# CS205 Final term Updated File SPRING 2025

# QASIM KHAN WORLD U tube channel. 03337435091

**Question: Mention the names of framework against which Nessus scanner gives Configuration Auditing features?**

**Ans**: Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA

**Q: Name the first lyer of CSMM**

Ans:

1: FOUNDATION

2 FUNDAMENTALS

3 Hardened

4 PROTECTED

5 MONITORED

6 . SECURED

**Question No 18: As for email and web browser protection which of the following browser and Email Client should be used in an Organization. You ca chose Multiple options? & Quiz.**

Ans: A. Fully Supported

B. Latest version

C. Initial version

D. Only Microsoft Browser and email Client

Cyber sec maturity matrix Layer names or Arrange Table:

related to services needs to be addressed immediately.

**Q No 56: CYBER SECURITY CHALLENGES:**

– Reactive
– Superficial
– Contention
– Box-Approach
– Governance-Overkill

**Q No 57: Topic No 254: CYBER SECURITY MATURITY MATRIX**

| Sr No | Layer |
|---|---|
| 1 | FOUNDATION |
| 2 | FUNDAMENTALS |
| 3 | Hardened |
| 4 | PROTECTED |
| 5 | MONITORED |
| 6 | . SECURED |

**I. FOUNDATION**

Edge FW With Filtering
Active Directory (WS/S)
Licensed Enterprise AV (WS/S)
Licensed Windows OS (WS/S) Or Open Source

**In Activity it is VM life cycle steps and remaning table**

## Topic no 127: Who Conducts Vulnerability Management

umber of teams and resources may be involved in the VM lifecycle

| 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 04: 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 05: What are some of the common vulnerability scanners?**

- Open VAS
- Nessus
- Qualys
- Rapid7

**Free tool offered. By Qualys (IMP)**

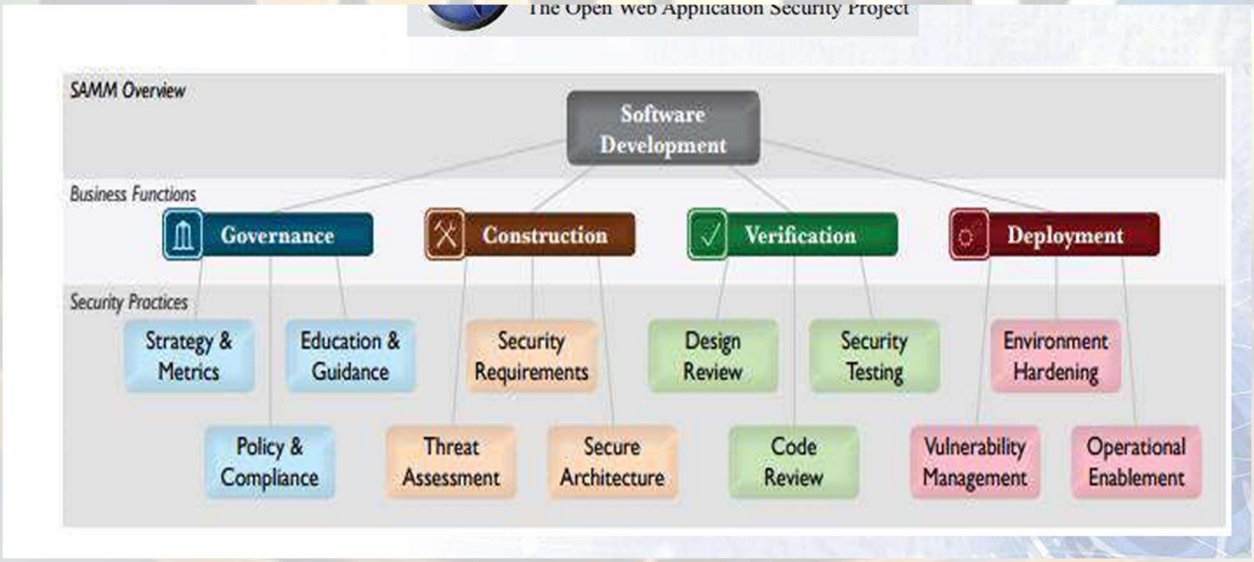
Browser check

SSL

**Qualys Free Scan**

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

Verfication phase names and Deploment in SDLC



## Free Tool offer by Qualys :

Free Qualys tools: –1. BrowserCheck –2. SSL

## Free Scan offer By A\Qualys

Qualys FreeScan – Vulnerability – OWASP – Patch Tuesday – SCAP

Question: Which is Vulnerability scanner used for both code and secure configuration Vulnerability

Ans: Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common

**Question No 75: Following table contains some** CHARACTERISTICS of exploit that causes security breaches you are required to identify the type of exploit as local or remote?

| | | |
|---|---|---|
| Required prior to the Vulnerability system | Local | ---- |
| Works over Network | ------ | Remote |
| Does not require any prior Access | ------- | Remote |
| Exploit in the through internet | ------- | Remote |

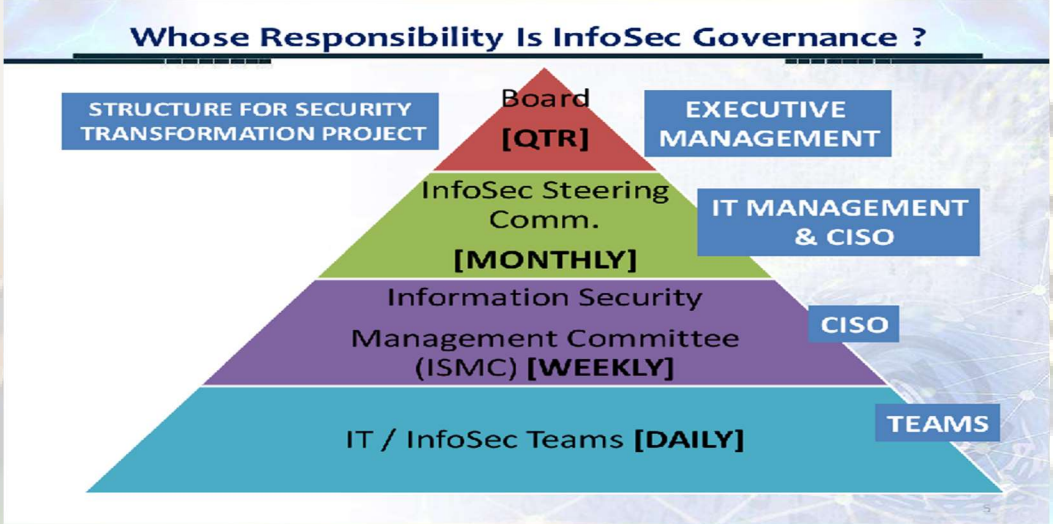
**Answer: Remote exploit**: – A remote exploit works over a network and exploits the security vulnerability without any prior access to the vulnerable system.

• **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

**Yeh Table Ho Ga Tier and responsibility ko arrange kerna ho ga:**

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 01: very important. Security Breach in HOME Department 2014**

**How much card played:** • 56 million payment cards compromised

**Which kind of vulnerability exploited:** Then they exploited a zero-day vulnerability in Windows Or Exploitable vulnerabilities were found in anthem network

**How much mail used**: The malware was also able to capture 53 million email addresses.

• 56 million payment cards compromised •

Early September 2014

– This malware was able to grab 56 million credit and debit cards. The malware was also able to capture 53 million email addresses (winter, 2014).

