worksheets—Part 2
Insert and delete cells, rows, and columns to restructure worksheets and maintain clean, organized datasets.

Searching Data within a Workbook
Locate and replace data using Find and Replace tools to quickly update, audit, and correct workbook content.

Working with Hyperlinks
Insert, modify, and remove hyperlinks to connect worksheets, workbooks, files, and web resources.

Working with Window Views
Freeze rows and columns, compare worksheets side by side, and work with multiple workbooks simultaneously for improved analysis and productivity.

Filtering Records
Apply AutoFilter and advanced filtering criteria to isolate specific records within tables and datasets.

Sorting Table Data
Sort data using single- and multi-column criteria to organize information logically and support analysis.

Working with References
Create formulas using relative and absolute references to perform accurate calculations across worksheets.

Using Mathematical Functions
Apply built-in mathematical functions such as SUM, AVERAGE, MIN, and MAX to analyze numerical data efficiently.

Microsoft Excel 2019

Using COUNT Functions
Use COUNT, COUNTA, and COUNTBLANK functions to evaluate data completeness and structure.

Using IF() Function
Build logical formulas using IF, nested IF, and SUMIF functions to support conditional calculations and decision-making.

Working with Text Functions
Manipulate text using functions such as LEFT, RIGHT, MID, LEN, UPPER, LOWER, CONCATENATE, and TEXTJOIN.

Formatting Cells—Part 1
Adjust cell alignment, text orientation, indentation, and wrapping to improve worksheet readability.

Formatting Cells—Part 2
Apply number formats, use the Format Cells dialog box, clear formatting, and apply cell styles for consistent presentation.

Summarizing Data Visually
Apply conditional formatting rules, including color scales, icon sets, and top/bottom rules, to highlight trends and outliers.

Working with Excel Tables
Convert data ranges into Excel tables to enable structured references, filtering, and enhanced formatting.

Formatting Excel Tables
Modify table styles, manage table rows and columns, and adjust table layout options for clarity and usability.

Creating Charts
Create pie charts, line charts, and chart sheets to visualize data and communicate insights effectively.

Modifying Charts
Add data series, switch data orientation, and customize chart elements to refine visual presentations.

Working with Sparklines and Chart Layouts and Styles
Insert sparklines, apply chart layouts, and style charts to enhance data storytelling.

Adding Alternative Text to Objects
Insert SmartArt objects and apply alternative text to improve accessibility and document compliance.

Inspecting Workbooks
Inspect workbooks for errors, accessibility issues, and compatibility concerns before sharing or publishing.

Modifying Workbook Properties and Displaying Formulas
Edit workbook properties and display formulas directly within worksheets for auditing and documentation purposes.

Saving Workbooks in Alternative File Formats
Save workbooks in multiple file formats to ensure compatibility across systems and applications.

Setting a Print Area
Define print areas and print titles to control how worksheets are printed across multiple pages.

Configure Print Settings
Adjust page orientation, margins, and print options to produce clean, professional printed output.

Microsoft Word 2019

23 Labs

Designed to build practical Word skills through guided practice, these labs progress from navigation and document formatting to tables, lists, references, graphics, SmartArt, collaboration tools, and change tracking—making them ideal for workplace productivity and digital communication pathways.

Navigating within Word
Search for text within documents, move directly to specific locations and objects, and create links to internal document sections for efficient navigation.

Formatting a Word Document – Part 1
Show and hide formatting symbols and hidden text, configure page setup options, and control document layout for consistent formatting.

Formatting a Word Document – Part 2
Insert and customize headers and footers, manage page numbering, and apply layout elements that support professional document standards.

Saving Word Documents
Save documents in alternate file formats, modify document properties, and configure print settings to ensure compatibility and proper output.

Inspecting Word Documents
Locate and remove hidden properties and personal information, identify compatibility issues, and prepare documents for secure sharing.

Editing Text
Find and replace text, insert symbols and special characters, and add or modify text boxes to enhance document content and structure.

Formatting Text – Part 1
Apply formatting using the Format Painter, configure line spacing and paragraph indentation, and standardize text appearance throughout documents.

