masterskill
education through innovation

aci LEARNING | SKILL LABS

30 Bird–CompTIA A+ Core 2 (Exam 220-1202), Skill Labs

Course Specifications

Course Number: ACI76-011SL_rev1.0
Lab Length: Approximately 34 hours

Simulations

1. 30 Bird - Configuring a Wi-Fi Network Connection (Ch 3, Mod B)
2. 30 Bird - Setting up 2FA (Ch 6, Mod A)
3. 30 Bird - Troubleshooting Network Connectivity (Ch 6, Mod C)
4. 30 Bird - Configuring a Wi-Fi Network Router (Ch 6, Mod C)

Labs

30 Bird - Operating System Types, Filesystems, and Lifecycle Compatibility (Ch 1, Mod A)

Introduction

Objective

By completing this lab, you will be able to:

Operating System Fundamentals

- Differentiate between major operating system (OS) platforms.
- Understand kernel architectures and system structures.
- Identify appropriate OS choices for specific use cases.
- Compare licensing models across different platforms.

Filesystem Technologies

- Compare filesystem features and limitations.
- Understand file allocation and storage methods.
- Identify compatibility considerations between filesystems.
- Implement appropriate filesystem choices for various scenarios.

Lifecycle Management

- Understand OS support lifecycles and end-of-life (EOL) implications.
- Plan upgrade and migration strategies.
- Ensure hardware and software compatibility.
- Manage legacy system requirements.

Overview

This comprehensive theory lab provides in-depth knowledge of operating system fundamentals—critical understanding for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1102 exam, you'll develop expertise in distinguishing between OS types, understanding filesystem structures, and managing OS lifecycle considerations essential for professional IT environments.

Through guided reading and practical exercises, you'll master the differences between Windows, macOS, Linux, and Chrome OS, understand various filesystem implementations, and learn lifecycle management

strategies. This knowledge is fundamental for IT professionals who must select, deploy, and maintain appropriate OSs that meet organizational requirements while ensuring compatibility and longevity.

	Key Term	Description
1	Operating system	Software managing hardware resources and providing user interface
2	Kernel	Core component managing system resources and hardware communication
3	Filesystem	Method of organizing and storing data on storage devices
4	Distribution	Specific version or variant of an OS (common with Linux)
5	End of life (EOL)	Point when vendor stops supporting an OS version
6	Journaling	Filesystem feature tracking changes to prevent corruption
7	File Allocation Table (FAT)	Simple filesystem structure used in FAT filesystems
8	Extended support	Phase providing only security updates for an OS
9	Fragmentation	File storage scattered across non-contiguous disk sectors
10	Mount point	Directory where a filesystem is attached in the directory tree
11	Partition	Logical division of a physical storage device
12	File permissions	Access control settings for files and directories
13	System requirements	Minimum hardware specifications for OS installation
14	Compatibility mode	Feature allowing older software to run on newer OS versions
15	Rolling release	Continuous update model without discrete version numbers

30 Bird - macOS and Linux Desktop Features and Utilities (Ch 1, Mod B)

Introduction

Objective

By completing this lab, you will be able to:

macOS Proficiency

- Navigate the macOS interface and file system effectively.
- Configure system settings through System Preferences.
- Utilize macOS-specific utilities and features.
- Troubleshoot common macOS issues.

Linux Desktop Mastery

- Work with various Linux desktop environments.
- Execute essential command-line operations.
- Manage software through package managers.
- Configure Linux system settings.

Cross-Platform Skills

- Compare Unix-based systems with Windows.
- Understand file permissions and security models.
- Use terminal and command-line interfaces effectively.
- Support users across different platforms.

Overview

This comprehensive theory lab provides in-depth knowledge of macOS and Linux desktop environments—critical understanding for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1102 exam, you'll develop expertise in navigating, configuring, and supporting these Unix-based operating systems that play vital roles in modern computing environments.

Through guided reading and practical exercises, you'll master the distinctive features of macOS including Finder navigation, System Preferences, Terminal usage, and ecosystem integration. You'll also explore Linux desktop environments, command-line tools, package management, and system administration. This knowledge is fundamental for IT professionals who must support diverse computing platforms in heterogeneous environments.

	Key Term	Description
1	Finder	macOS file manager and desktop interface
2	Terminal	Command-line interface for Unix commands
3	Package manager	System for installing and managing software packages
4	Desktop environment	Graphical interface layer for Linux systems
5	Dock	macOS application launcher and window manager
6	Repository	Online software package collection for Linux
7	Mission Control	macOS window and desktop space management
8	Systemd	Modern Linux init system and service manager
9	Homebrew	Third-party package manager for macOS
10	File permissions	Access control system for files and directories
11	Time Machine	macOS automated backup solution
12	Distribution	Complete Linux OS package with kernel and software
13	Kernel module	Loadable kernel extensions for hardware and features
14	Spotlight	macOS system-wide search functionality
15	Shell	Command-line interpreter (bash, zsh, etc.)

30 Bird - Operating System Installations and Upgrades (Ch 1, Mod C)

In this lab, you will gain hands-on experience with installing, configuring, and troubleshooting modern operating systems, including Windows 11 and Ubuntu Linux. You will perform clean installations, upgrades, partitioning, driver updates, user profile management, and recovery procedures. These tasks directly support the CompTIA A+ 220-1202 objectives, particularly Objective 1.1 (Operating System Installations and Upgrades), Objective 1.2 (Operating System Configuration), Objective 1.3 (Troubleshooting), and Objective 1.4 (System Management).

masterskill
education through innovation

aci LEARNING | SKILL LABS

As a personal computer (PC) technician, it is critical to understand how to install and configure operating systems, resolve installation issues, manage storage and user profiles, and maintain system health. These skills ensure you can support end-users, maintain business continuity, and keep systems secure and up to date. Mastery of these objectives is essential for passing the CompTIA A+ certification and succeeding in IT support roles.

30 Bird - Windows Edition Features and Comparison (Ch 1, Mod C)

Introduction

Objective

By completing this lab, you will be able to:

Windows Edition Identification

- Distinguish between consumer and business Windows editions.
- Identify feature differences across Windows 10 and 11 editions.
- Understand Windows edition upgrade paths and limitations.
- Recognize appropriate editions for specific deployment scenarios.

Feature Set Comparison

- Compare security features across different Windows editions.
- Understand management capabilities in business editions.
- Identify networking features exclusive to professional editions.
- Evaluate virtualization support across Windows editions.

Licensing and Deployment

- Understand Windows licensing models and activation methods.
- Identify volume licensing options for enterprise deployments.
- Compare Original Equipment Manager (OEM), retail, and volume license rights.
- Select appropriate editions based on organizational needs.

Overview

This comprehensive theory lab provides in-depth knowledge of Microsoft Windows editions—critical understanding for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1102 exam, you'll develop expertise in distinguishing between Windows editions, understanding their feature sets, and making informed recommendations for specific use cases in professional environments.

Through guided reading and practical exercises, you'll master the differences between Windows Home, Pro, Enterprise, and Education editions, understand licensing models, feature availability, and deployment scenarios. This knowledge is fundamental for IT professionals who must select, deploy, and support appropriate Windows editions that meet organizational requirements while optimizing costs and functionality.

	Key Term	Description
1	Windows edition	Specific version of Windows with defined feature set and licensing terms
2	BitLocker	Full-disk encryption feature available in Pro and higher editions
3	Domain join	Ability to connect to Active Directory domains for centralized management
4	Group Policy	Centralized configuration management system for Windows computers

	Key Term	Description
5	Hyper-V	Built-in virtualization platform for running virtual machines
6	Volume licensing	Bulk licensing program for organizations purchasing multiple licenses
7	Windows Autopilot	Cloud-based deployment service for zero-touch device provisioning
8	Long-Term Servicing Channel (LTSC)	LTSC providing stable, rarely updated Windows versions
9	Credential Guard	Virtualization-based security protecting domain credentials
10	AppLocker	Application control policies restricting software execution
11	Key Management Service (KMS)	KMS for automatic volume license activation
12	Software Assurance	Microsoft program providing upgrade rights and additional benefits
13	DirectAccess	Always-on Virtual Private Network (VPN) technology for seamless corporate network access
14	BranchCache	Distributed caching technology optimizing Wide Area Network (WAN) bandwidth usage
15	Windows Update for Business	Service enabling IT control over update deployment

30 Bird - Application and Cloud Service Deployment (Ch 1, Mod D)

Introduction

Objective

By completing this lab, you will be able to:

Application Deployment Mastery

- Understand various application installation methods.
- Deploy software according to system requirements.
- Manage application dependencies and compatibility.
- Implement automated deployment strategies.

Cloud Service Integration

- Configure cloud-based productivity suites.
- Understand Software as a Service (SaaS) models.
- Manage cloud storage and synchronization.
- Implement single sign-on solutions.

Modern Deployment Technologies

- Use application virtualization techniques.
- Understand containerization concepts.
- Deploy progressive web applications.
- Manage hybrid cloud environments.

masterskill
education through innovation

aci LEARNING | SKILL LABS

Overview

This comprehensive theory lab provides in-depth knowledge of modern application installation and cloud service deployment—critical understanding for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1102 exam, you'll develop expertise in traditional software installation methods, modern deployment technologies, and cloud-based productivity solutions that define contemporary IT environments.

Through guided reading and practical exercises, you'll master application deployment strategies across different platforms, understand containerization and virtualization, and configure cloud-based productivity tools. This knowledge is fundamental for IT professionals who must efficiently deploy, manage, and support both traditional applications and modern cloud services in enterprise environments.

	Key Term	Description
1	Software as a service (SaaS)	Cloud-based software delivery model via subscription
2	Application virtualization	Technology isolating applications from the operating system
3	Single sign-on (SSO)	Authentication method using one credential set for multiple services
4	Container	Lightweight, portable application package with dependencies
5	Progressive web application (PWA)	Web application with native app-like capabilities
6	Multi-factor authentication	Security requiring multiple verification methods
7	Application programming interface (API)	API for service integration
8	Tenant	Dedicated instance of a cloud service for an organization
9	Federation	Trust relationship between identity systems
10	Orchestration	Automated management of containers or services
11	Microservices	Architecture dividing applications into small services
12	Identity provider (IdP)	Service managing user authentication
13	Open authorization (OAuth)	Authorization framework for API access
14	Hybrid cloud	Computing environment combining on-premises and cloud
15	Files on-demand	Cloud storage feature downloading files when needed

masterskill
education through innovation

aci LEARNING | SKILL LABS

30 Bird - Scripting and AI (Ch 1, Mod D)

Introduction

Objective

This hands-on lab provides comprehensive practice in implementing scripting solutions and AI-assisted troubleshooting—critical skills for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in various scripting languages, automation techniques, and AI-powered tools that enhance productivity and problem-solving capabilities in modern IT environments.

