A1-MileStone

1. A) For this condition, privacy and confidentiality were violated. For the privacy, I did not authorize Facebook share my personal information to any other third party, because of the loos restrictions by the Facebook's API, the personal information was download and used by Oxford Analytica. For the confidentiality, Facebook's confidentiality was violated by Oxford Analytica, Facebook should not authorize Oxford Analytica to access the user information data, but the API let Oxford Analytica access and download the data without any restrictions.

   B) For this condition, availability was violated, the availability means the system or data is there when you want it, but the Facebook prevent all further incoming requests even from the normal user, so user's availability was violated.

   C) For this condition, integrity was violated. Integrity means When you receive data, you get the “right” data, the fake profiles would make data "wrong".

   D) For this condition, integrity and privacy. The secret server farm which means the save and use my data without my authorized, they can use these data free without any supervision. Also the secret server can create any data they want, it can make the data “wrong” which means the integrity is violated.

2. A) This scenario represents fabrication. The commits which cannot recognize would be the fake commit, fabrication is using the data like normal but actually false to cover up the truth.

   B) This scenario represents modification. The changes to an authentication protocol for access to secret client files means modification.

   C) This scenario represents interception. The data received by others without authority means interception.

   D) This scenario represents interruption. The hacker interrupt "me" access to sensitive files.

3. A) Place some incriminating documents on the desk of a co-worker with a history of misbehavior.

B) Eliminating the "footprint" of your system and data in a timely manner and installing firewalls and protection software on your computers and mobile phones. Always back up important files, whether in electronic or physical form.

C) Check your computer and mobile phone at any time for viruses and malware. Observe frequently there are no suspicious processes in background, and check if you have been tracked by suspicious individuals.

D) Minimize the traces that you left behind during the investigation. Make a backup of the system before each investigation. After the investigation, restore the system to the situation where you did not investigate. Flat fashion makes no things happen.

Exploit Description:

- way of exploit: Buffer overflow
- Target: the copy_file function:

```
while ((c = fgetc(src_file)) != EOF) {
    *p1 = c;
    p1++;}
```

this function didn't check the length of src_file which has fixed size, This arises the possibility of overflowing the buffer that make change on stack.

- Idea of exploit:
  - Create a virus file: we already know the copy_file function's buffer is 3072, and we need to change it's EIP so we need add additional 9 after it, which is 4 for others, 4 for EIP and 1 for '\0'. I wanna easy to find the shell code address, so I fill up NOP at the beginning of the file, so I jump to any of these NOP can find the shell code; After that, copy the shell code to this file, then fill up with the address we wanna jump to.
  - Find the address: use the GDB to check the submit file, set a breakpoint at the line 119 which is the end of copy file to the buffer, and then check the frame by using "info frame", after that use "p &buf" can find the buffer address is 0x……, and then use "x/200 0x…… "

to see the detail of the stack, then its very easy to find many NOP and the shell code address, also check whether the EIP we wanna change is changed.

- After that use the “execve” function to let the submit read the file we make, when the program run until the copy_file function, the buffer overflow would happened and after this function end, it would jump to the address we set and then run the shell code, the shell code would give us root authority.