COURSE SYLLABUS

Windows and Active Directory Security Fundamentals Course (Self-Paced)

Learn how Windows and Active Directory secure users and computers, and how to spot where a real environment falls short.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/windows-active-directory-security-course-self-paced

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Windows Security Fundamentals: Accounts and Local Security

- Lessons:
  - The Windows Security Model at a Glance
  - Local Accounts versus Domain Accounts
  - Local Security Policy and Where to Find It
- Applied activity: Learners review a screenshot of the Local Security Policy console and identify which setting controls a described security requirement, such as password complexity or account lockout.

Module 2: Introduction to Active Directory: Domains, Forests, and Objects

- Lessons:
  - What Active Directory Actually Manages
  - Domains, Trees, and Forests
  - Organizational Units and Directory Objects
  - A Guided Look at Active Directory Users and Computers
- Applied activity: Learners review a screenshot of an Active Directory Users and Computers console and identify the organizational units, user objects, and computer objects shown, then describe how the structure reflects the organization.

Module 3: Users, Groups, and Permissions in Active Directory

- Lessons:
  - Creating and Managing User Accounts
  - Security Groups versus Distribution Groups
  - Nesting Groups and Why It Matters
  - Assigning Permissions the Right Way
- Applied activity: Learners review a short, described group membership structure, including nested groups, and determine which users end up with access to a sensitive resource, then flag anything that violates least privilege.

Module 4: Group Policy Fundamentals

- Lessons:
  - What Group Policy Does and Why It Exists
  - Group Policy Objects and How They Are Linked
  - Reading a Group Policy Management Console Screenshot
  - Common Security Settings Managed Through Group Policy
- Applied activity: Learners review a screenshot of the Group Policy Management Console showing several linked GPOs and determine, for a described user in a specific organizational unit, which policies apply and in what order.

Module 5: Authentication in Windows and Active Directory

- Lessons:
  - How Windows Authentication Works, at a Conceptual Level
  - Kerberos: The Default Authentication Protocol
  - NTLM and Why It Still Matters
  - Multifactor Authentication in a Windows Environment
- Applied activity: Learners review a short, simplified description of a login event and identify whether Kerberos or NTLM was most likely used, based on the details given.

Module 6: Securing Windows Endpoints: Hardening Basics

- Lessons:
  - What Hardening Means for a Windows Endpoint
  - Patch Management and Why It Cannot Be Skipped
  - Reducing the Attack Surface: Unused Services and Software
  - Windows Defender and Built-In Security Tools
- Applied activity: Learners review a short, described list of services and software running on an endpoint and identify which ones should likely be disabled or removed to reduce attack surface, and why.

Module 7: Zero Trust versus Traditional Perimeter Security

- Lessons:
  - The Traditional Model: Trust Inside the Perimeter
  - Why the Traditional Model Breaks Down
  - Zero Trust Principles in a Windows and Active Directory Context
  - Comparing the Two Models Side by Side
- Applied activity: Learners review a short scenario in which an attacker compromises one workstation and evaluate how far that attacker could move under a traditional, perimeter-trusted model versus a zero trust model applied to the same Active Directory environment.

Module 8: Common Weaknesses and Defensive Best Practices

- Lessons:
  - Common Active Directory Misconfigurations
  - Privileged Account Hygiene
  - Building a Defensible Baseline: A Recap
- Applied activity: Learners review a short, described Active Directory environment with several common misconfigurations and identify at least three, explaining the risk each one creates.