Through guided exercises, you'll master essential scripting practices including script file identification, batch and PowerShell execution, task automation, system information gathering, and AI-assisted analysis. You'll also learn to leverage AI tools like Microsoft Copilot for script explanation, modification, system configuration assistance, and troubleshooting guidance. These skills are fundamental for improving efficiency, reducing manual tasks, and utilizing modern AI technologies in professional IT support.

Overview

Learning Objectives

By completing this lab, you will be able to:

Scripting Fundamentals and Implementation

- Identify common script file types and their applications
- Execute basic batch scripts for Windows automation
- Run PowerShell scripts for advanced system management
- Create custom scripts for task automation and system administration

System Automation and Information Gathering

- Automate routine tasks using scripting technologies
- Gather comprehensive system information through scripts
- Implement monitoring and reporting automation
- Develop maintenance scripts for regular system tasks

AI-Assisted IT Support and Development

- Utilize Microsoft Copilot for script analysis and explanation
- Leverage AI for script modification and enhancement
- Apply AI assistance for system settings configuration
- Use AI-powered troubleshooting for problem resolution

Lab Task Overview

Task	Description
Identify Common Script File Types	Recognize and categorize different scripting file extensions
Execute a Basic Batch Script	Run Windows batch files for system automation

Task	Description
Execute a Basic PowerShell Script	Execute PowerShell commands for advanced system management
Automate a Task with Scripting	Create custom scripts for routine task automation
Gather System Information with Scripting	Use scripts to collect comprehensive system data
Use Copilot to Explain a Script	Leverage AI to understand script functionality and purpose
Use Copilot to Modify a Script	Apply AI assistance for script enhancement and customization
Use Copilot for System Settings Help	Utilize AI for system configuration guidance
Use Copilot for Troubleshooting Steps	Apply AI-powered assistance for problem resolution

CompTIA A+ Objective Mapping

Task Area	Exam Objective Reference
Script File Types	4.0 Operational Procedures
Batch Script Execution	1.0 Operating Systems
PowerShell Execution	1.0 Operating Systems
Task Automation	1.0 Operating Systems
System Information	1.0 Operating Systems
Script Explanation	1.0 Operating Systems
Script Modification	1.0 Operating Systems
System Settings Assistance	1.0 Operating Systems
AI Troubleshooting	3.0 Software Troubleshooting

Getting Started

Before beginning the hands-on tasks, follow these steps to access your virtual lab environment:

1. **Click** the **Start** button in your lab portal to provision the lab environment.
2. **Click** the computer image or "Launch VM" button in the right pane when the lab loads to open the Windows virtual machine window.
3. **Wait** for Windows 11 to finish booting. When you see the lock screen, **double-click** anywhere to reveal the login prompt.
4. **Select** the **Student** account (if prompted).
5. **Login** with the password Passw0rd.(case sensitive).
6. Once logged in, you are ready to begin the lab activities below.

If you encounter any issues starting the lab or logging in, notify your instructor for assistance.

Before you begin the hands-on tasks in this lab, you will gain practical experience implementing scripting solutions and AI-assisted tools that are increasingly important in modern IT environments. You will learn to automate routine tasks, gather system information efficiently, and leverage artificial intelligence for enhanced problem-solving and productivity.

These skills are essential for improving operational efficiency, reducing manual errors, and staying current with emerging technologies that transform IT support and system administration. Mastery of these tasks directly aligns with CompTIA A+ exam objectives and prepares you for the evolving landscape of AI-enhanced IT professional responsibilities.

	Key Term	Description
1	Batch Script	Windows command-line script file with .bat or .cmd extension
2	PowerShell Script	Advanced Windows scripting environment with .ps1 extension
3	Script Automation	Process of using scripts to perform tasks without manual intervention
4	System Information Gathering	Automated collection of hardware and software configuration data
5	Microsoft Copilot	AI-powered assistant integrated into Microsoft products
6	Artificial Intelligence	Computer systems performing tasks typically requiring human intelligence
7	Machine Learning	AI subset enabling systems to learn and improve from experience
8	Natural Language Processing	AI capability to understand and generate human language
9	Script Execution Policy	PowerShell security feature controlling script execution permissions
10	Command Line Interface	Text-based interface for executing commands and scripts
11	Variable Assignment	Process of storing data in named containers within scripts
12	Error Handling	Script techniques for managing and responding to execution errors

30 Bird - Windows Settings and Personalization (Ch 2, Mod B)

Introduction

Objective

By completing this lab, you will be able to:

System Configuration

- Navigate and customize all Windows Settings categories.
- Configure display, sound, and power management settings.
- Manage system notifications and update settings.
- Optimize performance through advanced system configurations.

Operating System Management

- Configure and troubleshoot user accounts and permissions.
- Manage installed applications and Windows features.
- Implement proper file system and storage configurations.
- Troubleshoot common operating system and driver issues.

Hardware Integration

- Install and configure peripheral devices.
- Manage device drivers and resource allocation.
- Configure multiple display setups.
- Optimize power plans for different hardware configurations.

Security Implementation

- Configure user authentication and access controls.
- Implement appropriate privacy settings.
- Manage Windows Defender and firewall settings.
- Configure encryption and data protection features.

Accessibility and Productivity

- Implement accessibility features for diverse user needs.
- Configure language and regional settings.
- Optimize settings for maximum productivity.
- Manage network and sharing configurations.

Overview

This hands-on lab provides comprehensive practice in configuring and managing Windows operating system settings—a critical skill set for IT professionals and CompTIA A+ certification candidates. Covering objectives from both the 220-1101 and 220-1102 exams, you'll develop proficiency in:

- System configuration and optimization
- Operating system management and troubleshooting
- Hardware and software integration
- Security and access control implementation

Through guided exercises, you'll master both graphical user interface (GUI) and keyboard navigation techniques while learning industry best practices for Windows administration in professional environments.

	Key Term	Description
1	Display settings	Options for adjusting screen resolution, scaling, and multiple monitors
2	Personalization	Customization of desktop themes, backgrounds, and colors
3	Power options	Settings that control power plans, sleep, and battery usage
4	Accessibility	Features that improve usability for users with disabilities
5	Regional settings	Configuration of time zone, date/time formats, and language preferences
6	Windows Update	Service for downloading and installing system updates and patches

	Key Term	Description
7	Application management	Installing, uninstalling, and managing programs
8	Device management	Managing printers, peripheral devices, and drivers
9	Network & Sharing Center	Interface for managing network connections and sharing settings
10	Audio settings	Managing sound devices, playback, and volume controls
11	File Explorer	File management tool for navigating and organizing files and folders
12	Indexing	Process that enables fast file and content searches in Windows

30 Bird - Windows Graphical and Command-line Management Tools (Ch 2, Mod C)

Introduction

Objective

This lab provides hands-on experience with managing a Windows environment through both graphical user interfaces (GUIs) and command-line interfaces (CLI). The exercises cover essential system tools, resource management, configuration settings, and administrative tasks using both interfaces. These tasks directly support the CompTIA A+ 220-1202 objectives, particularly Objective 1.2 (Operating System Configuration), Objective 1.3 (Troubleshooting), Objective 1.4 (System Management), and Objective 4.0 (Command-Line Tools).

Overview

In this lab, you will learn to:

- Monitor and analyze system performance using Task Manager and Resource Monitor
- Manage system resources and administrative tools with MMC snap-ins
- Gather and interpret system information for troubleshooting
- Optimize disk performance and use built-in maintenance utilities
- Navigate and manage the file system using command-line tools
- Configure and troubleshoot network settings with CLI utilities
- Adjust system configuration and startup options using System Configuration Utility
- Safely edit and backup the Windows Registry
- Apply and manage Group Policy for system-wide settings
- Leverage built-in Windows system tools for effective administration

Proficiency in both GUI and CLI methods is essential for effective Windows system administration. These skills enable efficient system management, issue troubleshooting, performance optimization, and task automation. The ability to work effectively in both interfaces is crucial for Information technology (IT) professionals, as different scenarios may require different approaches. Mastery of these objectives is important for CompTIA A+ certification and professional IT support roles.

	Key Term	Description
1	Task Manager	Tool for monitoring and managing running processes, performance, and startup programs in Windows.
2	MMC Snap-in	Modular administrative tools added to the Microsoft Management Console for system management.

	Key Term	Description
3	Resource Monitor	Utility for real-time monitoring of CPU, memory, disk, and network usage.
4	System Configuration Utility	Tool (msconfig) for managing startup options, services, and boot settings.
5	Command-Line Interface (CLI)	Text-based interface for executing commands and managing the system.
6	Registry Editor	Tool (regedit) for viewing and editing the Windows Registry.
7	Group Policy	Framework for managing and configuring operating system, application, and user settings in a Windows environment.
8	Disk Cleanup	Utility for removing unnecessary files to free up disk space.
9	Defragmenter and Optimize Drives	Tool for optimizing and defragmenting hard drives to improve performance.
10	Network troubleshooting commands	Commands such as ipconfig, ping, netstat, and nslookup for diagnosing network issues.

30 Bird - Windows OS Troubleshooting (Ch 2, Mod D)

Introduction

Objective

By completing this lab, you will be able to:

System Diagnostics and Analysis

- Analyze Blue Screen of Death errors and identify root causes.
- Diagnose performance issues and implement optimization solutions.
- Troubleshoot boot problems and system startup failures.
- Investigate application crashes and compatibility issues.

System Performance and Stability

- Resolve memory-related warnings and optimize resource usage.
- Manage Windows services and troubleshoot service failures.
- Improve system stability through configuration and maintenance.
- Implement system recovery and restore procedures.

Advanced Troubleshooting Techniques

- Use built-in Windows diagnostic tools effectively.
- Interpret system logs and error messages accurately.
- Apply systematic troubleshooting methodologies.
- Document problems and solutions for future reference.