Formatting Text – Part 2
Clear existing formatting, apply built-in styles, and use text effects to improve readability and visual consistency.

Ordering and Grouping Text
Format text into multiple columns, insert page, section, and column breaks, and adjust page setup options to control document flow.

Creating Word Tables
Insert tables, convert text to tables, and resize rows and columns to organize information clearly and efficiently.

Modifying Word Tables – Part 1
Convert tables to text, sort table data, and configure cell margins and spacing to improve table readability.

Modifying Word Tables – Part 2
Configure repeating header rows, merge and split cells, and refine table structure for multi-page documents.

Managing a List with Word – Part 1
Format paragraphs as numbered and bulleted lists, define custom numbering formats, and customize bullet characters.

Managing a List with Word – Part 2
Adjust list levels, restart or continue numbering, and set custom starting values to manage complex list structures.

Creating and Managing References
Insert footnotes and endnotes, modify reference properties, and manage citations within long-form documents.

Using Content Building Blocks
Insert and edit citations using predefined source types, manage reusable content elements, and maintain consistency across documents.

Working with Table of Contents
Insert and customize a table of contents, update entries automatically, and control heading-based navigation.

Microsoft Word 2019

Creating Graphic Elements
Insert images, shapes, and 3D models to enhance visual communication within documents.

Formatting Graphic Elements
Apply picture styles, artistic effects, and visual enhancements to improve document presentation.

Using SmartArt Graphics
Insert SmartArt graphics, modify content and layout, format SmartArt elements, and capture screenshots or screen clippings.

Modifying Graphic Elements
Remove picture backgrounds, format 3D models, position objects precisely, and wrap text around visual elements.

Using the Comments Feature
Add, review, reply to, resolve, and delete comments to support collaboration and document feedback workflows.

Tracking and Reviewing Changes
Track changes, review edits, accept or reject revisions, and lock or unlock change tracking to control document editing.

Administering a SQL Database Infrastructure

21 Labs

Designed to build SQL Server administration skills through guided practice, these labs progress from encryption and permissions to backup/restore, integrity maintenance, monitoring, indexing, high availability, and disaster recovery solutions—making them ideal for database administration and infrastructure pathways.

Data Encryption
Implement data encryption using keys and column-level encryption to protect sensitive information at rest and enforce secure data handling within SQL Server environments.

Backup and Connection Encryption
Encrypt database backups and configure SSL/TLS to secure database connections, ensuring data protection during storage and transmission.

Manage Database Object Permissions
Configure and manage permissions on database objects to control access, enforce least privilege, and protect data integrity across users and roles.

Configure Security Options
Configure SQL Server security options, implement row-level security, and secure sensitive data through advanced access controls.

Configure Audits for SQL Server
Configure and manage server-level and database-level audits to track activity, support compliance requirements, and maintain visibility into database operations.

Backing Up Databases
Perform database backups using industry-standard strategies to ensure data availability and support recovery objectives.

Administering a SQL Database Infrastructure

Piecemeal Restore of Database and File Groups
Execute piecemeal restores of databases and filegroups to recover critical data while minimizing downtime.

Working with Restore Options
Manage restore options, including point-in-time recovery, to support precise and controlled database restoration scenarios.

Maintaining Database Integrity
Maintain database integrity through consistency checks and maintenance operations that ensure reliable and accurate data storage.

Monitoring the Database Activity
Monitor database activity to identify performance issues, track usage patterns, and support proactive database administration.

Configuring Database Collection and UCP
Configure data collection, the Management Data Warehouse, and Utility Control Point (UCP) to centralize monitoring and performance analysis.

Managing a Query Store
Configure and manage Query Store to capture query performance data and troubleshoot execution plan regressions.

Using Trace and Extended Events
Use SQL Trace and Extended Events to capture detailed diagnostic information for performance tuning and troubleshooting.

Managing Indexes
Create, modify, and maintain indexes to improve query performance and optimize database efficiency.

Managing Statistics
Manage database statistics to support accurate query optimization and consistent performance.

Managing Operators
Configure SQL Server operators to support automated alerts, notifications, and job monitoring.

Managing SQL Servers
Administer SQL Server instances, manage configurations, and maintain operational stability across environments.

