Global Information Assurance Certification Paper

The Use of 'Social Engineering' as a means of Violating Computer Systems

Assignment by: Malcolm Allen
Version of Assignment: GSEC Practical Assignment version 1.2f (amended August 13, 2001)

Introduction:

'Social Engineering' is an practice that can be used to exploit what has long been considered the 'weakest link' in the security chain of an organisation - the 'human factor'.

As a security professional, it is important to be familiar with this threat, the techniques that could be used and the countermeasures that can be implemented to protect against it. By having this understanding, a security professional can ensure that appropriate protective measures are undertaken.

The following topics are covered in this paper to provide a guide to 'Social Engineering' as a means of violate a computer system(s):

- Definition;
- Commonly used techniques;
- Key traits to consider;
- Countermeasures;
- Auditing countermeasures.

Definition:

What is 'Social Engineering'? Various authors have provided definitions, such as:

> *"Social engineering can be regarded as 'people hacking', basically its hacker jargon for soliciting unwitting participation from a person inside a company rather than breaking into the system independently"*
> - Vigilante. "Social Engineering". *Internet Security*.

> *"Social engineering is a hack that uses brains instead of computer brawn. Hackers call data centres and pretend to be customers who have lost their password or show up at a site and simply wait for someone to hold a door open for them. Other forms of social engineering are not so obvious. Hackers have been known to create phoney web sites, sweepstakes or questionnaires that ask users to enter a password."*
> - Karen J Bannan. *Internet World*. Jan 1, 2001.

> *"Term used among crackers and samurai for cracking techniques that rely on weaknesses in the wetware rather than software. The aim is to trick people into revealing passwords or other information that compromises a target systems security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or an employee with an urgent access problem"*
> - Unknown Author. " Social Engineering". The Jargon Dictionary

However, it is probably most succinctly described by Harl in 'People Hacking' as:

"…the art and science of getting people to comply to your wishes."

Common Techniques:

A variety of techniques can be used in a 'Social Engineering' attack. Each technique relies on the strength, skill and ability of the individual employing them.

As with any attack, the aggressor will probably undertake some research of the target organisation. This research is commonly known as 'footprinting'. The information gained - even if not helpful - may be used to obtain further information.

Upon the completion of the 'footprinting' phase - which is most likely to be the longest phase of the attack from the attacker's perspective - the attacker may use one of a number of techniques to achieve their objective. It is useful to note that each technique can be categorised into one of two 'attack' categories. The first category is the 'human-based attack', which relies on interpersonal relationships to provide information. The second category is the 'computer-based attack', which relies on technology to trick an individual into supplying information.

Some of the most common techniques used are:

- **Direct Approach** - An aggressor may directly ask a target individual to complete a task (for example, a phone call to a receptionist asking them for their username and password). While this is the easiest and the most straightforward approach, it will most likely not succeed, as any security conscious individual will be mindful of providing such information.

- **Important User** - By pretending to be a senior manager of an organisation, with an important deadline, the attacker could pressure the Helpdesk operator into disclosing useful information, such as:

  - the type of remote access software used;
  - how to configure it;
  - the telephone numbers to the RAS server to dial;
  - the appropriate credentials to log in to the server.

  Upon obtaining this information, the attacker could then set up remote access to the organisation's network. They could then call back hours later to explain that they had forgotten their account password and request for it to be reset.

- **Helpless User** - An attacker may pretend to be a user who requires assistance to gain access to the organisation's systems. This is a simple process for an attacker to carry out, particularly if they have been unable to obtain/research enough information about the organisation. For example, the attacker would call a secretary within the organisation pretending to be a new temp who is having trouble accessing the organisation's system. By not wishing to offend the person, or appear incompetent, the secretary may be inclined to help out by supplying the

username and password of an active account.

- **Technical Support Personnel** - By pretending to belong to an organisation's technical support team, an attacker could extract useful information from the unsuspecting user community. For example, the attacker may pretend to be a system administrator who is trying to help with a system problem and requires the user's username and password to resolve the problem.