Overview

This hands-on lab provides comprehensive practice in diagnosing and resolving common Windows operating system issues—critical skills for information technology (IT) professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in systematic troubleshooting methodologies, diagnostic tool usage, and problem resolution techniques essential for maintaining stable Windows environments.

Through guided exercises, you'll master essential troubleshooting practices including Blue Screen of Death (BSOD) analysis, performance optimization, boot problem resolution, application crash diagnosis, service management, memory issue resolution, system stability improvement, and system recovery procedures. These skills are fundamental for providing effective technical support and maintaining reliable computing environments in professional settings.

	Key Term	Description
1	Blue Screen of Death (BSOD)	Critical system error requiring immediate restart
2	Event Viewer	Windows tool for viewing system logs and error messages
3	Performance Monitor	Tool for tracking system resource usage and performance
4	System File Checker	Utility that scans and repairs corrupted system files
5	Memory Diagnostic	Tool that tests system RAM for errors and failures
6	Safe Mode	Diagnostic startup mode with minimal drivers and services
7	System Restore	Feature that reverts system to previous working state
8	Task Manager	Tool for monitoring and managing running processes
9	Device Manager	Utility for managing hardware devices and drivers
10	Registry Editor	Tool for viewing and modifying Windows registry database
11	Boot Configuration Data	Database containing boot-time configuration parameters
12	Windows Recovery Environment	Special diagnostic and repair environment

30 Bird - Windows Networking Configuration (Ch 3, Mod C)

Introduction

Objective

This lab is designed to help you develop practical Windows networking skills that align with CompTIA A+ objectives. By completing these exercises, you will build competence in network configuration and troubleshooting that is directly applicable to real-world IT support scenarios.

Task-Specific Objectives:

Configure IP Addressing

- Understand IPv4 addressing.
- Configure static IP addresses.
- Verify IP configuration.

Configure DNS Settings

- Configure Domain Name System (DNS) server addresses.
- Test DNS resolution.
- Flush and manage DNS cache.

Configure Windows Firewall Rules

- Create inbound and outbound rules.
- Configure rule properties.
- Test firewall configurations.

Configure File and Printer Sharing

- Set up file sharing.
- Configure sharing permissions.
- Access shared resources.

Map Network Drives

- Map drives using different methods.
- Configure persistent connections.
- Troubleshoot mapping issues.

Establish a VPN Connection

- Configure VPN settings.
- Connect to a VPN server.
- Troubleshoot VPN connectivity.

Test Network Connectivity

- Use network diagnostic tools.
- Interpret test results.
- Troubleshoot connectivity issues.

Configure Network Discovery

- Enable or disable network discovery.
- Configure network profiles.
- Troubleshoot discovery issues.

Configure Proxy Settings

- Configure manual and automatic proxy settings.
- Test proxy configurations.
- Troubleshoot proxy issues.

Configure Network Locations

- Understand network location types.
- Configure location settings.
- Troubleshoot location-based issues.

Expected Outcomes

Upon successful completion of this lab, you will be able to:

- Configure and verify IP addressing on Windows systems.
- Set up and test DNS configurations.
- Create and manage Windows Firewall rules.
- Configure and troubleshoot file and printer sharing.
- Map network drives and establish VPN connections.

- Use network diagnostic tools to test and troubleshoot connectivity.
- Configure network discovery and proxy settings.
- Manage network locations and profiles.

Overview

Welcome to this hands-on lab focused on Windows Networking Configuration. This lab provides practical experience in configuring and managing network settings in Windows, a critical skill for IT professionals and CompTIA A+ certification candidates. You'll develop proficiency in IP configuration, DNS settings, firewall rules, and network troubleshooting.

Why This Lab Matters

Networking forms the foundation of modern IT infrastructure, and the ability to configure and troubleshoot network settings is fundamental to roles including the following:

- IT support specialist
- Network administrator
- System administrator
- Help desk technician
- Technical support engineer

What You'll Learn

Through carefully designed exercises, you will be able to:

- Configure and verify IP addressing.
- Set up and test DNS configurations.
- Create and manage Windows Firewall rules.
- Configure file and printer sharing.
- Map network drives and establish VPN connections.
- Troubleshoot network connectivity issues.

Real-World Application

These skills apply to the following scenarios:

- Setting up office networks
- Troubleshooting connectivity issues
- Securing network communications
- Configuring remote access solutions
- Managing network resources

Certification Alignment

This lab supports CompTIA A+ (220–1102) preparation, addressing key objectives in Domain 4.0 (Operational Procedures). The hands-on experience will help you pass certification exams while building practical skills.

Lab Scenario

You are an IT support specialist at a medium-sized company. The network administrator has asked you to configure the network settings on several Windows workstations. Your tasks include setting up IP addressing, configuring DNS, setting up file sharing, and ensuring secure network communications.

	Key Term	Description
1	IP Address	A unique identifier assigned to each device on a network (e.g., 192.168.1.1)
2	Subnet Mask	Defines which part of an IP address is the network portion (e.g., 255.255.255.0)
3	Default Gateway	The device that routes traffic between different networks (typically a router)
4	DNS	Domain Name System, translates domain names to IP addresses.
5	Firewall	Security system that monitors and controls network traffic based on predetermined rules
6	VPN	Virtual Private Network, creates a secure encrypted connection over the Internet.
7	Network Share	A shared resource on a network, such as files or printers
8	Network Drive	A drive letter mapped to a network share for easy access
9	Proxy Server	An intermediary server that forwards requests between clients and other servers
10	Network Profile	A collection of networks and sharing settings (Public, Private, or Domain)
11	DHCP	Dynamic Host Configuration Protocol, automatically assigns IP addresses to devices.
12	NAT	Network Address Translation, allows multiple devices to share a single public IP.
13	Port	A virtual point for network communications (e.g., 80 for HTTP, 443 for HTTPS)
14	Latency	The time it takes for data to travel from source to destination
15	Bandwidth	The maximum rate of data transfer across a network path

30 Bird - Social Engineering Attacks (Ch 4, Mod A)

Introduction

Objective

By completing this lab, you will be able to:

Social Engineering Recognition

- Identify common social engineering attack vectors and tactics.
- Analyze phishing attempts and suspicious communications.
- Recognize physical security threats and unauthorized access attempts.
- Understand psychological manipulation techniques used by attackers.

Security Policy Implementation

- Configure strong password policies and enforcement mechanisms.
- Implement User Account Control measures.
- Establish account lockout policies for failed authentication attempts.

Browser Security

- Configure browser security settings against malicious content.
- Implement firewall rules and network protection.
- Update software and operating systems for security patches.

Overview

This hands-on lab provides comprehensive practice in understanding, identifying, and defending against social engineering attacks—critical skills for information technology (IT) professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in recognizing human-based security threats and implementing appropriate countermeasures to protect organizational assets.

Through guided exercises, you'll learn to configure security policies, implement user account controls, strengthen authentication mechanisms, and establish protective measures against manipulation tactics used by cybercriminals. These skills are essential for creating defense-in-depth strategies that address the human element of cybersecurity, which remains the weakest link in most security frameworks.

	Key Term	Description
1	Social Engineering	Psychological manipulation of people to divulge confidential information or perform actions
2	Phishing	Fraudulent attempt to obtain sensitive information by disguising as trustworthy entity
3	Spear Phishing	Targeted phishing attack directed at specific individuals or organizations
4	Pretexting	Creating fabricated scenarios to engage victims and steal information
5	Baiting	Offering something enticing to spark curiosity and prompt victims to take action
6	Tailgating	Following someone into a restricted area without proper authorization
7	Vishing	Voice-based phishing conducted over telephone calls
8	Smishing	Short Message Service (SMS)-based phishing attacks conducted through text messages
9	Whaling	Phishing attacks targeting high-profile individuals like executives
10	Multifactor Authentication	Security system requiring multiple verification methods
11	User Account Control	Windows security feature that prevents unauthorized changes
12	Password Policy	Set of rules designed to enhance security through strong passwords

masterskill
education through innovation

aci LEARNING | SKILL LABS

30 Bird - Windows Local Security Controls (Ch 5, Mod A)

Introduction

Objective

By completing this lab, you will be able to:

Security Software Configuration

- Configure Windows Defender Antivirus for comprehensive threat protection
- Manage Windows Firewall settings and rules for network security
- Implement Windows Update policies for security patch management
- Configure login options including multi-factor authentication

Access Control and User Management

- Manage user accounts and implement principle of least privilege
- Configure NTFS and share permissions for data protection
- Implement Local Security Policy configurations
- Manage file and folder attributes for security control

Data Protection and Encryption

- Implement BitLocker-To-Go encryption for removable media
- Configure Group Policy for centralized security management
- Establish secure authentication mechanisms
- Implement data protection through access controls and encryption

Overview

This hands-on lab provides comprehensive practice in configuring Windows security settings—critical skills for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in implementing comprehensive security configurations that protect systems from unauthorized access, malware threats, and data breaches through systematic security hardening and policy implementation.

Through guided exercises, you'll master essential security practices including Windows Defender configuration, firewall management, user account administration, BitLocker encryption, permission management, local security policies, Windows Update configuration, login options, Group Policy implementation, and file attribute management. These skills are fundamental for creating secure computing environments that protect organizational assets while maintaining user productivity and system functionality.

