Social Engineering Index

1. Before starting
    1. What is this training for?

This training is focused on provide basic knowledge and some guidelines for information gathering and influencing in order to succeed on LEA operations.

    2. What should you expect from this training?

Attending this training will not make you a “human hacker” in one week, but will provide you with concepts knowledge and resources to improve your communication skills in order to improve yourself in LEA activities.

Social Engineering is not a bidirectional communication way, so you will have to learn about yourself before trying to engage others.

This training will include topics based on psychology, non-verbal communications, story telling and tech tools. All this topics will conform a base that you will be able to use to improve all those skills in order to become better on communications and information gathering, that, in the end, is the final task of all LEA activities, whether for hacking targets, gathering evidences, obtaining cooperation or even interrogations.

We will focus, as is obvious, on facilitating infection deployment on technological environments, but same idea is applicable to every other aspect of human relationships.

2. Introduction
    1. Definition

Social Engineering most accepted definition is “the act of influencing someone to take an action that may or may not be in their best interest”.
This definition involves professions like doctors, therapists, teachers, law enforcement agents, etc.

    2. Why SE works?

The simple and natural answer is: TRUST.
Trust is closely linked to benevolence (http://www.ocf.berkeley.edu/~reetaban/triple%20helix/trust%20and%20decision%20making.pdf).
Those people that are best social engineers, are considered by others as “the friendliest” people they ever met. And that friendly behavior, makes people trust on them. Trust leads to information leakage and information leakage to a compromise.
So, build your target trust, and you will get what you need.

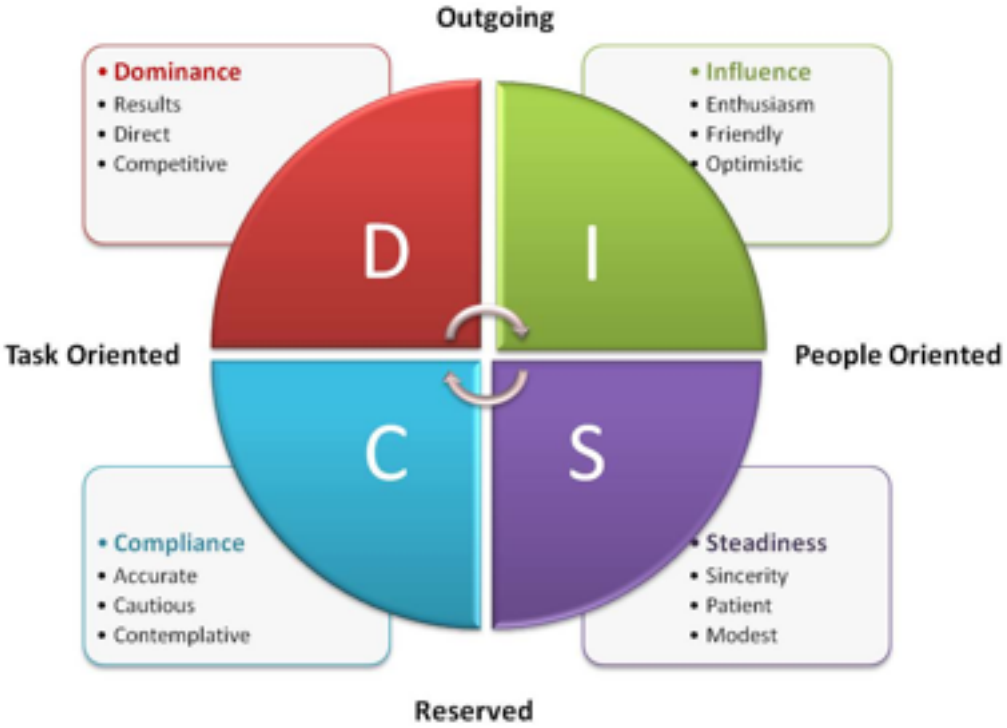
    3. Know yourself (DISC)

