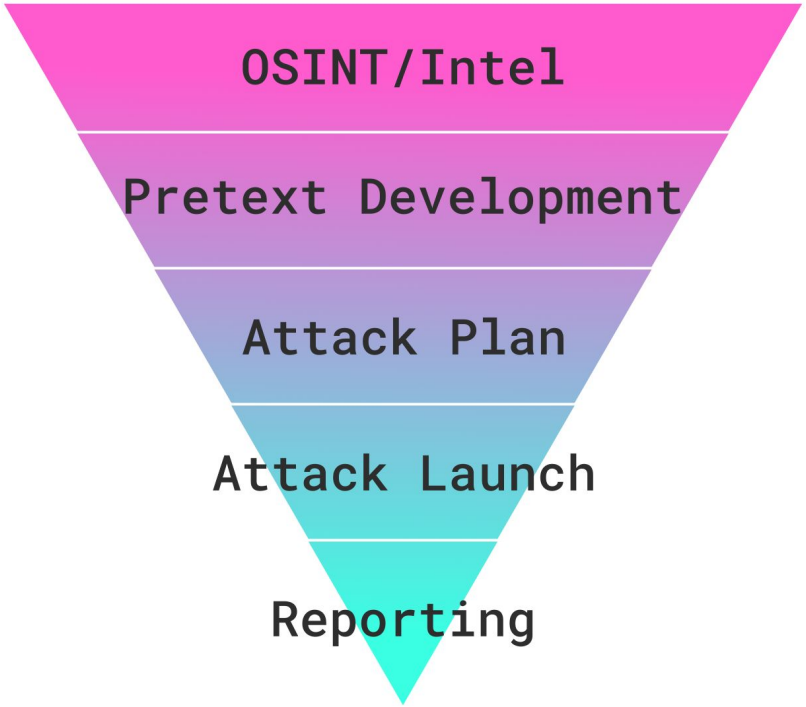

crackc
crackchester
chester
Social Engineering 2
Workshop 10 - 09/03/23

Social Engineering Pyramid



Open Source Intelligence (OSINT)

What *information* do you need to gain access to a target?

What *buildings* do they have and *where* are they located? Do they have a byod or internet access policy? Are there floor plans of any buildings?

You can also get information on employees. Finding out what their **role** is and if they work from home is useful. You could also get *personal information* and try to form a way with that in mind

Physical OSINT

Clothing - What uniforms if any are people wearing?

Entries and exits - You will need to get in with as *little notice* as possible and out in the same way

Requirements for entry - Key card access or a pin pad?

Is there any perimeter security or security staff?

What is the lobby setup like?

Accessing Cameras

A popular piece of webcam software for windows 7 was called *webcam 7*. It’s not so hard to find webcams that still use this software with a well structured google search such as

intitle:"Webcam 7" inurl:8080 -intext:8080

There might be exposed cameras like these in your targets location, it will always be worth it to try and find any

