TRAINING

SPECTEROPS

ADVERSARY TACTICS
TRADECRAFT ANALYSIS

Knowledgeable detection engineers and red team operators know that while there are many effective products, all of them have gaps that can be exploited by a sophisticated adversary. A mature security program must continuously test and enhance product detection configurations to have an effective response capability. Unfortunately, they often run into a number of limitations, primarily in a lack of understanding of the:

1. attack technique itself
2. telemetry used for each detection
3. effectiveness of the detection

The result often leads to blind spots within the detection and response capabilities, ineffective detection strategy, and a false sense of security in the organization's ability to respond to advanced threat actors. When simulating sophisticated attacks, red team operators need to truly understand how a given technique works, the telemetry/artifacts it generates, and the strategies and biases that a defender might use to detect a technique. How organizations may respond to attackers is crucial in red team attack planning, technique selection, and evasion.

In Adversary Tactics: Tradecraft Analysis, we will present and apply a general tradecraft analysis methodology for offensive TTPs, focused on Windows components. We will discuss Windows attack techniques and learn to deconstruct how they work underneath the hood. For various techniques, we will identify the layers of telemetry sources and learn to understand potential detection choke points. Finally, the course will culminate with students creating their own technique evasion and detection strategy. You will be able to use the knowledge gained to both use your telemetry to create robust detection coverage across your organization, and truly assess the efficacy of that coverage.

Whether you are a red team operator or detection engineer, you will have a comprehensive understanding of several attack chains. Red team operators will learn an approach to analyzing their own tools, a better understanding of which techniques to select to evade detection, and how to better describe to defenders why an evasion was successful. Detection engineers will understand how to craft a strategy to create robust detections and better detect families of attacks.

DAY 1
- Attack and Detection Strategies
- Naive PSExec Overview
- Tradecraft Analysis Process
- Capability Identification
- Capability Deconstruction
- IPC Mechanisms

DAY 2
- Securable Objects
- Identifying Choke Points
- Telemetry Source Identification
- How EDR Tools Work
- Organic Logging
- SACLs
- Function Hooking
- Kernel Callback Functions
- ETW

DAY 3
- Operationalizing Telemetry
- Understanding Attacker Controlled Fields
- Operationalizing Detection Research
- Operationalizing Evasion Research
- Understanding the Triage, Investigation, and Remediation Process
- Evading the Response Process
- Documentation & Evaluation Metrics
- Detection Documentation
- Evasion Documentation

DAY 4
- Defensive Capstone
- Offensive Capstone

TRAINING

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

Advances in defensive capability provided by stock/default configurations have made it increasingly difficult for red team operators to rely on capabilities provided by red team toolsets to avoid detection. On the other hand, reliance on stock product detection configurations often leads to blind spots within the detection and response capabilities, ineffective detection strategy, and a false sense of security in the organization's ability to respond to advanced threat actors. Utilizing operational approaches SpecterOps had developed in our red team operations and detection development programs this course will present: a general tradecraft analysis methodology for offensive TTPs, deconstruct how they work underneath the hood, identify the layers of telemetry sources and learn to understand potential detection choke points, and how red team operators can use this knowledge to develop evasion strategies. This course is meant as a follow-on to our popular Adversary Tactics: Red Team Operations and Adversary Tactics: Detection, diving deep into technical aspects of several attack techniques and Windows internals within the context of a general tradecraft analysis methodology, and meant for expert operators and analysts looking to craft robust detection and evasion strategies.

Why isn't this material taught in other places?

SpecterOps consultants have a level of technical depth required to understand the building blocks of adversary tradecraft. Not only do we understand the tradecraft, but we are able to make it accessible to others via blogs, tools, and this training course.

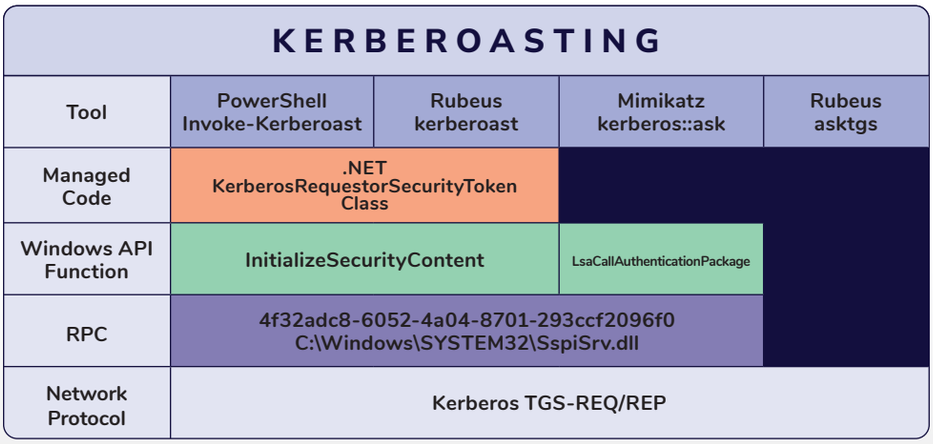
Who should take your courses?

This course is intended for expert blue teamers, detection engineers, and red team operators. Participants should be familiar with detection engineering and/or red team operations, and be generally comfortable with Windows internals, attack technique analysis, offensive tools and techniques

Why SpecterOps?

SpecterOps demystifies adversary tradecraft by understanding the foundational building blocks of an attack. Members of our team think differently about attacks and pioneered concepts around tradecraft deconstruction through our "Capability Abstraction" blog series. The same concepts allow our team to talk about effective mitigations against adversary techniques in every blog post and conference presentation that we give.

Capability Abstraction



Your organization has just implemented the leading detection and response products. Are they configured with default configuration? How much faith should you have in your ability to detect sophisticated attacks? How would you simulate attacks to ensure robust detections are in place? This course will teach the importance of understanding the inner workings of attack techniques and telemetry availability and provide a workflow for developing robust detection analytics or data driven evasion decisions. Focusing on various Windows components and attacker TTPs, you will dive deep into how software abstracts underlying capabilities and how attackers can interact with deeper layers to bypass superficial detection capabilities.

REAL RESULTS

An in-depth understanding of the inner workings of various Windows component attacker TTPs and detection telemetry availability.

A practical approach and workflow for developing robust detection analytics or data driven evasion decisions.

An approach for red team operators to analyze how their tools trip detection logic, and a better understanding of how to utilize techniques more likely evade detection.

SPECTEROPS

Learn more at **specterops.io**

Email **info@specterops.io**