CompTIA

Exam Questions SY0-601

CompTIA Security+

https://certificationstime.com/

Questions & Answers
PDF

→ Latest Exam Questions
→ Verified Answers
→ 99% Success Rate
→ Free 90 Days Update
→ Instant Access
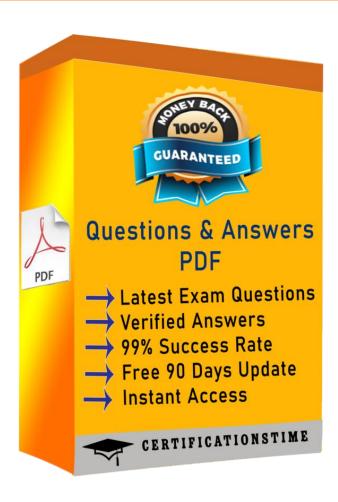
CERTIFICATIONSTIME

QUESTION 1

The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered

throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.

B. Segment the network with firewalls.

C. Update all antivirus signatures daily.

D. Implement application blacklisting.

Correct Answer: B

QUESTION 2

A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues

from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has

worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING:   REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Get Certified In First Attempt

visit - https://certificationstime.com/

Which of the following network attacks is the researcher MOST likely experiencing?

A. MAC cloning

B. Evil twin

C. Man-in-the-middle

D. ARP poisoning

Correct Answer: C

QUESTION 3

Which of the following should be put in place when negotiating with a new vendor about the timeliness of the

response to a significant outage or incident?

A. MOU

B. MTTR

C. SLA

D. NDA

Correct Answer: C

QUESTION 4

A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to

be non-disruptive and user friendly. Which of the following technologies should the IT manager use when

implementing MFA?

A. One-time passwords

B. Email tokens

C. Push notifications

D. Hardware authentication

Correct Answer: C

QUESTION 5

A RAT that was used to compromise an organization's banking credentials was found on a user's computer.

The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system

as part of a remote management tool set. Which of the following recommendations would BEST prevent this

from reoccurring?

A. Create a new acceptable use policy.

B. Segment the network into trusted and untrusted zones.

C. Enforce application whitelisting.

D. Implement DLP at the network boundary.

Correct Answer: C

QUESTION 6

A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of

the organization's vulnerabilities. Which of the following would BEST meet this need?

A. CVE

B. SIEM

C. SOAR

D. CVSS

Correct Answer: D

Full Access:

https://certificationstime.com/updated/sy0-601-exam-dumps-pdf/