Pen Testing People

Ryan O'Horo
IOActive, Inc.

Session ID: HT1-302
Session Classification: Intermediate

RSA CONFERENCE 2012

Introduction

- I’m a hacker for hire, so my job is to get information from people
- This makes social engineering an important part of what I do
- I’m going to discuss what goes on inside the mind of a social engineer

- So that you can know how to better train your employees ... my targets

Inside the Mind of a Social Engineer

Hackers vs. Social Engineers

- The security industry is constantly worried about the next hacker exploit
- As professionals, our focus is to foil their efforts and mitigate their attacks
- We build security into every point of the infrastructure
  - Intrusion detection/prevention
  - Firewalls
  - Access control lists
- But social engineers are hackers, too...

Hackers vs. Social Engineers

- Social engineers are more dangerous
  - Industry spends fewer resources on securing access to people
  - SE attacks leave little/no audit trail
- Social engineers take the shortest path to the data
  - No need to bypass IDS or firewalls
  - Just ASK for what they want

SE Attack Types

- Physical
  - Requires high degree of attacker confidence
  - Entering a physical building is risky
  - Cameras and physical descriptions can betray you
- Voice/Phone
  - Requires fairly high degree of attacker confidence
  - Attacker must be a quick (and SMOOTH) talker
  - Phone calls are difficult to render untraceable

SE Attack Types

- Email Phishing
  - Includes email blasts: spray and pray method
  - Build massive recipient lists then apply statistics to increase chances of success
  - High visibility
- Email Spearphishing
  - Targets known parties: focused intent method
  - Pinpoints highest-value targets based on effort for the attacker

SE Attacks: Misunderstood

- Social engineering attacks are reported with far less frequency than standard hacking attempts
- They're also improperly classified
  - A malware infection could likely be the result of a social engineering attack
- The Anti-Phishing Working Group receives about 30,000 phishing reports per month

Psychological Vulnerabilities and Information Disclosure

Authenticating to People

- Just like authenticating to infrastructure software/hardware
- The brain is wired to recognize faces and we can identify shared information
  - So we're good at authenticating people we know
- But what about people we don't know or can't see?
  - We've been socially trained to accept numerous unsafe authentication factors...

Authenticating to People

- Framing allows us to implicitly trust people who look and play the part we expect
- People in authority
  - Law enforcement (police or security)
  - Delivery personnel (UPS, FedEx, USPS)
- Phone calls at work
  - We expect a customer or colleague
  - At large companies you expect to speak with people you've never met in person
    - Contrast with personal calls; we're more skeptical of an unknown number/contact

Authenticating to People

- Email is the killer
- People have insufficient information about email senders to authenticate them
- Headers can be forged and convincing pretexts presented, lending legitimacy
  - Pretext is key; it's the back story/premise under which an attacker engages the target
  - If I tell you I'm from IT support and we've discovered an issue with your account, are you more or less likely to give me your password?

Motivators to a Convincing Pretext

Human Behavior

- Exploiting behavioral motivators improves the positive response rate of an SE attack
  - **Fear**. Are you afraid of losing your job or offending an acquaintance?
  - **Guilt**. Have you wronged someone and want to make amends?
  - **Gossip**. Who doesn't want to know the latest juicy celebrity or political gossip?
  - **Greed**. Are you an heir to Nigerian royalty?

Human Behavior

- Implying urgency or enforcing a deadline
  - Helps prevent investigations into legitimacy
  - Significantly improves positive response rates

Respond in the next 10 minutes and we'll throw in an extra bonus knife sharpener that teleports you into the future!

Reconnaissance for a Convincing Pretext

Social Networks

- LinkedIn, Twitter, and Facebook provide a wealth of incredibly valuable, freely-available social information
- The point is to exploit knowledge about people and their relationships to people/organizations
  - The attacker seeks to align themselves with the victim's expectations
  - Must create a framework/context inside of which the ruse/ask seems normal to the victim

Search Engines

- Google Hacking
  - You can discover almost anything about a company or its employees with the right search terms
    - Employee names
    - Employee titles
    - Websites (webmail, external employee portals)
    - Templates for formal communication
- Press Releases/Public Documents
  - Companies love to brag about promotions, achievements, and new technologies
  - You end up appearing knowledgeable about the company, its products, and its goals

Case Study: LinkedIn

- High-profile company with great SE controls including domain monitoring for possible phishing/filtering email
- Sidestep controls by creating a fake LinkedIn profile based on a real job listing
  - Fit requirements of job listing
  - Fun biographical data plus employment/education history
  - Photo from Facebook
- Friend as many corporate employees as possible
  - 300 connection requests yielded 66 connections, many of who were in information security
- Now what?

