CS 205 Fall 2024 File Objective Subjective 2024

CS 205 Mid-Term Objective File by M. Qasim Ali 3337435091

U tube channel QASIM KHAN WORLD

MCQS: 1. --------- an attack in which attacker alter the system resources is called are?

A. Active attack

B. Passive attack

C. Direct attack

D. Indirect attack

2. Students are not Allowed to bring cell phone in the exam hall is example of?

A. Security Policy

B. Security Council

C. Security mechanism

D. Security service

3. ---------- are three pillars of information security?

ANS: confidentiality, integrity, availability.

4. Ransom ware is _____?

Ans: Is a type of attack that encrypt data on computers and servers.

5. NESSUS tool is used at _____ layer in information security transformation framework?

A. Security governance

B. Security engineering

C. Vulnerability management.

D. Security hardening

6. _____ mean effective management of security program?

A. Sec governance

B. Sec engineering

C. Vulnerability management.

D. Sec hardening

7. Which of the following will be considered the most specific standard / framework applicable only to specific type of industry?

A. ISO27002.2013

B. COBIT

C. PCI.DSS

D. ISO27001.2013

8. Which of the following may be applied to any type of industry in which information technology is being used?

A. ISO27002.2013

B. COBIT, and ISMS

C. COBIT, ISMS, PCI

D. PCI, DSS, ISMS

9. ____are challenges of information security?

A. Lack of budget and insufficient resources allocation

B. Highly specialized and continuously changing technology

C. Cloud and IOT

D. lack of owner ship, department silos, missing security hardening

10. There are ____ main steps in information security life cycle

A. 6

B. 7

C. 9

D. 11

11. Regionally the most well developed cyber security strategy and framework Developed by Malaysia is at rank _____?

A. 1

B. 2

C. 3

D. 4 12. ____ is prevention of the unauthorized use of a resource?

A. Access control

B. Data integrity

C. non repudiation

D. availability

13. The next generation firewall should be placed at _____?

A. Inside the data center

B. Where it is physically secret

C. Inside the DMZ

D. At the network perimeter and at the entrance to the data center

14: Major security function performed be the perimeter NGN firewall are____?

A. Web sec and email sec.

B. Malware filtering, access list fur traffic filtering band width filtering

C. Wan interface

D. APPT attack prevention

15. The key challenges with mobile technology is that _____?

A. It Is leading to wastage of time and distraction

B. Traditional enterprise security perimeter boundary has disappeared.

C. Location the user can be tracked

D. Apps on mobile device may be Trojans.

16. The recommend manners to protect sensitive data with a VM is to

A. Encrypt data stored on workstation

B. Encrypted stored on virtual and cloud servers.

C. Encrypt data stored on USB

D. Encrypt data stored file servers

17. One of the main challenge in small sized organization related to security is_____?

A. Lack of fund data center

B. Lack of budget and resources allocate for security.

C. Lack of security vender

D. Lack of security devices

18. At which point a malicious entity/ black hat hackers attack for website defacement in an IT network____?

A. Edge router or edge firewall

B. Web server in DMZ

C. Email gate way

D. Data center switch

19. How web and email can be secured against malware and attacks in and Enterprise IT network?

A. BY blocking unauthorized traffic at edge

B. By keeping a good and updated solution

C. By using web security an email ant spam gateway

D. By using malware protection at edge.

20. _____ are the main phases/steps in a business continuity life cycle.

A. analysis, design, implement and validate

B. id entity, analyze, design, execute

C. Id entity, analyze, design, and execute, measure,

D. Analyze, implementation and valid ate

21. _____ enterprises have their own vulnerability scanner?

A. 90%

B. 75%

C. 50%

D. 5%

22. _____ project sequence is followed in information projects.

