SEC699: Purple Team Tactics – Adversary Emulation for Breach Prevention & 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

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:

- An in-depth course section on how to develop Ansible playbooks that deploy a full multi-domain enterprise environment for adversary emulation at the press of a button
- Development of custom MITRE Caldera modules for automated adversary emulation. If you truly want to build an emulation pipeline, automation is key!
- Building adversary emulation plans that mimic real-life threat actors such as APT-28, APT-34, and Turla
- Building a proper process, tooling, and planning for purple teaming
- Cross-forest attacks where students attempt to escalate privileges from their own isolated forest to the common course forest
- Bypass methods for some common defense techniques (e.g., application whitelisting, Attack Surface Reduction)
- SIGMA rule-building to detect advanced adversary 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 5 will be heavily hands-on:
- Every morning, we will lecture on an "advanced" technique (e.g., domain delegation attacks)
- After the morning lecture, we will perform a purple team exercise (both emulation and detection) for a specific threat actor. The advanced technique will be included in the emulation plan
- 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.

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Section Descriptions

SECTION 1: Introduction, Automation, and Lab Building

In section 1 we will lay the foundations for the rest of the week by:

- Learning how to build a purple team in-house, covering process, approach, and tooling
- Leveraging the power of Ansible automation to deploy our lab infrastructure
- 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 Caldera)

TOPICS: Introduction; Course Objectives; Purple Teaming Using MITRE ATT&CK; Purple Team Planning and Follow-up; Automation; Ansible Automation; Building an Emulation and Detection Pipeline; Building a Stack for Detection; Rule-Based Versus Anomaly-Based Detection; Building a Stack for Adversary Emulation; Automated Emulation Using MITRE Caldera

SECTION 2: Advanced Initial Execution Techniques – Threat Actor APT-28

Sections 2 to 5 follow a common structure:

- We will first perform a lecture and stand-alone lab on an advanced adversary technique and how it can be emulated.
- Afterwards, we will build an emulation plan for a specific threat actor. The emulation plan will include the advanced technique covered in the lecture.
- All techniques in the emulation will first be executed manually.
- Upon manual completion of the emulation plan, we will review which steps of the plan could have been detected, and how. We will implement community SIGMA rules, but also develop our own rules to detect the steps of the emulation plan.
- We will proceed by emulating the same plan in Caldera, where we will develop our own ATT&CK techniques as required.
- We will test our implemented SIGMA rules by executing the automated adversary plan

TOPICS: Topic for the Section – Advanced Initial Execution; Threat Actor for the Section – APT-28; Implement Detection Use Cases; Execute Adversary Emulation Plan – Automated

SECTION 3: Advanced Active Directory Attacks – Threat Actor APT-34

TOPICS: Topic for the Section – Advanced AD Attacks; Threat Actor for the Section – APT-34; Implement Detection Use Cases; Execute Adversary Emulation Plan – Automated

SECTION 4: Stealth Persistence Strategies – Threat Actor Turla

TOPICS: Topic for the Section – Stealth Persistence; Threat Actor for the Section – Turla; Implement Detection Use Cases; Execute Adversary Emulation Plan – Automated

SECTION 5: Azure AD Attacks – Threat Actor APT-30

TOPICS: Topic for the Section – Azure AD Attacks; Threat Actor for the Section – APT-30; Implement Detection Use Cases; Execute Adversary Emulation Plan – Automated

SECTION 6: Purple Team 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!

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

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.