Configuring Log Shipping
Configure log shipping using SQL Server Management Studio and Transact-SQL to support disaster recovery and high availability.

Backup to Azure
Configure database backups to Azure to extend backup strategies into hybrid and cloud-based environments.

Implementing Availability Groups
Implement Always On availability groups to provide high availability and data redundancy across SQL Server instances.

Implementing Failover Clusters
Configure failover cluster instances to support fault tolerance and ensure database availability during hardware or service failures.

Developing SQL Databases

25 Labs

Designed to build SQL development skills through guided practice, these labs progress from schema design and constraints to stored procedures, triggers, transactions, locking analysis, and performance optimization techniques—making them ideal for database development and data engineering pathways.

Designing a Relational Database Schema
Design normalized relational database schemas that support efficient data storage, enforce relationships, and enable scalable, maintainable database solutions.

Creating Columnstore Indexes
Implement columnstore indexes to improve performance for analytical queries and large data sets in modern SQL Server environments.

Best Practices in Index Creation
Apply indexing best practices to balance query performance, storage efficiency, and maintenance overhead in production databases.

Creating and Implementing Views
Create and deploy database views to simplify data access, enforce abstraction, and support consistent reporting and application queries.

Creating Indexes
Design and implement indexes to accelerate query execution and improve overall database responsiveness.

Maintaining Columnstore Indexes
Maintain columnstore indexes through monitoring and optimization to ensure sustained performance as data changes over time.

Creating Constraints
Define and enforce constraints to maintain data integrity, prevent invalid data entry, and support reliable database operations.

Effects of Constraints on DML Statements
Analyze how constraints affect INSERT, UPDATE, and DELETE operations, balancing data integrity with application behavior.

Creating Stored Procedures with Parameters
Develop parameterized stored procedures to encapsulate business logic, improve performance, and support reusable database operations.

Error Handling and Streamlining Stored Procedures
Implement structured error handling and streamline stored procedures to improve reliability, maintainability, and troubleshooting.

Creating Triggers
Create triggers to automate database actions in response to data changes and enforce business rules at the database level.

Creating User-Defined Functions
Develop scalar and table-valued user-defined functions to modularize logic and extend SQL Server functionality.

Impact of Transactions on DML Statements
Evaluate how transactions affect data modification operations, ensuring consistency and reliability during multi-step processes.

Implicit and Explicit Transactions — Creating Savepoints
Implement implicit and explicit transactions with savepoints to control rollbacks and maintain data integrity during complex operations.

Manage Isolation Levels
Configure transaction isolation levels to balance concurrency, consistency, and performance in multi-user environments.

Serializable and Snapshot Isolation
Apply serializable and snapshot isolation to manage concurrency while minimizing blocking and contention.

Developing SQL Databases

Identifying and Analyzing Locking Issues
Identify locking and blocking issues and analyze their impact on performance and concurrency.

Implementing Memory-Optimized Tables and Native Stored Procedures
Implement memory-optimized tables and natively compiled stored procedures to support high-throughput, low-latency workloads.

Optimizing Statistics
Optimize database statistics to ensure accurate query plans and consistent performance.

Optimizing Indexes
Analyze index usage, identify missing or inefficient indexes, and optimize indexing strategies using dynamic management views.

Optimizing Query Plans – Part 1
Analyze execution plans to identify i nefficiencies and improve query performance through targeted tuning.

Optimizing Query Plans – Part 2
Refine query optimization techniques to address complex performance bottlenecks and execution plan regressions.

Monitoring Performance Using SQL Trace and Extended Events
Monitor database performance using SQL Trace, Extended Events, and integrated tools to diagnose issues and support proactive tuning.

Optimizing Performance for Database Instances – Part 1
Optimize database instance performance with a focus on tempdb configuration and resource usage.

Optimizing Performance for Database Instances – Part 2
Apply advanced instance-level optimization techniques to improve scalability, stability, and throughput.

Querying Data with Transact-SQL

16 Labs

Designed to build T-SQL querying skills through guided practice, these labs progress from SELECT basics to joins, aggregations, subqueries, table expressions, pivoting, temporal/non-relational data, and error handling—making them ideal for data analysis and SQL fundamentals pathways.