A. Establish track, implement across IT

B. Pilot, implement across IT, continues improvement.

C. Establish track, MSB, pilot, implement across IT, continues improvement

D. Establish track, MSB, implement across IT

23. ____ category has maximum number of CIS benchmark

A. Operating system 36

B. Mobile device.

C. network device.

D. Cloud providers

24. _____ category has minimum number of CIS benchmark

A. Multifunction print device. 01

B. mobile device

C. network device.

D. Cloud provider

25. What does audit explain abut control in CIS benchmark?

A. Describe the control

B. Describe the benefit

C. Tells how to check the controls.

D. Tells how to apply controls

26. According to applicability CIS device control in _____ category?

A. Level1 and level 2

B. Scored and unscored.

C. Cat1, Cat2, Cat3

D. High critical, low critical

27. Frequency of updating the signature file for antivirus program must be set to ___?

A. Daily basis

B. weekly basis

C. fortnightly basis

D. Monthly basis

28. The direct console user interface should be _____ ?

A. Disable

B. Enable

C. Partially enabled

D. Monitored

30. Internationalized domain name are displayed as

A. Little ENDIAN

B. Big ENDIAN

C. UTFr32

D. UNICODE

31. Information security is combination of _____?

ANS: People process and technology

32. Under which category of CIS benchmark MS window servers fall?

A. server software

B. Mobile device

C. Operating system

D. Cloud providers

33. OWASP, cloud security alliance, ISACA and ISC2 are example of _____?

A. Cyber security government organization

B. cyber security professional associations

C. Research organization

D. International security operations

34. MS Exchange serve falls under _____ category of CIS benchmark.

A. Operating system

B. server software

C. Desktop software

D. Cloud providers

35. What is the function of active directory AD in an enterprise network?

A. Pushing out security policies through GPO

B. Windows update and configurations

C. Log collections and analysis

D. Network operation and performance management (not sure) r can also verify.

36. DISA gives us the following features set as compared to CIS

A. Excellent control coverage with some useable terminology

B. User friendly and for small/medium size organization

C. Good control with no useable terminology (Nut sure may be A. see comparison table)

D. Cat tool to check the compliance with standard

37. N+1 redundancy pattern is sometimes referred As_____?

A. High Availability

B. parallel redundancy

C. active passive

D. Active Active

38. The best Model in Pakistan to effectively address the weakness in the cyber security is to adopt_____?

A. ISMS

B. Four layer security transformation

C. COBIT

D. CIS security benchmarks

39. _____ is technique used to gain unauthorized access to computer, wherein the intruder send messages with a source IP address that has been forged to indicate that the messages are coming from a trusted source?

A. Man in middle

B. Denial of the service

C. Zombie

D. Spoofing

40. The key and most important element in the management process is ____r?

A. Risk documentation

B. Risk determination

C. Risk assessment

D. Risk policy

41. _____ is the first layer in the information security transformation framework?

A. Security governance

B. security engineering

C. Vulnerability management

D. Security hardening

42. Purpose of SIEM solution is _____?

A. Malware filtering, access list fur traffic filtering, bandwidth filtering

B. Log aggregation, security events dashboard, event correlation and root cause analysis

C. Log collections

D. Malicious traffic detection

43. _____ are four layers of transformation model in sequence?

Ans: Security hardening, vulnerability management, security engineering, security governance

44. Surprisingly in _____ of all organization in Pakistan (All type) security posture has been found to be deficient.

A. 80%

B. 85%

C. 90%

D. 95%

45. If a system enters into _____ state, it is a security violation.

A. initial

B. Final

C. Secure

D. Unsecure

46: CIS critical control require to ensure that ------- is take.

For improving security posture

47: is the best stage in a 3rd party penetration tasking.

System port scanning

48____ is a part of deficient program structure and cause failure of security.

ANS: Ineffective Information Security Management Committee (ISMC)

– Not taking along other stakeholders

– Inexperienced IT or security leadership

– IT team not incentivized May be any one of these options available

49: PCI data security standard applies to _____ type of organization.

ANS: card environment to protect cardholder data

ANS: All companies that accept, process, store or transmit credit card into maintain a secure environment. (Both are correct check the mcqz in exams)

50: UEM tool combine the management of multiple endpoint in a single.

ANS: Single Console

51: _____ is an open source vm tool.

ANS: OpenVAS

52**: The CISO requires well-rounded ability in ____.**

(its ans is complicated see option ans select in paper one the following given.)

(have 5-10 years' experience in IT followed by 3-5 years in Information Security, A CISO requires good people management skills as the security transformation project

53: The information security transformation project will likely fail if _____ if are not adequately address.

ANs: leadership, strategy/structure, execution

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

(i) Three
(ii) Four
(iii) Five
(iv) Six

55: how many days Nessus scanner offer trial version?

(i) 7 days
(ii) 15 days
(iii) 30 days
(iv) 45 days

56: _____ solution can be implemented to lower the chance of spoofed of modified emails from valid email address?