	Key Term	Description
1	Windows Defender	Microsoft's built-in antivirus and anti-malware solution
2	Windows Firewall	Network security system controlling inbound and outbound traffic
3	BitLocker-To-Go	Encryption technology for protecting removable storage devices
4	NTFS Permissions	File system-level access controls for folders and files
5	Share Permissions	Network-level access controls for shared folders
6	Local Security Policy	Windows tool for configuring security policies on local computer
7	Group Policy	Centralized configuration management system for Windows networks

	Key Term	Description
8	User Account Control	Security feature preventing unauthorized system changes
9	Windows Hello	Biometric authentication system for secure login
10	Security Identifier	Unique identifier assigned to user accounts and groups
11	Access Control List	List defining permissions for users and groups on resources
12	Principle of Least Privilege	Security concept limiting access to minimum required resources

30 Bird - Windows Local Security Configuration (Ch 5, Mod A)

Introduction

Objective

By completing this lab, you will be able to:

Security Configuration

- Configure and manage Windows Defender Antivirus settings
- Implement Windows Firewall with Advanced Security rules
- Create and modify local security policies
- Configure encryption using EFS

Account Management

- Create and manage local user accounts with appropriate permissions
- Configure User Account Control (UAC) settings
- Apply principle of least privilege to user accounts

System Protection

- Configure Windows Update settings for security patches
- Implement file and folder permissions using NTFS
- Set up audit policies for security monitoring
- Configure system restore and backup options

Policy Implementation

- Implement local Group Policy settings
- Monitor security events and logs

Compliance and Best Practices

- Apply security baselines for different environments
- Document security configurations
- Troubleshoot common security issues
- Maintain compliance with security standards

masterskill
education through innovation

aci LEARNING | SKILL LABS

Overview

This hands-on lab provides comprehensive practice in configuring and managing Windows local security settings—essential skills for IT professionals and CompTIA A+ certification candidates. Covering objectives from both the 220-1101 and 220-1102 exams, you'll develop proficiency in:

- Windows security configuration and hardening
- User account and permission management
- System protection and encryption implementation
- Security policy configuration and enforcement

Through guided exercises, you'll master both GUI and command-line techniques while learning industry best practices for securing Windows systems in professional environments.

	Key Term	Description
1	Windows Defender	Built-in antivirus and anti-malware solution in Windows
2	Windows Firewall	Network security system that monitors and controls network traffic
3	User Account Control (UAC)	Security feature that prevents unauthorized system changes
4	Local Security Policy	Settings that control security behavior on a local computer
5	New Technology File System (NTFS) permissions	File system permissions controlling access to files and folders
6	Encrypting File System (EFS)	File encryption feature built into NTFS
7	Password policy	Rules governing password complexity and usage
8	Account lockout policy	Settings that lock accounts after failed login attempts
9	Windows Update	Service for downloading and installing security patches
10	Security baseline	Standard security configuration for systems
11	Principle of least privilege	Security concept of minimal necessary permissions

30 Bird - Windows Security Controls (Ch 5, Mod B)

Introduction

Objective

Welcome to this comprehensive hands-on lab focused on Windows Security Controls. In today's digital landscape, where cyber threats are increasingly sophisticated, understanding and implementing robust security measures is not just important—it's absolutely critical. This lab is designed to transform you from a passive user of Windows Security features into a confident administrator capable of implementing enterprise-level security configurations.

Why This Lab Matters

In an era where data breaches and cyberattacks make daily headlines, organizations are investing heavily in security professionals who can protect their systems and data. This lab provides you with the practical,

hands-on experience that employers value most. By completing these exercises, you'll develop the skills needed to:

- Protect systems from malware and unauthorized access
- Implement security best practices in real-world scenarios
- Troubleshoot common security issues
- Configure enterprise-level security policies
- Secure sensitive data through encryption and access controls

Who Benefits from This Lab

This training is specifically designed for:

- Aspiring IT Security Specialists looking to build foundational security skills
- System Administrators who need to secure Windows environments
- Help Desk Professionals who are the first line of defense against security threats
- Network Administrators responsible for maintaining secure network access
- IT Professionals preparing for CompTIA A+ and Security+ certifications
- Anyone who wants to understand how to protect Windows systems in an increasingly dangerous digital world

Overview

What You'll Learn

This lab is structured to take you from fundamental security concepts to advanced configurations. Through hands-on exercises, you'll gain practical experience in:

Threat Protection

- Configure and optimize Windows Defender Antivirus for maximum protection.
- Implement real-time scanning and cloud-delivered protection.
- Schedule and analyze system scans.

Network Security

- Create and manage Windows Firewall rules for inbound and outbound traffic.
- Configure advanced firewall profiles (Domain, Private, Public).
- Monitor and troubleshoot firewall activity.

Access Control

- Create and manage local user accounts with appropriate permissions.
- Implement and test User Account Control (UAC) settings.
- Configure password policies and account lockout policies.

Data Protection

- Implement file and folder encryption using Encrypting File System (EFS).
- Recover encrypted files using recovery certificates.
- Configure BitLocker for full-disk encryption (where applicable).

System Hardening

- Configure and apply security templates.
- Implement security policies through Local Security Policy.
- Harden system configurations against common attack vectors.

Maintenance and Monitoring

- Configure and manage Windows Update settings.
- Review security logs and event viewer.
- Implement security baselines and compliance checks.

By the end of this lab, you'll have the practical skills needed to secure Windows systems in both small business and enterprise environments, making you a valuable asset in any IT security role.

Real-World Application

The skills you'll acquire in this lab are directly transferable to critical IT security scenarios that professionals face daily:

Enterprise Security Implementation

- Deploy and manage security policies across an organization's Windows infrastructure.
- Respond to security incidents by analyzing and mitigating threats.
- Implement defense-in-depth strategies to protect against evolving cyber threats.

Compliance and Auditing

- Configure systems to meet industry standards (National Institute of Standards and Technology [NIST], Center for Internet Security [CIS], International Organization for Standardization [ISO] 27001).
- Prepare for security audits by implementing proper controls and documentation.
- Ensure compliance with regulations like General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS).

Incident Response

- Detect and respond to security breaches using built-in Windows tools.
- Analyze security logs to identify suspicious activities.
- Implement remediation strategies for compromised systems.

Security Consulting

- Assess and harden Windows systems for clients.
- Provide recommendations for security improvements.
- Implement security baselines and best practices.

IT Administration

- Manage user access and permissions effectively.
- Secure sensitive data through encryption and access controls.
- Maintain system security through regular updates and monitoring.

These practical applications demonstrate how the skills you'll learn are not just theoretical concepts but essential tools for protecting organizations from the growing threat of cyberattacks.

masterskill
education through innovation

aci LEARNING | SKILL LABS

30 Bird - Malware Defense (Ch 5, Mod B)

Introduction

Objective

By completing this lab, you will be able to:

Malware Detection and Response

- Identify and analyze malware symptoms and behaviors.
- Quarantine potentially infected files safely.
- Execute proper malware removal procedures.

Security Software Management

- Configure and update antivirus and anti-malware software.
- Interpret scan results and security alerts.

System Protection and Hardening

- Block malicious websites and content.
- Create system backups for recovery purposes.
- Implement preventive security measures.

Overview

This hands-on lab provides comprehensive practice in implementing malware defense strategies and procedures—critical skills for information technology (IT) professionals and CompTIA A+ certification candidates. Covering objectives from the 220–1202 exam, you'll develop proficiency in detecting, preventing, and removing malware threats from computer systems.

Through guided exercises, you'll master essential security practices including configuring antivirus software, performing system scans, quarantining threats, and implementing preventive measures. These skills are fundamental for maintaining system security and protecting against the ever-evolving landscape of malware threats that organizations face daily.

	Key Term	Description
1	Malware	Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems
2	Antivirus	Software designed to detect, prevent, and remove malicious software
3	Real-time Protection	Continuous monitoring of system activities to detect threats immediately
4	Quarantine	Isolated storage area where suspected malware is safely contained
5	Signature Database	Collection of known malware patterns used for detection
6	Heuristic Analysis	Behavior-based detection method that identifies suspicious activities
7	System Scan	Comprehensive examination of files and system areas for threats
8	Firewall	Network security system that monitors and controls network traffic
9	Zero-day Threat	Previously unknown malware that exploits undiscovered vulnerabilities
10	Rootkit	Malware that hides deep within the operating system

	Key Term	Description
11	Trojan Horse	Malware disguised as legitimate software
12	Ransomware	Malware that encrypts files and demands payment for decryption

30 Bird - System Hardening (Ch 6, Mod A)

Introduction

Objective

By completing this lab, you will be able to:

Security Policy Implementation

- Configure comprehensive password policies and enforcement mechanisms
- Implement account lockout policies for failed authentication attempts
- Manage user account permissions and privilege restrictions
- Configure screen lock settings for unauthorized access prevention

System Configuration Hardening

- Configure and manage Windows Firewall settings
- Disable unnecessary services and minimize attack surface
- Update operating systems and applications systematically
- Implement data encryption for information protection

Access Control Management

- Establish principle of least privilege for user accounts
- Configure automatic update mechanisms for security patches
- Implement screen saver policies with password protection
- Manage service accounts and system-level permissions

Overview

This hands-on lab provides comprehensive practice in implementing system hardening techniques—critical skills for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in securing Windows systems through systematic configuration of security controls, user account management, service hardening, and data protection measures.

Through guided exercises, you'll master essential hardening practices including password policy enforcement, account lockout configuration, firewall management, service minimization, permission control, screen lock implementation, data encryption, and automated update configuration. These skills are fundamental for creating secure computing environments that resist both external attacks and internal security breaches while maintaining system functionality and user productivity.

	Key Term	Description
1	System Hardening	Process of securing computer systems by reducing vulnerabilities
2	Attack Surface	Total number of possible entry points for unauthorized access
3	Principle of Least	Security concept limiting user access to minimum required resources

	Key Term	Description
	Privilege	
4	Service Minimization	Disabling unnecessary services to reduce security exposure
5	Data Encryption	Process of converting data into coded format to prevent unauthorized access
6	Account Lockout	Security mechanism that disables accounts after failed login attempts
7	Screen Lock	Security feature requiring authentication to access active sessions
8	Group Policy	Windows administrative template system for managing security settings
9	BitLocker	Microsoft's full disk encryption technology
10	Windows Update	Microsoft's system for delivering security patches and updates
11	User Account Control	Windows security feature preventing unauthorized system changes
12	Firewall Rules	Network traffic filtering configurations for security protection

30 Bird - Data Destruction and Disposal Methods (Ch 6, Mod A)

Introduction

Objective

By completing this lab, you will be able to:

Data Sanitization Methods

- Perform data overwriting procedures on Windows and Linux systems
- Execute secure file deletion using specialized tools and techniques
- Understand physical destruction methods for storage devices
- Verify data sanitization effectiveness through testing procedures.

Compliance and Best Practices

- Follow industry-standard data disposal protocols and procedures
- Understand regulatory requirements for data destruction
- Implement proper documentation and certification processes
- Establish organizational policies for secure data handling

Cross-Platform Operations

- Perform data sanitization on both Windows and Linux operating systems
- Use built-in and third-party tools for secure data removal
- Understand filesystem differences in data storage and recovery
- Apply appropriate methods based on storage technology and requirements

Overview

This hands-on lab provides comprehensive practice in implementing secure data disposal and sanitization procedures—critical skills for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in various data destruction methods, verification techniques, and compliance requirements that ensure complete data removal from storage devices.

Through guided exercises, you'll master essential data disposal practices including data overwriting, secure file deletion, physical device destruction, sanitization verification, and regulatory compliance procedures. These skills are fundamental for protecting sensitive information, maintaining privacy compliance, and preventing data breaches through improper disposal of storage media and computing devices.

	Key Term	Description
1	Data Sanitization	Process of deliberately and permanently removing data from storage devices
2	Data Overwriting	Method of writing random data over existing files to prevent recovery
3	Secure Deletion	Permanent removal of files using cryptographic or overwriting techniques
4	Physical Destruction	Complete physical destruction of storage media to prevent data recovery
5	Data Remnants	Residual data that may remain after standard deletion procedures
6	NIST Guidelines	National Institute standards for media sanitization procedures
7	Certificate of Destruction	Official documentation proving secure data disposal completion
8	Data Recovery	Process of retrieving deleted or lost data from storage devices
9	Degaussing	Method using magnetic fields to erase data from magnetic storage
10	Cryptographic Erasure	Data destruction through encryption key deletion
11	HIPAA Compliance	Healthcare data protection regulations requiring secure disposal
12	Chain of Custody	Documentation trail ensuring secure handling of sensitive devices

30 Bird - Browser Security Hardening (Ch 6, Mod A)

Introduction

Objective

By completing this lab, you will be able to:

Browser Security Configuration

- Update web browsers to latest versions for security patches.
- Manage browser extensions and plugins safely.
- Configure pop-up blockers and malicious content protection.
- Implement secure Domain Name System (DNS) settings for threat protection.

Privacy and Data Protection

- Clear browsing data and cache for privacy maintenance.
- Configure private browsing modes for sensitive activities.
- Manage browser permissions for websites and applications.
- Implement tracking protection and advertising controls.

Authentication and Access Management

- Configure browser-based password management systems.
- Manage certificate settings and secure connections.

- Implement multifactor authentication for browser accounts.
- Configure browser sync settings for security and convenience.

Overview

This hands-on lab provides comprehensive practice in implementing browser security configurations—critical skills for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in securing web browsers against various threats including malicious downloads, privacy violations, tracking, and social engineering attacks through systematic security hardening and policy implementation.

Through guided exercises, you'll master essential browser security practices including software updates, extension management, pop-up blocking, data clearing procedures, private browsing configuration, permission management, DNS security, password management, and tracking protection. These skills are fundamental for protecting users from web-based threats while maintaining productivity and ensuring safe Internet usage in professional environments.

	Key Term	Description
1	Browser extension	Software add-on that extends browser functionality
2	Pop-up blocker	Security feature preventing unwanted advertising windows
3	Private browsing	Mode that doesn't save browsing history or data
4	Tracking protection	Feature blocking websites from monitoring user activity
5	Secure DNS	DNS service providing malware and phishing protection
6	Browser cache	Temporary storage of website data for faster loading
7	Cookie management	Control of website data storage for tracking and functionality
8	Certificate validation	Process verifying website identity and encryption
9	Password manager	Tool storing and generating secure passwords
10	Content Security Policy	Web security standard preventing code injection attacks
11	HTTPS enforcement	Requiring encrypted connections for secure communication
12	Cross-site tracking	Method websites use to monitor users across multiple sites

30 Bird - Mobile Device and Security Configuration (Ch 6, Mod B)

Introduction

Objective

By the end of this lab, students will be able to:

- Configure various authentication methods on mobile devices including biometric and multi-factor authentication.
- Implement encryption strategies for data at rest and in transit on mobile platforms.
- Deploy and manage mobile device management (MDM) solutions for enterprise environments.
- Configure application permissions and security settings to minimize attack surfaces.
- Establish remote wipe and location tracking capabilities for lost or stolen devices.

- Implement network security configurations including VPN and secure Wi-Fi connections.
- Configure backup and recovery options while maintaining security compliance.
- Apply security policies that comply with organizational and regulatory requirements.

Overview

Mobile devices have become essential tools in both personal and professional environments, making their security configuration critical for protecting sensitive data and maintaining organizational compliance. This lab explores comprehensive mobile device security configuration strategies, including authentication methods, encryption techniques, and mobile device management (MDM) solutions. Students will learn to implement security policies that balance user accessibility with robust protection against modern threats.

	Key Term	Description
1	Mobile Device Management (MDM)	A comprehensive solution that allows organizations to remotely manage, configure, and secure mobile devices, enforcing policies and maintaining compliance across the enterprise mobile fleet
2	Trusted Execution Environment (TEE)	A secure area within a mobile device's main processor that runs in isolation from the standard operating system, providing hardware-based security for sensitive operations and data storage
3	Biometric authentication	Security methods that use unique biological characteristics such as fingerprints, facial features, or iris patterns to verify user identity on mobile devices
4	Application sandboxing	A security mechanism that isolates mobile applications from each other and system resources, preventing unauthorized access to data and limiting the impact of potential security breaches
5	Certificate pinning	A security technique where mobile applications are configured to only accept specific digital certificates, preventing man-in-the-middle attacks even if the device's certificate store is compromised
6	Mobile Application Management (MAM)	A targeted approach to securing and managing specific applications on mobile devices without requiring full device control, often used in Bring Your Own Device (BYOD) environments
7	Containerization	The practice of creating isolated environments on mobile devices that separate personal and corporate data, allowing secure access to business resources while maintaining user privacy
8	Remote wipe	A security feature that allows administrators to remotely delete all data from a lost or stolen mobile device, protecting sensitive information from unauthorized access
9	Secure boot	A security standard that ensures a device boots using only software that is trusted by the device manufacturer, preventing rootkits and other low-level malware
10	Data Loss Prevention (DLP)	Policies and technologies designed to prevent sensitive data from being copied, transmitted, or accessed in unauthorized ways on mobile devices
11	Multi-factor Authentication (MFA)	A security approach requiring two or more verification methods from different categories (something you know, have, or are) to access mobile device resources
12	Virtual Private Network (VPN)	An encrypted connection between a mobile device and a private network, ensuring secure data transmission over public or untrusted

	Key Term	Description
		networks
13	App wrapping	A mobile application management technique that adds a security layer around existing applications without modifying their source code, enabling policy enforcement
14	Jailbreaking/rooting	The process of removing software restrictions imposed by device manufacturers, which while providing additional functionality, significantly compromises device security
15	Mobile Threat Defense (MTD)	Advanced security solutions that provide real-time threat detection and response capabilities for mobile devices, protecting against malware, network attacks, and application vulnerabilities

30 Bird - Wireless Security Protocols and Authentication (Ch 6, Mod C)

Introduction

Objective

By completing this lab, you will be able to:

Wireless Security Fundamentals

- Understand wireless attack vectors and vulnerabilities.
- Compare encryption protocols and their effectiveness.
- Identify appropriate security measures for different scenarios.
- Recognize signs of wireless security breaches.

Protocol Implementation

- Configure WPA2 and WPA3 security settings.
- Implement enterprise authentication with RADIUS.
- Deploy certificate-based authentication.
- Manage pre-shared keys effectivel.

Advanced Wireless Security

- Understand 802.1X authentication framework.
- Configure guest network isolation.
- Implement MAC address filtering appropriately.
- Deploy wireless intrusion detection system.

Overview

This comprehensive theory lab provides in-depth knowledge of wireless security protocols and authentication methods—critical understanding for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1102 exam, you'll develop expertise in securing wireless networks, understanding encryption standards, and implementing authentication mechanisms that protect against evolving wireless threats.

Through guided reading and practical exercises, you'll master the evolution of wireless security from Wired Equivalent Privacy (WEP) through Wi-Fi Protected Access (WPA3), understand various authentication methods including enterprise implementations, and learn to configure secure wireless environments. This

knowledge is fundamental for IT professionals who must design, deploy, and maintain secure wireless networks in residential and enterprise settings.

	Key Term	Description
1	WPA3	Latest Wi-Fi security protocol with enhanced encryption
2	802.1X	Port-based network access control standard
3	RADIUS	Remote Authentication Dial-In User Service
4	EAP	Extensible Authentication Protocol framework
5	CCMP	Counter Mode with CBC-MAC Protocol encryption
6	SAE	Simultaneous Authentication of Equals in WPA3
7	TKIP	Temporal Key Integrity Protocol (deprecated)
8	PMK	Pairwise Master Key in WPA key hierarchy
9	Captive Portal	Web page for network access authentication
10	PEAP	Protected Extensible Authentication Protocol
11	Forward Secrecy	Protection of past sessions from future compromise
12	4-Way Handshake	WPA2 key establishment process
13	GTK	Group Temporal Key for broadcast traffic
14	WPS	Wi-Fi Protected Setup (vulnerable)
15	KRACK	Key Reinstallation Attack against WPA2

30 Bird - SOHO Malware Removal (Ch 6, Mod D)

Introduction

Objective

By completing this lab, you will be able to:

Malware Removal Process

- Implement the systematic seven-step malware removal methodology.
- Investigate and verify malware symptoms effectively.
- Quarantine infected systems to prevent spread.
- Execute proper remediation and system cleaning procedures.

Security Implementation

- Configure strong password policies and multi-factor authentication.
- Implement User Account Control and privilege management.
- Update software and operating systems for security patches.
- Manage firewall settings and network protection.

Recovery and Prevention

- Schedule automated security scans and monitoring.
- Enable system restore and create recovery points.
- Secure browser and email settings against future threats.
- Educate users on security best practices and threat recognition.

Overview

This hands-on lab provides comprehensive practice in implementing malware removal procedures for Small Office/Home Office (SOHO) environments—critical skills for information technology (IT) professionals and CompTIA A+ certification candidates. Covering objectives from the 220–1202 exam, you'll develop proficiency in the systematic approach to malware detection, quarantine, removal, and system recovery following established industry best practices.

Through guided exercises, you'll master the seven-step malware removal process including investigating symptoms, quarantining infected systems, disabling system restore, remediating infections, updating security software, scheduling scans, and educating end users. These skills are essential for maintaining system security in small business environments where dedicated IT security staff may be limited and comprehensive protection strategies are crucial.

