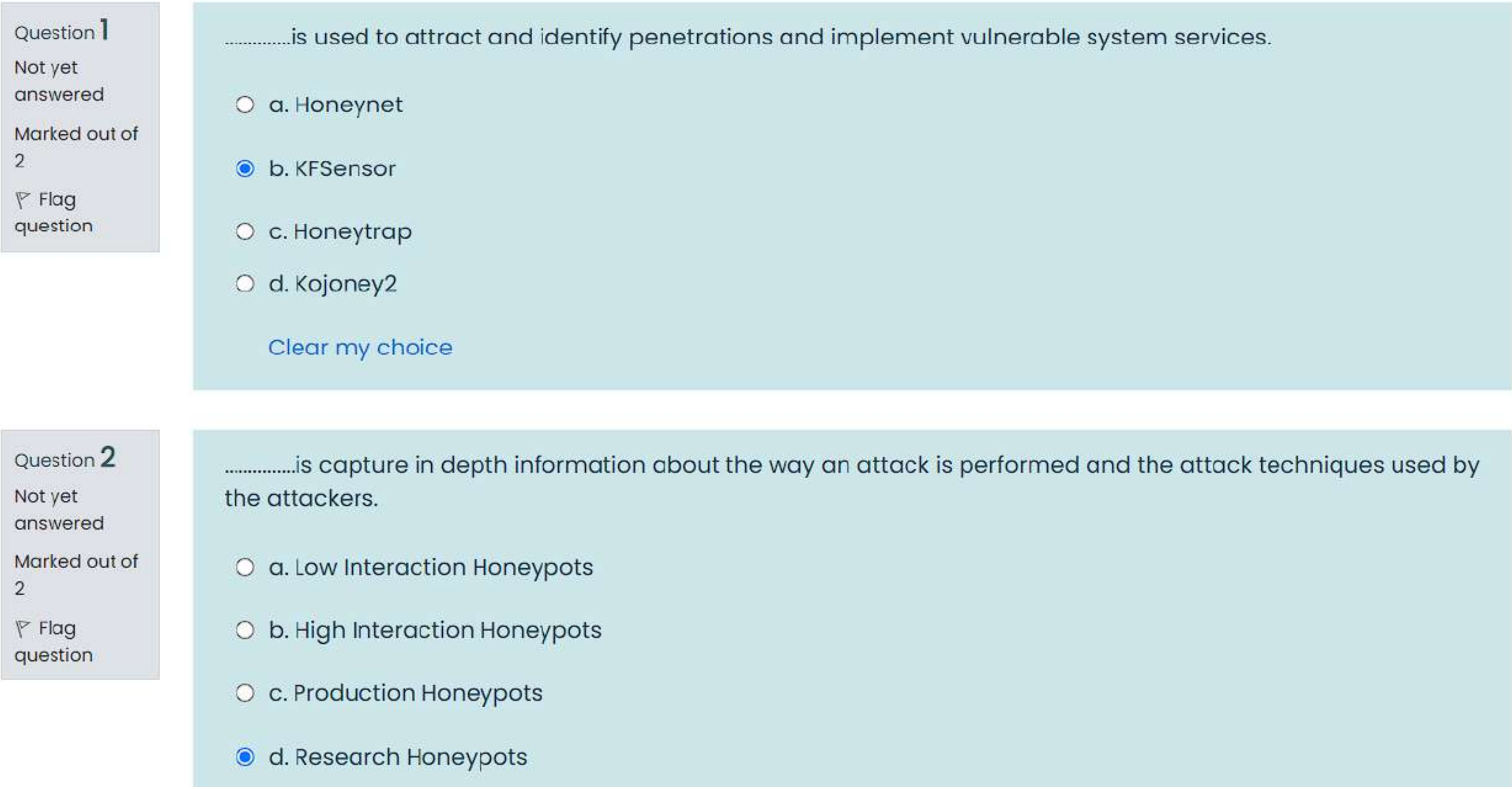


Question 1

Not yet answered

Marked out of 2

Flag question

..............is used to attract and identify penetrations and implement vulnerable system services.

○ a. Honeynet

● b. KFSensor

○ c. Honeytrap

○ d. Kojoney2

Clear my choice

Question 2

Not yet answered

Marked out of 2

Flag question

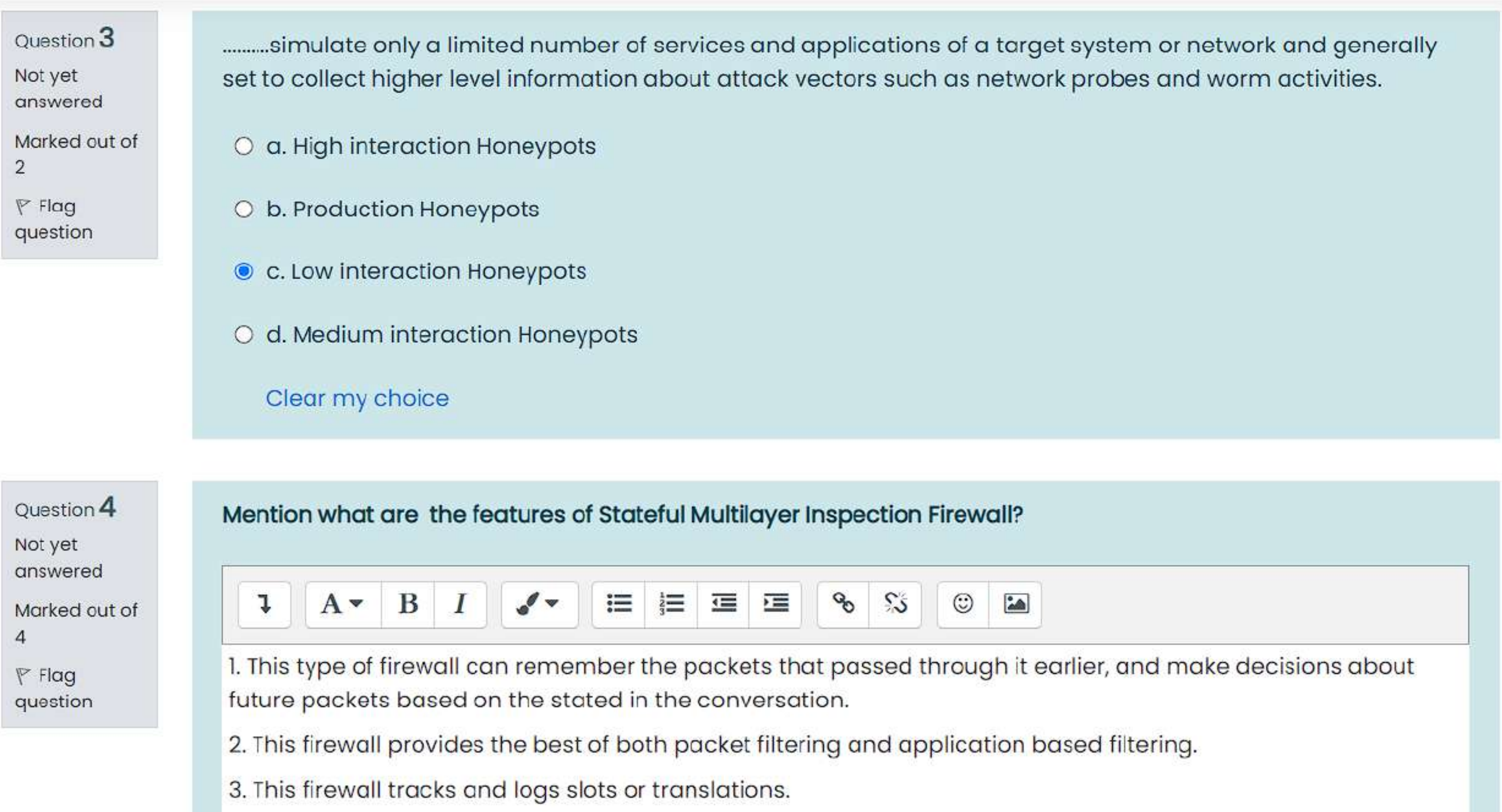
................is capture in depth information about the way an attack is performed and the attack techniques used by the attackers.

○ a. Low Interaction Honeypots

○ b. High Interaction Honeypots

○ c. Production Honeypots

● d. Research Honeypots



Question 3

Not yet answered

Marked out of 2

Flag question

..........simulate only a limited number of services and applications of a target system or network and generally set to collect higher level information about attack vectors such as network probes and worm activities.

○ a. High interaction Honeypots

○ b. Production Honeypots

● c. Low interaction Honeypots

○ d. Medium interaction Honeypots

Clear my choice

Question 4

Not yet answered

Marked out of 4

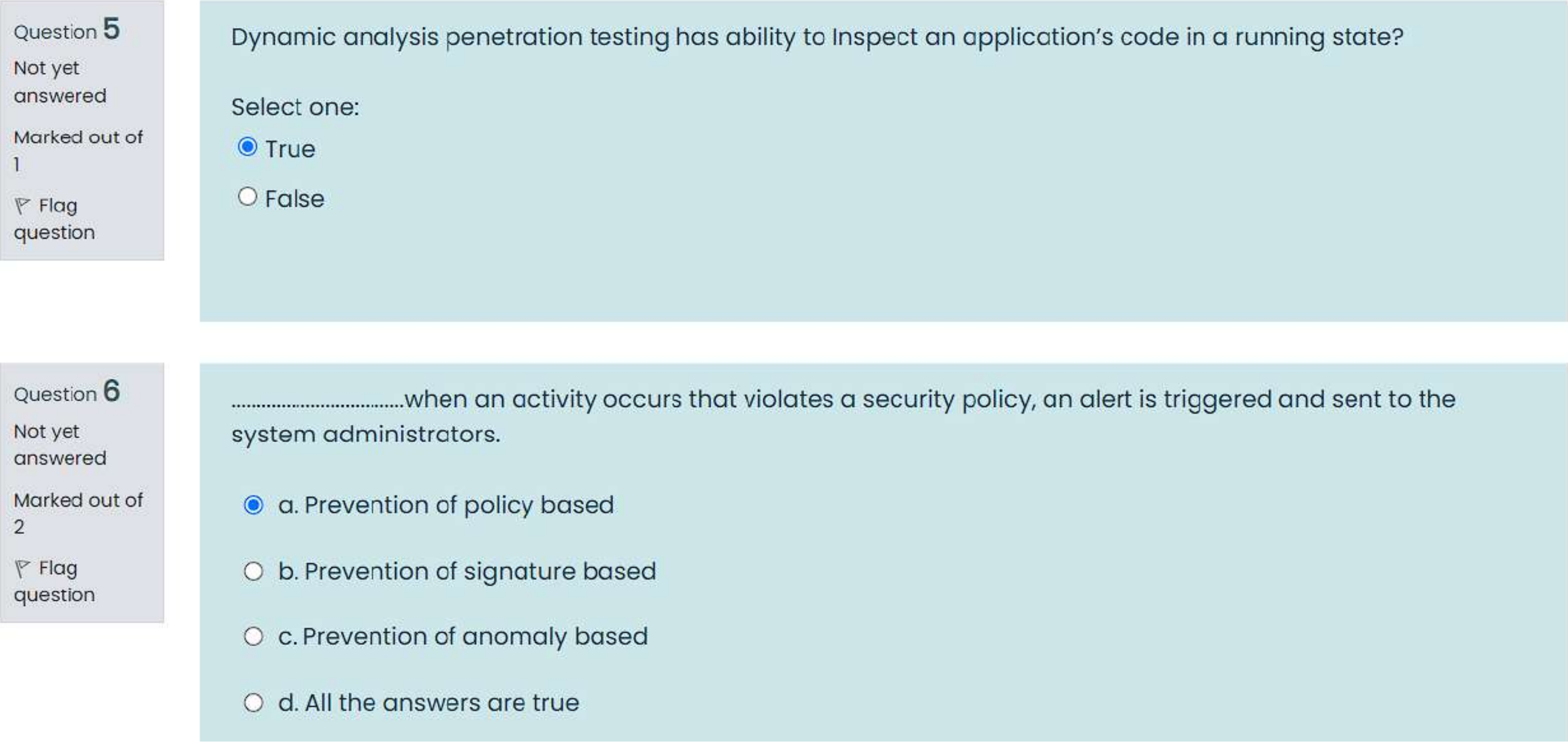
Flag question

Mention what are the features of Stateful Multilayer Inspection Firewall?

1. This type of firewall can remember the packets that passed through it earlier, and make decisions about future packets based on the stated in the conversation.

2. This firewall provides the best of both packet filtering and application based filtering.

3. This firewall tracks and logs slots or translations.



Question 5

Not yet answered

Marked out of 1

Flag question

Dynamic analysis penetration testing has ability to Inspect an application's code in a running state?

Select one:

● True

○ False

Question 6

Not yet answered

Marked out of 2

Flag question

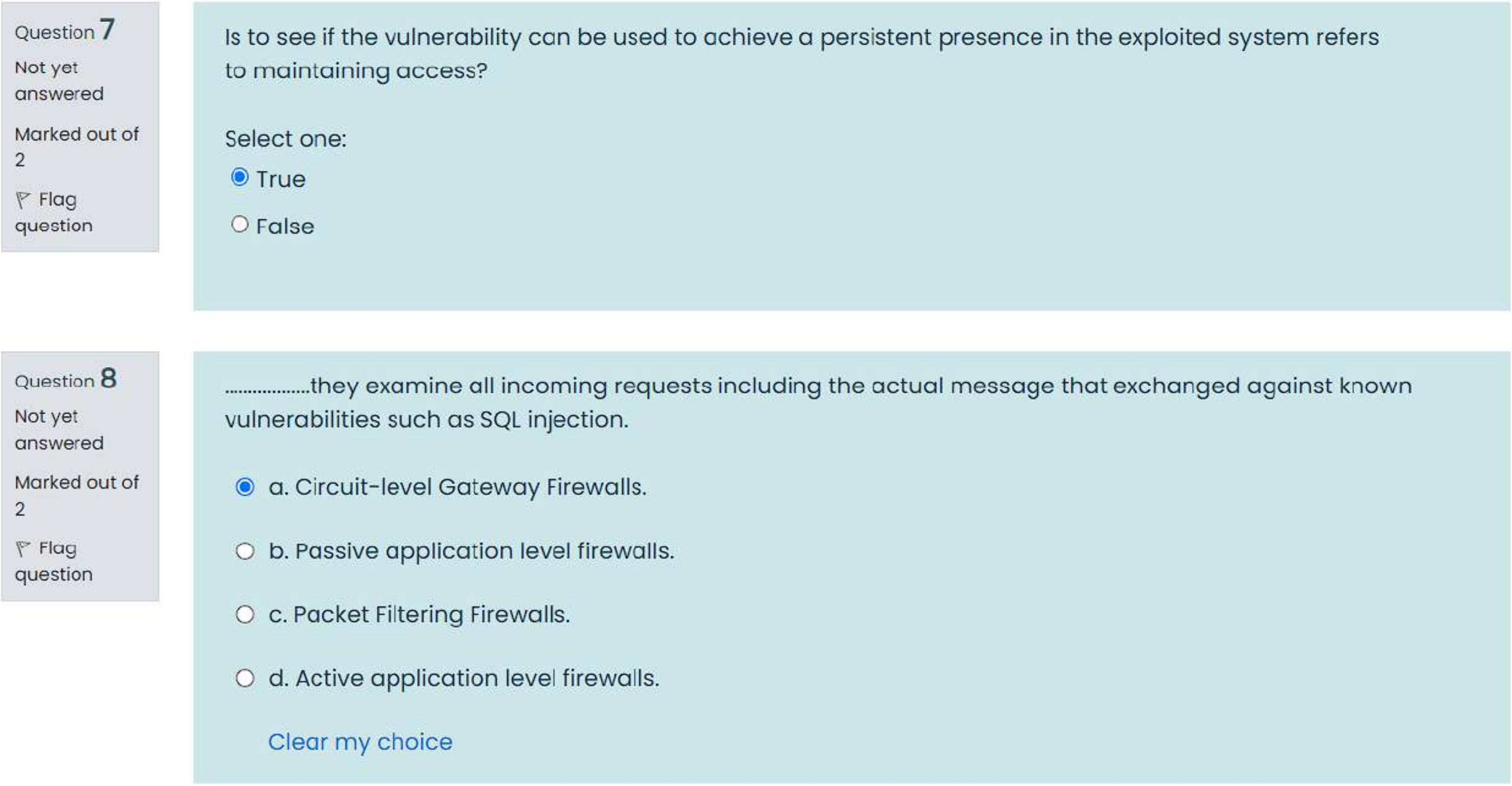
...............................when an activity occurs that violates a security policy, an alert is triggered and sent to the system administrators.

● a. Prevention of policy based

○ b. Prevention of signature based

○ c. Prevention of anomaly based

○ d. All the answers are true



Question 7

Not yet answered

Marked out of 2

Flag question

Is to see if the vulnerability can be used to achieve a persistent presence in the exploited system refers to maintaining access?

Select one:

● True

○ False

Question 8

Not yet answered

Marked out of 2

Flag question

..................they examine all incoming requests including the actual message that exchanged against known vulnerabilities such as SQL injection.

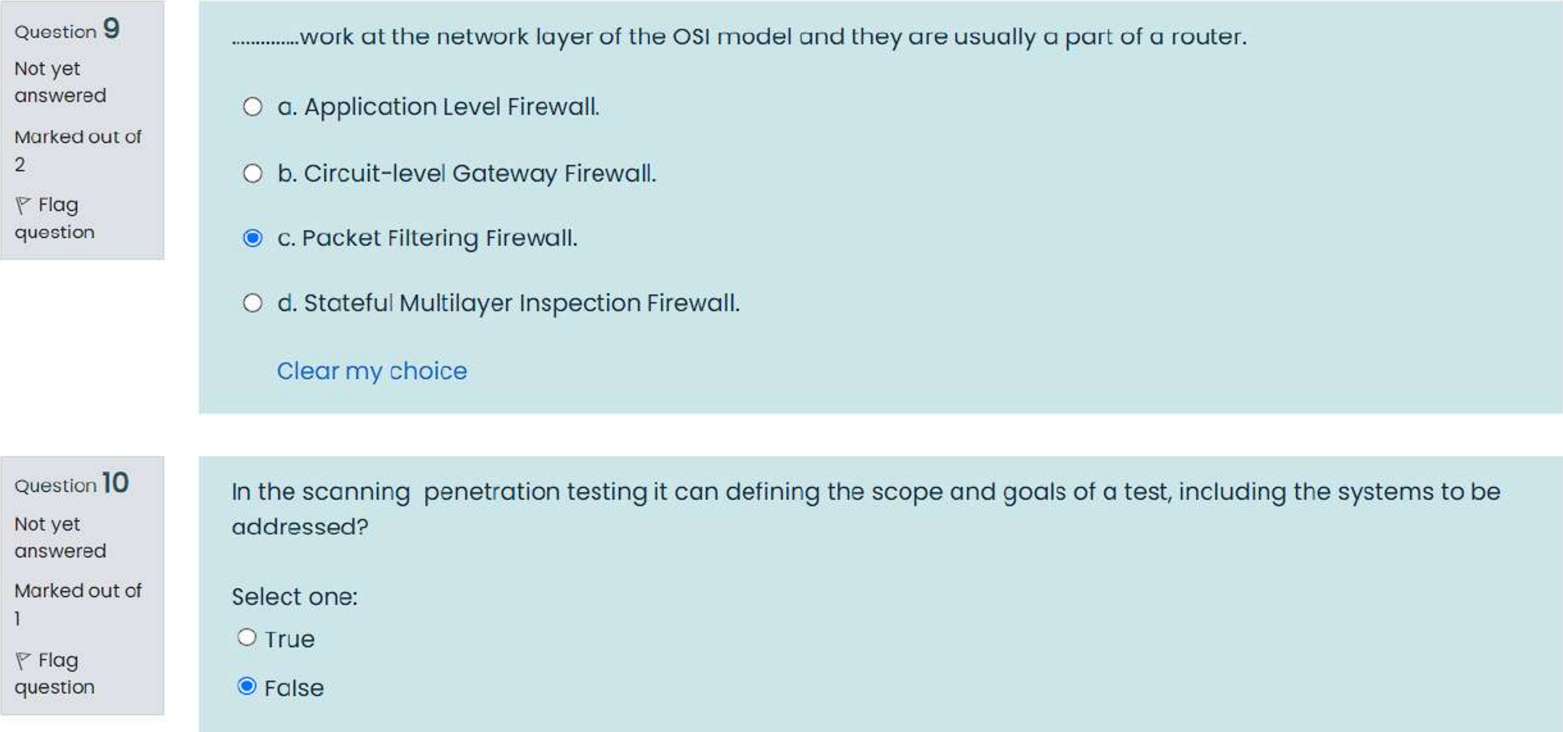
● a. Circuit-level Gateway Firewalls.

○ b. Passive application level firewalls.

○ c. Packet Filtering Firewalls.

○ d. Active application level firewalls.

Clear my choice



Question 9

Not yet answered

Marked out of 2

Flag question

..............work at the network layer of the OSI model and they are usually a part of a router.

○ a. Application Level Firewall.

○ b. Circuit-level Gateway Firewall.

● c. Packet Filtering Firewall.

○ d. Stateful Multilayer Inspection Firewall.

Question 10

Not yet answered

Marked out of 1

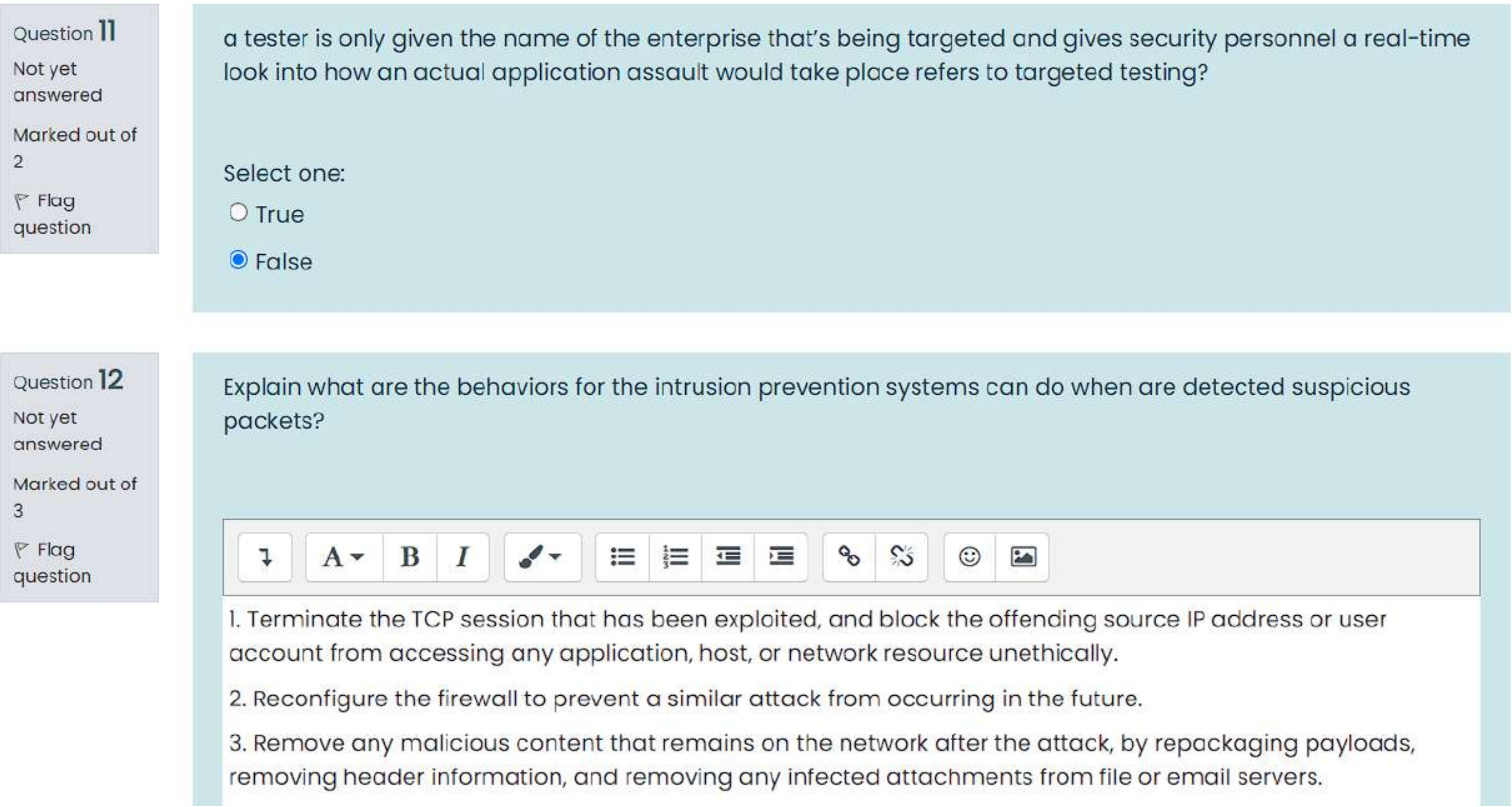
Flag question

In the scanning penetration testing it can defining the scope and goals of a test, including the systems to be addressed?

Select one:

○ True

● False



Question 11

Not yet answered

Marked out of 2

Flag question

a tester is only given the name of the enterprise that's being targeted and gives security personnel a real-time look into how an actual application assault would take place refers to targeted testing?