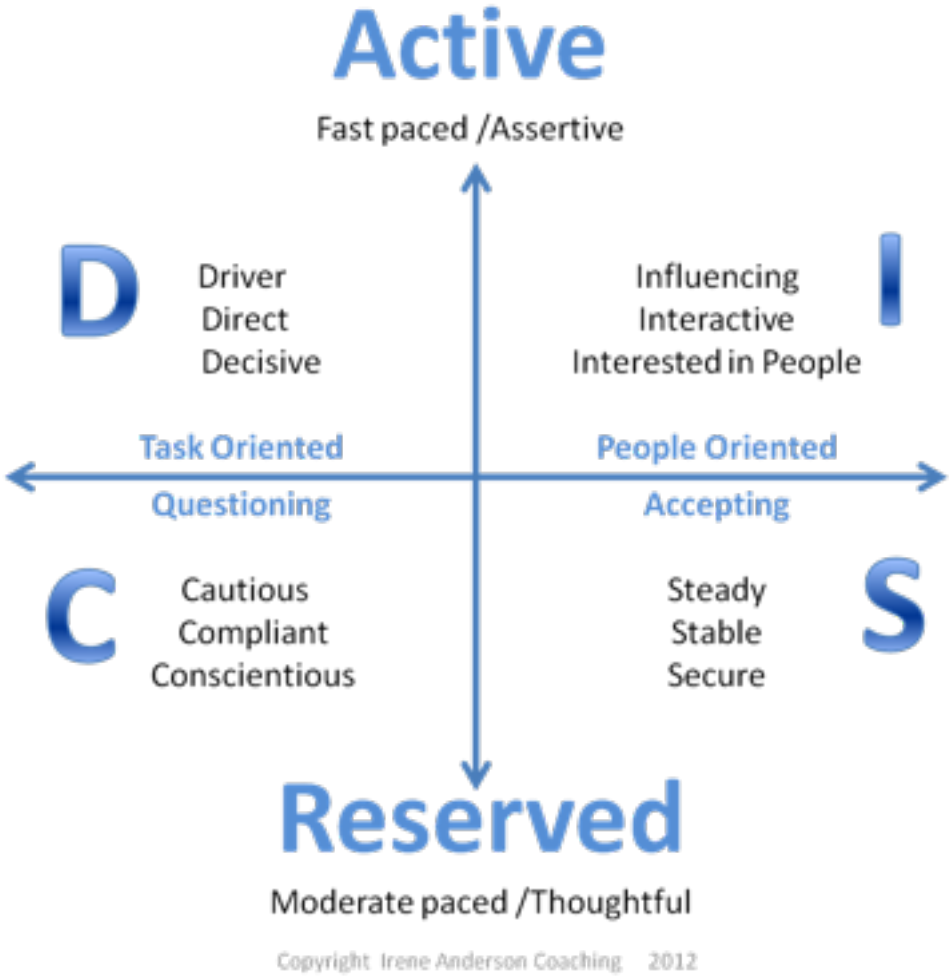
“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” Sun Tzu, The Art of War

You won´t need to do a psychological profile of yourself and your SE targets, but would be good to know yourself communication style, so you would be able to identify others and understand best approaching ways.
(http://www.triaxiapartners.com/corp/diagnostics-and-assessments/disc-assessments-pdi)

Learning how you are, you would know your pros and cons, and you will learn how to use them with other people depending on their DISC type.

http://es.slideshare.net/azazzet/modelo-disc-y-su-interpretacion





- Dominance:

Dwight Shrute - D style

https://www.youtube.com/watch?v=BMlGpDfyxEA

  - How D is:
    - Perceives oneself as more powerful than the environment, and perceives the environment as unfavorable.
    - Task oriented, direct, assertive, objective.
    - Motivated by results and challenging.
    - It´s independent and controller.
    - Carries our with dialogs. Give orders without explanations.
  - How should be treated:

    - Challenge him.
    - Establish rules and limits.
    - Be an example with actions, not with words
    - Talk directly and honestly.
  - To convince him, present him the benefits.
  - To disagree him, find a comfortable agree point and start discussing from there.

- Inducement:

Michael Scott - i Style

https://www.youtube.com/watch?v=AZ3v7V2CZu8

  - How I is:
    - Perceives oneself as more powerful than the environment, and perceives the environment as favorable.
    - People oriented, persuasive, sociable.
    - Motivated by visibility and recognition.
    - Optimistic and emote.
    - Wants to be in the focus, being listened.
  - How should be treated:
    - Give him visibility and support his ideas.
    - Help him to share and to move from ideas to facts.
    - To make him comfortable stay under him. Or to dominate him, stand up and higher.
  - To convince him, be positive and validate him
  - To disagree him,… better just let him calm down. Don´t go on direct confrontation.

