Elicitation Unleashed

To become a successful social engineer, one must learn how to extract information from someone or something, the techniques that a social engineer uses are the same techniques spies and agencies like the CIA and DOD use .

Elicitation is used to get to know people better. We use this to make mental judgments of IF and HOW we will develop a relationship with a person. In the case of an individual or group of people, this is something we do every day by talking, listening, and asking questions.

The Social Engineering Tactics

The goal of elicitation is to extract information that is meaningful and relevant to the overall objective of gaining access to the target assets. The familiarity of the communication process can help when you’re engaged in active elicitation from a target. The simple process of having a conversation, sharing information, and asking well placed questions should not trigger a defensive reaction from the individual if it’s done in a seemingly innocent and casual manner.

On The Internet

Elicitation via electronic means is also a viable and active attack vector. Spoofed emails and malicious websites that fool a user into providing their personal information or account credentials are excellent examples of eliciting information for use in obtaining access to a target system.

Elicitation Preloading

Preloading is influencing subjects before the event. Think about a movie's pre-release trailers. They use desired outcome words such as “The best film you have ever seen!” This technique works great when introducing anything. Preloading is a component of a social engineer attack.

How to Become a Successful Elicitor

we can simply say, "How to be a great communicator".

Steps To Success

The steps to becoming a great elicitor may seem simplistic, but initiating these on the fly is not so easy, especially without notes and to make it seem natural.

1. To become a successful elicitor it’s crucial to understand how to communicate with people.

2. You must learn to be adaptive, this means your communication must be made to fit the environment and situation.

3. It is crucial to build a bond or relationship with the potential "target".

4. Your communications should also match your pretext, otherwise you might seem out of place to the people your communicating with. If your pretext is a member of the IT staff then you need to know, understand, and be able to effectively communicate enough technical information to appear convincing.

5. Really it all boils down to this: You must know how to ask intelligent questions that will force a response. Questions that can be answered with a simple "Yes" or "No" are not good questions at all.

Consider the questions "Hot out today isn't it?" and "What do you think of today's weather?". There is a world of difference between them. One almost forces the target to just nod and say "Yup" or "Not too bad"... whereas the other might elicit a response like, "I think it is too hot today. It makes my allergies act up". The second response provides much more valuable information about this person.

Types of Questions

Open Ended

When we ask good open-ended questions we will learn about a person's perspectives, values, and goals as well as interesting little info about them that can be used later on. In addition, this builds a feeling of closeness and rapport with the target.

Close Ended

Close ended questions give us control of the conversation and allow us to lead where it may or may not go.

Neutral

This type of question does not tell the person how we want them to answer, there is no leading or directing, it is just.... neutral and can go either way. "How do you like the weather today?" is an example of a neutral question.

Leading

These type of questions really force or try to lead the person down the path to the answer you want. "This weather is pretty hot isn't it?" Beware though, these questions should only be used after you have penetrated resistance, otherwise you can turn the person off and loose all control.

Assumptive

This is a powerful tool because we can put the person at ease by assuming certain things about them, their actions or thoughts. "Whats the most paper you've ever stolen from the company at once?" This question assumes they have stolen paper or other things and may put them at ease that they don't have to admit it. Whatever the answer, it is key to act as if you expected it or you loose the power in the elicitation.

Key Points

Now that we have in mind the type of questions we can use we should also keep these key points in mind:

Too many questions can shut down the interaction

Too little may make the person uncomfortable

Ask only one question at a time, too many will cloud the answer you get

Use a narrowing approach to questions to gain the most information

References :

DOD Polygraph Course

Brad Smith, aka theNURSE, donated a copy of the DOD's Polygraph Passing Course given to their agents. In this course it outlines many different aspects of a good social engineer that all tie into elicitation, all of which will be discussed in this framework.

<http://social-engineer.org/wiki/archives/BecomeSuccessElicit/dodpi-interrogation.pdf>

The CIA's Secret Manual on Coercive Questioning

<http://www.parascope.com/articles/0397/kubarkin.htm>