Course Title:

Red Team Tactics: Tooling, Evasion & Strategy

INSTRUCTORS:

Instructional Designer / Senior Security Consultant Chris Truncer

Principal Security Consultant Mike Saunders

Senior Security Consultant Corey Overstreet

Description: Modern day attackers are tirelessly developing new tradecraft and methodologies that allow them to successfully compromise hardened targets. While it may look easy from the outside, there are many steps hidden from view that attackers take to ensure their success.

This class will cover the advanced challenges that red teamers consistently face and provide techniques to succeed in formidable scenarios. You will start with no information, build a profile on your target, persist within their environment, bypass modern defenses, and achieve the goals of your test.

This course is designed for attendees who have experience performing red team assessments and want to take their skillset to the next level. You will learn the latest techniques that modern attackers are using today and test yourself in an environment that is based off real-world networks and defenses.

COURSE OUTLINE	
Introduction	The introduction will highlight the topics of the course, the course agenda, class requirements, a description of what red teaming is, and final notes before the class begins!
Command and Control Options	The command and control options will discuss various C2 tools that can be used on red team assessments but will primarily focus on Cobalt Strike. We will discuss various listeners and students will configure their own.
Malleable Profiles	We will cover all the malleable profile options that you can use on your assessments to help prevent your beacons from being discovered. This includes network indicators, modifying the staging process, changing default beacon behavior, and modifying in-memory indicators.
Command and Control Configuration	Command and Control configuration will discuss best practices for building (and defending) your C2 infrastructure. This will cover purchasing domains, building domain reputation, domain fronting, and protections with mod_rewrite. This section will conclude by reviewing Cobalt Strike's

	Resource Kit and cover normal Cobalt Strike usage.
Aggressor Scripting	The aggressor scripting section will begin by covering Aggressor's origin and exploring basic functions. We'll discuss scenarios where Aggressor scripts can help augment your team by automating common steps, followed by coding these scripts. This will cover most stages of the attack lifecycle and we'll help build and provide scripts to all students.
OSINT	The open-source intelligence gathering section will cover sources and techniques for capturing useful data without ever interacting with customer infrastructure. We're going to look at network information, DNS records, Just-Metadata, e-mail address gathering, and more.
Active Recon	Active recon documents methods to capture information about your target when you will be directly interacting with their infrastructure, resources, etc. We'll discuss live host identification, NMap timing strategy, subdomain enumeration, e-mail address validation, and sweeping active web servers.
Phishing	The phishing section will discuss all of the phishing processes starting with properly standing up phishing infrastructure and testing delivery methods. We'll discuss scenario development, common scenarios

	that work well, and finally spend considerable time on developing phishing malware.
Application Allowlisting	The application allowlisting section will cover all major application allowlisting bypasses that have been recently published. We'll also weaponize each application allowlisting bypass for use on red team assessments.
Antivirus Evasion	Anti-virus evasion will cover a variety of shellcode injection techniques, and the various Windows API calls which make it possible, what stagers are and how they work, past cases of developing bypasses for anti-virus signatures, and customizing your malware to be extremely targeted.
EDR Evasion Overview	There are multiple options that attackers can use to bypass different EDR solutions that are available on the market today. This section will highlight how EDRs attempt to identify malicious behavior, how you can try to circumvent detection, and provide links to useful code for performing this task.
Persistence	The persistence section will be a massive library of persistence techniques, both old-school and new school in nature. We'll cover both user and admin level persistence techniques.
Initial Access, Recon, and Lateral Movement	The initial access portion will discuss the first steps you should take after receiving

	a callback. We'll investigate PowerShell and how to use it for assessments (or more specifically, System.Management.Automation.dll), mapping trusts from one domain to another, and different techniques to laterally move from one system to another.
Attacking the Cloud	The attacking the cloud section will focus on different cloud assets that teams may encounter during a red team assessment. The section will cover various cloud providers (AWS and Azure) along with different tools and techniques that can be used to identify misconfigurations and exploit them within a cloud environment.
Finalizing the Assessment	The class will end with a discussion about different methods of finalizing a red team assessment. Typically, this results in your POC asking you to gain access to specific data, etc. But what happens if you are unable to accomplish the objective? What happens if you do accomplish the objective, but the data is too sensitive to extract from your customer's network? We'll look into other alternatives that will still provide value to the customer. We'll end with everyone's favorite section: customer management techniques.