

The Value of Social Engineering

1 Day Workshop (8 hours)

Learn the basics of social engineering and how to safely and ethically conduct assessments. Discover how to construct and conduct pretexts that evaluate policies as well as existing defenses. Find out how to expand your company's current defensive posture by safely testing the most vulnerable component, the human.

1. Social Engineering
 - a. Definition basics
 - b. Considerations
 - c. Legalities
 - d. Value to client
 - e. Impact to client
 - f. Why?
2. Where to begin?
 - a. Do you need to test?
 - b. What are you testing?
 - c. Purpose of testing
 - d. Alignment of testing with policies
 - e. How to test policies
 - f. Measuring the effectiveness of policies
 - g. Rewriting policies/review
 - h. Employee education
3. Planning Social Engineering Assessments
 - a. Goal = Show impact to the client
 - b. Facilitate goal by targeting policies and systems
 - c. Select the target
 - d. Gather information on the target
 - e. OSINT
 - f. Planning for failure
 - g. How to plan pretexts
 - h. Creation of checklist
 - i. Deciding what data to record
 - j. Recording and documentation
 - k. Final deliverable?
4. Executing Social Engineering Attacks
 - a. Pretexts
 - b. Phone pretext
 - c. Basic Pretexts
5. Putting it all together
 - a. Final report
 - b. Collecting evidence for client
 - c. How to present findings
 - d. What to consider report
 - e. How to present findings without risk to self or employees
 - f. How to show relevance/impact to client