(i) Enterprise antivirus
(ii) Film solution
(iii) DMARC policy and verification

(iv) Next generation Firewall

57: The function most closely associated with the "SOC" is?

(i) Security management
(ii) Security engineering
(iii) Security frameworks
(iv) Security operation

58: Guidelines are an optional form of?

(i) Procedures
(ii) Work instructions (Not sure)
(iii) Standards
(iv) Policies

59: is the recommended timeline for effective information security transformation program ?

(i) 15 months
(ii) 18 months
(iii) 12 months (Actual ans is 12 to 15 month require)
(iv) 6 months

60: Enterprise Technology Governance & Risk Management Framework is a combination of
Ans:

SBP state bank of Pakistan

61: **Pakistan ranked almost at the bottom of the table in International ranking by ITU and Pakistan rank**

is 67th

49: In small sized security organization in Pakistan, It is likely the number of security stall will?

Ans: 1-5 or 2-4

50: In Medium sized security organization in Pakistan, It is likely the number of security stall will?

Ans: 10-15

51: In Large sized security organization in Pakistan, It is likely the number of security stall will?

Ans: 30

52: What was the old name ISO27002:2013?

Ans: ISO17799

Subjective Part QASIM KHAN WORLD u tube channel 03337435091

Subjective Fall 2024

Question No 01: What is information security By SANS

Ans: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

What is Security hardening Define?

Ans: Security Hardening is the process of configuring the IT assets to maximize security of the IT asset and minimize security risks

Question nu 04: How many layers involved in information security transformation frame work? You are required to write the name.

Ans: 1. **Security Hardening**; Security controls on IT assets & process

2. **Vulnerability Management**; patching

3. **Security Engineering**; More complex security design & solutions

4. **Security Governance**; Managing the information security program

Q No.03 : Write any five steps in information security programns:

Ans

- Assessing security risks and gaps
- Implementing security controls
- Monitoring, measurement, & analysis
- Management reviews and internal audit
- Accreditation/testing

Q No. 04: Who Are The Players In Information Security?

- Government
- Industry & sectors
- International organizations
- Professional associations
- Academia and research organizations
- Vendors and supplier

Q No 05: Bangladesh Bank SWIFT Hack – Feb 2016

send more than three dozen fraudulent money transfer requests.
– USD 81 million stolen
– Total impact could have been USD 1 billion

Recover 19 Million

Not claim : 81 million

Q No 06: Steps in Security engineering: (Repeated)

– Assess risk profile

– Research security solutions

– Design security architecture

– Implement security controls & solutions

– Test and validate security posture

Q No 07: Types of activities for security engineering:

• FW granular access lists

• Building an effective DMZ architecture

• Segregating the network with VLANs

• Adding a security tool such as SIEM, FW, DLP, NAC, etc

• App-DB encryption

Q No. 08: SSh protocols versions names

Description:
SSH supports 2 different and incompatible protocols:
SSH1 and SSH2.
SSH1 was the original protocol & was subject to security issues. SSH2 is more advanced and secure.

Q No 09: Info security Governance Block.

Initial

- Policy
- Responsibility
- Recourse and priority
- Periodic review

Intermediate

- Change management
- SOP,s
- Awareness

Monitoring

Mature

- Risk management
- Internal audit
- Incident management

Q No 10: Info sec Governance Block arrange them. (Aise table ho ga usko arrange kerna ho ga. yad ker lo initail intermdiate and mature blocks k Name) sari yad ker lain intial inter and maure

Awareness	Intermediate
Monitoring	Intermediate
Policy	Initial
Periodic review	Initial
Internal Audit	Mature
Responsibility	Initial
Risk management	Mature
Recourse and priority	Initial

Q No 11: Topic No 198: How To Build Effective Info Sec Governance? (Imp Repeated)

• Key success factors: (***see also minor detail of all these 06 points***)

– Leadership

– Strategy

– Structure

– Reporting

– Project management

– Culture

• **Leadership**: – Executive management role – Tone at the top Drive pressing priority – Approves budgets and resources – Periodic review of progress

• **Strategy**: – How the objectives will be practically achieved while achieving the technical, governance, and performance goals – How the organization will gear up and focus for the security transformation

• **Structure:** –What hierarchies, team structures, reporting lines, and resources will come together – How will different teams work together to achieve the common goals?

• **Reporting**: – What will be reported? – What will be the frequency of reports? – Who will perform review and assurance? – Who will monitor and track progress?

