

DUMPS ARENA

CompTIA Security+ Exam 2023

CompTIA SY0-601

Version Demo

Total Demo Questions: 20

Total Premium Questions: 726

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1 - (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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services

internally developed application that bypasses account login.	Application	Botnet	Enable DDoS protection
		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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: 2**

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: 3**

During a routine scan of a wireless segment at a retail company, a security administrator discovers several devices are connected to the network that do not match the company's naming convention and are not in the asset inventory. WiFi access is protected with 256-bit encryption via WPA2. Physical access to the company's facility requires two-factor authentication using a badge and a passcode. Which of the following should the administrator implement to find and remediate the issue? (Choose two.)

- A. Check the SIEM for failed logins to the LDAP directory.
- B. Enable MAC filtering on the switches that support the wireless network.
- C. Run a vulnerability scan on all the devices in the wireless network.
- D. Deploy multifactor authentication for access to the wireless network.
- E. Scan the wireless network for rogue access points.
- F. Deploy a honeypot on the network.

ANSWER: B E

QUESTION NO: 4

A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

- A. The Diamond Model of Intrusion Analysis
- B. The Cyber Kill Chain
- C. The MITRE CVE database
- D. The incident response process

ANSWER: A**Explanation:**

Reference: <https://cyware.com/educational-guides/incident-response/what-is-the-diamond-model-of-intrusion-analysis-5f02>

QUESTION NO: 5 - (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:

Commands	SSH Client
<code>chmod 644 ~/.ssh/id_rsa</code>	
<code>chmod 777 ~/.ssh/authorized_keys</code>	
<code>ssh-keygen -t rsa</code>	
<code>scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys</code>	
<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>	
<code>ssh -i ~/.ssh/id_rsa user@server</code>	
<code>ssh root@server</code>	

ANSWER:

Commands	SSH Client
<code>chmod 644 ~/.ssh/id_rsa</code>	<code>ssh-keygen -t rsa</code>
<code>chmod 777 ~/.ssh/authorized_keys</code>	<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>
<code>ssh-keygen -t rsa</code>	<code>chmod 644 ~/.ssh/id_rsa</code>
<code>scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys</code>	<code>ssh root@server</code>
<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>	
<code>ssh -i ~/.ssh/id_rsa user@server</code>	
<code>ssh root@server</code>	

Explanation:

QUESTION NO: 6

Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

- A. DLP
- B. HIDS
- C. EDR
- D. NIPS

ANSWER: C

QUESTION NO: 7

An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data. Which of the following is the attacker most likely using?

- A. Base64 encoding
- B. Steganography
- C. Data encryption
- D. Perfect forward secrecy

ANSWER: B

Explanation:

References: How to Hide Files Inside Files [Images, Folder] - Raymond.CC Blog; How to Hide Data in a Secret Text File Compartment - How-To Geek; How to Hide Data Within an Image - Medium

QUESTION NO: 8

A security administrator needs to provide secure access to internal networks for external partners. The administrator has given the PSK and other parameters to the third-party security administrator. Which of the following is being used to establish this connection?

- A. Kerberos
- B. SSL/TLS
- C. IPSec
- D. SSH

ANSWER: C**Explanation:**

IPSec is a protocol suite that provides secure communication over IP networks. It uses encryption, authentication, and integrity mechanisms to protect data from unauthorized access or modification. IPSec can operate in two modes: transport mode and tunnel mode. In tunnel mode, IPSec can create a virtual private network (VPN) between two endpoints, such as external partners and internal networks. To establish a VPN connection, IPSec requires a pre-shared key (PSK) or other parameters to negotiate the security association. References: <https://www.comptia.org/content/guides/what-is-vpn>

QUESTION NO: 9

Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log in to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Choose two.)

- A. COPE
- B. VDI
- C. GPS
- D. TOTP
- E. RFID
- F. BYOD

ANSWER: B E**QUESTION NO: 10**

A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

- A. CASB
- B. SWG
- C. Containerization
- D. Automated failover

ANSWER: C

QUESTION NO: 11

An engineer wants to inspect traffic to a cluster of web servers in a cloud environment Which of the following solutions should the engineer implement? (Select two).