	Key Term	Description
1	SOHO	Small Office/Home Office environment with limited IT resources
2	Malware Remediation	Process of detecting, isolating, and removing malicious software
3	System Quarantine	Isolation of infected systems to prevent malware spread
4	System Restore	Windows feature that reverts system to previous clean state
5	Boot Sector Virus	Malware that infects the system boot process
6	Rootkit	Malware that hides deep within the operating system
7	Windows Defender	Microsoft's built-in antivirus and anti-malware solution

30 Bird - Mobile OS and Application Troubleshooting (Ch 6, Mod D)

Introduction

Objective

By the end of this lab, students will be able to:

- Diagnose and resolve common mobile operating system issues including boot problems, system crashes, and performance degradation.
- Troubleshoot application-specific problems such as crashes, freezes, and compatibility issues.
- Use built-in and third-party diagnostic tools to identify root causes of mobile software problems.
- Perform safe mode troubleshooting and system recovery procedures on mobile devices.
- Analyze system logs and crash reports to identify problematic applications or services.
- Implement optimization techniques to improve mobile device performance and battery life.
- Resolve synchronization and connectivity issues between mobile devices and cloud services.
- Apply systematic troubleshooting methodologies specific to mobile platforms.

masterskill
education through innovation

aci LEARNING | SKILL LABS

Overview

Mobile operating systems and applications present unique troubleshooting challenges due to their diverse hardware configurations, frequent updates, and complex interaction between system services and third-party applications.

This lab provides comprehensive training in diagnosing and resolving common mobile OS and application issues across iOS and Android platforms. Students will develop systematic troubleshooting methodologies, learn to use diagnostic tools, and understand the underlying causes of mobile software problems to implement effective solutions.

	Key Term	Description
1	Kernel panic	A critical system error in the mobile operating system kernel that causes the device to stop functioning and typically triggers an automatic restart or recovery mode
2	Boot loop	A condition where a mobile device continuously restarts without successfully loading the operating system, often caused by corrupted system files or failed updates
3	Safe mode	A diagnostic startup mode that loads only essential system services and disables third-party applications, used to isolate software problems from system issues
4	Android Debug Bridge (ADB)	A versatile command-line tool that enables communication between a computer and an Android device for debugging, file transfer, and system modifications
5	Memory leak	A software bug where an application fails to release allocated memory after use, gradually consuming available RAM and degrading system performance
6	Force stop	An action that immediately terminates an application and all its associated processes, clearing it from memory and stopping any background services
7	Cache partition	A dedicated storage area on mobile devices that stores temporary files and frequently accessed data to improve performance, which can become corrupted and cause issues
8	Factory reset	A process that restores a mobile device to its original manufacturer settings, erasing all user data, applications, and configurations
9	Over-the-air-update (OTA)	A method of distributing operating system and software updates wirelessly to mobile devices without requiring physical connections or manual installation
10	Logcat	Android's logging system that collects and displays system debug output, including stack traces when applications crash and messages from applications
11	System image	A complete copy of the mobile operating system including all system files, drivers, and preinstalled applications, used for recovery and restoration purposes
12	Wake lock	A mechanism that prevents a mobile device from entering sleep mode, which can cause battery drain when applications fail to release wake locks properly
13	Dalvik/ART cache	Compiled application code stored by Android's runtime environment to improve performance, which may need clearing when experiencing application issues

	Key Term	Description
14	Crash reporter	A system service that collects information about application and system crashes, generating detailed logs for troubleshooting and debugging purposes
15	Thermal throttling	An automatic process where mobile devices reduce processor speed to prevent overheating, which can cause performance issues and application slowdowns

30 Bird - Mobile Security Issue Troubleshooting (Ch 6, Mod D)

Introduction

Objective

By the end of this lab, students will be able to:

- Identify common indicators of mobile device security compromise including unusual behavior patterns and performance anomalies.
- Use mobile security scanning tools and built-in security features to detect malware and vulnerabilities.
- Analyze permission abuse and identify potentially malicious applications through behavior analysis.
- Implement secure remediation procedures for compromised devices while preserving user data when possible.
- Troubleshoot authentication and encryption issues affecting device security.
- Diagnose and resolve mobile-specific attack vectors such as SMS phishing and malicious Wi-Fi networks.
- Perform security hardening procedures to prevent future compromises.
- Document security incidents and provide user education to prevent recurrence.

Overview

Mobile devices face an evolving landscape of security threats ranging from malware and phishing attacks to sophisticated exploits targeting operating system vulnerabilities. This lab focuses on identifying, diagnosing, and resolving security-related issues on mobile devices, including both reactive troubleshooting of active threats and proactive identification of security weaknesses. Students will develop skills in recognizing security breach indicators, using security assessment tools, and implementing remediation strategies while maintaining device functionality and user data integrity.

	Key Term	Description
1	Mobile malware	Malicious software specifically designed to compromise mobile devices, including viruses, trojans, spyware, and ransomware adapted for mobile platforms
2	Smishing	SMS-based phishing attacks that use text messages to trick users into revealing sensitive information or installing malicious applications
3	Jailbreak and root Detection	Security features that identify when device security restrictions have been removed, potentially exposing the system to additional threats
4	Certificate pinning bypass	An attack technique that circumvents application security by defeating certificate validation, enabling man-in-the-middle attacks
5	Mobile Threat Defense (MTD)	Comprehensive security solutions that provide real-time protection against various mobile threats including network attacks and application vulnerabilities
6	Stagefright	A category of vulnerabilities in Android's media processing libraries

	Key Term	Description
		that could be exploited through specially crafted MMS messages or media files
7	Banking Trojan	Sophisticated malware designed to steal financial credentials by overlaying fake interfaces over legitimate banking applications
8	Zero-click exploit	Advanced attacks that compromise devices without requiring user interaction, often targeting messaging or communication applications
9	SIM swapping	A social engineering attack where attackers transfer a victim's phone number to a SIM card they control, bypassing SMS-based authentication
10	Pegasus-type spyware	Advanced surveillance software capable of complete device compromise, often used in targeted attacks against high-value individuals
11	App side-loading	Installing applications from sources outside official app stores, which bypasses security reviews and increases malware risk
12	Overlay attack	Malware technique where malicious apps display fake interfaces over legitimate applications to capture sensitive information
13	Cryptojacking	Unauthorized use of mobile device resources to mine cryptocurrency, causing battery drain and performance issues
14	BlueBorne	A set of vulnerabilities in Bluetooth implementations that allow attackers to take control of devices without user interaction
15	Mobile forensics	The process of recovering and analyzing digital evidence from mobile devices while maintaining chain of custody for legal purposes

30 Bird - Personal Computer Security Troubleshooting (Ch 6, Mod D)

Introduction

Objective

By completing this lab, you will be able to:

Security Incident Investigation

- Troubleshoot network connectivity issues potentially caused by malware.
- Investigate suspicious desktop alerts and security warnings.
- Analyze false antivirus alerts and social engineering attempts.
- Identify and assess altered or corrupted system files.

System Recovery and Remediation

- Recover missing or renamed files from security incidents.
- Resolve unwanted notifications and system alerts.
- Diagnose and fix operating system update failures.
- Restore browser functionality after security compromises.

Performance and Stability Restoration

- Resolve browser redirection and hijacking issues.
- Diagnose and improve degraded browser performance.
- Remove random and frequent pop-up advertisements.
- Restore normal system operation after malware removal.

masterskill
education through innovation

aci LEARNING | SKILL LABS

Overview

This hands-on lab provides comprehensive practice in diagnosing and resolving personal computer security issues—critical skills for information technology (IT) professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in identifying security threats, analyzing suspicious system behavior, and implementing effective remediation strategies that restore system security and functionality.

Through guided exercises, you'll master essential security troubleshooting practices including network connectivity analysis, desktop alert investigation, antivirus validation, system file integrity checking, data recovery procedures, notification management, update failure resolution, browser security repair, performance optimization, and malicious pop-up removal. These skills are fundamental for maintaining secure computing environments and responding effectively to security incidents in professional settings.

	Key Term	Description
1	Malware infection	System compromise by malicious software affecting normal operation
2	Browser hijacking	Unauthorized modification of browser settings and behavior
3	False positive	Legitimate software incorrectly identified as malicious
4	System file corruption	Damage to critical operating system files affecting functionality
5	Adware	Software that displays unwanted advertisements and pop-ups
6	Browser redirection	Automatic forwarding to unintended websites
7	Rogue antivirus	Fake security software designed to deceive users
8	Network isolation	Disconnection from network resources due to security issues
9	Registry corruption	Damage to Windows registry database affecting system behavior
10	Performance degradation	Reduced system speed and responsiveness due to security issues
11	Pop-up blocker	Browser feature preventing unwanted advertising windows
12	Security alert fatigue	User desensitization to legitimate security warnings

30 Bird - SOHO Networking (Ch 7, Mod A)

Introduction

Objective

By completing this lab, you will be able to:

Router Configuration and Management

- Configure router administrative access and password security.
- Implement firewall rules and port forwarding configurations.
- Manage DHCP services and IP address assignment.
- Configure DMZ settings for network segmentation.

Network Security Implementation

- Enable router firewall protection and access controls.
- Implement MAC address filtering for device authentication.
- Configure content filtering and parental controls.
- Update router firmware for security patches.

Network Administration

- Assign static IP addresses for critical network devices.
- Monitor network traffic through router logs and analytics.
- Configure wireless security settings and access controls.
- Troubleshoot common SOHO networking issues.

Overview

This hands-on lab provides comprehensive practice in configuring and securing Small Office/Home Office (SOHO) networking equipment—critical skills for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in router configuration, network security implementation, and network management practices essential for small business environments.

Through guided exercises, you'll master essential SOHO networking practices including router password management, firewall configuration, port forwarding setup, Dynamic Host Configuration Protocol (DHCP) administration, static Internet Protocol (IP) assignment, Media Access Control (MAC) address filtering, Demilitarized Zone (DMZ) configuration, firmware updates, content filtering, and log analysis. These skills are fundamental for creating secure, reliable network infrastructures that support business operations while protecting against cyber threats and unauthorized access.

