



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



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

[Click to Save Answer &](#)



vulms.vu.edu.pk/

**Question # 2 of 10 (Start time: 06:49:13 PM, 16 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

[Click to Save](#)

**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

- | | |
|-----------------------|--------------------------|
| <input type="radio"/> | Public cloud storage |
| <input type="radio"/> | Authorized cloud storage |
| <input type="radio"/> | Hybrid cloud storage |
| <input type="radio"/> | Private cloud storage |

[Click to Save](#)

Question # 2 of 10 (Start time: 06:46:48 PM, 18 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



vulms.vu.edu.pk/Quiz/QuizC

13





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

- | | |
|-----------------------|-----------------------|
| <input type="radio"/> | Authenticated mode |
| <input type="radio"/> | Deep scan mode |
| <input type="radio"/> | Dedicated mode |
| <input type="radio"/> | 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 S





Which cis control is described in this module?

Select the correct option

- | | |
|-----------------------|----------------------------|
| <input type="radio"/> | Malware defenses |
| <input type="radio"/> | Data recovery capabilities |
| <input type="radio"/> | Wireless access control |
| <input type="radio"/> | Boundary defenses |

click





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



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](#)

vulms.vu.edu.pk/Quiz/QuizC

13





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





BC210428185: 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 :

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 (ids)
- 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 be compliant with which protocol to streamline reporting?

Select the correct option

- | | |
|-----------------------|-------|
| <input type="radio"/> | Scap |
| <input type="radio"/> | Cis |
| <input type="radio"/> | Fisma |
| <input type="radio"/> | 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

- | | |
|-----------------------|--|
| <input type="radio"/> | Requires very less time and effort |
| <input type="radio"/> | Consists of complicated security activities which take more time and effort. |
| <input type="radio"/> | Its not very beneficial to implement so kept at the later stage |
| <input type="radio"/> | 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

- | | |
|-----------------------|---|
| <input type="radio"/> | Which require bio-metrics for authentication |
| <input type="radio"/> | Which require mutual multi-factor authentication |
| <input type="radio"/> | Which require digital certificates for authentication |
| <input type="radio"/> | 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

- | | |
|-----------------------|----------------|
| <input type="radio"/> | Foundational |
| <input type="radio"/> | Advanced |
| <input type="radio"/> | Organizational |
| <input type="radio"/> | 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](#)

Each person with administrator account should be authorized by?

Select the correct option

<input type="radio"/>	Senior executive
<input type="radio"/>	Help-desk team
<input type="radio"/>	Network administrator
<input type="radio"/>	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: 1

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

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

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

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

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

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

Cis cat pro

Fim

Active directory

Click to Save Answer & Move to Next Question

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

- | | |
|-----------------------|-------------------------|
| <input type="radio"/> | Basic controls |
| <input type="radio"/> | Organizational controls |
| <input type="radio"/> | Foundational controls |
| <input type="radio"/> | Advanced controls |

Click to Save Answer & Move to Next Question

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

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

- | | |
|-----------------------|-----------------------------------|
| <input type="radio"/> | On-site devices |
| <input type="radio"/> | Mobile devices |
| <input type="radio"/> | Off-site devices |
| <input type="radio"/> | Each of the organization's system |

Click to Save Answer & Move to Next Question

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

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

Total Marks: 1

Automated configuration monitoring tools should be 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

4G

Quiz
vulms.vu.edu.pk



SC210437967: SAMINA YAQOUB

Time left: 08 min(s)

CS305 - Information Security (Quiz No.3)

Quiz Start Time: 02:49 PM, 19 August 2022

Question # 1 of 10 (Start time: 02:49:54 PM, 19 August 2022)

Total Marks: 1

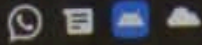
Which of the following can be used to look for unusual attack mechanisms on organizations' network boundaries?

