DUMPSBOSS.COM

CompTIA Security+ Exam

CompTIA SY0-601

Version Demo

Total Demo Questions: 20

Total Premium Questions: 726

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

QUESTION NO: 1

The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the following would BEST address this security concern?

A. Install a smart meter on the staff WiFi.

B. Place the environmental systems in the same DHCP scope as the staff WiFi.

C. Implement Zigbee on the staff WiFi access points.

D. Segment the staff WiFi network from the environmental systems network.

ANSWER: D

QUESTION NO: 2

A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

A. Dual power supply

B. Off-site backups

C. Automatic OS upgrades

D. NIC teaming

E. Scheduled penetration testing

F. Network-attached storage

ANSWER: A B

QUESTION NO: 3

A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user Information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

A. Identity processor

B. Service requestor

C. Identity provider

D. Service provider

E. Tokenized resource

F. Notarized referral

ANSWER: C D

QUESTION NO: 4

Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

A. Data encryption

B. Data masking

C. Anonymization

D. Tokenization

ANSWER: A

Explanation:

Reference: https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/tokenization-vs-encryption.html

QUESTION NO: 5

Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

A. Hashing

B. Salting

C. Integrity

D. Digital signature

ANSWER: A

Explanation:

Hashing is a cryptographic function that produces a unique fixed-size output (i.e., hash value) from an input (i.e., data). The hash value is a digital fingerprint of the data, which means that if the data changes, so too does the hash value. By comparing the hash value of the downloaded file with the hash value provided by the security website, the security analyst can verify that the file has not been altered in transit or corrupted.

QUESTION NO: 6

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

A. MAC filtering

B. Zero trust segmentation

C. Network access control

D. Access control vestibules

E. Guards

F. Bollards

ANSWER: C E

Explanation:

Network access control (NAC) is a technique that restricts access to a network based on the identity, role, device, location, or other criteria of the users or devices. NAC can prevent unauthorized or malicious devices from connecting to a network and accessing sensitive data or resources.

Guards are physical security personnel who monitor and control access to a facility. Guards can prevent unauthorized or malicious individuals from entering a facility and plugging in a remotely accessible device.

QUESTION NO: 7

An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?