**Q no 02: Topic no 125: Security Breach Case Study 2: Anthem**

**How much People effected**: Affected 78.8 million individuals

**How Much Account used or utilized:** The attacker utilized at least 50 accounts

**How much system compromised**: compromised at least 90 systems

**Which way used**: A phishing email containing malicious content (Also MCQZ)

## Topic No 145: WHAT IS SECURITY ENGINEERING?

- Security Engineering is the third layer of the Security Transformation Model

- Consists of more in-depth and complicated security activities which take more time and effort
- Many times related to security architecture
- **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
- **Why at Layer 3 of Security Transformation Model?**
    - Low hanging fruit first

- Teams tend to get bogged down with advanced security tasks
    - These take time, effort, and often budget approval

## Topic No 146: WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING?

- Security architecture as per best-practices
- The right security devices in the right places
- Effective security configuration of security devices (features)
- Optimum operation of security devices
- Aggregate controls

**Types of security testing ya Names**

: – Vulnerability assessment (VA)

– Penetration testing (PT)

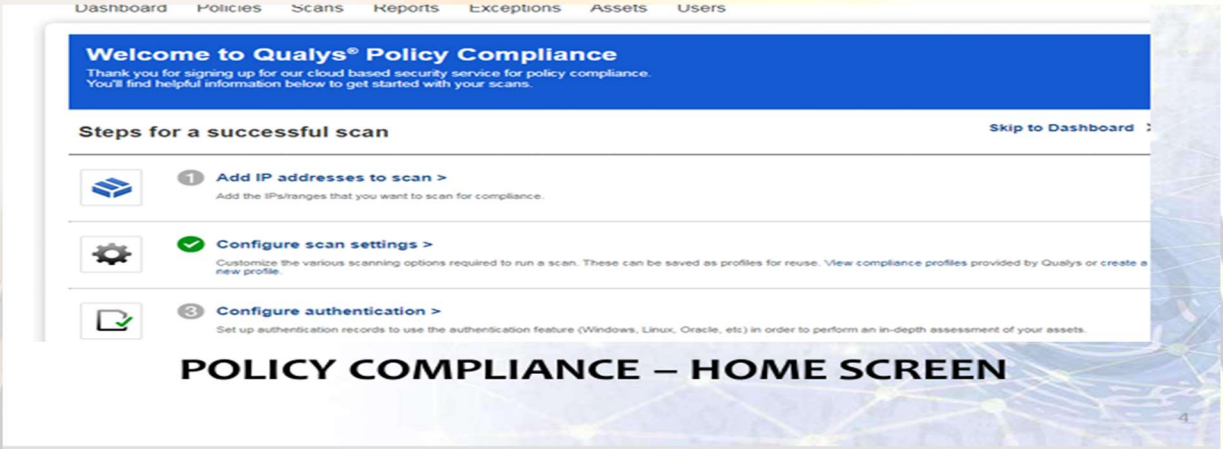
– Other security tests through various automated tools

– Code review (initiated in test environment)

**Question: The phase which is not a part of security hardening:?**

Ans: Implement risk generation.

Baqi sec hardening k steps hon ge. Yeh ni ho ga oper wala aik just





***Which required secondary encryption***

***Talnet*** **No**

***FTP*** **No**

***HTTP*** **No**

***SSH*** **Yes**

**Question: Write the security function for which assets management help?**

**Ans:** 1. Patch management

2. Software whitelisting

3. Software assets discovery and management

4. Enterprise tracking and reporting

**Table wale block arrange kernen the :**

**Initial**

- Policy
- Responsibility
- Recourse and priority
- Periodic review

**Intermediate**

- Change management
- SOP,s
- Awareness
- Monitoring

**Mature**

- Risk management
- Internal audit
- Incident management

**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 |

## OBJECTIVE CS205 FINAL TERM BY M.QASIM ALI KHAN

## QASIM KHAN WORLD U TUBE CANNEL 03337435091

**Question No 01: where should source code be kept as best practice?**

A. Access control system
B. Change control system
C. Version control system
D. Source control system

**Question No 02: ---------type of scripting languages should be used in email clients and web browsers**

A. Authorized scripting languages
B. Client side scripting languages
C. Server-side scripting languages
D. Scripting languages slowed by vendor

**Question No 03: All network traffic to or from the internet must pass through ---------- to filter unauthorized connections**

