1. a) Explain why a SYN flood attack can cause denial of service. *(6 marks)*

b) Explain the operation of the Unix set-uid (suid) permission. *(6 marks)*

c) Which of the following C programs are vulnerable to a stack smashing attack? Outline how the selected program enables the attack to be carried out. *(6 marks)*

```
void main1(int argc, char* argv[]){
  char buffer[6];
  strcpy(buffer,argv[0]);
}/*main1*/
```

```
void main2(int argc, char* argv[]){
  char buffer[6];
  strcpy(buffer,"long text");
}/*main2*/
```

d) Sketch how a Domain and Type Enforcement mechanism, such as that used by SELinux can help safeguard against a Trojan Horse. *(6 marks)*

e) Explain the difference between an Access Control List (ACL) and a capability. *(6 marks)*

(Total 30 marks)

---

2. a) A simple multilevel secure database management system is to be designed. Each row in a database table is assigned a separate security-level, and subjects at any security-level may access the table (but not necessarily every record in the table). For example, consider the following employee relation table (*emp-id* is primary key).

emp-id	*level*	Name
0031	topsecret	Mulder
0200	secret	Scully
1002	secret	Jones

Given the usual ordering between the specified security levels, a secret process may read the Scully and Jones' entries but not the Mulder entry, and so forth.

i. Propose suitable multilevel security rules that govern read/write access by subjects to table rows. You should assume that when a new row is inserted into the table it is assigned the security-level of the subject inserting it. *(10 marks)*

ii. Given that primary key values are unique in a table, explain how a Trojan-Horse running at top-secret could establish a covert-channel and signal *one* bit of information to a subject operating at secret. Describe how the covert channel should be closed. *(5 marks)*

b) A conventional (non-MLS) linux server currently hosts an email-service plus a DBMS service that is used to store only topsecret employee data.

The owner is concerned about Trojan Horse attack and estimates that, in terms of lost of reputation, among other things, unauthorized leakage of top-secret employee data would cost $500,000, while unauthorized access to email would cost $10,000. The probability of such an attack on a conventional linux system that hosts both services is estimated to be 0.1. If the services were to be hosted on an MLS system then the probability of attack would reduce to 0.0001. Assume that an MLS system costs $5,000, while a standard linux server costs $500 and that their operational costs are zero.

Use this information to carry out a *Risk Assessment* and advise the company on how best to configure the system(s) and mitigate the risk of Trojan Horse attack. *(10 marks)*

(Total 25 marks)

---

3. Users interact with a networked application system via a simple command-line interface available on Port 666 of the application's hosting server. Users authenticate at this interface by providing a user-id/password pair, which the application checks against the authorized users file `~/users`. The (Java) application system uses Java class `AppUsers` to lookup/manage the user-id/passwords stored in this file.

   The application command-line interface provides a password change operation, whereby the user provides his old password along with a request to change to a new password. This results in the application invoking the `AppUsers` operation:

```
public String changePass(String userid, String old, String new){ ... }
```

   which first confirms that the current password for `userid` is `old` and, if so, then changes `userid`'s password in `~/users` to `new`; otherwise the password is unchanged.

   a) What are the threats to the `AppUsers` data? Describe how Java's security architecture can be used to help protect the sensitive `AppUsers` data. In particular, your answer should include: a suitable Java security policy and an explanation how a new Java permission is declared and used by `changePass` and whether `changePass` should be treated as a privileged operation. *(15 marks)*

   b) Describe the Clark Wilson security model. Use the application system in Question 3(a) above to illustrate your answer. *(10 marks)*

(Total 25 marks)