A. Apply a DLP solution.

B. Implement network segmentation

C. Utilize email content filtering,

D. isolate the infected attachment.

ANSWER: B

QUESTION NO: 8

A security analyst is reviewing output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1
```

Which of the following types of attack is MOST likely being conducted?

A. SQLi

B. CSRF

C. Session replay

D. API

ANSWER: B

Explanation:

Reference: https://owasp.org/www-community/attacks/csrf#:~:text=Cross%2DSite%20Request%20Forgery%20(CSRF,which%20they're%20currently%20authenticated.&text=If%20the%20victim%20is%20an,compromise%20the%20entire%20web%20application

QUESTION NO: 9

A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Choose two.)

A. Password and security question

B. Password and CAPTCHA

C. Password and smart card

D. Password and fingerprint

E. Password and one-time token

F. Password and voice

ANSWER: C D

QUESTION NO: 10

A Chief Information Officer is concerned about employees using company-issued laptops lo steal data when accessing network shares. Which of the following should the company Implement?

A. DLP

B. CASB

C. HIDS

D. EDR

E. UEFI

ANSWER: A

QUESTION NO: 11

A security engineer needs to implement the following requirements:

- All Layer 2 switches should leverage Active Directory for authentication.
- All Layer 2 switches should use local fallback authentication of Active Directory is offline. - All Layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Choose two.)

A. Implement RADIUS.

B. Configure AAA on the switch with local login as secondary.

C. Configure port security on the switch with the secondary login method.

D. Implement TACACS+.

E. Enable the local firewall on the Active Directory server.

F. Implement a DHCP server.

ANSWER: A C

QUESTION NO: 12

A security administrator Is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).

A. IPSec

B. SFTP

C. SRTP

D. LDAPS

E. S/MIME

F. SSL VPN

ANSWER: A F

Explanation:

IPSec (Internet Protocol Security) is a technology that provides secure communication over the internet by encrypting traffic and authenticating it at both the sender and receiver. It can be used to create secure tunnels between two or more devices, allowing users to access resources securely and privately.

SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses an SSL/TLS connection to encrypt traffic between two or more devices. It is a secure and reliable solution for providing remote access, as all traffic is encrypted and authenticated. Additionally, SSL VPNs can also be used to restrict access to certain websites and services, making them a secure and robust solution for remote access.

QUESTION NO: 13 - (HOTSPOT)

HOTSPOT

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Hot Area:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet / RAT / Logic Bomb	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services

internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

ANSWER:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing

Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

Explanation:

QUESTION NO: 14

After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:

A. privilege escalation

B. footprinting

C. persistence

D. pivoting.

ANSWER: D

QUESTION NO: 15

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO).

A. MAC filtering

B. Zero trust segmentation

C. Network access control

D. Access control vestibules

E. Guards

F. Bollards.

ANSWER: A C

Explanation:

MAC filtering is a method of allowing or denying access to a network based on the MAC address of the device attempting to connect. By creating a list of approved MAC addresses, the organization can prevent unauthorized devices from connecting to the network.

Network Access Control (NAC) is a security solution that allows organizations to restrict access to their networks based on the device's identity, configuration, and security posture. This can be used to ensure that only legitimate devices are allowed to connect to the network, and any unauthorized devices are blocked.

QUESTION NO: 16

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file. After the capture is complete, the analyst needs to review the first transactions quickly

and then search the entire series of requests for a particular string. Which of the following would be BEST to use to accomplish this task? (Choose two.)

A. head

B. tcpdump

C. grep

D. tail

E. curl

F. openssl

G. dd

ANSWER: B D

Explanation:

Reference: https://science.hamptonu.edu/compsci/docs/iac/packet_sniffing.pdf

QUESTION NO: 17

A company would like to set up a secure way to transfer data between users via their mobile phones The company's top pnonty is utilizing technology that requires users to be in as close proximity as possible to each other. Which of the following connection methods would BEST fulfill this need?

