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.pass2lead.com/sy0-501.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 Chief Executive Officer (CEO) is staying at a hotel during a business trip. The hotel\\'s wireless network does not show a lock symbol. Which of the following precautions should the CEO take? (Select TWO).

A. Change the connection type to WPA2.

B. Change TKIP to CCMR

C. Use a VPN.

D. Tether to a mobile phone.

E. Create a tunnel connection with EAP-TTLS.

Correct Answer: CE

QUESTION 2

DRAG DROP

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)

1.

Hostname: ws01

2.

Domain: comptia.org

3.

IPv4: 10.1.9.50

4.

IPV4: 10.2.10.50

5.

Root: home.aspx

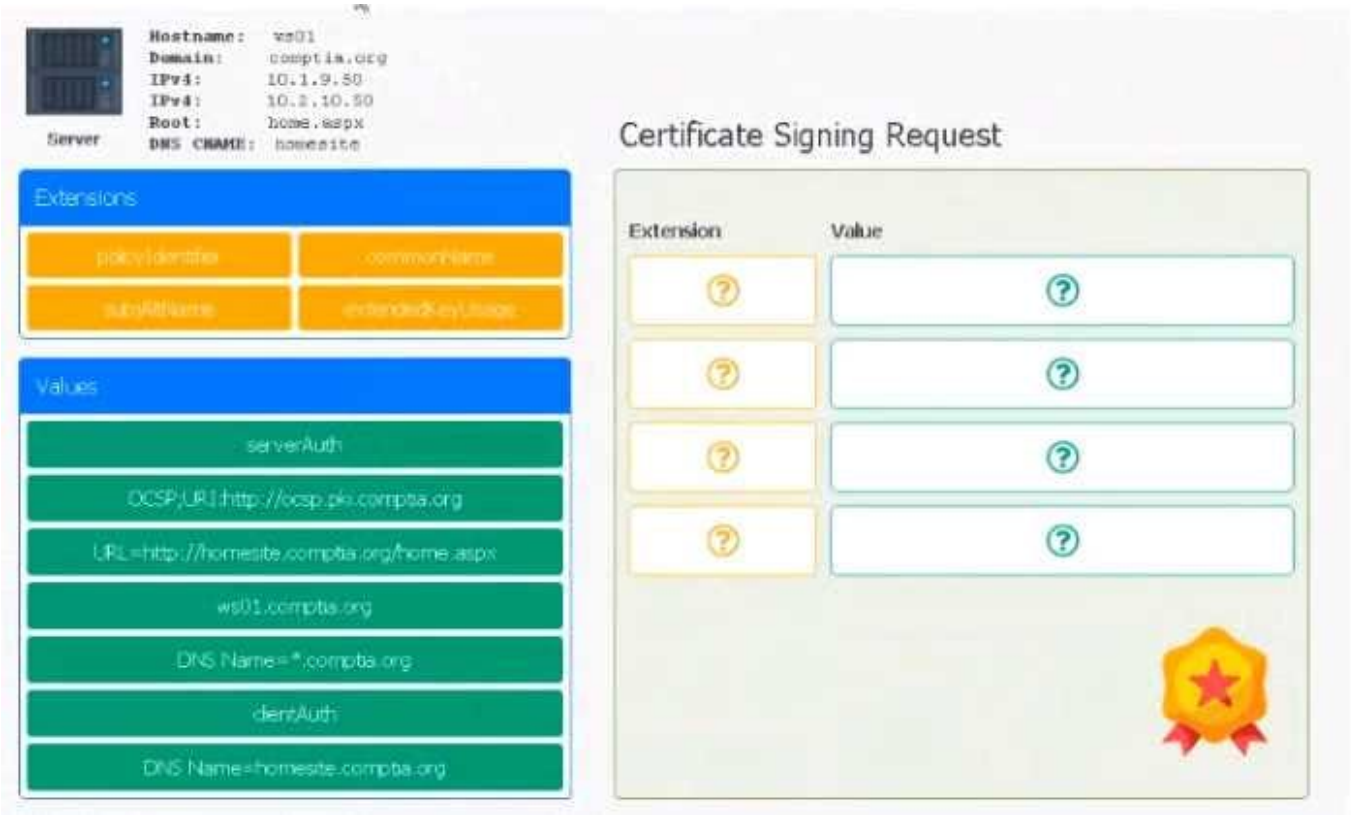
6.

