CS 205 current paper SPRING 2024 MID TERM Exam FIL

Made By Muhammad Qasim Ali 03337435091

https://chat.whatsapp.com/L2hJUzYHNIe1d6Qmfp5SPm

https://youtu.be/5Q8idWcvZtI

U Tube channel : VU STUDY LAB

Q 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

Q No 02: Information security by SANS define

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

Q No .03: Three pillars of information security Implementation: (yeh implementation hai)

– People
– Process
– Technology

Q No .04: Three pillars of information security (CIA)

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

Q No 05: Transformation model layers

Ans:

1. Security hardening
2. Vulnerability management (VM)
3. Security engineering
4. Security governance

Q No. 06: 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. 07: Who Are The Players In Information Security?

- Government
- Industry & sectors

• International organizations
• Professional associations
• Academia and research organizations
• Vendors and supplier

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: What is a disaster?

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

Q No. 10: 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. 11: Types of security testing:

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

Q No 13: What are some of the common vulnerability scanners?

- Open VAS
- Nessus
- Qualys
- Rapid7

Q No 14: Free tool offered. By Qualys (IMP)

Browser check,

SSL

Q No 15 : Qualys Free Scan

1. Vulnerability

– 2. OWASP

– 3. Patch Tuesday

– 4. SCAP

Q No 16: Which team have primary ownership

Ans: Information security team

Q No 17: which team tests the patches in environment?

Ans: IT ops team

Q No 18: Info security Governance initial 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 19: 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 20: Question: Which kind of vulnerability scanner used code-based vulnerabilities and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

Ans: Use a SCAP-validated vulnerability scanner

Q No 21: 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 22: 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 23: Typical security tools used in an enterprise:

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

Q No 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

Q No 25: 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 26: 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 27: CIS benchmark in profile applicability

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

Q No 28: Disa STIG component/content names

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

Q No 29: 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 30: Security transformation project:

• Security transformation project time line:

– Project initiation: 2 Mths

– Layer 1: security hardening of IT assets (6 Mths) –

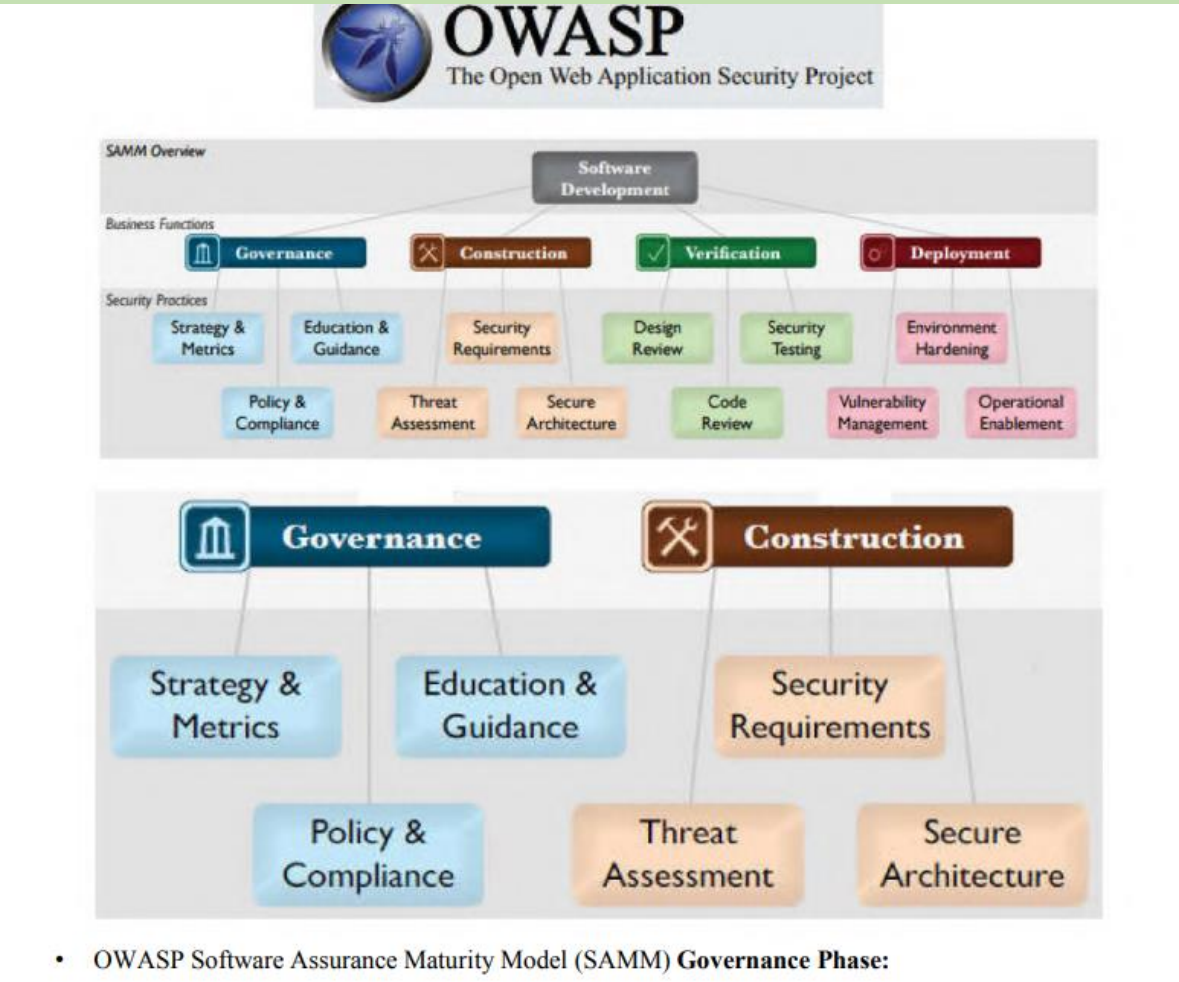
Layer 2: VM (1 Mth)

– Layer 3: security engineering (1 Mth)

– Layer 4: Governance & ISO cert.(3 Mths

CCI (Control Correlation Identifier) (for Mcqz only. CCi stands for ?)

Q No 31: OWASP Software Assurance Maturity Model (SAMM) **Governance Phase:**
– Strategy & Metrics
– Education & Guidance
– Policy & Compliance
OWASP Software Assurance Maturity Model (SAMM) **Construction Phase:**
– Security Requirements
– Threat Assessment
Secure Architecture



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

Q No 32: 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 33: 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 34: 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 35: Bangladesh Bank SWIFT Hack – Feb 2016: Hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests.
– Requests sent to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.
– USD 81 million stolen
– Total impact could have been USD 1 billion

Recover 19 Million

Not claim : 81 million

Q No 37: • Who implements the security controls?

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

Q No 38: 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 39: • 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

SN	ACTIVITY	TEAM	SUPPORTED BY
1	ANALYZE ASSETS	INFOSEC	IT OPS TEAM
2	PREPARE SCANNER	INFOSEC	-
3	RUN VULNERABILITY SCAN	INFOSEC	-
4	ASSESS RESULTS	INFOSEC	IT OPS TEAM
5	TEST & PATCH SYSTEMS	IT OPS TEAM	INFOSEC
6	VERIFY (RE-SCAN)	INFOSEC	IT OPS TEAM
7	REPORT FINDINGS	INFOSEC	IT STEERING COMMITTEE

Q No 41: Remote exploit:

– 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 42: 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 43: 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 44: 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,