A. Application layer filtering proxy

B. Session layer filtering proxy

C. Network layer filtering proxy

D. System layer filtering proxy

**Question No 04: ISO31000 guidelines are centered on----------?**

A. Organization context
B. Leadership and commitment
C. Planning
D. operation

**Question No 05: The function most closely associated with the "soc" is**

A. Security management

B. Security engineering

C. Security frameworks

D. Security operations

**Question No 06: Assign resources, assigning roles and communicating role fall under ---------- clause.**

A. Support

B. Leadership

C. Performance evaluation

D. Operation

**Question No 07: Creating related to policy and ISMS fall under ------ clause**

A. Support

B. Leadership

C. Performance evaluation

D. Operation

**Question No 09: Controlling planned changes and risk assessment fall under _____ clause.**

A. Operation

B. Support

C. Leadership

D. Performance evaluation.

**Question No 10: Monitoring, measurement and analysis fall under _____ clause.**

A. Operation

B. Support

C. Leadership

D. Performance evaluation

**Question No 11: Employee screening Must be conducted**

A. After employment

B. Prior to employment

C. During employment

**Question No 12: Which of the following come under equipment physical and environmental security control?**

A. Working in secure areas

B. Secure delivery and loading areas

C. Clear desk and clear screen policy

D. Physical entry controls

**Question No 13: OWASP software assurance maturity model undertake software security testing and validation during**

A. Governance and deployment

B. Governance and verification

C. verification and deployment

D. Communication and Governance

**Question No 14: _____ is the 6th layer of Cyber security maturity matrix.**

A. Monitored

B. Secured

**Question No 15: _____ is the fifth layer of cyber security maturity matrix.**

A. Monitored

B. Secured

**Question No 16: The enterprise technology governance and risk management framework is considered as a best combination of _____**

Ans: is a combination of COBIT, ITIL, and ISMS ISO27001

**Question No 17: Stage 2 of security transformation model is**

Ans: Vulnerability Management

**Question No 18: _____ is the goal of performing vulnerability assessment**

A. To fix many things as possible as efficiently as possible

B. Testing security that is assume to be secure

C. Technical assessment designed to achieve specific goal

D. Focus on how an existing configuration is compared to a standard

**Question No 19: PHP security guidelines cover which type of attack**

Ans: Injection attack

**Question No 20: _____ is the Goal of Performing Audit?**

Ans: Focus on how an existing configuration is compared to a standard

**Question No 21: Complex Password should be enforced to survive_____**

Ans: Dictionary Attack

**Question N 22: _____- are considered type of security assessment?**

Ans: Threat Assessment

**Question No 23: There are------ benefits of version control.**

ANS: SEVEN

**Question No 24: _____ assessment is designed to determine whether an attacker can achieve specific goals when facing your current security posture?**

A. Threat Assessment
B. Bug bounty
C. Penetration testing
D. Red team exercise

**Question No 25: How many steps are involved in policy scan of Qualys**

Ans: Five

**Question No 26: Are the key benefits of security transformation project implementation to an organization?**

Ans : Prevention of attacks

**Question No 27: ---------- Protocols is used for assigning address dynamically?**

Ans: DHCP

**Question No 28: As per security life cycle validation activity should be performed**

Ans: After applying controls

**Question No 29: To prevent attacks fraud and pilferage an effective information security transformation program is essential for _____?**

A. IT organization
B. Medium sized organization
C. Small size organization
D. Any organization having IT setup

**Question No 30: Vulnerability management is _____ steps cycle?**

Ans: Five steps

**Question No 31: ------- action is recommended for organization having very good security posture and have a score higher than 85% ?**

Ans: Go for ISO27001 certification or Go for ISO certification

**Question No 32: At_____ layer of transformation model CIS critical control are implemented**

A. Security engineering
B. Security governance
C. Vulnerability management
D. Security hardening

**Question No 33: Should be deployed to limit and control that which device can be connected to the network?**

Ans: 802.1x

**Question No 34: Inventory of authorized and unauthorized software control require making list of??**

Ans: Authorized software and version

**Question No 35: An authentic information security head always**

Ans: Give credit where its due

**Question No 36: Candidness of info sec head means that he_____?**

Ans: Honesty and straight talk

**Question No 37: -------- Technique / Solution can be used to analyze and block inbound email attachments with malicious behavior.**

