

CS205

فائل منسل ٹرم کرنٹ پیپر

PAID

SOVED

CURRENT

PAPER

03016812299

سر رائے افضل



_____ type of scripting languages should be used in email clients and web browsers.

Choices:

Authorized scripting languages



Client-side scripting languages



Server-side scripting languages



Scripting languages allowed by vendor



Information Security (CS205)

Question: 14 (Marks: 1)

_____ version of security related updates should be applied on network devices.

Choices:

Latest

☐

Default

☐

Latest and stable

☐

Oldest

☐

Information Security (CS205)

Question: 15 (Marks: 1)

All network traffic to or from the internet must pass through _____ to filter unauthorized connections.

Choices:

☐ Application layer filtering proxy

☐ Session layer filtering proxy

☐ Network layer filtering proxy

☐ System layer filtering proxy

The function most closely associated with the "soc" is _____.

Choices:

☒ Security management

☐ Security engineering

☐ Security frameworks

☐ Security operations

Information Security (CS205)

Question: 19 (Marks: 1)

Assigning resources, assigning roles, and communicating roles fall under _____ clause.

Choices:

☐ Support

☐ Leadership

☐ Performance evaluation

☐ Operation

Creating awareness related to policy and isms fall under _____ clause.

Choices:

Support



Operation



Performance evaluation



Leadership



Creating awareness related to policy and isms fall under _____ clause.

Choices:

☐ Support

☐ Operation

☐ Performance evaluation

☐ Leadership

The objective of COBIT is to help organizations_____.

Choices:

Create optimal value from it by balancing benefits with risk



Implement a strong governance of it



Manage it effectively while ensuring business continuity



Create a single page it dashboard

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

Choices:

Approved security configuration

☐

Recommended security configuration by vendor

☐

Latest security configuration released by vendor

☐

Latest security configuration released by vendor

Controlling planned changes and risk assessment fall under _____ clause.

Choices:

☐ Leadership

☐ Support

☐ Operation

☐ Performance evaluation

Information Security (CS205)

Question: 22 (Marks: 1)

Monitoring, measurement, and analysis fall under _____ clause.

Choices:

Support



Leadership



Performance evaluation



Operation

Employee screening should be conducted _____.

Choices:

After employment (hiring)



Prior to employment (hiring)



During employment (hiring)



Which of the following come under equipment physical and environmental security controls?

Choices:

☐ Working in secure areas

☐ Secure delivery and loading areas

☐ Clear desk and clear screen policy

☐ Physical entry controls

Owasp software assurance maturity model (samm) undertakes software security testing and validation during_____.

Choices:

☐ Governance and deployment

☐ Governance and verification

☐ Verification and deployment

☐ Construction and governance

_____ is the sixth layer of cyber security maturity matrix.

Choices:

☒ Monitored

☐ Secured

☐ Protected

☐ Hardened

_____ is the fifth layer of cyber security maturity matrix.

Choices:

☒ Monitored



☐ Hardened



☐ Protected



☐ Foundation



The enterprise technology governance and risk management framework is considered combination of _____.

Choices:

☐ COBIT, ITIL, ISMS ISO27002

☐ COBIT, ITIL, ISMS ISO27001

☐ COBIT, ITIL, PCI-DSS

☐ ITIL, ISACA, NIST

TIME LEFT

78

Click here to search

Stage 2 of security transformation model refers to _____.

Choices:

Security governance



Security engineering



Security hardening



Vulnerability management



_____ is the goal of performing vulnerability assessment.

Choices:

☒ To fix as many things as possible as efficiently as possible

☐ Testing security that is assume to be secure

☐ Technical assessment designed to achieve specific goal

☐ Focuses on how an existing configuration is compared to a standard

PHP security guidelines cover which type of attacks?

Choices:

Denial of service attacks



Brute force attacks



Injection attacks



Dictionary attacks



_____ is the goal of performing audit.

Choices:

☐ Testing security that is assumed to be secure

☐ Technical assessment designed to achieve specific goal

☐ To fix as many things as possible as efficiently as possible

☐ Focuses on how an existing configuration compares to a standard

Complex passwords should be enforced to survive_____.

Choices:

Dictionary attacks



Injection attacks



Dos attacks



Phishing attacks



_____ are considered types of security assessment.

Choices:

☒ Threat simulation

☐ Threat assessment

☐ Threat intelligence

☐ Logs collection and analysis

There are _____ benefits of version controlling.

Choices

☒ Seven

☐

☐ Eight

☐ Nine

☐ Ten

There are _____ benefits of version controlling.

Choices:

Seven



Eight



Nine



Ten



_____ assessments is designed to determine whether an attacker can achieve specific goals when facing your current security posture.

Choices:

☐ Threat assessment

☐ Bug bounty hunting

☐ Penetration testing

☐ Red team exercise

How many steps are involved in policy compliance scan of qualys?