Case Study: LinkedIn

- Request admission to company's LinkedIn employees-only group, which required HR approval
  - A legitimate-looking profile and 66 employee connections comes in handy!
- Result: audience of more than 1000 employees
- Posted malicious link to the group wall, which purported to offer a beta test sign-up page
- In two days, 87 hits provided access to vulnerable systems (40% of which were from inside the corporate network)
- On third day, an astute employee blew the whistle
  - But the damage was done
  - No one in InfoSec was notified of the breach

Case Study: Email Phishing

- Created a fake change-password page using a corporate template provided by your company's website
  - passwords-yourcompany.com
  - passwords.yourcompany.com (HTML obscures actual link)
- Fake email request urges users to change passwords in alignment with new company policy
- LinkedIn identified best target set (~36 users)
  - No IT or IT management
  - No one likely to take the initiative and report an attack
- 70% response rate, which is common
  - Some responded multiple times they were so eager to comply

Sample Attack Scenario: Physical

- Attacker pretends to be an interview candidate, having conducted research to identify names/times/places
  - Maybe even scheduled an actual interview
- Hurriedly enters lobby with coffee-stained document
- Politely explains resume is ruined and asks receptionist to reprint it
- Hands receptionist USB drive that contains malicious PDF with remote access payload
- Game over...
  - Attacker has infiltrated the internal network

Create a Social Engineering Engagement

Starting from Scratch

- The old-fashioned way to run an SE engagement
  - Perform detailed reconnaissance
  - Create website clone, complete with SSL certificate
  - Create email template
  - Dump to sendmail
  - Generate a valid SSL certificate to prevent credentials from being transmitted in the clear
- Primary attack vectors
  - Malicious websites and credential theft (the focus of my work)
  - Malware
  - Phones

Using the Phone

- All you REALLY need is a good story and a telephone
- But a caller ID spoofing service can be useful
  - Numbers coming from outside the target's area code are viewed with suspicion
  - Instead, spoof a number for the target's company (found via Google)
- Okay, you also need nerves of steel

- I suggest companies run regular, randomized SE engagements once every 1-2 quarters

Social Engineering Toolkit

- The automated way to run an SE engagement
  - Makes the process almost idiot proof
- Anyone in corporate infosec should be intimately familiar with the SET to stay abreast of the most current attacks
  - Even if you don't use it as part of your own SE engagements
- Features
  - Automatically creates malicious email payloads
  - Automatically clones website templates for credential theft
  - Integrated with Metasploit for malicious payloads
- The key is coming up with the right pretext

Incident Response and Education

What Should You Do?

- Create a global security mailing list that distributes incident response and training emails
  - Its existence should be widely known and listed in official communications
- In addition to standard incident response measures, when an SE attack is reported:
  - Email the global security list and alert users to in-progress attack
  - If user account information was leaked, restrict and start monitoring that account to gather details around attacker's origin, actions, and intent
  - Identify exploited weaknesses and fix them
  - Learn from and talk about the experience

What Should Users Do?

- **Be suspicious!**
- Push back/ask questions when someone requests information
  - It's okay to be rude when protecting the safety of your data
- Confirm validity of the request or action by calling or emailing via *previously established channels*
  - I sometimes put misleading contact information in my emails to prevent reports
- Report ALL suspicious emails, phone calls, or in-person requests

Keep Information Moving

- Share newsworthy examples
  - Gets the conversation going and raises awareness
  - People tend to ignore what isn't in the news
- Continue to communicate recommendations and guidelines to keep people mindful
- Appoint someone to monitor your company's social network presence
  - In the LinkedIn case study, the HR rep who moderated the group didn't perform due diligence likely because the group's sensitivity was not known or communicated

Final Points

Need to convince your company to let you socially engineer your own employees?

- Cite statistics: the DefCon 19 Social Engineering CTF report is a great place to start[1]
- Cite newsworthy social engineering attacks
- Anti-Phishing Working Group[2]
  - They have statistics, policy guidelines, and user education materials you can cut/paste into your own policy emails

1. http://www.social-engineer.com/downloads/Social-Engineer_Defcon_19_SECTF_Results_Report.pdf
2. http://www.antiphishing.org/

Apply

- Create a channel for sharing security information
- Create a framework for testing
- Raise awareness through engaging education
- Audit your social engineering resistance
- Feed information back to end users

- Don’t let your data be handed to attackers

Finally

Thank you!

Fear Guilt Gossip Greed

Ryan O'Horo

Email: ryan.ohoro@ioactive.com