Social Engineering Workshop

1. Class Schedule and Outline
    1. Day One – SE, OSINT, Report Writing & Hands-on techniques
    2. Day Two – Hands-on techniques & Social Engineering Capture the Flag (CTF).
        - i. OSINT
        - ii. Objectives
        - iii. Targets
        - iv. Scoring
        - v. Final Submission Rules
        - vi. Judging Deadlines and Schedule
1. Social Engineering
    1. What is it?
    2. Why?
    3. Social Engineering is Bullshit
        - i. The history behind the phrase
        - Ii. How we will define it for this workshop
    1. How can it be used?
    2. Applying to assessments?
    3. Ethics of use?
    4. 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.
1. The Four Phases of a Social Engineering Assessment (PREP)
    1. Planning
    2. Recon
    3. Execution
    4. Postmortem
2. Planning Social Engineering Assessments
    1. How to show impact
    2. Planning for failure
    3. Planning for the report
    4. Legal considerations
    5. How to sell services to a client
    6. Statement of Work for an assessment

    7. Legal paperwork that MUST be in place
    8. Planning the whole assessment
3. Recon for Social Engineering Assessments
    1. OSINT
    2. What is OSINT
    3. OSINT resources
    4. How to OSINT like Redteam
4. Executing Social Engineering Assessments
    1. Planning and executing Assessments
    2. Verbal vs Nonverbal pretexts
    3. Pretext examples
    4. How to record attacks
    5. Execution of attacks
5. Postmortem for Social Engineering Assessments
    1. Recording data
    2. How to capture information
    3. How to write the final report
    4. 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
1. Humans
    1. Reading people
    2. People watching
    3. Rapport building
        - i. SPORTS!!!
    1. The Five Senses
    2. Planning considerations
    3. How to have a conversation
    4. How to start a conversation
    5. How to END a conversation
    6. Thinking like an adversary
2. Tools & Resources
    1. How to find
    2. Make your own
    3. Resources
        - i. Thrift shops
        - ii. Relators
        - iii. Pawn shops
        - iv. Public records
    1. Practicality vs Seen on TV

    2. Legal issues
2. In Real Life
    1. When things go wrong
    2. What actually works
    3. Redteam tricks
    4. Thinking like an adversary / criminal
3. Hands-on exercise 1
    1. Thrift shop
    2. Each team has $10 and 10 minutes
    3. Purchase uniform
    4. Present pretext with findings
4. Hands-on exercise 2
    1. OSINT Test
    2. Locate the assigned YouTube personality’s home or residence
    3. Present your findings, describe how you found it
    4. Prescribe recommendations to address what you found
5. Social Engineering CTF
    1. Objectives
    2. OSINT
    3. Target: Pangaea Security
    4. How to play
    5. Time limit and final report
    6. Day 2 full OSINT CTF
    7. All OSINT Targets are live

About the Trainers:

Billy Boatright:

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."

Aaron Crawford:

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 wherever he can.