SEC467: Social Engineering for Security Professionals

2 Day Course	12 CPEs	Laptop Required

You Will Learn

- The psychological underpinnings of social engineering
- How to successfully execute your first social engineering test in your company or as a consultant
- Social engineering knowledge to develop new variations of attacks or increase your snare rate
- How to manage some of the ethical and risk challenges associated with social engineering engagements
- How to enhance other penetration testing disciplines by understanding human behavior and how to exploit it

Who Should Attend

- Penetration testers looking to increase their testing 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

Author Statement

"Social engineering has always been a critical part of the cyber criminals' toolkit and has been at the core of innumerable attacks over the years. Organizations are taking significant interest in social engineering as a part of penetration testing, yet many penetration testers do not have social engineering skills in their attack toolkit. We are passionate about changing that and opening up a new set of attack possibilities. That being said, this is an area filled with ethical challenges, risks, and even legal landmines. So we've done our best to share our experiences in the course in a way that enables people to reap the benefits of our experiences without enduring the pitfalls we have dealt with over the years."

—Dave Shackleford and James Leyte-Vidal

Social engineering is an amazingly effective technique that has one important advantage over many other attacks, it allows adversaries or testers to bypass many of the technological controls in an environment by enabling them to act as, or with the assistance of, a trusted insider.

Any organization that employs humans is subject to risk. Social engineering allows the adversary to achieve a foothold in environments where technical controls may have made gaining such a foothold very difficult. Successful social engineering utilizes psychological principles and technical techniques to measure your success, manage the associated risk, and prepare an organization for social engineering attacks.

SEC467: Social Engineering for Security Professionals provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. The course provides tools and techniques for testers to identify flaws in their environments that are vulnerable to social engineering attacks. Defenders taking this course will note common tools and techniques that will enable them to prepare responses and countermeasures within their organizations. SEC467 covers the principles of persuasion and the psychological foundations required to craft effective attacks. It then bolsters that information with numerous examples of what works, drawing on the experiences of both cyber criminals as well as the course authors. You will 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 will also learn how to conduct pretexting exercises. We'll wrap up the course with a fun Capture-the-Human exercise to put what you have learned into practice. This is the perfect course to open up new attack possibilities, better understand the human vulnerability in attacks, and practice snares that have proven themselves in tests time and time again.

Section Descriptions

SECTION 1: Social Engineering Fundamentals, Recon, and Phishing

Section one of the course introduces you to key social engineering concepts, the goals of social engineering, and a myriad of reconnaissance tools to help prepare you for successful campaigns. We complete the section with exercises centered around the most popular and scalable form of social engineering: phishing. Each exercise includes how to execute the attack, what works and what doesn't, and how to report on the attack to help the organization improve its defenses.

TOPICS: Psychology of Social Engineering; Targeting and Recon; Secure and Convincing Phishing; Tracking Clicks; Secure Phishing Forms

SECTION 2: Media Drops and Payloads, Pretexting, Physical Testing, and Reporting

Section 2 builds on the principles covered in the previous section 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 build a bespoke payload that works and looks the part of your selected snare. We will then introduce another powerful skill with pretexting and cover how it can be combined to get payloads running. We end the section with a Capture-the-Human exercise in which students can apply their newly found skills and with a look at the top do s 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; Social Engineering: Where It All Fits; Risky Business