Subject:

Social Engineering

- gather info about the user (most important)
- build a strategy & a backdoor based on the info

★ You need social engineering when you cannot become the man-in-the-middle.

★ MALTEGO is an information gathering tool. Target can be a website, company, person etc.

★ To run it: go to kali → maltego → run

→ login to the software

→ You can install transformers acc. to needs.

★ Create a new graph. This is the main workplace where info is shown.

→ On the left are entities. You can select any acc. to use.

→ You can modify properties of any entity.

★ Lets put a new person to the graph.

→ Set the first name & last name

→ Right click the entity → all transforms

↓

ask whatever you want

→ Say you search for websites, it will show you all the information about websites that are associated with that name.

→ Delete the things not useful.

→ Get the information you need to create an attack strategy.

★ One you get, say, an email address of the ~~associated~~ Target person & say you have their twitter then:

Subject :

PAGE NO.
DATE :

→ copy the profile link
→ add a twitter entity from the entities in maltego
↳ go to manage entities to add an entity if its not already there.
→ set the link of the twitter entity as the URL you got.
→ Run the transform (say get twitter friends)
→ You can use friends to set up an attack.

☆ Now, lets gather info using email.
→ In maltego, add email address entity.
→ change properties
→ run transform. & get all info needed.

☆ You can keep going to gather more info abt the target. After gathering is done, we need to analyze it.
→ You can create a complete mind-map of the info you have for the target.

☆ Now, we need to know how to combine our backdoor with a normal file so that user doesn't get to know whats wrong.

→ We will use a download & execute script that:
→ downloads a normal file to display to user
→ downloads the backdoor ~~in~~ & run in the background.

☆ In the code (downloaded from udemy), just change the $urls variable.
↳ include, say, an image link
↳ and the backdoor link (use direct urls)

Subject :

PAGE NO.:
DATE:

★ Compile the script to an executable & change icon.
↳ rename file & change extention to .au3
↳ go to kali → compile script t...
↳ source: file that we made
↳ destination: exe file
↳ change icon of the exe.
↳ convert

★ This will make it an .exe executable.
→ copy this to the web-server
→ listen for incoming connections on metasploit
→ once windows target runs the .exe, the image will be displayed on their PC, meanwhile you'll gain full access to it.

★ We now need to spoof the extension .exe to .jpg if an image ; .pdf if a pdf etc.

↳ Copy the name of the file.
↳ say old = social-eng.exe
→ say new = social-exe
→ we want = social.jpg
↳ To this, we'll do a right to left reader
→ new name we want is :
~~gtrgpj.exe~~
social gpj.exe
→ now put right-to-left ch:
→ go to google & search right to left Override
→ copy the character & add it:
→ social-gpj.exe
↑
the character

Subject :

PAGE NO.:
DATE:

→ Now file name will be shown as:

socialexe.jpg

* Rather than sending it directly, send it via a zip file so that browser does not remove right-to-left override.