SY0-601$^{Q\&As}$

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An employee\\'s company account was used in a data breach Interviews with the employee revealed:

The employee was able to avoid changing passwords by using a previous password again. The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.

Which of the following can be implemented to prevent these issues from reoccuring? (Select TWO)

A. Geographic dispersal

B. Password complexity

C. Password history

D. Geotagging

E. Password lockout

F. Geofencing

Correct Answer: CF

QUESTION 2

Which of the following Gieuster recovery tests ie the LEAST time coneuntng for tie easier recovery tearm?

A. Tabletop

B. Parallel

C. Full interruption

D. Simulation

Correct Answer: A

QUESTION 3

Which of the following types of disaster recovery plan exercises requires the least interruption to IT operations?

A. Parallel

B. Full-scale

C. Tabletop

D. Simulation

Correct Answer: C

QUESTION 4

An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that is discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box

B. Red-team

C. Bug bounty

D. Gray-box

E. Black-box

Correct Answer: B

Definitions from the most up to date Comptia handbook.

bug bounty=Reward scheme operated by software and web services vendors for reporting vulnerabilities. Where a pen test is performed on a contractual basis, costed by the consultant, a bug bounty program is a way of crowd sourcing detection of vulnerabilities. Some bug bounties are operated as internal programs, with rewards for employees only. Most are open to public submissions (tripwire.com/state-of-security/security-data-protection/cyber-security/essential-bugbounty-programs).

red team=The "hostile" or attacking team in a penetration test or incident response exercise.

QUESTION 5

A local coffee shop runs a small WiFi hotspot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies should the coffee shop use in place of PSK?

A. WEP

B. MSCHAP

C. WPS

D. SAE

Correct Answer: D

WPA3 - Simultaneous Authentication of Equals (SAE) replaces Pre-shared Key (PSK) in WPA2-Personal.

QUESTION 6

A security engineer is installing a WF io protect the company\\'s website from malicious wed requests over SSL, Which of the following is needed io meet the objective?

A. A reverse proxy

B. A decryption certificate

C. A split-tunnel VPN

D. Load-balanced servers

Correct Answer: B

WAF can only block abnormal traffic by filtering the plaintext data.

QUESTION 7

A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable To improve security? (Select TWO.)

A. RADIUS

B. PEAP

C. WPS

D. WEP-EKIP

E. SSL

F. WPA2-PSK

Correct Answer: AF

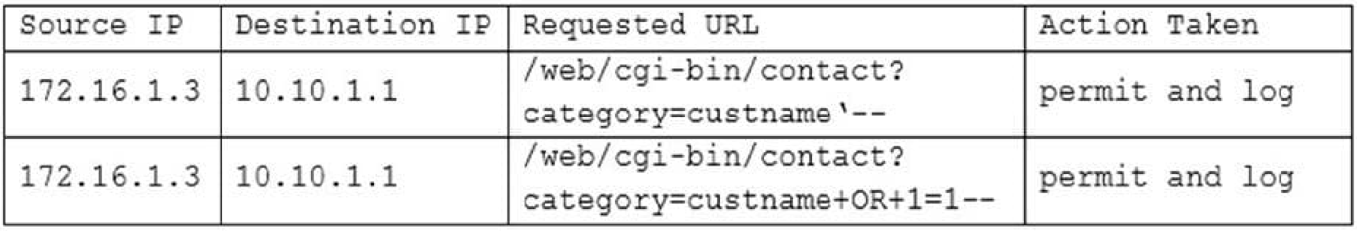
WPA2-PSK: WPA works using discrete modes for enterprise and personal use.

The most recent enterprise mode, WPA-EAP, uses a stringent 802.1x authentication.

The latest personal mode, WPA-PSK, uses Simultaneous Authentication of Equals (SAE) to create a secure handshake.

QUESTION 8

A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. A search of the WAF logs reveals the following output:



Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact? category=custname'--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact? category=custname+OR+1=1--	permit and log

Which of the following is MOST likely occurring?

A. XSS attack

B. SQLi attack

C. Replay attack

D. XSRF attack

Correct Answer: B

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. The giveaway here is the 1=1 in the query which is

essentially creating a condition that will automatically be true.

======================

Helpful Info:

XSS (Cross-Site Scripting) attacks -a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. Replay Attack - a kind of man-in-the-middle attack in which an attacker sniffs messages being sent on a

channel to intercept them and resend them under the cloak of authentic messages. CSRF (Cross Sit Request Forgery)- attacks that target functionality that causes a state change on the server, such as changing the victim\\'s email address or

password, or purchasing something.

QUESTION 9

A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?

A. Tokenization

B. Input validation

C. Code signing

D. Secure cookies

Correct Answer: B

QUESTION 10

During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

A. 1s

B. chflags

C. chmod

D. lsof

E. setuid

Correct Answer: C

Chmod removes the setuido permission, that is, it removes the S bit. Setuido is the specific permission, but it is removed with Chmod. https://www.cbtnuggets.com/blog/technology/system-admin/linux-file-permissions-understanding-setuid-setgid-and-the-sticky-bit

QUESTION 11

An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would BEST support the new office?

A. Always On

B. Remote access

C. Site-to-site

D. Full tunnel

Correct Answer: C

key word "expanded its operations" - a new office has been opened that needs to connect to already existing offices.

QUESTION 12

A security monitoring company offers a service that alerts its customers if their credit cards have been stolen. Which of the following is the MOST likely source of this information?

A. STIX

B. The dark web

C. TAXI

D. Social media

E. PCI

Correct Answer: B

QUESTION 13

The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going the polls. This is an example of:

A. prepending

B. An influence campaign

C. A watering-hole attack.

D. Intimidation.

E. Information elicitation.

Correct Answer: B

From Chapter 1 Social Engineering Techniques Influence campaigns involve the use of collected information and selective publication of material to key individuals in an attempt to alter perceptions and change people\\'s minds on a topic. One can engage in an influence campaign against a single person, but the effect is limited. Influence campaigns are even more powerful when used in conjunction with social media to spread influence through influencer propagation. Influencers are people who have large followings of people who read what they post, and in many cases act in accordance or agreement. This results in an amplifying mechanism, where single pieces of disinformation can be rapidly spread and build a following across the Internet.

Reference: https://www.darpa.mil/program/influence-campaign-awareness-and-sensemaking

QUESTION 14

An analyst receives multiple alerts for beaconing activity for a host on the network, After analyzing the activity, the analyst observes the following activity:

1.

A user enters comptia.org into a web browser.

2.

The website that appears is not the comptia.org site.

3.

The website is a malicious site from the attacker.

4.

Users in a different office are not having this issue.

Which of the following types of attacks was observed?

A. On-path attack

B. DNS poisoning

C. Locator (URL) redirection

D. Domain hijacking

Correct Answer: B

Only some client have this problem about web tarns to malicious site. So choose B.

QUESTION 15

The Chief information Securtty Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside cornpany. Additionally, the CISO would Ske this solution to provide the same protections even when a company laptop or mobile device ts away from # home office. Which of the following should the CISO choose?

A. CASB

B. Next-generation SWG

C. NGFW

D. Web-application firewall

Correct Answer: A