DNS CNAME:homesite.

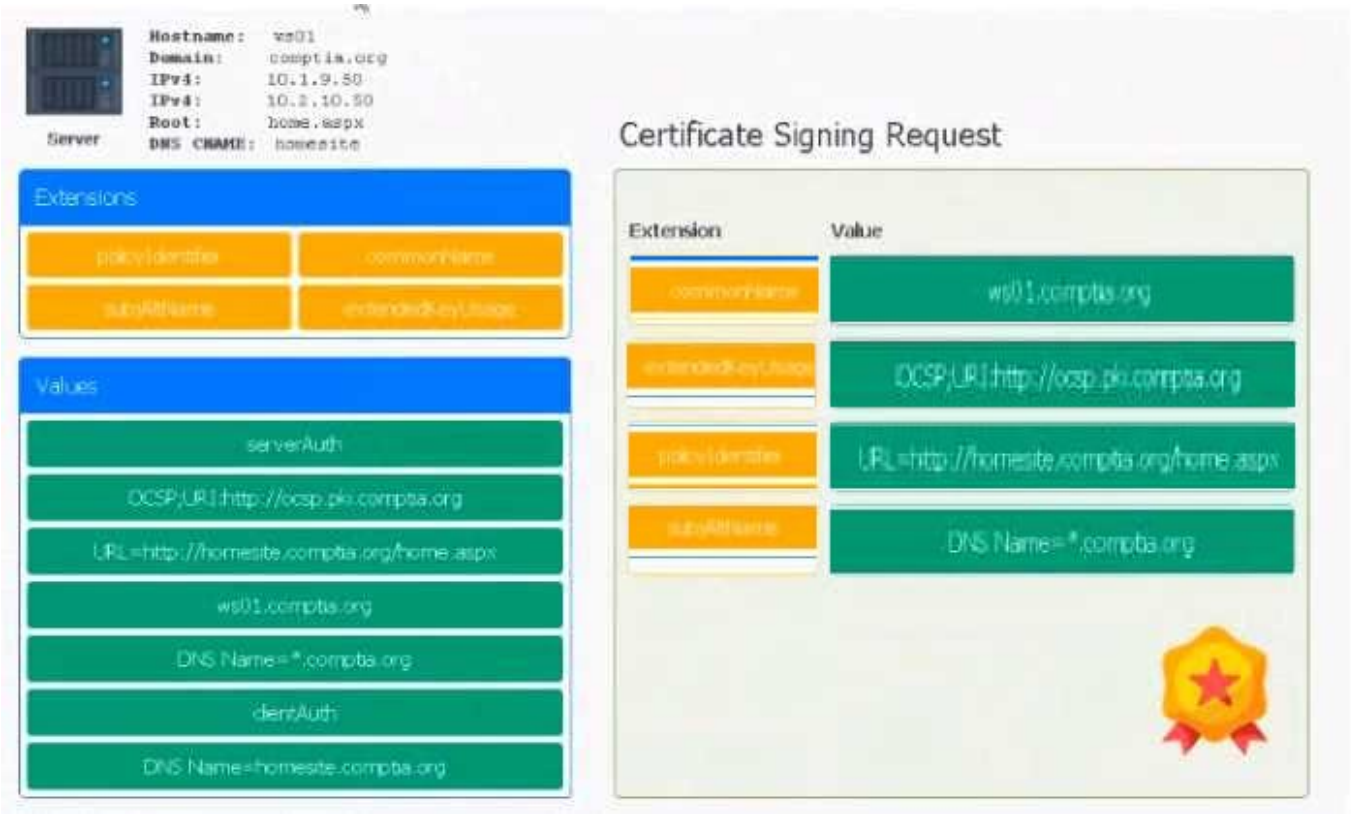
Instructions:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.

