**Title:** Ethical Social Engineering Field Operations
**Date/Time**: (2-Days) Wednesday-Thursday, April 11-12, 8am-5pm

**Description**:
Learn the basics of offensive and defensive social engineering techniques 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.

**Instructor 1:** Aaron Crawford (@SquirrelsNaBrrl)
As a certified security professional with over 23 years of experience in the security industry, Aaron Crawford eats, sleeps and continually drinks from the security fire hose. This passion for IT and Security lead him to form the Insider Security Agency. In his spare time, he runs Squirrels In A Barrel, an independent training and learning resource for the Security industry. His fascination with Social Engineering led him to form the World Championship of Social Engineering. A global Social Engineering capture the flag contest that allows participants to learn and safely practice Social Engineering, within the world's largest Social Engineering sandbox. Alongside with his work on social engineering Aaron can also be found serving as the founder of the Skeleton Crew scholarship for DefCon.

Professionally known as one of the most fearless, proficient and successful Social Engineers, Aaron can be found creating new technologies and techniques to further the field of Social Engineering and speaking about them where ever he can.

**Instructor 2:** Billy Boatright (@fuzzy_l0gic)
Billy began his social engineering career without even knowing it. He was a bartender on the Las Vegas Strip for the better part of a decade. He won numerous awards from all over the world as a Top-ranked Flair Bartender. He has taken the skills he learned behind the bar to the Information Security world. Billy has been a Judge for the Social Engineering Capture the Flag event at Defcon. He is also the namesake for the BSides Las Vegas Social Engineering Capture the Flag Championship Belt. Billy also volunteers time and expertise to the Las Vegas ISSA Chapter as a Board Member. He is also a member of the BSides Las Vegas Senior Staff.

Billy has multiple degrees and numerous certifications. However, when asked about them he will gladly quote George Moriarty, "The shining trophies on our shelves can never win tomorrow's game."

**Course Outline:**

1. Social Engineering
    a. What is it?
    b. Why?
    c. Social Engineering is Bullshit
        i. The history behind the phrase
        ii. How we will define it for this workshop
    d. How can it be used?
    e. Applying to assessments?

    f. Ethics of use?
    g. Legal considerations
        i. How to use
        ii. How to plan
        iii. How to get legal help
        iv. Human Experimentation laws
        v. Considerations
        vi. Legal obligations
        vii. THE LAW.
2. The Four Phases of a Social Engineering Assessment (PREP)
    a. Planning
    b. Recon
    c. Execution
    d. Postmortem
3. Planning Social Engineering Assessments
    a. How to show impact
    b. Planning for failure
    c. Planning for the report
    d. Legal considerations
    e. How to sell services to a client
    f. Statement of Work for an assessment
    g. Legal paperwork that MUST be in place
    h. Planning the whole assessment
4. Recon for Social Engineering Assessments
    a. OSINT
    b. What is OSINT
    c. OSINT resources
    d. How to OSINT like Redteam
5. Executing Social Engineering Assessments
    a. Planning and executing Assessments
    b. Verbal vs Nonverbal pretexts
    c. Pretext examples
    d. How to record attacks
    e. Execution of attacks
6. Postmortem for Social Engineering Assessments
    a. Recording data
    b. How to capture information
    c. How to write the final report
    d. How to debrief your final report
        i. What to say and not say
        ii. How to present information
        iii. What to present
        iv. Appearance and hygiene for clients
        v. Legal considerations – COPYRIGHT/TRADEMARKS

7. Humans
    a. Reading people
    b. People watching
    c. Rapport building
        i. SPORTS!!!
    d. The Five Senses
    e. Planning considerations
    f. How to have a conversation
    g. How to start a conversation
    h. How to END a conversation
    i. Thinking like an adversary
8. Tools & Resources
    a. How to find
    b. Make your own
    c. Resources
        i. Thrift shops
        ii. Relators
        iii. Pawn shops
        iv. Public records
    d. Practicality vs Seen on TV
    e. Legal issues
9. In Real Life
    a. When things go wrong
    b. What actually works
    c. Redteam tricks
    d. Thinking like an adversary / criminal
10. Hands-on exercise 1
    a. Thrift shop
    b. Each team has $10 and 10 minutes
    c. Purchase uniform
    d. Present pretext with findings
11. Hands-on exercise 2
    a. OSINT Test
    b. Locate the assigned YouTube personality's home or residence
    c. Present your findings, describe how you found it
    d. Prescribe recommendations to address what you found
12. Social Engineering CTF
    a. Objectives
    b. OSINT
    c. Target: Pangaea Security
    d. How to play
    e. Time limit and final report
    f. Day 2 full OSINT CTF
    g. All OSINT Targets are live

**Who Should Attend**:
This course is intended for anyone interested in learning offensive or defensive social engineering techniques with hands on labs and a CTF.

**Student Requirements** (what should they bring with them)

- Class materials will be provided and announced closer to launch date
- Must be able to travel/walk short distances
- Must be prepared clothing-wise for indoors and outdoors as some field trips will take place
- Laptops/tablets are not required but will be needed if wanting to participate in the labs and the capture the flag
- Laptops/tablets should be capable of connecting to the internet
- NO laptops or equipment from employers is allowed (Please don't bring your company laptop to a security conference.)
- No photography or video is allowed of the instructors due to employment and safety issues (Everything else can be filmed and is encouraged.)
- Personal note taking equipment