Cs 205 mid-term file by M. Qasim Ali and Madam Sabahat Jabeen. 03337435091

M. Qasim Ali CS 205. 03337435091. U tube channel DIGITAL WORLD

MCQS:

1. An attack in which attacker alter the system resources is called ------?
   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 control
   C. Security mechanism
   D. Security service
3. ---------- are three pillars of information security security?
   ANS: confidentiality, integrity, availability.
4. Ransomware is _____?
   Ans: a type of attack that encrypt data on computer and servers.
5. NESSUS tool is used at _____ layer in information security transformation framework?
   A. Sec governance
   B. Sec engineering
   C. Vulnerability management.
   D. Sec 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 recourse allocation

DIGITAL WORLD VU CS205.

B. Highly specialized and continuously changing technology

C. Cloud and IOT

D. lack of owner ship, department silos, missing security hardening (I think D, may be A)

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 secure

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 NGN fire wall are____?

A. Web sec and email sec.
B. Malware filtering, access list for traffic filtering bandwidth filtering
C. Wan interface
D. APPT attack prevention

DIGITAL WORLD VU CS205.

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

A. It Is leading to wastage of time and distraction

B. Traditional enterprise security perimeter boundary has disappeared.

C. Location o the user can be tracked

D. Apps on mobile device may be Trojans.

16. The recommended 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 good data center

B. Lack of budget and resources allocate for security.

C. Lack of security vendor

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 antispam gateway

D. By using malware protection at edge.

DIGITAL WORLD VU CS205.

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

A. analysis, design, implement and validate

B. identity, analyze, design, execute

C. Identity, analyze, design, execute, measure,

D. Analyze, implementation and validate

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, continuous improvement.

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

D. Establish track, MSB, implement across IT

23. ____ category has maximum number of CIS benchmark

A. Operating system

B. Mobile device.

C. network device.

D. Cloud providers

24. _____ category has minimum number of CIS benchmark

A. Multifunction point device.

B. mobile device

C. network device.

D. Cloud provider

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

A. Describe the control

B. Describe the benefit

C. Tells how to check the controls.

DIGITAL WORLD VU CS205.

D. Tells how to apply controls

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

A. Level1 and level 2

B. Scored and un scored.

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

29. A program or device that can monitor data traveling over a network is called____ ?

A. Hoax

B. Router

C. Sniffer (Conform from google)

D. Spoof

30. Internationalized domain name are displayed as

A. Little ENDIAN

B. Big ENDIAN

C. UTF-32

D. UNICODE

31. Information security is combination of _____?

ANS: People process and technology

DIGITAL WORLD VU CS205.

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 collection and analysis

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

36. DISA gives us the following feature 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 unusable terminology (Not 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

DIGITAL WORLD VU CS205.

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 ____-?

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 for traffic filtering, bandwidth filtering

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

C. Log collection

D. Malicious traffic detection

DIGITAL WORLD VU CS205.

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

DIGITAL WORLD VU CS205.

CS 205 Mid term short notes for Sprimng 2023

Made By Muhammad Qasim Ali For any Query 03337435091

Question no 01: What is Cyber Security?

– Precautions taken to guard against unauthorized access to data (in electronic form) or information Systems connected to the internet

1. Information security by SANS define

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

Question No 02: There are three pillars related to implementation of information security . mention the name? •

Three pillars of information security Implemention: (yeh implementation hai)

– People

– Process
– Technology

Question No.03: You are required to identify and write the name of three main pillars of information security?

(Just names main ap name he likhna.)

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

Question no 04: How many layers involved in information security transformation framework? you are required to write the name.

Ans: There are Four main layers or steps involved in information security transformation framework. Names written as under

A. Security Hardening
B. Vulnerability management
C. Security Engineering
D. Security Governance

Question No 05: 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 hardware
D. Continuous vulnerability assessment and remediation.
E. Controlled use of administrative privilege.

Question no 06: Write the name of any two Famous SIEM solution that are available in market

Ans: Leading SIEM solutions:

LogRhythm,

IBM Q-Radar,

Splunk,

Elastic Search

Question# 07: Write the name of different stake holder that will conduct the security hardening.

Ans: Involvement of various stakeholders for security hardening

DIGITAL WORLD VU CS205

– Operations teams

– Security team

– IT management

– Consultant

– Business

Question# 08: How different versions SSH protocols support? Write the names?

Ans: : SSH supports 2 different and incompatible protocols:

SSH1 and SSH2. (just name likh dain yeh bhe kafi hai)

SSH1 was the original protocol & was subject to security issues.

SSH2 is more advanced and secure.

