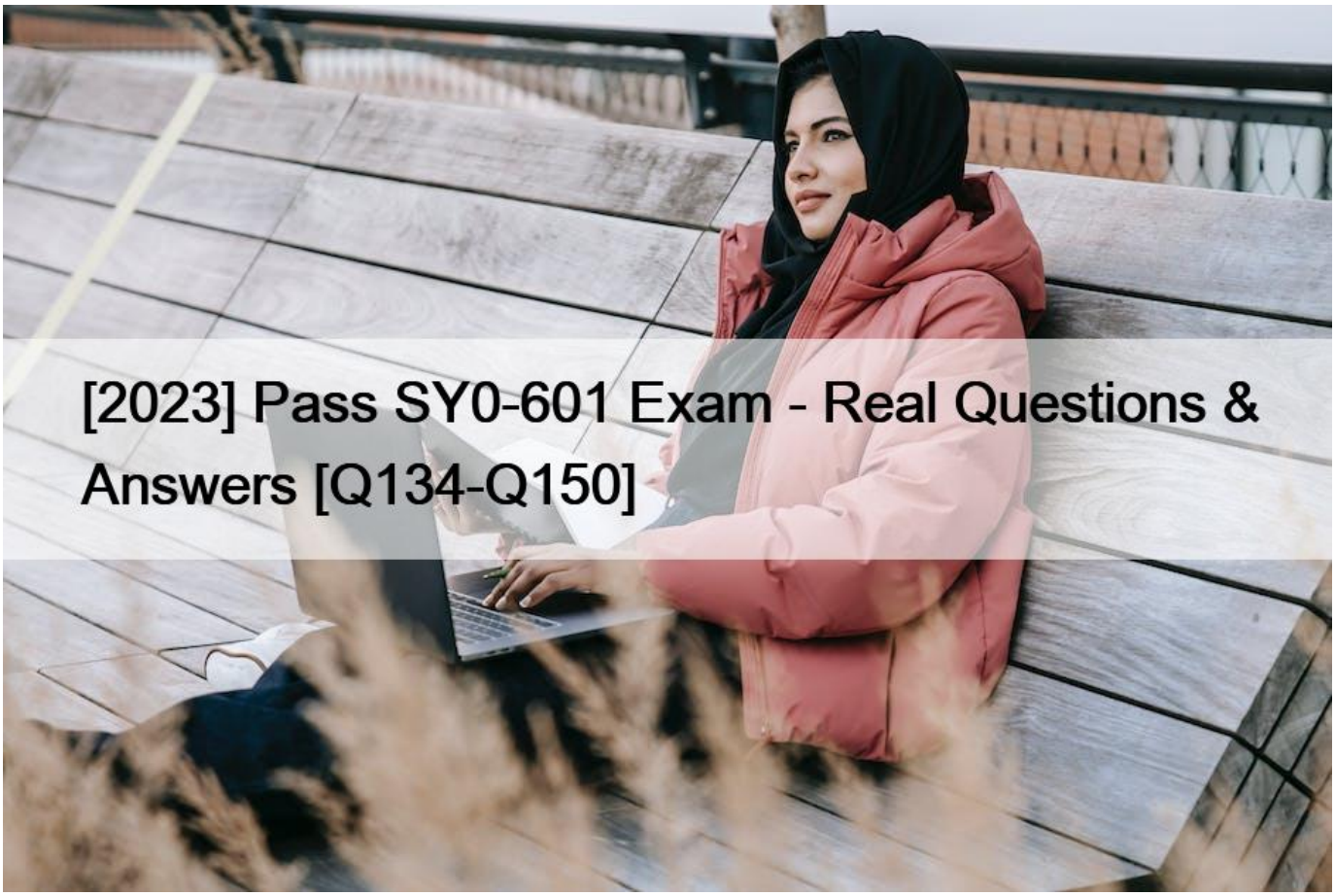
[2023 Pass SY0-601 Exam - Real Questions & Answers [Q134-Q150



[2023] Pass SY0-601 Exam - Real Questions and Answers
SY0-601 Exam Questions Get Updated [2023] with Correct Answers

NO.134 A security administrator installed a new web server. The administrator did this to increase the capacity for an application due to resource exhaustion on another server. Which of the following algorithms should the administrator use to split the number of the connections on each server in half?
* Least connection
* Weighted least connection
* Round-robin
* Weighted response

Round-robin is a type of load balancing algorithm that distributes traffic to a list of servers in rotation. It is a static algorithm that does not take into account the state of the system for the distribution of tasks. It assumes that all servers have equal capacity and can handle an equal amount of traffic.

NO.135 An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:

Which of the following BEST describes the type of password attack the attacker is performing?
* Dictionary
* Pass-the-hash
* Brute-force
* Password spraying

NO.136 A company recently expenenced an attack dunng which #5 main website was directed to the atacker’s web server, allowing the attacker to harvest credentials from unsuspecting customers. Vhich of the following snould the company Implement to prevent this type of attack from accurting in the future?
* IPSec
* SSL/TLS
* DNSSEC
* S/MIME

NO.137 A security team is providing input on the design of a secondary data center that has the following requirements:+ Anatural disaster at the primary site should not affect the secondary site. The secondary site should have the capability for failover during traffic surge situations.+ The secondary site must meet the same physical security requirements as the primary site. The secondary site must provide protection against power surges and outages.