	Key Term	Description
1	SOHO router	Network device providing Internet connectivity and local network services
2	Default gateway	Router IP address that devices use to access external networks
3	DHCP server	Service that automatically assigns IP addresses to network devices
4	Port forwarding	Routing external connections to specific internal network devices
5	MAC address filtering	Security feature allowing only authorized devices to connect
6	DMZ	Demilitarized zone providing isolated network segment for servers
7	Firmware	Router's operating system software controlling device functionality
8	Content filtering	Feature blocking access to inappropriate or malicious websites
9	Static IP address	Manually assigned IP address that doesn't change automatically
10	Network address translation	Technology allowing multiple devices to share single public IP
11	Quality of service	Network traffic prioritization for optimal performance
12	Wireless security protocol	Encryption standard protecting wireless network communications

masterskill
education through innovation

aci LEARNING | SKILL LABS

30 Bird - Documentation and Asset Management Best Practices (Ch 8, Mod A)

Introduction

Objective

By the end of this lab, students will be able to:

- Create comprehensive technical documentation including network diagrams, system configurations, and standard operating procedures.
- Implement and maintain asset management systems that track hardware and software throughout their lifecycles.
- Develop knowledge base articles and troubleshooting guides that effectively capture and share technical knowledge.
- Design documentation templates and standards that ensure consistency across technical teams.
- Use documentation management tools and version control systems for collaborative documentation efforts.
- Establish asset tagging and tracking procedures that maintain accurate inventory records.
- Create disaster recovery documentation and runbooks for critical system restoration.
- Implement documentation review and update processes that ensure information remains current and accurate.

Overview

Effective documentation and asset management form the backbone of successful IT operations, enabling organizations to maintain accurate inventories, track changes, resolve issues efficiently, and ensure compliance with regulatory requirements.

This lab explores comprehensive approaches to creating, maintaining, and using various forms of IT documentation while implementing robust asset management systems. Students will learn industry best practices for documenting technical procedures, maintaining asset databases, and establishing documentation workflows that support both operational efficiency and strategic decision-making.

	Key Term	Description
1	Configuration Management Database (CMDB)	A centralized repository that stores information about IT assets and their relationships, enabling comprehensive understanding of infrastructure dependencies and supporting change impact analysis
2	Asset lifecycle management	The process of managing IT assets from initial planning and procurement through deployment, maintenance, and eventual retirement or disposal, optimizing value throughout each stage
3	Knowledge base	A structured repository of information containing solutions, procedures, and technical documentation designed to capture organizational knowledge and enable self-service problem resolution
4	Standard Operating Procedure (SOP)	Detailed, written instructions describing how to perform routine technical tasks consistently, ensuring quality and compliance regardless of who performs the work
5	Network diagram	Visual representation of network infrastructure showing devices, connections, and logical relationships, essential for understanding system architecture and troubleshooting connectivity issues
6	Runbook	Comprehensive documentation containing detailed procedures for system operations, incident response, and recovery processes, enabling consistent execution of critical IT tasks

	Key Term	Description
7	Asset tag	Unique identifier physically attached to IT equipment or logically assigned to software, enabling tracking throughout the asset lifecycle and maintaining accurate inventory records
8	Documentation taxonomy	Hierarchical classification system organizing documentation into logical categories and subcategories, facilitating information retrieval and maintaining consistency across document repositories
9	Version control	System for tracking changes to documentation over time, maintaining revision histories, and enabling rollback to previous versions when needed
10	Service catalog	Comprehensive listing of IT services available to users, including descriptions, service levels, request procedures, and associated costs, serving as the primary interface between IT and business users
11	Technical debt	The implied cost of additional rework caused by choosing limited solutions now instead of better approaches, including documentation shortcuts that complicate future maintenance
12	Single Source of Truth (SSOT)	Principle ensuring each piece of information is stored in exactly one location, eliminating confusion from conflicting documentation versions and ensuring consistency
13	Tribal knowledge	Undocumented information known only to specific individuals or groups, representing organizational risk when key personnel leave or become unavailable
14	Application Programming Interface (API) documentation	Technical specifications describing how to interact with APIs, including endpoints, parameters, authentication requirements, and response formats
15	Disaster Recovery Plan (DRP)	Comprehensive documentation outlining procedures, resources, and responsibilities for restoring IT services following catastrophic events, ensuring business continuity

30 Bird - Change Management Process Implementation (Ch 8, Mod A)

Introduction

Objective

By the end of this lab, students will be able to:

- Design and implement formal change management processes aligned with Information Technology Infrastructure Library (ITIL) best practices.
- Classify changes based on risk, urgency, and impact to determine appropriate approval paths.
- Create comprehensive change proposals including risk assessments, rollback plans, and success criteria.
- Facilitate Change Advisory Board (CAB) meetings and present technical changes to diverse stakeholders.
- Develop and execute change implementation plans that minimize service disruption.
- Implement emergency change procedures that balance speed with necessary controls.
- Perform post-implementation reviews to capture lessons learned and improve future changes.
- Use change management tools and automation to streamline processes while maintaining governance.

masterskill
education through innovation

aci LEARNING | SKILL LABS

Overview

Change management represents a critical discipline in IT operations that ensures modifications to technology systems occur in controlled, predictable ways that minimize risk while enabling business evolution. This lab explores comprehensive change management processes from initial request through implementation and post-change review. Students will learn to balance the need for technological advancement with operational stability, understanding how proper change management reduces incidents, improves success rates, and maintains stakeholder confidence in IT services.

	Key Term	Description
1	Change Advisory Board (CAB)	A group of stakeholders responsible for evaluating and approving changes based on risk assessment, business impact, and technical feasibility
2	Request for Change (RFC)	A formal proposal documenting a desired modification to IT systems, including justification, impact analysis, and implementation details
3	Standard change	Preapproved, low-risk changes following established procedures that can be implemented without CAB review, such as routine patches or password resets
4	Emergency change	High-priority modifications required to resolve critical issues or security vulnerabilities, following expedited approval processes with subsequent review
5	Change window	Scheduled time periods when changes can be implemented with minimal impact on business operations, often during nights or weekends
6	Rollback plan	Documented procedures for returning systems to their previous state if changes produce unacceptable results or fail to meet success criteria
7	Forward Schedule of Change (FSC)	A calendar showing all approved changes and their planned implementation dates, enabling coordination and conflict identification
8	Post-Implementation Review (PIR)	Formal evaluation conducted after change completion to assess success, identify issues, and capture improvement opportunities
9	Change model	Repeatable process templates for specific change types that standardize approaches and reduce planning effort for routine modifications
10	Configuration Item (CI)	Any component requiring management to deliver IT services, tracked through the change management process to maintain accurate configuration records
11	Impact analysis	Systematic evaluation of how proposed changes might affect systems, services, users, and business processes, informing risk assessment and planning
12	Change freeze	Temporary suspension of non-emergency changes during critical business periods or major events to ensure maximum stability
13	Remediation plan	Procedures for addressing issues discovered during or after change implementation without requiring full rollback to previous states
14	Technical review	Detailed evaluation of change technical aspects by subject matter experts to identify potential issues before CAB consideration
15	Change success rate	Key metric measuring the percentage of changes completed successfully without causing incidents or requiring rollback procedures

masterskill
education through innovation

aci LEARNING | SKILL LABS

30 Bird - Policy, Licensing, and Privacy Compliance (Ch 8, Mod B)

Introduction

Objective

By the end of this lab, students will be able to:

- Develop and implement IT policies that align with organizational objectives and regulatory requirements.
- Manage software licensing compliance including audits, true-ups, and various licensing models.
- Implement privacy protection measures compliant with regulations like GDPR, CCPA, and HIPAA.
- Design and maintain acceptable use policies (AUPs) that protect organizational resources while respecting user needs.
- Establish data classification systems and handling procedures ensuring appropriate protection levels.
- Create incident response policies addressing both technical and legal requirements for breach notification.
- Implement retention policies balancing business needs, legal requirements, and storage costs.
- Conduct compliance audits and maintain documentation demonstrating regulatory adherence.

Overview

Technology professionals must navigate complex landscapes of organizational policies, software licensing requirements, and privacy regulations that govern modern IT operations. This lab examines the critical intersection of technical implementation and regulatory compliance, focusing on how IT professionals ensure their organizations meet legal obligations while maintaining operational efficiency.

Students will learn to interpret and implement various compliance requirements, manage software licensing, protect personal data, and establish policies that balance security needs with business objectives and legal mandates.

	Key Term	Description
1	Acceptable Use Policy (AUP)	Document defining permitted and prohibited activities when using organizational IT resources, establishing behavioral expectations and consequences for violations
2	Software Asset Management (SAM)	Systematic approach to managing software throughout its lifecycle, ensuring license compliance while optimizing costs and reducing risks
3	General Data Protection Regulation (GDPR)	Comprehensive European Union privacy law establishing requirements for processing personal data and granting individuals specific rights over their information
4	Data Classification	Process of categorizing information based on sensitivity and required protection levels, enabling appropriate security controls and handling procedures
5	Privacy Impact Assessment (PIA)	Systematic evaluation of how proposed systems or processes might affect individual privacy, identifying risks and mitigation strategies
6	Right to be Forgotten	Legal concept allowing individuals to request deletion of their personal data under certain circumstances, also known as erasure rights
7	Data Processing Agreement (DPA)	Contract between data controllers and processors defining responsibilities and requirements for handling personal data in compliance with privacy regulations
8	License True-Up	Process of reconciling actual software usage with purchased licenses, identifying and remediating any compliance gaps or optimization

	Key Term	Description
		opportunities
9	Purpose Limitation	Privacy principle restricting use of personal data to purposes for which it was collected unless additional consent is obtained
10	Retention Policy	Formal guidelines determining how long different types of data should be kept and when it should be securely destroyed or archived
11	California Consumer Privacy Act (CCPA)	California state law granting consumers rights regarding their personal information and imposing obligations on businesses collecting such data
12	End User License Agreement (EULA)	Legal contract between software vendor and user defining terms of use, restrictions, and limitations of liability
13	Data Minimization	Privacy principle advocating collection and processing of only the minimum personal data necessary to achieve specified purposes
14	Audit Trail	Chronological record of system activities enabling reconstruction and examination of sequences of events for compliance verification
15	Legal Hold	Process preserving potentially relevant information when litigation or investigation is reasonably anticipated, suspending normal retention policies

30 Bird - Backup and Recovery Strategies (Ch 8, Mod C)

Introduction

Objective

This hands-on lab provides comprehensive practice in implementing backup and recovery solutions—critical skills for IT professionals and CompTIA A+ certification candidates. Covering objectives from the 220-1202 exam, you'll develop proficiency in various backup methodologies, recovery procedures, and data protection strategies essential for maintaining business continuity and protecting against data loss in professional environments.

