# CS2107 In-Lecture Quiz 3 - Answers
# 26 October 2022

**1.** [0.5 mark] As discussed in the lecture, TLS supports both unilateral and mutual authenticated key exchange. Now, consider a typical e-commerce site like Amazon, Shopee or Lazada. The web server and a user need to authenticate each other. How is the authentication process usually carried out?

   **a) First, the user's browser performs TLS unilateral authentication to verify the server. Then, after a secure channel is established, the server conducts a password-based authentication to verify the user.**

   b) First, the user's browser performs TLS mutual authentication to verify the server. Then, after a secure channel is established, the server conducts a password-based authentication to verify the user.

   c) First, the server conducts a password-based authentication to verify the user. Then, using the user's password and server's public key, TLS mutual authentication is carried out.

   d) First, the server conducts a password-based authentication to verify the user. Then, the user's browser performs TLS unilateral authentication to verify the server.

   e) The user's browser and the server perform TLS mutual authentication to authenticate each other with no user password involved.

**2.** [0.5 mark] The following are correct issue(s) faced by different access control representations, ***except***:

   a) Access Control Matrix (ACM) would be very large and with many empty cells

   b) ACL can't easily answer what files that a certain user can access

   c) Capabilities can't easily answer which users can access a certain file

   d) Both ACL and capabilities can still be too large, especially if there are many users and files in the system

   **e) Intermediate control whereby users are grouped can be too slow if there are many files in the system**

**3.** [1 mark] Suppose you know that Alice, in your local area network, is about to connect to a remote server using the insecure Telnet protocol. You want to capture Alice's username and password, which are sent in clear by her Telnet client. Subsequently, you want to check that the contacted Telnet server is still alive. What are the most suitable UNIX/Linux tools (in the correct order required) that you should run on your host to accomplish the two tasks?

a) ping then nmap

b) nmap then Wireshark

**c) Wireshark then ping**

d) Wireshark then nslookup

e) nmap then ping

**4.** [1 mark] Suppose the user `alice` is in the `hr` group.
Consider the following `f1` file:

```
-rwxr-x---   2   alice   hr   1024   5 Oct 2022   f1
```

Which statement below is correct?

**a) `alice` has write access, `root` has write access**

b) alice has write access,  root doesn't have write access

c) alice doesn't have write access, root has write access

d) alice doesn't have write access, root doesn't have write access

e) None of the other options

**5.** [1 mark] The user `bob` is not in the `admin` group.
Consider the following executable file `f2`:

```
-rwsr-xr-x  1  root  admin   1024   6 Oct 2022   f2
```

If bob executes `f2`,which statement below about the invoked process is correct?

**a) The process' real UID is `bob`, its effective UID is `root`**

b) The process' real UID is `bob`, its effective UID is `bob`

c) The process' real UID is `root`, its effective UID is `bob`

d) The process' real UID is `root`, its effective UID is `root`

e) bob doesn't have the access right to execute the file `f2`

**6.** [1 mark] Suppose Alice and Bob perform a Diffie-Hellman key exchange with pre-agreed *g*=2 and *p* as a prime number > $2^{15}$. Alice, however, sends 4 to Bob; and Bob sends 8 to Alice. What is the key agreed by Alice and Bob?

a) 4

b) 8

c) 12

d) 32

**e) 64**