Question# 09: Three types of redundant site models:

- Hot site
- Cold site
- Warm site

Question#10: **: SECURITY HARDENING – SOFTWARE APPLICATIONS SOFTWARE SECURITY WORKFLOW ?** **(Most Repeated question)**

1. Research Security Controls
2. 2. Apply Security Controls (Hardening)
3. 3. Code Review & Automated Testing (Validation)
4. 4. Harden Server Environment
5. 5. Pen Test & Accreditation (Move to PROD)

Question#11: **Write any five steps in information security program**

Ans: A. Assessing security risks and gaps

B. Implementing security controls

C. Monitoring, measurement, & analysis

D. Management reviews and internal audit

E. Accreditation/testing

DIGITAL WORLD VU CS205.

Question#12: **CIS benchmark in profile applicability** (also see page no 94, 95 too L1,L2)

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

Question#13: OSI Security Architecture

• Security service is a service that ensures adequate security of the system or data transfer
– Authentication – Access control – Data confidentiality – Data integrity – Non-repudiation – Availability

Question#14: Question 05: 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

Question#15: Disa STIG component/content names

STIG content:
– General information (title)
– Discussion
– Check content
– Fix text
– CCI (References)

Question#16:OWASP Software Assurance Maturity Model (SAMM) **Governance Phase:**
– Strategy & Metrics
– Education & Guidance
– Policy & Compliance

Question#17: OWASP Software Assurance Maturity Model (SAMM) **Construction Phase:**
– Security Requirements
– Threat Assessment
Secure Architecture

Question#18: 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

Question#19: What is the function of active directory in an enterprise network?

Active Directory is a directory service by Microsoft that provides centralized management and authentication for users, computers, and resources in an enterprise network, facilitating secure access and efficient administration.

Or

DIGITAL WORLD VU CS605.

: ACTIVE DIRECTORY (AD) • Active Directory (AD) is essential not only to regulate account management (authentication and authorization) but also to enforce and manage security controls

Question#20: 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.

Question#21: 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.

Question#22: What is an IT asset?

– An IT asset is any resource such as hardware, software, and information, human
Owned or utilized by the organization for IT processing

Question#23: Typical security tools used in an enterprise:

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

Question#24: 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
• SOC:
– SIEM
– VM
• System AV
• Server HIPS
• UTM

DIGITAL WORLD VU CS205.

• Mobile device – MDM

Question#25: Backup considerations:

– What to back up?
– Backup location?
– Frequency of backup?
– Backup operator?
– Backup checker (verification)?
– Backup test & security methods?
– Technology & tools used for backup?

Question#26: Common challenges with box security?

1: Other challenges with "box security" approach: –

2: Shortage of staff (IT & security)

3: Training and skill required to operate the sophisticated devices and features

What is box security

"Box Security" refers to a prevalent approach in the industry, especially in larger organizations in which
the solution for every security challenge is in the form of a "box" or device

• **Box for :**
– Email security
– Web security
– FW
– IPS
– APT attack prevention
– DDOS prevention
– Network DLP
– Network Forensics
– Others

Question#27: What is a disaster?

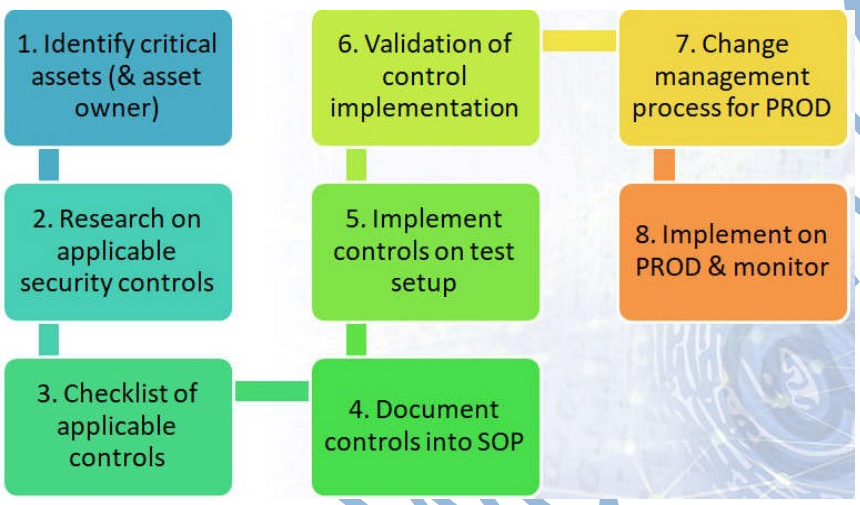
– Any significant event that causes disruption of information technology processing facilities, thus affecting the operations of the business.

Question#28: 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

DIGITAL WORLD VU CS205.

Question#29: Security hardening 8 step methology



DIGITAL WORLD CS205.

M. Qasim Ali CS 205. 03337435091. U tube chanel DIGITAL WORLD

Question#30: IT Asset life cycle:



CIS and DISA comparission

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)

M. Qasim Ali CS 205 . 03337435091

Qasim.tahir@sngpl.com.pk. Qasimali106376@gmail.com