Select the correct option

- Host-based intrusion prevention (HIPS) system
- Network-based intrusion detection (NIDS) sensor
- Network-based intrusion prevention (NIPS) system
- Host-based intrusion detection (HIDS) sensor

Click on Submit Answer to Submit to Inset Question

2:50



Quiz

vulms.vu.edu.pk



BC2T642T667: SAMINA YADOOB

Time left 72 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:49 PM, 19 August 2022

Question # 1 of 10 (start time: 02:49:54 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?

Empty text input field for the question answer.

Select the correct option

- Host-based intrusion prevention (HIPS) systems
- Network-based intrusion detection (NIDS) sensors
- Network-based intrusion prevention (NIPS) systems
- Host-based intrusion detection (HIDS) sensors

Click on Score, Answer & Move to next Question

BC219477807: SAMINA YAQOOB

Time Left 46 sec(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:49 PM, 19 August 2022

Question # 1 of 10 (Start time: 02:49:54 PM, 19 August 2022)

Total Marks: 1

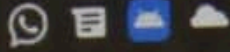
Which of the following can be used to look for unusual attack mechanisms on organization's network boundaries?

Select the correct option

- Host-based intrusion prevention (HIPS) systems
- Network-based intrusion detection (NIDS) sensors
- Network-based intrusion prevention (NIPS) systems
- Host-based intrusion detection (HIDS) sensors

Click to give answer & Move to next Question

2:51



Quiz
vulms.vu.edu.pk



IC210427607: SAMINA YAQOUB

Time Left 80
sec(s)

ICS205 - Information security (Quiz No.3)

Quiz Start Time: 02:49 PM, 19 August 2022

Question # 2 of 10 (Start time: 02:51:16 PM, 19 August 2022)

Total Marks: 1

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 version of OS only
- Hardened versions of OS only

Click to Show Answer & Move to Next Question



BC213427607, SAMINA YAGDOOB

Time Left 78 sec(s)

CS205 - information security (Quiz No.3)

Quiz Start Time: 02:49 PM, 19 August 2022

Total Marks: -

Question # 3 of 10 (start time: 02:52:07 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 same password on all the systems
- Use short passwords which are easy to remember
- Use passwords longer than 14 characters

Click to Show Answer & Move to Next Question



BC210427607 SAMINA YAQOUB

Time left 86 sec(s)

cs205 - information security (Quiz No.1)

Quiz Start Time: 02:49 PM, 19 August 2022

Question # 4 of 10 (start time: 02:52:01 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

- Mobile devices
- CD-ROM devices
- On-site devices
- Each of the organization's systems

[Click to view answer & Move to next Question](#)



Quiz

vulms.vu.edu.pk

BC210427607: SAMINA YAQOUB

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 organization

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

Click to Start



210427687 SAMINA YAQOOB

Time Left 67
sec(s)

005 - Information Security (Quiz No.1)

Quiz Start Time: 02:48 PM, 19 August 2022

Question # 6 of 10 (Start time: 02:54:26 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 be on priority basis?

Select the correct option

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

Click to Save Answer & Move to Next Question

2:55



Quiz
vulms.vu.edu.pk



BC219427987 SAMINA YAQOUB

Time Left
4:1

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:49 PM, 19 August 2022

Question # 8 of 10 (Start time: 02:54:28 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

Medium risk vulnerabilities

Low risk vulnerabilities

High risk vulnerabilities

Click to Show Answer & Move to Next Question

2:55

4G



Quiz
vulms.vu.edu.pk



BU210427607 - SAMINA YAQOUB

Time Left: 85
min(s)

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:49 PM, 19 August 2022

Question # 7 of 10 (Start time: 02:55:45 PM, 19 August 2022)

Total Marks:

In which mode should vulnerability scanning be performed?

Select the correct option

Authenticated mode

Deep scan mode

Declassified mode

Non-Authenticated mode

Click to Show Answer & Solve the Next Question!



