SY0-301

CompTIA Security+ 2012

Document version: 8.04.11

Important Note About SY0-301 PDF

techeXams' **SY0-301 PDF** is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this exam questions. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. It's our guarantee.

Copyright

Disclaimer

Question: 1

Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

A. Connect the WAP to a different switch

B. Create a voice VLAN

C. Create a DMZ

D. Set the switch ports to 802.1q mode

Answer: B

Question: 2

Which of the following security tools can Jane, a security administrator, use to deter theft?

A. Virtualization

B. Cable locks

C. GPS tracking

D. Device encryption

Answer: B

Question: 3

Which of the following can be implemented on a laptop hard drive to help prevent unauthorized access to data?

A. Full disk encryption

B. Key escrow

C. Screen lock

D. Data loss prevention

Answer: A

Question: 4

Which of the following network devices allows Jane, a security technician, to perform malware inspection?

A. Load balancer

B. VPN concentrator

C. Firewall

D. NIPS

Answer: D

Question: 5

Which of the following is a valid server-role in a Kerberos authentication system?

A. Token issuing system

B. Security assertion server

C. Authentication agent

D. Ticket granting server

Answer: D

Question: 6

The accounting department needs access to network share A to maintain a number of financial reporting documents. The department also needs access to network share B in HR to view payroll documentation for cross-referencing items. Jane, an administrative assistant, needs access to view one document in network share A to gather data for management reports. Which of the following gives accounting and Jane the correct rights to these areas?

A. Accounting should be given read/write access to network share A and read access to network share B. Jane should be given read access for the specific document on network share A.

B. Accounting should be given read/write access to network share A and read access to network share B. Jane should be given read access to network share A.

C. Accounting should be given full access to network share A and read access to network share B. Jane should be given read/write access for the specific document on network share A.

D. Accounting should be given full access to network share A and read access to network share
B. Jane should be given read/write access to network share A.

Answer: A

Question: 7

Which of the following creates ciphertext by changing the placement of characters?

A. Transposition cryptography

B. Hashing

C. Elliptical cryptography

D. Digital signatures

Answer: A

Question: 8

Which of the following malware types uses stealth techniques to conceal itself, cannot install itself without user interaction, and cannot automatically propagate?

A. Rootkit

B. Logic bomb

C. Adware

D. Virus

Answer: A

Question: 9

When Pete, an employee, leaves a company, which of the following should be updated to ensure Pete's security access is reduced or eliminated?

A. RSA

B. CA

C. PKI

D. CRL

Answer: D

Question: 10

Which of the following should Matt, an administrator, change FIRST when installing a new access point?

A. SSID broadcast

B. Encryption

C. DHCP addresses

D. Default password

Answer: D

Question: 11

A datacenter has two rows of racks which are facing the same direction. Sara, a consultant, recommends the racks be faced away from each other. This is an example of which of the following environmental concepts?

A. Fire suppression

B. Raised floor implementation

C. Hot and cool aisles

D. Humidity controls implementation

Answer: C

Question: 12

Which of the following password policies is the MOST effective against a brute force network attack?

A. Password complexity

B. Password recovery

C. 30 day password expiration

D. Account lockout

Answer: D

Question: 13

Which of the following would BEST be used by Sara, the security administrator, to calculate the likelihood of an event occurring?

A. SLE

B. ALE

C. ROI

D. ARO

Answer: D

Question: 14

Which of the following should Matt, an administrator, implement in a server room to help prevent static electricity?

A. GFI electrical outlets

B. Humidity controls

C. ESD straps

D. EMI shielding

Answer: B

Question: 15

Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building Sara should immediately implement which of the following?

A. Acceptable Use Policy

B. Physical security controls

C. Technical controls

D. Security awareness training

Answer: D

Question: 16

Pete, an IT security technician, has been tasked with implementing physical security controls for his company's workstations. Which of the following BEST meets this need?

A. Host-based firewalls

B. Safe

C. Cable locks

D. Remote wipe

Answer: C

Question: 17

Which of the following creates ciphertext by replacing one set of characters for another?

A. Substitution cryptography

B. Elliptical cryptography

C. Digital signatures

D. Transposition cryptography

Answer: A

Question: 18

Sara, the IT Manager, would like to ensure that the router and switches are only available from the network administrator's workstation. Which of the following would be the MOST cost effective solution to ensure that only the network administrator can access these devices?

A. Restrict console ports

B. Time of day restrictions

C. Implement ACLs

D. Implement an out-of-band administrative network

Answer: C

Question: 19

A company is performing internal security audits after a recent exploitation on one of their proprietary applications. Sara, the security auditor, is given the workstation with limited documentation regarding the application installed for the audit. Which of the following types of testing methods is this?

A. Sandbox

B. White box

C. Black box

D. Gray box

Answer: D

Question: 20

A web server sitting in a secure DMZ has antivirus and anti-malware software which updates daily. The latest security patches are applied and the server does not run any database software. A day later, the web server is compromised and defaced. Which of the following is the MOST likely type of attack?

A. Header manipulation

B. Zero day exploit

C. Session hijacking

D. SQL injection

Answer: B

Question: 21

Which of the following protocols is MOST likely associated with network audit logging?

A. ICMP

B. FTPS

C. DNS

D. SNMP

Answer: D

Question: 22

Pete, a security administrator, is asked to install and configure centralized software to securely manage and collect statistics from all of the company's network devices. Which of the following should the software support?

A. 802.1x

B. ICMP

C. SNMPv3

D. SNMP

Answer: C

Question: 23

A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

A. Block port 23 on the L2 switch at each remote site

B. Block port 23 on the network firewall

C. Block port 25 on the L2 switch at each remote site

D. Block port 25 on the network firewall

Answer: B

Question: 24

Pete, a security administrator, is informed that people from the HR department should not have access to the accounting department's server, and the accounting department should not have access to the HR department's server. The network is separated by switches. Which of the following is designed to keep the HR department users from accessing the accounting department's server and vice-versa?

