BC210424756: PALWASHA ALTAF

Time Left 89 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:23 PM, 19 August 2022

Question # 1 of 10 (Start time: 02:23:19 PM, 19 August 2022)

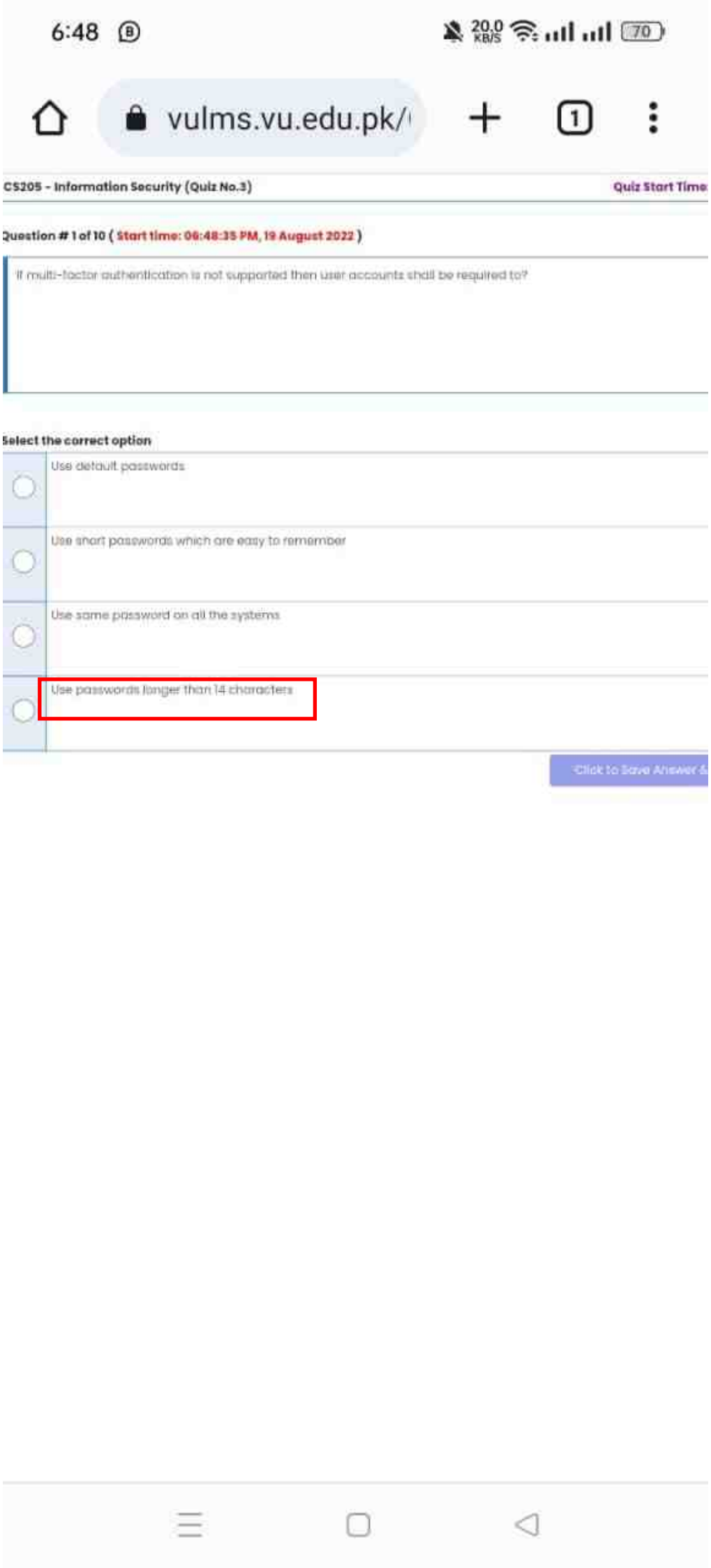
Total Marks: 1

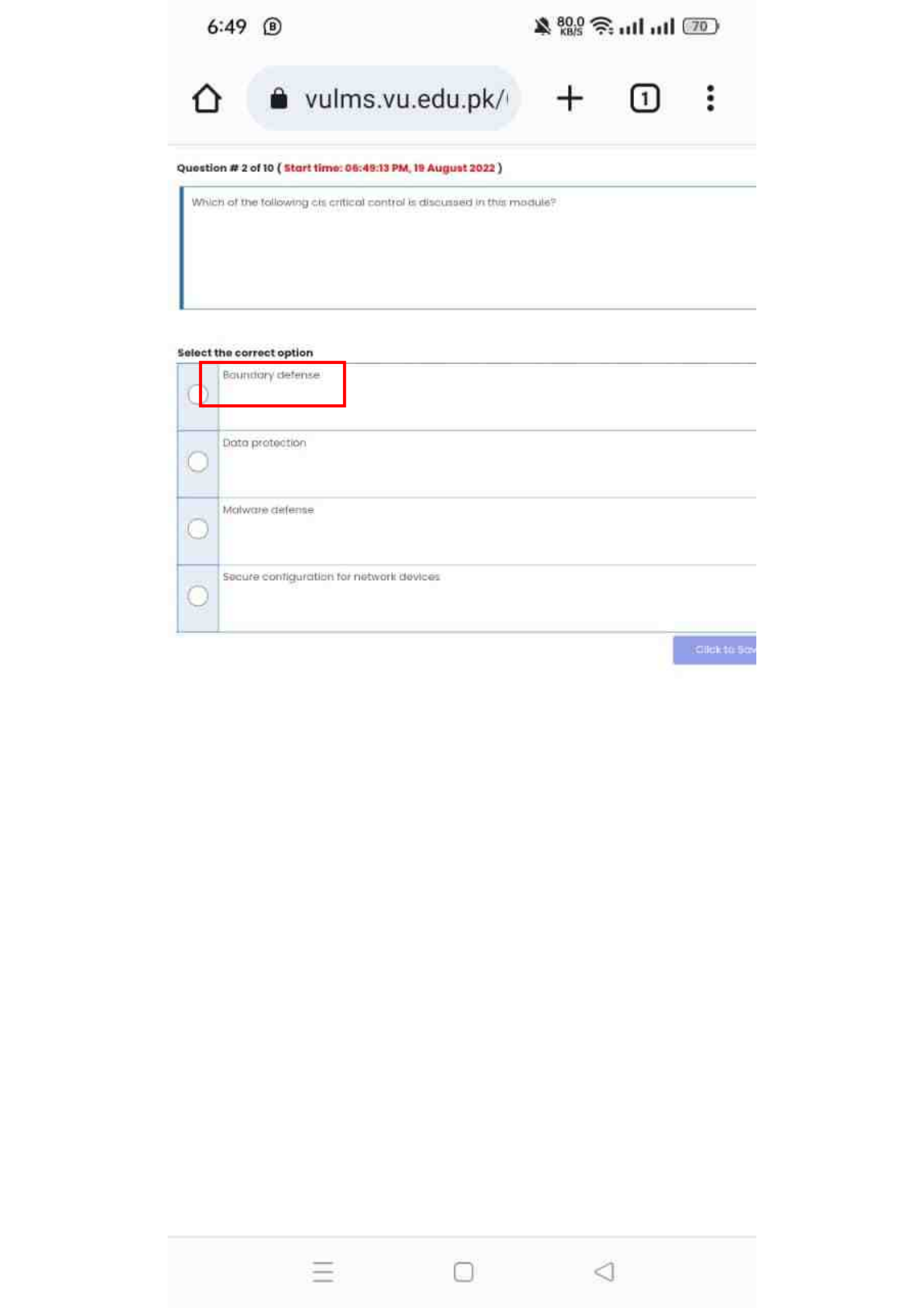
Which of the following can be used to look for unusual attack mechanisms on organization's network boundaries?

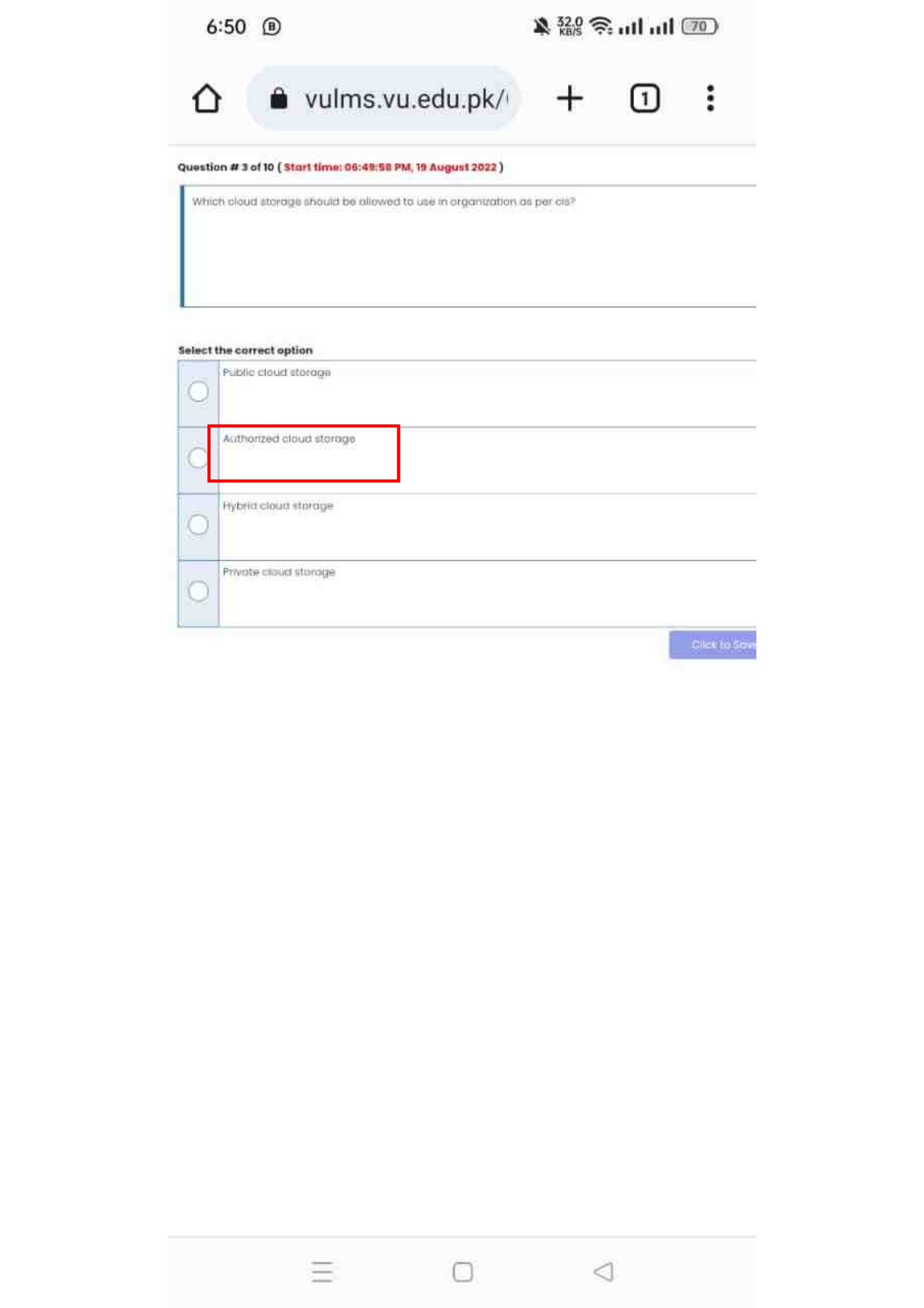
Select the correct option

- Network-based intrusion prevention (ips) system
- Host-based intrusion detection (ids) sensors
- Host-based intrusion prevention (ips) system
- Network-based intrusion detection (ids) sensors

Click to Save Answer & Move to Next Question


6:48
vulms.vu.edu.pk/
CS205 - Information Security (Quiz No.3)
Quiz Start Time
Question # 1 of 10 (Start time: 06:48:35 PM, 19 August 2022)
If multi-factor authentication is not supported then user accounts shall be required to?
Select the correct option
Use default passwords
Use short passwords which are easy to remember
Use same password on all the systems
Use passwords longer than 14 characters


6:49
vulms.vu.edu.pk/
Question # 2 of 10 (Start time: 06:49:13 PM, 19 August 2022)
Which of the following cis critical control is discussed in this module?
Select the correct option
Boundary defense
Data protection
Malware defense
Secure configuration for network devices


6:50
vulms.vu.edu.pk/
Question # 3 of 10 (Start time: 06:49:58 PM, 19 August 2022)
Which cloud storage should be allowed to use in organization as per cis?
Select the correct option
Public cloud storage
Authorized cloud storage
Hybrid cloud storage
Private cloud storage

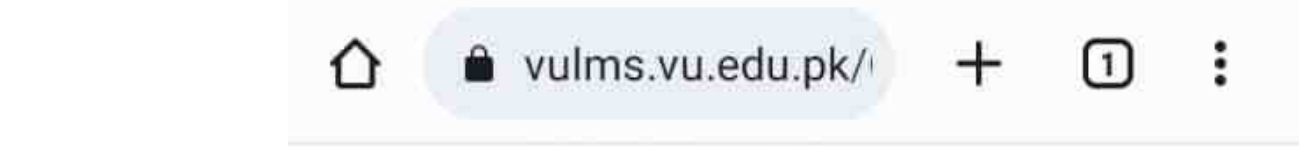
Question # 2 of 10 (Start time: 06:48:48 PM, 10 August 2022)

As per cis critical security framework what is recommended for network boundaries of an organization?

Select the correct option

- Deny communication with all open ports
- Deny communication over unauthorized TCP ports
- Deny communication over unauthorized UDP ports
- Deny communication over unauthorized TCP or UDP ports

Click to Save Answer & Move to



Question # 4 of 10 (Start time: 06:51:05 PM, 19 August 2022)

Which of the following can be used to block malicious traffic on organization's network boundaries?

Select the correct option

- Network-based intrusion prevention (ips) system
- Host-based intrusion prevention (ips) system
- Network-based intrusion detection (ids) sensors
- Host-based intrusion detection (ids) sensors

Click to Save Answer

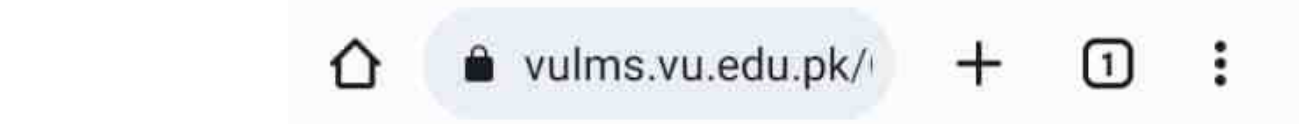
CS205 - Information Security (Quiz No.3)

Question # 5 of 10 (Start time: 06:52:27 PM, 19 August 2022)

In which mode should vulnerability scanning be performed?

Select the correct option

- Authenticated mode
- Deep scan mode
- Dedicated mode
- Un-authenticated mode

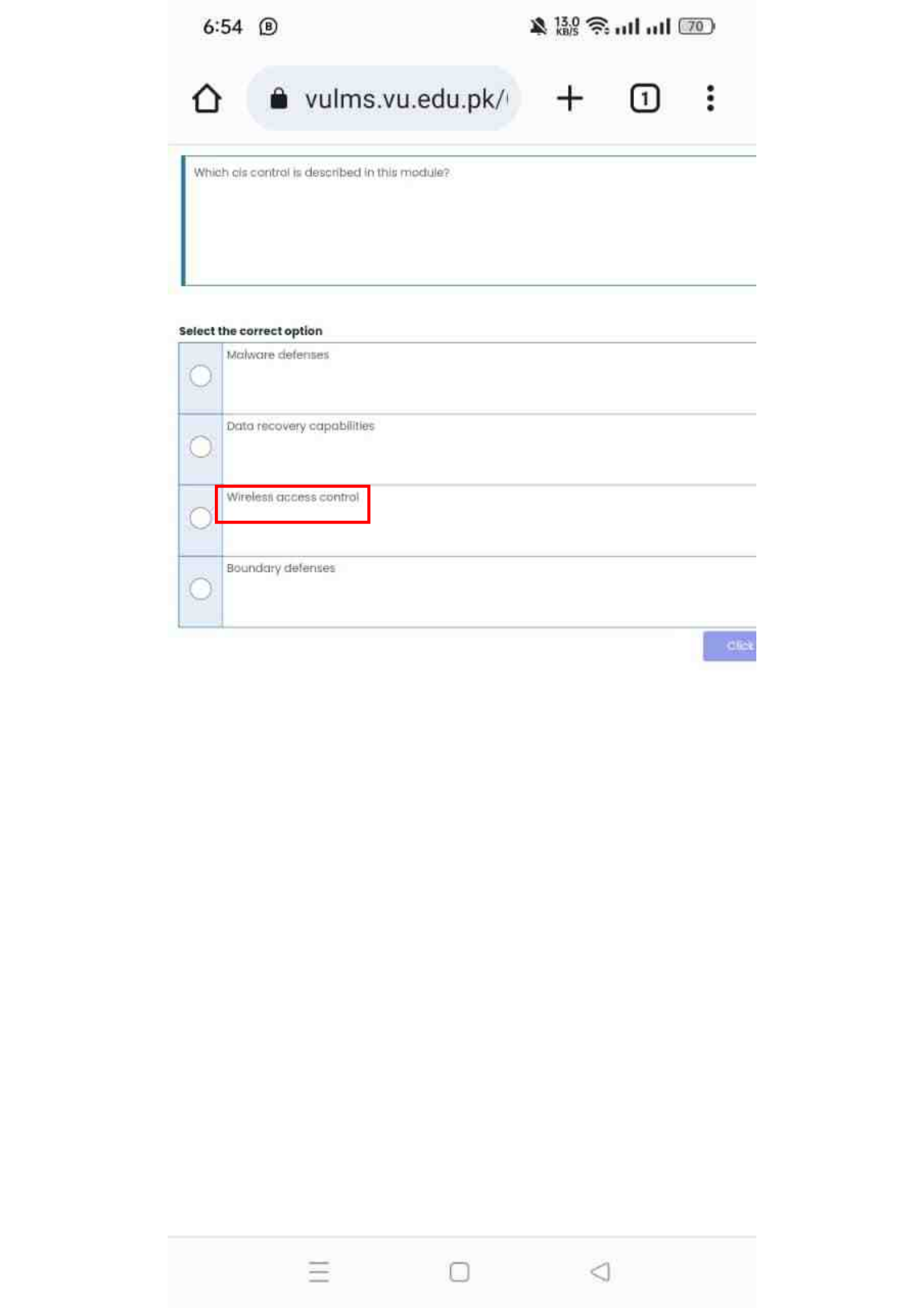


As per cis which authentication protocols should be used by wireless networks?

Select the correct option

- Which require smart cards for authentication
- Which require mutual multi-factor authentication
- Which require bio-metrics for authentication
- Which require digital certificates for authentication

Click to


6:54
vulms.vu.edu.pk/
Which cis control is described in this module?
Select the correct option
Malware defenses
Data recovery capabilities
Wireless access control
Boundary defenses

Which policy is recommended by data protection control of cis for mobile devices usage in an organization?

Select the correct option

- Hard drive of mobile devices should be encrypted
- Mobile devices should not be allowed
- Employees should use only personal mobile devices
- Mobile devices are allowed for higher management only

Click to Save An

CS205 - Information Security (Quiz No.3) Quiz S

Question # 7 of 10 (Start time: 06:55:04 PM, 19 August 2022)

From which type of systems URL requests should be logged in order to identify potentially malicious activity?

Select the correct option

- Mobile devices
- On-site devices
- Each of the organization's system
- Off-site devices

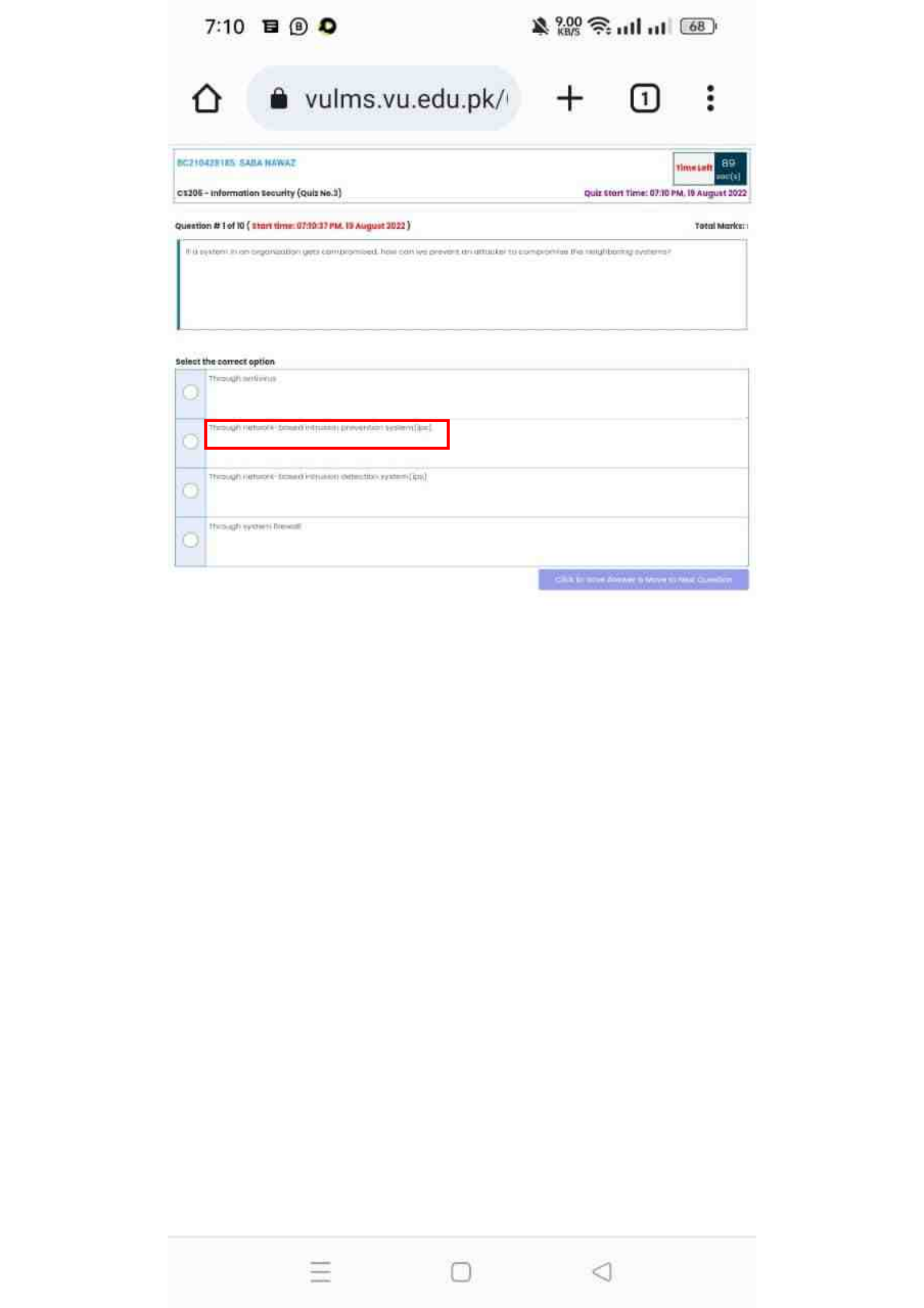
Click to Save

What should standard secure configuration images represent?

Select the correct option

- Default configuration version of OS only
- Hardened versions of OS only
- Hardened versions of underlying OS and application installed on system
- Hardened versions of application installed on system only

Click to S


7:10
9.00 KB/S
68
vulms.vu.edu.pk/
BC210423185 SABA NAWAZ
Time Left 89 sec(s)
CS205 - Information Security (Quiz No.3)
Quiz Start Time: 07:10 PM, 19 August 2022
Question # 1 of 10 (Start time: 07:10:37 PM, 19 August 2022)
Total Marks: 1
If a system in an organization gets compromised, how can we prevent an attacker to compromise the neighboring systems?
Select the correct option
Through antivirus
Through network- based intrusion prevention system.[ips]
Through network- based intrusion detection system.[ips]
Through system firewall
Click to save Answer & Move to Next Question

Question # 7 of 10 (Start time: 07:14:22 PM, 19 August 2022)

Automated configuration monitoring tools should compliant with which protocol to streamline reporting?

Select the correct option

- Scap
- Cis
- Fisma
- Disa

Click to Save

CS205 – Information Security (Quiz No.3)

Question # 8 of 10 (Start time: 07:14:58 PM, 19 August 2022)

why security engineering is placed at layer 3 of transformation model?

Select the correct option

- Requires very less time and effort
- Consists of complicated security activities which take more time and effort
- Its not very beneficial to implement so kept at the later stage
- Because it's a low hanging fruit

Question # 9 of 10 (Start time: 07:15:40 PM, 19 August 2022)

As per cis which authentication protocols should be used by wireless networks?

Select the correct option

- ○ Which require bio-metrics for authentication
- ○ Which require mutual multi-factor authentication
- ○ Which require digital certificates for authentication
- ○ Which require smart cards for authentication

BC210424756: PALWASHA ALTAF

Time Left 87 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:23 PM, 19 August 2022

Question # 2 of 10 (Start time: 02:25:34 PM, 19 August 2022)

Total Marks: 1

What should an organization do to control access to sensitive information on need-to-know basis?

Select the correct option

- Locate all sensitive information on separate vlans
- Store sensitive information on multiple servers
- Store all sensitive information on single server
- Locate all sensitive information on single vlans

Click to Save Answer & Move to Next Question

BC210424756: PALWASHA ALTAF

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:23 PM, 19 August 2022

Question # 3 of 10 (Start time: 02:27:16 PM, 19 August 2022)

Total Marks: 1

If multi-factor authentication is not supported then user accounts shall be required to?

Select the correct option

- Use short passwords which are easy to remember
- Use default passwords
- Use same password on all the systems
- Use passwords longer than 14 characters

Click to Save Answer & Move to Next Question

BC210424756: PALWASHA ALTAF

Time Left 89 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:23 PM, 19 August 2022

Question # 4 of 10 (Start time: 02:28:24 PM, 19 August 2022)

Total Marks: 1

As per cis framework what is the best practice to store logs generated from system?

Select the correct option

- Store logs on a machine other than which generates
- Store logs on the same machine which generates
- Aggregate logs to a central management system
- Store logs on different dispersed locations

Click to Save Answer & Move to Next Question

BC210424756: PALWASHA ALTAF

Time Left 89 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:23 PM, 19 August 2022

Question # 5 of 10 (Start time: 02:30:00 PM, 19 August 2022)

Total Marks: 1

Before deploying any new devices in a networked environment what should be done with passwords?

Select the correct option

- Create very small passwords
- Keep the default passwords
- Change the default passwords
- Remove the passwords

Click to Save Answer & Move to Next Question

BC210424756: PALWASHA ALTAF

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:23 PM, 19 August 2022

Question # 6 of 10 (Start time: 02:31:08 PM, 19 August 2022)

Total Marks: 1

Wireless access control comes under which category of cis top 20 controls?

Select the correct option

- Foundational
- Advanced
- Organizational
- Basic

Click to Save Answer & Move to Next Question

BC210424756: PALWASHA ALTAF

Time Left 89 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:23 PM, 19 August 2022

Question # 7 of 10 (Start time: 02:32:36 PM, 19 August 2022)

Total Marks: 1

why security engineering is placed at layer 3 of transformation model?

Select the correct option

- Consists of complicated security activities which take more time and effort
- Requires very less time and effort
- Because it's a low hanging fruit
- Its not very beneficial to implement so kept at the later stage

Click to Save Answer & Move to Next Question

BC210424756: PALWASHA ALTAF

Time Left 89 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:23 PM, 19 August 2022

Question # 8 of 10 (Start time: 02:33:41 PM, 19 August 2022)

Total Marks: 1

Which policy is recommended by data protection control of cis for mobile devices usage in an organization?

Select the correct option

- Mobile devices are allowed for higher management only
- Employees should use only personal mobile devices
- Mobile devices should not be allowed
- Hard drive of mobile devices should be encrypted

Click to Save Answer & Move to Next Question

Question # 9 of 10 (Start time: 02:35:07 PM, 19 August 2022) Total Marks: 1

Each person with administrator account should be authorized by?

Select the correct option

- Senior executive
- Help-desk team
- Network administrator
- System administrator

Click to Save Answer & Move to Next Question

Question # 10 of 10 (Start time: 02:36:31 PM, 19 August 2022) **Total Marks:**

Frequency of running automated vulnerability scanner against all systems on a network in an enterprise should be?

Select the correct option

- Weekly
- Fortnightly
- Monthly
- Quarterly

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 1 of 10 (Start time: 02:37:28 PM, 19 August 2022)

Total Marks: 1

As per malware defense control why DNS query logging should be enabled?

Select the correct option

- Continuously monitor and defend organization's servers and workstations
- analyze and block inbound email attachments with malicious behavior
- To lower the chance of spoofed or modified emails from valid email addresses
- To detect host-name lookup for known malicious domains

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 2 of 10 (Start time: 02:38:50 PM, 19 August 2022)

Total Marks: 1

Frequency of running automated vulnerability scanner against all systems on a network in an enterprise should be?

Select the correct option

- Quarterly
- Monthly
- Weekly
- Fortnightly

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 3 of 10 (Start time: 02:39:32 PM, 19 August 2022) **Total Marks:** 1

After getting vulnerability scanning results patches should be applied to?

Select the correct option

- Client machines only
- Network devices only
- Critical servers only
- All the systems throughout the organization

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 89 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 4 of 10 (Start time: 02:40:47 PM, 19 August 2022) **Total Marks:** 1

Which policy is recommended by data protection control of cis for mobile devices usage in an organization?

Select the correct option

- Hard drive of mobile devices should be encrypted
- Employees should use only personal mobile devices
- Mobile devices should not be allowed
- Mobile devices are allowed for higher management only

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 86 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 5 of 10 (Start time: 02:42:01 PM, 19 August 2022) **Total Marks:** 1

Which of the following system configuration management tool is used for Linux systems?

Select the correct option

- Puppet
- Cls cat pro
- Fim
- Active directory

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 6 of 10 (Start time: 02:43:36 PM, 19 August 2022)

Total Marks: 1

Boundary defense controls comes under which category of cis critical controls?

Select the correct option

- Basic controls
- Organizational controls
- Foundational controls
- Advanced controls

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 89 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 7 of 10 (Start time: 02:44:32 PM, 19 August 2022)

Total Marks: 1

When a vulnerability scan is run and report is generated and shared with respective resources, which vulnerabilities they should fix on priority basis?

Select the correct option

- Medium risk vulnerabilities
- High risk vulnerabilities
- Critical risk vulnerabilities
- Low risk vulnerabilities

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 86 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 8 of 10 (Start time: 02:45:35 PM, 19 August 2022)

Total Marks: 1

From which type of systems URL requests should be logged in order to identify potentially malicious activity?

Select the correct option

- On-site devices
- Mobile devices
- Off-site devices
- Each of the organization's system

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 90 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 9 of 10 (Start time: 02:46:42 PM, 19 August 2022)

Total Marks: 1

Which cis control is described in this module?

Select the correct option

- Wireless access control
- Boundary defenses
- Malware defenses
- Data recovery capabilities

Click to Save Answer & Move to Next Question

DC180200074: MUHAMMAD QASIM ALI KHAN TAHIR

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:37 PM, 19 August 2022

Question # 10 of 10 (Start time: 02:48:35 PM, 19 August 2022)

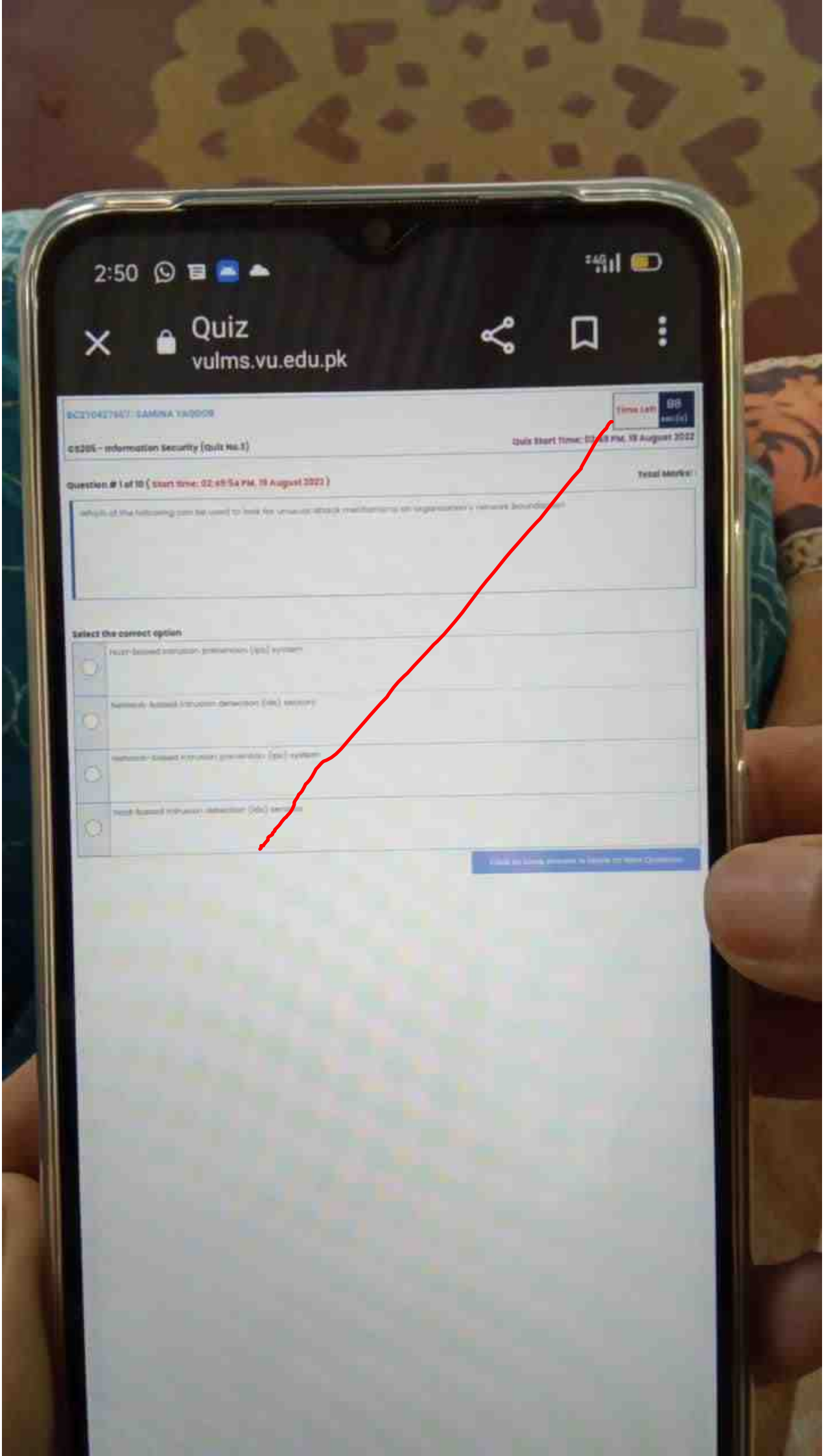
Total Marks: 1

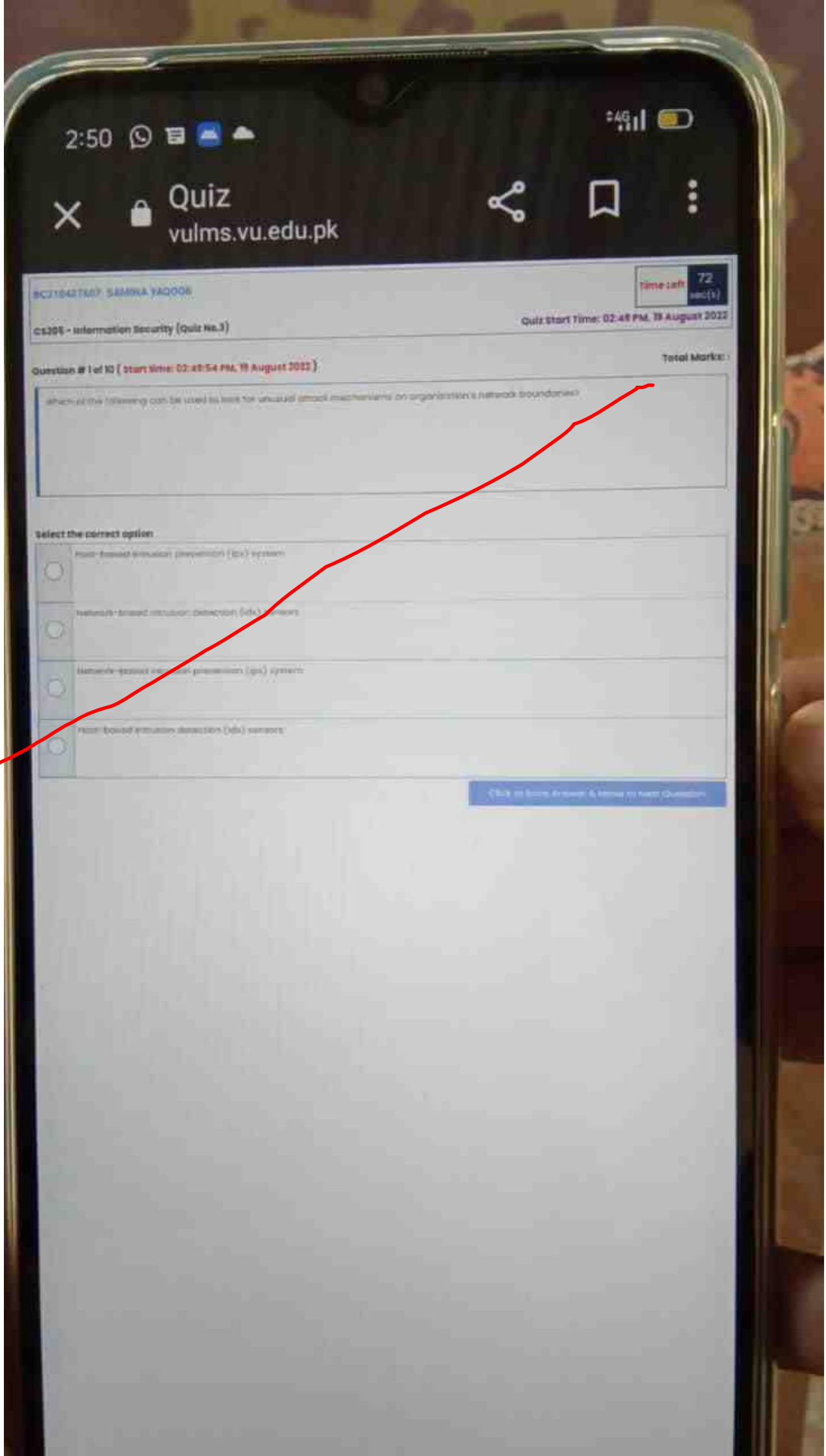
Automated configuration monitoring tools should compliant with which protocol to streamline reporting?

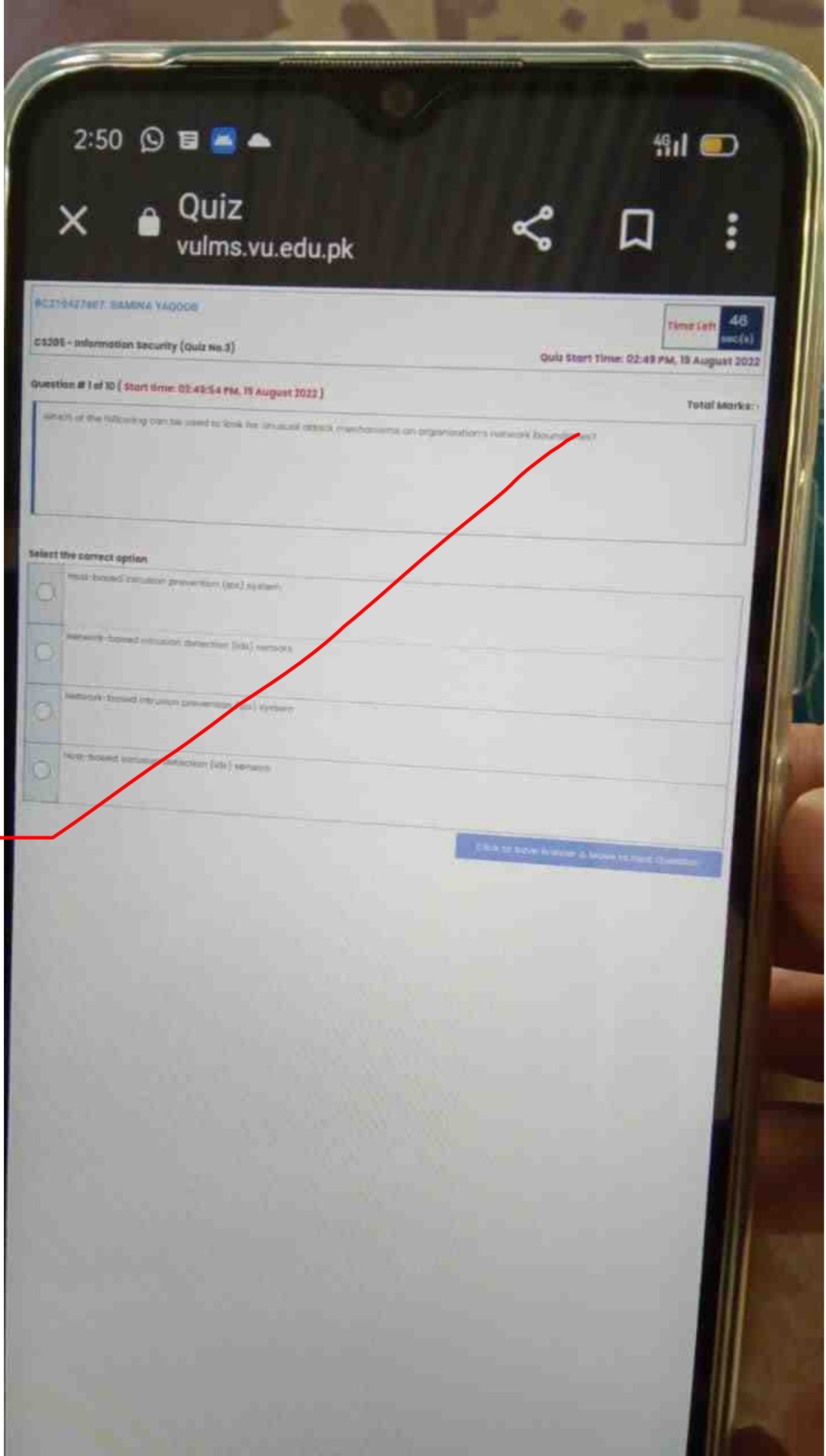
Select the correct option

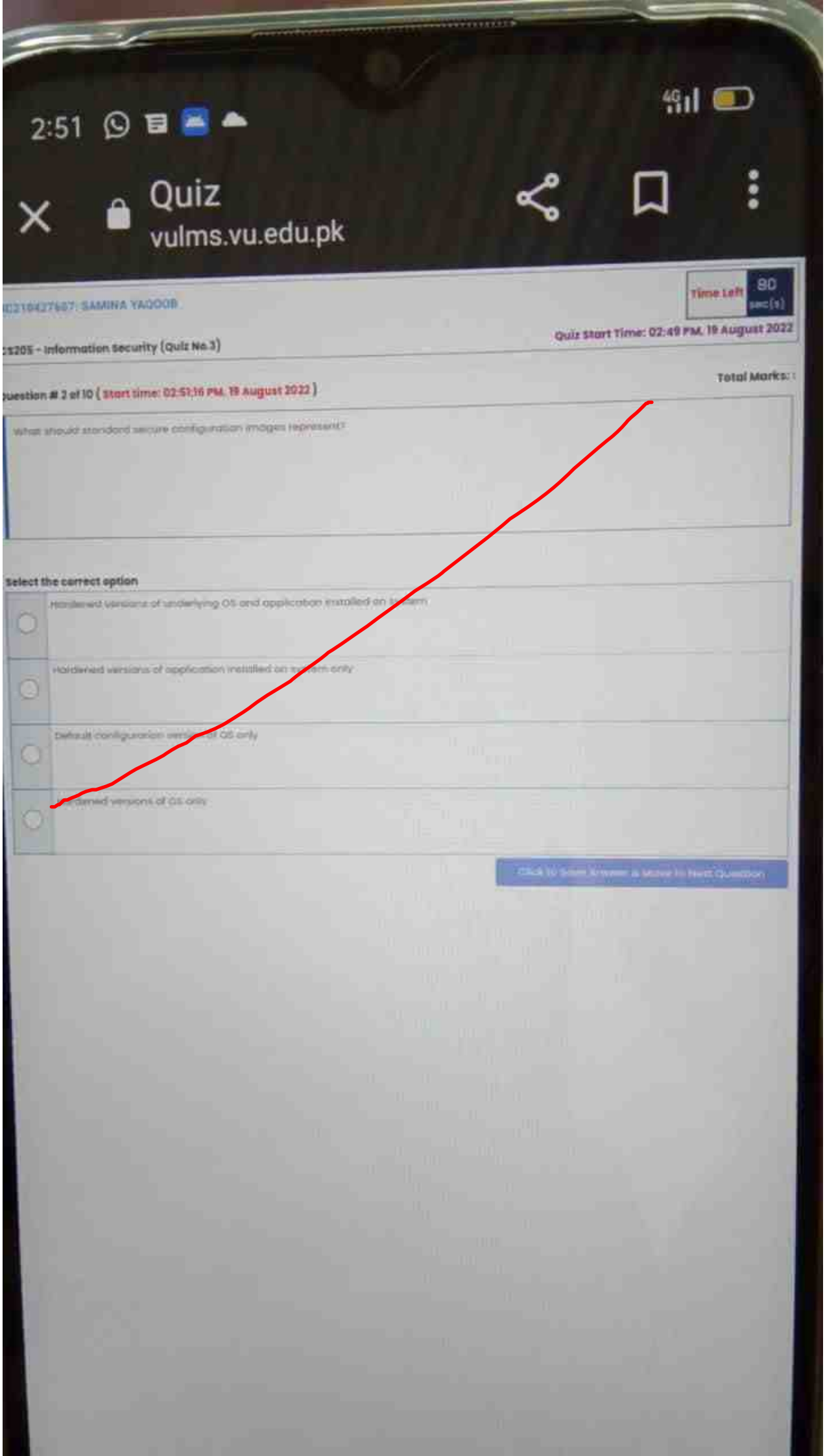
- Disa
- Cis
- Scap
- Fisma

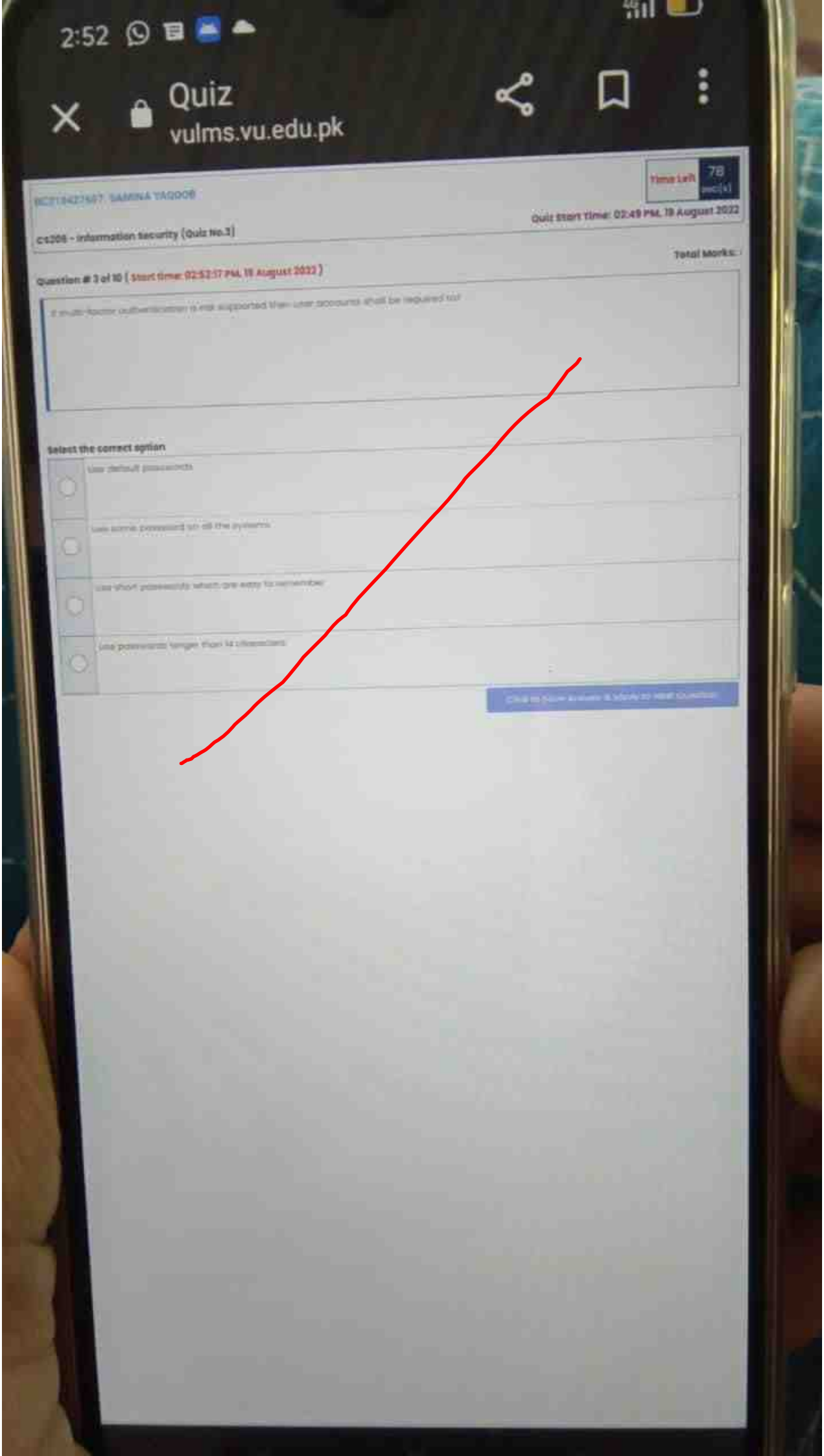
Click to Save Answer & Move to Next Question

