Social Engineering Using Social Networking Sites

Roberto Marmo
University of Pavia, Italy

INTRODUCTION

The protection of information is of vital importance to organisations and governments, therefore the development of measures to counter illegal access to information is an area that receives increasing attention. Information security is the specific discipline that regards the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.

Even though the effectiveness of security measures to protect sensitive information is increasing, the human element remains a weak link because people remain susceptible to manipulation in order to obtain unauthorized information. Social engineering is the art of using human skills and persuasion techniques to obtain unauthorized information and to gain access to a myriad of sensitive services and data is called. Social networking sites are an ever more popular way for people to stay connected, in touch with other people across the globe, therefore a lot of social data are publicly available, a useful source of data to attackers.

The aim of this contribution is to describe some technologies and methodologies to execute social engineering using social media as specific approach, it also discusses background, knowledge, challenges and critical factors necessary for successful implementation or detection.

Background

A social network is a social structure made of individuals (organizations, company ecc.) also called nodes, which are connected by links represent relationships and interactions between individuals. Social networking sites are an ever more popular way for people to stay connected, in touch with other people across the globe. They become an integral part of personal lives. Business opportunities are formed and lost online. Social network is capable of holding all the private information that one feeds it with. It is thus the responsibility of a user to be accountable of the content one posts via the network.

Persuasion has always been part of human interaction. It can be used to influence and support good or improved behavior (Martin, 2014), but it can also be used to trick and manipulate people into performing actions that can end in some kind of loss, divulging confidential information (Mitnick, 2002) or giving money to fraudsters.

The brain creates routines, which can help deal with and process things more efficiently. But these routines can also compromise the ability to pay attention and to cause the brain to bypass details which would help detect fraudulent content. In addition to that, people generally believe that they are good at detecting social engineering attacks. Research, however, indicates that people perform poorly on detecting lies and deception (Qin, 2007; Marett, 2004).

DOI: 10.4018/978-1-5225-9715-5.ch054

Social Engineering

4

Social engineering is a process that cyber criminals use to psychologically manipulate an unsuspecting person into divulging sensitive details through the use of specific techniques. This approach is not enough to breach the security of an individual or a company, it is a fundamental step to obtain useful information to execute some successive malicious activity.

Social engineering is an extremely powerful tool that can be deployed to bypass complex and secure infrastructure and systems. It is superior to most other forms of hacking in that it can breach even the most secure systems, as the users themselves are the most vulnerable part of the system. Instead of technical attacks on systems, cyber criminals try to exploit the human's element of security and inherently psychological manipulation. In fact, according to a security industry survey, social engineering tops the list of the 10 most popular hacking methods.

Kevin Mitnick coined the term "Social Engineering" which has been repeatedly mentioned in several articles and papers on network and information security. There are various definitions of social engineering and also a number of different models of social engineering attack (Mouton, 2015, 2016).

The process of doing social engineering is known as a social engineering attack. Social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion.

Social engineering is deeply entrenched in both computer science and social psychology, knowledge on both disciplines is required to perform an attack.

A trivial example of a social engineering attack is when an attacker wishes to connect to an organisation's network (Mouton, 2016). As a result of his research, the attacker finds out that a help-desk staff member knows the password to the organisation's wireless network. In addition, the attacker gained personal information regarding the staff member who has been identified as the target. The attacker initiates a conversation with the target, using the acquired information to establish trust (in this case the attacker misrepresents himself as an old school acquaintance of the target). The attacker subsequently exploits the established trust by asking permission to use the company's wireless network facility to send an e-mail. The helpdesk attendant is willing to supply the required password to the attacker due to the misrepresentation, and the attacker is able to gain access to the organisation's network and achieve his objective.

The work of Mouton (2016) proposes detailed social engineering attack templates that are derived from real-world social engineering examples. The proposed social engineering attack templates attempt to alleviate the problem of limited documented literature on social engineering attacks by mapping the real-world examples to the social engineering attack framework. Mapping several similar real-world examples to the social engineering attack framework allows one to establish a detailed flow of the attack whilst abstracting subjects and objects.

The attacks of Kevin Mitnick (Mitnick, 2002) showed how devastating sophisticated social engineering attacks are for the information security of both companies and governmental organizations.