
Attack process

We have presented some basic steps that are required to initiate a social engineering attack against your target. This is not the only method or even the one that is the most likely to succeed, but it should give you an idea of what social engineering entails. Intelligence gathering, identifying vulnerable points, planning the attack, and execution are the common steps taken by social engineers to successfully divulge and acquire the target information or access:

1. **Intelligence gathering**: There are many techniques to determine the most luring target for your penetration test. This can be done by harvesting corporate e-mail addresses across the Web using advanced search engine tools, collecting personal information about people working for the target organization through online social networks, identifying third-party software packages used by the target organization, getting involved in corporate business events and parties, and attending conferences, which should provide enough intelligence to select the most accurate insider for social engineering purposes.
2. **Identifying vulnerable points**: Once the key insider has been selected, we would move forward to establish the trust relationship and friendliness. This would ensure that an attempt to hijack any confidential corporate information would not harm or alert the target. Maintaining a high level of covertness and concealment during the whole process is important. Alternatively, we can also investigate to find out if the target organization is using older versions of the software, which can be exploited by delivering the malicious contents via an e-mail or the Web, which can, in turn, infect the trusted party's computer.
3. **Planning the attack**: Whether you plan to attack the target directly or passively using an electronic-assisted technology is your choice. Based on the identified vulnerable entry points, we could easily determine the path and method of an attack. For instance, we found a friendly customer service representative, Bob, who will unwittingly execute any malicious files from his e-mail without any prior authorization from the senior management.
4. **Execution**: During the final step, our planned attack should be executed with confidence and patience to monitor and assess the results of the target exploitation. At this point, social engineers should hold enough information or access to the target's property, which would allow them to further penetrate the corporate assets. On successful execution, the exploitation and acquisition process is completed.