A. Cellular

B. NFC

C. Wi-Fi

D. Bluetooth

ANSWER: B

Explanation:

NFC allows two devices to communicate with each other when they are in close proximity to each other, typically within 5 centimetres. This makes it the most secure connection method for the company's data transfer requirements.

QUESTION NO: 18

A corporate security team needs to secure the wireless perimeter of its physical facilities to ensure only authorized users can access corporate resources. Which of the following should the security team do? (Refer the answer from CompTIA SY0-601 Security+ documents or guide at comptia.org)

A. Identify rogue access points.

B. Check for channel overlaps.

C. Create heat maps.

D. Implement domain hijacking.

ANSWER: A

Explanation:

Based on CompTIA SY0-601 Security+ guide, the answer to the question is A. Identify rogue access points.

To secure the wireless perimeter of its physical facilities, the corporate security team should focus on identifying rogue access points, which are unauthorized access points that have been set up by employees or outsiders to bypass security controls. By identifying and removing these rogue access points, the team can ensure that only authorized users can access corporate resources through the wireless network.

https://www.comptia.org/training/books/security-sy0-601-study-guide

QUESTION NO: 19 - (SIMULATION)

SIMULATION

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

INSTRUCTIONS

Perform the following steps:

1. Configure the RADIUS server.

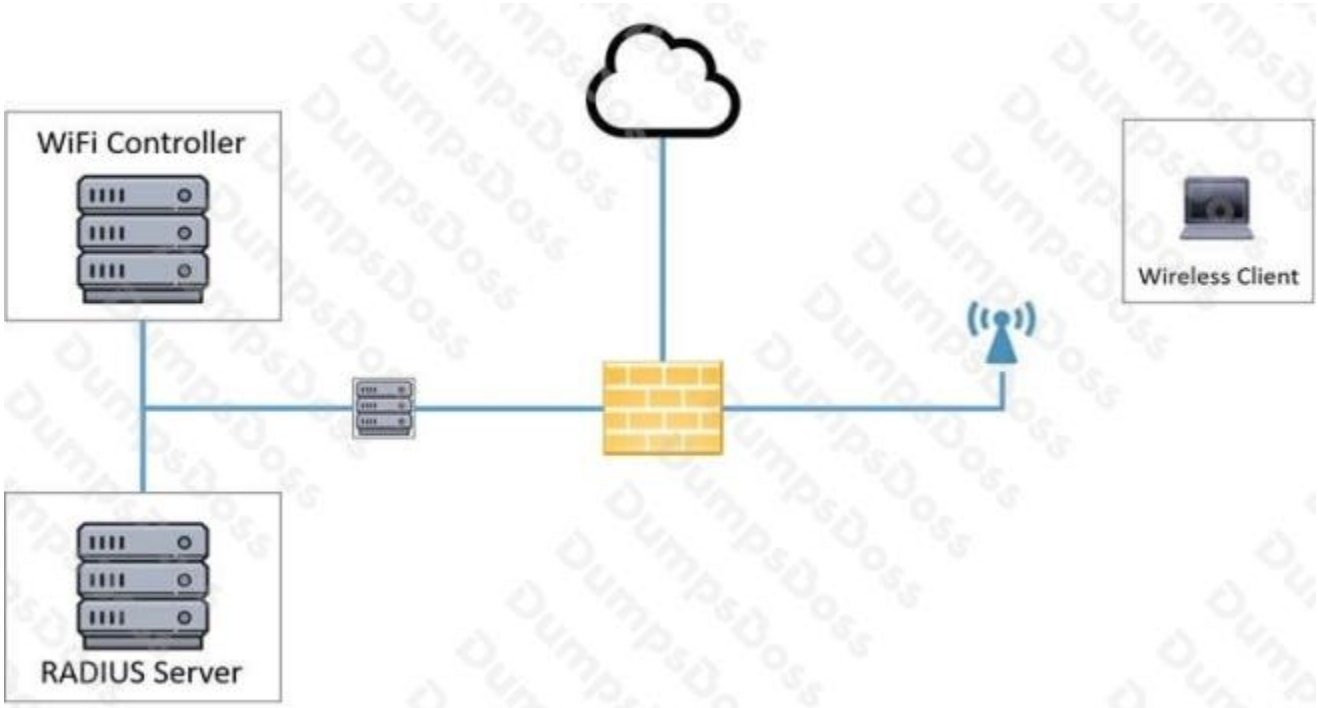
2. Configure the WiFi controller.

3. Preconfigure the client for an incoming guest. The guest AD credentials are:

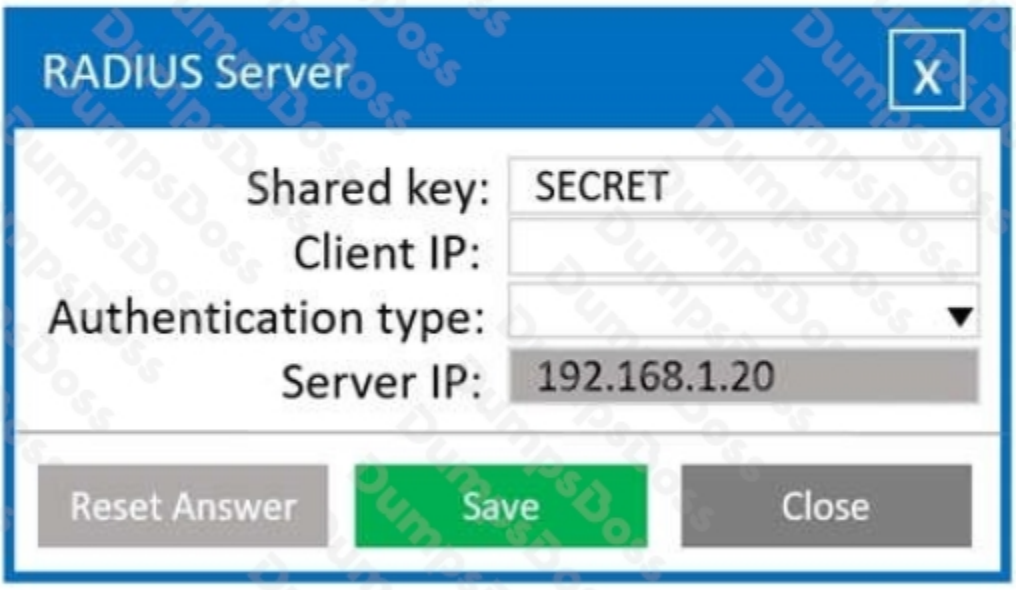
User: guest01

Password: guestpass

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


WiFi Controller
Wireless Client
RADIUS Server


WiFi Controller
X
SSID:
CORPGUEST
Shared key:
AAA server IP:
PSK:
Authentication type:
Controller IP:
192.168.1.10
Reset Answer
Save
Close


RADIUS Server
X
Shared key:
SECRET
Client IP:
Authentication type:
Server IP:
192.168.1.20
Reset Answer
Save
Close


Wireless Client
SSID:
Username:

ANSWER: See explanation below.

Explanation:

Configure the settings as shown below:

QUESTION NO: 20 - (DRAG DROP)

DRAG DROP

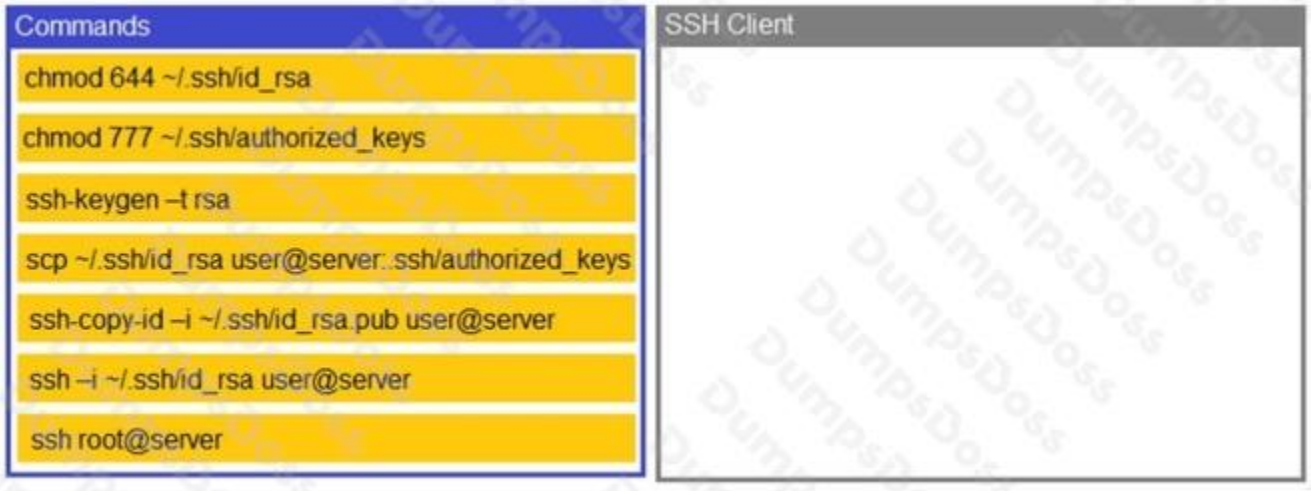
A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



ANSWER:

Explanation: