The Social Engineering Engagement Methodology—A Formal Testing Process of the People and Process

The security of an organization is composed of technology, people and processes. In the last few years, many organizations have done a good job addressing technology but have focused very little on the people and processes.

This presentation reviews the formal methodology for performing Social Engineering Engagements. The method is divided into four sections including the Pre-Engagement, Pre-Assessment, Assessment and Post-Assessment.

The Pre-Engagement is the sales process for performing the assessment. In this section, we will review the business justification and headlines of current attacks.

Pre-Assessment if focused on identifying the scope of the project, limitation, targets and attack vectors. Also included are examples of what information must be gathers for use in the assessment and post assessment phase.

The most interesting and tedious part is the actual assessment. In this section, we will discuss how to engage the target, utilize company information, how to achieve the goal and what to do when you are caught. Included in this section is also how and what to document about every contact.

Post assessment is the analysis and reporting phase. In it, we will review documenting findings, and mapping them to recommendations.
The Social Engineering Engagement

Joe Klein, CISSP NSA-IAM/IEM Greenbelt-6+
jsklein@mindspring.com

Agenda

Definitions
The Process
Pre-Assessment
Assessment
Post Assessment
Parting Words
References
Definitions

What is he talking about?

Social Engineering (political science)

Pejorative term used to describe the intended effects of authoritarian systems of government. The implication is that some governments, or powerful private groupings, are intending to change or "engineer" the citizenry. Laws and tax policies can influence behavior, and progressive politics often promote socially influential policies. A general meaning is any attempt by a government to alter society. Whether a government is supporting or altering a society depends upon what is the purpose of government.
Definitions

Social Engineering (computer security)
The practice of conning people into revealing sensitive data
A way to attack systems protected against other methods i.e. Firewalls, etc
One of the most famous social engineers in recent history is Kevin Mitnick.

“DefCon 11 T-Shirt”
“Social Engineering Specialist --- Because there is no patch for Human Stupidity”

Why Social Engineering?
Security is based on People, Processes and Technology
Identifies weaknesses in People
   Has staff been trained to protect passwords?
Identifies weaknesses in Processes
   Has technical staff been trained not to publish internal network diagrams?
Identifies weakness in Technical controls
   Hijacking backup tapes, Laptop Security, etc
Validation (Testing) may be required by law or regulation
   SOX, HIPAA, FISMA,...
Definitions

Types of Social Engineering

Authority
“I Am…”
President, HR, Security, etc

Liking
Similar Interest
sports, company, college, location
Interest in the other person
10’s attack

Reciprocation
Appear Helpful
Gain Favor

Consistency
This is my job and the way I do it

Social Validation
Follow what others are doing – Team Member

Scarcity
Win a prize, something for nothing
Get your name in...

digital self defense
Definitions

Personality Traits which make Social Engineering possible!

“Not my Job”
Chance for gaining acceptance or to gain a favor
Trust relationship
Moral duty
Guilt
Identification
Desire to be Helpful
Cooperation

Possible Legal Liability/Obstacles

Fraud Laws
Misrepresentation
Fraudulent Purposes
Party/Consent Exception
If you are going to record the discussion
Illegal Interception of Data Possessing
Illegal Tools & devices

digital self defense
The Process

Why a Process?

The Industry has a problem

Organizations which need assessments
- Have no Apple to Apple measure of service
- Receive inconsistent assessments

Organizations which perform assessments
- No way to show competency, except through prior work
- Competency is based on the experience of a few individuals

digital self defense
A Potential Solution

INFOSEC Assurance – Capability Maturity Model (IA-CMM)

- CMM Created by Carnegie Mellon to identify and highlight process maturity
- NSA and Industry applied it to Information Security
- Allows a third party measurement of assessment team process and documentation
- Provides a methodology/framework which fits Types of assessment
  - White team, Blue team, Red team
  - Supports all types of legal requirements
    - HIPAA, FISMA, DITSCAP, SOX, GLBi, MARCOM, etc

The Process (Based on IA-CMM)

Pre-Assessment
- Contracts & “Get of Jail Free Card”
- Definitions & Scope of Work
- Limitations of Project
- Creation of Cover story
- Approval of Methods
- Pre-Work – “The Grind”

Assessment
- Doing the job
- Assessment Documentation

Post Assessment
- Reporting
- Mitigation
Pre-Assessment

Contracts
- Authorized Signer
- Time Period of Assessment
- Contract Time
- Definition of Report

“Get of Jail Free Card”
- The Code Word
- “Chris Jones”
- Prepared Document
- Contact Numbers & Names

digital self defense
Pre-Assessment

Definitions & Scope of Work
Types of SE Engagement?
  Physical
    Delivery
    Employee
    Vendor
    Bribe
  Telephonically
    External (With and without caller ID spoofing)
    Internal
    Internal with voice mail
  Mail
    Paper
    Media
  E-Mail
  Link
  Attachment

Levels of Intensity

Pre-Assessment

Types of Social Engineering Attacks
  Plausible Personal Request
  By just answering a few questions
  Using really interesting e-mail
  The Trojan Horse
Pre-Assessment

Limitations of Project

Time
  Days on Project
  Days on Site
Money

Pre-Assessment

Creation of Cover story
  Where are you from?
  Who do you work for?
  What do you do?
Pre-Assessment

Approval of Methods
Review by Customer Management and Legal
Discuss Political Implications Of Methods and Findings

Pre-Assessment

Pre-Work – “The Grind”
Internet
Phone Number
Contact Names, titles, interests, locations
Local Lunch Restaurants
Telephonically

digital self defense
Assessment

Doing the work

Assessment

Know your story.
Be prepared to answer any question related to your topic, know keywords, names, etc.

Confidence.
Be confident and aggressive, your worst enemy is usually yourself. If you look and sound the part, people don't ask questions. If they get suspicious, be aggressive like "I'm just trying to do my job"

Look the part.
If you're dressed for the part, people automatically trust you. After all, who's going to wear a utility belt with multi-meters and wire cutters and stuff if they're not actually from the phone company?
Assessment

Document

Every event, phone call or encounter
  Date, time and location
  Discussion
  Did you achieve your goal

Assessment

When things go wrong
  Minor Problem
    Use your cover story
  Being Stopped
    Use your cover story or
    Admit to project – “Get of out Jail Card”
  Being Discovered
    Admit to project – “Get of out Jail Card”
Post Assessment

The Report

Process and Discovery
Define Methods
Document Discoveries
Identify Weakness
Recommend Mitigation

Identification of Targets
Names, Contact Information
Disclosure of this report may
Can Get Someone Fired or Demoted
Against EU Laws

digital self defense
### Post Assessment

#### Mitigation

**Security Policies**
- Hiring
- Escort
- Vendor/Visitor
- Badge
- Camera
- Tail-Gating
- Document Handling & Labeling
- Shredding

- Discussion of Confidential information outside the office
- Sign-In
- Building
- More Secured Areas i.e. Server Room
- Anti-Malware
- (Virus/Trojan/Spyware)
- Unauthorized Software

---

**Security Procedures**
- Incident Handling
- Telephone System
  - Voice Mail Passwords/Names
  - Out of Office
  - Enable DID to assist in phone traces
  - Control Overseas long distance service
- E-Mail Systems
  - Out of Office
  - Anti-Malware

---

digital self defense
Post Assessment

Mitigation

Good Physical Security - Outside & Inside
Mark Sensitive Documents
Signage
  All Doors
Enclosing the Smoking Lounge
Periodic Audits

Security Awareness Program

Goals
  Recognize the Signs
  How to protect
  Who to contact
Make it specific to Job Classification!
  IT – Help Desk, Programmers, System admins
  Management
  Other
Make it Fun!
Post Assessment

Security Awareness Program Message

The audio is NOT true!

Employees at all levels need to believe that they are an important part of the overall security strategy designed to protect the organization, its assets, and all those that work and live on at the facilities from the negative consequences of social engineering.

SEC-U-R-IT-Y

Parting Words
Parting Words

Sign all contracts before work is started
Over Communicate with customer
Have “get out of jail free” documentation with you at all times
Follow and document all activities
Have Fun!

References

Where to find more
References

Definitions
http://en.wikipedia.org/wiki/Social_engineering_%28political_science%29
IA-CMM - http://www.iatrp.com/
http://www.blackhat.com
http://www.sans.org
http://www.defcon.org
http://www.cert.org
http://www.us-cert.gov
http://www.socialengineering101.com

The Social Engineering Engagement

Joe Klein, CISSP NSA-IAM...
jsklein@mindspring.com