BC210427607: SAMINA YAQOUB

Time Left 83

Cs205 - Information Security (Quiz No.3)

Quiz Start Time: 02:49 PM, 19 August 2022

Question # 8 of 10 (start time: 02:56:48 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 network-based intrusion detection system(ips)
- Through antivirus
- Through network-based intrusion prevention system(ips)
- Through system firewall

Click to Save Answer & Move to Next Question



BC219427607: SAMINA YAQOOB

Time Left 82

CS205 - Information Security (Quiz No.3)

Quiz Start Time: 02:49 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

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

Click on Show Answer & Move to Next Question



BC210427687: SAMINA YAQOUB

Time Left 5:4
sec(s)

CS305 - Information Security (Quiz No.3)

Quiz Start Time: 02:49 PM, 19 August 2022

Question # 10 of 10 (Start time: 02:58:41 PM, 19 August 2022)

Total Marks: 1

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

Select the correct option

Public cloud storage

Private cloud storage

Hybrid cloud storage

Authorized cloud storage

Click on Give Answer & Move to Next Question



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

Total

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



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 Next

CS205 - Information security (Quiz No.3)

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

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

Total Marks: 10

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 of systems at organization's network boundaries

Click to Save Answer & Move to Next Question

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 Quest



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 to Next Question](#)



0321942777: MAHMOOD WAQAR

Time Left 00 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)

Total

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 Question

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 2022

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

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



Question # 1 of 10 (start time: 03:18:06 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

- 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

Question # 2 of 10 (Start time: 03:19:42 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

Question # 3 of 10 (Start time: 03:20:28 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

- 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](#)

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



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

- | | |
|-----------------------|--|
| <input type="radio"/> | Network-based intrusion detection system |
| <input type="radio"/> | File integrity monitoring solution |
| <input type="radio"/> | Security information and event management system |
| <input type="radio"/> | Host-based data loss prevention (dip) |

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)

CS205 - 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





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

- | | |
|-----------------------|--|
| <input type="radio"/> | Through network-based intrusion detection system(ips) |
| <input type="radio"/> | Through system firewall |
| <input type="radio"/> | Through network-based intrusion prevention system(ips) |
| <input type="radio"/> | Through antivirus |

[Click to Save Ans](#)

**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

- | | |
|-----------------------|---|
| <input type="radio"/> | Deny communication over unauthorized TCP ports |
| <input type="radio"/> | Deny communication with all open ports |
| <input type="radio"/> | Deny communication over unauthorized UDP ports |
| <input type="radio"/> | Deny communication over unauthorized TCP or UDP ports |

Click

**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

<input type="radio"/>	Data protection
<input type="radio"/>	Boundary defense
<input type="radio"/>	Malware defense
<input type="radio"/>	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



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

- | | |
|-----------------------|-------|
| <input type="radio"/> | Scop |
| <input type="radio"/> | Cis |
| <input type="radio"/> | Disa |
| <input type="radio"/> | 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

<input type="radio"/>	Should block that account
<input type="radio"/>	Should not allow
<input type="radio"/>	Issue a log entry and alert
<input type="radio"/>	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

<input type="radio"/>	Used for composing documents
<input type="radio"/>	Isolated from organization's primary network
<input type="radio"/>	Have internet access
<input type="radio"/>	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

- | | |
|-----------------------|------------------|
| <input type="radio"/> | Puppet |
| <input type="radio"/> | Active directory |
| <input type="radio"/> | Fim |
| <input type="radio"/> | 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

- | | |
|-----------------------|---|
| <input type="radio"/> | Hard drive of mobile devices should be encrypted |
| <input type="radio"/> | Mobile devices should not be allowed |
| <input type="radio"/> | Employees should use only personal mobile devices |
| <input type="radio"/> | Mobile devices are allowed for higher management only |

[Click to](#)



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

Total

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

select the correct option

Off-site devices

On-site devices

Mobile devices

Each of the organization's system

Click to Save Answer & Move to Next Question





CS205 - Information Security (Quiz No.3)

Quiz Start Time: 04:20 PM, 19 August 2022

Question # 2 of 10 (Start time: 04:22:20 PM, 19 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

Click to Save Answer & Move to Next Question



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

Total Marks

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 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



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





Question # 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?

