Syllabus for Training: InfowarCon October 31, 2018

Joshua Crumbaugh is one of the world's leading security awareness experts and internationally-renowned cybersecurity speaker. He is the developer of the Human Security Assurance Maturity Model (HumanSAMM) and Chief Hacker at PeopleSec. He is also an expert social engineer who has talked his way into bank vaults, fortune 500 data centers, corporate offices, restricted areas of casinos and more. His experiences highlighted a significant need for a better "human solution" -- This led him to a passion in social engineering and better-understanding ways to stop social engineering attacks.

PRESENTATION EXPERIENCE
BlackHat Europe 2017
Hacker Halted 2017
ShowMeCon 2017
BSides Huntsville 2017
CarolinaCon 2017
SFISSA Conference 2017
RocketSecure 2017
BSides Huntsville 2018
Insider Threat Summit 2018
ISOneWorld 2018
5th Information Security Conference 2018 (Athens Greece)
HackMiami 2018
NRC Live Cyber Insecurity 2018 (KEYNOTE - The Hague Netherlands)

TOPIC SUMMARY
This training is designed to give attendees the tactics, confidence, and training necessary to become a highly successful social engineer. Attendees will learn how to chain attacks, increase the probability of success, plan for attacks and so much more. Anyone who desires to be able to do things like talk their way into bank vaults, data centers, SCIFs or casino money cages needs to attend this training. We will have a hands-on portion of the education where attendees will put their newfound knowledge to use in a fun phone-based exercise designed to exercise their knowledge.

MINIMUM COURSE REQUIREMENTS
Bring a Laptop with: 4 GB of RAM at Minimum and Quad-Core Processor at Minimum Ability to Run Virtual Machines
Understanding of basic social engineering concepts
Understanding of basic network penetration testing concepts

TARGET AUDIENCE
This course is targeted toward individuals looking to enhance their social engineering knowledge and capabilities. This course will give them the skills necessary to excel in social engineering.

TRAINING OUTLINE
- Introduction to Social Engineering
  - Background
  - Importance
  - Mediums
  - Definitions/Terminology
  - Tools
- Red team social engineering tactics
  - Recon - OSI
    - The how what and why of recon
  - Planning
    - How to create an effective plan

    - Physical/In Person
        - Considerations
        - Planning
        - Attire
        - Body Language
        - Timing
    - Phone Based Engineering (Vishing)
        - Considerations
        - Planning
    - Email Based (Phishing)
        - Considerations
        - Phishing URLs
        - Bypassing Email Filters
        - Crafting emails
        - Payloads
        - Phishing susceptibility trends
    - Social Media
        - Considerations
        - Planning
        - Tactics
        - Fake profiles
    - Network based social engineering
        - MITM web message injection
        - Fake PW prompts
    - Communications Compromise
        - The who, how and why of utilizing compromised communications channels for social engineering
    - Long term vs short term considerations
    - Payload handling tips
        - Firewall bypass
        - AV Bypass
- Advanced Social Engineering
    - Blinding through desire
        - Never underestimate human blindness when it comes to personal self-interest.
    - Creating diversions
    - Denial of Thinking attacks
        - How to prevent the target from thinking about their actions during the moment
    - Targeting
        - Finding the right target can guarantee success
        - Targeting specific to each of the social engineering tactics
    - Common human vulnerabilities
    - Making people trust you
    - Surveillance Avoidance
    - Wasting target time to get what you want
    - The “My Boss” rule
    - Teaming scenarios
    - Chaining attack vectors