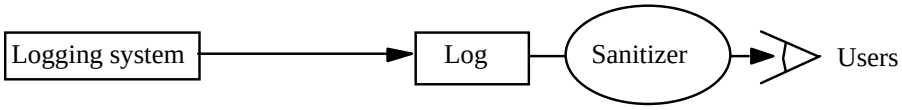
Name: **ID:** ***(Total = 40 Marks)***

1) Match between the two columns in the table below: ***5 Marks***

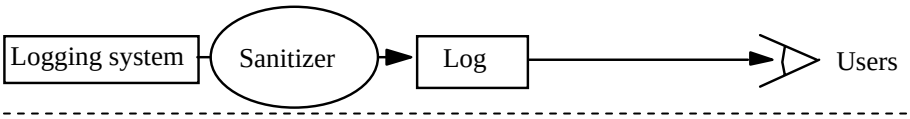
Logger	Builds a model of "normal" system behavior, and alerts when a deviation from the model is detected
Analyzer	Reports results of investigation to take action
Notifier	Report information, usually controlled by parameters
Signature-based IDS	Examine information looking for something unexpected
Anomaly-Based IDS	Detects attacks by matching against a database of known attacks

2) Which of the two logging organizations provides the following facilities? (some answers may include both examples) ***6 Marks***

Logging Sanitization Organization



Example [1]



Example [2]

a) Provides user privacy protected from system administrators:

b) Provides user privacy protected from all other users:

c) Real Data simply not recorded correctly (data are scrambled before recording) to provide protection:

d) Faster to record in the logging system:

e) Faster for all users to read from the logging system:

3) Two systems: [1] One system built with security features in all its designing stages ***4 Marks***
[2] The other system built without security consideration and then it is added late

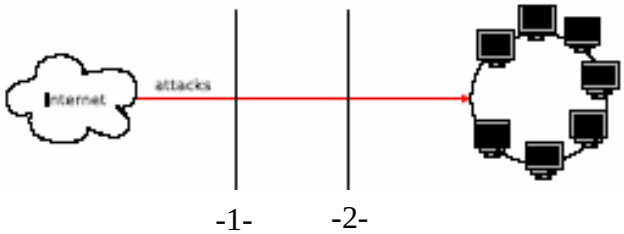
a) Which system is expected to have less security holes?

b) Which system is expected more flexible to be upgraded?

c) Which system is expected more complex to design?

d) Which system is expected more expensive and secure?

4) Two lines of defense are to describe the systems as shown in the figure. ***7 Marks***
Determine which line of defense relates to each of the following:



a) Firewalls:

b) Anti-virus software:

c) Signature-based IDS:

d) Misuse-based detection:

e) Authentication:

f) Access control:

g) Specification-based detection:

5) Circle the correct choice related to the intrusion detection systems: ***4 Marks***

a) Although (Signature based IDS Anomaly based IDS Network-based IDS Host-based IDS) is able to detects new attacks, it usually produce a high number of false alarms as well as its requirement of extensive training sets of data to determine its normal usage.

b) Although (Signature based IDS Anomaly based IDS Network-based IDS Host-based IDS) detects at application layer and has no trouble with encryption, it is harder to manage.

c) Although (Signature based IDS Anomaly based IDS Network-based IDS Host-based IDS) is simple, effective, and easy to administer, it can't detect new attacks nor slightly modified viruses.

d) Although (Signature based IDS Anomaly based IDS Network-based IDS Host-based IDS) is easy to deploy (install) and suitable to monitor many hosts, it is difficult in processing encrypted protocols.

---

6) Consider the network security system to be built for an industrial company similar to the one discussed in class: ***4 Marks***
Dividing the company into 3 internal organizations or groups: Customer Service Group (CSG), Development Group (DG), and Corporate Group (CG); which group relates to the following (*one answer per question*):

a) Maintains customer data:

b) Handles patents and lawsuits:

c) Study customer feedback:

d) Interface between clients & other internal organizations:

e) Corporate info protected by attorney privilege:

f) Credit card numbers:

g) Plans and prototypes for new products:

h) Development data for future products:

---

7) Circle the correct answer according to the consistency checks: ***3 Marks***

a) Keep sensitive info (confidential integral available public in DMZ at proxy).

b) Only employees who handle (future plans patents purchases lawsuits developments maintenances) can access customer data, and only they and customer can alter it.

c) Releasing (email sensitive website firewall hubs internet) info requires corporate approval.

---

8) Consider filling the gaps in the figure from below by representing the proper letters (A,B,C,D) ***5 Marks***

a) Customer data subnet:

b) Outer firewall:

c) Development subnet:

d) Web server:

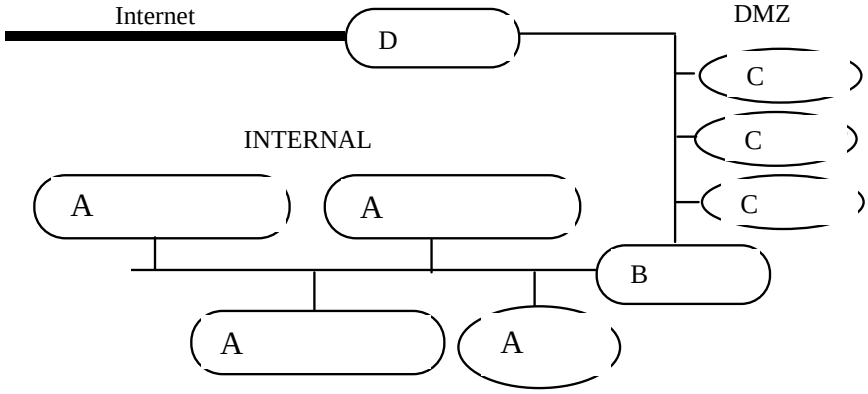
e) Inner firewall:

f) DNS server:

g) Internal mail server:

h) Corporate data subnet:

i) Mail server:



---

9) Circle all correct words in the sentences below according to the knowledge from Network security prospective: ***2 Marks***

a) When info moves from internet to inside network (Confidentiality Integrity Availability None from before) is important and (Confidentiality Integrity None from before) is **not** important.

b) When info moves out to the internet from inside network (Confidentiality Integrity Availability None from before) is important and (Confidentiality Integrity None from before) is **not** important.