Question # 1: Answer questions using AGREE or DISAGREE and adding one sentence ONLY for explanation. Giving NO explanation or Irrelevant details will get you NO credit. Each question carries 1 point. [1 x 10 = 10 Points]

a. Botnets are networks of compromised computers that are controlled remotely by one or more cyber criminals. Cyber criminals infect a victim's computer with bots using phishing attacks and browser vulnerabilities.
AGREE. BotNets are distributed devices under a central command and control. Used to launch distributed attacks and are difficult to shut down immediately.

b. Access control ensure that authorized users who have access to sensitive data will not misuse it.
AGREE. After authorization users are given, selective access to resources based on their duties.

c. Message Authentication Code and digital signature both verified with the same type of key.
DISAGREE. MAC uses shared key while digital signatures uses public-private key pairs.

d. A common approach for creating polymorphic viruses uses encryption technology and mutation engine.
AGREE. Encryption hides the payload and mutation engine introduce changes in code to avoid signature detection.

e. An attacker would like to delete all of the tables in the insecure database. To delete the users table using the given SQL query, the attacker pass in the following as the uid: **`0; DROP TABLE users;`**

```
$query = "SELECT name FROM users WHERE uid = $UID";
```

AGREE. UID = 0 will most probably return no rows but drop table users statement will executes only if the user has privilege on users table. In ORACLE RDBMS, the USERS table is owned by SYS by default with no drop/delete/update access to other accounts.

f. A gateway firewall does not defend against a trusted party inside the firewall that becomes malicious and attempts to breach other computers within the network.
AGREE. Firewall at the gateway only restrict packets coming in or going out of the network. A malicious insider with access can breach any computer inside the network.

g. IT security risk assessment process cannot be executed without identify organization's assets.
AGREE. Security risk is primarily associated with digital assets which the organization possesses. Therefore, asset inventory plays a key role in making the security policy before execution of any IT security risk assessment process.

h. Rootkit has no role in helping hacker (bad guy) install software.
DISAGREE. A rootkit is hidden software components that allows hackers to get into a system without detection.

i. Network based intrusion detection monitors the characteristics of a single host and the events occurring within that host for suspicious activity.
DISAGREE. NID monitors and mitigate network wide threats by placing sensors at various places across network and decision support with the help of a central controller. However, host events can also be used in NID.

j. Baseline approach in risk assessment generally recommended only for small organizations without the resources to implement more structured approaches.
AGREE. Hiring consultant and implementing their recommendation are costly and better suited to mid-to-large sized organizations.

Question # 2: Provide suitable short-answers to the following questions with correct justification. Partial marks will *NOT* be given without justification. Each question carries 2 points. [2 x 5 = 10 Points]

a. An attacker is trying to attack the company Wahoo and its users. Assume that users always visit Wahoo's website with an HTTPS connection, using RSA and AES encryption. If the attacker obtains a copy of Wahoo's certificate, could the attacker impersonate (spoof) the Wahoo web server to a user?
YES. A copy of Wahoo's certificate installed on the hacker's web server is not sufficient, as s/he needs phishing emails (or some other method) to trick user to come to his /her server.

b. Can QR codes help launch phishing attacks?
YES. A carefully crafted URL in the QR code (hidden from the eyes of the user) can create many web security issues.

c. Imran was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment. Meanwhile, Asif, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of the attack, the server crashed and Asif needed to reboot the system, as no one was able to access the resources of the company. This process involves human interaction to fix it. Explain what kind of DoS attack was best illustrated in the scenario above?
This scenario does not gives details of the DoS attack. However, it makes Brownies Inc. infrastructure unavailable.

d. The software company Snoracle (slogan: "Unwakeable") is selling a new defense against intrusions. Their software looks at the source IP address on all incoming packets, and if it finds any IP address that accounts for more than 1% of traffic over the last hour, it installs an entry in the router that blocks all packets from that address for the next 24 hours. Is this a great solution against intrusions?

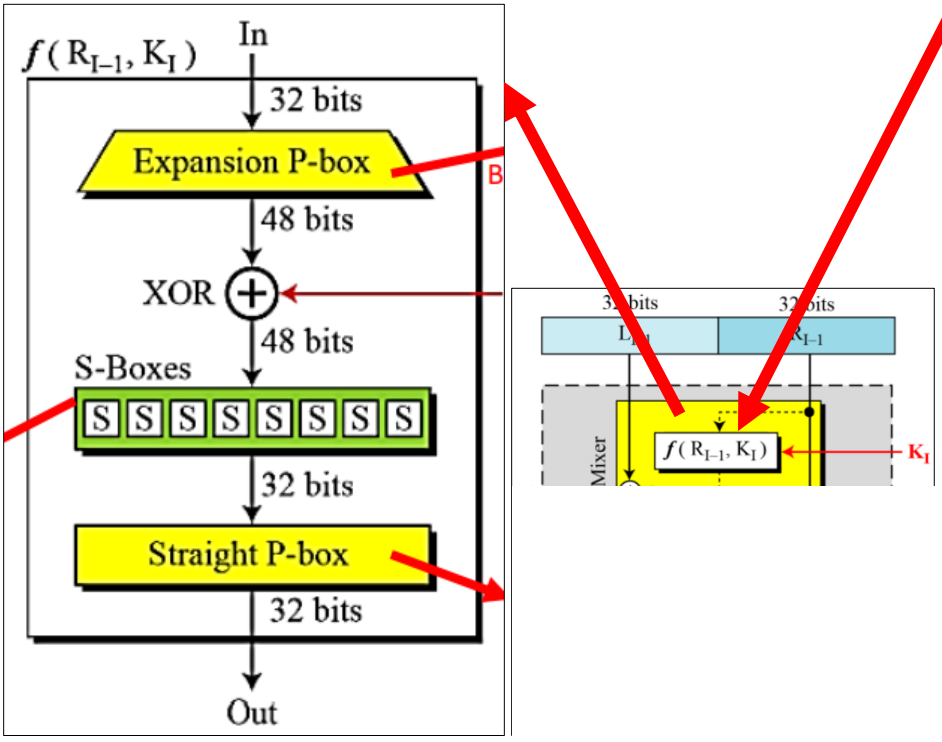
The solution describe seems to work if intrusions count are low. Otherwise, installing a new entry for each unique source IP address will pollute the routing table of the router…thus slowing down routing operations. A separate firewall box to perform this operation seem best.

e. Consider two scenarios: i) online shopping and ii) government portal. Who will be the targets, victims, in each of these scenarios and what will be the countermeasures in each of them.

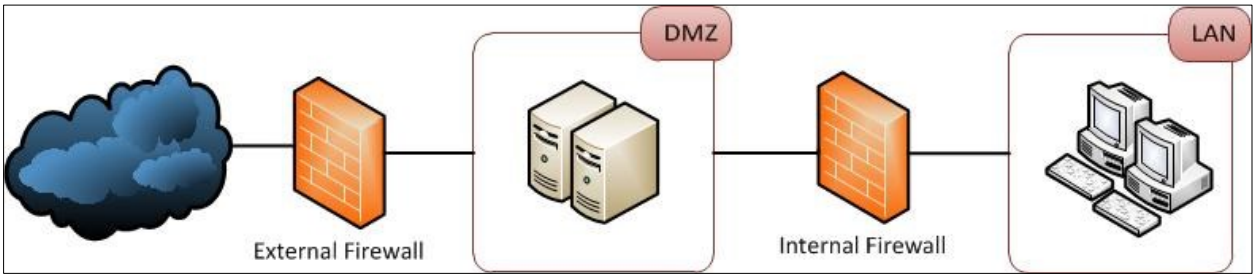
Online Shopping: Any attack on an online shopping portal could target primarily the company and indirectly the clients (stolen credit cards). Countermeasure will be based on the type of attack, which is not given in the question. For example, for simple DoS attacks we can use the method given in part (d) above.

Question # 3: Illustrate (*detailed labelled diagram that conveys a concept and architecture*) the answers of the following questions using a suitable diagram. Textual answers will get no credit. *Incomplete diagram and missing labels will get very low scores.* Each question carries 3 points. [3 x 5 = 15 Points]

a. DES is based on Feistal Network, which is an invertible function. Draw the Feistal function.



b. Propose a secure architecture for the network in such a way that your company's Webserver and Mail server can be contacted from outside without any restriction and the intranet is kept hidden from outside.



c. What is the difference between a false positive and a false negative in the context of an Intrusion Detection System? Depict using a diagram.