- **Reverse Social Engineering (RSE)** - A legitimate user is enticed to ask the attacker questions to obtain information. With this approach, the attacker is perceived as being of higher seniority than the legitimate user who is actually the target.

  A typical RSE attack involves three parts:

  - ***Sabotage*** - After gaining simple access, the attacker either corrupts the workstation or gives it an appearance of being corrupted. The user of the system discovers the problem and tries to seek help
  - ***Marketing*** - In order to ensure the user calls the attacker, the attacker must advertise. The attacker can do this by either leaving their business cards around the target's office and/or by placing their contact number on the error message itself
  - ***Support*** - Finally, the attacker would assist with the problem, ensuring that the user remains unsuspicious while the attacker obtains the information they require.

- **E-mail** - The use of a topical subject to trigger an emotion which leads to unwitting participation from the target. There are two common forms that may be used. The first involves malicious code, such as that used to create a virus. This code is usually hidden within a file attached to an email. The intention is that an unsuspecting user will click/open the file; for example, 'IloveYou' virus, 'Anna Kournikova' worm or more recently the 'Vote-A' email aware worm. The second equally effective approach involves chain mail and Virus hoaxes. These have been designed to clog mail system by reporting a non existent virus or competition and requesting the recipient to forward a copy on to all their friends and co-workers. As history has shown, this can create a significant snowball effect once started.

- **Website** - A ruse used to get an unwitting user to disclose potentially sensitive data, such as the password they use at work. For example, a website may promote a factitious competition or promotion, which requires a user to enter in a contact email address and password. The password entered may very well be similar to the password used by the individual at work.

Other techniques used may include:

- Somebody looking over the shoulder of a person as they type in their password.
- A visitor watching users and their behaviour patterns.
- An attacker sifting through rubbish looking for clues to unlock an organisation's IT treasures.

Key traits to consider:

Whichever technique is used, if it involves certain traits, the target is likely to comply with the request(s). These traits include:

- The movement of responsibility away from the target, such that they consider they are not solely responsible for their actions.
- The perception by the target that, by conforming with the request, they may get on the 'right side' of somebody who could award them future benefits, more commonly known as "getting in with the boss".
- The target's instinct to act morally in helping someone out, thus avoiding the feeling of guilt.
- Communication on a personal level, resulting in the target voluntarily complying with the request without realising the pressure being applied.
- The target believes they are making a reasoned decision in exchange for a small loss of their time and energy.

The likelihood of the target's compliance is further increased if:

- The attacker is able to avoid conflict by using a consultative approach rather than an aggressive one.
- The attacker is able to develop and build a relationship through previous dealings. The target will probably comply with a large request having previously complied with smaller one.
- The attacker is able to appeal to the target's senses, such as sight and sound. By appealing to such senses, the attacker will be able build a better relationship with their target by appearing 'human' rather than just a voice or email message.
- The attacker has a quick mind and is able to improvise.

Countermeasures:

Is there an effective way to fully protect against such an attack? The answer is 'No'. The reason is simple. No matter what controls are implemented, there will always be the possibility of the 'human factor' being influenced by a social, political and/or cultural event.

Nevertheless, as with any threat, there are ways in which to reduce the likelihood of success. To one with an appreciation of the threat, knowledge of the techniques that could be used and the countermeasures that can be implemented are extremely important.

Set out below is a list of core controls that can be implemented to protect against such an attack:

- **Security policy** - A sound security policy will ensure a clear direction on what is expected of staff within an organisation. For example, support teams should only

offer assistance for a defined range of activities.

