Social Engineering 1

Workshop 9 - 02/03/23

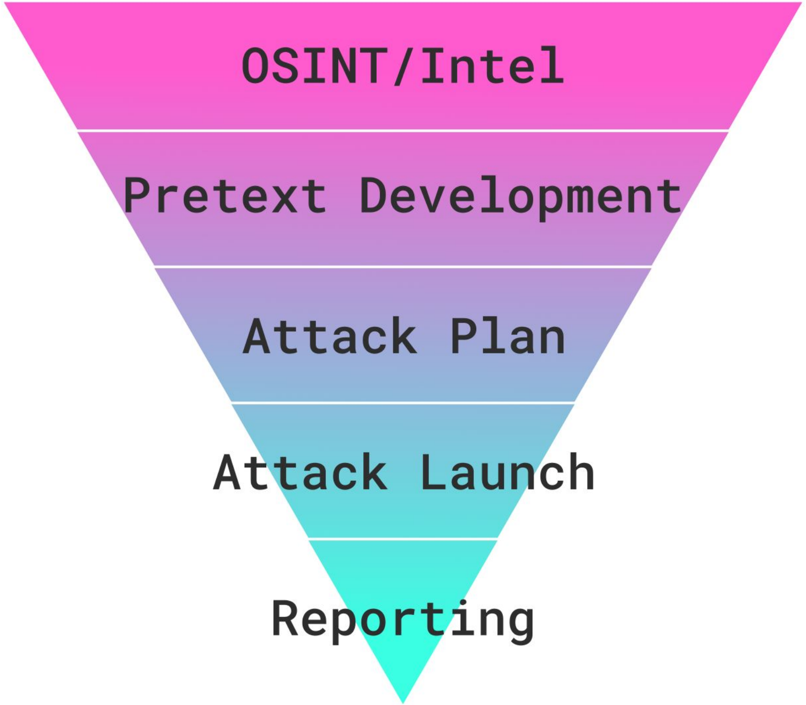
Crackchester.cc

Check every once in a while to see what **events** we have running soon

Whether you missed a **workshop** or just want a **recap** then check out the workshops page for all our past content

If you want to find out about any **opportunities** from our **partners** then visit our partners page

Social Engineering Pyramid



Open Source Intelligence (OSINT)

What kind of questions should you ask? What information do you need to get from a target?

For a corporation its things such as social media, who their vendors are and how payments are issued and accepted. Whether they have call centers and where they are located along with their other buildings along with their specific policies.

When its an individual then its background information like **hobbies**, which you can find with social media. What their **job** is and are there mentions of them online? Websites with forums, clubs etc? If they are a homeowner there could be documents for this along with taxes or liens

Using Google To Search Targets

Search Operators	Usage Examples
intext	intext:apple
site	site:apple.com
inurl	inurl:apple
filetype	apple filetype:pdf
cache	cache:apple.com
info	info:apple.com / id:apple.com

Profiling Through Communication

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

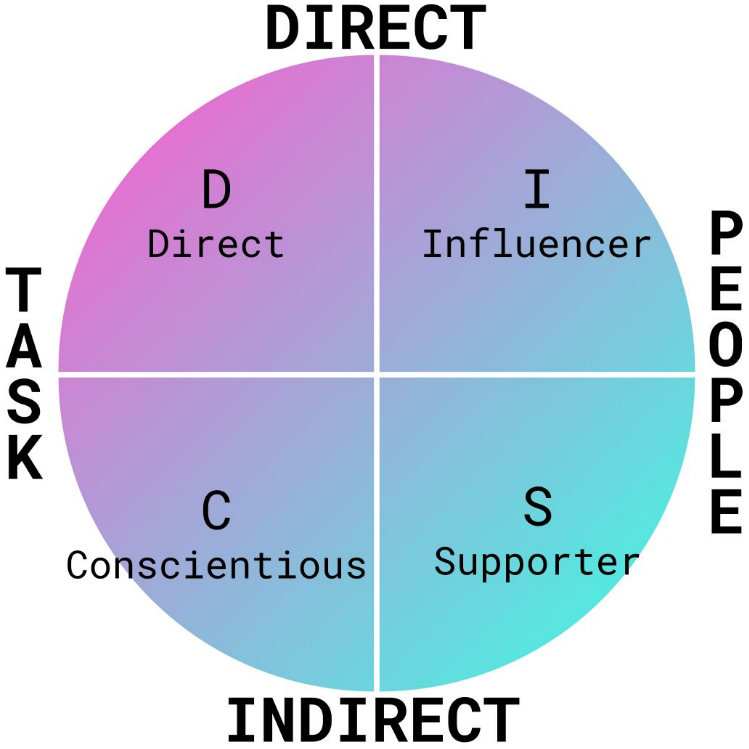
Every person can be placed into one of:

- 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

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

Attack Plan

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

Such as **rewriting all your notes** in a more helpful way and making sure you have all the pieces you need to gain entry

More detailed attack plans can even be used to gain access to buildings.

Attack Launch

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

Make sure that you have **practised** this enough as this will help with nerves and keep conversations flowing

Don’t follow a script, this can make you freeze if something unscripted happens, keep notes and make sure you can think things up on the spot if you need

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 figure out where it is

You will need to question our committee in order to find out your OSINT and progress from there

Good Luck!

Crackchester

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