Working with SELECT Queries
Construct flexible and efficient SELECT queries by filtering data with predicates, returning distinct results, sorting output, limiting result sets, and querying across multiple tables using aliases and row-limiting techniques.

Working with SET Operators
Combine and compare result sets using SET operators to merge, intersect, or differentiate data returned from multiple queries.

Using Joins
Retrieve related data from multiple tables using inner, outer, and cross joins to support accurate reporting and relational analysis.

Implementing Functions
Apply scalar and table-valued functions to transform data, encapsulate logic, and simplify complex query expressions.

Working with Aggregate Data
Summarize and analyze data using aggregate functions to calculate totals, averages, counts, and other metrics critical for business insights.

Querying Data with Transact-SQL

Working with Built-In Functions
Use built-in conversion, logical, and system functions to manipulate values, enforce data consistency, and support advanced query logic.

Modifying Data
Insert, update, and delete records safely and efficiently while maintaining data integrity in transactional environments.

Working with Subqueries
Build nested queries using correlated and non-correlated subqueries to solve complex data retrieval challenges.

Working with APPLY Operators
Leverage APPLY operators to evaluate table-valued expressions per row, enabling more dynamic and flexible query designs.

Working with Table Expressions
Use derived tables and Common Table Expressions (CTEs) to structure complex queries for improved readability and maintainability.

Grouping with Pivoting Data
Group and pivot data to transform row-based results into summarized, column-based formats suitable for analysis and reporting.

Working with Temporal Tables
Query system-versioned temporal tables to analyze historical data changes and track point-in-time records.

Working with Non-Relational Data
Query and manipulate non-relational and semi-structured data within SQL Server to support modern application workloads.

Working with Stored Procedures and Views
Create and query stored procedures and views to encapsulate logic, enforce security, and simplify data access.

Implementing Error Handling
Implement structured error handling using TRY...CATCH, THROW, and RAISERROR to build resilient and maintainable SQL solutions.

Working with Data Types and Null Values
Manage data types and NULL values effectively to ensure accurate calculations, comparisons, and query results.

Oracle Database 12c – Installation and Administration

18 Labs

Designed to build Oracle 12c administration skills through guided practice, these labs progress from instance and network configuration to storage, security, auditing, performance, backup/recovery, scheduling automation, upgrades, and data migration—making them ideal for Oracle DBA and enterprise database pathways.

Oracle Database Instances
Manage Oracle database instances by configuring initialization parameters, controlling startup and shutdown operations, reviewing alert logs, and monitoring system activity through dynamic performance views.

Configuring an Oracle Network Environment
Configure and manage Oracle networking components, including listeners and client-side connectivity, to enable secure and reliable communication between databases and applications.

Oracle Database 12c – Installation and Administration

Managing Database Storage Structures
Design and manage database storage using tablespaces and datafiles while implementing effective space allocation and growth strategies.

Administering User Security
Control database access by creating users, roles, and profiles, and granting or revoking privileges to enforce security and least-privilege principles.

Managing Space
Monitor database space usage and implement proactive space management techniques to maintain availability and performance.

Managing Data Concurrency and Undo
Configure undo management, monitor locking behavior, and resolve concurrency conflicts to support reliable multi-user database operations.

Implementing Oracle Database Auditing
Audit database activity using standard, fine-grained, and unified auditing to track usage, support compliance requirements, and investigate security events.

Using Backup and Recovery Concepts
Design and configure backup strategies using RMAN, control files, redo logs, archived logs, and the fast recovery area to protect critical data.

Performing Database Recovery
Execute recovery procedures for user errors and system failures, including control files, redo logs, and critical datafiles, to restore database operations quickly.

Moving Data
Transfer data between databases using Oracle Data Pump and SQL*Loader to support migrations, integrations, and environment refreshes.

Managing Database Performance
Monitor and analyze performance metrics to identify bottlenecks and optimize database responsiveness and throughput.

Managing Resources Using Database Resource Manager
Control CPU, memory, and workload prioritization using Database Resource Manager to ensure fair and predictable resource usage.

