REDTEAM
SECURITY TRAINING

Social Engineering Operational Plan

Prepared for: United States Army, Fort Mead

Jeremiah Talamantes, CISSP, CHFI, CEH, CCENT, CCISO
REDTEAM SECURITY TRAINING, LLC

CLIENT Fort Meade, United States Army
TARGET LOCATION NAME/ADDRESS 4409 Llewellyn Ave, Fort Meade, MD 20755
TARGET GPS COORDINATES 39.1138° N, 76.7268° W
TARGET PHOTO(S)

Figure 1: Aerial view of the target location

OBJECTIVE(S)

Test the staff's security awareness and identify weaknesses in personnel security relating to their adherence to security policies. The team will also test physical security controls of the Data Center. This includes, but is not limited to: perimeter fence, cameras, perimeter readers, & building external doors, from the perspective of a motivated attacker.

TARGET CONTROLS

Testing of any of the following target controls:

- Incident response - deceive eyes-on camera responders with camouflage
- Incident response – test responders by attempting to bypass security controls covertly
- Outer perimeter – bypass physical security controls covertly (ie: fencing)

- Inner perimeter – lock pick a building exterior door lock, bypass a building exterior door, or tailgate into a building
- *Personnel security awareness – clone RFID badge (if the opportunity presents)*
- *Outer perimeter – bypass RFID access with cloned badge (if opportunity presents)*

ROLE/TEAM MEMBER

(REQUIRED DUTIES: COMS, TIMEKEEPER, KIT, LOGISTICS)

- **TEAM LEADER:** Jen: Deploy and pick up team. Report on target security movement, long-range. Mission lead, monitor scanner.

- **SENIOR OPERATOR:** Melissa: Tail operators and stick at outer perimeter point and report on target security movement short-range.

- **OPERATOR:** George: Breach inner and outer perimeter – gather video/photographic footage inside and exfil. Progress by radio to Team Leader. Clone RFID, if possible.

- **OPERATOR:** Donald: Breach inner and outer perimeter – gather video/photographic footage inside and exfil. Clone RFID, if possible.

DATE/TIME

- 11/29/18 – 12/11/18: Recon (done)
- 12/11/18 – 12/14/18: Recon & Execution

OPERATION

(Subject to change without notice; not all phases may be applicable)

RECON

(Identify the Targets)

- [Leverage intel from recon performed during a previous visit]
- Stake out position #1 (Infil point)
- Stake out position #2 (Employee entrance)
- Observe physical security controls
- Observe security patrols
- Note any deficiencies in personnel security awareness

WEAPONIZATION
(Prepare the Operation)

- Suit up in camo at a nearby location
- Load kit into infiltration team's bags
- COMS check

DELIVERY
(Launch the Operation)

- Recon parking lot for minimal activity, once quiet
- Deploy team to Position #1
- Team Leader to offsite position
- Infil team arrives at Position #1

EXPLOITATION
(Gain Access to Target/Victim)

- Exploit the existence in physical cover at Position #1 and other physical security controls to breach outer perimeter
- Infil team searches for a point to make entry and bypass the inner perimeter; OR
- Exploit the opportunity for tailgating through Position #2 – employee break or smoking area – or other positions as the team sees fit to breach the inner perimeter
- Overtly engage staff inside the perimeter. Observe and note any policy violations

ACTIONS ON OBJECTIVE
(Custom Defined)

- Acquire video and photographic evidence while inside
- Briefly meander through the immediate location
- Do not spend more than 20 minutes onsite
- Exfil to Rally Point

TERRAIN/WEATHER

Light to medium brush around outer perimeter. Gravel/paved entrance. Warm clothing required. Desert camo BDUs, combat boots, etc.

EXFILTRATION (EXFIL)

Upon radio report from the team indicating progress, the Team Leader will determine "mission success" and give the EXFIL TRIGGER call over the radio to the team. The team will start the EXFIL process. The team will disconnect, pack up their kit, re-lock any picked locks and minimize any traces of presence.

RALLY POINT: the south end of the Proline parking lot

EXFIL TRIGGERS

TEAM LEADER WILL GIVE THE CALL OVER THE RADIO

"BINGO" = MISSION SUCCESS. Carry out pre-defined EXFIL procedures as above.

EMERGENCY EXFIL

Upon radio report from the team or Team Leader, the emergency exfil call will be given. Likely compromises include: police scanner chatter, visitors, alarms. The team will exfil immediately once the EXFIL TRIGGER call is given over the radio.

EMERGENCY RALLY POINT: 39.094212, -76.731073, Wilson Street

EMERGENCY EXFIL TRIGGERS

TEAM LEADER WILL GIVE THE CALL OVER THE RADIO

"TURTLE" = HUNKER DOWN AND HIDE
"SNAKE" = EXFIL BY QUIETLY SNEAKING OUT
"RABBIT" = EXIT IMMEDIATELY

KIT

	(4) radios	
(2) torches	(1) Battery power screwdriver	(2) binoculars
(2) night vision goggles	(1) thermal cam	(2) GoPro camera
(3) Desert camo BDUs	(1) GoPro head mount	(2) GoPro chesty mount
(1) emergency ladder	(3) red head lamps	
(2) hand claws	(2) foot claws	(1) RFID card cloner

PRETEXT ITEMS

- Civilian clothes (Black parka w/hoodie, dark colored pants)
- Yellow safety vests
- Construction helmets

OTHER

None at this time.