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.pass2lead.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A security analyst sees the following log output while reviewing web logs:

```
[02/Feb2019:03:39:21 -0000] 23.35.212.99 12.59.34.88
- "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswrd HTTP/1.0" 80 200 200
[02/Feb2019:03:39:85 -0000] 23.35.212.99 12.59.34.88
- "GET /uri/input.action?query=/../../../etc/password HTTP/1.0" 80 200 200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

A. Secure cookies

B. Input validation

C. Code signing

D. Stored procedures

Correct Answer: B

QUESTION 2

A candidate attempts to go to but accidentally visits http://comptiia.org. The malicious website looks exactly like the legitimate website. Which of the following best describes this type of attack?

A. Reconnaissance

B. Impersonation

C. Typosquatting

D. Watering-hole

Correct Answer: C

Typosquatting is a type of cyberattack that involves registering domains with deliberately misspelled names of well-known websites. The attackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes. Visitors may end up at these alternative websites by inadvertently mistyping the name of popular websites into their web browser or by being lured by a phishing scam. The attackers may emulate the look and feel of the legitimate websites and trick users into entering sensitive information or downloading malware. References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting

QUESTION 3

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

A. openssl

B. hping

C. netcat

D. tcpdump

Correct Answer: D

tcpdump for sure. OpenSSL is what might be used to secure traffic, but tcpdump is a packet analyzer that will show you if data is being sent in the clear. It will verify OpenSSL is working.

QUESTION 4

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 5

A large industrial system\\'s smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company\\'s security manager notices the generator\\'s IP is sending packets to an internal file server\\'s IP.

Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation

B. Firewall whitelisting

C. Containment D. isolation

Correct Answer: A

Segmentation. DMZ and VLAN are examples of segmentation. You can configure the device to be on its own isolated network while having access to the third-party vendor. The device will still try to communicate with the file server but traffic will be dropped and logged. This is how you would want to set up IoT and untrusted devices.