Lesson 5: Social Engineering

by Justin David Pineda

When I studied and took EC-Council's Certified Ethical Hacker (CEH) in 2013, I learned a very important lesson: even if you follow the hacking methodologies, it only has a 10% success rate. This lesson has, on the other hand, 90% success rate. In gist: Why would you spend a lot of time to brute force a password when you can just ask for it? That's social engineering.

Social Engineering is an attempt to gain information from a victim or target through manipulation and deceit. The attacker attempts to gain the victim's trust then exploits the emotions of the latter.

Note: There is a reading I wrote in 2011 that is relevant with this lesson. Copies will be/are given during class.

Why is Social Engineering very successful?

In the past lessons, we studied about Defense in Depth. This means that in every layer of security, there should be protection. Now in Network Security for instance, you may deploy and implement a firewall. The firewall has its limitations but it will strictly enforce whatever rules are written in the ACL. If it says allow web traffic, it will allow web traffic. If it says deny FTP traffic then it will deny FTP traffic.

Problems rise when humans intervene. Let's say a school enforces a "No ID, No Entry" policy. All students are required to wear their ID upon entering the school. One day, one student forgot to bring his ID but the guard still allowed him to enter because they're friends. Is it correct for a guard to make exceptions even if there's an explicit ID policy? What if the said student brought his friends? Will the guard still allow it because they're friends?

Humans or wetware are the weakest link in the security chain because they simply make a lot of exceptions. That's why the human vulnerability is a weakness that no patch can perfectly fix.

Ethics: Social Engineering in Penetration Testing

In penetration testing, a third party service provider actively tests the security solutions implemented in the network. Active testing means exploiting discovered weaknesses in security. One of the tests is the social engineering test. In this case, the pen tester tries to bypass security through social engineering.

For example, the company security policy requires the use of a badge/ID to enter the office. The pen tester will carry a lot of heavy things so the guard will help him instead of looking for the ID. The pen tester successfully enters the facility with the guard as accessory to the crime. After the pen testing, the guard is terminated due to abandonment of duty during the test.

It is the job of the pen tester to lure people into breaking the policy. The targets, out of good-will, will help them. But in the end, they will be terminated. Is that ethical?

Steps in Social Engineering

There are three steps in social engineering.

1. Information Gathering
   In this step, the social engineer gathers as many information about his target as possible. He can do online searches in social networking sites, stalk the target to learn his routines and talk to his friends to learn more about his likes.
2. Developing Relationships
   After you have gathered enough information about your target, it's time to build relationship. Let's say you learned that the target likes Justin Bieber. You can create a "perfect encounter" with him in his daily routine. You could probably sit beside him in a bus and have a little chitchat about Justin Bieber. Ideally, you can build a relationship with the "serendipitous meeting." In some cases, you will need to "invest" on something. If you learned that the target is in a lot of debt, aside from being a Justin Bieber fan, you can use that to your advantage for the next step.
3. Exploitation
   In the last step, you push through with your goal of eliciting the information you need from the target. You may have allowed your target to borrow a sum of money from you so that he can pay his debt. Now, you can use that to your advantage. You can ask for the information and remind him that he is in debt so he should return the favor. In this case, you are successful in your mission.

Types of Social Engineering Attacks

The Social Engineering Attacks can be classified into 2 categories:

1. Non-technical – Doing social engineering in a traditional way
   a. Dumpster diving – Literally checking the target's garbage.
   b. Shoulder surfing – Glancing at other person's computer, cellphone or paper.
   c. Impersonation – Pretending to be key personnel in your target's company.
   d. Tailgating – Walking in the vicinity after the person ahead of you taps his badge to open the access door.
2. Technical – Doing social engineering using technology
   a. Phishing – Getting target's information using fake e-mail or website.
   b. Spear phishing – A type of phishing targeting a particular person.
   c. Pharming – A type of phishing targeting a group of people/organization.
   d. Vishing – Deceiving target using telephone/cellphone/smart phone.

----- NOTHING FOLLOWS -----