Choices:

Three



Four



Five



Six



_____ are the key benefits of security transformation project implementation to an organization.

Choices:

☒ IT teams get experience and aware of security

☐ Prevention of attacks

☐ IT teams get incentives

☐ Management becomes aware of IT team's capability

Question: 5 (Marks: 1)

_____ protocol is used for assigning addresses dynamically.

Choices:

DCP



HTTP



DHCP



IP

_____ are the key benefits of security transformation project implementation to an organization.

Choices:

☒ IT teams get experience and aware of security

☐ Prevention of attacks

☐ IT teams get incentives

☐ Management becomes aware of IT team's capability

As per security lifecycle, validation activity should be performed _____.

Choices:

Before applying controls



After applying controls



Periodically



Annually

Information Security (CS205)

Question: 34 (Marks: 1)

To prevent attacks, fraud and pilferage an effective information security transformation program is essential for _____.

Choices:

☒ IT organizations

☐ Medium-sized organizations

☐ Small-sized organizations

☐ Any organization having IT setup

Information Security (CS205)

Question: 7 (Marks: 1)

Vulnerability management is _____ steps cycle.

Choices:

Three



Four



Five



Six



_____ is the recommended timeline for effective information security transformation program.

Choices:

☐ 15 months

☐ 18 months

☐ 12 months

☐ 6 months

Question: 8 (Marks: 1)

Stage 2 of security transformation model refers to _____.

Choices:

☒ Security governance



☐ Security engineering



☐ Security hardening



☐ Vulnerability management



_____ plays an instrumental role in success of information security transformation program.

Choices:

☐ IT team led by CIO

☐ Business team

☐ Internal audit team

☐ Higher management

For how many days NISSUS scanner offers trial version?

Choices:

7 days

☒

15 days

☐

30 days

☐

45 days

Information Security (CS205)

Question: 40 (Marks: 1)

Candidness quality of infosec head means that he _____.

Choices:

Promote performance and merit

☐

Encourage solo-flight of team members

☐

Honesty and straight talk

☐

Adjust players in right position

☐

Information Security (CS205)

Question: 38 (Marks: 1)

_____ action is recommended for organizations having very good security posture and have score higher than 85%.

Choices:

☒ Go for risk assessment



☐ Third party security review



☐ Go for is027001 certification



☐ Information security transformation program



Information Security (CS205)

Question: 10 (Marks: 1)

At _____ layer of transformation model CIS critical security controls are implemented.

Choices:

Security governance

☐

Security engineering

☐

Vulnerability management

☐

Security hardening

☐

Question: 11 (Marks: 1)

_____ should be deployed to limit and control that which devices can be connected to the network.

Choices:

802.1x

☐

802.11g

☐

802.11b

☐

802.11n

☐

Inventory of authorized and unauthorized software control requires making a list of _____.

Choices:

☐ Authorized asset and version

☐ Authorized operating system and version

☐ Authorized software and version

☐ Unauthorized software and version

An authentic information security head always _____.

Choices:

☒ Take credit of everything

☐ Never admit mistakes and failure

☐ Give credit where it is due

☐ Very strict and disciplined

Candidness quality of infosec head means that he _____.

Choices:

☐ Promote performance and merit

☐ Encourage solo-flight of team members

☐ Honesty and straight talk

☐ Adjust players in right position

Information Security (CS205)

Question: 48 (Marks: 5)

Following table contains some characteristics of exploits that cause security breaches. You are required to identify the type of exploit as Local or Remote for each of the given characteristics.

Characteristics	Exploit Type (Local / Remote)
Requires prior access to the vulnerable system	
Works over a network	
Does not require any prior access to the vulnerable system	
Exploit initiated through the Internet	

Answer:



Answer :

|

Write the name of first layer of the Cyber Security Maturity Model/Matrix (CSMM)?

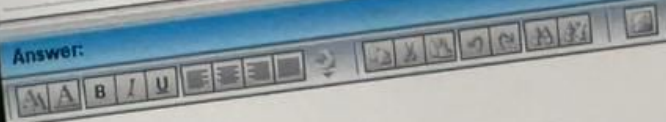
Answer:



Identify any two security functions from the given list for which asset management helps:

1. Network Congestion
2. Patch Management
3. Identification of future Viruses
4. Enterprise tracking and reporting
5. Internal IP fragmentation

Answer:



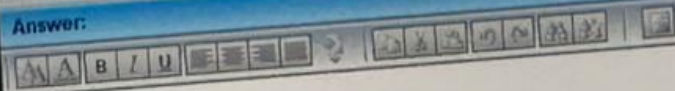
administrator:
System (1) Pro
Place webcam
Use wired mo
nothing attac
strictly not a
Immediately
Violation of
Report soft
"overseas
https://joi
Sent at 09:
me: AOA
Sent at 09:
me: 1 230
Sent at 0
me: Any
Sent at 1
me: Sir
Sent at
me: hel
Sent at
Muzzan
Sent a

Information Security (CS205)

Question: 42 (Marks: 3)

Which vulnerability scanner is used to look for both code-based and configuration-based vulnerabilities?

