SY0-501 Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

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

https://www.lead4pass.com/sy0-501.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A systems administrator wants to implement a wireless protocol that will allow the organization to authenticate mobile devices prior to providing the user with a captive portal login. Which of the following should the systems administrator configure?

A. L2TP with MAC filtering

B. EAP-TTLS

C. WPA2-CCMP with PSK

D. RADIUS federation

Correct Answer: D

RADIUS generally includes 802.1X that pre-authenticates devices.

QUESTION 2

An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to. This is because the encryption scheme in use adheres to:

A. Asymmetric encryption

B. Out-of-band key exchange

C. Perfect forward secrecy

D. Secure key escrow

Correct Answer: C

Exam E

QUESTION 3

A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:

```
Context Details for Signature 20000018334
Context: Parameter
Actual Parameter Name: Account_Name
Parameter Value: SELECT * FROM Users WHERE Username='1' OR '1'='1' AND Password='1' OR '1'='1'
```

Based on this data, which of the following actions should the administrator take?

A. Alert the web server administrators to a misconfiguration.

B. Create a blocking policy based on the parameter values.

C. Change the parameter name `Account_Name\\' identified in the log.

D. Create an alert to generate emails for abnormally high activity.

Correct Answer: D

QUESTION 4

An organization would like to set up a more robust network access system. The network administrator suggests the organization move to a certificate-based authentication setup in which a client-side certificate is used while connecting. Which of the following EAP types should be used to meet these criteria?

A. EAP-TLS

B. EAP-FAST

C. EAP-MD5

D. EAP-TTLS

Correct Answer: A

QUESTION 5

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

QUESTION 6

A security analyst is determining the point of compromise after a company was hacked. The analyst checks the server logs and sees that a user account was logged in at night, and several large compressed files were exfiltrated. The analyst then discovers the user last logged in four years ago and was terminated. Which of the following should the security analyst recommend to prevent this type of attack in the future? (Choose two.)

A. Review and update the firewall settings

B. Restrict the compromised user account

C. Disable all user accounts that are not logged in to for 180 days

D. Enable a login banner prohibiting unauthorized use

E. Perform an audit of all company user accounts

F. Create a honeypot to catch the hacker

Correct Answer: BE

QUESTION 7

An analyst generates the following color-coded table shown in the exhibit to help explain the risk of potential incidents in the company. The vertical axis indicates the likelihood or an incident, while the horizontal axis indicates the impact.

High	Yellow	Red	Pink
Medium	Green	Yellow	Red
Low	Green	Green	Yellow
	Low	Medium	High

Which of the following is this table an example of?

A. Internal threat assessment

B. Privacy impact assessment

C. Qualitative risk assessment

D. Supply chain assessment

Correct Answer: C

QUESTION 8

An organization\\'s employees currently use three different sets of credentials to access multiple internal resources. Management wants to make this process less complex. Which of the following would be the BEST option to meet this goal?

A. Transitive trust

B. Single sign-on

C. Federation

D. Secure token

Correct Answer: B

QUESTION 9

For each of the given items, select the appropriate authentication category from the drop down choices.

Select the appropriate authentication type for the following items:

Hot Area:

Item	Response
Fingerprint scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
PIN number	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Retina Scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication

Correct Answer:

Item	Response
Fingerprint scan	Biometric authentication
Hardware token	One Time Password
Smart card	Multi-factor
Password	PAP authentication
PIN number	PAP authentication
Retina Scan	Biometric authentication

Biometrics refers to a collection of physical attributes of the human body that can be used as identification or an authentication factor. Fingerprints and retinas are physical attributes of the human body.

Two types of tokens exist, Time-based one-time password (TOTP) tokens and HMACbased one-time password (HOTP). TOTP tokens generate passwords at fixed time intervals, whereas HOTP tokens generate passwords not based on fixed

time intervals but instead based on a non-repeating one-way function, such as a hash or HMAC operation.

Smart cards can have Multi-factor and proximity authentication embedded into it.

PAP allows for two entities to share a password in advance and use the password as the basis of authentication. The same goes for PIN numbers.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 282, 285

http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle

http://en.wikipedia.org/wiki/Smart_card#Security

QUESTION 10

An organization has the following password policies:

Passwords must be at least 16 characters long.

A password cannot be the same as any previous 20 passwords.

Three failed login attempts will lock the account for five minutes.

Passwords must have one uppercase letter, one lowercase letter, and one non- alphanumeric symbol.

A database server was recently breached, and the incident response team suspects the passwords were compromised. Users with permission on that database server were forced to change their passwords for that server. Unauthorized and suspicious logins are now being detected on a completely separate server. Which of the following is MOST likely the issue and the best solution?

A. Some users are reusing passwords for different systems; the organization should scan for password reuse across systems.

B. The organization has improperly configured single sign-on; the organization should implement a RADIUS server to control account logins.

C. User passwords are not sufficiently long or complex: the organization should increase the complexity and length requirements for passwords.

D. The trust relationship between the two servers has been compromised: the organization should place each server on a separate VLAN.

Correct Answer: A

QUESTION 11

Which of the following BEST explains the difference between a credentialed scan and a non- credentialed scan?

A. A credentialed scan sees devices in the network, including those behind NAT, while a non- credentialed scan sees outward-facing applications.

B. A credentialed scan will not show up in system logs because the scan is running with the necessary authorization, while non-credentialed scan activity will appear in the logs.

C. A credentialed scan generates significantly more false positives, while a non-credentialed scan generates fewer false positives

D. A credentialed scan sees the system the way an authorized user sees the system, while a non- credentialed scan sees the system as a guest.

Correct Answer: D

QUESTION 12

Which of the following controls does a mantrap BEST represent?

A. Deterrent

B. Detective

C. Physical

D. Corrective

Correct Answer: C

QUESTION 13

A recent internal audit is forcing a company to review each internal business unit\\'s VMs because the cluster they are installed on is in danger of running out of computer resources. Which of the following vulnerabilities exist?

A. Buffer overflow

B. End-of-life systems

C. System sprawl

D. Weak configuration

Correct Answer: C

QUESTION 14

A company is allowing a BYOD policy for its staff. Which of the following is a best practice that can decrease the risk of users jailbreaking mobile devices?

A. Install a corporately monitored mobile antivirus on the devices.

B. Prevent the installation of applications from a third-party application store.

C. Build a custom ROM that can prevent jailbreaking.

D. Require applications to be digitally signed.

Correct Answer: D

QUESTION 15

An audit has revealed that database administrators are also responsible for auditing database changes and backup logs. Which of the following access control methodologies would BEST mitigate this concern?

A. Time of day restrictions

B. Principle of least privilege

C. Role-based access control

D. Separation of duties

Correct Answer: D

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: