SOCIAL ENGINEERING ATTACK

Assignment

Name : Pathima Shahama Tamber
Student Number : MS15903020
Subject : Penetration Testing
Submitted Date : 29/03/2016

1.0 Question

The students will be divided into groups. The instructor will monitor the groups as they put together a plan that will allow them to gain as much information about a computer system or network on the SLIIT campus **without the use of a computer.** Strictly by asking questions or gathering information from easily accessible locations. (example: Trash can) The data that is gathered will be compiled and presented as a group project to the class. The written report will be 10~15 pages And include any countermeasures that can be put in place.

2.0 Answers

Assuming Computer Laboratory were the target (Answer are in *Italian* Format)

1. Casually ask one of the workers at the Laboratory how many computers they have.

   Why would this information be important to a potential hacker?

   Hacker can get a knowledge about how many target sources they have to cover and how they can attack to the target.

2. Casually ask one of the workers at the Laboratory what OS the computers are using.

   Why would this information be important to a potential hacker?

   Hacker can gain knowledge about the attacking source information. They can easily sort-out how to attack to the target. Attacker can gain knowledge about what are the available vulnerabilities available for that particular OS. By using those details attacker can decide what techniques have to used to attack the network or system.

3. Casually ask one of the workers at the Laboratory if they know the IP address information for their computer.

   Why would this information be important to a potential hacker?

   IP address is the unique identification of a computer. Hacker can easily identify the target and send or receive information if the IP address is known. Hacker can use a tools or a technique to attack the system.

4. Casually ask one of the workers at the Laboratory if they are using a firewall because you are having problems with your software.

   Why would this information be important to a potential hacker?

   Firewall will prevent arbitrary incoming traffic from hitting the computer. This stops most remote exploits. If the hacker get to know there is no any firewall installed, hacker can easily access into the system without any barrier.

5. Casually ask one of the workers at the Laboratory if any of the computers use a know router.

   Why would this information be important to a potential hacker?

   If hacker knows router details such as ISP, router types … etc he can try to attack the router to get into it. If the user did not changed the default password of the router the hacker can get a benefit from it. Hacker can access to the router using default username and password, he can do any modification as he wish.

6. Casually ask one of the workers at the Laboratory if they know the password to the computer.

   Silly enough, why would this information be important to a potential hacker?

   If the hacker knows the password of the laboratory computers he can any harm to the system. Even though SLIIT have tools to monitor who logged to the computers the hacked computer will detect as a authorized user.

7. Casually ask one of the workers at the Laboratory if the network uses an intrusion detection system of some kind because your software isn't working.

   Why would this information be important to a potential hacker?

   If the hacker knows the Intrusion Detection System(ISP) details such as vendor, version …etc hacker can take an advantage over those details. He can decide what kind of tools and techniques he has to attack the system. If SLIIT won't using any ISP hacker can easily get into the system by using simple hacking techniques.

This portion allows a computer at the target location to be used.

8. Ask if you can use one of the computers in the Laboratory, accidently forgetting your ID card.

   Why would this be important to a potential hacker?

   ID card is used to identify authorized person to access to SLIIT or Computer Laboratory. ID card will uniquely identify each person who has a authorization. The ID card found by the hacker may be a staff ID card that has used to access to server rooms or data centers or other restriction areas. By using that ID card hacker can access to restricted areas physically and he can do any harm to those areas or modify privileges or delete data.