• **Project Management**: – How will an exceptional execution discipline be built? – How will milestones and performance be tracked? – How will project management best-practices be utilized?

• **Culture:** – How will an open, cooperative, authentic, and committed culture be built? – How will contention and conflict be eliminated? – How will a performance driven culture be promoted?

Q No 12: What are some of the common vulnerability scanners?

– Open VAS

– Nessus
– Qualys
– Rapid7

Free tool offered. By Qualys (IMP)

Browser check

SSL

Qualys Free Scan

1. Vulnerability – 2. OWASP – 3. Patch Tuesday – 4. SCAP

Q No 13: Topic no 118: What Are The Steps In VM Lifecycle?

VM Steps:

1. Analyze assets
2. Prepare scanner
3. Run vulnerability scan
4. Assess results
5. Patch systems
6. Verify (re-scan)

Q No 14: Topic no 57: Pre-requisites For Security Hardening

1. Security program approved
2. Consultant on board
3. Project kick-off meeting held
4. ISMC team identified and their loading for this project communicated
5. Appraisal linkage of core resources announced by CIO

Q No 15: Types of security testing: (IMP)

– Vulnerability assessment (VA)
– Penetration testing (PT)
– Other security tests through various automated tools
– Code review (initiated in test environment)

Q No 16: Which vulnerability scanner is used to look for both code based and configuration based vulnerability?

Answer: Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities and configuration-based vulnerabilities.

Question 17: In the Qualys Guard scanning methodology once the TCP port scanning has been performed mention the detection test?

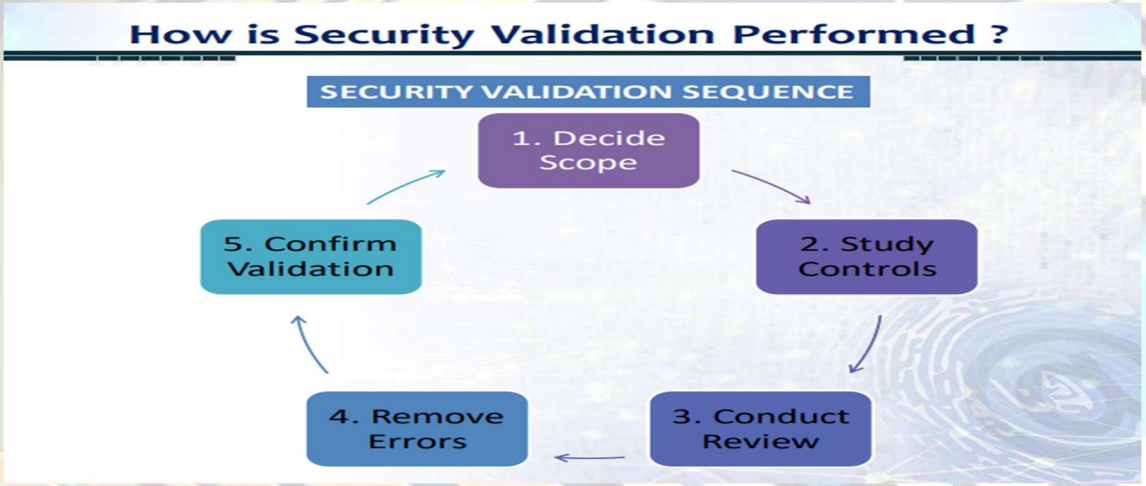
Answer: OS Detection

– Once the TCP port scanning has been performed, the scanner tries to identify the operating system running on the host.
– This detection is based on sending specific TCP packets to open and closed ports.

Q No 18: Topic No 262: What is Security Validation?

• What does security validation mean?

– To confirm via walk-through of system or device that the security controls implemented by an IT team have actually been implemented correctly



Q no 19: What is a patch?

– "A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs"

What are general steps for patch management? (yeh steps mostly ate hain exams main)

Step1: Establish baseline IT assets inventory

Step 2: Gather software patch and vulnerability information

Step3: identify vulnerability relevancy and filter to assign to end point

Q No 20: Who implements the security controls?

– Under the Security Transformation Model, security controls are implemented by the IT teams

Who conducts security validation?

– Security controls are validated by the Information Security team or by a third party consultant following the principle of segregation of duty

Q No 21: Why do we need to validate security controls?