Through guided exercises, you'll master essential backup and recovery practices including full system backups, incremental and differential backup strategies, automated scheduling, file restoration procedures, system state recovery, backup integrity testing, rotation schemes, documentation procedures, and offsite backup simulation. These skills are fundamental for ensuring data availability, minimizing downtime, and implementing comprehensive disaster recovery strategies.

Microsoft removed WINNT Backup starting with Windows 11, it is available for download and use with reduced functionality. Microsoft recommends backing up to OneDrive or using a 3rd party solution. We have chosen to use a commercial backup program that has backup functionality for demonstrating these backup features.

Overview

Learning Objectives

By completing this lab, you will be able to:

- Backup Strategy Implementation
- Perform full system backups for comprehensive data protection.
- Execute incremental and differential backup procedures.
- Schedule automated backup operations for consistency.
- Implement backup rotation schemes for long-term data retention.

Recovery and Restoration Procedures

- Restore individual files and folders from backup archives.
- Recover entire systems to previous operational states.
- Test backup integrity and verify restoration capabilities.
- Document backup and recovery procedures for operational continuity.

Data Protection and Management

- Simulate offsite backup procedures for disaster recovery.
- Implement backup testing and validation protocols.
- Establish backup retention policies and compliance requirements.
- Create comprehensive backup documentation and procedures.

Lab Task Overview

Task	Description
Perform a full system backup.	Create comprehensive backup of entire system.
Perform an incremental backup.	Execute backup of changed data since last backup.
Perform a differential backup.	Create backup of changes since last full backup.
Schedule automated backups.	Configure automatic backup operations.
Restore files from a backup.	Recover individual files and folders.
Test backup integrity.	Verify backup completeness and restoration capability.
Document a backup plan.	Create comprehensive backup procedures.

CompTIA A+ Objective Mapping

Task Area	Exam Objective Reference
Full system backup	1.0 Operating Systems
Incremental backup	4.0 Operational Procedures
Differential backup	1.0 Operating Systems
Automated scheduling	4.0 Operational Procedures
File restoration	1.0 Operating Systems
System recovery	1.0 Operating Systems
Backup testing	4.0 Operational Procedures
Documentation	1.0 Operating Systems

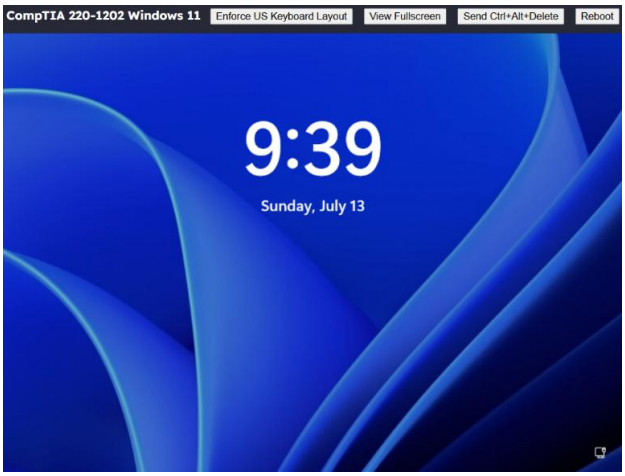
Getting Started

Before beginning the hands-on tasks, follow these steps to access your virtual lab environment:

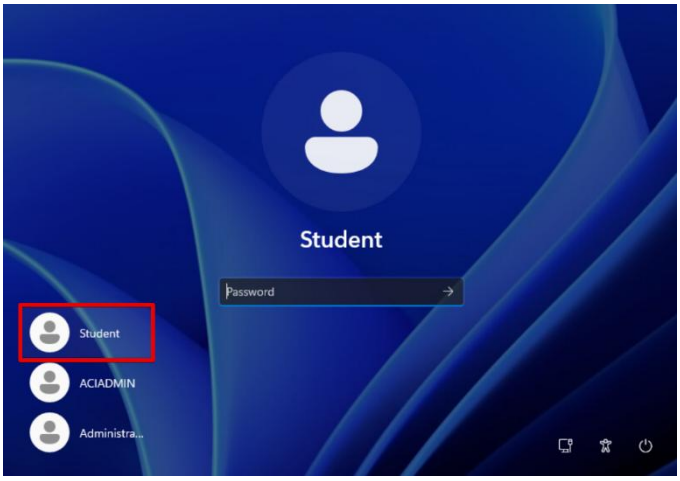
1. **Click** the Start button in your lab portal to provision the lab environment.

2. **Click** the computer image or Launch VM button in the right pane when the lab loads to open the Windows virtual machine window.

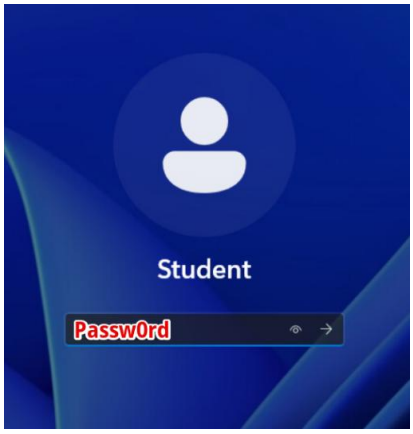
3. **Wait** for Windows 11 to finish booting. When you see the lock screen, **double-click** anywhere to reveal the login prompt.



4. **Select** the Student account (if prompted).



5. **Log in** with the password Passw0rd (case sensitive).



6. Once logged in, you are ready to begin the lab activities below.

If you encounter any issues starting the lab or logging in, notify your instructor for assistance.

Before you begin the hands-on tasks in this lab, you will gain practical experience implementing backup and recovery solutions that are critical for maintaining business continuity and data protection in professional environments. You will learn to create comprehensive backup strategies, test recovery procedures, and establish automated protection systems using real-world backup tools and methodologies. These skills are essential for preventing data loss, ensuring system availability, and meeting organizational compliance requirements. Mastery of these tasks directly aligns with CompTIA A+ exam objectives and prepares you for professional data protection responsibilities.

	Key Term	Description
1	Full backup	Complete backup of all selected data regardless of previous backups
2	Incremental backup	Backup of only data changed since the last backup of any type
3	Differential backup	Backup of data changed since the last full backup
4	Synthetic full backup	Reconstructed full backup created from existing backup components
5	Backup rotation	Systematic cycling of backup media to ensure data retention
6	Recovery point objective	Maximum acceptable data loss measured in time
7	Recovery time objective	Maximum acceptable downtime for system restoration
8	Grandfather-Father-Son	Traditional backup rotation scheme using three generations
9	3-2-1 backup rule	Best practice requiring 3 copies, 2 different media, 1 offsite
10	Backup integrity	Verification that backup data is complete and restorable
11	System state backup	Backup of operating system configuration and system files
12	Bare metal recovery	Complete system restoration to new or reformatted hardware

30 Bird - Safety Procedures and Environmental Controls (Ch 9, Mod B)

Introduction

Objective

By the end of this lab, students will be able to:

- Identify and mitigate electrical hazards including proper grounding, circuit protection, and lockout/tagout procedures.
- Implement proper ergonomic practices to prevent repetitive strain injuries and musculoskeletal disorders.
- Handle and dispose of hazardous materials including batteries, toner, and electronic waste according to regulations.
- Design and maintain appropriate environmental controls for temperature, humidity, and air quality in technology spaces.
- Use personal protective equipment (PPE) appropriately for various technical tasks and environments.

- Implement fire suppression and emergency response procedures specific to technology environments.
- Apply electrostatic discharge (ESD) prevention techniques when handling sensitive electronic components.
- Establish safety training programs and maintain compliance with occupational safety regulations.

Overview

Working with technology equipment requires comprehensive understanding of safety procedures and environmental controls to protect both personnel and equipment. This lab addresses the critical intersection of personal safety, equipment protection, and environmental responsibility in IT operations.

Students will learn to identify and mitigate physical hazards, implement proper handling procedures for sensitive equipment, and establish environmental controls that ensure optimal operating conditions while minimizing ecological impact. These skills are essential for IT professionals working in data centers, repair facilities, or any environment where technology equipment is deployed or maintained.

	Key Term	Description
1	Lockout/Tagout (LOTO)	Safety procedure ensuring equipment remains de-energized during maintenance by physically locking power sources and tagging them with worker identification
2	Ground Fault Circuit Interrupter (GFCI)	Electrical safety device that quickly disconnects power when detecting current leakage, preventing electrical shock injuries
3	Electrostatic Discharge (ESD)	Transfer of static electrical charge between objects at different potentials, potentially damaging sensitive electronic components
4	Arc Flash	Explosive release of energy caused by electrical faults, producing extreme heat, pressure waves, and blinding light requiring specialized protective equipment
5	Material Safety Data Sheet (MSDS)	Document providing detailed information about hazardous materials including composition, hazards, handling procedures, and emergency response measures
6	Personal Protective Equipment (PPE)	Safety gear including gloves, safety glasses, and protective clothing worn to minimize exposure to workplace hazards
7	Hot Aisle/Cold Aisle	Data center design pattern segregating equipment intake and exhaust air to optimize cooling efficiency and prevent hot air recirculation
8	Clean Agent Fire Suppression	Fire suppression systems using electrically non-conductive gases that extinguish fires without damaging electronic equipment
9	Dew Point	Temperature at which water vapor condenses into liquid, critical for preventing condensation damage in technology environments
10	Approach Boundary	Defined distances from energized electrical equipment determining required qualifications and protective equipment for personnel access
11	Emergency Power Off (EPO)	System allowing immediate disconnection of all power to a facility area during emergencies, required in many data center designs
12	Ergonomics	Science of designing workspaces, equipment, and procedures to optimize human well-being and overall system performance
13	VESDA (Very Early Smoke Detection Apparatus)	Highly sensitive smoke detection system using air sampling to identify fire risks before traditional detectors activate
14	Anti-static Wrist Strap	Grounding device worn during electronic work that safely dissipates static charges from the human body

	Key Term	Description
15	e-Waste	Discarded electronic equipment requiring special handling and recycling procedures due to hazardous materials and data security concerns