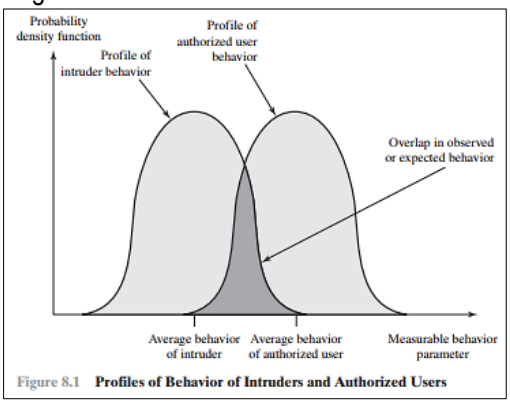


Figure 8.1 **Profiles of Behavior of Intruders and Authorized Users**

d. Show a scheme of database encryption using a block diagram involving client and server.

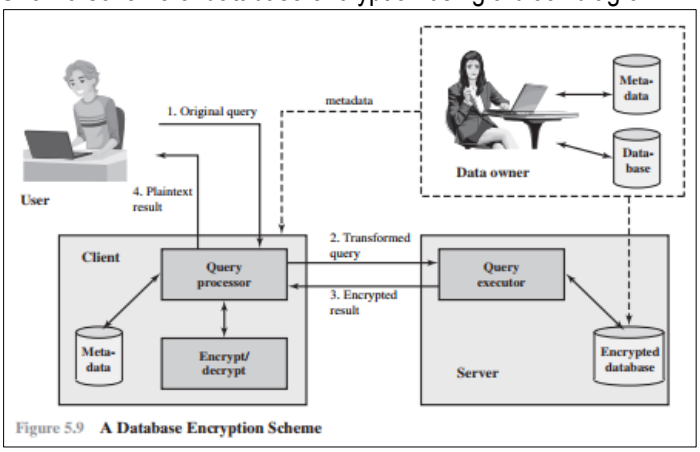


Figure 5.9 **A Database Encryption Scheme**

e. How can an access control function be organized? Illustrate using various control mechanisms.

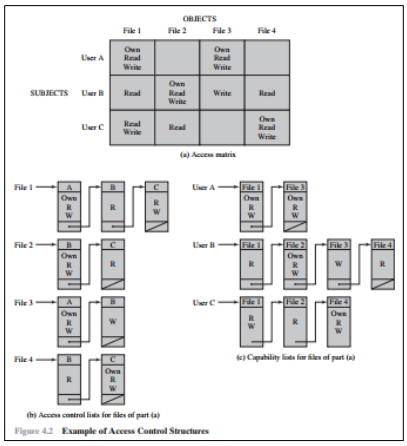


Figure 4.2 **Example of Access Control Structures**

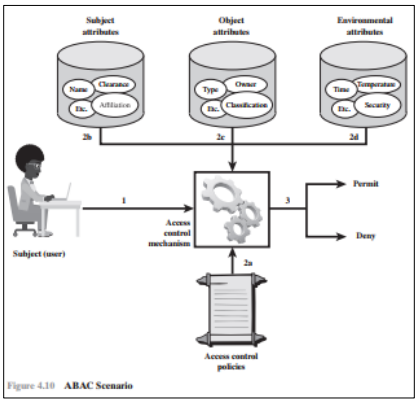
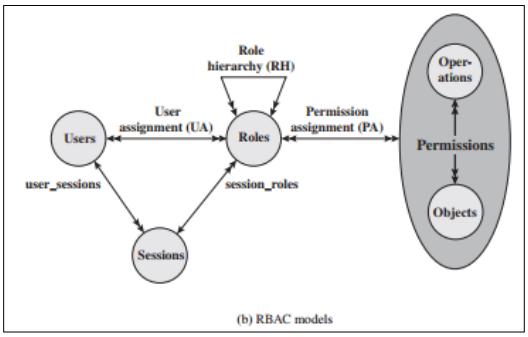


Figure 4.10 **ABAC Scenario**



(b) RBAC models

Question # 4: Answer the questions brief textual explanation. Each question carries 3 points. [3 x 3 = 09 Points]

a. Suppose you are tasked to demonstrate your abilities to analyze a piece of malicious code and report the following:

Task # 1: You found that the code has three different ways for propagation. Briefly describe each, explaining functionality and specific propagation steps.

Need explanations of following three propagation methods in 2-3 lines each.

