SY0-401 Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-401 Exam with 100% Guarantee

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

https://www.lead4pass.com/SY0-401.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An administrator needs to submit a new CSR to a CA. Which of the following is a valid FIRST step?

A. Generate a new private key based on AES.

B. Generate a new public key based on RSA.

C. Generate a new public key based on AES.

D. Generate a new private key based on RSA.

Correct Answer: D

Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The private key is needed to produce, but it is not part of, the CSR. The private key is an RSA key. The private encryption key that will be used to

protect sensitive information.

Note: A CSR or Certificate Signing request is a block of encrypted text that is generated on the server that the certificate will be used on. It contains information that will be included in your certificate such as your organization name, common

name (domain name), locality, and country. It also contains the public key that will be included in your certificate. A private key is usually created at the same time that you create the CSR.

QUESTION 2

A security administrator is using a software program to test the security of a wireless access point. After running the program for a few hours, the access point sends the wireless secret key back to the software program. Which of the following attacks is this an example of?

A. WPS

B. IV

C. Deauth

D. Replay

Correct Answer: C

QUESTION 3

A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application. The security administrator notices that the new application uses a port typically monopolized by a virus. The security administrator denies the request and suggests a new port or service be used to complete the application\\'s task. Which of the following is the security administrator practicing in this example?

A. Explicit deny

B. Port security

C. Access control lists

D. Implicit deny

Correct Answer: C

Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted.

QUESTION 4

A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.

VPN log:

```
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
```

Corporate firewall log:

```
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
```

Workstation host firewall log:

```
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
```


Which of the following is preventing the remote user from being able to access the workstation?

A. Network latency is causing remote desktop service request to time out

B. User1 has been locked out due to too many failed passwords

C. Lack of network time synchronization is causing authentication mismatches

D. The workstation has been compromised and is accessing known malware sites

E. The workstation host firewall is not allowing remote desktop connections

Correct Answer: B

QUESTION 5

A fiber company has acquired permission to bury a fiber cable through a famer\\'s land. Which of the following should be in the agreement with the farmer to protect the availability of the network?

A. No farm animals will graze near the burial site of the cable

B. No digging will occur near the burial site of the cable

C. No buildings or structures will be placed on top of the cable

D. No crops will be planted on top of the cable

Correct Answer: B