**SOCIAL ENGINEERING OUTLINE**

STEP 1: RECONNAISSANCE

* Drawing/ fine tuning organization chart
* Use Google for email harvesting, personnel details, office extension & cell phones no
* Collecting company official communication media (letterhead, business card, memo)
* Mapping latest/ any interesting activities related to the organization (from newspapers, blog, magazines, etc)
* Other intel (either from competitors/ corporate intel/ civil records, etc)

STEP 2: SCANNING FOR HUMAN VULNERABILITIES

* Examining physical controls (guards, door access, CCTV, sensors)
* RF sniffing via open wireless LAN (gaining more info)
* Identify & listing of 3rd party access to organization (cleaner, guards, pesticide controller, supplier)
* Recording persistent information (delivery time, office schedule, weekend activities)

STEP 3: PLANNING THE ATTACK

* Layout all the gathered information (list on war board – confidential)
* Preparing all required tools
* Selection of exploitation
* Strategy coordination (inclusive mocking the role play, memorizing the intels, finalized every single activities’ objective)

STEP 4: PERFORMING THE TEST

* Setting up phishing site & email to the target
* Perform call interaction to various departments (using SpoofCard to spoof originated phone numbers)
* Dumpster diving (even can offer some recycling offer)
* Authentication bypass (Door access RFID cloning – if any, duplication of staff IDs)
* Applying for some jobs (contract basis)

STEP 5: REPORTING