– To check the completeness of the controls

– To check the correctness of the controls

– As an overall assurance

Q No. 22: Mention any two factors behind insecure software.

01, Connectivity,

02, Extensibility.

03. Complexity:

Q No 23: Write name of any five activities performed in accreditation process.

01. Organize, 02. . Prepare Checklist, 3. Confirm Tests, 4. Documentation & Processes (Complete)
5. Team Meeting, 6. Issue Accreditation

Q No. 24: What is a disaster?

– Any significant event that causes disruption of information technology processing facilities, thus affecting the operations of the business.

What is disaster recovery (DR)?

– DR is an area of security that allows an organization to maintain or quickly resume mission critical (IT) functions following a disaster

Q No 25: Yeh question atta hai Responsibility ni hoti to apne activity and Detail ko match kerna ho ga

ACTIVITY	RESPONSIBLE	DETAIL
POLICY	DEVELOPED BY CISO SIGNED OFF BY BOARD/EXECUTIVE	SETS THE SCOPE, OBJECTIVES, FRAMEWORK, REQUIREMENTS
RESPONSIBILITY & AUTHORITY	BOARD/EXECUTIVE	ASSIGNS ROLES, RESPONSIBILITIES, AND AUTHORITY FOR INFOSEC PROGRAM
RESOURCE ASSIGNMENT & PRIORITY SETTING	BOARD/EXECUTIVE	ALLOCATION OF RESOURCES AND BUDGET FOR THE INFOSEC FUNCTIONS
PERIODIC REVIEW	BOARD/EXECUTIVE	MONITOR AND REVIEW THAT THE GOALS OF THE INFOSEC PROGRAM ARE BEING MET

Q No 26: What type of assets do not have a CIS/DISA STIG?

Ans: – Software applications (ASP.NET, PHP, Other)

– Other applications such as asterisk deployments

Q No 27: Typical security tools used in an enterprise:

– Enterprise antivirus
– MS Active Directory (AD)
– Vulnerability manager
– Logs management
– Network & performance monitoring
Automated backups

Q No 28: Topic No 25: Major Components: Enterprise IT Network

• Edge router

- NGN FW
- DMZ:
- IPS & N-DLP
- Distribution switch
- Data center switch & FW
- Access switch
- NAC

Q No 29: Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL COVERAGE	GOOD	EXCELLENT
ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
USER FRIENDLINESS	GOOD	SATISFACTORY
UNUSABLE TERMINOLOGY	NO	YES
CONTROL DETAIL	GOOD	SATISFACTORY
TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)

Q No 30: CIS benchmark in profile applicability

– Profile applicability (ASA 8.X, ASA 9.X)
– Description
– Rationale
– Audit
– Remediation
– Default value
– References

Q No 31: Disa STIG component/content names

STIG content:

– General information (title)

– Discussion
– Check content
– Fix text
– CCI (References)

Q No 32: OWASP Software Assurance Maturity Model (SAMM) **Governance Phase:**

– Strategy & Metrics
– Education & Guidance
– Policy & Compliance

Q No 33: OWASP Software Assurance Maturity Model (SAMM) Construction Phase:

– Security Requirements
– Threat Assessment
Secure Architecture

Q No 34: Topic No 268: Software Security Testing & Validation–1 (imp)

• The OWASP Software Assurance Maturity Model (SAMM) undertakes software security testing & validation during the following phases:

– Verification

– Deployment

• OWASP Software Assurance Maturity Model (SAMM) Verification Phase:

– Design Review

– Code Review

– Security Testing

• OWASP Software Assurance Maturity Model (SAMM) **Governance Phase:**

Q No 35: What is business continuity? (BC.)

– Business Continuity (BC) is the capability of the org to continue delivery of products or services at acceptable predefined levels following a disruptive incident

Q No 36: How web and email can secured against malware and attacks in enterprise.

To secure web and email in an enterprise, implement antivirus software, firewalls, and intrusion detection systems. Train employees on security best practices, use email encryption, update software, employ MFA, monitor traffic, backup data, and conduct security assessments

Q No 37: Software security flow?

Software security flow refers to the systematic process of identifying, assessing, and mitigating security risks and vulnerabilities in software applications, following a structured approach to ensure the development of secure and robust software systems.

Q No 38: Remote exploit: (Yeh remote local wala table shape main bhe a sakta hai)

– A remote exploit works over a network and exploits the security vulnerability **without any prior access** to the vulnerable system.