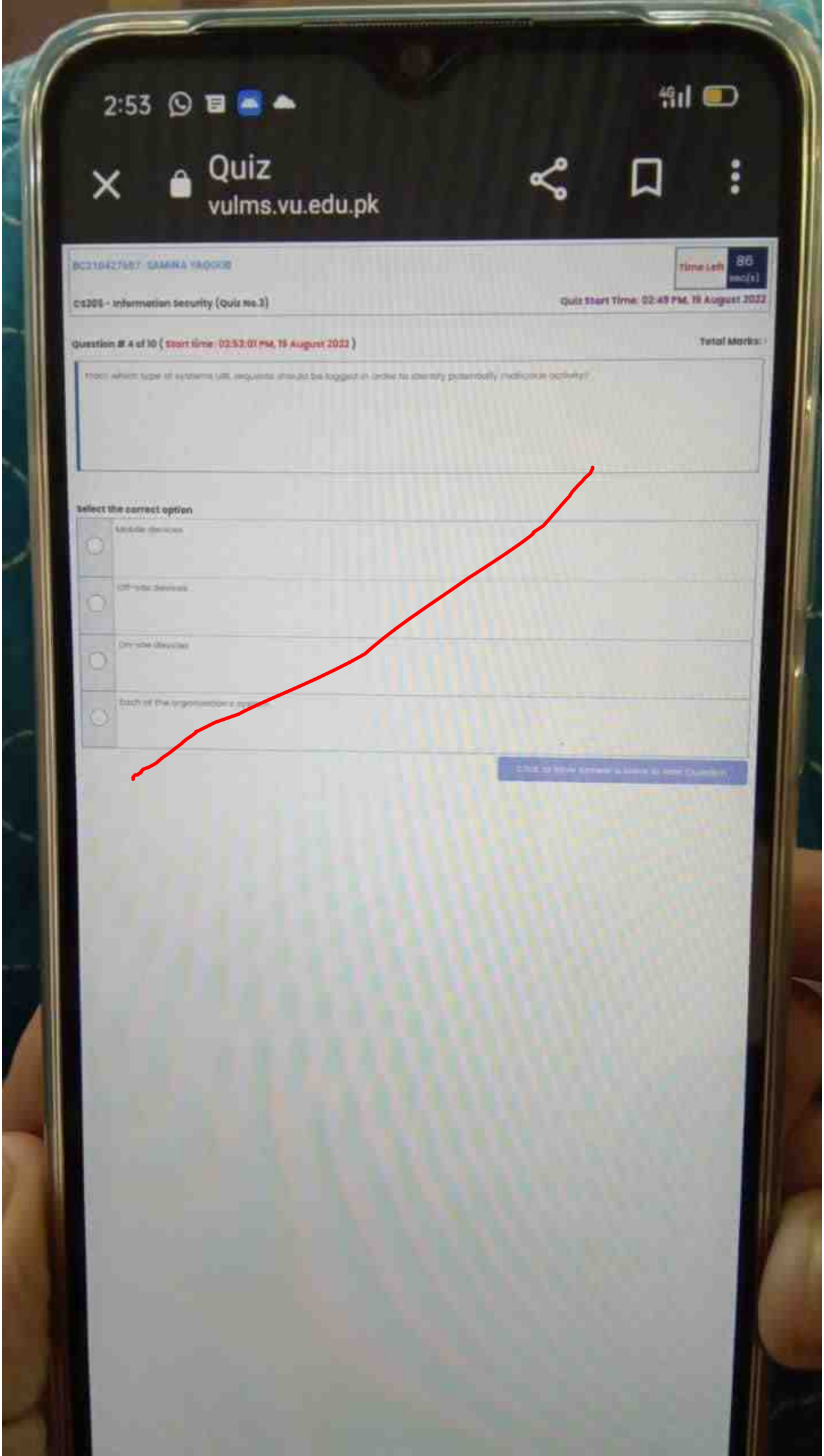

2:50
Quiz
vulms.vu.edu.pk
CS205 - Information Security (Quiz No.5)
Question # 1 of 10 (Start time: 02:49:54 PM, 19 August 2022)
Select the correct option

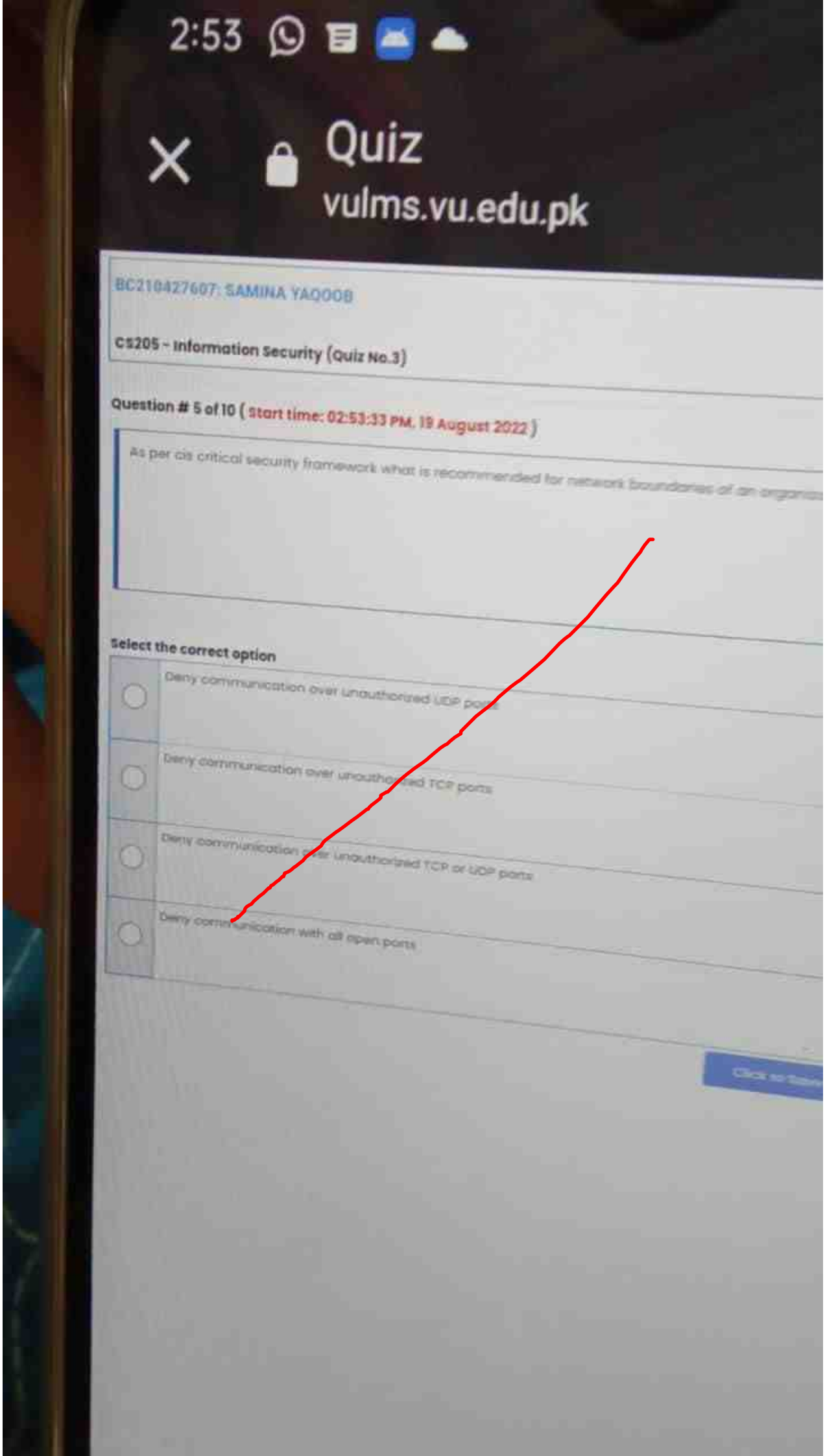

2:50
Quiz
vulms.vu.edu.pk
Time Left
72
sec(s)
CS305 - Information Security (Quiz No.3)
Quiz Start Time: 02:48 PM, 19 August 2022
Question # 1 of 10 (Start time: 02:49:54 PM, 19 August 2022)
Total Marks:
Select the correct option:

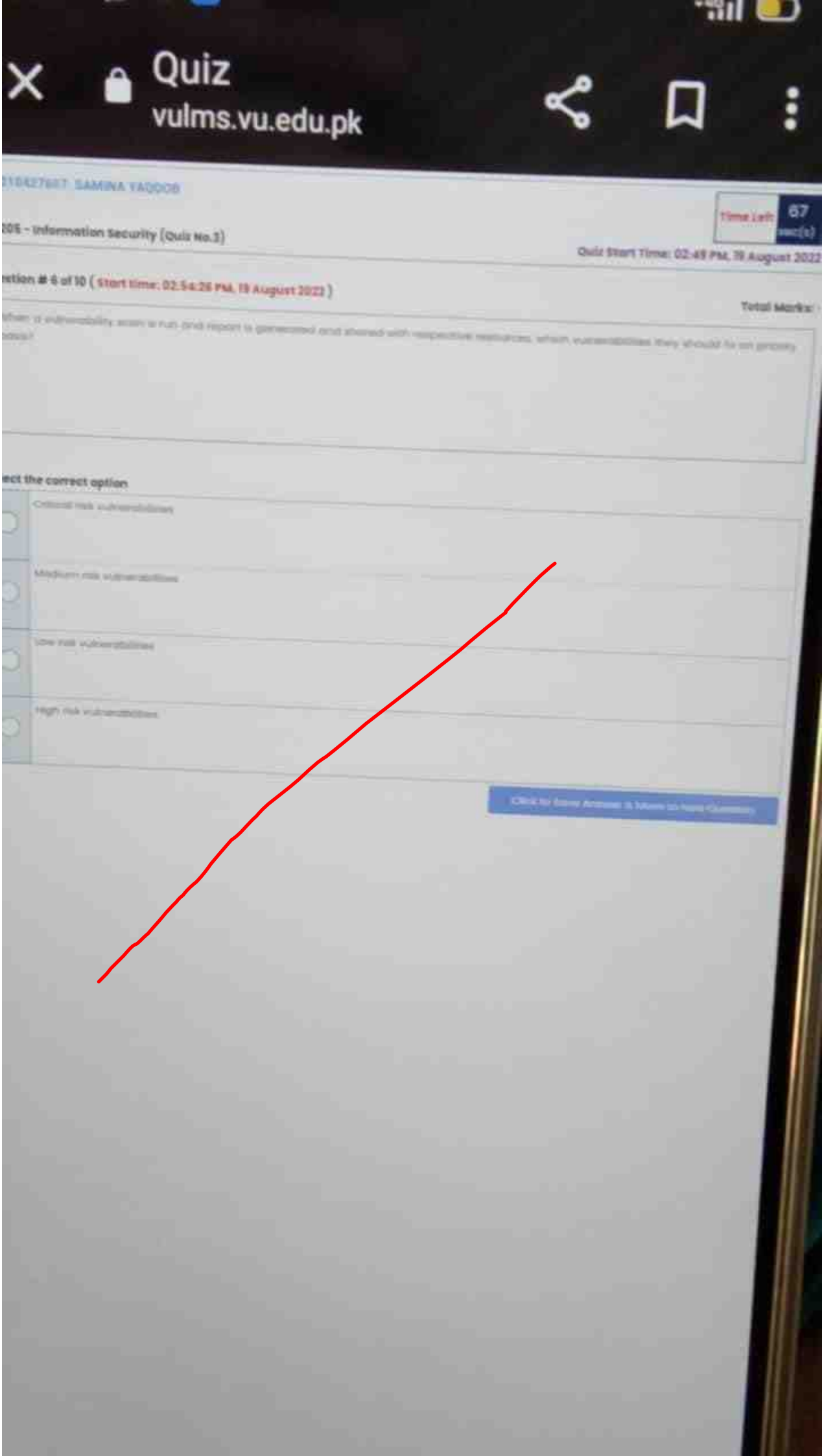

2:50
Quiz
vulms.vu.edu.pk
CS205 - Information Security (Quiz No.3)
Time Left
48
sec(s)
Quiz Start Time: 02:49 PM, 15 August 2022
Question # 1 of 10 (Start time: 02:49:54 PM, 15 August 2022)
Total Marks:
Select the correct option

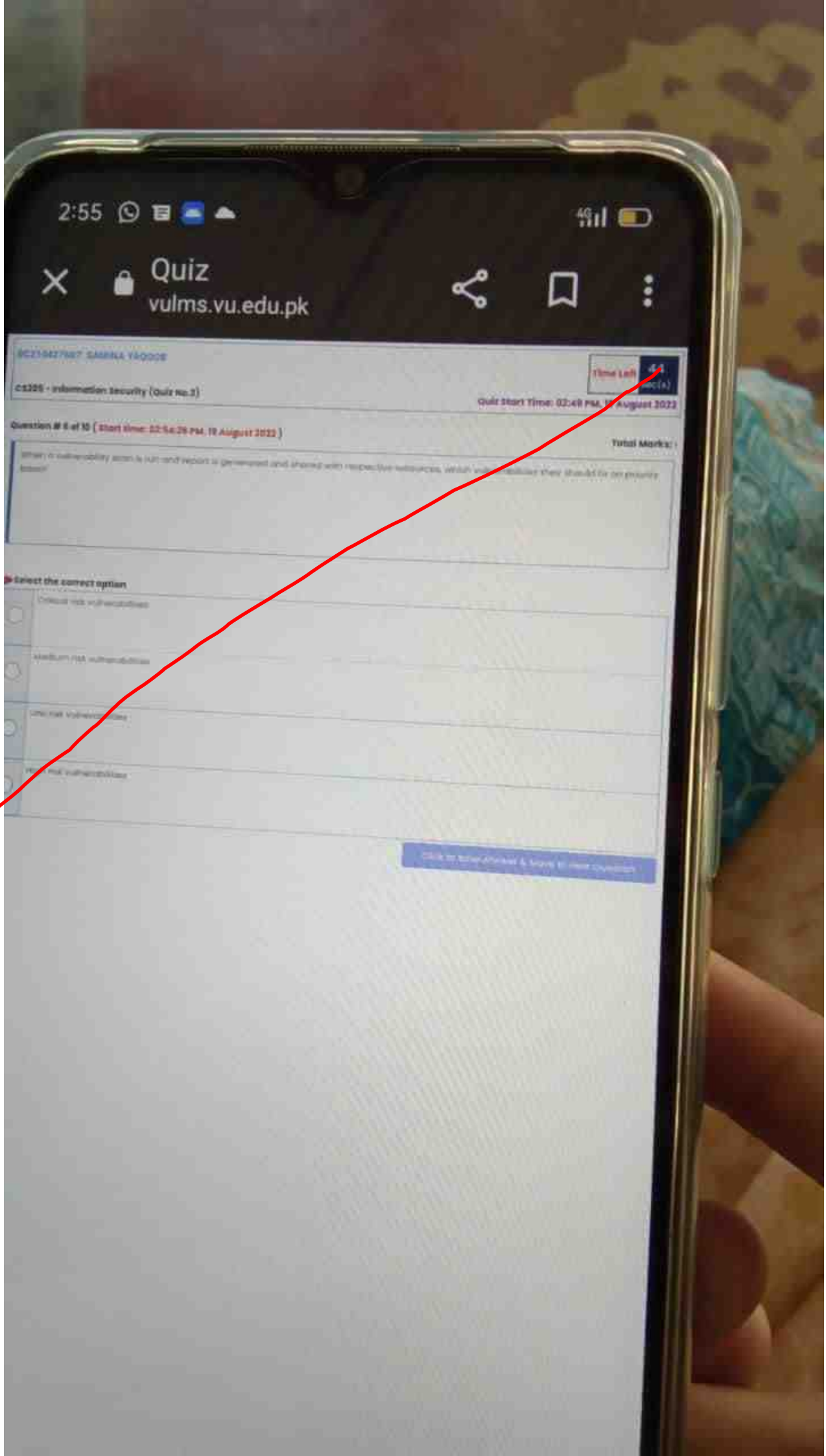

2:51
Quiz
vulms.vu.edu.pk
Time Left
80
sec(s)
Quiz Start Time: 02:49 PM, 19 August 2022
Total Marks:
Question # 2 of 10 (Start time: 02:51:16 PM, 19 August 2022)
What should standard secure configuration images represent?
Select the correct option
Hardened versions of underlying OS and application installed on system
Hardened versions of application installed on system only
Default configuration versions of OS only
Hardened versions of OS only

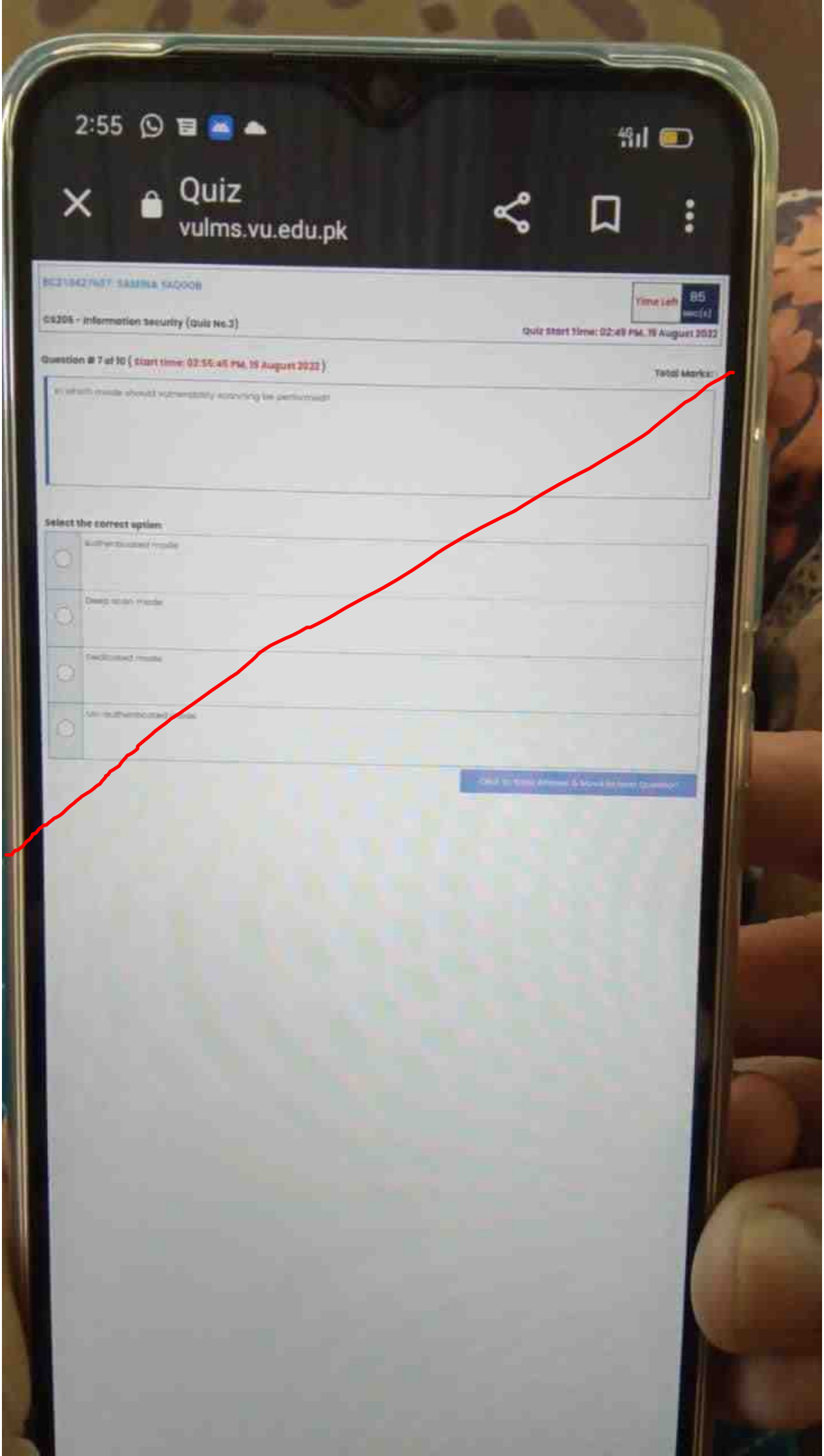

2:52
Quiz
vulms.vu.edu.pk
Time Left
78
sec(s)
Quiz start time: 02:49 PM, 19 August 2022
CS205 - Information Security (Quiz No.3)
Total Marks:
Question # 3 of 10 (Start time: 02:52:17 PM, 19 August 2022)
Select the correct option

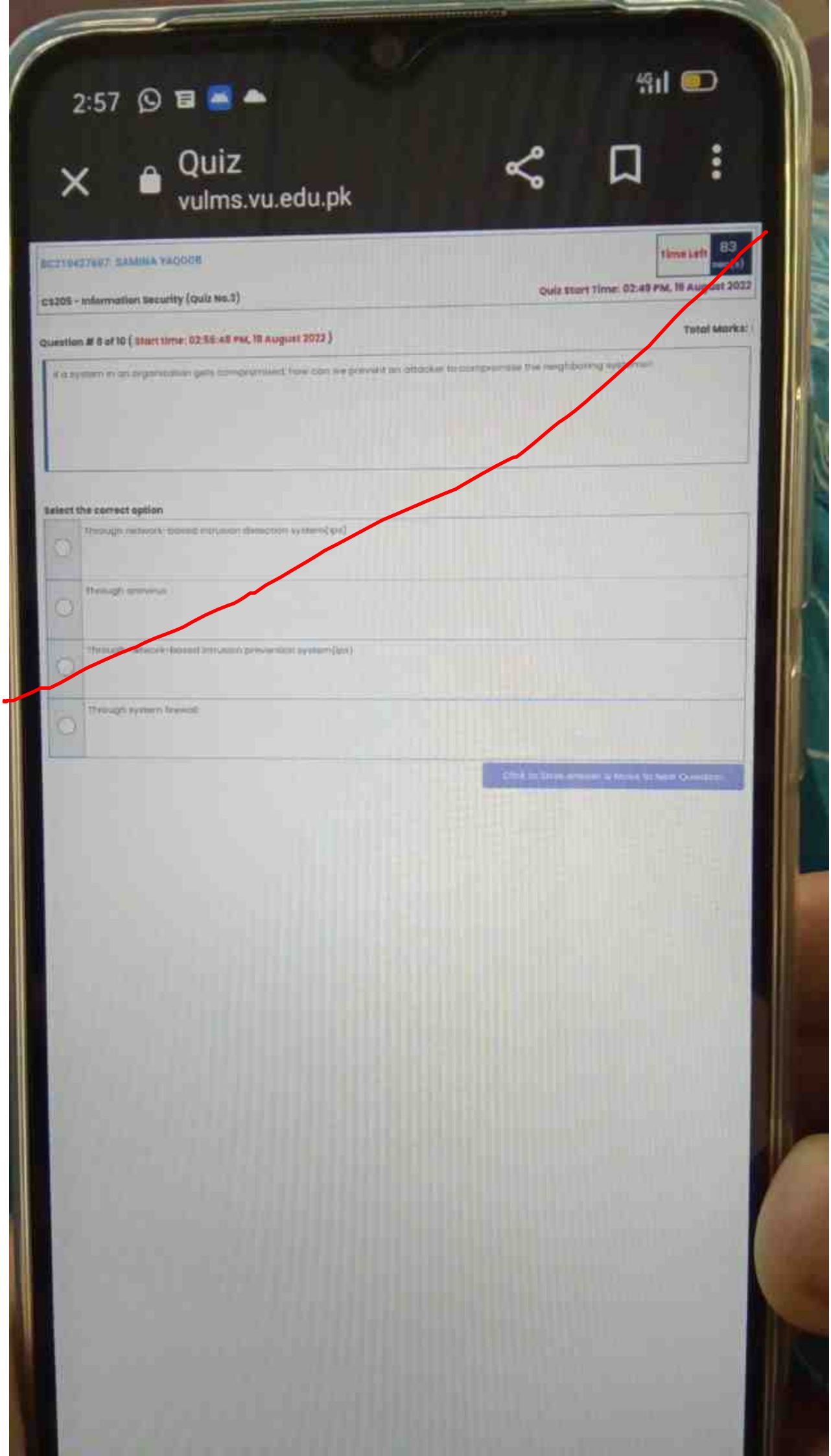

2:53
Quiz
vulms.vu.edu.pk
Time Left
86
sec(s)
CS205 - Information Security (Quiz no.3)
Quiz Start Time: 02:49 PM, 15 August 2022
Question # 4 of 10 (Start time: 02:53:01 PM, 15 August 2022)
Total Marks:
Select the correct option