Select 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





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



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





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



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 2022

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

- | | |
|-----------------------|------------------|
| <input type="radio"/> | Fim |
| <input type="radio"/> | Cis cat pro |
| <input type="radio"/> | Active directory |
| <input type="radio"/> | 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

as a fixed time of 90 seconds. So you have to save your answer before 90 seconds. But due to unstable internet, you may lose 10-15 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. Therefore, it is the best option.

Back Button / Backspace Button while attempting a question, otherwise you will lose that question.

the page unnecessarily, **specially** when following messages appear:

Logout: Now loading next question...

JavaScript must be enabled in your browser, otherwise you will not be able to attempt the quiz.

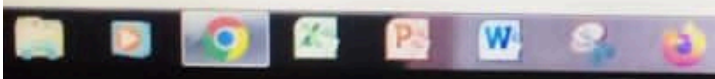
if you lose access to internet (like power failure or disconnection of internet), you will be able to attempt the quiz only if that you have to complete the quiz before expiry of the deadline.

failed to attempt the quiz in given time then no re-take of offline quiz will be held.

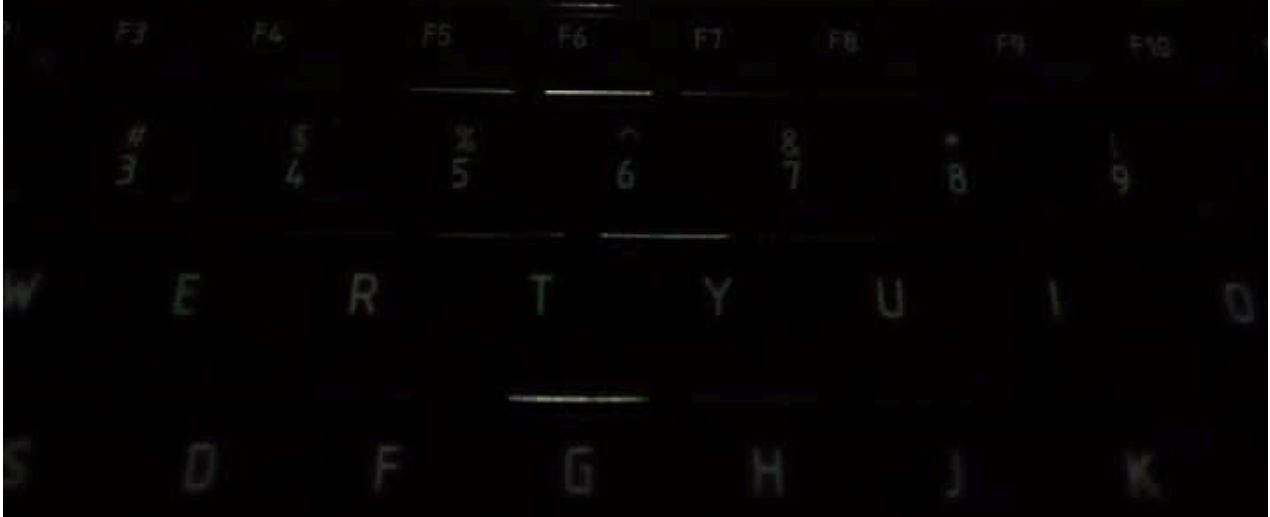
Academic Integrity

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 (i.e. helping tools, etc.) action will be made against such student(s) including cancellation of their quiz.



TOSHIBA



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



TOSHIBA

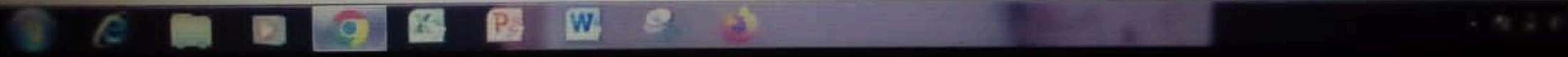
Question # 2 of 10 (Start time: 04:45:35 PM, 19 August 2022)

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

Click to show answer 0/0





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 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](#)



BC210426997: ISRA HUMA

CS205 - Information Security (Quiz No.3)

Quiz Start Time

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 Answer](#)

Search...





