Social-Engineer.Org
Defcon 18 Social Engineer CTF
Agenda:

- What is Social Engineering?
- Who is Social-Engineer.org?
- Goal of the social engineering CTF?
- Statistics and analysis of data
- Questions & Answer
What is Social Engineering?

Social engineering is the act of manipulating a person to accomplish goals that *may* or *may not* be in the “target's” best interest.
Who is Social-Engineer.Org?

• Created the world’s first framework for Social Engineering
• Social Engineering based Podcast with over 16,000 subscribers
• Social Engineering based Newsletter with over 3000 subscribers
• Over 40 years of collective industry experience
SE CTF Goals:

To Prove or Disprove:

• That social engineering is a valid attack vector
• That even unskilled people can obtain information
• If security awareness programs are effective
• That even short calls from non-professional social engineers can lead to devastating information leaks
SE CTF Structure:

- Contestants signed up two months beforehand.
- One month before the contest, they were assigned a target.
- Instructed to research and write a report about the target.
- At DefCon, contestants used time limited call to obtain as many flags as possible.
- Limitations on call content and allowed pretexts.
Statistics & Analysis of Data

We broke the statistics out into groups:

- Executive Overview
- Dossiers
- Targeted Employees
- Pretexts Used
- Information Returned
Stats & Analysis - Executive Overview

Number of Companies Called: 15
Possible Flags: 25
Number of Companies Compromised: 14
Days Contest Was Held: 2
Total Phone Calls Made: 135
Companies Who Put Up a Fight: 7
Employees Who Put Up a Fight: 11
Stats & Analysis – Dossiers

Primary Information Sources:
• Google
• LinkedIn
• FaceBook

Interesting Approaches
• Google Street View
• Google “Dorks”
“Proper mitigation of this is quite an undertaking for most companies as it requires proper and effective awareness training for all employees...”
Stats & Analysis – Pretexts Used

“A pretext works as the story that is being told as part of the social engineering attempt. It provides the justification for the questions being asked....”
Stats & Analysis – Pretexts Used

**Survey** – Simple but does not yield much information

**Internal Employee** – Complex and justifies information requests, but collapsed on many contestants
Stats & Analysis – Employee Resistance

- Some Resistance
- No Resistance
“Even when some degree of resistance would be encountered, bypassing this was in every case simply a matter of calling back and reaching a different employee.”
Stats & Analysis – Information Returned

Company Logistics

- In House IT Support?
- Do you use badges for bldg access?
- Time Deliveries are made?
- Who they use for shipping?
- Who supplies Food?
- Is there a cafeteria?
- Who Does offsite backup?
- How are documents disposed of?
- Trash Handling?

Social-Engineer.Org
“When information is perceived to have no value, no effort will be placed into its protection.”
Stats & Analysis – Information Returned

Popular Technical Information

- What Service Pack?
- What OS is in use?
- Version of PDF Reader?
- PDF Reader?
- Version of browser?
- Browser?
- Version of Mail client?
- Mail Client?
- Open a Fake URL

Social-Engineer.Org
Stats & Analysis – Information Returned

Popular Technical Information

“With it being proven to be a simple task to have a target organization open a specific URL…a malicious social engineer has an easy path to a foothold into an organization. “

Social-Engineer.Org
Stats & Analysis – Information Returned

Other Technical Information

- VPN Software?
- Do You use VPN?
- Do you block certain sites?
- ESSID Name?
- Wireless on site?
- Make and Model of computer used?
- Anti-virus Used?
“This sort of information being provided across the phone is shocking not due to the sensitivity level, but rather due to why would a caller legitimately need to know the information requested?”
Stats & Analysis – Information Returned

**Employee Information**

- How long they have been with company?
- Days of Months Paid?
- Employee Termination Process
- New Hire Process?
- Employee Schedules?
- Name of PBX?
- PBX System?

Social-Engineer.Org
Stats & Analysis – Information Returned

Employee Information

“In the cases where this information was obtained, it was directly related to rapport that was established toward the beginning of the calls. Once this bond was established, contestants would inquire about this information as part of small talk.”
Stats & Analysis – Information Returned

Other Observations

• Being busy is a level of protection
• Small talk facilitated many flag captures
• Number called could determine if the call was trusted or not
SE CTF Goals:

To Prove or Disprove:

• That social engineering is a valid attack vector.
• That even unskilled people can obtain information.
• Security awareness programs are NOT effective.
• That even short calls from non-professional social engineers can lead to devastating information leaks.
Q&A