UEEN3113 / 3413 Server Configuration and Management
Revision 2

1. What is the action to allow a new user to be able to perform sudo
   a. without any limitation?

      Add the new user to the sudo group.

   b. on specific commands?

      Edit and configure the permission in /etc/sudoers file with visudo.

2. Briefly explain the reason NOT to simply add a user into sudo group.

   Any user in sudo group has the same privilege as root, which can perform any action.

3. Briefly explain two advantages of GPT partitioning over MBR partitioning.

   GPT partitioning able to handle larger capacity whereas MBR can't handle disk size more than 2TB.
   In GPT partitioning, each partition is identified by their unique id. Thus, the disk swapping has no effect in partitions identification.

4. Write the commands to create the "cm_db" database and then grant all privileges to new user "cmadmin" on the database, "cmadmin" should be able to login remotely.

   create database cm_db;
   grant all privileges on cm_db.* to 'cmadmin'@'%';

5. A user can't access to mysql server remotely.

   a) Output from *netstat* and *ping* command show that mysql server is running without issue and the user able to ping to the server. The user has been added into the database correctly with appropriate privileges granted. What is the possible issue that causes the remote access is denied?

      The configuration file might not been configure to allow remote access, where bind-address is still 127.0.0.1

   b) Make the necessary change to allow remote access to mysql server.

      bind-address 0.0.0.0

6. Write the command to enable SSL support in apache.

   a2enmod ssl

7. What is the command to confirm that apache server is running with SSL support and listening to the correct ports.

   netstat –tulpn | grep apache

8. Is a self-signed SSL certificate sufficient for the use in a company's intranet?

   Since it is company's intranet, a self-signed certificate of course can be trusted.

9. Write the command to disable a website site in apache in which the site configuration file is "cm-ssl.conf".

   a2dissite cm-ssl.conf

10. Explain how the *keepalived* could maintain the reliability of web server.

    Another server in the group will take over if the main server fails.

11. Given that *tcpdump* is the only sniffing tool available in the server, use the tool to capture the network packets and store it in a file named "td_pkt".

    tcpdump -w td_pkt

12. An analysis of the *tcpdump* output shows that there is high traffic from a host which is only used by guest and no other staff will be using it. Suggest one suspicious activity that might had happened to that host.

    The host might be compromised by insider or outsider to attack the server.

13. Write a command that will display all ports that are listening and connected, for TCP and UDP.

    netstat -natu

14. Write a command to display IPv6 routing table.

    netstat –rn –A inet6

15. Write a command to display all available interfaces.

    ifconfig / ip a / tcpdump -D

16. Write a command to capture packets from eth0 and store to a file named **today.pcap**.

    sudo tcpdump -w today.pcap -i eth0

17. Write a command to read packets from port 22 on eth1.

    sudo tcpdumb –i eth1 port 22

18. Look for all opened ports in hosts with IP range 192.168.66.110 – 192.168.66.200

    sudo nmap 192.168.66.110-200