Select one:

○ True

● False

Question 12

Not yet answered

Marked out of 3

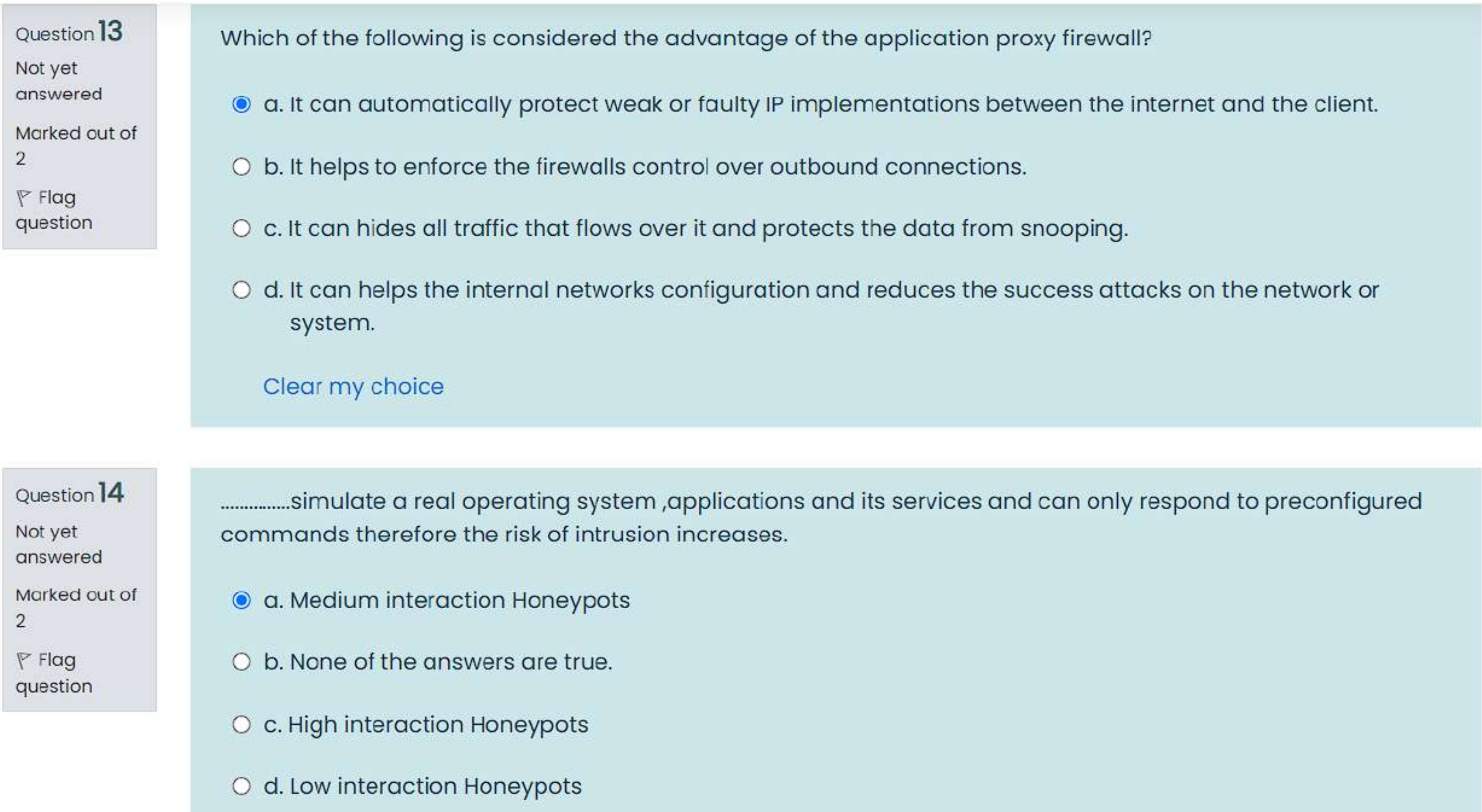
Flag question

Explain what are the behaviors for the intrusion prevention systems can do when are detected suspicious packets?

1. Terminate the TCP session that has been exploited, and block the offending source IP address or user account from accessing any application, host, or network resource unethically.

2. Reconfigure the firewall to prevent a similar attack from occurring in the future.

3. Remove any malicious content that remains on the network after the attack, by repackaging payloads, removing header information, and removing any infected attachments from file or email servers.



Question 13

Not yet answered

Marked out of 2

Flag question

Which of the following is considered the advantage of the application proxy firewall?

- ● a. It can automatically protect weak or faulty IP implementations between the internet and the client.
- ○ b. It helps to enforce the firewalls control over outbound connections.
- ○ c. It can hides all traffic that flows over it and protects the data from snooping.
- ○ d. It can helps the internal networks configuration and reduces the success attacks on the network or system.