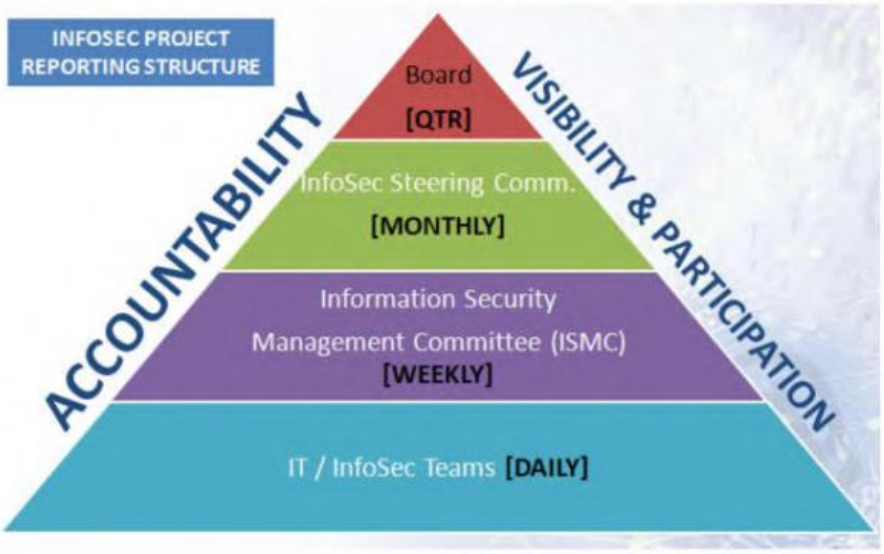
NSA

Q No 45: Identify two security function from the which 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 46: **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 47: 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 48. Yeh CAT 1,2, ya 3 wale detail oper niche ho gi arrange kerne ho gi yeh detail.

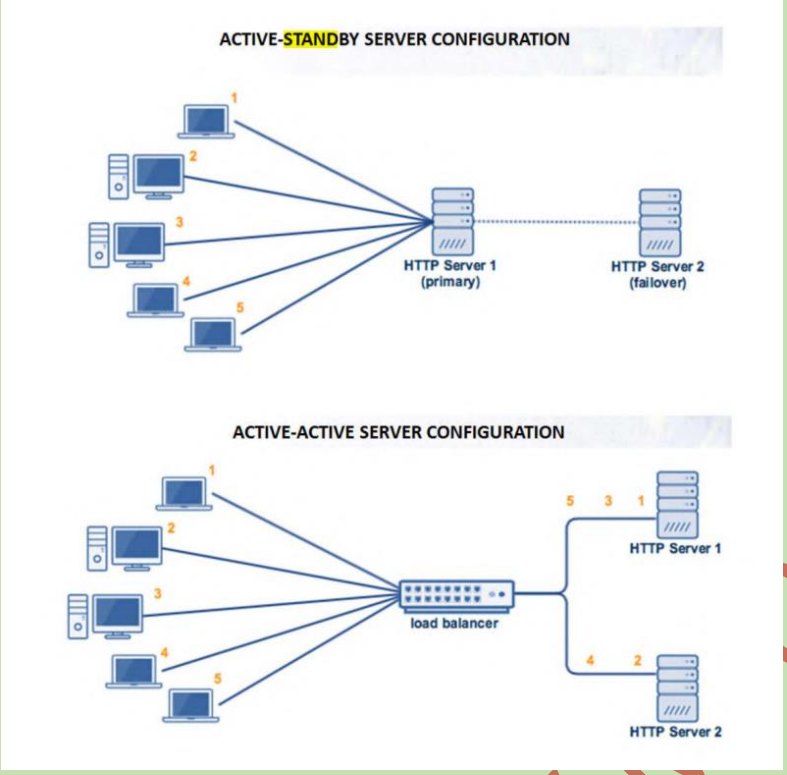
SEVERITY	DISA CATEGORY CODE GUIDELINES
CAT 1	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT 2	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability,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

curity

Q No 49: **Write the Names of Common SIEM solution for security Event detection?**