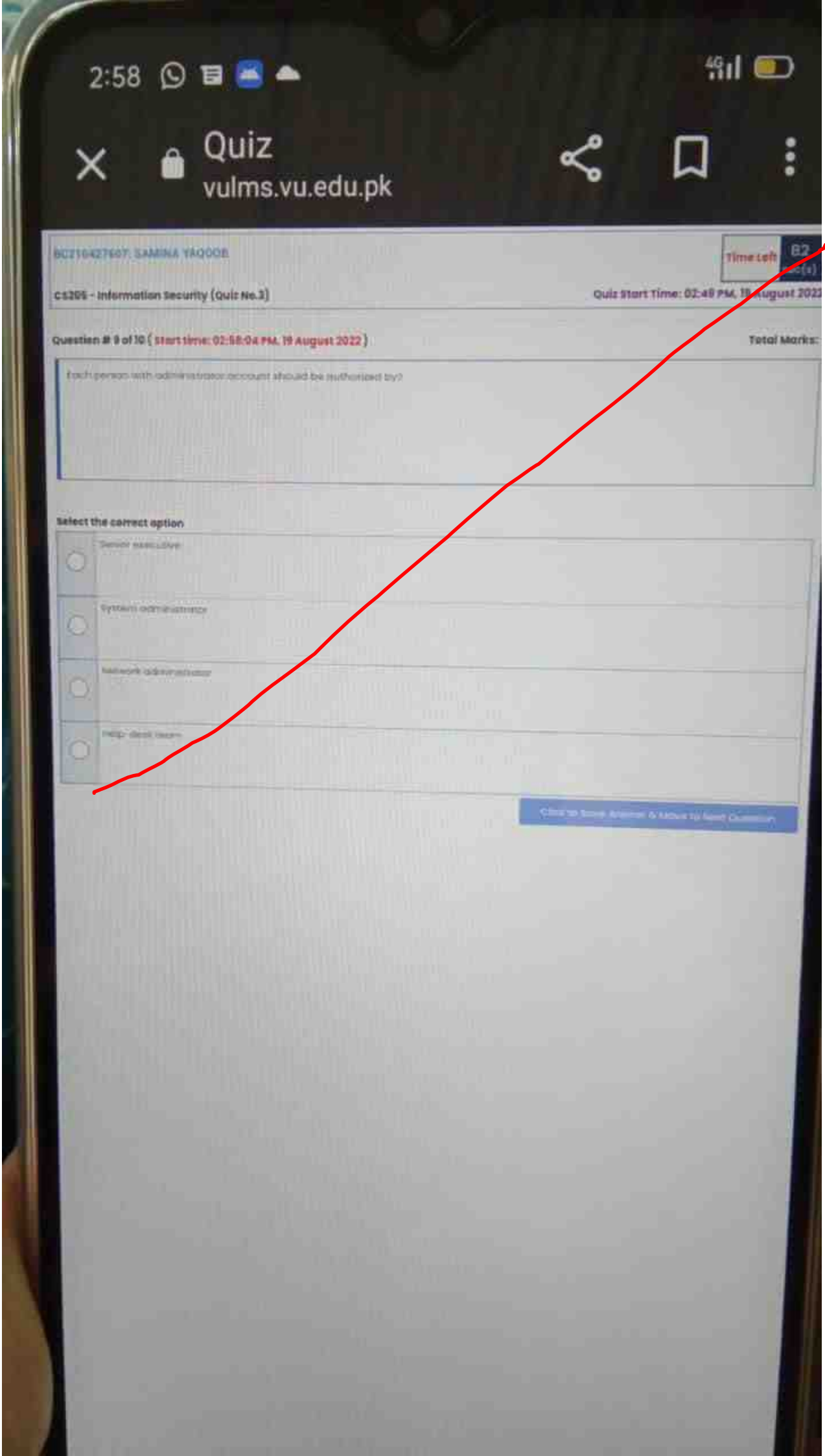

2:53
Quiz
vulms.vu.edu.pk
BC210427607: SAMINA YAQOOB
CS205 - Information Security (Quiz No.3)
Question # 5 of 10 (Start time: 02:53:33 PM, 19 August 2022)
As per cis critical security framework what is recommended for network boundaries of an organi
Select the correct option
Deny communication over unauthorized UDP ports
Deny communication over unauthorized TCP ports
Deny communication over unauthorized TCP or UDP ports
Deny communication with all open ports

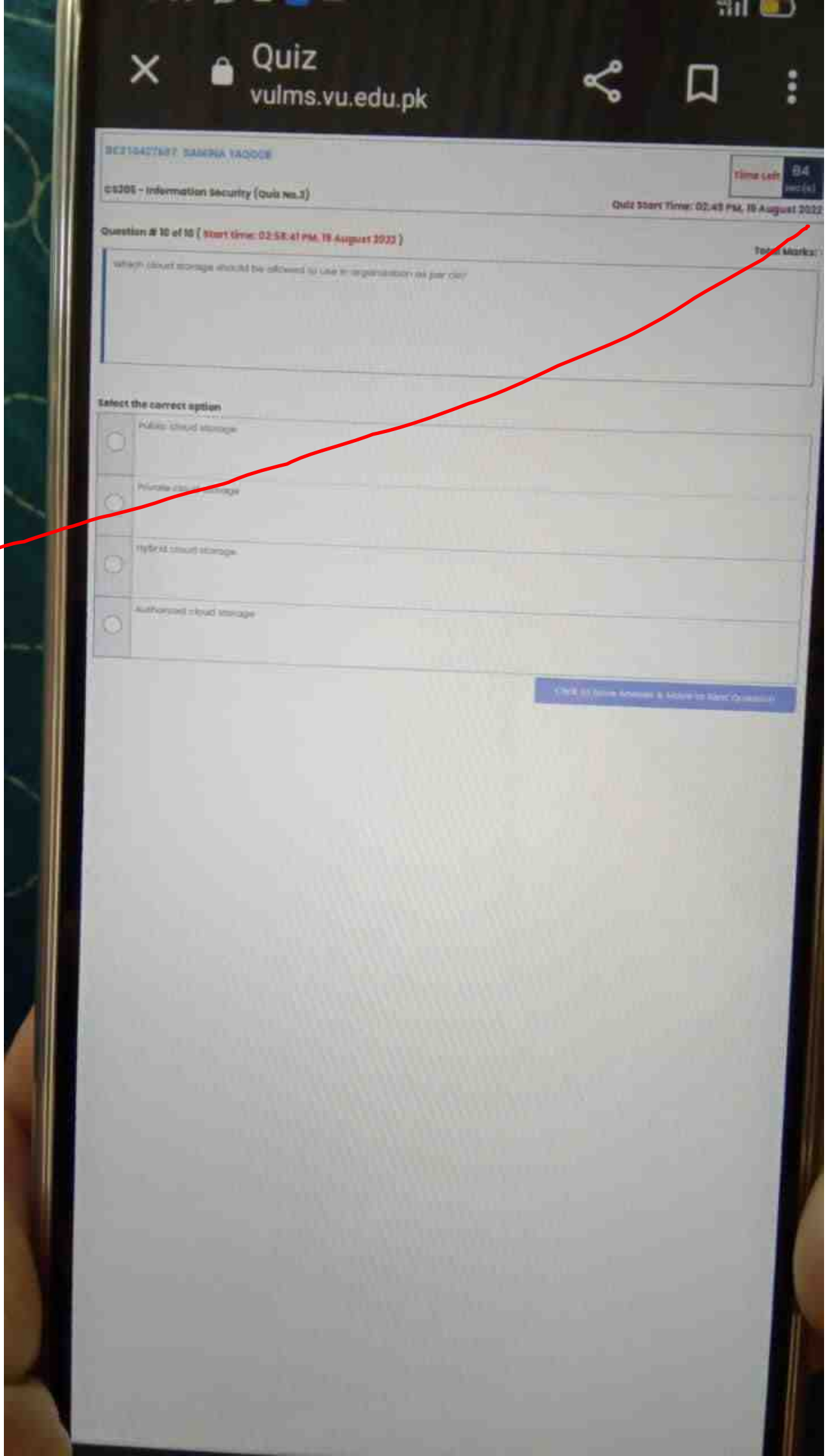

Quiz
vulms.vu.edu.pk
Time Left
67
sec(s)
Quiz Start Time: 02:49 PM, 19 August 2022
Total Marks:
ect the correct option


2:55
Quiz
vulms.vu.edu.pk


2:55
Quiz
vulms.vu.edu.pk
CS205 - Information Security (Quiz No.3)
Time Left
85
sec(s)
Quiz Start Time: 02:49 PM, 15 August 2022
Question # 7 of 10 (Start time: 02:55:45 PM, 15 August 2022)
Total Marks:
Select the correct option:


2:57
Quiz
vulms.vu.edu.pk
Time Left
CS205 - Information Security (Quiz No.3)
Question # 8 of 10 (Start time: 02:56:48 PM, 18 August 2022)
Total Marks:
Select the correct option
Through network based intrusion detection system(ids)
Through antivirus
Through network based intrusion prevention system(ips)
Through system firewall


2:58
Quiz
vulms.vu.edu.pk
BC210427607, SAMINA YAQOOB
Time Left
CS205 - Information Security (Quiz No.3)
Quiz Start Time: 02:48 PM, 19 August 2022
Question # 9 of 10 (Start time: 02:58:04 PM, 19 August 2022)
Total Marks:
Each person with administrator account should be authorized by?
Select the correct option
Server executive
System administrator
Network administrator
Help desk team


Quiz
vulms.vu.edu.pk
CS305 - Information Security (Quiz No.3)
Question # 10 of 10 (Start time: 02:58:47 PM, 19 August 2022)
Which cloud storage should be allowed to use in organization as per csp?
Select the correct option
Public cloud storage
Private cloud storage
Hybrid cloud storage
Authorized cloud storage

Question # 1 of 10 (Start time: 03:03:21 PM, 19 August 2022) **Total**

Why should we use soap validated vulnerability scanner?

Select the correct option

- Because it looks for both code-based and configuration-based vulnerabilities
- Because of in-depth scanning feature
- Because it looks for code-based vulnerabilities
- Because of excellent reporting feature

Click to Save Answer & Move to Next Que

Which of the following tools can be used to enforce access controls to data?

Select the correct option

- Network-based intrusion detection system
- Host-based data loss prevention (dlp)
- File integrity monitoring solution
- Security information and event management system

Click to Save Answer & Move to Ne

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 03:03 PM, 19 August 2

Question # 3 of 10 (Start time: 03:05:06 PM, 19 August 2022)

Total Ma

Why cis recommends to configure monitoring system in an organization's network?

Select the correct option

- To block data loss through organization's network boundaries
- To record the network packets passing through the boundary
- To block malicious traffic at organization's network boundaries
- To detect compromise at systems at organization's network boundaries

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3) Quiz Start Time: 03:03 PM, 19 Augu

Question # 4 of 10 (Start time: 03:06:04 PM, 19 August 2022) Total

If a system in an organization gets compromised, how can we prevent an attacker to compromise the neighboring systems?

Select the correct option

- Through network-based intrusion detection system(ips)
- Through system firewall
- Through network-based intrusion prevention system(ips)
- Through antivirus

Click to Save Answer & Move to Next Ques

CS205 - Information Security (Quiz No.3) Quiz Start Time: 03:03

Question # 5 of 10 (Start time: 03:06:29 PM, 19 August 2022)

Centrally managed anti-malware software should be used in an organization to

Select the correct option

- Continuously monitor and defend organization's servers
- Continuously monitor and defend organization's workstations
- Continuously monitor and defend organization's servers and workstations
- Continuously monitor and defend organization's edge routers

Click to Save Answer & Move t

Time Left sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 03:03 PM, 19 August 2022

Question # 6 of 10 (Start time: 03:07:30 PM, 19 August 2022)

Total Marks:

As per malware defense control why DNS query logging should be enabled?

Select the correct option

- Continuously monitor and defend organization's servers and workstations
- To detect host-name lookup for known malicious domains
- analyze and block inbound email attachments with malicious behavior
- To lower the chance of spoofed or modified emails from valid email addresses

Click to Save Answer & Move to Next Question

Question # 7 of 10 (start time: 03:08:17 PM, 19 August 2022) Tota

In an enterprise which softwares should be allowed to install and execute?

Select the correct option

- Only paid software
- Softwares included in whitelist
- Softwares displayed on notice board
- Any freely available software

Click to Save Answer & Move to Next Que

BC210427079: MAHNOOR WAQAR

Time Left 87 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 03:03 PM, 19 August 2022

Question # 8 of 10 (Start time: 03:09:00 PM, 19 August 2022)

Total Marks: 1

When a vulnerability scan is run and report is generated and shared with respective resources, which vulnerabilities they should fix on priority basis?

Select the correct option

- Critical risk vulnerabilities
- Low risk vulnerabilities
- Medium risk vulnerabilities
- High risk vulnerabilities

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3) Quiz Start Time: 03:03 PM, 19 August 2

Question # 10 of 10 (Start time: 03:11:08 PM, 19 August 2022) Total Ma

Automated tools should be used to verify and compare the network devices configuration with

Select the correct option

- Latest security configuration released by vendor
- Some 3rd party recommended configuration
- Approved security configuration
- Default security configuration released by vendor

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3)

Question # 9 of 10 (Start time: 03:09:35 PM, 19 August 2022)

What should an organization do to control access to sensitive information on need-to-know basis?

Select the correct option

- Locate all sensitive information on separate vlans
- Store sensitive information on multiple servers
- Locate all sensitive information on single vlans
- Store all sensitive information on single server

Click to

CS205 - Information Security (Quiz No.3) Quiz Start Time: 03:18 PM, 19 August 2022

Question # 1 of 10 (Start time: 03:18:06 PM, 19 August 2022) Total Marks:

As per boundary defense control of cis what should be done with network traffic at proxy?

Select the correct option

- Block all the network traffic
- Allow all the network traffic
- Use blacklist to allow access to sites without decrypting
- Decrypt all encrypted network traffic prior to analyzing the content

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3) Quiz Start Time: 03:18 PM, 19 August 2022

Question # 2 of 10 (Start time: 03:19:42 PM, 19 August 2022) Total Marks:

If multi-factor authentication is not supported then user accounts shall be required to?

Select the correct option

- Use short passwords which are easy to remember
- Use default passwords
- Use same password on all the systems
- Use passwords longer than 14 characters

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 03:18 PM, 19 August 2022

Question # 3 of 10 (Start time: 03:20:28 PM, 19 August 2022)

Total Marks:

As per cis framework what is the best practice to store logs generated from system?

Select the correct option

- Aggregate logs to a central management system
- Store logs on a machine other than which generates
- Store logs on the same machine which generates
- Store logs on different dispersed locations

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 03:18 PM, 19 August 2022

Question # 4 of 10 (Start time: 03:22:06 PM, 19 August 2022)

Total Marks: 1

Which cloud storage should be allowed to use in organization as per cis?

Select the correct option

- Authorized cloud storage
- Private cloud storage
- Hybrid cloud storage
- Public cloud storage

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3) Quiz Start Time: 03:18 PM, 19 August 2022

Question # 5 of 10 (Start time: 03:23:10 PM, 19 August 2022) Total Marks: 1

Which of the following tools can be used to enforce access controls to data?

Select the correct option

- Network-based intrusion detection system
- File integrity monitoring solution
- Security information and event rmanagement system
- Host-based data loss prevention (dlp)

Click to Save Answer & Move to Next Question

BC210426290: SIDRA SAJAD

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 03:18 PM, 19 August 2022

Question # 6 of 10 (Start time: 03:24:00 PM, 19 August 2022)

Total Marks: 1

How can an authorized wireless access point connected to a wired network can be detected?

Select the correct option

- Through network-based intrusion detection system
- Through wireless intrusion detection system
- Through host-based data loss prevention (dlp)
- Through file integrity monitoring solution

Click to Save Answer & Move to Next Question

BC210426290: SIDRA SAJAD

Time Left 90 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 03:18 PM, 19 August 2022

Question # 7 of 10 (Start time: 03:24:51 PM, 19 August 2022)

Total Marks: 1

why security engineering is placed at layer 3 of transformation model?

Select the correct option

- Its not very beneficial to implement so kept at the later stage
- Consists of complicated security activities which take more time and effort
- Because it's a low hanging fruit
- Requires very less time and effort

Click to Save Answer & Move to Next Question

BC210426290: SIDRA SAJAD

Time Left 89 sec(s)

C$205 - Information Security (Quiz No.3)

Quiz Start Time: 03:18 PM, 19 August 2022

Question # 8 of 10 (Start time: 03:25:36 PM, 19 August 2022)

Total Marks: 1

What should a system do whenever an administrator account is added or removed?

Select the correct option

- Should block that account
- Should not allow
- Issue a log entry and alert
- Require super admin rights

Click to Save Answer & Move to Next Question

BC210426290: SIDRA SAJAD

Time Left 90 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 03:18 PM, 19 August 2022

Question # 9 of 10 (Start time: 03:27:04 PM, 19 August 2022)

Total Marks: 1

Frequency of running automated vulnerability scanner against all systems on a network in an enterprise should be?

Select the correct option

- Monthly
- Weekly
- Fortnightly
- Quarterly

Click to Save Answer & Move to Next Question

BC210426290: SIDRA SAJAD

Time Left 89 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 03:18 PM, 19 August 2022

Question # 10 of 10 (Start time: 03:27:39 PM, 19 August 2022)

Total Marks: 1

Wireless access control comes under which category of cis top 20 controls?

Select the correct option

- Advanced
- Foundational
- Basic
- Organizational

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3) **Quiz Star**

Question # 1 of 10 (Start time: 04:10:18 PM, 19 August 2022)

If a system in an organization gets compromised, how can we prevent an attacker to compromise the neighboring systems?

Select the correct option

- Through network-based intrusion detection system(ips)
- Through system firewall
- Through network-based intrusion prevention system(ips)
- Through antivirus

Click to Save An

CS205 - Information Security (Quiz No.3)

Question # 2 of 10 (Start time: 04:11:28 PM, 19 August 2022)

As per cis critical security framework what is recommended for network boundaries of an organization?

Select the correct option

- Deny communication over unauthorized TCP ports
- Deny communication with all open ports
- Deny communication over unauthorized UDP ports
- Deny communication over unauthorized TCP or UDP ports

Clic

Question # 3 of 10 (Start time: 04:12:22 PM, 19 August 2022)

Which of the following cis critical control is discussed in this module?

Select the correct option

- Data protection
- Boundary defense
- Malware defense
- Secure configuration for network devices

BC210428622: RABIA SHAHID

CS205 - Information Security (Quiz No.3)

Question # 4 of 10 (Start time: 04:13:10 PM, 19 August 2022)

If multi-factor authentication is not supported then user accounts shall be required to?

Select the correct option

- ○ Use short passwords which are easy to remember
- ○ Use passwords longer than 14 characters
- ○ Use same password on all the systems
- ○ Use default passwords

Click

CS205 - Information Security (Quiz No.3) Quiz Start

Question # 5 of 10 (Start time: 04:13:42 PM, 19 August 2022)

Automated configuration monitoring tools should compliant with which protocol to streamline reporting?

Select the correct option

- Scap
- Cis
- Disa
- Fisma

Click to Save Ans

CS205 - Information Security (Quiz No.3)

Question # 6 of 10 (Start time: 04:14:26 PM, 19 August 2022)

What should a system do whenever an administrator account is added or removed?

Select the correct option

- Should block that account
- Should not allow
- Issue a log entry and alert
- Require super admin rights

CS205 - Information Security (Quiz No.3)

Question # 7 of 10 (Start time: 04:15:29 PM, 19 August 2022)

What type of machine should network administrators use for administrative tasks?

Select the correct option

- Used for composing documents
- Isolated from organization's primary network
- Have internet access
- Email and browsing facility available

CS205 - Information Security (Quiz No.3)

Question # 8 of 10 (Start time: 04:16:22 PM, 19 August 2022)

What should an organization do to control access to sensitive information on need-to-know basis?

Select the correct option

- Locate all sensitive information on separate vlans
- Store sensitive information on multiple servers
- Store all sensitive information on single server
- Locate all sensitive information on single vlans

Click to

CS205 - Information Security (Quiz No.3)

Question # 9 of 10 (Start time: 04:17:05 PM, 19 August 2022)

Which of the following system configuration management tool is used for Linux systems?

Select the correct option

- Puppet
- Active directory
- Firn
- Cis cat pro

Question # 10 of 10 (Start time: 04:17:58 PM, 19 August 2022)

Which policy is recommended by data protection control of cis for mobile devices usage in an organization?

Select the correct option

- Hard drive of mobile devices should be encrypted
- Mobile devices should not be allowed
- Employees should use only personal mobile devices
- Mobile devices are allowed for higher management only

Click to

uestion # 1 of 10 (Start time: 04:20:07 PM, 19 August 2022) Tot

From which type of systems URL requests should be logged in order to identify potentially malicious activity?

elect the correct option

- Off-site devices
- On-site devices
- Mobile devices
- Each of the organization's system

Click to Save Answer & Move to Next Qu


16:23
Quiz
vulms.vu.edu.pk
CS205 - Information Security (Quiz No.3)
Quiz Start Time: 04:20 PM, 10 August 2
Question # 2 of 10 (Start time: 04:22:20 PM, 10 August 2022)
Total Mar
As per malware defense control why DNS query logging should be enabled?
Select the correct option
to detect host-name lookup for known malicious domains
to lower the chance of spoofed or modified emails from valid email addresses
analyze and block inbound email attachments with malicious behavior
Continuously monitor and defend organization's servers and workstations

uestion # 3 of 10 (Start time: 04:22:59 PM, 19 August 2022) Total Mar

Centrally managed anti-malware software should be used in an organization to.

elect the correct option

- Continuously monitor and defend organization's servers
- Continuously monitor and defend organization's servers and workstations
- Continuously monitor and defend organization's workstations
- Continuously monitor and defend organization's edge routers

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3) Quiz Start Time: 04:20 PM, 19 August 2

Question # 4 of 10 (Start time: 04:24:12 PM, 19 August 2022) Total Mar

Which cis control is described in this module?

Select the correct option

- Boundary defenses
- Malware defenses
- Wireless access control
- Data recovery capabilities

Click to Save Answer & Move to Next Question

uestion # 5 of 10 (Start time: 04:24:46 PM, 19 August 2022) Total Mar

Which policy is recommended by data protection control of cis for mobile devices usage in an organization?

elect the correct option

- Employees should use only personal mobile devices
- Mobile devices should not be allowed
- Hard drive of mobile devices should be encrypted
- Mobile devices are allowed for higher management only

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3) Quiz Start Time: 04:20 PM, 19 August 20

Question # 6 of 10 (Start time: 04:25:21 PM, 19 August 2022) Total Mark

Which of the following can be used to block malicious traffic on organization's network boundaries?

Select the correct option

- Host-based intrusion prevention (ips) system
- Network-based intrusion detection (ids) sensors
- Network-based intrusion prevention (ips) system
- Host-based intrusion detection (ids) sensors

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3) Quiz Start Time: 04:20 PM, 19 August 2

Question # 7 of 10 (Start time: 04:25:58 PM, 19 August 2022) Total Mar

Why should we use scap validated vulnerability scanner?

Select the correct option

- Because it looks for both code-based and configuration-based vulnerabilities
- Because of in-depth scanning feature
- Because it looks for code-based vulnerabilities
- Because of excellent reporting feature

Click to Save Answer & Move to Next Question

Quiz
vulms.vu.edu.pk

Question # 8 of 10 (Start time: 04:26:45 PM, 19 August 2022) Total M

How can an authorized wireless access point connected to a wired network can be detected and alerts can be generated?

Select the correct option

- Through network vulnerability scanning tools
- Through host-based data loss prevention (dlp)
- Through file integrity monitoring solution
- Through network-based intrusion detection system

Click to Save Answer & Move to Next Quest

CS205 - Information Security (Quiz No.3) Quiz Start Time: 04:20 PM, 19 August 202

Question # 9 of 10 (Start time: 04:27:17 PM, 19 August 2022) Total Marks

In an enterprise which softwares should be allowed to install and execute?

Select the correct option

- Softwares displayed on notice board
- Any freely available software
- Only paid software
- Softwares included in whitelist

Click to Save Answer & Move to Next Question

CS205 - Information Security (Quiz No.3) Quiz Start Time: 04:20 PM, 19 August 2

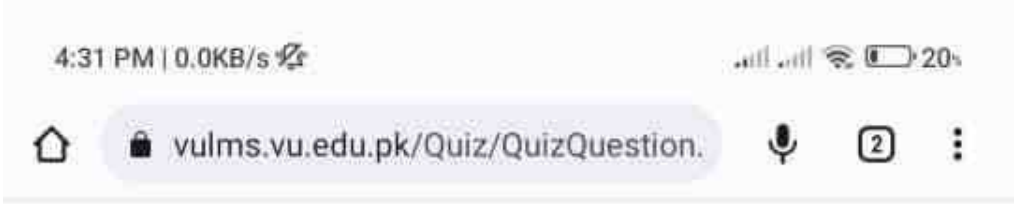
Question # 10 of 10 (Start time: 04:27:44 PM, 19 August 2022) Total Mar

Which of the following system configuration management tool is used for Linux systems?

Select the correct option

- Firn
- Cis cat pro
- Active directory
- Puppet

Click to Save Answer & Move to Next Question



BC200403880: MUBEEN MUSTAFA

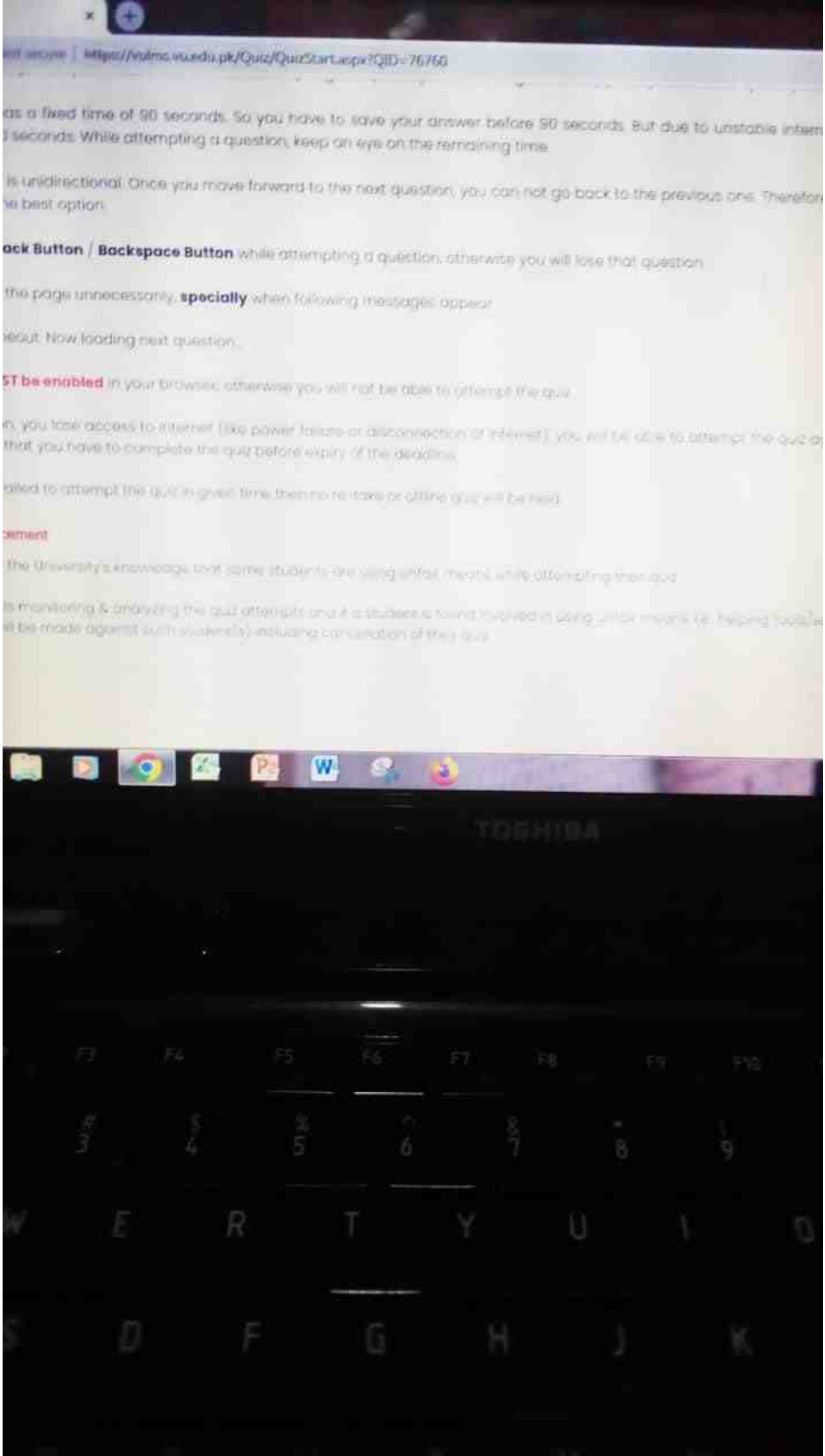
CS205 - Information Security (Quiz No.3)

Question # 10 of 10 (Start time: 04:31:33 PM, 19 August 2022)

Each person with administrator account should be authorized by?

Select the correct option

- Help-desk team
- System administrator
- Network administrator
- Senior executive


https://vulms.vu.edu.pk/Quiz/QuizStart.aspx?QID=76760
as a fixed time of 90 seconds. So you have to save your answer before 90 seconds. But due to unstable intern
seconds. While attempting a question, keep an eye on the remaining time.
is unidirectional. Once you move forward to the next question, you can not go back to the previous one. Therefor
e best option.
ack Button / Backspace Button while attempting a question, otherwise you will lose that question.
the page unnecessarily, specially when following messages appear.
esult: Now loading next question.
ST be enabled in your browser, otherwise you will not be able to attempt the quiz.
n, you lose access to internet (like power failure or disconnection of internet), you will be able to attempt the quiz a
that you have to complete the quiz before expiry of the deadline.
ailed to attempt the quiz in given time then no re-take or offline quiz will be held.
cement
the University's knowledge that some students are using unfair means while attempting their quiz.
is monitoring & analyzing the quiz attempts and if a student is found involved in using unfair means (ie. Helping tools)
t be made against such student(s) including cancellation of the quiz.
TOSHIBA

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 04:44 PM, 19 August 202

Question # 1 of 10 (Start time: 04:44:02 PM, 19 August 2022)

Total Marks

As per cis critical controls from how many minimum synchronized time resources all networks devices and servers should retrieve time?

Select the correct option

- As many as possible
- Three
- Two

Question # 2 of 10 (Start time: 04:45:35 PM, 19 August 2022)

As per boundary defense control of cis what should be done with network traffic at proxy?

Select the correct option

- Allow all the network traffic
- Decrypt all encrypted network traffic prior to analyzing the content
- Use blacklist to allow access to sites without decrypting
- Block all the network traffic

CS205 - Information Security (Quiz No.3) **Total Questions :10**

Please read the following instructions carefully!

1. Quiz will be based upon Multiple Choice Questions (MCQs).

2. You have to attempt the quiz online. You can start attempting the quiz any time within given date(s) of a particular subject by clicking the link for Quiz in VULMS.

3. Each question has a fixed time of 90 seconds. So you have to save your answer before 90 seconds. But due to unstable internet speeds, it is recommended that you should save your answer within 80 seconds. While attempting a question, keep an eye on the remaining time.

4. Attempting quiz is unidirectional. Once you move forward to the next question, you can not go back to the previous one. Therefore before moving to the next question, make sure that you have selected the best option.

5. **DO NOT** press **Back Button / Backspace Button** while attempting a question, otherwise you will lose that question.

6. **DO NOT** refresh the page unnecessarily, **specially** when following messages appear.
   Saving...
   Question Timeout. Now loading next question...

7. **Javascript MUST be enabled** in your browser, otherwise you will not be able to attempt the quiz.

8. If for any reason, you lose access to internet (like power failure or disconnection of internet), you will be able to attempt the quiz again from the question next to the last shown question, but remember that you have to complete the quiz before expiry of the deadline.

9. If any student failed to attempt the quiz in given time then no re-take or offline quiz will be held.

Important Announcement

1. It has come to the University's knowledge that some students are using unfair means while attempting their quiz.

2. The University is monitoring & analyzing the quiz attempts and if a student is found involved in using unfair means, i.e., helping tools/software, web extension, add-ons etc., an Unfair Means Case (UMC) will be made against such student(s) including cancellation of their quiz.

Start Quiz

BC210426997: ISRA HUMA

CS205 - Information Security (Quiz No.3) Quiz Start Tir

Question # 2 of 10 (Start time: 06:37:44 PM, 19 August 2022)

The dedicated machine used by administrators for administrative tasks should have following features

Select the correct option

- Isolated from organization's primary network
- Have internet access
- All routine operational functions can be performed on it
- Email and browsing facility available

Click to Save Answe

CS205 - Information Security (Quiz No.3)

Question # 3 of 10 (Start time: 06:38:51 PM, 19 August 2022)

why security engineering is placed at layer 3 of transformation model?

Select the correct option

- Because it's a low hanging fruit
- Consists of complicated security activities which take more time and effort
- Its not very beneficial to implement so kept at the later stage
- Requires very less time and effort

CS205 - Information Security (Quiz No.3)

Question # 4 of 10 (Start time: 06:39:28 PM, 19 August 2022)

Why should we use scap validated vulnerability scanner?

Select the correct option

- Because it looks for both code-based and configuration-based vulnerabilities
- Because it looks for code-based vulnerabilities
- Because of in-depth scanning feature
- Because of excellent reporting feature

Question # 5 of 10 (Start time: 06:40:02 PM, 19 August 2022)

Before deploying any new devices in a networked environment what should be done with passwords?

Select the correct option

- Create very small passwords
- Change the default passwords
- Remove the passwords
- Keep the default passwords

Click to Save An

Question # 6 of 10 (Start time: 06:40:50 PM, 19 August 2022)

From which type of systems URL requests should be logged in order to identify potentially malicious activity?

Select the correct option

- Mobile devices
- On-site devices
- Off-site devices
- Each of the organization's system

Click to Save Answ

Question # 7 of 10 (Start time: 06:42:10 PM, 19 August 2022)

As per malware defense control why DNS query logging should be enabled?

Select the correct option

- analyze and block inbound email attachments with malicious behavior
- To lower the chance of spoofed or modified emails from valid email addresses
- Continuously monitor and defend organization's servers and workstations
- To detect host-name lookup for known malicious domains

CS205 - Information Security (Quiz No.3)

Question # 8 of 10 (Start time: 06:43:27 PM, 19 August 2022)

What should standard secure configuration images represent?

Select the correct option

- Hardened versions of application installed on system only
- Hardened versions of underlying OS and application installed on system
- Hardened versions of OS only
- Default configuration version of OS only

Question # 9 of 10 (Start time: 06:44:32 PM, 19 August 2022)

Automated tools should be used to verify and compare the network devices configuration with

Select the correct option

- Approved security configuration
- Some 3rd party recommended configuration
- Default security configuration released by vendor
- Latest security configuration released by vendor

CS205 - Information Security (Quiz No.3)

Question # 3 of 10 (Start time: 06:38:51 PM, 19 August 2022)

why security engineering is placed at layer 3 of transformation model?

Select the correct option

- Because it's a low hanging fruit
- Consists of complicated security activities which take more time and effort
- Its not very beneficial to implement so kept at the later stage
- Requires very less time and effort

CS205 - Information Security (Quiz No.3) Qu

Question # 10 of 10 (Start time: 06:45:38 PM, 19 August 2022)

What should an organization do to control access to sensitive information on need-to-know basis?

Select the correct option

- Locate all sensitive information on single vlans
- Store sensitive information on multiple servers
- Locate all sensitive information on separate vlans
- Store all sensitive information on single server

Click to S

CS205 - Information Security (Quiz No.3) **Total Questions :10**

Please read the following instructions carefully!

1. Quiz will be based upon Multiple Choice Questions (MCQs).

2. You have to attempt the quiz online. You can start attempting the quiz any time within given date(s) of a particular subject by clicking the link for Quiz in VULMS.

3. Each question has a fixed time of 90 seconds. So you have to solve your answer before 90 seconds. But due to unstable internet speeds, it is recommended that you should solve your answer within 60 seconds. While attempting a question, keep an eye on the remaining time.

4. Attempting quiz is unidirectional. Once you move forward to the next question, you can not go back to the previous one. Therefore before moving to the next question, make sure that you have selected the best option.

5. **DO NOT** press **Back Button / Backspace Button** while attempting a question, otherwise you will lose that question.

6. **DO NOT** refresh the page unnecessarily, **specially** when following messages appear:
   Saving...
   Question Timeout. Now loading next question...

7. **Javascript MUST be enabled** in your browser, otherwise you will not be able to attempt the quiz.

8. If for any reason, you lose access to internet (like power failure or disconnection of internet), you will be able to attempt the quiz again from the question next to the last shown question. But remember that you have to complete the quiz before expiry of the deadline.

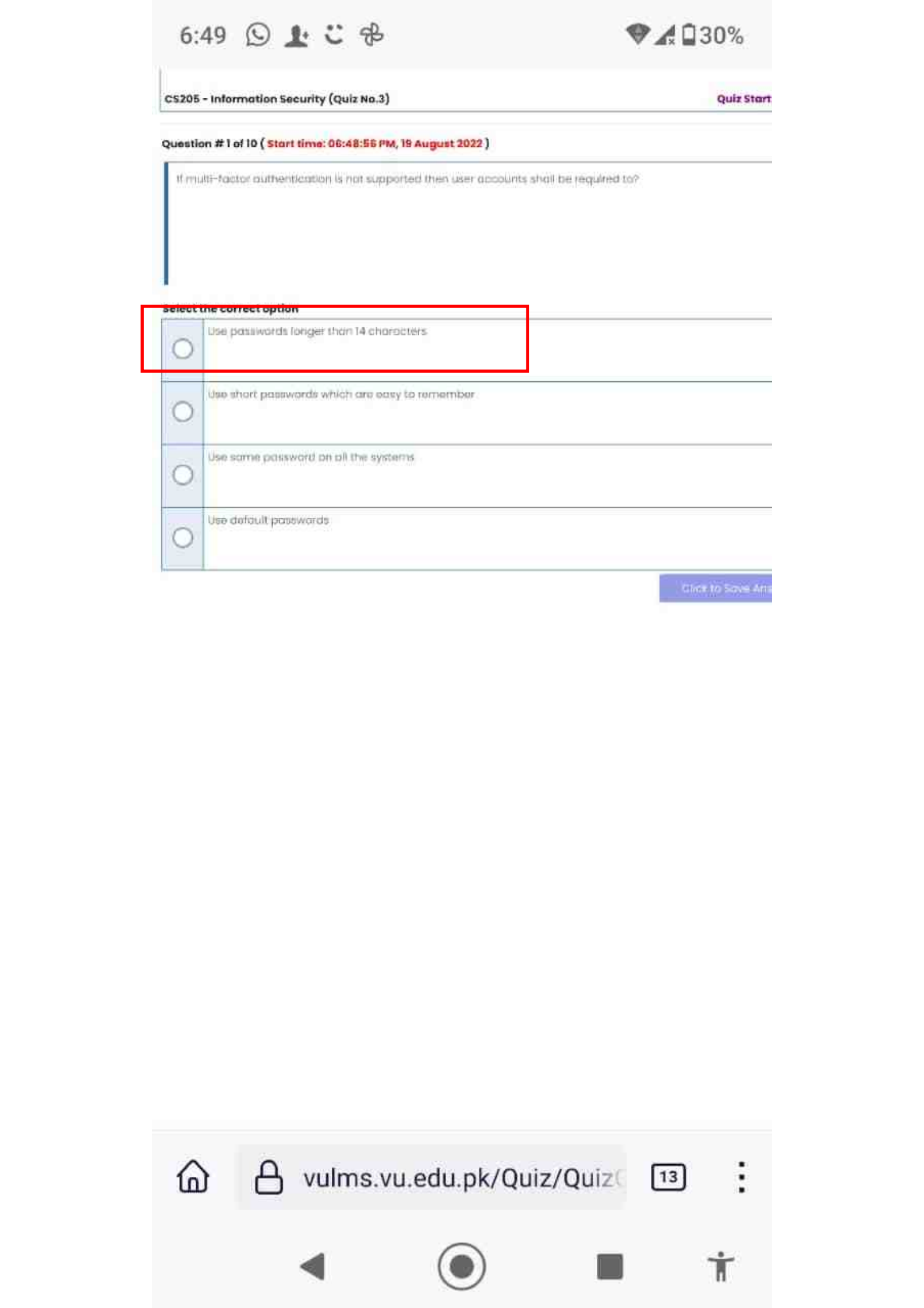
9. If any student failed to attempt the quiz in given time then no re-take or offline quiz will be held.

Important Announcement

1. It has come to the University's knowledge that some students are using unfair means while attempting their quiz.

2. The University is monitoring & analyzing the quiz attempts and if a student is found involved in using unfair means i.e., helping tools/software, Web Extension, Add-ons etc. an Unfair Means Case (UMC) will be made against such student(s) including cancellation of their quiz.

Start Quiz


6:49
30%
CS205 - Information Security (Quiz No.3)
Quiz Start
Question # 1 of 10 (Start time: 06:48:56 PM, 19 August 2022)
If multi-factor authentication is not supported then user accounts shall be required to?
Select the correct option
Use passwords longer than 14 characters
Use short passwords which are easy to remember
Use same password on all the systems
Use default passwords
vulms.vu.edu.pk/Quiz/Quiz
13

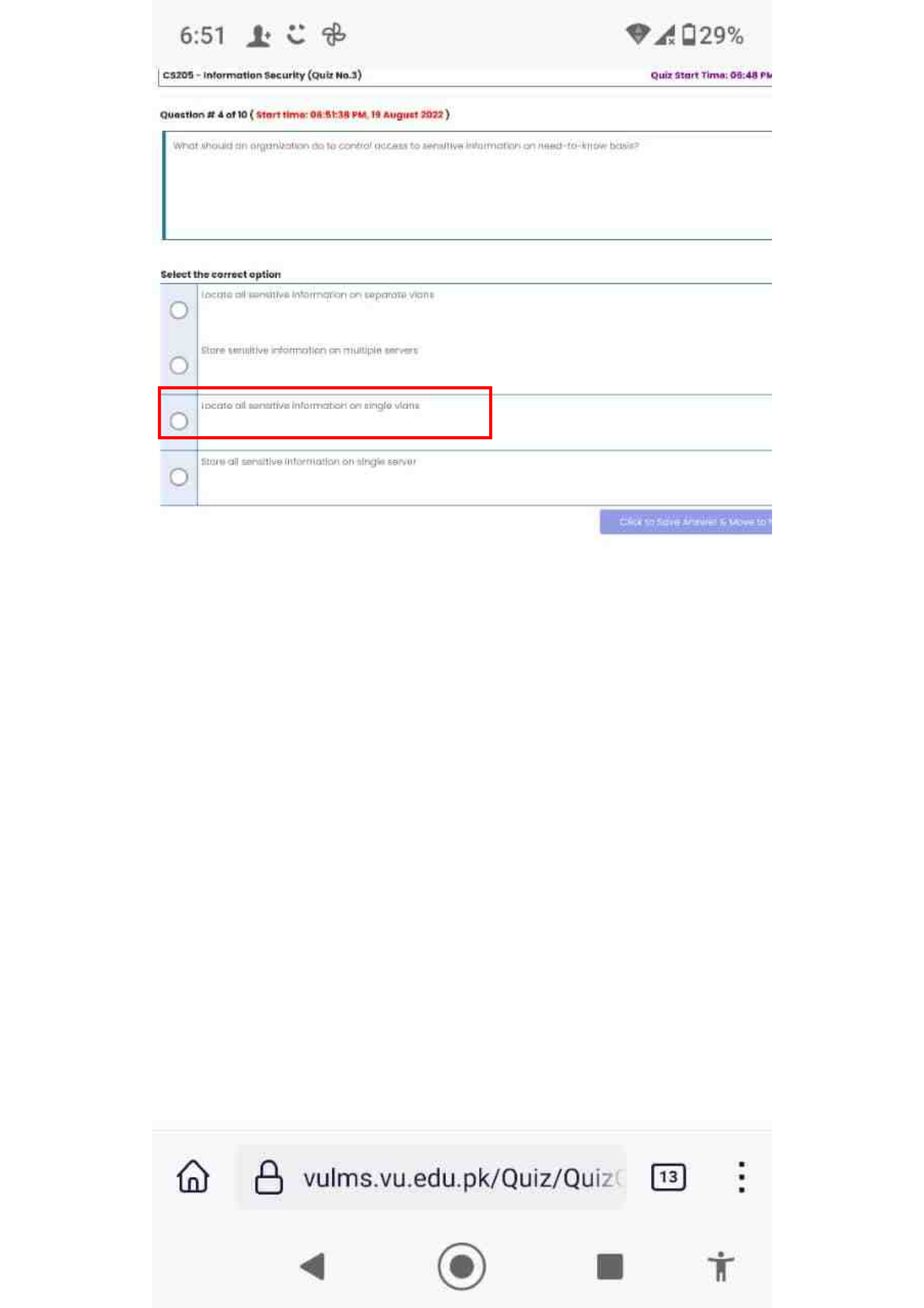
Question # 3 of 10 (Start time: 06:50:48 PM, 19 August 2022)

If a system in an organization gets compromised, how can we prevent an attacker to compromise the neighboring systems?