Select and Place:



Correct Answer:



QUESTION 3

A developer is building a new web portal for internal use. The web portal will only the accessed by internal users and will store operational documents. Which of the following certicate types should the developer install if the company is MOST interested in minimizing costs?

A. Wildcard

B. Code signing

C. Root

D. Self-signed

Correct Answer: A

QUESTION 4

Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and the sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe\\'s emails were intercepted. Which of the following MOST likely caused the data breach?

A. Policy violation

B. Social engineering

C. Insider threat

D. Zero-day attack

Correct Answer: A

QUESTION 5

While monitoring the SIEM, a security analyst observes traffic from an external IP to an IP address of the business network on port 443. Which of the following protocols would MOST likely cause this traffic?

A. HTTP

B. SSH

C. SSL

D. DNS

Correct Answer: B

QUESTION 6

An administrator needs to protect five websites with SSL certificates. Three of the websites have different domain names, and two of the websites share the domain name but have different subdomain prefixes. Which of the following SSL certificates should the administrator purchase to protect all the websites and be able to administer them easily at a later time?

A. One SAN certificate

B. One Unified Communications Certificate and one wildcard certificate

C. One wildcard certificate and two standard certificates

D. Five standard certificates

Correct Answer: A

QUESTION 7

A security analyst is looking for a solution to help communicate to the leadership team the severity 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: C

QUESTION 8

During a routine check, a security analyst discovered the script responsible for the backup of the corporate file server has been changed to the following:

```
date = get_currentdate()
if date = $userA.Birthdate then
   exec ' rm -rf /'
end if
```

Which of the following BEST describes the type of malware the analyst discovered?

A. Keylogger

B. Rootkit

C. RAT

D. Logic bomb

Correct Answer: D

QUESTION 9

Ann. An employee in the payroll department, has contacted the help desk citing multiple issues with her device, including: Slow performance Word documents, PDFs, and images no longer opening A pop-up Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor.

With which of the following is the device MOST likely infected?

A. Spyware

B. Crypto-malware

C. Rootkit

D. Backdoor

Correct Answer: D

QUESTION 10

A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server. Which of the following represents the MOST secure way to configure the new network segment?

A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.

B. The segment should be placed in the existing internal VLAN to allow internal traffic only.

C. The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.

D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

Correct Answer: A

QUESTION 11

The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small

server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does

business having varying data retention and privacy laws.

Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers

B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location

C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations

D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

Correct Answer: C

QUESTION 12

A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name. Which of the following should the security engineer use?

A. Wildcard certificate

B. Extended validation certificate

C. Certificate chaining

D. Certificate utilizing the SAN file

Correct Answer: D

SAN = Subject Alternate Names

QUESTION 13

A company has critical systems that are hosted on an end-of-life OS. To maintain operations and mitigate potential vulnerabilities, which of the following BEST accomplishes this objective?

A. Use application whitelisting.

B. Employ patch management.

C. Disable the default administrator account.

D. Implement full-disk encryption.

Correct Answer: A

QUESTION 14

An active/passive configuration has an impact on:

A. confidentiality

B. integrity

C. availability

D. non-repudiation

Correct Answer: C

QUESTION 15

A security administrator wants to determine if a company\\'s web servers have the latest operating system and application patches installed. Which of the following types of vulnerability scans should be conducted?

A. Non-credentialed

B. Passive

C. Port

D. Credentialed

E. Red team

F. Active

Correct Answer: D

Latest SY0-501 Dumps SY0-501 PDF Dumps SY0-501 VCE Dumps