Clear my choice

Question 14

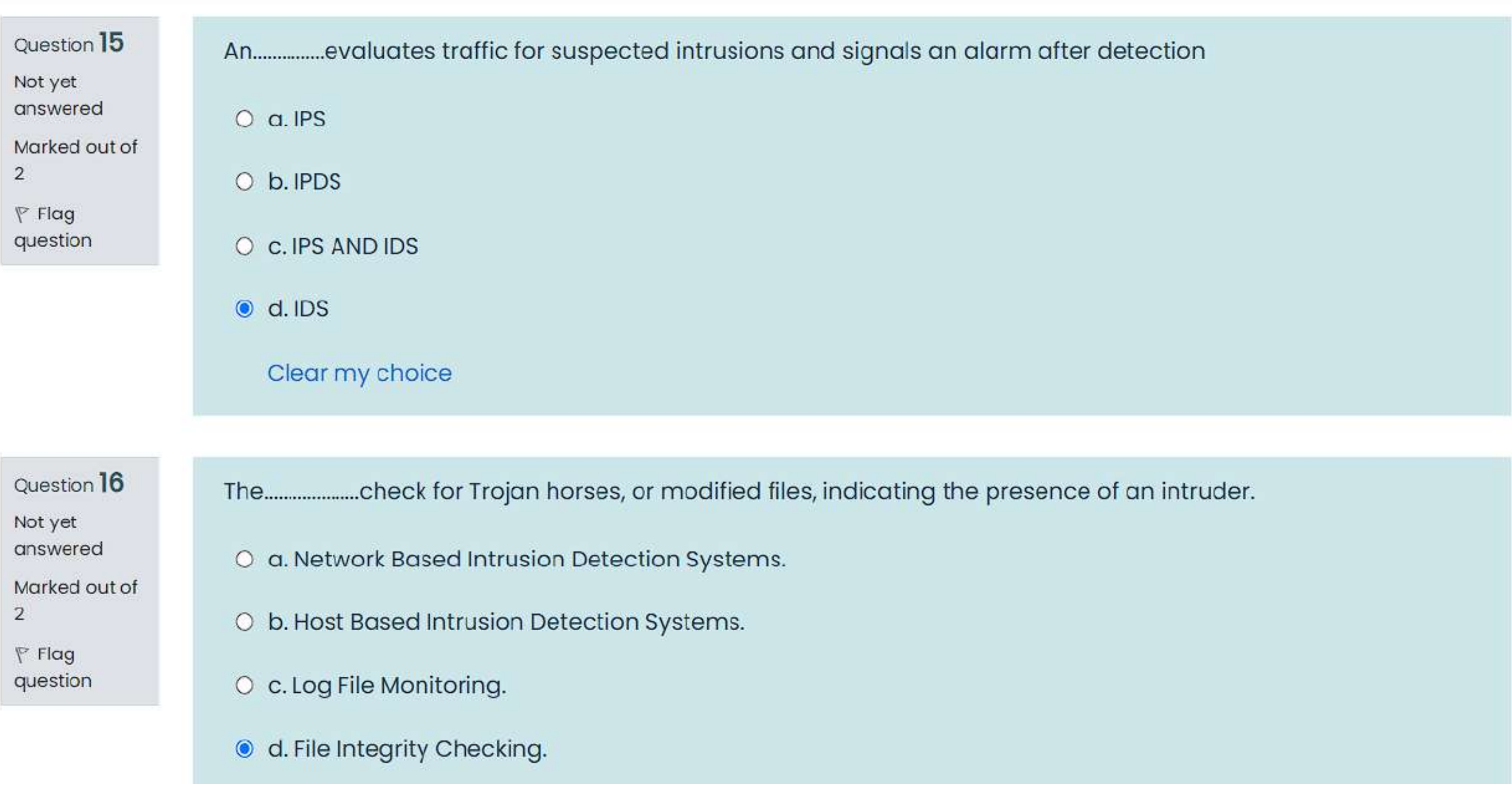
Not yet answered

Marked out of 2

Flag question

……………simulate a real operating system ,applications and its services and can only respond to preconfigured commands therefore the risk of intrusion increases.

- ● a. Medium interaction Honeypots
- ○ b. None of the answers are true.
- ○ c. High interaction Honeypots
- ○ d. Low interaction Honeypots



Question 15

Not yet answered

Marked out of 2

Flag question

An..............evaluates traffic for suspected intrusions and signals an alarm after detection

○ a. IPS

○ b. IPDS

○ c. IPS AND IDS

● d. IDS

Clear my choice

Question 16

Not yet answered

Marked out of 2

Flag question

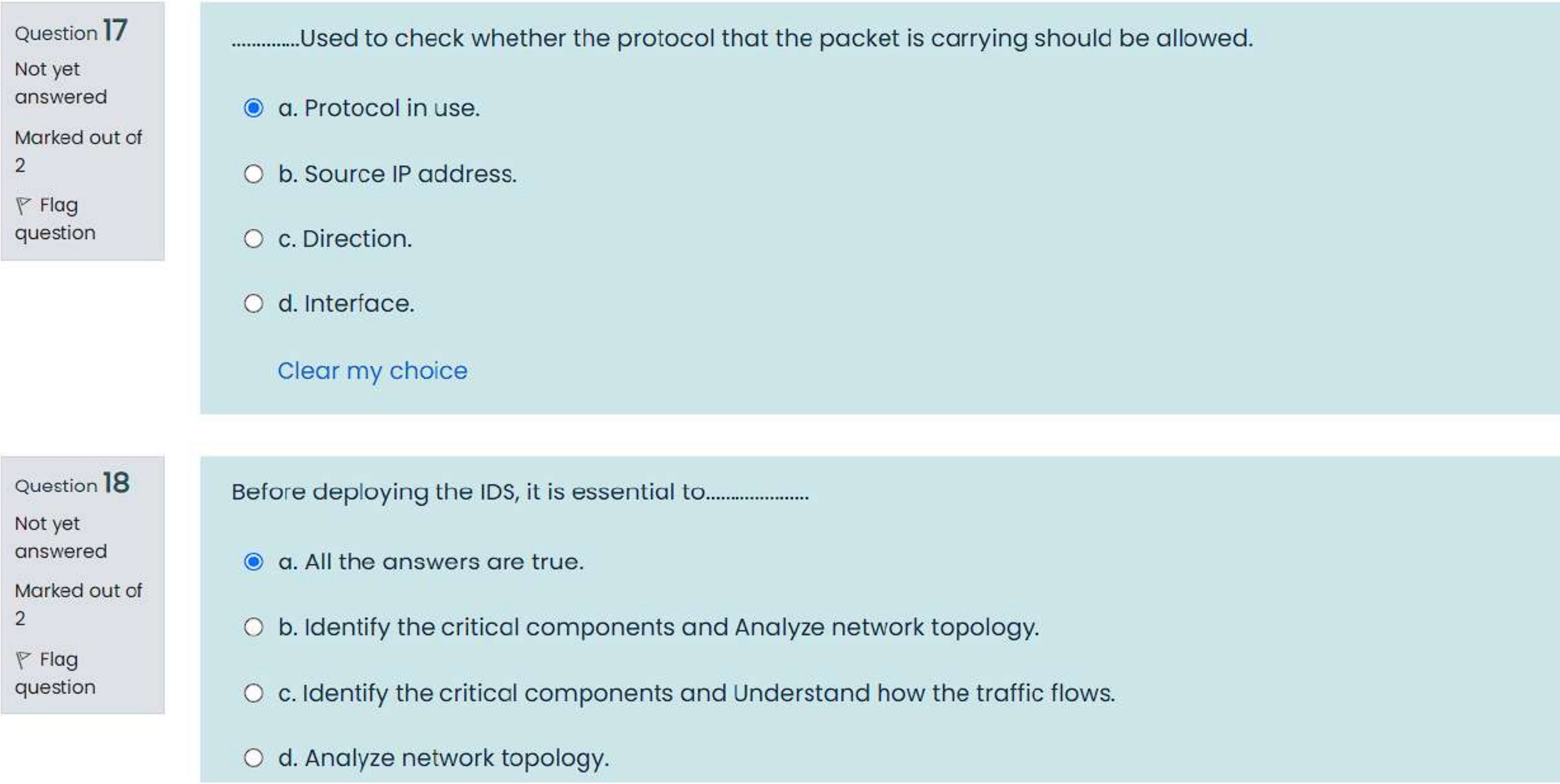
The...................check for Trojan horses, or modified files, indicating the presence of an intruder.

○ a. Network Based Intrusion Detection Systems.

○ b. Host Based Intrusion Detection Systems.

○ c. Log File Monitoring.

● d. File Integrity Checking.



Question 17
Not yet answered
Marked out of 2
Flag question

..............Used to check whether the protocol that the packet is carrying should be allowed.

● a. Protocol in use.

○ b. Source IP address.

○ c. Direction.

○ d. Interface.

