- Each part in question # 1 carries 1 mark and from question # 2 to question # 5 each part carries 3 marks.

Time allowed: 180 minutes **Max. Marks**: 50

Question # 1: State Agree or Disagree and provide one-sentence justification. Partial marks will be given where no justification is provided.

a) Computing a hash for a data item using a cryptographic hash function such as SHA-1 requires possession of the correct secret key**. (1) DISAGREE**

b) Digital signatures use public-key cryptography to provide both integrity and authentication. **(1) AGREE**

c) The strength of authentication systems is inversely proportional to the number of factors incorporated by the system. **(1) DISAGREE**

d) Authentication is the verification that the credentials of a user or other system entity are valid. **(1) AGREE**

e) How a virus spreads is dependent on the payload it executes on each system it infects. **(1) DISAGREE**

Reasons are simple can be discussed with the teacher**.**

Question # 2:

a) Differentiate between risk, vulnerability, and threat, in the context of network security. **(3)**

A: A risk is defined as the result of a system being secure but not secured sufficiently, thereby increasing the likelihood of a threat. A vulnerability is a weakness or breach in your network or equipment (e.g. modems, routers, access points). A threat is the actual means of causing an incident; for instance, a virus attack is deemed a threat.

b) You are watching an encrypted conversation between Alice and Bob. You notice that the prefixes of any of the cipher texts agree for several hundred bytes. In addition, these identical prefixes are always a multiple of 16 bytes long. However, you never observe two identical chunks of cipher text of any significant length following the identical prefixes. Conjecture what cipher is being used, what mode of operation is being used, and what Alice and Bob are doing wrong**. (3)**

Solution

Full credit will be given for an answer as AES or DES in ECB mode, with some explanation (e.g., all messages have long, common headers

c) Consider that "Javed" has the option of using DES only for encryption purposes despite the fact that better algorithms such as AES do exist for encryption. "Javed" chose to use the following keys for encryption (Figure 1). Has he chosen the right keys for encryption? Is there any specific issue in using such keys? Please give exact reason why or why not he may use these keys? What happens if "Javed" uses a single key multiple times? **(3)**

Keys before parities drop (64 bits)	*Actual key (56 bits)*
0101 0101 0101 0101	0000000 0000000
1F1F 1F1F 0E0E 0E0E	0000000 FFFFFFF
E0E0 E0E0 F1F1 F1F1	FFFFFFF 0000000
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFF

Figure 1: Keys of Encryption

Solution:

Weak Keys Four out of 2^{56} possible keys are called weak keys. A weak key is the one that, after parity drop operation (using Table 6.12), consists either of all 0s, all 1s, or half 0s and half 1s.
The round keys created from any of these weak keys are the same and have the same pattern as the cipher key. For example, the sixteen round keys created from the first key is all made of 0s; the one from the second is made of half 0s and half 1s.

After two encryptions with the same key the original plaintext block is created. Note that if "Javed" uses the encryption algorithm two times, not one encryption followed by another decryption.

Key: 0x0101010101010101
Plaintext: *0x1234567887654321* Ciphertext: 0x814FE938589154F7

Key: 0x0101010101010101
Plaintext: 0x814FE938589154F7 Ciphertext: *0x1234567887654321*

Question # 3:

a) Differentiate between malwartizing and click jacking (at least 3 differences). **(3)**

Solution:

Malvertizing:

- Places malware on websites without actually compromising them
- The attacker pays for advertisements that are highly likely to be placed on their intended target websites and incorporate malware in them
- Using these malicious ads, attackers can infect visitors to sites displaying them
- The malware code may be dynamically generated to either reduce the chance of detection or to only infect specific systems
- Has grown rapidly in recent years because they are easy to place on desired websites with few questions asked and are hard to track
- Attackers can place these ads for as little as a few hours, when they expect their intended victims could be browsing the targeted websites, greatly reducing their visibility

Clickjacking:

- Vulnerability used by an attacker to collect an infected user's clicks
    - The attacker can force the user to do a variety of things from adjusting the user's computer settings to unwittingly sending the user to Web sites that might have malicious code
    - By taking advantage of Adobe Flash or JavaScript an attacker could even place a button under or over a legitimate button making it difficult for users to detect

- A typical attack uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page
- The attacker is hijacking clicks meant for one page and routing them to another page

b) Suppose you bought a new smartphone and are enthusiastic about game applications available for it. When you download and start to install one game application, you are asked to approve the access permissions granted to it. It wants permission to "Send SMS messages" and to "Access your address-book". What threat might the application pose to your smartphone, should you grant these permissions and proceed to install it? **(3)**

Solution:

If when you download and start to install some game app, you are asked to approve the access permissions "Send SMS messages" and to "Access your address-book", you should indeed be suspicious that a game wants these types of permissions, as it would not seem needed just for a game. Rather it could be malware that wants to collect details of all your contacts, and either return them to the attacker via SMS, or allow the code to send SMS messages to your contacts, perhaps enticing them to also download and install this malware. Such code is a trojan horse, since it contains covert functions as well as the advertised functionality.

c) Explain signature based and anomaly-based detection. How Anomaly based detection is better than signature-based detection? **(3)**

Solution:

Signature Based Detection:

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules

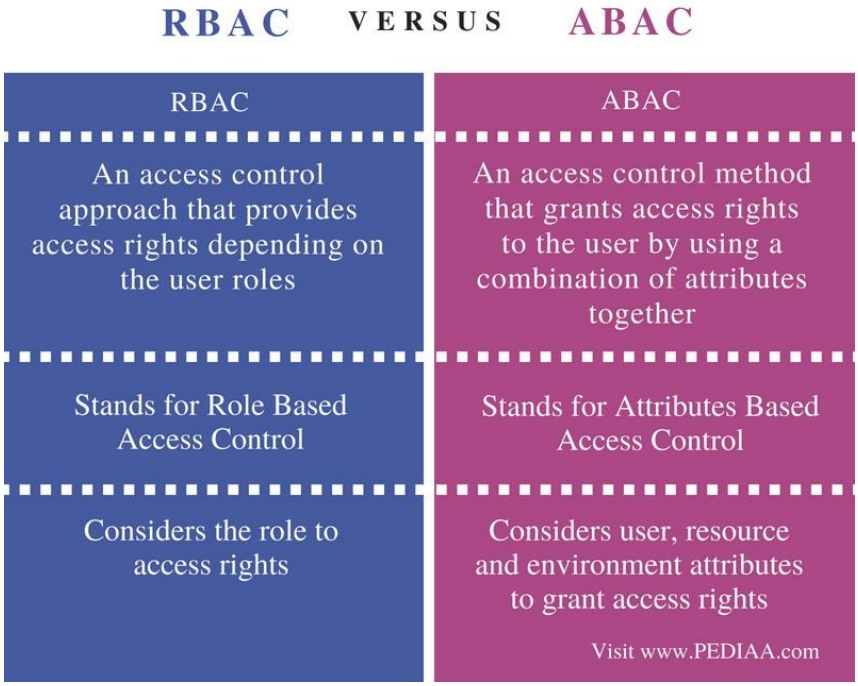
Anomaly Based Detection:

- Involves the collection of data relating to the behavior of legitimate users over a period of time.
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder.

Why better: Anomaly based detects novel attacks

Question # 4:

a) Differentiate between Role-based and Attribute-based Access Controls. **(3)**



Roles examles are HR Manager, Director etc.

Attributes are location, time etc.

b) A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server. Based on this information, what should be one of your key recommendations to the bank regarding the placement of the server? **(3)**

Solution:

Place a front-end web server in a demilitarized zone that only handles external web traffic

c) Which particular type of SQL Injection is shown in Figure 2? Justify your answer. **(3)**

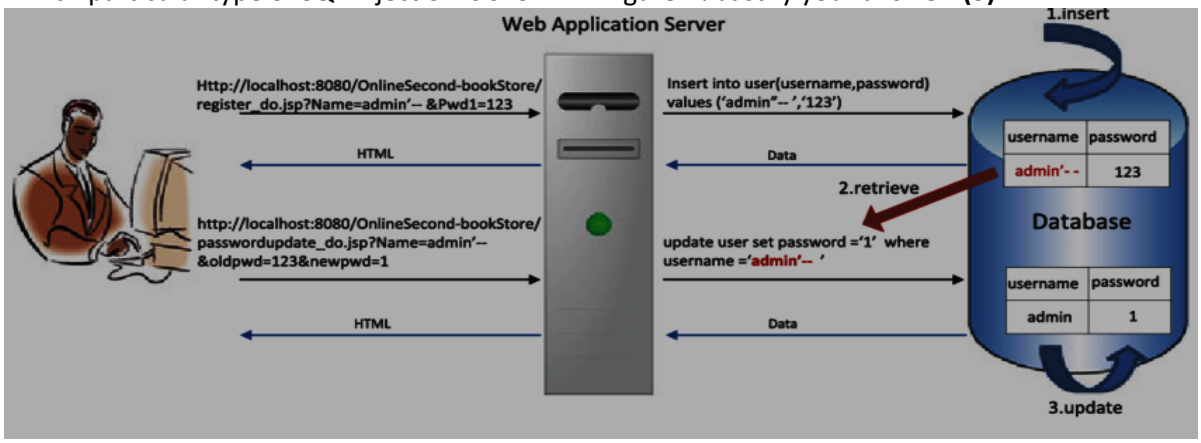


Figure 2: SQL Injection Attack

Solution:

SQL 2nd order Injection. Read the idea of 2nd order SQL injection.

Question # 5:

a) Which is worse in terms of Firewall detection, and why? A false positive or a false negative? **(3)**

A: A false negative is the worse. A false positive is simply a legitimate result that just got incorrectly flagged and blocked. While it's irksome, it's by no means fatal or difficult to correct. But a false

negative means that something bad has slipped through the firewall undetected, and that means a host of problems down the road.

b) SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set (Table 1):

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Table 1: A Packet Filter Rule Set

Describe the effect of each rule. **(3)**

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Table 1: A Packet Filter Rule Set

SOLUTION:

A. Inbound mail from an external source is allowed (port 25 is for SMTP incoming).
B. This rule is intended to allow a response to an inbound SMTP connection.
C. Outbound mail to an external source is allowed.

D. This rule is intended to allow a response to an outbound SMTP connection.

E. This is an explicit statement of the default policy. All rule sets include this rule implicitly as the last rule.

For all messages, the external network is on the other side (beyond gateway) of our local network. This needs to be mentioned. Moreover, A is linked to B and C is linked to D. E if default policy applied after all rules from A to D.

c) An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up. What is the most likely cause? **(3)**

Solution:

The most likely cause if all network devices are not all synchronized (discussed in class).

Question # 6

a)

Extended Access Control Matrix

A

SUBJECTS	OBJECTS: S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
	subjects			files		processes		disk drives	
S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
S_2		control		write *	execute			owner	seek *
S_3			control		write	stop			

* - copy flag set

b)

Database Encryption Scheme

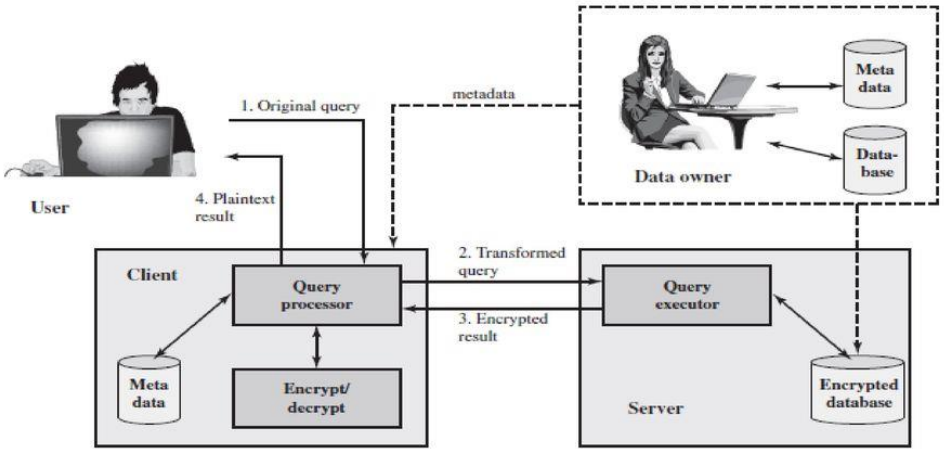


Figure 5.9 **A Database Encryption Scheme**

- **Data owner:** organization that produces data to be made available for controlled release
- **User:** human entity that presents queries to the system
- **Client:** frontend that transforms user queries into queries on the encrypted data stored on the server
- **Server:** an organization that receives the encrypted data from a data owner and makes them available for distribution to clients

c)