Select the correct option

- Through antivirus
- Through network-based intrusion detection system(ips)
- Through network-based intrusion prevention system(ips)
- Through system firewall

Click to Save Answer & Move to


6:51
29%
CS205 - Information Security (Quiz No.3)
Quiz Start Time: 06:48 PM
Question # 4 of 10 (Start time: 06:51:38 PM, 19 August 2022)
What should an organization do to control access to sensitive information on need-to-know basis?
Select the correct option
Locate all sensitive information on separate vlans
Store sensitive information on multiple servers
Locate all sensitive information on single vlans
Store all sensitive information on single server
vulms.vu.edu.pk/Quiz/Quiz
13

CS205 - Information Security (Quiz No.3) Quiz Start Time: 06:4

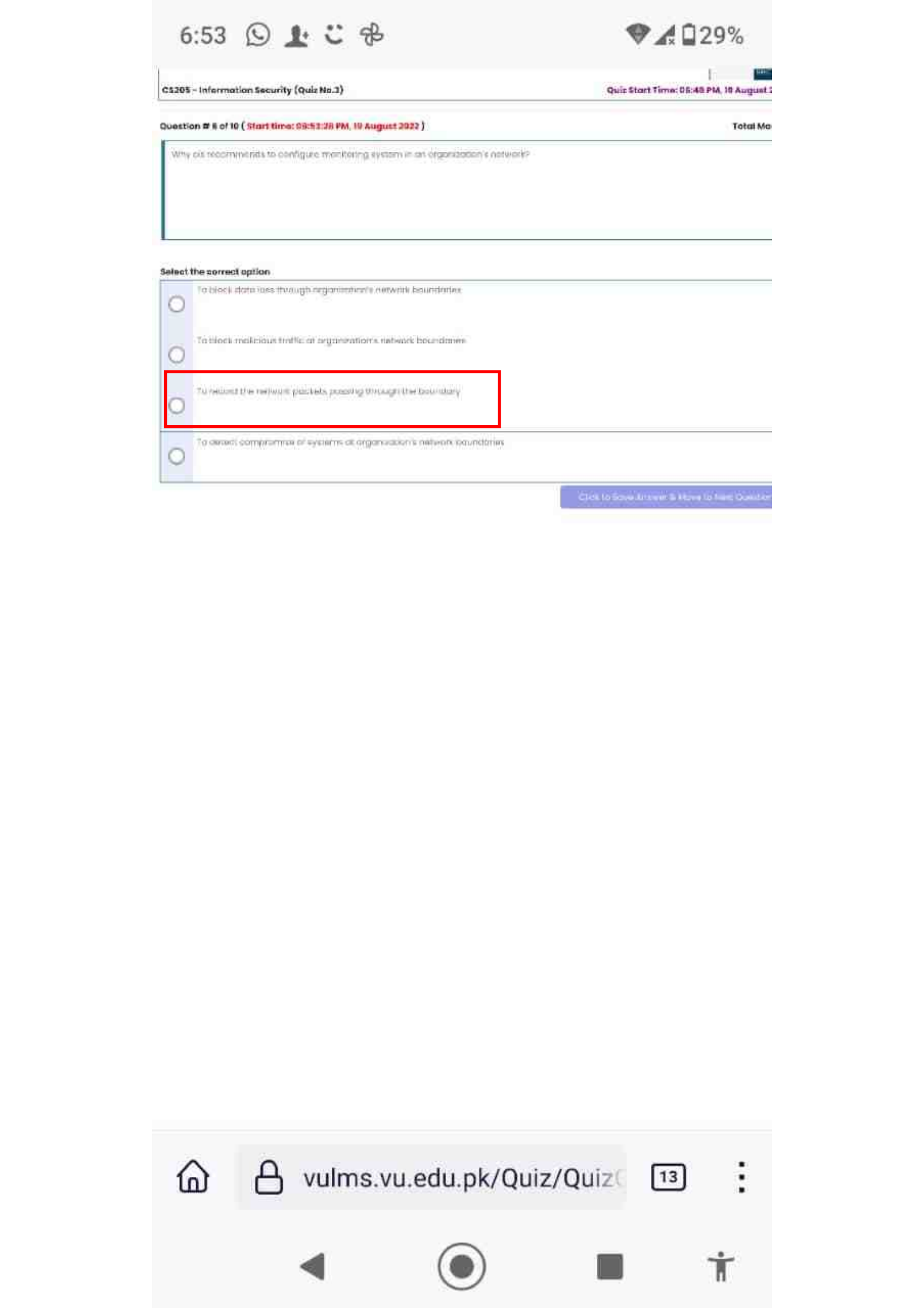
Question # 5 of 10 (Start time: 06:52:20 PM. 19 August 2022)

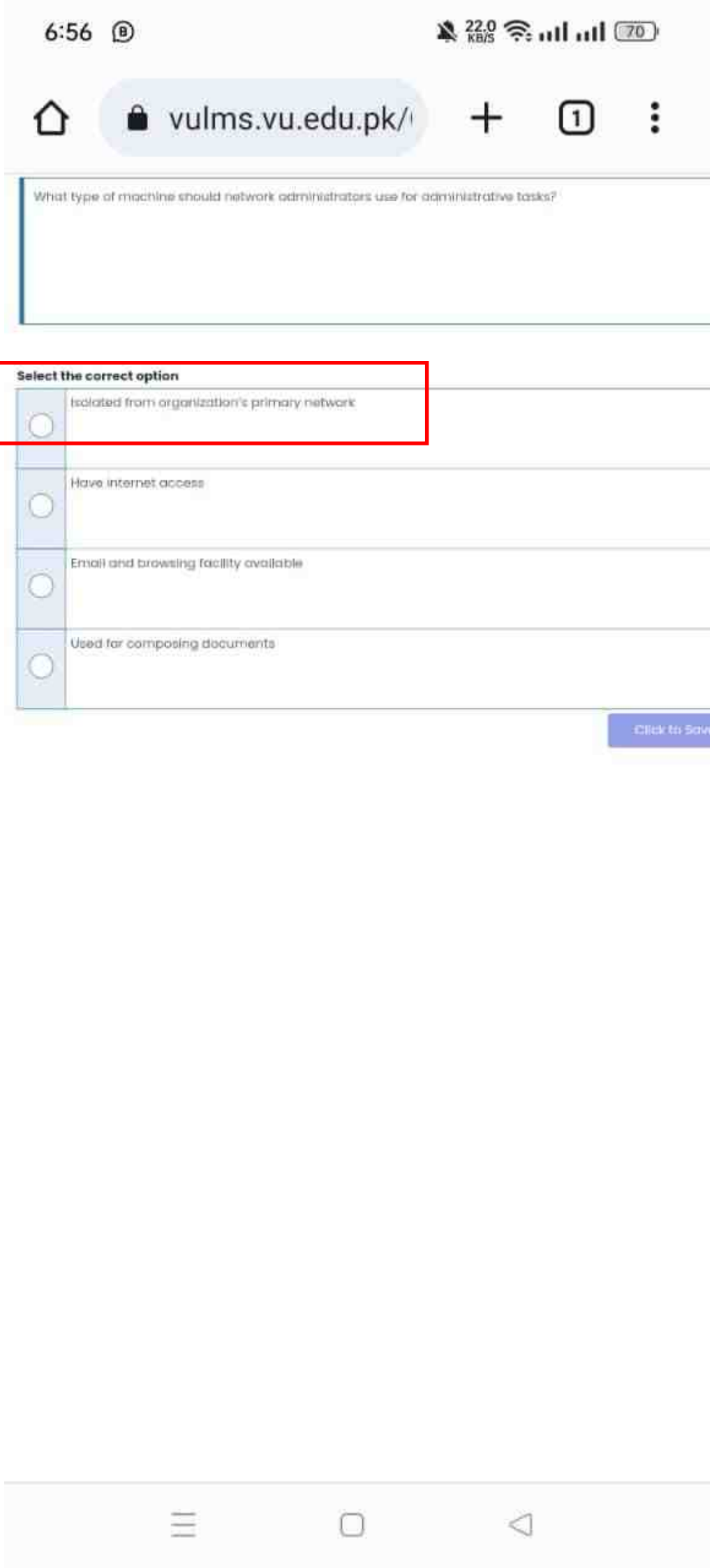
why security engineering is placed at layer 3 of transformation model?

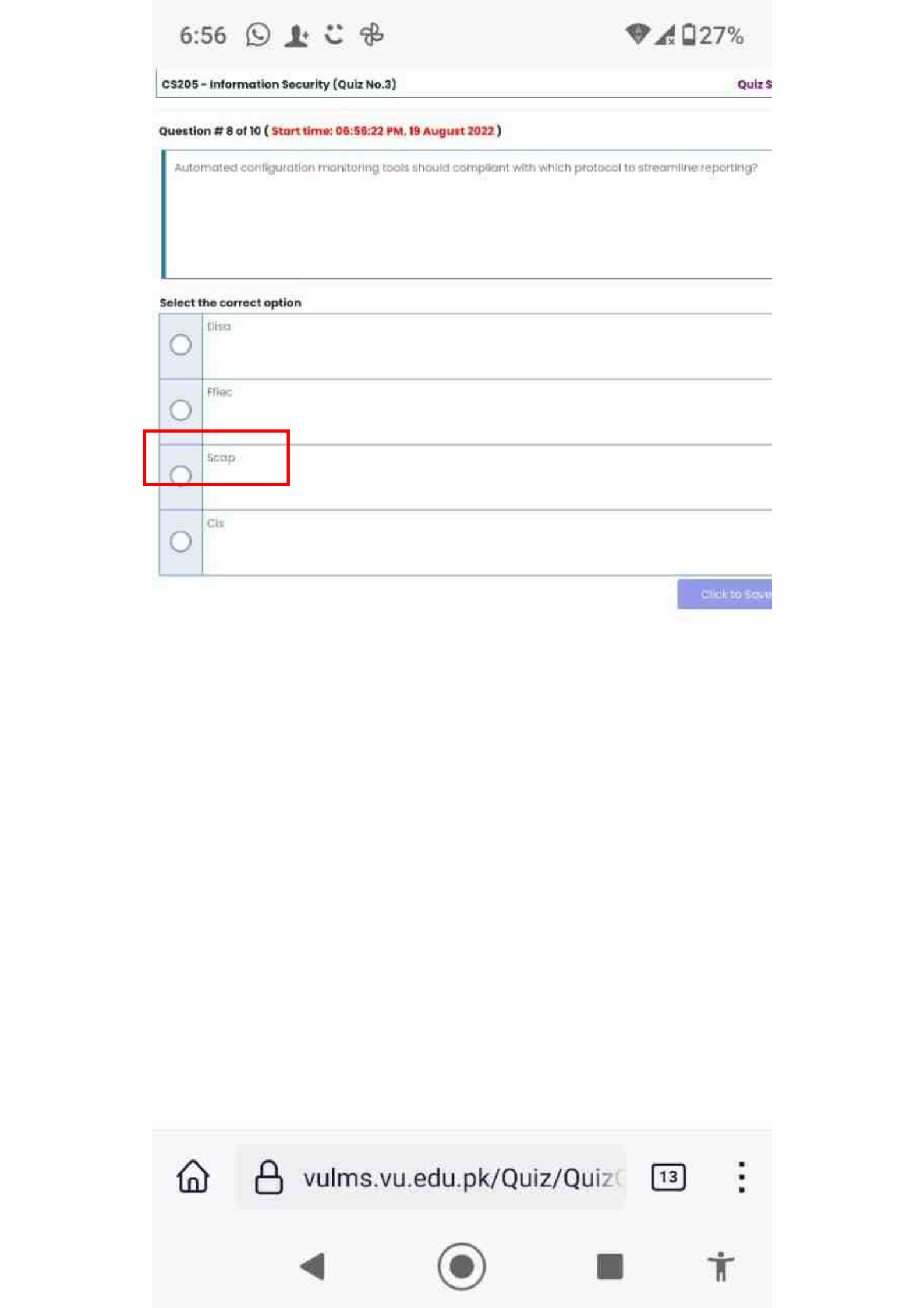
Select the correct option

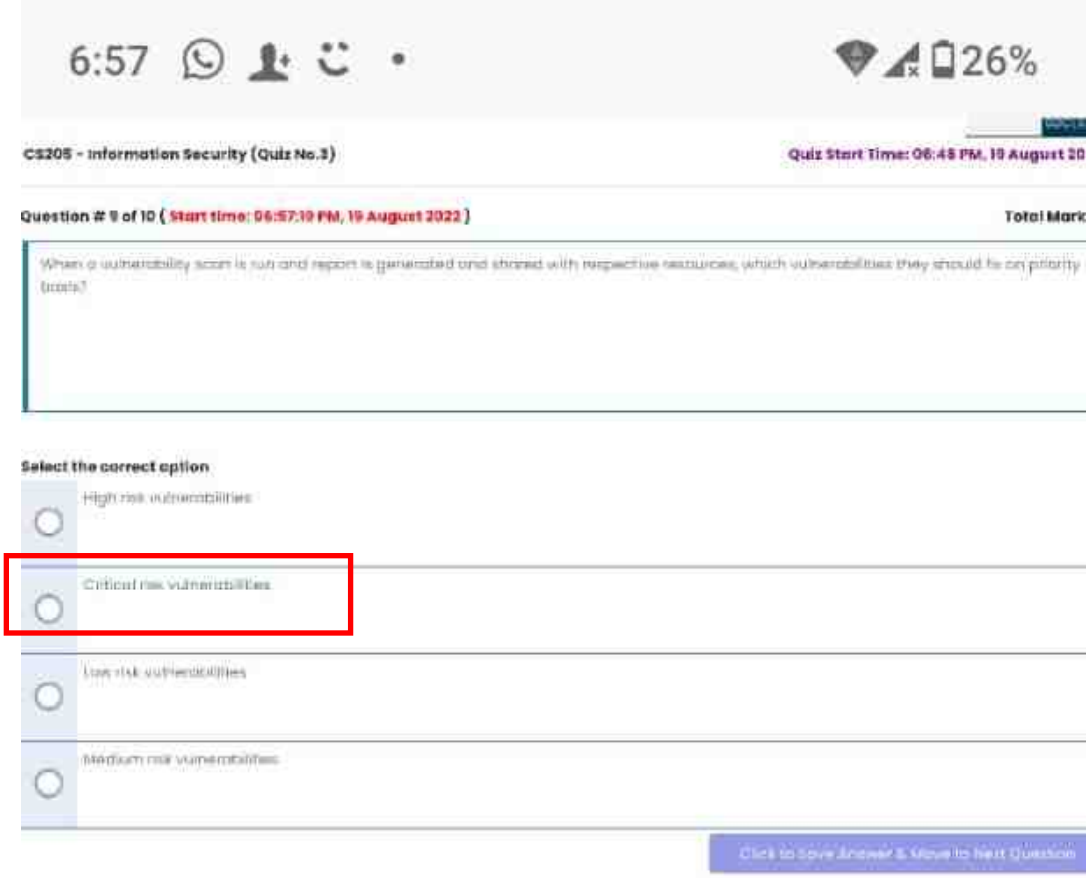
- Requires very less time and effort
- Because it's a low hanging fruit
- Consists of complicated security activities which take more time and effort
- Its not very beneficial to implement so kept at this later stage

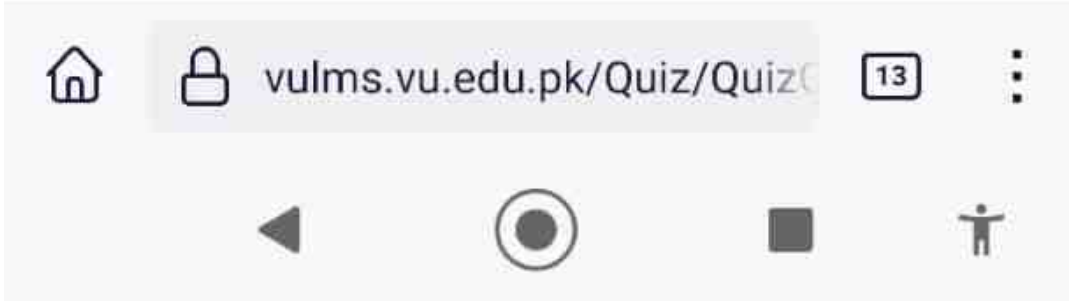
Click to Save Answer & Move


6:53
29%
CS205 – Information Security (Quiz No.3)
Quiz Start Time: 05:48 PM, 10 August
Question # 6 of 10 (Start time: 09:53:28 PM, 10 August 2022)
Total Mo
Why it's recommended to configure monitoring system in an organization's network?
Select the correct option
To block data loss through organization's network boundaries
To block malicious traffic at organization's network boundaries
To record the relevant packets passing through the boundary
To detect compromise of systems at organization's network boundaries
vulms.vu.edu.pk/Quiz/Quiz
13


6:56
22.0 KB/S
70
vulms.vu.edu.pk/
What type of machine should network administrators use for administrative tasks?
Select the correct option
Isolated from organization's primary network
Have internet access
Email and browsing facility available
Used for composing documents


6:56
27%
CS205 - Information Security (Quiz No.3)
Quiz S
Question # 8 of 10 (Start time: 06:56:22 PM, 19 August 2022)
Automated configuration monitoring tools should compliant with which protocol to streamline reporting?
Select the correct option
Disa
Ffiec
Scap
Cis
Click to Save
vulms.vu.edu.pk/Quiz/Quiz
13


6:57
26%
CS205 - Information Security (Quiz No.3)
Quiz Start Time: 06:48 PM, 19 August 20
Question # 9 of 10 (Start time: 06:57:19 PM, 19 August 2022)
Total Mark
When a vulnerability scan is run and report is generated and shared with respective resources, which vulnerabilities they should fix on priority basis?
Select the correct option
High risk vulnerabilities
Critical risk vulnerabilities
Low risk vulnerabilities
Medium risk vulnerabilities
Click to Save Answer & Move to Next Question


vulms.vu.edu.pk/Quiz/Quiz
13

YouTube Maps

10424460: FAIZA MUBEEN

205 – Information Security (Quiz No.3)

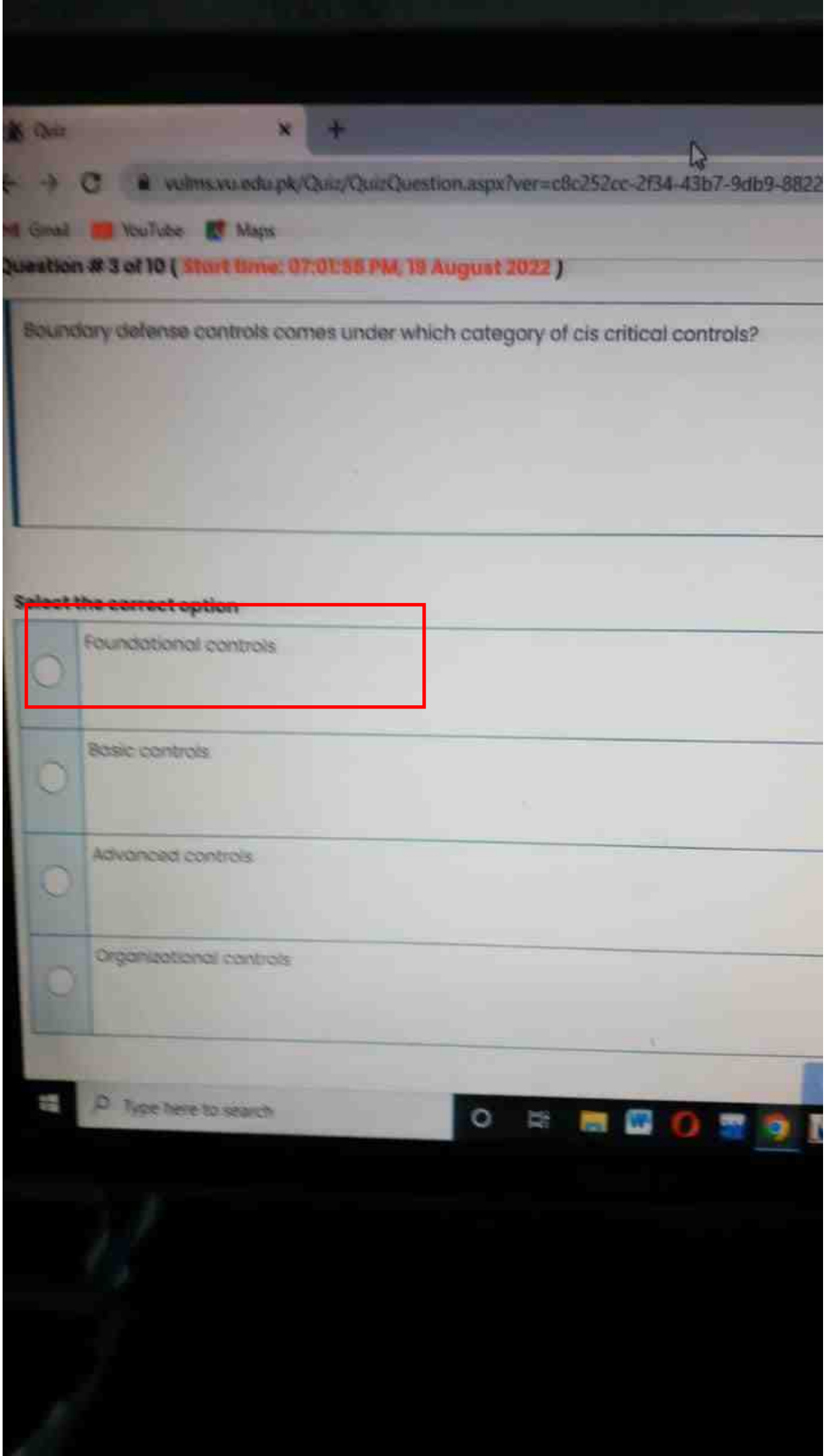
Question # 1 of 10 (Start time: 07:00:29 PM, 19 August 2022)

As per malware defense control why DNS query logging should be enabled?

Select the correct option

- Continuously monitor and defend organization's servers and workstations
- To lower the chance of spoofed or modified emails from valid email addresse
- To detect host-name lookup for known malicious domains

Type here to search


Quiz
vulms.vu.edu.pk/Quiz/QuizQuestion.aspx?ver=c8c252cc-2f34-43b7-9db9-8822
Gmail
YouTube
Maps
Question # 3 of 10 (Start time: 07:01:55 PM, 19 August 2022)
Boundary defense controls comes under which category of cis critical controls?
Select the correct option
Foundational controls
Basic controls
Advanced controls
Organizational controls
Type here to search

vulms.vu.edu.pk/Quiz/QuizQuestion.aspx?ver=4d5dfeaf-921c-48

Gmail YouTube Maps

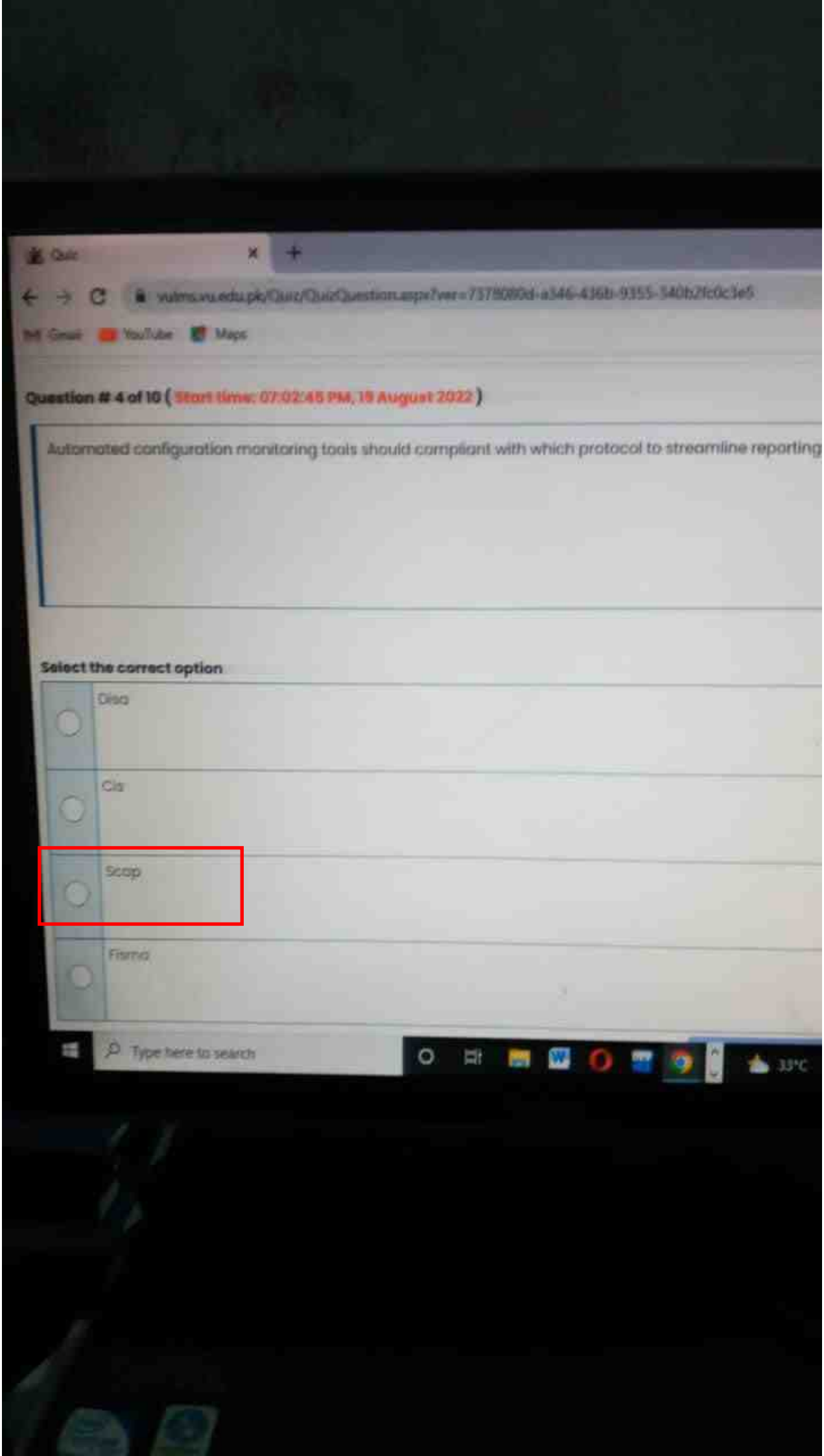
Question # 2 of 10 (Start time: 07:01:15 PM, 10 August 2022)

In an enterprise which softwares should be allowed to install and execute?