Clear my choice

Question 18
Not yet answered
Marked out of 2
Flag question

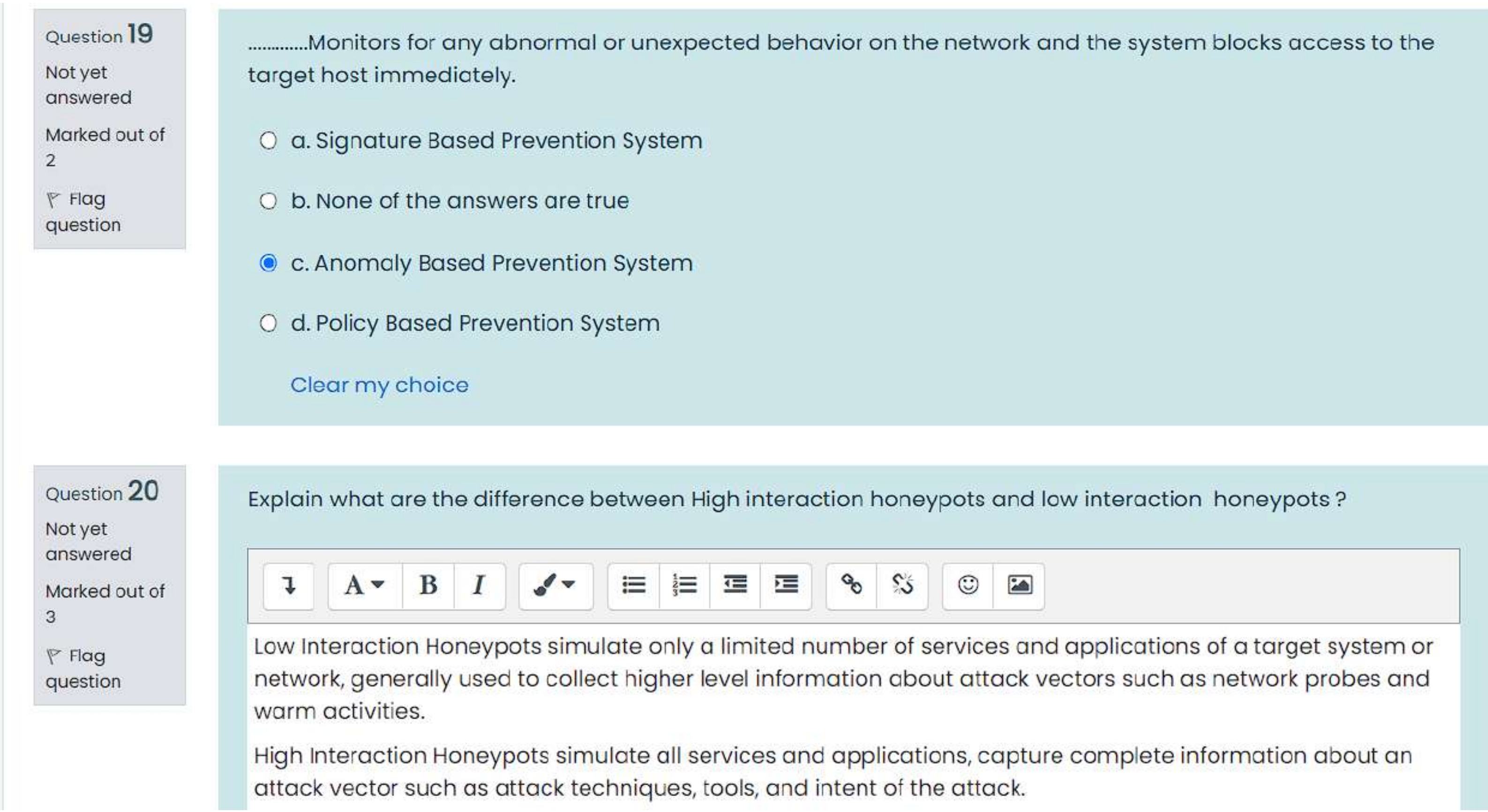
Before deploying the IDS, it is essential to.....................

● a. All the answers are true.

○ b. Identify the critical components and Analyze network topology.

○ c. Identify the critical components and Understand how the traffic flows.

○ d. Analyze network topology.



Question **19**

Not yet answered

Marked out of 2

Flag question

............Monitors for any abnormal or unexpected behavior on the network and the system blocks access to the target host immediately.

