SEC567

Social Engineering for Penetration Testers

Two-Day Course
12 CPEs
Laptop Required

Who Should Attend

- Staff or consultant penetration testers looking to increase their test breadth and effectiveness
- Security defenders looking to enhance their understanding of attack techniques to improve their defenses
- Staff responsible for security awareness and education campaigns who want to understand how cyber criminals persuade their way through their defenses

You Will Be Able To

- Take on your first social engineering test in your company, or as a consultant
- Improve your social engineering know how to develop new variations or increase your snare rate
- Equip you to deal with some of the ethical and risk challenges associated with social engineering engagements
- Enhance other penetration testing disciplines through understanding human behavior and how to exploit it

"SEC567 is an awesome class. The Capture-the-Human exercise brings it all together."

-Ryan Krukoski, Krukoski Consulting

SANS

SEC567 Training Formats
(subject to change)

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

Summit Events
www.sans.org/summit

Private Training
www.sans.org/onsite

SEC567: Social Engineering for Penetration Testers provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. Successful social engineering utilizes psychological principles and technical techniques to measure your success and manage the risk. SEC567 covers the principles of persuasion and the psychology foundations required to craft effective attacks and bolsters this with many examples of what works from both cyber criminals and the authors experience in engagements. On top of these principles we provide a number of tools (produced in our engagements over the years and now available in the course) and also labs centered around the key technical skills required to measure your social engineering success and report it to your company or client.

You'll learn how to perform recon on targets using a wide variety of sites and tools, create and track phishing campaigns, and develop media payloads that effectively demonstrate compromise scenarios. You'll also learn how to conduct pretexting exercises, and we wrap the course with a fun "Capture the Human" exercise to put what you've learned into practice. This is the perfect course to open up new attack possibilities, to better understand the human vulnerability in attacks and to let you practice snares that have proven themselves in tests time and time again.

Course Day Descriptions

567.1 HANDS ON: Social Engineering Fundamentals, Recon, and Phishing

In day 1 of the course we introduce you to key social engineering concepts, the goals of social engineering and a myriad of reconnaissance tools that will help prepare you for successful campaigns. We complete the day with exercises centered around the most popular and scalable form of social engineering, phishing. Each section includes how to execute the attack, what works and what doesn't and how to report on it to help the organization improve their defenses.

Topics: **Social engineering introduction; The Psychology of Social Engineering; Social Engineering Goals; Setting up for Success; Targeting and Recon; Secure & Convincing Phishing; Tracking Clicks; Secure Phishing Forms**

567.2 HANDS ON: Media Drops and Payloads, Pretexting, Physical Testing, and Reporting

In day 2 we build on the principles covered in day 1 of the course to focus heavily on payloads for your social engineering engagements. We will cover how to avoid detection, limit the risk of your payloads causing issues and how to build a bespoke payload that works and looks the part of your selected snare. Following that we will introduce another powerful skill with pretexting and cover how these can be combined to get payloads running. We end the day with a capture the flag where students can apply their new found skills and a section covering the top dos and don'ts in an engagement.

Topics: **USB and Media Drops; Building a Payload; Clicks That Work; Successful Pretexting; Tailgating and Physical Access; Social Engineering Reports; SE: Where it all Fits; Risky Business**

"Everyone talks about social engineering, but no one knows in-depth how to conduct a proper social engineering penetration test. SEC567 exposes you to tools and techniques to execute a social engineering engagement that provides value to executives and others." -Srinath Kannan, Ernst & Young

SANS