- **Local exploit:**

– **A local exploit requires prior access to the vulnerable** system and usually increases the privileges of the person running the exploit past those granted by the system administrator.

Q No 39: Ensure Use of Only Fully Supported Browser & Email Clients:

Ensure that only **fully supported web browsers & email clients are allowed** to execute in the org, ideally only using the latest version of the browsers & email clients provided by the vendor.

Q No 40: This table was given and arrange this

Whose Responsibility Is InfoSec Governance ?

TYPICAL ORGANIZATIONAL TIERS AND RESPONSIBILITIES

TIER	RESPONSIBILITY
BOARD (STEERING COMMITTEE)	ORGANIZATIONAL COMMITMENT, APPROVE BUDGET, DIRECT
IT MANAGEMENT (CIO)	REVIEW, MONITOR, PROPOSE
CISO/SECURITY HEAD	PLAN, BUILD, RUN
IT & SECURITY TEAMS	IMPLEMENT/EXECUTE

Q No 41: Question: Mention the name of frame work against which nessus scanner gives configuration auditing feature?

Answer: – Configuration auditing:

CERT,

CIS,

COBIT/ITIL,

DISA STIGs,

FDCC, ISO,

NIST,

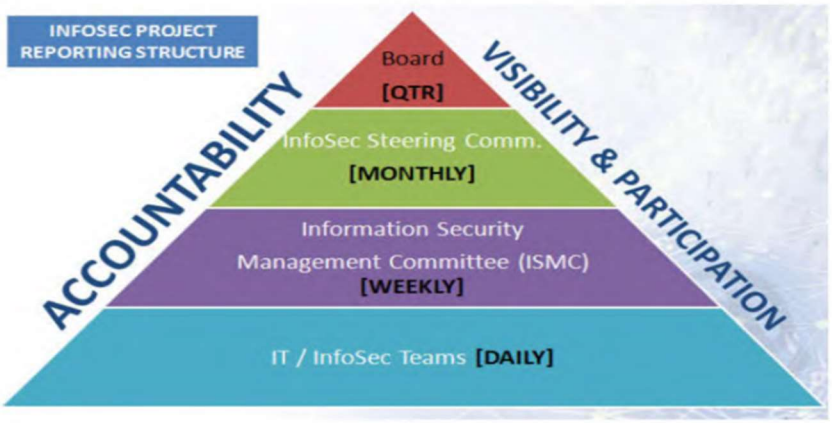
NSA

Q No 42: Identify two security function from the Asset management helps with the following security functions:

Answer: Patch management

Enterprise tracking and reporting

– Annual appraisals, security awards and recognition



Security is everyone's responsibility and has to gradually take its place in org culture

Q No 43: **Three types of redundant site models:**

• Hot site • Expensive site

Cold site • Cheapest

• warm site

– Mirror of primary data center –

Populated with servers, cooling, power, and office space

– Running concurrently with main/primary data center (synching)

– Minimal impact

• Cold site (cheapest): – Office or data center space without any server related equipment installed – Power, cooling and office space – Servers/equipment migrated in event of primary site failure

• Warm site (middle ground): – Middle ground between hot site and cold site – Some pre-installed server hardware (ready for installation of production environments) – Requires engineering support to activate

Q No 44: Backup considerations:

– What to backup?

– Backup location?

– Freq of backup?

– Backup operator?

– Backup checker (verification)? – Backup test & security methods? – Technology & tools used for backup