- Submission:

Pam Beesly- S style

https://www.youtube.com/watch?v=heRbyUAuyKo

  - How S is:
    - Perceives oneself as less powerful than the environment, and perceives the environment as favorable.
    - Pleasant, patient, organized and persistent.
    - Wants to be part of the tribe. Being integrated.

    - Avoid conflicts and try to calm others conflicts around.
    - Do not initiate changes neither relationships.
  - How should be treated:
    - Workgroup with specialized tasks. Be friendly and recognize his value.
    - Remember him objectives but let him be warm with you.
    - Validate his ideas or let him know yours minimize troubles.
  - To convince him, minimize his problems/troubles with your ideas and talk about cooperation.
  - To disagree him,… well, just find what he disagrees and disagree with him.

- Compliance:

Angela Martin - C Style

https://www.youtube.com/watch?v=clMgH1zmPXQ

  - How C is:
    - Perceives oneself as less powerful than the environment, and perceives the environment as unfavorable.
    - Precise, meticulous, detailed y logic.
    - Looks for quality and rules following.
    - Caution is his way and do not tell to much.
    - Will listen, and ask what and why.
  - How should be treated:
    - Ask him for precision and don´t try to be more right than him.
    - Let him process information about changes and, when needed, validate his plans.
    - Explain what and why and be patient with his explanations.
  - To convince him, be right with data and answer what and why.
  - To disagree him, same thing: give him facts and data.

Video examples
4 guys discussing about communication
https://www.youtube.com/watch?v=BDeWNv6pa5A

Videos de The Office
http://discprofiles.blogspot.com.es/2013/05/disc-personality-styles-the-office-d-style-i-style-s-style-c-style.html

Dealing with a D
https://www.youtube.com/watch?v=UnAEmf_bwqs

3. Approach Techniques

Target of this chapter is being able to identify potential information sources, engage them and get information.

How to build a confidence relationship:

1. Artificial time constrains:

   Let your target knows you are not going to take much of his time. Time is a non returnable value and very personal. So let targets know that, you need 1 minute, that your wife is coming to pick you up, whatever that lets target knows when he would be free of you again.

   It´s important that this is clear when you start talking. Apart from that, be confidence with the process and use topics you know enough well as conversation starters.

2. Accommodating nonverbals.

   Body language is first thing coming unconsciously to our minds when we interact with somebody, so our target should read in our nonverbals, same thing our words say.

   If we are extremely focused on our objectives, we would be nervous and show that through our nonverbals. And this is a problem if it´s not our intention. We have to dominate our nonverbals. Instead of thinking on “I must get this info”, think about how interesting would be a conversation with your target.

   Avoid any aggressive body language, will never help.

3. Slower rate of speech.

   Adjust the way you talk. Fast speech is a stress signal. And, unless thats your pretext, you need to look quite. People with slower speech rate engage better than faster, who looks like promoting something.

4. Sympathy or assistance theme

   One of the most common human behaviors is helping others. So, a good starting questions is “Can you help me, please?”

   But your request should be easy, if it isn´t, your target could reject because takes more effort helping you than the benefit of helping (endorphins).

   Remember Time Constraints, your request must be time limited.

   Don´t be threatening. Make sure your target don´t feel your problem will become his problem.

5. Ego suspension

   Everybody likes to be the smartest, the best, the one that is right,… So let your target feel that. Tell him you don´t know, tell him you are sorry, and most important. Conversation is about your target not about you. You are not interesting for him and you are not interested on yourself but on what your target would told you.

   This will make people think how good listener you are and that is comfortable talking to you.

   Of course, most important thing of ego suspension is forgetting about our own knowledge and desires. We will have to deal with people with different moral rules and we won´t have to disagree them directly with ours.

6. Validate others

   We want to become part of target´s tribe, so we have to understand how they are and be part of it. So, we have to listen actively, not pretend to be listening, not thinking on our plans or next sentences.

   Be thoughtful, it will make a very good impression of you.

   Validate what they think and say. Agree them or make them explain why, but do not combat them.