Select the correct option

- Any freely available software
- Only paid software
- Softwares displayed on notice board
- Softwares included in whitelist

Type here to search


Quiz
vulms.vu.edu.pk/Quiz/QuizQuestion.aspx?ver=7378080d-a346-436b-9355-540b2fc0c3e5
Gmail
YouTube
Maps
Question # 4 of 10 (Start time: 07:02:45 PM, 18 August 2022)
Automated configuration monitoring tools should compliant with which protocol to streamline reporting
Select the correct option
Diso
Cis
Scap
Firma
Type here to search
33°C

vulms.vu.edu.pk/Quiz/QuizQuestion.aspx?ver=f8352e75-0e0b-453c-866b-7c8

Gmail YouTube Maps

BC210424480: FAIZA MUBEEN

CS205 - Information Security (Quiz No.3)

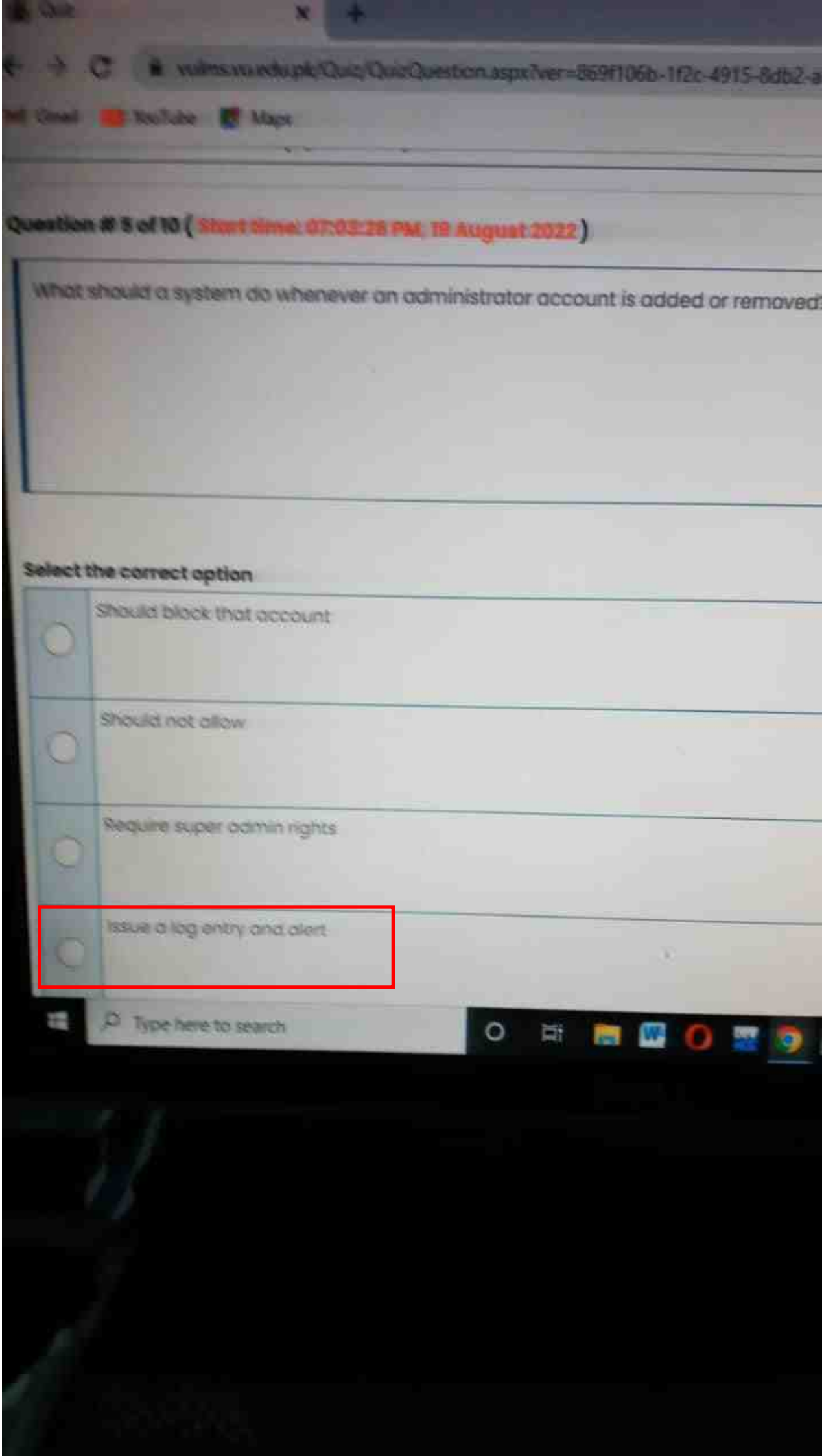
Question # 1 of 10 (Start time: 07:00:29 PM, 18 August 2022)

As per malware defense control why DNS query logging should be enabled?

Select the correct option

- Continuously monitor and defend organization's servers and workstations
- To lower the chance of spoofed or modified emails from valid email addresses
- To detect host-name lookup for known malicious domains

Type here to search


Question # 5 of 10 (Start time: 07:03:28 PM, 19 August 2022)
What should a system do whenever an administrator account is added or removed
Select the correct option
Should block that account
Should not allow
Require super admin rights
Issue a log entry and alert
Type here to search

DC190200248: FIZA ASMA

Time Left 84 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 07:01 PM, 19 August 2022

Question #1 of 10 (Start time: 07:01:53 PM, 19 August 2022)

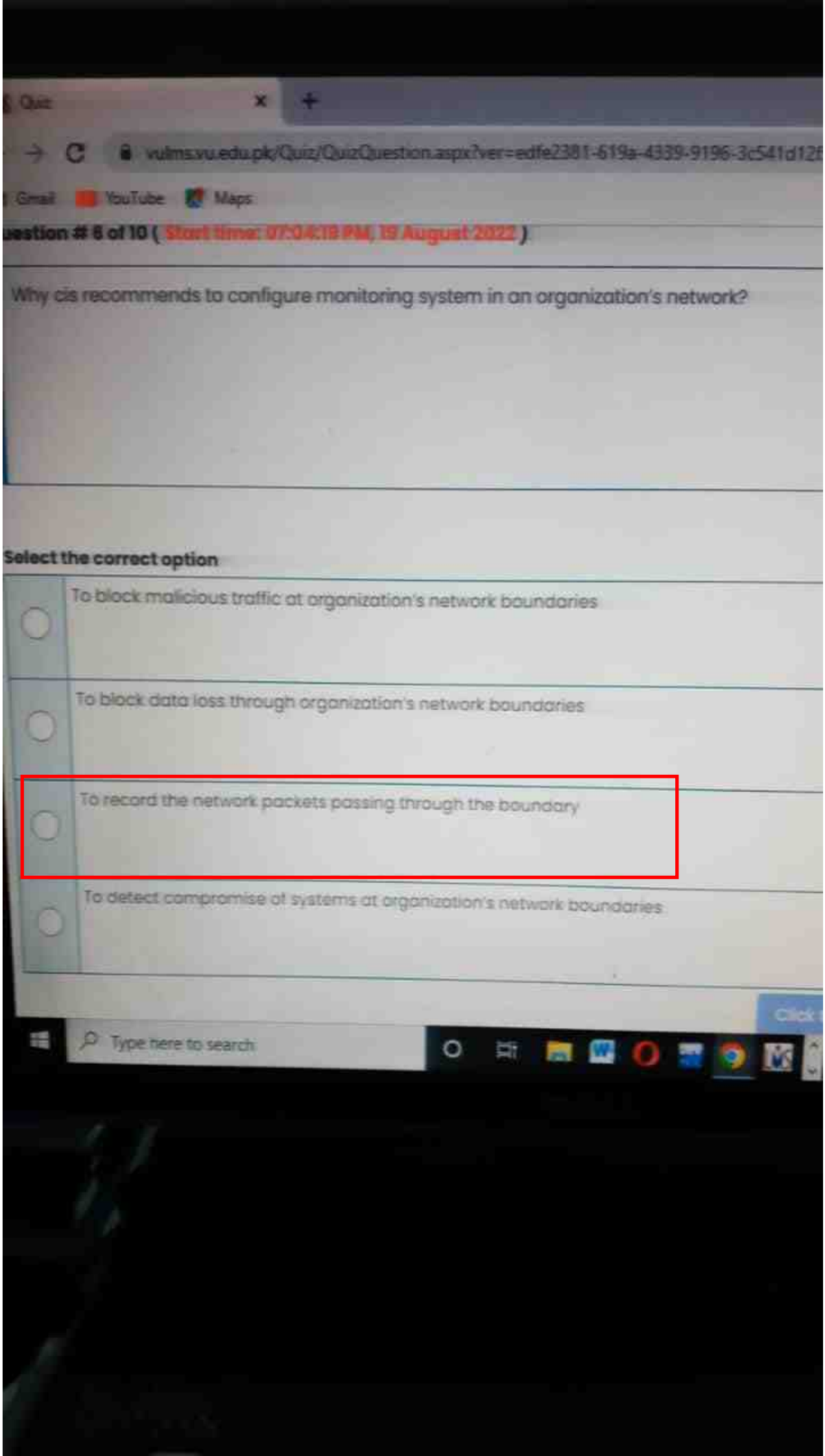
Total Marks: 1

why security engineering is placed at layer 3 of transformation model?

Select the correct option

- Consists of complicated security activities which take more time and effort
- Because it's a low hanging fruit
- Its not very beneficial to implement so kept at the later stage
- Requires very less time and effort

Click to Save Answer & Move to Next Question


Quiz
vulms.vu.edu.pk/Quiz/QuizQuestion.aspx?ver=edfe2381-619a-4339-9196-3c541d12f
Gmail
YouTube
Maps
uestion # 6 of 10 (Start time: 07:04:18 PM, 19 August 2022)
Why cis recommends to configure monitoring system in an organization's network?
Select the correct option
To block malicious traffic at organization's network boundaries
To block data loss through organization's network boundaries
To record the network packets passing through the boundary
To detect compromise of systems at organization's network boundaries
Type here to search

DC190200248: FIZA ASMA

Time Left 80 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 07:01 PM, 19 August 2022

Question # 2 of 10 (Start time: 07:03:02 PM, 19 August 2022)

Total Marks: 1

Boundary defense controls comes under which category of cis critical controls?

Select the correct option

- Basic controls
- Organizational controls
- Foundational controls
- Advanced controls

Click to Save Answer & Move to Next Question

DC190200248: FIZA ASMA

Time Left 74 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 07:01 PM, 19 August 2022

Question # 3 of 10 (Start time: 07:03:54 PM, 19 August 2022)

Total Marks: 1

In which mode should vulnerability scanning be performed?

Select the correct option

- Un-authenticated mode
- Deep scan mode
- Dedicated mode
- Authenticated mode

Click to Save Answer & Move to Next Question

vulms.vu.edu.pk/Quiz/QuizQuestion.aspx?ver=05ecfad4-884e-4b5e-ad7-fac3e411121b

Gmail YouTube Maps

Total Marks: 1

Question # 8 of 10 (Start time: 07:08:07 PM, 19 August 2022)

Which of the following can be used to look for unusual attack mechanisms on organization's network boundaries?

Select the correct option

- Host-based intrusion prevention (ips) system
- Host-based intrusion detection (ids) sensors
- Network-based intrusion prevention (ips) system
- Network-based intrusion detection (ids) sensors

DC190200248: FIZA ASMA

Time Left 82 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 07:01 PM, 19 August 2022

Question # 4 of 10 (Start time: 07:05:54 PM, 19 August 2022)

Total Marks: 1

Which of the following can be used to block malicious traffic on organization's network boundaries?

Select the correct option

- Host-based intrusion detection (ids) sensors
- Host-based intrusion prevention (ips) system
- Network-based intrusion detection (ids) sensors
- Network-based intrusion prevention (ips) system

Click to Save Answer & Move to Next Question

Question # 8 of 10 (Start time: 07:08:07 PM, 10 August 2022) **Total Marks: 1**

Which of the following can be used to look for unusual attack mechanisms on organization's network boundaries?

Select the correct option

- Host-based intrusion prevention (ips) system
- Host-based intrusion detection (ids) sensors
- Network-based intrusion prevention (ips) system
- Network-based intrusion detection (ids) sensors

DC190200248: FIZA ASMA

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 07:01 PM, 19 August 2022

Question # 7 of 10 (Start time: 07:09:08 PM, 19 August 2022)

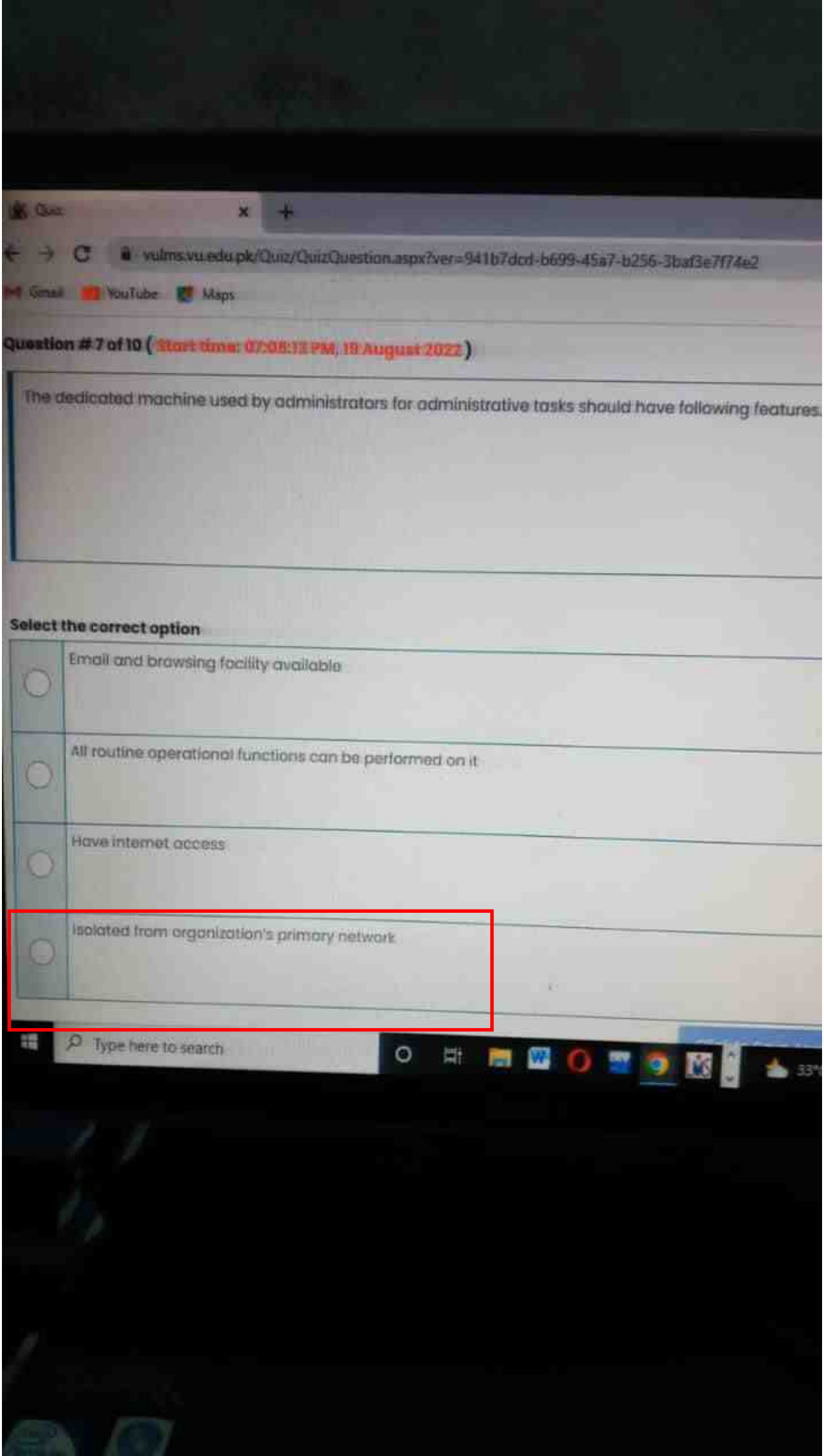
Total Marks: 1

As per limitation and control of network control of cis active ports, protocols and services should be associated to

Select the correct option

- All the assets in asset inventory
- Software assets in asset inventory
- Active directory domain
- Hardware assets in asset inventory

Click to Save Answer & Move to Next Question


vulms.vu.edu.pk/Quiz/QuizQuestion.aspx?ver=941b7dcd-b699-45a7-b256-3baf3e7f74e2
Gmail
YouTube
Maps
Question # 7 of 10 (Start time: 07:05:11 PM, 19 August 2022)
The dedicated machine used by administrators for administrative tasks should have following features.
Select the correct option
Email and browsing facility available
All routine operational functions can be performed on it
Have internet access
Isolated from organization's primary network
Type here to search

DC190200248: FIZA ASMA

Time Left 87 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 07:01 PM, 19 August 2022

Question # 5 of 10 (Start time: 07:07:13 PM, 19 August 2022)

Total Marks: 1

From which type of systems URL requests should be logged in order to identify potentially malicious activity?

Select the correct option

- Each of the organization's system
- Off-site devices
- On-site devices
- Mobile devices

Click to Save Answer & Move to Next Question

DC190200248: FIZA ASMA

Time Left 86 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 07:01 PM, 19 August 2022

Question # 9 of 10 (Start time: 07:11:04 PM, 19 August 2022)

Total Marks: 1

Which policy is recommended by data protection control of cis for mobile devices usage in an organization?

Select the correct option

- Mobile devices should not be allowed
- Employees should use only personal mobile devices
- Mobile devices are allowed for higher management only
- Hard drive of mobile devices should be encrypted

Click to Save Answer & Move to Next Question

DC190200248: FIZA ASMA

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 07:01 PM, 19 August 2022

Question #10 of 10 (Start time: 07:11:44 PM, 19 August 2022)

Total Marks: 1

The dedicated machine used by administrators for administrative tasks should have following features.

Select the correct option

- All routine operational functions can be performed on it
- Isolated from organization's primary network
- Have internet access
- Email and browsing facility available

Click to Save Answer & Move to Next Question

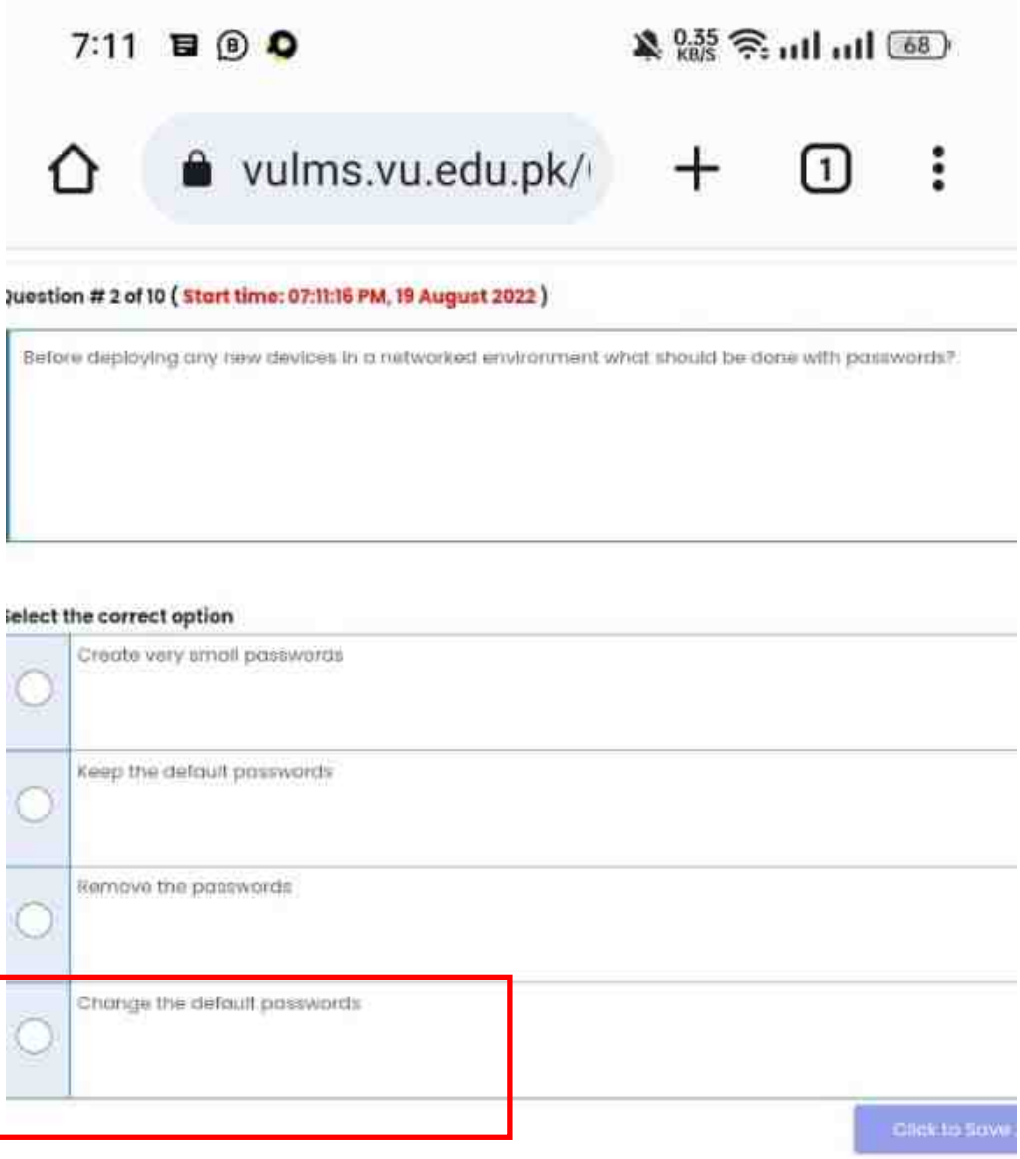
Question # 9 of 10 (Start time: 07:08:55 PM, 19 August 2022)

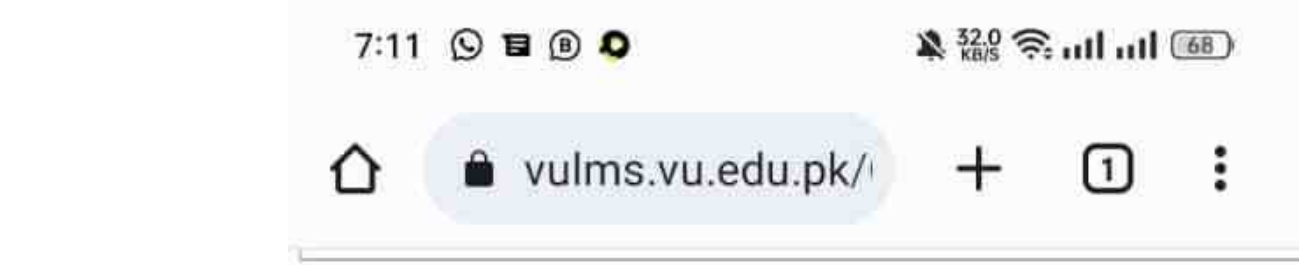
Total Marks: 1

As per boundary defense control of cis what should be done with network traffic at proxy?

Select the correct option

- Decrypt all encrypted network traffic prior to analyzing the content
- Allow all the network traffic
- Use blacklist to allow access to sites without decrypting
- Block all the network traffic


7:11
0.35 KB/S
68
vulms.vu.edu.pk/
1
uestion # 2 of 10 (Start time: 07:11:16 PM, 19 August 2022)
Before deploying any new devices in a networked environment what should be done with passwords?
elect the correct option
Create very small passwords
Keep the default passwords
Remove the passwords
Change the default passwords
Click to Save



Question # 3 of 10 (Start time: 07:11:49 PM, 19 August 2022)

Which of the following tools can be used to enforce access controls to data?

Select the correct option

- File integrity monitoring solution
- Security information and event management system
- Host-based data loss prevention (dlp)
- Network-based intrusion detection system

Click to Sav

DC190200248: FIZA ASMA

CS205 - Information Security (Quiz No.3)

Question # 6 of 10 (Start time: 07:08:19 PM, 19 August 2022)

Which cis control is described in this module?

