Social Engineering Lab

Darshan Mehta and Raj Pandya

Part 1: Race to crack the security code!

Use you social engineering skills to get your way into this persons email account!

Below is the information you know about him:

Name: Landro Baresi

Birthdate: March 4th 1984

Hints and Tools: https://www.osintframework.com

https://inteltechniques.com

Suggestions:

- With the help of Google and Facebook, a lot of information is publicly available for you to use.
- Begin with searching 'Victim Name Facebook Profiles' on Google and click the first link. This will bring up a list of Facebook profiles that match this users name. Sometimes, if the name isn't popular, Facebook will show results for similar names. You can always modify the URL to get FB to search for exactly what you want.
- Once you've done that, scan through the list of profiles that match this user. To see more information about an individual, you may have to login to your own account — hint: you don't have to be friends with an individual to see their information all the time. You simply need to be logged in.
- Now that you've found their profile, this part is easy — look through their profile, click on various sub-sections of FB such as 'Photos', 'About Me', 'Associated Websites' and you will find connections to other profiles.
- For our case, you want to get to know the person a little better so look for LinkedIn and Instagram. Both of these social media websites provide intimate details about a persons career and personal life style, giving you the advantage of imitating them in social engineering attacks.
- On LinkedIn, again, click through various sections and you'll see 'Contact Info', which contains an email.
- Taking the domain of that email, you should now be at the email service providers login page. It can be tough to guess someones password. Fortunately, nowadays, when creating an email account, you have to link a phone number with it.
- Unfortunately for Landro, he's using a very old email service provider that allows you to reset his password with a simple security question.

- Try to reset his password by answering correctly to only one question. Hint: remember we mentioned Instagram earlier? When social engineering, it's important you keep track of all the users information and connect it to create a map of the person.
- Great! You've spent the last hour or two trying to figure out his security answer and you're in! Now you can extort him by sending him emails through his own account, you can send emails to his contacts to spread your attacks, and so much more.
- But don't. Be a good citizen and report any malicious activity that you see someone doing in regards to social engineering. It's illegal so be a good human being!

Part 2: Find information on your partners with OSINT!

OSINT is a very powerful dictionary of free tools that can be used to find publicly available information. Check out some of our suggestions below and see if you can find out information on your parents, friends, and relatives!

Suggested tools:
- https://inteltechniques.com/menu.html
  - Username > Username Search Engines > Check Usernames
  - Transportation > Vehicle Records > Vehicle Purchase Records
  - Archives > Web > Look for previous versions of UTM websites
    - http://www.cs.toronto.edu/~arnold/

Lesson:
As we get more and more deeper into this age of technology, our privacy seeps away for convenience, for pleasure, for belongingness. With that, attackers are finding various ways to exploit these weaknesses of our society and look, they only need a handful of people to fall for it a month (out of the billions of tech users). We hope that we've shined a light on the importance of protecting your information, and we truly hope you share this with your friends and family —

Be careful what you post online.
Make sure you have 2FA set up on all accounts.
Question everything that you get from the web — information, downloads, etc.