7. Ask How? When? Why?

   Do not ask yes-or-no questions because they would most probably answer you with just a “yes” or a “no” and that´s not too much info.

   It´s much better asking open questions that would let target speaks and therefore, give extra info to the social engineer.

Taking ah hah or moving head and nodding tells your targets that you are interesting on what they saying so they would feel comfortable talking more.
Ask reflexive questions: make a question from a part of targets sentence. Example:

T - I went on vacations last mont
SE - On vacations?
T - Yes, I went with my wife to Seichelles.
SE - With your wife?
T - Oh, Mary got a new job and has only one vacations week per year.
…

You can also repeat what your target said in a summarized way so he will notice you were listening him. It is called “paraphrasing”.
Little pauses would allow you to thing on whats next in your conversation driving.

8. Quid Pro Quo

   Basically, if you want something, you have to give something. If you just request, your target would become nervous as he realizes that he is giving and not receiving. You can add info inside your questions like
   “Oh, are those your kids with your dog? My daughter is 5 and she also has a boxer”
   You can say this pointing at targets picture on the desk. You are telling info about you before he tells anything, and you are becoming part of two tribes your partner belongs to: “parents” and “dog-owners”.
   Info you provide doesn’t need to be real, but should be something you can keep alive and you can emulate without mistakes. Improtant think is that target doesn’t thing he is monologuing even if he is.
   Keep in mind when you provide info, that conversation is about the target, not about you. Target is not interested in your life.

9. Gift Giving

   Giving something valuable to other people makes rapport between them and you. The most important thing here is word “valuable”. Gift doesn’t need to be something expensive, but something target wants and/or needs. And much better if it is something that demonstrates that you listen what target is saying, that you are sincerely interested. This will make target more comfortable with you.

   Gifts could be suggestions or even warnings. If you are at your desks, on a call and can’t take a note, if somebody offers you a pen, is helping you a lot. If you are watching your Facebook at office computer and somebody tells you that boss is coming to the area and he is really pissed off today, you will thank a lot that warning.

10. Manage Expectations

    Following previous techniques, you are making your target feels better after meeting you. So focusing on that, those techniques will be easier to apply than if you are thinking specifically on them.
    Never forget the info you want to acquire from you target, but don’t let him feel bad about meeting you because will make him close against you in case you have to come back to him.
    So, if our first target is making the other person feel good, then the second part, gathering information, would be much easier.

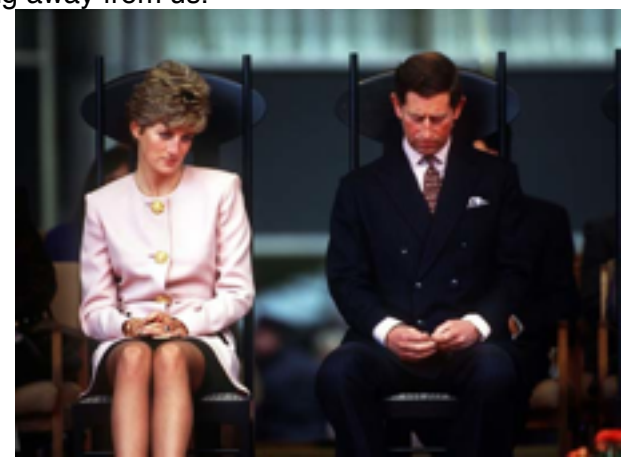
Choose and analyze your target(s):
You can’t attack without a plan. In fact, first of all, you have to choose your target. You have to find the person in your target organization who can provide you the info you need. That info source should also accomplish with the physical and personality that you can manage.

So, if you would like to attack your own organization, as a complete stranger, who do you select as your first target? Remember that you have to choose target based on what you could know from an unknown person, so ask you some questions about target:

- Who
    - Age
    - Sex
    - Employment / access
    - Family
    - Income
    - Social habits
    - Communication style
    - Needs or wants
    - Hobbies / interests
    - Political affiliation

Make your body match your pretext:
Identify if a person is “close” to approaches:

- Body is angling away from us.

