TRAINING

SPECTEROPS

ADVERSARY TACTICS
RED TEAM OPERATIONS

As organizations work to keep from becoming the next breach headline, they are increasingly looking to exercise their defenses through simulation of the sophisticated attackers they now face. Organizations that have started to adopt an "assume breach" mentality understand that it's not a matter of if they're compromised by these adversaries, but when. The best way to test enterprise security operations against advanced threat actors is through red team exercises that leverage the same tactics, techniques and procedures (TTPs) as the adversaries themselves. If you're looking to learn the tradecraft of adversary simulation operations in enterprise environments, sharpen your offensive technical skillset, and understand how to detect modern advanced threat actor tradecraft, this is the course for you.

This intense course immerses students in a single simulated enterprise environment, with multiple networks, hardened endpoints, modern defenses, and active network defenders responding to red team activities. We will focus on in-depth attacker tradecraft post-initial access; braking out of the beachhead, establishing resilient command and control (C2) infrastructure, gain situational awareness through opsec aware host and network enumerations, perform advanced lateral movement and sophisticated Active Directory escalation, gain persistence (userland, elevated, and domain flavors), and perform advanced Kerberos attacks, data mining, and exfiltration.

A focus will be on "offense-in-depth", i.e. the ability to rapidly adapt to defensive mitigations and responses with a variety of offensive tactics and techniques. To drive this concept home, students will go up against live incident responders that will actively hunt for and block malicious activity in the environment. The responders will provide real-time feedback to students to demonstrate what artifacts attackers can leave behind, and how students can adapt their tradecraft to minimize their footprint. Come learn to use some of the most well-known offensive tools from the authors themselves, including co-creators and developers of PowerView, PowerShell Empire, Covenant, Apfell, Rubeus, GhostPack, and BloodHound.

DAY 1
- Introduction & Course Overview
- Lab & Course Range Infrastructure
- Red Team Operations
- Attack Infrastructure
- Host Situational Awareness
- PowerShell Weaponization
- Privilege Escalation

DAY 2
- An Introduction to Hunting
- Credential Abuse
- AD Situational Awareness
- Payload Methodology
- Pivoting and Lateral Movement
- SQL Abuse

DAY 3
- Opsec Considerations
- Domain Trusts
- Kerberos
- Golden Tickets
- Silver Tickets and Forged Ticket Detection

DAY 4
- Visualizing Attack Paths with BloodHound
- DPAPI
- Kerberos Delegation Abuse
- CTF and Capstone Conclusion
- Lab Debrief
- Defensive Debrief

TRAINING

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

We don't teach techniques—we teach tradecraft. Our course teaches the basics of how to execute Attack Paths or use offensive tools, but we also delve into the technological and operational theory behind them, helping the students understand how to operate and why rather than simply what to do. In a true "Red vs. Blue" fashion, we enlighten our students with the defender's perspective in the lectures and practical exercises, from detection and evasion logic to actively hunting students in the lab, pushing them to improve their tradecraft by making educated decisions.

Why isn't this material taught in other places?

Most courses focus solely on the practical aspects of executing attack techniques and lack the technical theory, operational context, and defensive perspective that make our Adversary Tactics: Red Team Operations course unique.

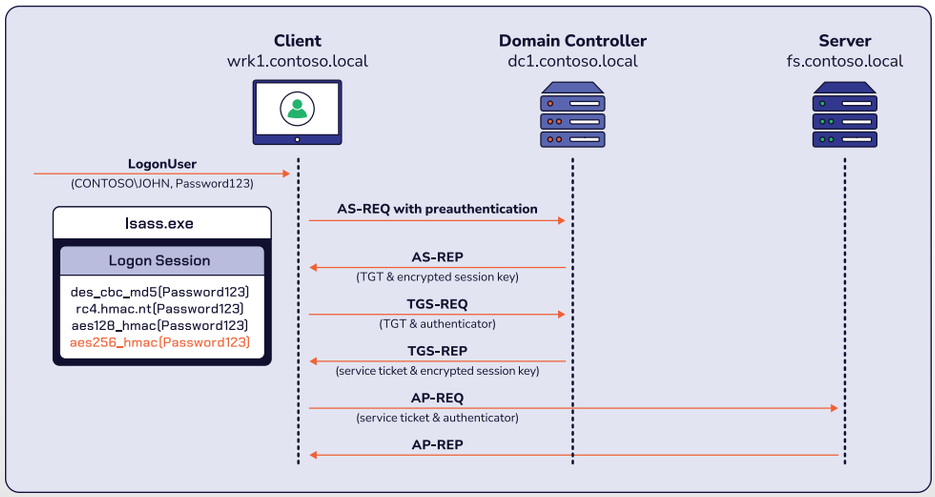
Who should take your courses?

- Red team operators seeking to solidify their understanding of red teaming concepts and tradecraft and become "enlightened actors" who understand the impact of each action performed and make risk-based decisions.
- Penetration testers seeking to utilize their offensive security skills to transition to covert red team operator roles.
- Blue teamers and general security practitioners seeking to gain an insight into adversary tactics and the offensive side.

Why SpecterOps?

SpecterOps is the organization who brought Red Team concepts into the commercial market, not just in concept, but through widely available tooling and content used by most providers today. Tools like BloodHound, Mythic C2, and Ghostwriter are in every offensive providers' arsenal. When we say leaders in offensive security, we mean it.

Kerberos Authentication Process Summary



REAL RESULTS

Students will learn the theoretical and practical considerations for planning a red team engagement and designing effective attack infrastructure and payloads.

Students will learn to apply a data-driven approach to making educated, risk-based tradecraft decisions to reduce the likelihood of detection.

Students will learn to identify and traverse Attack Paths in Active Directory/Windows environments.

Students will become familiar with a wide arsenal of attack tools and tradecraft alternatives for executing common TTPs and maneuvering toward the red team objectives.

Students will become proficient at common adversary tactics and be able to discuss the detectable artifacts they generate and applicable defensive mitigating controls.

SPECTEROPS

Learn more at **specterops.io**

Email **info@specterops.io**