○ a. Signature Based Prevention System

○ b. None of the answers are true

● c. Anomaly Based Prevention System

○ d. Policy Based Prevention System

Clear my choice

Question **20**

Not yet answered

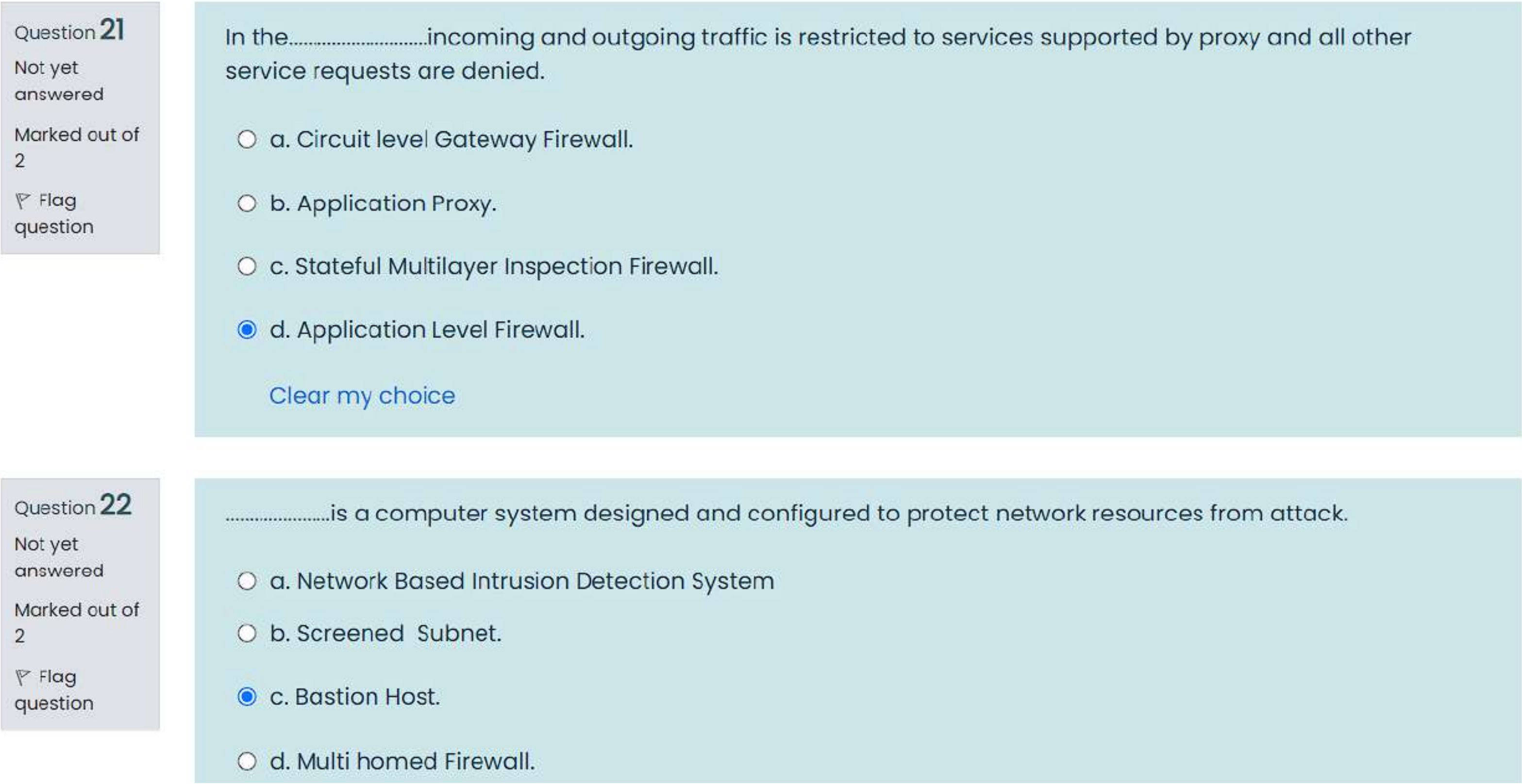
Marked out of 3

Flag question

Explain what are the difference between High interaction honeypots and low interaction honeypots ?

Low Interaction Honeypots simulate only a limited number of services and applications of a target system or network, generally used to collect higher level information about attack vectors such as network probes and warm activities.

High Interaction Honeypots simulate all services and applications, capture complete information about an attack vector such as attack techniques, tools, and intent of the attack.



Question 21

Not yet answered

Marked out of 2

Flag question

In the............................incoming and outgoing traffic is restricted to services supported by proxy and all other service requests are denied.

○ a. Circuit level Gateway Firewall.

○ b. Application Proxy.

○ c. Stateful Multilayer Inspection Firewall.

● d. Application Level Firewall.

Clear my choice

Question 22

Not yet answered

Marked out of 2

Flag question

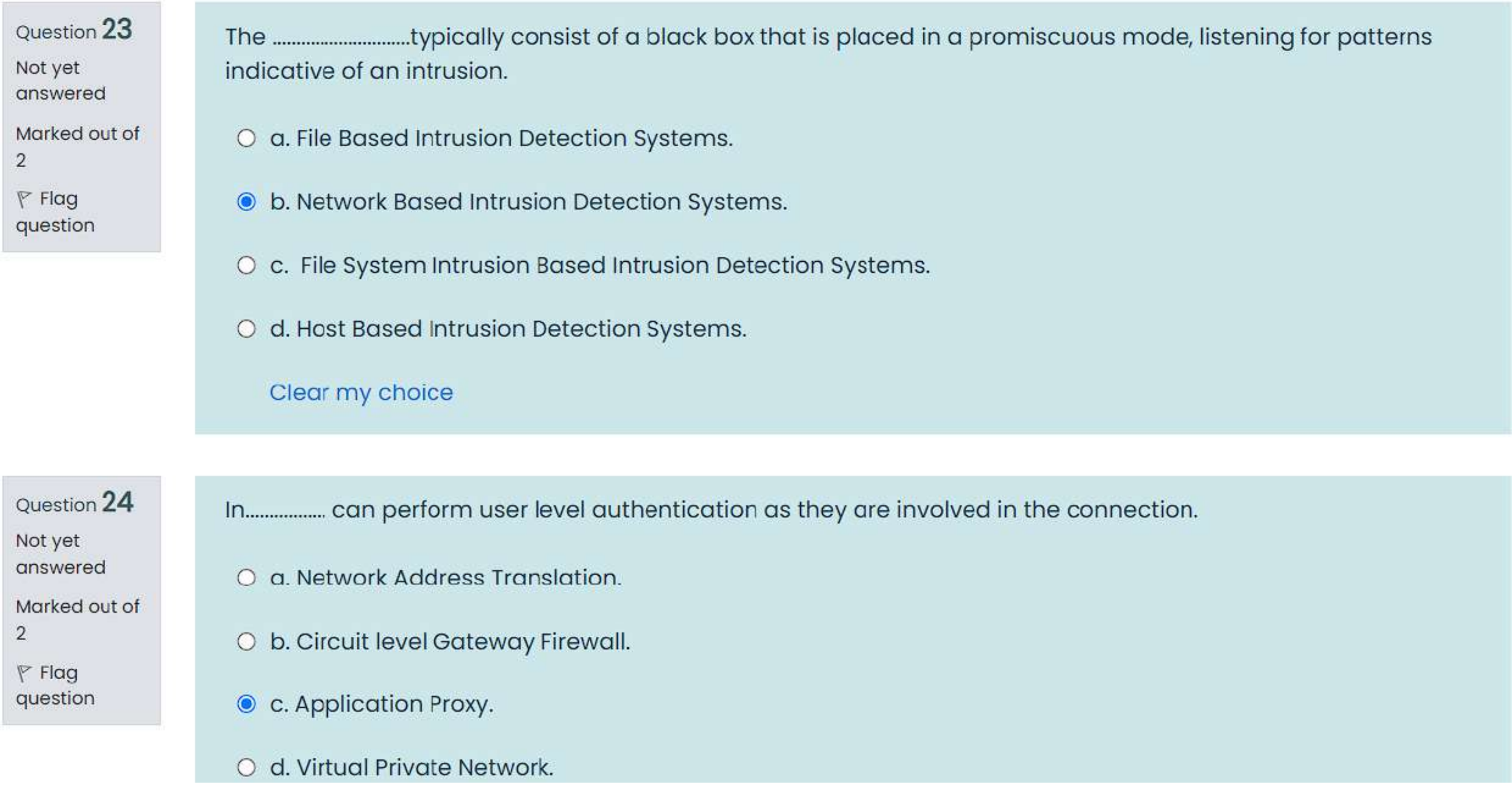
.....................is a computer system designed and configured to protect network resources from attack.

○ a. Network Based Intrusion Detection System

○ b. Screened Subnet.

● c. Bastion Host.

○ d. Multi homed Firewall.



Question 23

Not yet answered

Marked out of 2

Flag question

The ....typically consist of a black box that is placed in a promiscuous mode, listening for patterns indicative of an intrusion.

○ a. File Based Intrusion Detection Systems.

● b. Network Based Intrusion Detection Systems.

○ c. File System Intrusion Based Intrusion Detection Systems.

○ d. Host Based Intrusion Detection Systems.

Clear my choice

Question 24

Not yet answered

Marked out of 2

Flag question

In................ can perform user level authentication as they are involved in the connection.

○ a. Network Address Translation.

○ b. Circuit level Gateway Firewall.

● c. Application Proxy.

○ d. Virtual Private Network.