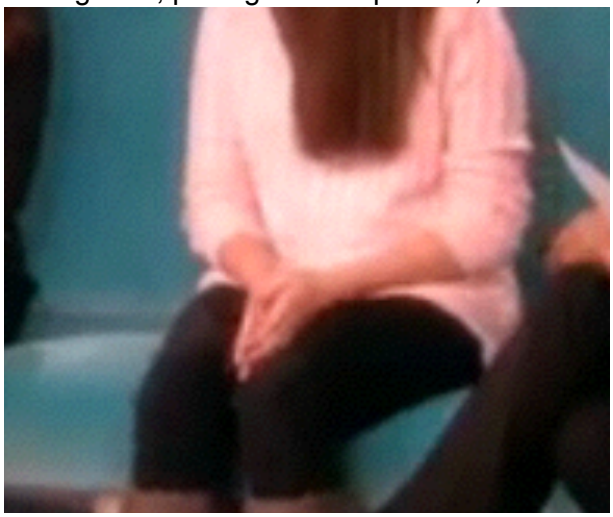


- Lip compression

- Brow furrowing (line between borrows)

- Palms don't display

  Closing hands together, putting them in pockets,



Target will be more "open" when:

- his body points to you, even bladed to you:

- greets you when you go closer by smiling, eyebrow flashing,…

- If is showing his hands, mainly showing palms up, target is welcoming you

The opened the target is, the easiest is to engage. If your target is closed to you, you have to adapt your speech and body language to try to open him to you.

Your brain judges people before you realizes:
http://www.washingtonpost.com/news/speaking-of-science/wp/2014/08/05/your-brain-helps-you-judge-a-face-before-you-even-see-it/

Props
Props are all those things that are part of people image, both physical an psychological that supports who they are or pretend to be. Clothes, jewelry, hair style, add-ons, gadgets,… Idea is having same external appearance you want to belong to.
So you need to know the attire your target will accept better. The image will convince him better. Pay attention to unusual things, both that you have to get to have desired attire, or that you have to get ride off.
Make a list with props to use and props to avoid.

i.e. if you pretend to be friendly in a motorbike pub, don´t go with a suit.
i.e. if you pretend to be plumber, don´t wear a suit.
i.e. if you pretend to be doctor, don´t show 1000 tattoos and piercings.
etc.

Goals expectation
You want to coax your target to tell you some info you need, but you have to decide, before engaging, what do you really need. So deciding, from all information you could gather, what would be good, what would be reasonable and what would be the ideal.
Make those three lists and based on what you are getting, decide when to retire from the engaging.

Starting the engagement

Your first approach is the first idea your target will have about you. And is longest lasting impression about.
Your props, body language and first words should match the role you want to play, both with its personality, intentions, desires,… So consider next options:

- Lateral topics: Start talking about a topic related with your target info, so you could move from that topic to the one you are interested in.
- Everybody complains: when somebody complains tells you about personal things that are disturbing and, interesting or not, means that target is confidence enough with you to share that personal info. You can provocate or complain
- Everybody wants to be believed. Find the topic your target is interested in being trusted.
- By de quid pro quo, offer something to your target before making a request
- Through total Ego Suspension, be under and behind your target: he “is” smarter, taller, stronger, more accomplished, more successful and more knowledgable than you. Don´t threat him.
- Flatter your target. So simple, so easy.
- Give extra value to the to the things target talks about. Add extra info that support your target facts.
- Tempt your target to correct your statements. Be carful, not offensive.

4. Elicitation

Elicitation is not just asking questions to get answers, is stimulating specific targets behaviors.

- People like to be polite.
- Professionals like to show how much well informed they are.
- The most you eulogize a person, the most he likes to talk about himself to get more flatters.
- People lies because they need, not because they like.
- If you look like worry, people will try to help.

Advises:

- Don´t be avaricious: people will tell you what you need. Give time and spend effort, but don´t make pressure or targets will close. Better inducting a topic than asking directly. To practice, ask some friend, colleague or relative about something very personal or uncomfortable to check how body language changes and remember it during your operations.
- Be natural: watch people know each other talking between them: body language, facial expressions, reactions, … Analyze and use it. To practice, go into others conversations. The most you practice, the more simpler and natural will become.
- Knowledge: gather info about topics you need to talk about. Don´t go talking to a doctor about medicine if you don´t know about. To practice, try to read about a topic you don´t know at all and try to keep an intelligence conversation with somebody that knows a lot about that topic.

