1. **2016-1**

   Circle or cross: "**T**" if True – "**F**" if False.

   T / **F**   Principle of least privilege: ~~programs, users and systems should be given unlimited privileges to perform their tasks.~~

   T / **F**   Computer system objects may be hardware or software.

   T / **F**   Breach of confidentiality involves unauthorized reading of data.

   T / **F**   Breach of integrity involves ~~preventing legitimate use of the system.~~

   T / **F**   Breach of availability involves unauthorized destruction of data.

   T / **F**   An attack is ~~always malicious and never accidental.~~

   T / **F**   Script kiddies are ~~persons who write scripts or codes to crack into computers.~~

2. **2016-2**

   Circle or cross: "T" if True – "F" if False.

   ```
   $ ls -al
   total 12
   drwxr-xr-x 3 demo demo 4096 Oct 17 17:05 .
   drwxrwxrwt 8 root root 4096 Oct 17 17:04 ..
   dr-x--x--x 2 demo demo 4096 Oct 17 17:06 tmp
   ```

   T / **F**   All users can enter directory `tmp/`.

   T / **F**   Only user demo can read directory `tmp/`.

   T / **F**   A cyber breach occurs when someone accesses a database through an insufficiently secured network connection.

   T / **F**   A physical breach occurs when an unauthorized person is able to physically access a piece of equipment.

   T / **F**   "**Security**" is an ~~internal~~ problem. On the other hand, "**protection**" also requires consideration of the ~~external~~ environment.

   T / **F**   A backdoor is a method of bypassing normal authentication.

   T / **F**   A trojan horse is an example of a backdoor.

   T / **F**   A Keylogger is the action of recording (covertly) a keyboard.

3. **2017-1**

Circle or cross: "T" if True – "F" if False.

T / **F**   ~~Security~~ is a mechanism for controlling processes or users to resources (Yakoob et. al.).

T / **F**   Operating Systems automatically apply permissions to files and folder, however users can manually apply them too (Yakoob et. al.).

T / **F**   Symmetric cryptography is much faster than asymmetric one.

T / **F**   Protection is strictly an internal problem. On the other hand, security is strictly an external problem.

T / **F**   The ~~security~~ mechanisms control access to a system. On the other hand, ~~protection~~ system prevents unauthorized access.

T / **F**   The three aspects to a protection mechanism are authentication, authorization, and access enforcement.

T / **F**   In GNU/Linux, users can be organized into groups, with a single Access Control List (ACL) for an entire group.

T / **F**   Trojan horses are often computer games software infected with viruses.

T / **F**   An access list is a list of objects and the operations allowed on those objects for each domain (OSC9).

T / **F**   If users are allowed to perform their own I/O operation, system integrity will be guaranteed (OSC9).

C Programing

```
001 /*
002  * (c) 2017 Rahmat M. Samik-Ibrahim
003  * This is free software.
004  * REV01 Thu Mar 30 17:32:33 WIB 2017
005  * START Thu Mar 30 12:13:58 WIB 2017
006  */
007
008 #include <stdio.h>
```

```
010 int tambah(int ii, int jj) {
011    return ii + jj;
012 }
013
014 void main() {
015    int ii = 4;
016    printf("The return of tambah is %d\n", tambah(1,ii));
017 }
```

Program Output (Line 016):

4. **2017-2**

Principle of least (01) dictates that programs, users, and even systems be given just enough privileges to perform their tasks (OSC9). (02) is strictly an internal problem (OSC9). (03) requires also consideration of the external environment within which the system operates (OSC9). A system is (04) if its resources are used and accessed as intended under all circumstances (OSC9). Security is often deployed for (05) against external threats (OSC9). Breach of (06) involves unauthorized reading of data (OSC9). Breach of (07) involves unauthorized modification of data (OSC9). Breach of (08) involves unauthorized destruction of data (OSC9). (09) of service involves unauthorized use of resources (OSC9).

(10) of service involves preventing legitimate use of the system (OSC9). (11) is when one participant in a communication pretends to be someone else (OSC9). In a session (12), an active communication session is intercepted (OSC9). A code segment that misuses its environment is called a (13) (OSC9). (14) are self-replicating and are designed to infect other programs (OSC9). A (15) is a process that uses the spawn mechanism to duplicate itself (OSC9). In a (16) encryption algorithm, the same key is used to encrypt and to decrypt (OSC9). In an (17) encryption algorithm, there are different encryption and decryption keys (OSC9). (18) are very useful in that they enable anyone to verify the authenticity of the message (OSC9). (19) is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively (WIKI).

Match the number of the sentence above with these following phrases:

[   ] Asymmetric   [   ] Availability   [   ] Confidentiality   [   ] Denial

[   ] Digital Signatures [   ] Hijacking   [   ] Integrity   [   ] Masquerading

[   ] Privacy   [   ] Privilege   [   ] Protection   [   ] Protection

[   ] Secure   [   ] Security   [   ] Symmetric   [   ] Theft

[   ] Trojan Horse   [   ] Viruses   [   ] Worm

C Programing	
| ```
001 /*
002  * (c) 2017 Rahmat M. Samik-Ibrahim
003  * http://rahmatm.samik-ibrahim.vlsm.org/
004  * This is free software.
005  * REV00 Mon Oct 16 21:15:03 WIB 2017
006  * START Mon Oct 16 21:15:03 WIB 2017
007  */
008
009 #include <stdio.h>
010
011 char globalChar='a';
012
``` | ```
013 char* getGlobal(void) {
014     char* charPTR=&globalChar;
015     printf("getGlobal1 %c\n", globalChar);
016     *charPTR='b';
017     printf("getGlobal2 %c\n", *charPTR);
018     return charPTR;
019 }
021 void main (void) {
022     char localChar='c';
023     printf("==== main1 %c\n", localChar);
024     localChar=*getGlobal();
025     printf("==== main2 %c\n", localChar);
026 }
``` |

Program Output: