CA403: Windows Security

39 Instructional Hours 57 CPEs 18 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive introduction to the core components, architecture, and operational principles of the Windows operating system. It explores both theoretical concepts and practical administration tasks, including system architecture, command-line usage, graphical interface navigation, process and memory management, and virtualization. Learners will also gain insight into system startup processes, storage management, file systems, and security mechanisms such as BitLocker and Active Directory. The course is designed to build a strong foundational understanding of how Windows operates internally and how to manage, troubleshoot, and secure Windows-based environments effectively.

You Will Be Able To

- Explain Windows architecture, including kernel and user mode operations
- Use command-line tools and scripting to automate system tasks
- Manage processes, applications, and system performance using built-in tools
- Configure storage, file systems, and disk management features
- Analyze system logs and troubleshoot issues using Event Viewer
- Implement basic Windows security measures, including encryption and access control

Who Should Attend

This course is intended for beginners to intermediate learners who want to build a solid foundation in Windows operating systems. It is suitable for students, IT support staff, aspiring system administrators, and cybersecurity learners who need practical knowledge of Windows internals, system management, and security fundamentals. No prior advanced experience is required, but basic computer literacy is recommended.

Relevant Combat Roles

- Windows System Administrator
- IT Support Specialist
- SOC Analyst (Tier 1)
- Cybersecurity Analyst

Topics Covered

Core system architecture & operation: Windows architecture (kernel, processes, threads, HAL), startup/boot process (BIOS, UEFI, Boot Manager, WinRE), and overall system components

User interaction & interfaces: Command-Line Interface (CLI), command shell with I/O redirection, and Graphical User Interface (GUI) including Windows 11 system applications

Process & performance management: Process management, Task Manager usage, and system performance monitoring tools

Storage & file systems: Storage management (basic/dynamic disks, storage spaces, disk tools) and file systems (NTFS, FAT, exFAT) with related utilities

System monitoring & automation: Event logging with Event Viewer and PowerShell fundamentals including basic scripting

Security & enterprise features: Windows security concepts (BitLocker, UAC, firewall basics), virtualization with Hyper-V, and Active Directory basics with authentication (Kerberos overview)

Labs

Windows Command-Line Operations & Automation
(Command Prompt usage, I/O redirection, piping, command chaining, scripting, and task automation with cmd)

Windows Performance & Process Analysis
(Task Manager monitoring, process management, startup analysis, CPU/memory utilization, and Performance Monitor diagnostics)

Windows Logging & Troubleshooting
(Event Viewer usage, event filtering, Security/Application/System log analysis, Event ID investigation, and troubleshooting workflows)

Windows Identity & Access Management
(Active Directory deployment, domain controller configuration, OU/user/group management, Kerberos authentication, and Group Policy administration)

Windows Account Administration & Credential Management
(User account provisioning, password resets, administrative account control, permissions, access tokens, and authentication management)

PowerShell Administration & Automation
(PowerShell cmdlets, scripting fundamentals, loops, conditional logic, automation workflows, environment variables, and Windows configuration management)