Elicitation principles:

Preloading elicitation:

With your behavior, gestures, expressions and personal image, you will have to tell your target the tone of conversation you are about to have. This will make target be ready in advance and not surprised. Also will avoid contradictions between your preload and conversation. You can study how journalists changes their expression way when they start giving a piece of news depending on the topic.

Invoke others Ego:

As explained, peoples ego is a very powerfull tool to make them talk. Not only arrogant people, but all of us. And everybody likes hearing good things about themselves, so we can feed our targets ego by flattering their stories/topics about themselves to make them talk more because they like to like.

Anyway, be sincere, do not exaggerate because then, a flatter could become in an insult.

Examples:

Good:
I read a nice comment about your product X in Amazon. I think it would be useful also for Y.
Bad:
I saw you sell best X product ever done. Tell me all about it.

Good:
Are those children in picture your sons? They look happy. 5 and 8 years old?
Bad:
Oh, your boys are cutest children every seen!

Good:
Ah, so you drive a Ford X. Is it so comfortable as it looks like?
Bad:
You are very intelligent buyer, Ford X is best car ever! Is it too expensive?

To practice, get a topic you know a little bit about somebody and ask him in a positive way to check how deep can you go in that topic.

Common interests:

One of the most normal ways to build a tribe is having same interests as other people: Bikers like to ride their motorbikes together, there are reading clubs, comic conventions, gastronomy clubs or conventions,…
Explore your targets hobbies and interests so you can learn about them to be able to have an interesting and intelligent conversation about things your target likes. Don´t pretend to know more than target. Remember you have to appeal to his ego and that´s very positive when someone is the best knowledgeable about the topic of a conversation and much much more if this topic is the person interest/hobby.

False statements
Be wrong, be absolutely wrong about a topic known by your target and you will get the correction.

Example:

> Petter told me you developed your client app for Android. Didn´t you found security failures about the platform?
> If your target was part of the project, he will feel directly involved by your statement and he will want to correct because the security problems are not so important, or there are not, or whatever is the truth.

And after target corrects you, you thanks for it and demonstrate he knows more than you so you would like to learn (yes, ego again).

Inhibition
This is a polite title for Alcohol. When people drinks, loose fears and embarrassment. One of the best examples are embassies. All Embassies make parties and other ambassadors and their crews are invited. Alcohol never lacks, and making other drinks keeping your own control is an art itself. Ambasadors work is getting info of other countries and alcohol is one of their tools. Yours too.

About questions:
Asking “what is your password?” does not work (usually). So try to get info pieces that would help you to realize which it could be.

- Open-ended questions:

An open-ended question shouldn’t be able to be answered with yes or no. Use simple questions to start with, even yes/no questions that lead you to ask the open-ended one.
You could ask to your target, in appropriate context, of course, if target´s car works with gas or diesel, and how did you calculated your distances/expenses to choose that gas/diesel?
You can use also reflexive questions based on your target answer and then keeping silence. Your target will need to fill that silence and the easiest why is answering the open question you asked.

- Close-ended questions:

These are the yes/no answered questions. Questioner provides the information and target just confirm or denny. Would be helpful to make target answering easy questions and, sometimes, could become a resource for false-statement placing that target would like to correct.
Do you have a red car?
Were you visiting Mr. Smith last Saturday evening?

- Leading questions:

Combines previous but are like if you were just giving info and waiting for confirmation. Would let your target understand what you know something he didn’t expect..
You drive a red card, don´t you?
You were visiting Mr. Smith last Saturday evening, weren’t you?

- Assumptive questions:

In this case, you let target asumes you already knows something wile you are asking other thing.

What car were you driving to go visiting Mr. Smith last Saturday evening?

In this case, you give the visit, the visited person and date as right, while you ask for the car. If target answers just about the car, then the other statements are true, if they were not true, he would correct you. Anyway, is really dangerous using wrong statements in this kind of questions because target can realize you have no idea what are you talking about.

Keep in mind that last Close-ended, Leading and Assumptive questions are very powerful in interrogations but in covered SE, could make your targets closes.

5. Information gathering
    1. No-Tech information gathering
    2. Technology based information gathering
6. Preparation tactics
    1. Pretexting
    2. Influence and Manipulation
7. Psychology
    1. Framing
    2. Non verbal communications
    3. Amygdala hijacking