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



Search...





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



Search...





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



Search...





Question # 6 of 10 (Start time: 06:40:56 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 Answer





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

Click

Search...





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

[Click to](#)



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

B

Search...





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

Search...



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 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](#)

vulms.vu.edu.pk/Quiz/QuizS

13



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

[Click to Save Ans](#)



vulms.vu.edu.pk/Quiz/QuizC

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



vulms.vu.edu.pk/Quiz/QuizC

13



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

Click to Save Answer & Move to Next



vulms.vu.edu.pk/Quiz/QuizC

13



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 the later stage

Click to Save Answer & Move



vulms.vu.edu.pk/Quiz/QuizC

13



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

[Click to Save Answer & Move to Next Question](#)



vulms.vu.edu.pk/Quiz/QuizC

13





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

Click to Save



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
- Ffilec
- Scap
- Cis

Click to Solve



vulms.vu.edu.pk/Quiz/QuizC

13



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/QuizC

13



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 addresses
- To detect host-name lookup for known malicious domains

Question # 3 of 10 (Start time: 07:01:56 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

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

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

- Dns
- Cis
- Scap
- Fisma



Type here to search



33°C

BC210424460: FAIZA MUBEEN

CS205 - 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 addresses
- To detect host-name lookup for known malicious domains

Question # 8 of 10 (Start time: 07:03:26 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
- Require super admin rights
- Issue a log entry and alert



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](#)



Question # 8 of 10 (Start time: 07:04:19 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



Click



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

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, 18 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

- | | |
|-----------------------|------------------------------------|
| <input type="radio"/> | All the assets in asset inventory |
| <input type="radio"/> | Software assets in asset inventory |
| <input type="radio"/> | Active directory domain |
| <input type="radio"/> | Hardware assets in asset inventory |

[Click to Save Answer & Move to Next Question](#)

Question # 7 of 10 (Start time: 07:08:13 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



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

- | | |
|-----------------------|-----------------------------------|
| <input type="radio"/> | Each of the organization's system |
| <input type="radio"/> | Off-site devices |
| <input type="radio"/> | On-site devices |
| <input type="radio"/> | 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: 07:06:58 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



Question # 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?

Select 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 (dip)
- Network-based intrusion detection system

[Click to Save](#)



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](#)



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

Click to





Question 10/10 (Start time: 07:12:44 PM, 15 August 2022)

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, 19 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





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?

Select the correct option

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

Click to Save An



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

- | | |
|-----------------------|-----------------------------|
| <input type="radio"/> | Require super admin rights |
| <input type="radio"/> | Issue a log entry and alert |
| <input type="radio"/> | Should block that account |
| <input type="radio"/> | Should not allow |



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

Click to Save





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

- | | |
|-----------------------|--|
| <input type="radio"/> | Boundary defense |
| <input type="radio"/> | Data protection |
| <input type="radio"/> | Malware defense |
| <input type="radio"/> | Secure configuration for network devices |



Question # 5 of 10 (Start time: 07:16:40 PM, 19 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



Question # 6 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

- | | |
|-----------------------|--|
| <input type="radio"/> | Network-based intrusion detection system |
| <input type="radio"/> | File integrity monitoring solution |
| <input type="radio"/> | Security information and event management system |
| <input type="radio"/> | Host-based data loss prevention (dlp) |

Click





BC210424372: MUBASHIRA NASEEM

CS205 - Information Security (Quiz No.3)

Quiz Sta

Question # 7 of 10 (Start time: 07:18:05 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

Click to Save A



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





BC210424372: MUBASHIRA NASEEM

CS205 - Information Security (Quiz No.3)

Qui

Question # 10 of 10 (Start time: 07:18:39 PM, 19 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

[Click to Save](#)