Automating Tasks Using Oracle Scheduler
Automate recurring administrative tasks and maintenance jobs using Oracle Scheduler to improve consistency and operational efficiency.

Installing Oracle Grid Infrastructure and Using Oracle Restart
Install and configure Oracle Grid Infrastructure and Oracle Restart to improve availability and simplify database recovery after failures.

Installing Oracle 12c
Install Oracle Database 12c software and create a functional database environment aligned with enterprise deployment standards.

Creating an Oracle Database Using DBCA
Create and configure Oracle databases using Database Configuration Assistant (DBCA) to streamline deployment and enforce best practices.

Upgrading to Oracle 12c
Prepare for and execute database upgrades using supported upgrade and migration methods, including manual upgrade processes.

Migrating Data Using Oracle Data Pump
Perform structured data migrations using Oracle Data Pump to move schemas and databases efficiently between environments.

Oracle Database 12c – SQL Fundamentals

10 Labs

Designed to build Oracle SQL fundamentals through guided practice, these labs progress from querying and sorting data to functions, joins, subqueries, DML, and introductory DDL—making them ideal for introductory SQL and Oracle database pathways.

Features of Oracle Database 12c
Explore the core architecture and feature set of Oracle Database 12c, including enhancements that support performance, scalability, and enterprise database operations.

Retrieving Data Using SQL Statements
Retrieve data using SQL SELECT statements by querying tables, selecting specific columns, and structuring basic queries to extract meaningful information from an Oracle database.

Restricting and Sorting Data
Filter query results using WHERE clauses, limit returned rows, and sort output with ORDER BY to control how data is presented and analyzed.

Using Single-Row Functions to Customize Output
Apply single-row functions to manipulate character, numeric, and date values within SELECT statements to format and transform query output.

Conversion Functions and Conditional Expressions
Convert data types using built-in conversion functions and implement conditional logic with expressions such as CASE to dynamically shape query results.

Reporting Aggregated Data Using Group Functions
Summarize and analyze data using aggregate functions, GROUP BY, and HAVING clauses to produce meaningful reports from large datasets.

Displaying Data from Multiple Tables Using JOIN
Combine data across related tables using SQL JOIN operations to construct comprehensive result sets from normalized database structures.

Using Subqueries
Write and troubleshoot subqueries, including single-row and multi-row subqueries, and combine result sets using SET operators to support advanced query logic.

Managing Tables Using DML Statements
Modify database data using INSERT, UPDATE, DELETE, and TRUNCATE statements while managing transactions to maintain data integrity.

Introduction to DDL Language
Define and manage database structures using DDL statements by creating tables, assigning data types, implementing constraints, and working with schema objects.

Hadoop Administration

6 Labs

Install and configure Hadoop 1.2.1, working directly with core components such as HDFS and MapReduce. Perform administrative tasks that demonstrate how data is stored, processed, and managed within a standalone Hadoop environment.

Hadoop 1.2.1

Install and configure Hadoop 1.2.1, working directly with core components such as HDFS and MapReduce. Perform administrative tasks that demonstrate how data is stored, processed, and managed within a standalone Hadoop environment.

MapReduce (WordCount with Hadoop)

Set up Eclipse to work with Hadoop and create a Java WordCount program. Run the MapReduce job on a Hadoop cluster to clean, analyze, and aggregate data using key-value pairs.

Hadoop 1.2.1 Cluster

Deploy and administer a Hadoop 1.2.1 cluster, configuring multiple nodes and validating inter-node communication. Manage distributed storage and processing while observing how cluster-based execution improves scalability and fault tolerance.

NameNode Failover

Explore the limitations of Hadoop 1 architecture and the mechanisms used to address NameNode failures. Gain practical insight into high-availability concepts that improve fault tolerance and prepare for real-world Hadoop troubleshooting.

Hadoop 2.7.3

Configure Hadoop 2.7.3 and explore the architectural changes introduced with YARN. Manage resource allocation, job execution, and core services to support modern Hadoop workloads in a single-node environment.

Hadoop 2.7.3 Cluster

Build and manage a Hadoop 2.7.3 cluster using YARN-based resource management. Configure cluster nodes, monitor job execution, and validate high-availability and scalability concepts used in enterprise big data environments.