Answer:



Information Security (CS205)

Question: 43 (Marks: 3)

Which of the following phases are not part of the Security Hardening Life cycle?

- Harden IT Asset
- Implement Risk Generation
- Periodic Validation
- Implement Additional Controls
- Seed Additional Threats

Answer:



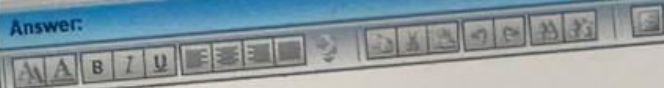
Information Security (CS205)

Question: 43 (Marks: 3)

Which of the following phases are not part of the Security Hardening Life cycle?

- Harden IT Asset
- Implement Risk Generation
- Periodic Validation
- Implement Additional Controls
- Seed Additional Threats

Answer:



Information Security (CS205)

Question: 44 (Marks: 3)

The QualysGuard scanning methodology focuses on different steps / tests. You are required to write the name of the second test involved in this scanning methodology.

Answer:



Information Security (CS205)

Question: 41 (Marks: 3)

Mention the names of security testing.

Answer:



Information Security (CS205)

Question: **50** (Marks: 5)

The following table shows the responsibilities of typical organizational tiers. You are required to mention the tier (Board or IT Management) associated with each responsibility.

Responsibility	Board / IT Management
Organizational Commitment	
Review	
Approve Budget	
Monitor	

Answer:



Information Security (CS205)

Question: 49 (Marks: 5)

The following table shows a list of security engineering activities and the teams who perform these activities but currently this list is mismatched. You are required to correctly match these activities with the associated teams and rearrange the given table:

ACTIVITY	TEAM
Security requirements	Network/IT security assisted by vendor
Security design	Information security with IT consultation
Security implementation	Information security team
Validating security requirements	Network/IT security assisted by vendor

Answer:



ACTIVITY TEAM

Security requirements Information security with IT consultation

Security design Information security team

Security implementation Network/IT security assisted by vendor

Validating security requirements Information security team

Here's a brief explanation for each match:

- **Security requirements:** Typically defined by Information security with IT consultation to ensure alignment with organizational goals.
- **Security design:** Designed by the Information security team, who are responsible for developing security architectures.
- **Security implementation:** Implemented by Network/IT security assisted by vendor, as they have the technical expertise to configure and deploy security controls.
- **Validating security requirements:** Validated by the Information security team, who ensure that the security requirements are met and aligned with the organization's security posture.

Question 43

Solution:

The phase that is not part of the Security Hardening Life cycle is:

- Implement Risk Generation

Question 44

Solution:

The second test involved in the QualysGuard scanning methodology is:

- Service Discovery

Question 45

Solution:

Two security functions for which asset management helps are:

1. Patch Management
2. Enterprise tracking and reporting

Responsibility	Board/IT Management
Organizational Commitment	Board
Review	IT Management
Approve Budget	Board
Monitor	Board

- **Organizational Commitment:** The Board is responsible for setting the overall direction and commitment to security.
- **Review:** IT Management reviews the implementation and effectiveness of security controls.
- **Approve Budget:** The Board approves the budget for security initiatives and ensures adequate resources are allocated.
- **Monitor:** The Board monitors the overall security posture and ensures that security risks are properly managed.

Question: 46 (Marks: 3)

Write the name of first layer of the Cyber Security Maturity Model/Matrix (CSMM)?

Solution:

The first layer of the Cyber Security Maturity Model/Matrix (CSMM) is "**Initial**".

Question: 48 (Marks: 5)

Following table contains some characteristics of exploits that cause security breaches you are required to identify the type of exploit as local or Remote for each of the given characteristics.

Characteristics	Exploit Type (Local/Remote)
Requires prior access to the vulnerable system	Local
Works over a network	Remote
Does not require any prior access to the vulnerable system	Remote
Exploit initiated through the Internet	Remote

Question 41

Solution:

Some common types of security testing include:

- Vulnerability Testing
- Penetration Testing
- Risk Assessment
- Compliance Testing
- Security Auditing

Question 42

Solution:

The vulnerability scanner used to look for both code-based and configuration-based vulnerabilities is:

- Nessus

Cs205 Final Term key 2025



01	C	11	A	21	A	31	B
02	A	12	C	22	C	32	D
03	B	13	B	23	B	33	B
04	B	14	C	24	D	34	D
05	C	15	A	25	C	35	C
06	B	16	A	26	A	36	D
07	C	17	A	27	A	37	—
08	A	18	D	28	B	38	D
09	C	19	A	29	A	39	C
10	D	20	┘	30	D	40	C

