SEC564

Red Team Operations and Threat Emulation

Two-Day Course
12 CPEs
Laptop Required

Who Should Attend

- Security professionals interested in expanding their knowledge of Red Teaming
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red Team members
- Blue Team members
- Forensics specialists who want to better understand offensive tactics

You Will Be Able To

Make the best use of a Red Team to understand and measure an organization's defenses. You will learn what Red Teaming is and how it differs from other security testing engagements. This course offers a unique view of the offensive security field of Red Teaming and the concepts, principles, and guidelines critical to a Red Team's success. It prepares you to design and create threat-specific goals to measure and train organizational defenders (CND/Blue Teams) and shows how a Red Team uses the "Get In, Stay In, and Act" methodology to achieve operational impacts.

This course provides the foundation needed to manage and operate a Red Team and conduct Red Team engagements. What is Red Teaming? ***Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate a real-world threat with the goals of training and measuring the effectiveness of people, processes and technology used to defend an environment.***

Red Teaming is built on the fundamentals of penetration testing, yet focuses on specific scenarios and goals used to evaluate and measure an organization's overall security defense posture. That posture includes people, processes, and technology. This course will explore Red Teaming concepts in depth to provide a clear understanding of what a Red Team is and its role in Security Testing.

Organizations spend a great deal of time and money on the security of their systems. Red Teaming uses a comprehensive approach to gain insight into an organization's overall security. Red Teams have a unique goal of testing an organization's ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization's security controls, help hone defensive capabilities, and measure the effectiveness of security operations.

The Red Team concept requires a different approach from a typical security test, and it relies heavily on well-defined tactics, techniques, and procedures (TTPs). These are critical if a Red Team is to successfully emulate a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist.

Course Day Descriptions

564.1 HANDS ON: Red Team Operations and Threat Emulation

Day 1 begins by introducing Red Team topics, concepts, and ideas. You will learn what Red Teaming is, how it is used, and how it compares to other security testing types such as vulnerability assessments and penetration tests. Several topics, concepts, and ideas that are specific to Red Teams, and which constitute the critical foundation of Red Teaming, are examined in order to provide a solid base of understanding.

Topics: **History and Origin; Red Teaming Introduction; Aspects of a Red Team; Standard Attack Platform; Red Team Role in Blue Team Training; Live Assessment Example; How to Succeed; Engagement Frequency; Security Misconceptions and Assumptions; Red Team Goals; Threat Perspective; Threat Emulation Scenarios; Tradecraft and TTPs; Social Engineering; Tools and Techniques; Web Shells**

564.2 HANDS ON: Managing a Red Team and Red Team Engagement

Day 2 continues with a heavy focus on Red Team tools and techniques. The day is filled with multiple exercises designed to explore various aspects of Red Teaming. During the exercises, you manage and control indicators of compromise (IOCs), design custom command and control channels, and use unique command and control tools. You will also learn Red Teaming concepts needed to control and manage a Red Team. These include how to interface with clients, collect and log engagement artifacts, successfully execute an engagement, manage deconfliction, properly end an engagement, and deliver a professional report.

Topics: **Tools and Techniques; Understanding and Controlling Tool Indicators; Red Team Engagement Roles and Responsibilities; Handling Client Data; Data Collection; Red Team Engagement; Flow Engagement Planning; Engagement Execution; Ending a Red Team Engagement; Red Team Engagement Reporting**

SANS

SEC564 Training Formats
(subject to change)

Live Training
www.sans.org/security-training/by-location/all

Private Training
www.sans.org/onsite