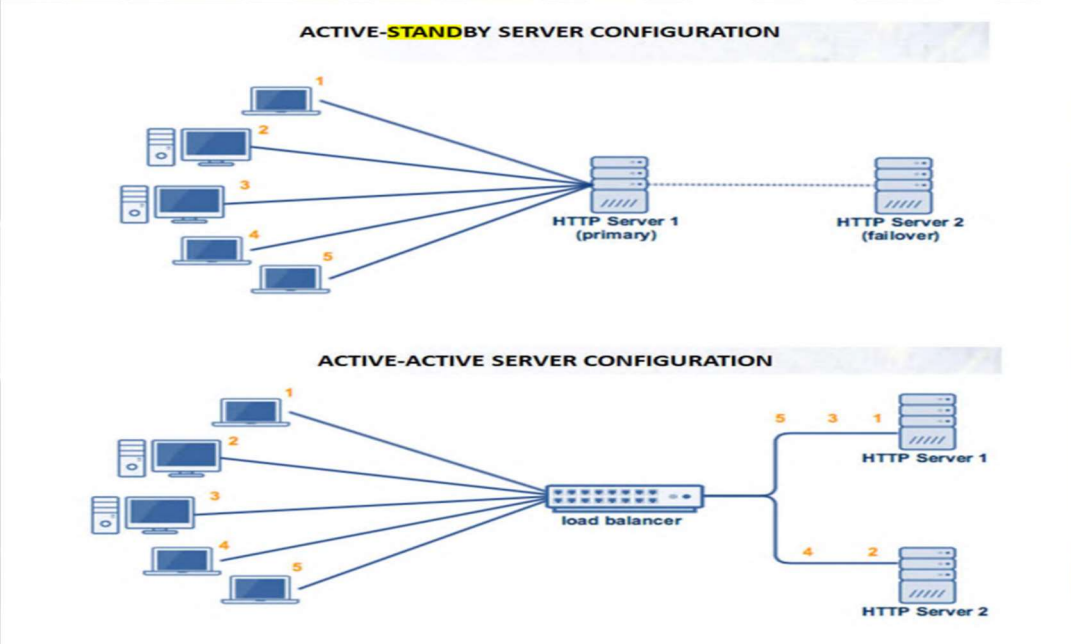
Q No 45. Yeh CAT 1,2, ya 3 wale detail oper niche ho gi arrange kerne ho gi yeh detail.

SEVERITY	DISA CATEGORY CODE GUIDELINES
CAT 1	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT 2	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT 3	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity

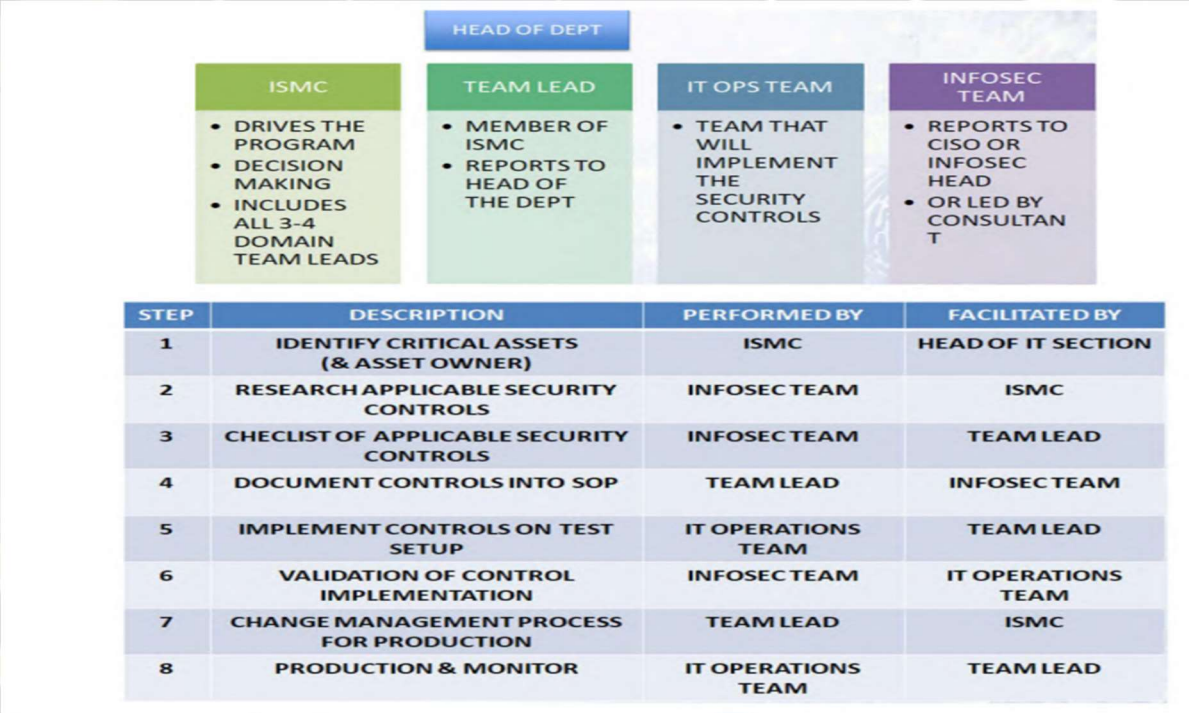
curity

Q No 46: **Write the Names of Common SIEM solution for security Event detection?**

A. LOgRhythm
B. IBM Q-Radar
C. Splunk



Q no 47: 8 Step Methodology.