A. Enterprise antivirus
B. Sandboxing
C. Siem solution
D. Fim solution

**Question No 39: The objective of COBIT is to help organization ----------.**

A. Create optical values from it by balancing benefits with risk
B. Implement a strong governance of it
C. Manage it effectively while ensuring business continuity
D. Create a single page it dashboard

**Question No 40: In security transformation model ownership of validation of controls lies with**

A. IT operation team
B. Business team
C. Info security or consultant
D. IT help desk team

**Question No 41: As per ISO27001 Operating procedure should be**

A. Confidential
B. Verbally communicated
C. Decided on adhoc basis
D. Documented and available to who need them

**Question No 41: It seems to conducting a successful security transformation project is more challenging in a?**

A. Large size organization
B. Medium size organization
C. Small sized organization
D. Environment where multiple sites are present

**Question No 42: Stage 2 of security transformation refers to**

A. Security Governance
B. Security engineering
C. Security hardening
D. Vulnerability management

**Question No 43: ---------should be used to ensure that critical system files have not been altered.**

A. CIS cat pro
B. Qualys vulnerability scanner
C. Security information and event monitoring tools
D. File integrity monitoring tool

**Question No 44: An authentic information head always ----------**

A. Take credit of every thing
B. Never admits mistakes and failure
C. Give credit where it is due
D. Very strict and disciplined

**Question No 45: Network performance degradation can be faced in ---------- step of VM cycle.**

A. Preparing the scanner
B. Analyzing the asset
C. Running the scanner
D. Applying the patches

**Question No 46: ---------- category vulnerabilities have the highest severity in Qualys scan.**

A. Level 2
B. Level 3
C. Level 4
D. Level 5

**Question No 47: ----------plays an instrumental role in success of security transformation program.**

A. IT team lead by CIO
B. Business team
C. Internal team
D. Highest management

**Question No 48: --------should be deployed to limit and control that which devices can be connected to the network?**

A. 802.1x
B. 802.11g
C. 802.11b
D. 802.11n

**Question No 49: in which phase of Security assessment, assessment method based on report format are decided**

A. Report finding
B. Build plan, scope and objectives
C. Assign role
D. Conduct assessment

**Question No 50: Automated tool should be used to verify and compare the network device configuration with ----------**

A. Approved security configuration
B. Recommended security configuration by vendor
C. Latest security configuration released by vendor
D. Default security configuration released by vendor

**Question No 51: Under security transformation model which team is responsible for validation of control?**

A. Business team
B. Info security team or consultant
C. IT operation team
D. IT help desk team

**Question No 52: The computer security resources center (CSRC) website guides user to ------- resources?**

A. CIS resources on computer , cyber, information security and privacy
B. SANS resources on computer, cyber, information security and privacy
C. NITS resources on computer , cyber, information security and privacy
D. PCI resources on computer , cyber, information security and privacy

**Question No 53: Complex password should be enforced to survive ----------?**

A. Dictionary attack
B. Injection attack
C. DOS attack
D. Phishing attack

**Question No 54: ---------- activities are carried out in phase 1 (Pilot phase) of information security transformation program?**

A. Perform hardening of Key IT asset in Test environment
B. Understand origination and its security issues
C. Develop ISMC
D. Identify assets for various phases

**Question No 55: Candidness quality of information security head means that he-----?**

A. Promote performance and merit
B. Encourage-solo flight of team member
C. Honesty and straight talk
D. Adjust players in right position

**Question No 56: ----------protocol used for Assigning address dynamically?**

A. DCP
B. HTTP
C. DHCP
D. IP

**Question No 57: -------Team has primary ownership of vulnerability management process?**

A. Information security team.
B. IT operation team
C. Business team
D. Risk and compliance team

**Question No 58: --------Rules are mentioned relate to C++ security hardening?**

A. Seven
B. Eight
C. Nine
D. Ten

**Question No 59: ------ is goal of performing audit**

A. Testing Security that is Assumed to be secure
B. Technical assessment design to achieve specific goals
C. To fix as many things are possible and efficiently as possible
D. Focuses on how on existing configuration compare to standard

