SPECTEROPS
Creators of BloodHound

TRAINING

ADVERSARY PERSPECTIVES

Active Directory

Real Results

- **A foundational understanding of how AD works**
- **A look at AD through the eyes of an adversary**
- **An understanding of how and why misconfigurations are introduced into AD**
- **An understanding of how misconfigurations can lead to data and asset compromise**

Dig into Active Directory! This course will help you roll up your sleeves and get hands-on with Active Directory (AD), enabling participants to gather answers directly when questions surrounding their organization's AD architecture arise in the future.

Learn AD components, not only how they work together, but also how they can work against your organization's security posture. Countless organizations leverage AD to provide the foundation or entirety of their production environment's identity and access management. But widespread usage doesn't mean AD is simple; beyond its architecture and design considerations lie security implications that can directly impact your organization.

Adversary Perspectives: Active Directory details key components of AD technology and architectures, focusing on the security implications of each.

We'll cover physical and logical components, forests and domains, Kerberos, and various tooling like ADUC—all from a security perspective. Course participants will get hands-on experience enumerating the architectures and security controls of a live Active Directory environment and will then analyze the data extracted.

What will you teach that students can't get elsewhere?

Adversary Perspectives: Active Directory is designed to provide students with a foundational understanding of Active Directory and how to secure it effectively. Students will be exposed to practical examples of common mistakes organizations make that introduce misconfigurations into an AD environment. This course **focuses on how a series of misconfigurations can turn into an attack path that an adversary can leverage** to compromise your most critical assets. Once the student understands attack paths, we provide the foundation to eliminate those issues with Attack Path Management.

DAY 1

Introduction
Physical and Logical Overview
Accounts and Access
LDAP
Groups
Forests and Domains

DAY 2

AD Security Principles and Models
Kerberos
Kerberos Delegation
Identifying Misconfigurations
AD Degradation
Attack Paths

Why isn't this material taught in other places?

This course focuses on avoiding the issues that create attack paths in the first place. SpecterOps has the technical depth to fully understand how these attack paths work, so specific guidance is delivered on how to avoid them all-together.

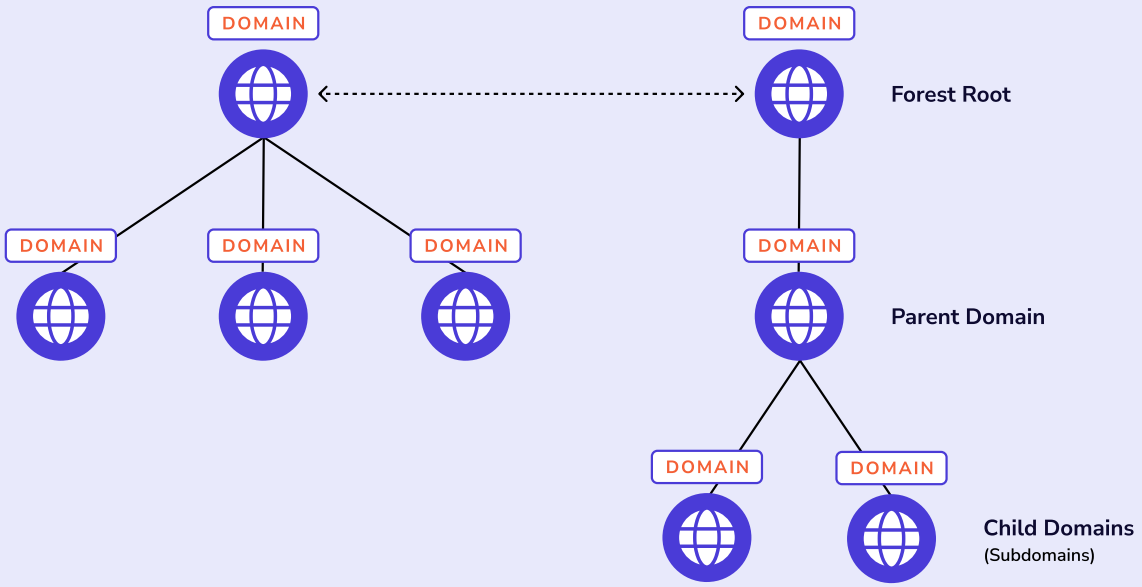
Who should take your courses?

- **Offensive and defensive security professionals** that are interested in or need a fundamental introduction to AD and its basic security principles
- **Identity and Access Management team members** who have administrative responsibilities over an AD environment

Stop being passive with your Active Directory! Kerberos, ADUC, Golden Tickets, Security Principals—have you come across these or similar words in penetration test reports or security bulletins and felt a little... lost? AD comprises many components that fulfill complex architectural requirements but can also open cracks through which attackers may slip. **Adversary Perspectives: Active Directory demystifies the various AD components and illustrates how these components can potentially introduce risks to your organization.**

This course empowers network defenders to directly look under the hood of their AD architecture and understand their environment better than attackers. Instructors share their knowledge and personal experiences testing AD in hundreds of environments to reveal not only common pitfalls in securing their environment but also how they commonly occur.

Forests and Domains



Why SpecterOps

Email info@specterops.io

Learn more at specterops.io

SpecterOps is at the forefront of researching and educating the industry on the risks associated with Active Directory. ADCS, SCCM, and ACE attack path research all originated from the SpecterOps team. We also release a series of tools, freely available to the community, to help educate folks on adversary tradecraft and empower people to reduce risk in their environments.

©2026 Specter Ops, Inc.