Select the correct option

- Wireless access control
- Data recovery capabilities
- Boundary defenses
- Malware defenses

Click

DC190200248: FIZA ASMA

Time Left 88 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 07:01 PM, 19 August 2022

Question # 8 of 10 (Start time: 07:10:16 PM, 19 August 2022)

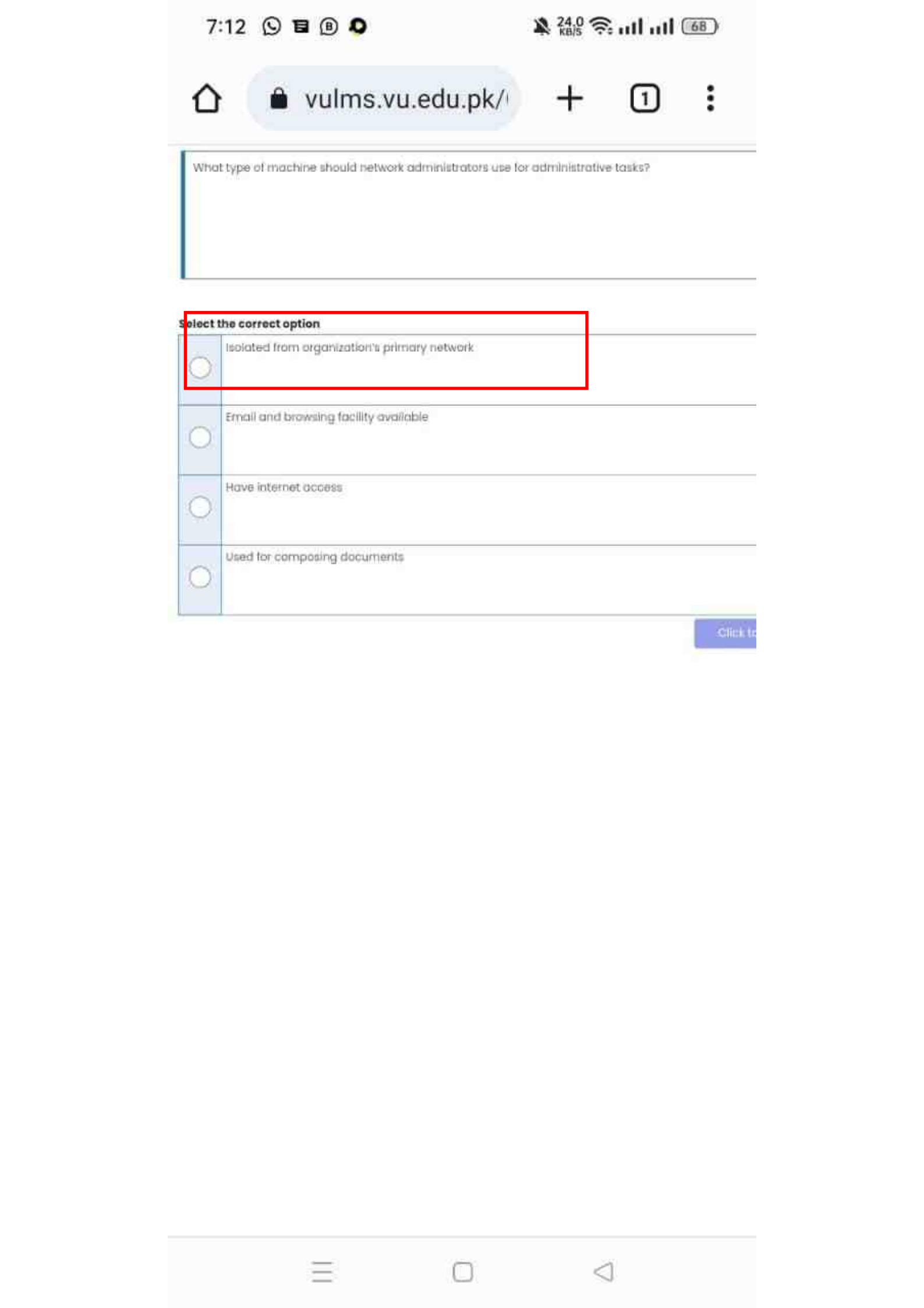
Total Marks: 1

As per malware defense control why DNS query logging should be enabled?

Select the correct option

- analyze and block inbound email attachments with malicious behavior
- To lower the chance of spoofed or modified emails from valid email addresses
- Continuously monitor and defend organization's servers and workstations
- To detect host-name lookup for known malicious domains

Click to Save Answer & Move to Next Question


7:12
vulms.vu.edu.pk/
What type of machine should network administrators use for administrative tasks?
Select the correct option
Isolated from organization's primary network
Email and browsing facility available
Have internet access
Used for composing documents

What should standard secure configuration images represent?

Select the correct option

- Hardened versions of OS only
- Default configuration version of OS only
- Hardened versions of application installed on system only
- Hardened versions of underlying OS and application installed on system

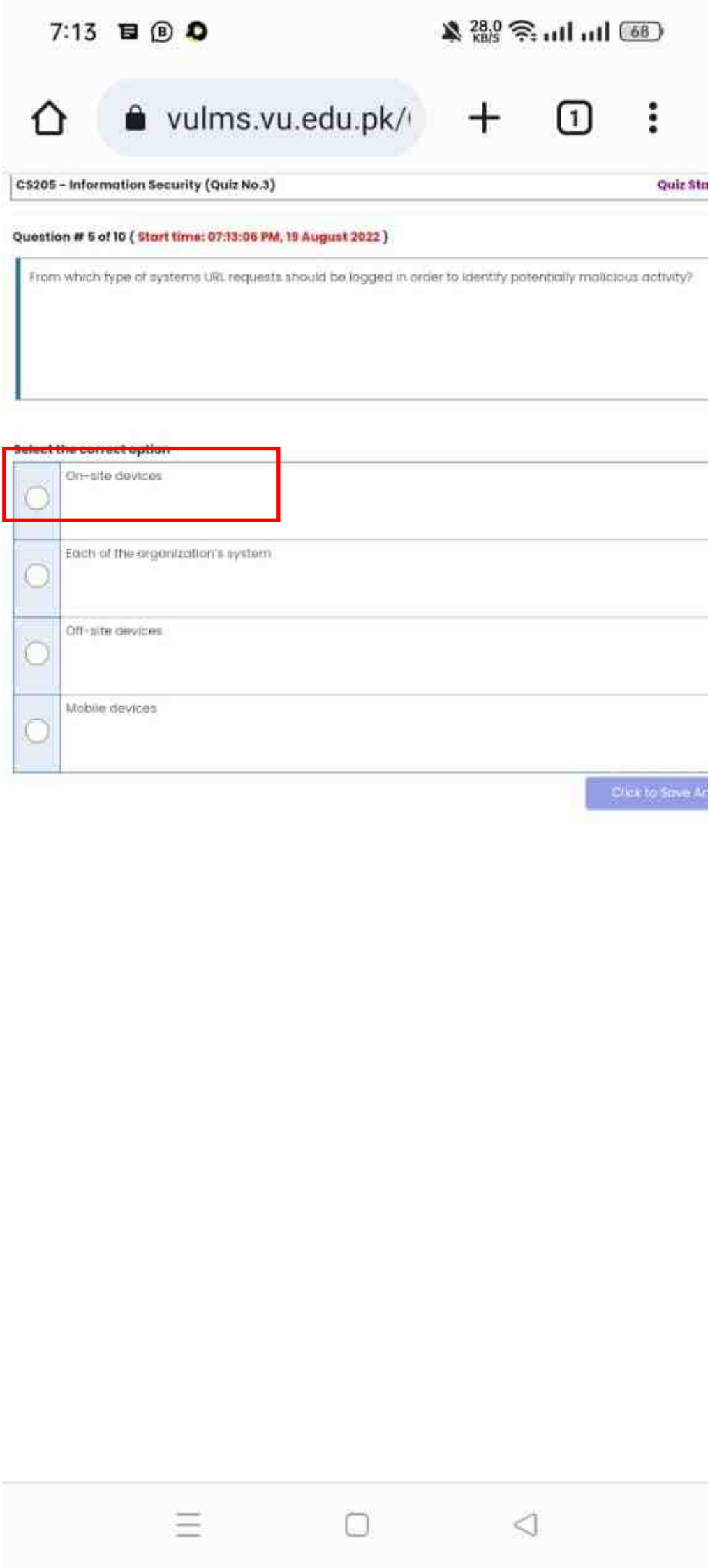
Question # 6 of 10 (Start time: 07:13:39 PM, 18 August 2022)

As per boundary defense control of cis what should be done with network traffic at proxy?

Select the correct option

- Block all the network traffic
- Allow all the network traffic
- Use blacklist to allow access to sites without decrypting
- Decrypt all encrypted network traffic prior to analyzing the content

Click to Save A


7:13
vulms.vu.edu.pk/
CS205 - Information Security (Quiz No.3)
Quiz Sta
Question # 5 of 10 (Start time: 07:13:06 PM, 19 August 2022)
From which type of systems URL requests should be logged in order to identify potentially malicious activity?
On-site devices
Each of the organization's system
Off-site devices
Mobile devices

BC210424372: MUBASHIRA NASEEM

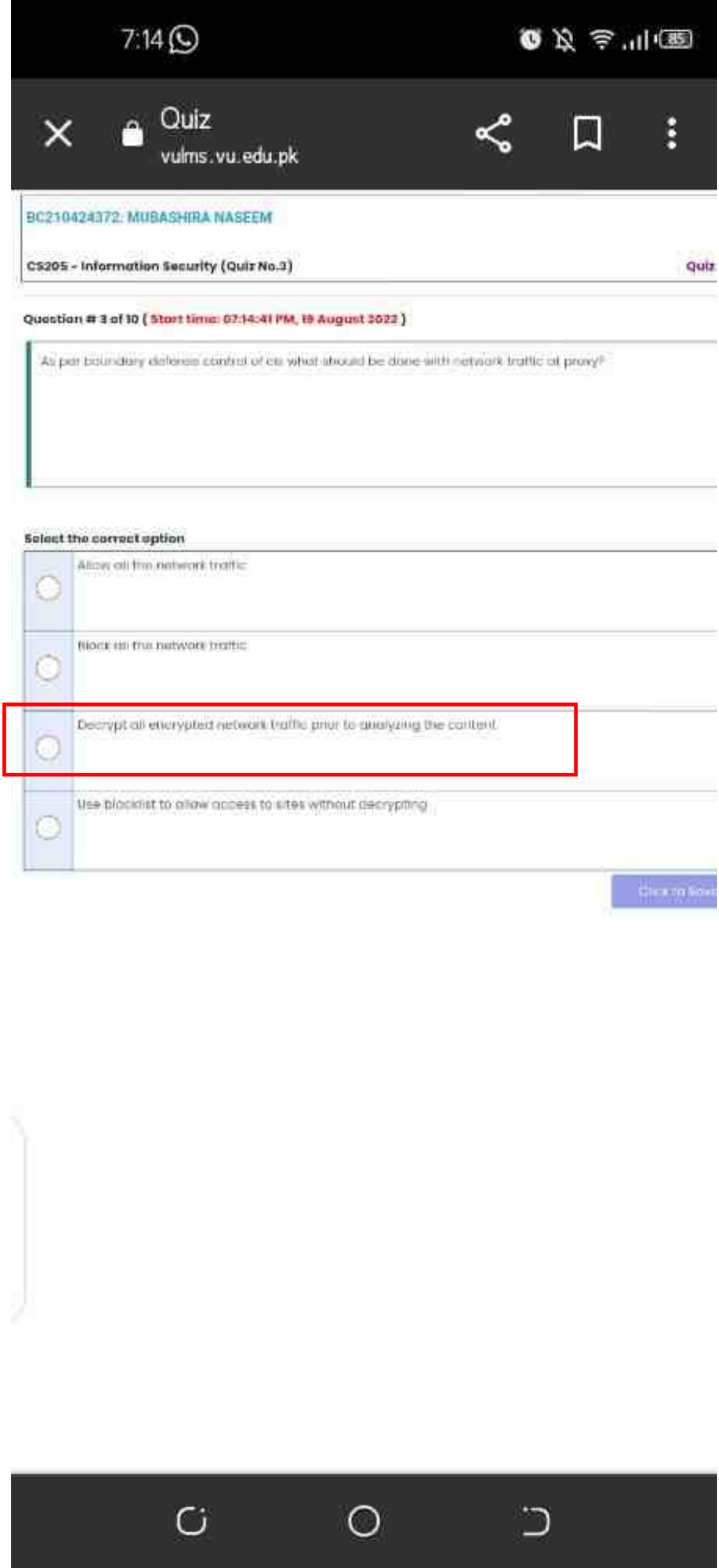
CS205 - Information Security (Quiz No.3)

Question # 2 of 10 (Start time: 07:13:28 PM, 19 August 2022)

What should a system do whenever an administrator account is added or removed?

Select the correct option

- Require super admin rights
- Issue a log entry and alert
- Should block that account
- Should not allow


7:14
Quiz
vulms.vu.edu.pk
BC210424372: MUBASHIRA NASEEM
CS205 - Information Security (Quiz No.3)
Quiz
Question # 3 of 10 (Start time: 07:14:41 PM, 19 August 2022)
As per boundary defense control of cis what should be done with network traffic at proxy?
Select the correct option
Allow all the network traffic
Block all the network traffic
Decrypt all encrypted network traffic prior to analyzing the content
Use blacklist to allow access to sites without decrypting

BC210424372: MUBASHIRA NASEEM

CS205 - Information Security (Quiz No.3)

Question # 4 of 10 (Start time: 07:15:45 PM, 19 August 2022)

Each person with administrator account should be authorized by?

Select the correct option

- System administrator
- Senior executive
- Help-desk team
- Network administrator

CS205 - Information Security (Quiz No.3)

Question # 10 of 10 (Start time: 07:16:11 PM, 19 August 2022)

Which of the following cis critical control is discussed in this module?

Select the correct option

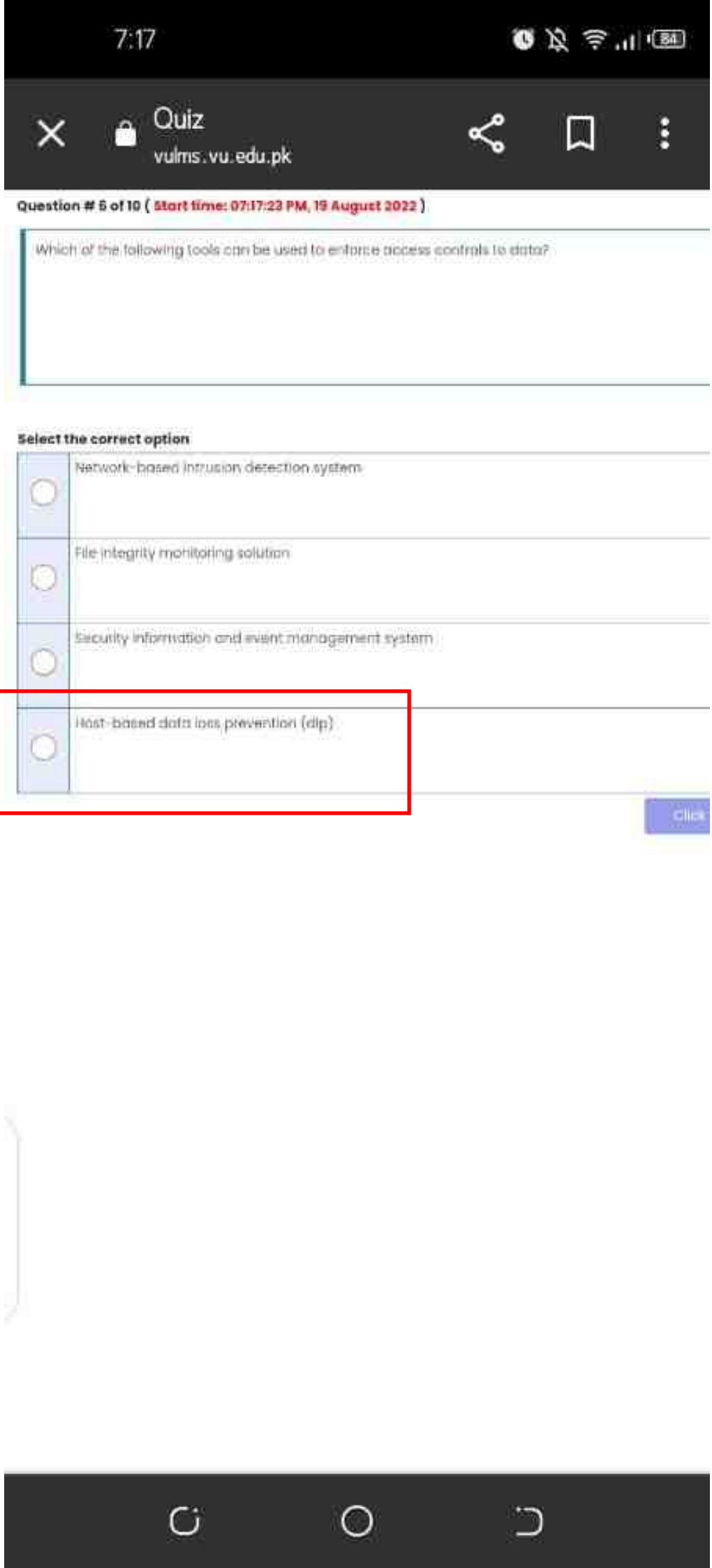
- Boundary defense
- Data protection
- Malware defense
- Secure configuration for network devices

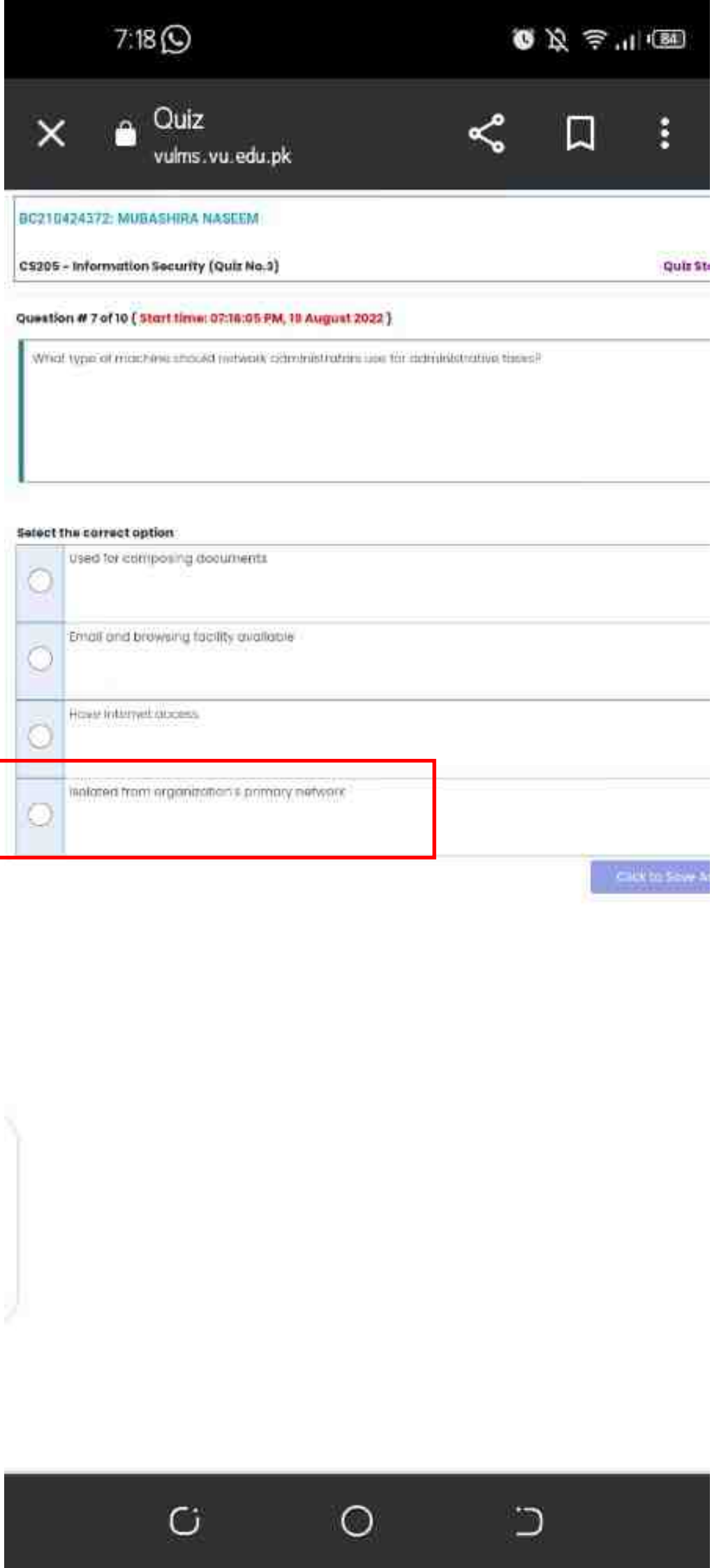
Question # 5 of 10 (Start time: 07:56:40 PM, 15 August 2022)

After getting vulnerability scanning results patches should be applied to?

Select the correct option

- All the systems throughout the organization
- Network devices only
- Client machines only
- Critical servers only

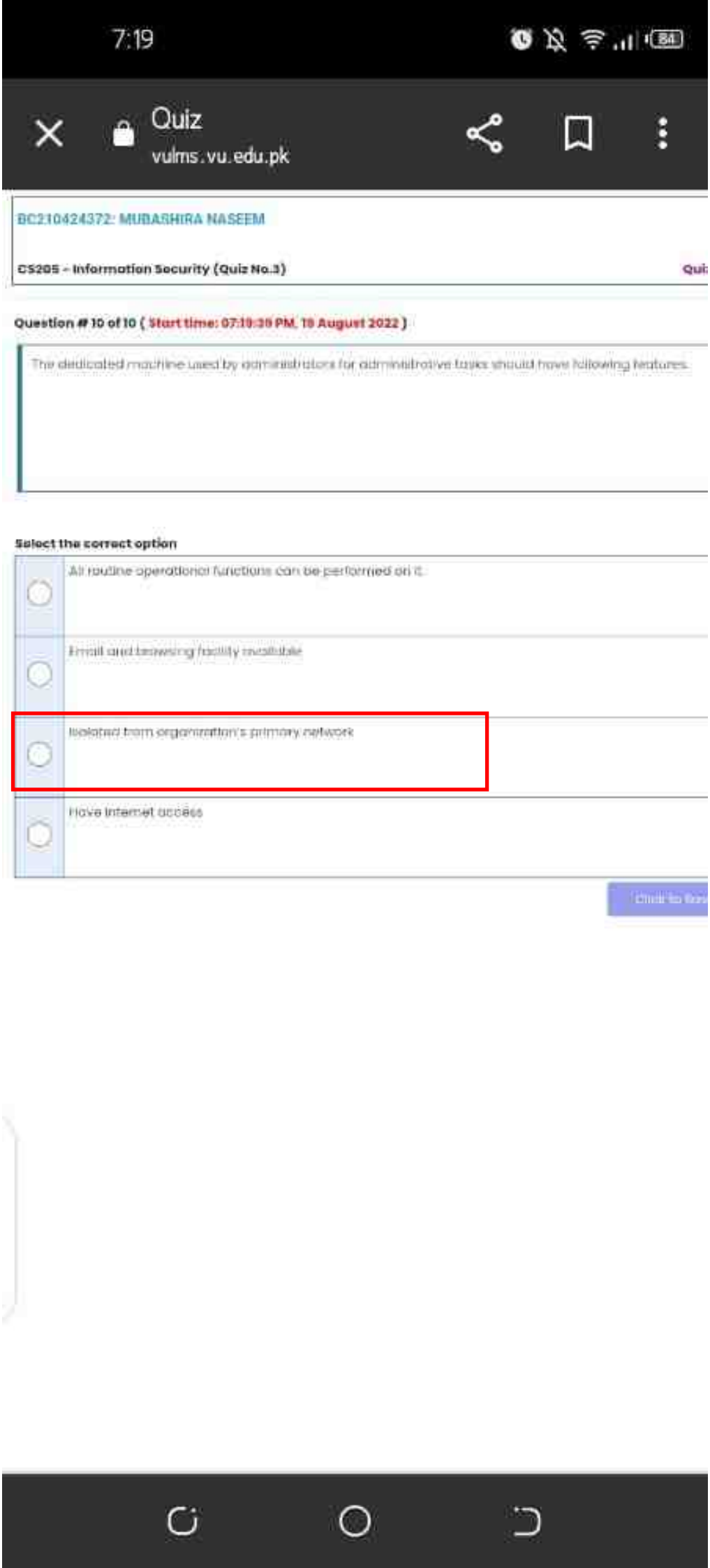

7:17
Quiz
vulms.vu.edu.pk
Question # 5 of 10 (Start time: 07:17:23 PM, 19 August 2022)
Which of the following tools can be used to enforce access controls to data?
Select the correct option
Network-based intrusion detection system
File integrity monitoring solution
Security information and event management system
Host-based data loss prevention (dlp)


7:18
Quiz
vulms.vu.edu.pk
BC210424372: MUBASHIRA NASEEM
CS205 - Information Security (Quiz No.3)
Question # 7 of 10 (Start time: 07:16:05 PM, 19 August 2022)
What type of machine should network administrators use for administrative tasks?
Select the correct option
used for composing documents
Email and browsing facility available
Have Internet access
Isolated from organization's primary network

As per malware defense control why DNS query logging should be enabled?

Select the correct option

- To detect host-name lookup for known malicious domains
- Continuously monitor and defend organization's servers and workstations
- analyze and block inbound email attachments with malicious behavior
- To lower the chance of spoofed or modified emails from valid email addresses


7:19
Quiz
vulms.vu.edu.pk
BC210424372: MUBASHIRA NASEEM
CS205 - Information Security (Quiz No.3)
Question # 10 of 10 (Start time: 07:19:39 PM, 18 August 2022)
The dedicated machine used by administrators for administrative tasks should have following features
Select the correct option
All routine operational functions can be performed on it
Email and browsing facility available
Isolated from organization's primary network
Have Internet access