Social Engineering

Ryan Cunningham
Final Exam

- **When:**
  - Friday 12/15 from 7pm-10pm

- **Where:**
  - Still getting this finalized

- **What:**
  - Multiple choice/short answer is comprehensive
  - MP3, MP4, MP5
Security News

- $70M? Bitcoin Heist
- JANUS vulnerability in Android patched
- OWASP changes
<table>
<thead>
<tr>
<th>OWASP Top 10 2013</th>
<th>OWASP Top 10 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2 – Broken Authentication and Session Management</td>
<td>A2:2017 – Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A3 – Cross-Site Scripting (XSS)</td>
<td>A3:2013 – Sensitive Data Exposure</td>
</tr>
<tr>
<td>A8 – Cross-Site Request Forgery (CSRF)</td>
<td>A8:2017 – Insecure Deserialization [NEW, Community]</td>
</tr>
<tr>
<td>A9 – Using Components with Known Vulnerabilities</td>
<td>A9:2017 – Using Components with Known Vulnerabilities</td>
</tr>
</tbody>
</table>
Social Engineering

- Psychological manipulation
- Espionage
- Confidence trick (con)
- Scam
- Swindle
- Fraud
- Lie
- “Using cheap dirty psychological tricks to get people to do what you want.” - Brian Brushwood
Pseudoscience and BS abounds in SE literature
- Neurolinguistic programming (NLP) - BS
- Using “microexpressions” - BS
- “Pick up artist” (PUA) - BS
WARNING!

- This stuff becomes very illegal very fast
Illusion of Transparency

- Cognitive bias
- Overestimate what people can tell about our thoughts
- Overestimate what we know about other people’s thoughts
- Dr. Elizabeth Newton tapping out songs
- It’s easier to lie than you think it is
Information Gathering

- Like any exploit, start with info on target
Information Gathering (Go deeper!)

- Employee social media
- Public records data
- Maps
- Local newspapers
- Technical documents, academic papers
- Training documents
- Dumpster diving
Elicitation

- Getting a target to do what you want them to do
HOW TO GET WHAT YOU WANT
Just Ask For It

- Dr. Ellen Langer at Harvard
- *The mindlessness of ostensibly thoughtful action: The role of “placebic” information in interpersonal interaction*
- “Excuse me, I have 5 pages. May I use the Xerox machine?” 60% compliance
- “Excuse me, I have 5 pages. May I use the Xerox machine, because I’m in a rush?” 94% compliance
- “Excuse me, I have 5 pages. May I use the Xerox machine, because I have to make some copies?” 93% compliance
- Get comfortable making people uncomfortable
Pretexting

- Use an invented scenario and/or identity
- Impersonate
  - coworkers
  - boss
  - customers
  - law enforcement
  - IT department
Get It Wrong

- “You guys use extension 5231, right?”
- “No, we use 1212.”
Make Them Like You

- Make them laugh
- Let them to talk about themselves
- Call them back
- Elicit sympathy
- Use the Ben Franklin effect, “Can you do me a favor?”
- If not liked, at least seem transparent
Reciprocity

- Give a gift
- Best if it doesn’t look like a bribe, time delay
- Dr. Dennis Regan of Cornell
- *Effects of a favor and liking on compliance*
- Subjects who got soda bought twice as many raffle tickets
- *Even if they reported disliking the assistant*
Distraction

- Misdirection
- Multitasking is an illusion
- Make them process information so they go on autopilot
Authority

- Business card
- Credential badges work
- Internal lingo
- Fake IDs/Badges
- Send a legal or policy document
- Or ... just wear a suit
Ask Questions

- Drive the conversation
- Appear to be the receiver when you’re actually the feeder
Tailgating/Piggybacking

- Follow someone with access
Social engineering is an indirect process

- Use elicitation to get an employee ID number
- to pretext as a company employee
- to gain information about management structure
- to pretext as an authority in the company
- to gain access to internal IT training documents
- to pretext as technical support
- to elicit access to an HR document
- just to learn who knows the information you need about your real target
Combined Attacks

- The real threat: combine social and technical exploits
- Spoof caller ID for elicitation
- Use SE to clone SIM card to bypass 2FA
- Hack a machine, “fix it”, then ask for information
- Tell them you are IT, give them your number to call
- Phishing/Vishing/Smishing
Baiting

- Drop physical media with malware in parking lot
- Tailor a personal gift
- "Leak" documents
Social Engineering Mitigation

- Be skeptical
- Ask for call back numbers
- Make sure employees understand sensitivity of data
- Have explicit, clear security policies
- Encourage employees to challenge authority and requests
- Audit employees by social engineering your own organization
Example: Real Future, Episode 8

https://youtu.be/bjYhmX_OUQQ?t=81
Example: Ghost in the Wires, Chapter 12