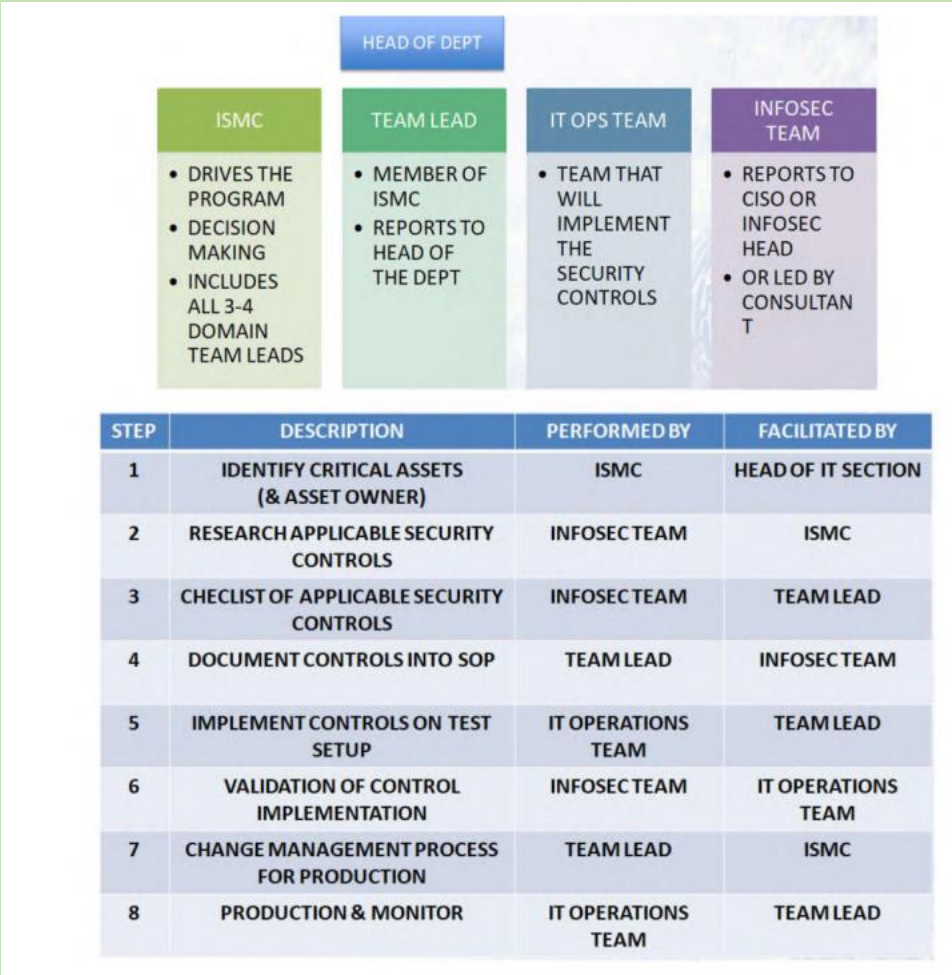
A. LOgRhythm
B. IBM Q-Radar
C. Splunk

D.



8 Step Methodolgy .

E.



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

Security hardening

is the process of configuring t asT assets to maximize security of the IT asset and minimize security risks

Education: – Integrates all of the skills and competencies into a common body of knowledge

– E.g. a degree program

• Don’ts:

– Share your password

– Click on suspicious email links

– Install unlicensed software on your PC

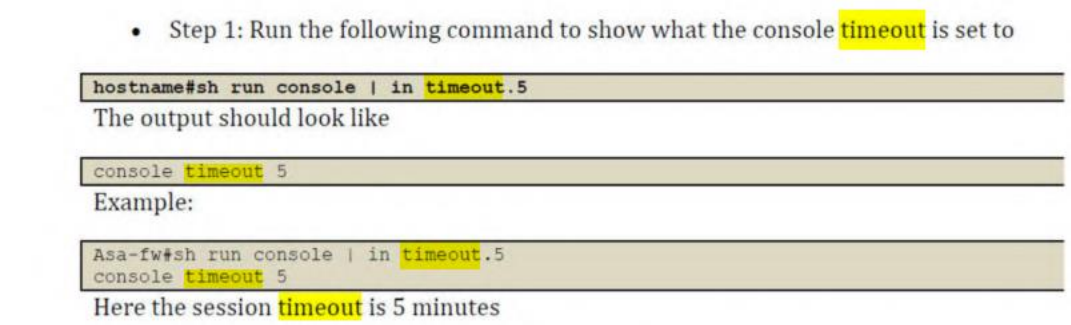
• Do's:

– 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

–



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