**Question No 60. Under security transformation model which team is responsible for implementing controls?**

A. It operation team
B. Security consultant
C. Risk compliance team
D. Business team

**Question No 61: In ----------assessment tester has full access to all internal information about the target?**

A. White box assessment
B. Grey box assessment
C. Black box assessment
D. Risk assessment

**Question No 62: -------- assessment is designed to determine whether an attacker can achieve specific goals when facing your current security posture?**

A. Threat assessment
B. Bug bounty hunting
C. Penetration testing
D. Red team exercise

**MCQ No 62: --------- are the key benefits of security transformation project implementation to an organization?**

A. IT team get experience and aware of security
B. Prevention of attack
C. IT team gets incentives
D. Management becomes aware of IT team capability

**Question No 63: --------- action is recommended for organization having very good security posture and has a score higher than 85%?**

A. Go for risk assessment
B. Third party security review
C. Go for ISO27001 certification
D. Information security transformation program

**Question No 64: Version of security related updates should be applied on network devices?**

A. Latest
B. Default
C. Latest and stable
D. Oldest

**Question No 65:: Most of the problem associated with week security posture is due to --------?**

A. Lack of awareness
B. Lack of funds
C. Lack of experience
D. Lack of commitment

**Question No 66: The information security policy need to be ----------?**

A. Review once in three year
B. Update once in five year
C. Locked in drawer and kept confidential
D. Regularly reviewed and approved for the changes

**Question No 67: In case of financial sector ---------- regulations need to be reviewed and understood to raise management support for security transformation?**

A. SBP
B. PTA
C. PEMRA
D. PEPRA

**Question No 68: Inventory of authorized and unauthorized software control require making a list of ------?**

A. Authorized access and version
B. Authorized operating system and version
C. Authorized software and version
D. Unauthorized software and version

**Question No 69: Which principle should be used when setting up a user in data base?**

A. Principle of normal user

B. Principle of administrative user
C. Principle of least privilege
D. Principle of highest privilege

Q. 70. …… which team has primary owner ship in vulnerability management?

ANS: **Information security team**

Q. 71. Steps involved in vulnerability management?
**Ans: Identify, classify, remediate, and mitigate the vulnerability**

**Q. 72:** For creating scanning policies, qualys built in policies library include**.**

**Ans: CIS and DISA policies**

**Q. 73.** What is the first step in automated mechanism of security hardening and validation??

**Ans: Scan an IT asset using Qualys nessus compliance scan**

**Q. 74.** There are------ benefits of version control**.**

**ANS: SEVEN**

**Q. 75**: ISO 31000 guidelines are centered on**?**

**Ans: Leadership and commitment.**

**48- chose the correct statement:**

A. Allow all IP address

B. Deny all IP address

C. Deny communication with known malicious IP address

D. Allow communication with unused IP address

**Question No 76**: **In small sized security organization in Pakistan, It is likely the number of security stall will?**

Ans: 1-5 or 2-4

**Question No 77: In Medium sized security organization in Pakistan, It is likely the number of security stall will?**

Ans: 10-15

**Question No 78**: **In Large sized security organization in Pakistan, It is likely the number of security stall will?**

Ans: 30 or Above 30

**Question No 79: What was the old name ISO27002:2013?**

Ans: ISO17799

**Question No 80: In PHP Guidelines " display error" shows**

A. On

B. off

C. True

D. False

**Question No 81: Android managers set as**

A. True

B. false

C. Enable

D. Disable

**55 Question No 82: by default Android managment set as ( is ka ans hai NoT ENABLE But option main not enable ni hai ap jo laga lo)**

A. True

B. False

C. Enable

D. Disable

**Question No 83: The number of ports is configurable, but the default scan**

Ans: approximately 1900 TCP ports and 180 UDP ports