A. ACLs

B. VLANs

C. DMZs

D. NATS

Answer: B

Question: 25

Which of the following is BEST utilized to actively test security controls on a particular system?

A. Port scanning

B. Penetration test

C. Vulnerability scanning

D. Grey/Gray box

Answer: B

Question: 26

Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

A. Internet content filter

B. Firewall

C. Proxy server

D. Protocol analyzer

Answer: A

Question: 27

Which of the following has serious security implications for large organizations and can potentially allow an attacker to capture conversations?

A. Subnetting

B. NAT

C. Jabber

D. DMZ

Answer: C

Question: 28

Upper management decides which risk to mitigate based on cost. This is an example of:

A. Qualitative risk assessment

B. Business impact analysis

C. Risk management framework

D. Quantitative risk assessment

Answer: D

Question: 29

Isolation mode on an AP provides which of the following functionality types?

A. Segmentation of each wireless user from other wireless users

B. Disallows all users from communicating directly with the AP

C. Hides the service set identifier

D. Makes the router invisible to other routers

Answer: A

Question: 30

Employees are reporting that unauthorized personnel are in secure areas of the building. This is MOST likely due to lack of security awareness in which of the following areas?

A. Impersonation

B. Logical controls

C. Physical security controls

D. Access control policy

Answer: C

Question: 31

A forensic image of a hard drive has been created. Which of the following can be used to demonstrate the image has not been tampered with?

A. Chain of custody

B. Document the image file's size and time stamps

C. Encrypt the image file

D. Hash of the image file

Answer: D

Question: 32

Which of the following secure protocols is MOST commonly used to remotely administer Unix/Linux systems?

A. SSH

B. SCP

C. SFTP

D. SNMP

Answer: A

Question: 33

Which of the following security concepts can Matt, a security administrator, implement to support integrity?

A. Digital signatures

B. Trust models

C. Key escrow

D. Recovery agents

Answer: A

Question: 34

Which of the following combinations represents multifactor authentication?

A. Smart card and hard token

B. Voice print analysis and facial recognition

C. Username and PIN

D. Cipher lock combination and proximity badge

Answer: D

Question: 35

Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected?

A. Application design

B. Application security

C. Initial baseline configuration

D. Management of interfaces

Answer: C

Question: 36

Which of the following is Jane, a security administrator, MOST likely implementing when deleting all the unneeded files and modules of a newly installed application?

A. Exception handling

B. Patch management

C. System file clean up

D. Application hardening

Answer: D

Question: 37

Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

A. Availability

B. Integrity

C. Accounting

D. Confidentiality

Answer: B

Question: 38

Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?

A. AES

B. Blowfish

C. RC5

D. 3DES

Answer: B

Question: 39

Which of the following best practices makes a wireless network more difficult to find?

A. Implement MAC filtering

B. UseWPA2-PSK

C. Disable SSD broadcast

D. Power down unused WAPs

Answer: C

Question: 40

Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

A. Logic bomb

B. Worm

C. Trojan

D. Adware

Answer: C

Question: 41

The use of social networking sites introduces the risk of:

A. Disclosure of proprietary information

B. Data classification issues

C. Data availability issues

D. Broken chain of custody

Answer: A

Question: 42

Which the following flags are used to establish a TCP connection? (Select TWO).

A. PSH

B. ACK

C. SYN

D. URG

E. FIN

Answer: B, C

Question: 43

Which of the following is MOST likely to result in data loss?

A. Accounting transferring confidential staff details via SFTP to the payroll department

B. Back office staff accessing and updating details on the mainframe via SSH

C. Encrypted backup tapes left unattended at reception for offsite storage

D. Developers copying data from production to the test environments via a USB stick

Answer: D

Question: 44

Sara, a security administrator, sends an email to the user to verify their password has been reset. Which of the following threats is BEST mitigated by this action?

A. Spear phishing

B. Impersonation

C. Hoaxes

D. Evil twin

Answer: B

Question: 45

Which of the following describes an LDAP injection attack?

A. Creating a copy of user credentials during the LDAP authentication session

B. Manipulating an application's LDAP query to gain or alter access rights

C. Sending buffer overflow to the LDAP query service

D. Using XSS to direct the user to a rogue LDAP server

Answer: B

Question: 46

Which of the following concepts defines the requirement for data availability?

A. Authentication to RADIUS

B. Non-repudiation of email messages

C. Disaster recovery planning

D. Encryption of email messages

Answer: C

Question: 47

Which of the following is an example of multifactor authentication?

A. Credit card and PIN

B. Username and password

C. Password and PIN

D. Fingerprint and retina scan

Answer: A

Question: 48

Which of the following is an attack designed to steal cell phone data and contacts?

A. Bluesnarfing

B. Smurfing

C. Fuzzing

D. Bluejacking

Answer: A

Question: 49

Which of the following best practices is commonly found at the end of router ACLs?

A. Time of day restrictions

B. Implicit deny

C. Implicit allow

D. Role-based access controls

Answer: B

Question: 50

Which of the following uses TCP / UDP port 53 by default?

A. DNS

B. SFTP

C. SSH

D. NetBIOS

Answer: A

Question: 51

An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future?

A. Business continuity planning

B. Quantitative assessment

C. Data classification

D. Qualitative assessment

Answer: C

Question: 52

Sara, the network administrator, was alerted to an unauthorized email that was sent to specific VIPs in the company with a malicious attachment. Which of the following types of attacks is MOST likely being described?

A. Vishing

B. Whaling

C. DDoS

D. Pharming

Answer: B