2>1: Teaming Up for Social Engineering Adventures

Jen Fox
@j_fox

#TeamworkMakesTheSchemeWork
• Sr. Security Consultant
• DEF CON 23 black badge, SECTF
The Project

- Internal/external technical pen test
- Social engineering: phone, phish, physical
- Goals:
  - Physical access to secured areas
  - Obtain user credentials
  - Deploy malware agents and gain foothold into internal network
  - Deploy physical device to grant access to internal network
Planning Call

YEAH, I'M GOING TO NEED YOU TO GO AHEAD AND
COME ON SITE FOR THE PHYSICAL SE
“One of the most interesting parts of the test was having an amount of freedom to obtain footholds on different network segments via a testing drop box. Primarily as a tester, you are on one network and either pivot to systems or are on a flat network; physically moving to other networks is very rare.”
“One thing that was more important to me personally was seeing the amount of prep work, dedication, and persistence required for Social Engineering.

Generally, you hear about the utter ownage that an SE campaign can bring. Actually seeing the work and the setup highlights the amount of difficulty (both technical and non-technical) that Social Engineers face.”
Attack Risk Chart

High
- After Hours Access
- NDE
- Theft

Medium
- Network Port Security
- Elicitation
- Badge Replication

Low
- Tailgating/Piggybacking
- Document Management
- USB Drops
- RFID Cloning

Courtesy @_sn0ww / @snowfensive
Pretext: Public

- Recon
- Where is IT dept?
- Lay of the land
Join the Employee Wellness
Weight Loss/Step Challenge

Sept. 14th - Nov. 22nd

Registration: 6 West Employee Wellness Office
Sept. 14th (Wed) & 16th (Fri)- 7:30-8:30am 11:30-12:30pm & 5-6pm (9/14)

Weigh-ins
-12:30pm

Enter in and lose a step tracking

You win by walking to each landmark.
The ultimate goal is to make it to December. More

SANS HackFest
Summit & Training
Day 1, night

- What pretext to use for next day?
- How to dress?
- Make a badge
• Print fake badge
• Internal network
• Keep looking for sensitive areas
Pretext: Intern and IT Analyst

• Why?
• Two people, one badge
• Research library
• Onsite awards event
• Random hallway meeting w/ CEO

Oh, the Places You’ll Go!
Goals: Last Day Onsite

• Make more inroads
• Additional areas accessed
• Run malware proxy on machines from a USB
Pretext: IT Analyst

• More dressed up than day 2
• “Need to install a patch”
Goals Met, Still Sad.
I’m back in Mike’s office ... he isn’t here!!

The computer isn’t locked

It seems so rude to plug in ... he is our stakeholder

You know what you need to do

You’re right. Agent deployed 😈
“We had previous pen tests from other companies. They weren’t bad tests, but what you and Adam did gave us a more complete picture of our environment.”