- **Good security architecture** - Smart infrastructure architecture will allow personnel to concentrate on more important duties. For example, by ensuring outbound firewall access controls are configured just as carefully as inbound controls, an administrator will know exactly how the networked environment will respond under certain events. This understanding will ensure that they are able to avoid spending their time on following up on 'false positive' events.
- **Management buy-in** - Managers require an understanding in their role to be able to define what requires protection and why. This understanding should ensure that appropriate protective measures are taken to protect against associated risks.
- **Education** - Simple solution that can be used to prevent these types of attacks. For example, a knowledgeable user can easily be advised that they should never give out any information without the appropriate authorisation and that they should report any suspicious behaviour. A good training and awareness program focusing on the type of behaviour that you require will undoubtedly pay for itself.
- **Limit Data leakage** - Reducing the amount of specific data available will ensure that the attack is not an effortless exercise. For example websites, public databases, Internet registries, and other publicly accessible data sources should only list generic information, such as main organisation phone number and job titles instead of employee name(s), for example 'site administrator' instead of 'Joe Bloggs'.
- **Incident response strategy** - A document response strategy will ensure that, if under pressure, a user will know exactly what procedures they need to follow. For example, if a user receives a request they should verify its authenticity before acting on the instructions they have received. If, however, they have already acted on the request then they should alert their administrator. It will then be the responsibility of the administrator to check with their user community to ensure no other user has followed the instructions of the request.

Testing Countermeasures:

Once the countermeasures have been implemented, there are two ways in which to ensure an organisation's ongoing preparedness for such an attack.

The first is to perform regular reviews of the countermeasures that have been implemented. These reviews will ensure that an acceptable standard is maintained on an ongoing basis.

The second and the least common used approach is to simulate an attack. This type of review is reliant on the information that it is able to obtain from the public domain about the organisation, as well as the value it could offer, versus the resource intensive overheads. It should also be noted that many organisations feel uncomfortable with this type of review.

Summary:

The skilled application of 'Social Engineering' can be a threat to the security of any organisation. As a security professional, it is important to understand the significance

of this threat and the ways in which it can be manifested. Only then can appropriate countermeasures be employed and maintained in order to protect an organisation on an ongoing basis.

References:

CERT Advisory CA-1991-04. "Social Engineering", Revised September 18, 1997.
URL: http://www.cert.org/advisories/CA-1991-04.html

Arthurs, Wendy. "A Proactive Defence to Social Engineering", August 2, 2001.
URL: http://www.sans.org/infosecFAQ/social/defence.htm

Bernz. "The Complete Social Engineering FAQ".
URL: http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt

Harl. "People Hacking". *The Psychology of Social Engineering*.

Horowitz, Alan S. "Top 10 security mistakes". *Computerworld,* July 9, 2001.

Hurley, Hanna. "Fear thyself". *Telepho*ny, June 21, 1999.

Lemos, Robert. "Mitnick teaches 'social engineering'". July 12, 2000.
URL:
http://netsecurity.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.zdnet.com%2Fzdnn%2Fstories%2Fnews%2F0%2C4586%2C2604480%2C00.html

Nelson, Rick. "Methods of Hacking: Social Engineering".
URL: http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html

Orr, Chris. "Social Engineering: A Backdoor to the Vault". September 5, 2000
URL: http://www.sans.org/infosecFAQ/social/backdoor.htm

Palumbo, John. "Social Engineering: What is it, why is so little said about it and what can be done?". July 26, 2000
URL: http://www.sans.org/infosecFAQ/social/social.htm

Scambray, Joel and McClure, Stuart and Kurt, George. "Hacking Exposed - Second Edition".

Stevens, George. "Enhancing Defences Against Social Engineering". March 26, 2001
URL: http://www.sans.org/infosecFAQ/social/defense_social.htm

Thompson, David. "The social engineering of security". June 11, 2001.
URL: http://www.zdnet.com/enterprise/stories/main/0,10228,2771372,00.html

Tims, Rick. "Social Engineering: Policies and Education a Must", February 16, 2001
URL: http://www.sans.org/infosecFAQ/social/policies.htm

Unknown Author. "Crime, Security, and Privacy". University of Memphis.

Unknown Author. " Social Engineering". The Jargon Dictionary
URL: http://info.astrian.net/jargon/terms/s/social_engineering.html