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.pass4itsure.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

Which of the technologies is used to actively monitor for specific file types being transmitted on the network?

A. File integrity monitoring

B. Honeynets

C. Tcpreplay

D. Data loss prevention

Correct Answer: D

QUESTION 2

A security analyst has identified malware spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT?

A. Review how the malware was introduced to the network.

B. Attempt to quarantine all infected hosts to limit further spread.

C. Create help desk tickets to get infected systems reimaged.

D. Update all endpoint antivirus solutions with the latest updates.

Correct Answer: B

Phases in the Incident Response Plan

1.

Preparation: The organization plans out how they will respond to attack, this can involve:

2.

Identification: Detecting and determining whether an incident has occurred.

3.

Containment: Once a threat has been identified, the organization must limit or prevent any further damage. 4. Eradication: The removal of the threat

5.

Recovery: Restoring systems affected by the incident

6.

Lessons Learned: Where the organization reviews their incident response and prepare for a future attack

QUESTION 3

During a forensic investigation, an analyst uses software to create a checksum of the affected subject\\'s email file. Which of the following is the analyst practicing?

A. Chain of custody

B. Data recovery

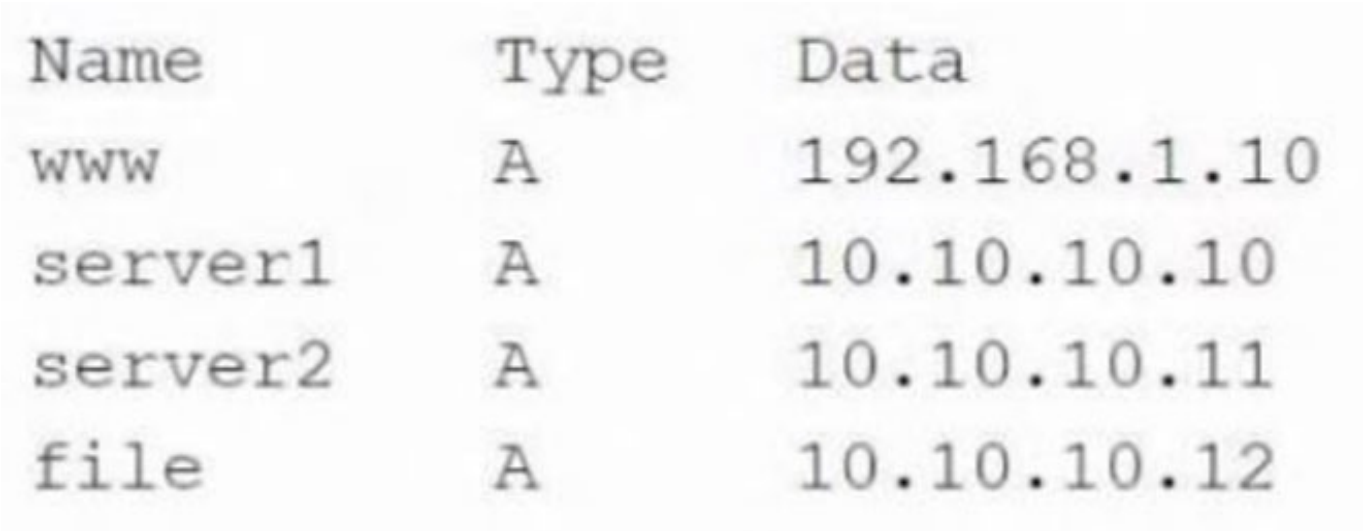
C. Non-repudiation

D. Integrity

Correct Answer: D

QUESTION 4

A security analyst is investigating some users who are being redirected to a fake website that resembles www.comptia.org. The following output was found on the naming server of the organization:



Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

Which of the following attacks has taken place?

A. Domain reputation

B. Domain hijacking

C. Disassociation

D. DNS poisoning

Correct Answer: D

DNS server cache poisoning aims to corrupt the records held by the DNS server itself. This can be accomplished by performing DoS against the server that holds the authorized records for the domain, and then spoofing replies to requests from other name servers. Another attack involves getting the victim name server to respond to a recursive query from the attacking host. A recursive query compels the DNS server to query the authoritative server for the answer on behalf of the client.

QUESTION 5

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan

B. A communications plan

C. A business continuity plan

D. A disaster recovery plan

Correct Answer: A