STEP	DESCRIPTION	PERFORMED BY	FACILITATED BY
1	IDENTIFY CRITICAL ASSETS (& ASSET OWNER)	ISMC	HEAD OF IT SECTION
2	RESEARCH APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	ISMC
3	CHECLIST OF APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	TEAM LEAD
4	DOCUMENT CONTROLS INTO SOP	TEAM LEAD	INFOSEC TEAM
5	IMPLEMENT CONTROLS ON TEST SETUP	IT OPERATIONS TEAM	TEAM LEAD
6	VALIDATION OF CONTROL IMPLEMENTATION	INFOSEC TEAM	IT OPERATIONS TEAM
7	CHANGE MANAGEMENT PROCESS FOR PRODUCTION	TEAM LEAD	ISMC
8	PRODUCTION & MONITOR	IT OPERATIONS TEAM	TEAM LEAD

• Don'ts:

– Share your password

– Click on suspicious email links

– Install unlicensed software on your PC

• Do's:

– Logout when getting up from your system

– Report security incident

Allowing Auto play to execute may introduce malicious code to a system	True
Auto play begins reading from a drive as soon media is inserted into the drive	True
– By default, Auto play is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive) and on network drives.	True
By default, Auto play is disabled on removable drives,	True

- Step 1: Run the following command to show what the console timeout is set to

```
hostname#sh run console | in timeout.5
```

The output should look like

```
console timeout 5
```

Example:

```
Asa-fw#sh run console | in timeout.5
console timeout 5
```

Here the session timeout is 5 minutes

Major Component of IT Enterprise IT NERWORK

• DMZ:

– Security zone with placement of published web server, web & email security GWs, app security GW

• **IPS:** – Intrusion prevention (signature based)

– May be feature in NGN-FW

• **Distribution switch**

– Connectivity to access switches, external exit point (WAN), and DC switch

• **Data center switch & FW**

– Data center filtering (malware & access-lists)

• **Access switch**

– User connectivity

– Switch port security & access switch security

• **NAC** – Network admission control (IEEE802.1X)

• **SIEM** – Logging & dashboard for events, root cause analysis, event correlation

• **Vulnerability Manager** – Vulnerability scanning and asset tracking

• **System AV** – Signature based malware prevention

• **Server HIPS IPS** features for servers, also file integrity check-in

• UTM – Multi-featured NGN FW device

• Mobile device

– MDM –

Security features for mobile device

• **Involvement of various stakeholders for security hardening**

– Operations teams – Security team – IT management – Consultant – Business

• **IT Operations teams:** – Study the security controls (CIS/DISA)

– Apply the security controls in pilot/test environment

– Report the completion of control implementation to ISMC

– Assist InfoSec team with validation

• **InfoSec team:** – Conduct validation of security controls implementation – Acquire checklist of controls from relevant IT team – Document the status of controls in the form of a checklist – Forward validation report to ISMC

• **IT management**: – Ensure IT operations teams receive required guidance and support – Sign-off on change management requests – Assist with planning down-time and business related downtime

• **Consultant or project director**: – Drives the security program – Ensures that strategy is aligned with project objectives – Ensures process and activities are moving at good momentum as per timeline

• **Business stakeholders:** – Provide downtime approvals if required – Help to engage other vendors if applicable

Question: Write the First step in automated Security hardening and validation name of tool Used?

Answer: Step 1: Scan an IT asset using Qualys compliance scan, NESSUS compliance scan, or CIS CAT PRO Tool

Question No: Enlist the first five CIS controls that eliminate the vast majority of your organization vulnerability

Ans: Following are the first five CIS control among CIS 20 controls.

A. Inventory of Authorized and unauthorized devices.

B. Inventory of Authorized and unauthorized software.

C. Secure configuration for software of hard ware

D. Continues vulnerability assessment and remediation

. E. Controlled use of administrative privilege.

Question no 12 : Three Pillars of Information Security?

- **Confidentiality**: keeping information secret
- **Integrity**: keeping information in its original form
- **Availability:** keeping information and information systems available for use

Question No 12 : Three pillars of information security Implemention: (yeh implementation hai)

– People
– Process
– Technology