SPECTEROPS
Creators of BloodHound

TRAINING

ADVERSARY TACTICS

Identity-Driven Offensive Tradecraft

Participants Will Learn

- How to use Clean Source Principle (CSP) analysis to methodically identify violations and discover both known and new attack paths
- How to abuse on-premises and hybrid identity architectures for lateral movement and privilege escalation in complex enterprise environments
- How to master various authentication and authorization mechanisms and execute elaborate attacks abusing them and their security dependencies for privilege escalation and system access to achieve red team objectives

Identity has become the connective thread across modern hybrid environments, making identity-driven attacks one of the most critical threat vectors organizations face today. Traditional network-based security approaches fail when attackers abuse authentication and authorization mechanisms to move laterally across on-premises and cloud boundaries. This advanced course equips red teamers and offensive security professionals with techniques to discover and exploit identity attack paths in complex environments—from familiar Active Directory weaknesses to cutting-edge cloud and supply chain attacks. Developed by practitioners who execute real-world identity assessments, this course teaches the methodology for identifying both known attack paths and discovering new primitives across diverse technology stacks.

As modern architecture increasingly shifts services and data from on-premises infrastructure to the cloud, identity becomes the thread that ties everything together. Adversary Tactics: Identity-driven Offensive Tradecraft is a follow-on to our Adversary Tactics: Red Team Operations course and offers an in-depth look at identity-driven attacks, targeting both on-premises and hybrid identities. Participants learn how to abuse the intricacies of different authentication and authorization mechanisms to traverse on-premises and cloud environments, gain access to integrated systems, and even cross tenants. Participants are equipped with a practical approach to identifying known attack paths and forging new ones within complex operational environments and across people, processes, and technology. **Technologies covered include Kerberos, NTLM, ADCS, ADFS, SAML, Okta, Entra ID, OAuth, Azure, and hybrid identities.** In typical SpecterOps fashion, "Red vs. Blue" discussions are incorporated into lectures to provide students with the defender's perspective and detection logic, as well as OPSEC considerations to counter them. A defender will also actively "hunt" students in the lab to push them to improve their tradecraft by making educated decisions.

DAY 1 →

Introduction

Attack Path Theory and The Clean Source Principle

Kerberos Delegation Abuse

Computer Authentication Coercion

DAY 2 →

NTLM Attacks

User Authentication Coercion

ADIDNS Tradecraft

ADCS Introduction

ADCS Abuse

Shadow Credentials

DAY 3 →

SAML Attacks

ADFS Tradecraft

Configuration Manager (SCCM) Attacks

Introduction to Okta

Okta Abuse

DAY 4

OAuth Introduction and Abuse

Entra ID and Hybrid Identities

Devices Identities and PRTs

Azure RM

Microsoft Graph

Cross-Tenant Attacks

Student Requirements

Students should have proficiency in the following:

- Windows and Active Directory fundamentals
- Operating through a C2 agent
- Payload generation
- Lateral movement techniques
- Credential abuse on Windows systems

Completion of the Adversary Tactics: Red Team Operators course is highly recommended but not strictly required.

Hardware Requirements

Participants must provide their own computer with a modern web browser installed to access training materials and complete the course's labs. All course materials and labs are hosted in the SpecterOps training portal; there are no local virtual machines or special software required to fully participate in the course or labs.

What's Included

During the course, participants will be provided access to a comprehensive range to perform course labs and goals.

Upon completion of the course, participants are provided with a copy of course slides, cheat sheets, and walkthroughs.

Email info@specterops.io

Learn more at specterops.io

Why SpecterOps

SpecterOps specializes in the identity systems that connect modern enterprise environments. By analyzing how authentication and authorization mechanisms are abused across on-premises, hybrid, and cloud security boundaries, our team uncovers the attack paths adversaries rely on. This work includes widely adopted research and tooling around ADCS, Active Directory, SCCM, and Entra ID that helps the security community better understand and defend against identity-driven attacks.