Profiling Through Communication

We can use the **DISC** method for identifying personalities

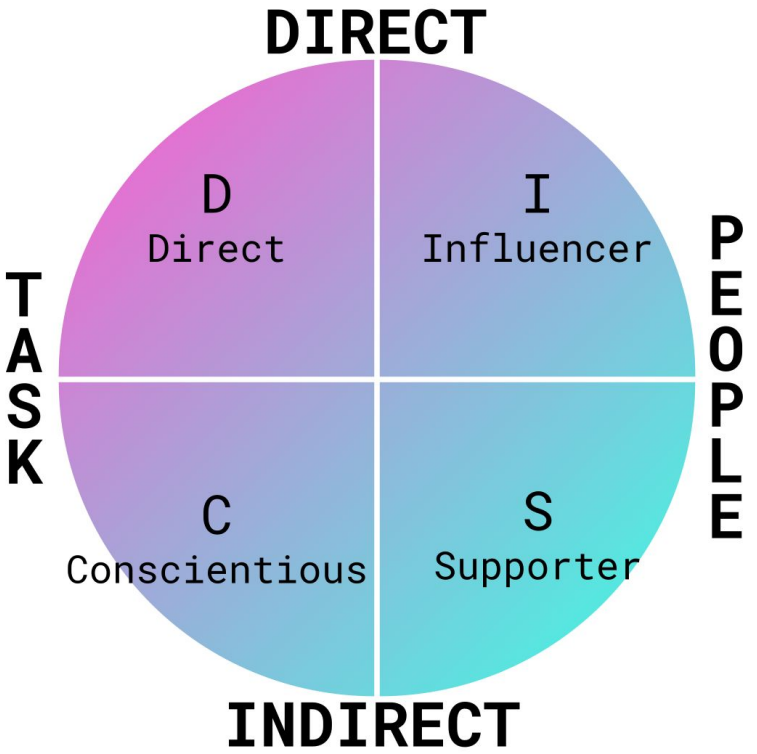
Every person can be placed into one of:

- Direct
- Influencer
- Supporter
- Conscientious

Once you figure out which they are you can ***direct the conversation*** to go how you want

Direct **I**nfluencer **S**upporter **C**onscientious

Profiling Through Communication



The DISC Method

Identifying a target's personality type:

D: A *direct* person will be firm, strong willed and forceful. Often they will be very results oriented

I: An *influencer* will act with enthusiasm, keep things optimistic and be lively and outgoing

S: *Supporters* will be accommodating, patient. They will act with tact and stay humble

C: *Conscientious* people will be analytical and systematic. They will usually act more private and reserved

Direct **I**nfluencer **S**upporter **C**onscientious

The DISC Method

When talking to each personality type If you're **in a position of authority** then you should aim to be:

D: Be direct and firm while trying to keep things brief

I: Act friendly and let them lead the conversation

S: Talking systematically and with consistency. Be friendly and **asking questions** clearly is important

C: Ensure knowledge relating to the target. Be detailed and reliable.

Direct **I**nfluencer **S**upporter **C**onscientious

The DISC Method

When you **aren't in a position of authority** such as talking to a helpline over the phone:

D: Give them options but make sure you get the result you want. Keep things logical and use facts.

I: Keep introducing new things to the conversation and don't talk too much. There should be a give and take.

S: Be patient and ask questions about how things work.

C: Use lots of data and statistics. Along with logic and facts. Maintaining reliability is key

Direct **I**nfluencer **S**upporter **C**onscientious

Pretexting

- What are your *goals*? Be ***specific*** about what you want to do.
- Understand the difference between reality and fiction and try to ground your answers in your personal knowledge.
- Knowing *how much* information to give away and *when* is a very important tool.
- Avoid short-term memory loss and keep things fluent by *practising* your pretext with a friend or colleague
- Getting support, What are the relevant tools or information?

Attack Plan

Planning an attack is using all the information you have to *strategise* a way into your target system.

You should have an entry and an exit route in your plan. You should also know about any cameras that can see you.

Knowing what you can't do is always important. You will need *authorisation* from the client in order to get away without repercussions.

Attack Launch

Once you have your **plan** it is time to put it into action

Make sure that you have **a *‘get out of jail free’* card**

Don’t follow a script, this can make you freeze if something unscripted happens, follow notes where you can but *improvise* where you can’t

Reporting

This is the step you're actually **getting paid** for.

You need to ***detail everything*** you've done up to this point in a ***concise*** way to show to your client.

It should include things such as their vulnerable OSINT and any methods that can be used to easily gain access to either their buildings or system

Your Turn

Hidden somewhere is a ***key*** for you to find, the *first* person to do so will ***win a prize*** at the end of our social engineering series!!!

Using the skills you just learnt you need to blend in and find the

Our helpline number is 07496 684 645

Once you find the key head over to crackchester.cc/admin to get the code to win the prize

Good Luck! :)

Crackchester

Here’s a link to our link tree where you can find all our socials and our discord!