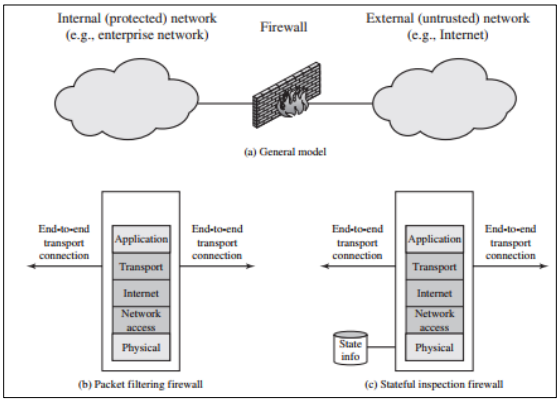
6.3 Propagation—Infected Content—Viruses
6.4 Propagation—Vulnerability Exploit—Worms
6.5 Propagation—Social Engineering—Spam E-mail, Trojans

Task # 2: You found that the code has four different ways to damage IT assets. Briefly describe each, explaining how systems are compromised to delete/damage/steal/ransom different digital assets.

Need explanations of following three propagation methods in 2-3 lines each.

6.6 Payload—System Corruption
6.7 Payload—Attack Agent—Zombie, Bots
6.8 Payload—Information Theft—Keyloggers, Phishing, Spyware
6.9 Payload—Stealthing—Backdoors, Rootkits

b. How different types of firewalls help in i) detection and ii) prevention of intrusion where IT assets are connected to a network? You answer should discuss each type of firewall.



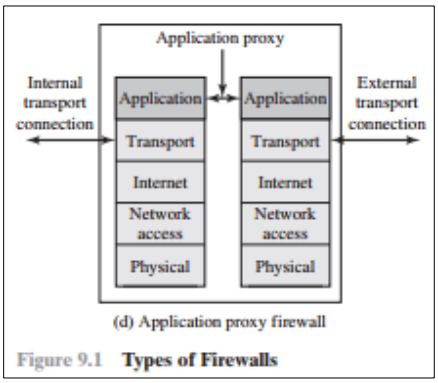
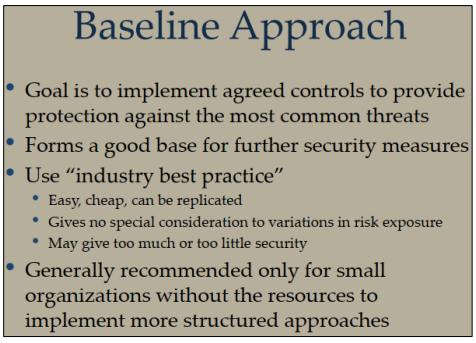
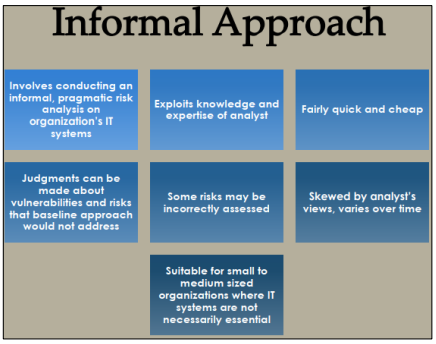


Figure 9.1 **Types of Firewalls**

Three type of firewalls i) packet filtering, ii) stateful inspection and application proxy. Student need to discussion detection and prevention separately for each type of firewall.

c. Compare and contrast i) baseline and ii) Informal approaches to security risk assessment when used by FAST-NU (KHI Campus). Which is better in your opinion and why?





Full marks given to answers that will list features of both approaches and select one as better giving an argument.

Question # 5: Answer the questions brief justification. Each question carries 3 points. [3 x 2 = 06 Points]

a. List the clauses of Pakistan law called Prevention of Electronic Crime Act, 2016 that provides legal action against cybercrimes you described in part (a) above.

Correct answer must list three crimes will give one line description and 2-3 line scenarios.

- Hate speech
- Electronic forgery and electronic fraud
- Identity theft
- Dignity/Modesty of a natural person.
- Child pornography
- Promoting malicious code
- Cyber Stalking
- Spamming

b. List two different ethical issues in information security. Suppose an IT manager has access to video footages of all cameras across some corporate campus. Explain ONE ethical responsibility, as per the corporate ethical code of conduct that the IT manager must follow while accessing these video.

Two key issues are: i) compromising individual or corporate privacy and ii) Personal integrity and honesty.

The two issues listed above are key responsibility of IT manager while being the custodian of the videos. The student need to write some key step of code of conduct (similar to IEEE and AITP) that the IT manager will use while accessing videos and keeping secondary information (the non-relevant information he/she gained by look at relevant parts of the videos) must be kept confidential all the times.