- A. CASB
- B. WAF
- C. Load balancer
- D. VPN
- E. TLS
- F. DAST

ANSWER: B C

Explanation:

A web application firewall (WAF) is a solution that inspects traffic to a cluster of web servers in a cloud environment and protects them from common web-based attacks, such as SQL injection, cross-site scripting, and denial-of-service¹. A WAF can be deployed as a cloud service or as a virtual appliance in front of the web servers. A load balancer is a solution that distributes traffic among multiple web servers in a cloud environment and improves their performance, availability, and scalability². A load balancer can also perform health checks on the web servers and route traffic only to the healthy ones. The other options are not relevant to this scenario. A CASB is a cloud access security broker, which is a solution that monitors and controls the use of cloud services by an organization's users³. A VPN is a virtual private network, which is a solution that creates a secure and encrypted connection between two networks or devices over the internet. TLS is Transport Layer Security, which is a protocol that provides encryption and authentication for data transmitted over a network. DAST is dynamic application security testing, which is a method of testing web applications for vulnerabilities by simulating attacks on them.

References: ¹: <https://www.imperva.com/learn/application-security/what-is-a-web-application-firewall-waf/> ²: <https://www.imperva.com/learn/application-security/load-balancing/> ³: <https://www.imperva.com/learn/application-security/cloud-access-security-broker-casb/> : <https://www.imperva.com/learn/application-security/vpn-virtual-private-network/> : <https://www.imperva.com/learn/application-security/transport-layer-security-tls/> : <https://www.imperva.com/learn/application-security/dynamic-application-security-testing-dast/> : <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-traffic-inspection> : <https://docs.microsoft.com/en-us/azure/private-link/inspect->

traffic-with-azure-firewall : <https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/application-gateway-before-azure-firewall>

QUESTION NO: 12

A Chief Security Officer (CSO) has asked a technician to devise a solution that can detect unauthorized execution privileges from the OS in both executable and data files and can work in conjunction with proxies or UTM. Which of the following would BEST meet the CSO's requirements?

- A. Fuzzing
- B. Sandboxing
- C. Static code analysis
- D. Code review

ANSWER: A**Explanation:**

Reference: <https://www.techtarget.com/searchsecurity/definition/fuzz-testing>

QUESTION NO: 13

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: 14**

A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

- A. Establish chain of custody
- B. Inspect the file metadata
- C. Reference the data retention policy
- D. Review the email event log

ANSWER: B

QUESTION NO: 15

A security analyst reviews web server logs and finds the following string
galleries?file—. /.././.././ . / . /etc/passwd

Which of the following attacks was performed against the web server?

- A. Directory traversal
- B. CSRF
- C. Pass the hash
- D. SQL injection

ANSWER: A

Explanation:

Directory traversal is an attack that exploits a vulnerability in a web application or a file system to access files or directories that are outside the intended scope. The attacker can use special characters, such as `../` or `..\`, to navigate through the directory structure and access restricted files or directories.

QUESTION NO: 16 - (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.

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



WiFi Controller

SSID: CORPGUEST

Shared key:

AAA server IP:

PSK:

Authentication type:

Controller IP: 192.168.1.10

Reset Answer Save Close

ANSWER: Seetheexplanationbelowforthesolution.

Explanation:

Wifi Controller

SSID: CORPGUEST

SHARED KEY: Secret

AAA server IP: 192.168.1.20

PSK: Blank

Authentication type: WPA2-EAP-PEAP-MSCHAPv2

Controller IP: 192.168.1.10

Radius Server

Shared Key: Secret

Client IP: 192.168.1.10

Authentication Type: Active Directory

Server IP: 192.168.1.20

Wireless Client

SSID: CORPGUEST

Username: guest01

Userpassword: guestpass

PSK: Blank

Authentication type: WPA2-Enterprise

QUESTION NO: 17

The security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted files. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?

- A. HIDS
- B. Allow list
- C. TPM
- D. NGFW

ANSWER: D**Explanation:**

Next-Generation Firewalls (NGFWs) are designed to provide advanced threat protection by combining traditional firewall capabilities with intrusion prevention, application control, and other security features. NGFWs can detect and block unauthorized access attempts, malware infections, and other suspicious activity. They can also be used to monitor file access and detect unauthorized copying or distribution of copyrighted material.

QUESTION NO: 18

A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

- A. Verification
- B. Validation
- C. Normalization
- D. Staging

ANSWER: A

QUESTION NO: 19

A company is designing the layout of a new datacenter so it will have an optimal environmental temperature. Which of the following must be included? (Choose two.)

- A. An air gap
- B. A cold aisle
- C. Removable doors
- D. A hot aisle
- E. An IoT thermostat
- F. A humidity monitor

ANSWER: B E**QUESTION NO: 20**

The new Chief Information Security Officer at a company has asked the security team to implement stronger user account policies. The new policies require:

- Users to choose a password unique to their last ten passwords
- Users to not log in from certain high-risk countries

Which of the following should the security team implement? (Select two).

- A. Password complexity
- B. Password history
- C. Geolocation
- D. Geospatial
- E. Geotagging
- F. Password reuse

ANSWER: B C