SEC699: Purple Team Tactics – Adversary Emulation for Breach Prevention and Detection

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Build a purple team in your organization
- Build realistic adversary emulation plans to better protect your organization
- Develop custom tools and plugins for existing tools to fine-tune your red and purple teaming activities
- Deliver advanced attacks, including application whitelisting bypasses, cross-forest attacks (abusing delegation), and stealth persistence strategies
- Building SIGMA rules to detect advanced adversary techniques

Prerequisites

- This is a fast-paced, advanced course that requires a strong desire to learn advanced red and blue team techniques. The following SANS courses are recommended either prior to or as a companion to taking this course: SEC599 and SEC560.
- Experience with programming in any language is highly recommended. At a minimum, students are advised to read up on basic programming concepts.
- You should also be well versed with the fundamentals of penetration testing prior to taking this course. Familiarity with Linux and Windows is mandatory. A solid understanding of TCP/IP and networking concepts is required. Please contact the author at **evanbuggenhout@nviso.be** if you have any questions or concerns about the prerequisites.

""I've been in this field a long time, and I've learned something new from each segment of SEC699. That's not something I'm used to at this point in my career."

— Taya Steere, **Lyft**

SEC699 is SANS' advanced purple team offering, with a key focus on adversary emulation for data breach prevention and detection. Throughout this course, students will learn how real-life threat actors can be emulated in a realistic, enterprise, environment. In true purple fashion, the goal of the course is to educate students on how adversarial techniques can be emulated and detected.

A natural follow-up to SEC599, this is an advanced SANS course offering, with 60 percent of class time spent on labs. Highlights of class activities include:

- A course section on typical automation strategies such as Ansible, Docker and Terraform. These can be used to deploy a full multi-domain enterprise environment for adversary emulation at the press of a button.
- Building a proper process, tooling, and planning for purple teaming
- Building adversary emulation plans that mimic real-life threat actors such as APT-28, APT-34, and Turla in order to execute these plans using tools such as Covenant and Caldera
- Building a proper process, tooling, and planning for purple teaming
- In-depth techniques such as Kerberos Delegation attacks, Attack Surface Reduction/ Applocker bypasses, AMSI, Process Injection, COM Object Hi-jacking and many more
- SIGMA rule-building to detect the above techniques
- A spectacular capstone that pits red and blue against one another. While red attempts to infiltrate the organization, blue builds a detection capability to detect adversary techniques.

Course authors Erik Van Buggenhout (the lead author SEC599) and James Shewmaker (the co-author SEC660) are both certified GIAC Security Experts (GSEs) and are hands-on practitioners who have built a deep understanding of how cyber attacks work through both red team (penetration testing) and blue team (incident response, security monitoring, threat hunting) activities. In this course, they combine these skill sets to educate students on adversary emulation methods for data breach prevention and detection.

The six-part SEC699 journey is structured as follows:

- In Section 1, we will lay the foundations that are required to perform successful adversary emulation and purple teaming. As this is an advanced course, we will go in-depth on several tools that we'll be using and learn how to further extend existing tools.
- Sections 2 to 4 will be heavily hands-on lecturing a number of advanced techniques and their defenses (focused on detection strategies). Section 2 focuses on Initial Access techniques, Section 3 covers Lateral Movement and Privilege Escalation, while Section 4 deals with Persistence.
- In Section 5, we will build an emulation plan for three different threat actors. These emulation plans will be executed in Covenant and Caldera.
- In Section 6, students will participate in an all-day lab that pits red and blue teams against one another. While red attempts to infiltrate the organization, blue builds a detection capability to detect adversary techniques.

Section Descriptions

SECTION 1: Adversary Emulation for Breach Prevention and Detection

In Section 1, we will lay the foundations for the rest of the course by:

- Leveraging the power of automation to deploy our lab infrastructure
- Learning how to build a purple team in-house, covering process, approach, and tooling
- Tracking purple teaming exercises using VECTR
- Building an emulation and detection pipeline using a variety of available technology (SIGMA for detection rule development, and various adversary emulation tools, with a focus on Covenant and Caldera)

Even if it's just the first section, this section is heavily hands-on as students will complete five different exercises.

TOPICS: Introduction; Key Tools

SECTION 2: Initial Intrusion Strategies Emulation and Detection

The following modules will be covered in Section 2:

- We'll start with a state-of-the-art overview on current attack strategies and defenses for initial execution.
- We will zoom in on built-in defenses provided by Microsoft such as the Anti Malware Scanning Interface (AMSI). How does it work, how effective is it and can it be bypassed?
- Controlling execution on your endpoints using Attack Surface Reduction (ASR) rules. Introduced in Windows 10, ASR rules are an additional security layer that can be used to prevent execution of malicious payloads. We will zoom in on there effectiveness and test several bypasses.
- Controlling execution on your endpoints using AppLocker. Introduced in Windows 7, Applocker is an application control technique that can be used to prevent execution of malicious payloads. We will zoom in on its effectiveness and test several bypasses.
- The rise of Endpoint Detection & Response (EDR) tools has provided organisations with a means to enable in-depth detection and perform immediate response activities on their endpoints. These tools have changed the security landscape and have forced adversaries to get creative. We will look at a number of EDR bypass strategies including Child-Parent Process ID spoofing, Command line argument spoofing, Process injection & hollowing and finally the use of direct syscalls. It gets quite technical here

TOPICS: Initial Intrusion Strategies; Emulating Adversarial Techniques and Detections; Going Stealth – Process Shenanigans

Who Should Attend

- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Red team members
- Blue team members
- Purple Team members
- Forensics specialists who want to better understand offensive tactics

SECTION 3: Privilege Escalation and Lateral Movement Emulation and Detection

The following modules will be covered in Section 3:

- Enumerating Active Directory resources and configurations to map the overall attack surface of an AD environment.
- Understanding the Local Security Authority Subsystem Service (LSASS) process. What is its purpose and how is it traditionally attacked? We will go in-depth and explan topics such as Security Support Provicers (SSPs) and Authentcation Packages (APs). After this explanation, we will zoom in on the execution and detection of LSASS dumping attacks using a variety of tools (including Mimikatz, Dumpert, ProcDump)
- Given the focus of security products on LSASS, we will also investigate other credential dumping techniques. How can adversaries steal credentials without touching LSASS? Key techniques will include Internal Monologue (NTLMv1 downgrade), NTDS.dit stealing and DCSync.
- Forcing Windows Authentication: Provided with network-level access (or an initial payload on a network-connected device), how can we obtain additional credentials through forcing other Windows systems to connect to us? Typical topics include the use of LLMNR, but also IPv6-based MitM attacks.
- A refresh on Kerberos and traditional attacks such as Kerberoasting, ASReproasting, golden tickets, silver tickets and the Skeleton Key attack. After the refresh, we will focus on advanced attack strategies, primarily focused on delegation attacks. We will cover unconstrained delegation, constrained delegation and resource-based constrained delegation.

TOPICS: Active Directory Enumeration; Credential Dumping; Kerberos Attacks

SECTION 4: Persistence Emulation and Detection

The following modules will be covered in Section 4:

- An explanation on the security boundaries in AD environment and how adversaries can possibly pivot between different domains and forests
- Explaining typical persistence strategies used by adversaries. We will also discuss typical detection strategies
- Abusing the Component Object Model (COM) to establish a persistent foothold in a target environment. Attacks we will cover include Phantom COM Objects and COM Search Order Hijacking
- Obtaining persistence through the use of Windows Management Instrumentation (WMI). We will explain WMI Event Filters, Event Consumers and Event Filter to Consumer bindings
- Establishing persistence through DLLs such as AppCert, AppInit and Netshell
- Leveraging Microsoft Office for persistence, with a key focus on template shenanigans and malicious add-ins
- Abusing the Application Compatibility Toolkit (ACT) to obtain persistence through application shims
- Stealth persistence using the AD

TOPICS: Pivoting Between Domains and Forests; Persistence Techniques

SECTION 5: Azure AD and Emulation Plans

The following modules will be covered in Section 5:

- We will first perform a lecture on Azure AD attack strategies. We will introduce Azure AD and its security mechanisms and how they can possibly be attacked. We will also look in logging strategies for Azure AD.
- Afterwards, we will build out emulation plans for three specific threat actors: APT-28, APT-34 and Turla.
- Upon completing the emulation plans, we will execute them using Caldera and Covenant

TOPICS: Azure AD; Executing Emulation Plans

SECTION 6: Adversary Emulation Capstone

In this final section of the SEC699 course, participants can choose whether to join the red or blue team in an epic capstone battle to infiltrate or defend the corporate environment. Students will leverage all of the tools and techniques they've learned throughout the course!