CS 458/658
Assignment 1
Hanzhang Chen
ID: 20574275

Q1.

a. This is a compromise of confidentiality and privacy. Privacy is your right to control access to your data/information, and confidentiality is access to systems or data is limited to authorized parties. A leak of the full profiles of close to 52 million unsuspecting users who were friends of the mobile application users, this violates their privacy. Also no one else should have access to these information except Facebook, which violates the data's confidentiality.
b. This is a compromise of availability. Although this seems to prevent the violation of privacy, it stops the user who are just legally using the service from those IP, which is compromise of availability.
c. This is a compromise of integrity. Adding fake data will affect users to get the 'right' information, which violates the definition of integrity.
d. This is a compromise of confidentiality, integrity and privacy. First, that company may not legally have access to the data, most of the staff may not know the existence of it. For integrity, it is the same reason as question (c), which is that this will avoid users to get the 'right' information/data. For privacy, that staff was privately told by the CSO, he/she should not share to others without the permission of CSO.

Q2.

a. Interception. An interception means that some unauthorized party has gained access to an asset. So here you see strange commits, which is a kind of interception.
b. Modification. If an unauthorized party not only accesses but tampers with an asset, the threat is a modification. So here you see changes to an authentication protocol for access to secret client files, which is a kind of modification.
c. Interception. An interception means that some unauthorized party has gained access to an asset. You found your data go through a hop, which means it might be exposed to someone else or organization you do not know, which is an interception.
d. Interruption. In an interruption, an asset of the system becomes lost, unavailable, or unusable. So here, you seem to have lost access to the more sensitive company files, which is an interruption.

Q3.

a. (Given example).
b. Eliminate all the clue that you have left when you were investigating.
c. Try to insert some code which can alert you if someone is accessing or modifying the data in those sensitive area, as well as making the code hard to be found. After that, record, review and keep them, so that you can know if the company is suspecting.
d. Try to do something else helpful to the company, shift their focus and ask for more opportunities to modify the files (here I mean grant privilege escalation). So that you can

have more chances to investigate what the company is secretly doing as well as protect yourself (since you have higher privileges, most of your operations will not be suspected, and you can even make fake documents to confuse them.)

Programming:

Exploit descriptions for sploit1.c:

- Using buffer overflow attack. So when we go through “submit.c”, we can easily find a function called: “print_usage”, which uses buffers and consumes a parameter called “cmd” which is given by ourselves. Also, if we want to let it execute, we have to use “-h” option.
- This attack works since we add more characters than the buffer can contain, and the part that overflows will be regarded as the return address. So we can make an address to the end of the character string and add shell code to gain root privilege.
  [Basically: NOP – Shellcode – return address]
  - Using gdb command “x/200x $esp” or check cmd value when running to print_usage to get return address.

Output:

```
user@cs458-uml:/share$ ./sploit1
Syntax:

▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒^▒1▒F▒F
▒
 ▒▒▒V
1ۅ▒@▒▒▒▒▒/bin/sh▒?▒▒?▒▒?▒▒?▒▒?▒▒?▒▒?▒▒?▒▒?▒▒?▒ <path> [log message]
-s, --submitted Show your submitted files
-v, --version               Show version
-h, --help                   Show this usage message
sh-3.1# exit
exit
user@cs458-uml:/share$
```