Which of the following should the security team recommend? (Select two).
* Coniguring replication of the web servers at the primary site to offline storage
* Constructing the secondary site in a geographically disperse location
* Deploying load balancers at the primary site
* Installing generators
* Using differential backups at the secondary site
* Implementing hot and cold aisles at the secondary site

b) Constructing the secondary site in a geographically disperse location would ensure that a natural disaster at the primary site would not affect the secondary site. It would also allow for failover during traffic surge situations by distributing the load across different regions. D. Installing generators would provide protection against power surges and outages by providing backup power sources in case of a failure. Generators are part of the physical security requirements for data centers as they ensure availability and resilience. Reference: 1 CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1: Explain the importance of secure staging deployment concepts 2 CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 3 CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls

NO.138 A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the

researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?
* MAC cloning
* Evil twin
* Man-in-the-middle
* ARP poisoning

NO.139 A security analyst sees the following log output while reviewing web logs:

```
[02/Feb2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswr
[02/Feb2019:03:39:85 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=/../../../etc/password HTTP/1.
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?
* Secure cookies
* Input validation
* Code signing
* Stored procedures

NO.140 Which of the following should a technician use to protect a cellular phone that is needed for an investigation, to ensure the data will not be removed remotely?
* Air gap
* Secure cabinet
* Faraday cage
* Safe

NO.141 A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users’ PCs. Which of the following is the MOST likely cause of this issue?
* TFTP was disabled on the local hosts
* SSH was turned off instead of modifying the configuration file
* Remote login was disabled in the networkd.conf instead of using the sshd.conf.
* Network services are no longer running on the NAS.

Disabling remote logins to the NAS likely involved turning off SSH instead of modifying the configuration file. This would prevent users from using SCP to transfer files to the NAS, even though the data is still viewable from the users’ PCs. Source: TechTarget

NO.142 To reduce and limit software and infrastructure costs, the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive dat a. Which of the following cloud services would BEST accommodate the request?
* laas
* Paas
* Daas
* SaaS

NO.143 A security analyst received the following requirements for the deployment of a security camera solution:

* The cameras must be viewable by the on-site security guards.

+ The cameras must be able to communicate with the video storage server.

* The cameras must have the time synchronized automatically.

* The cameras must not be reachable directly via the internet.

* The servers for the cameras and video storage must be available for remote maintenance via the company VPN.

Which of the following should the security analyst recommend to securely meet the remote connectivity requirements?
* Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on
* Deploying a jump server that is accessible via the internal network that can communicate with the servers
* Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering
* Implementing a WAF to allow traffic from the local NTP server to the camera server

A jump server is a system that is used to manage and access systems in a separate security zone. It acts as a bridge between two different security zones and provides a controlled and secure way of accessing systems between them12. A jump server can also be used for auditing traffic and user activity for real-time surveillance3. By deploying a jump server that is accessible via the internal network, the security analyst can securely meet the remote connectivity requirements for the servers and cameras without exposing them directly to the internet or allowing outgoing traffic from their subnet. The other options are not suitable because:

1. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on would not allow remote maintenance via the company VPN.

2. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering would not prevent direct internet access to the cameras or servers.

3. Implementing a WAF to allow traffic from the local NTP server to the camera server would not address the remote connectivity requirements or protect the servers from internet access.

Reference:

1: https://www.thesecuritybuddy.com/network-security/what-is-a-jump-server/ 3: https://www.ssh.com/academy/iam/jump-server 2: https://en.wikipedia.org/wiki/Jump_server

NO.144 During a recent security incident at a multinational corporation a security analyst found the following logs for an account called user:

Account	Login location	Time (UTC)	Message
user	New York	9:00 a.m.	Login: user, successful
user	Los Angeles	9:01 a.m.	Login: user, successful
user	Sao Paolo	9:05 a.m.	Login: user, successful
user	Munich	9:12 a.m.	Login: user, successful

Which Of the following account policies would BEST prevent attackers from logging in as user?
* Impossible travel time
* Geofencing
* Time-based logins
* Geolocation

NO.145 A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes

what the manager is doing?
* Developing an incident response plan
* Building a disaster recovery plan
* Conducting a tabletop exercise
* Running a simulation exercise

https://www.redlegg.com/solutions/advisory-services/tabletop-exercise-pretty-much-everything-you-need-to-know

NO.146 An incident has occurred in the production environment.Analyze the command outputs and identify the type of compromise.
Explanation

Command Output1 = Logic Bomb

A logic bomb is a type of malicious code that executes when certain conditions are met, such as a specific date or time, or a specific user action1. In this case, the logic bomb is a script that runs every minute and checks if there is a user named john in the /etc/password file. If there is, it drops the production database using a MySQL command3. This could cause severe damage to the system and the data.

To prevent logic bombs, you should use antivirus software that can detect and remove malicious code, and also perform regular backups of your data. You should also avoid opening suspicious attachments or links from unknown sources, and use strong passwords for your accounts1.

Command Output2 = backdoorA backdoor is a type of malicious code that allows an attacker to access a system or network remotely, bypassing security measures1. In this case, the backdoor is a script that runs every time the date command is executed and prompts the user to enter their full name. Then, it opens a reverse shell connection using the nc command and downloads a virus file from a malicious website using the wget command2. This could allow the attacker to execute commands on the system and infect it with malware.

To prevent backdoors, you should use antivirus software that can detect and remove malicious code, and also update your system and applications regularly. You should also avoid executing unknown commands or scripts from untrusted sources, and use firewall rules to block unauthorized connections

NO.147 An analyst is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services. Given this output from Nmap.

```
PORT     STATE
21/tcp   filtered
22/tcp   open
23/tcp   open
443/tcp  open
```

Which of the following should the analyst recommend to disable?
* 21/tcp
* 22/tcp
* 23/tcp
* 443/tcp

NO.148 Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions.

Which of the following solutions is the company Implementing?
* Privileged access management
* SSO
* RADIUS
* Attribute-based access control

NO.149 A Chief information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares Which of the following should the company implement?
* DLP
* CASB
* HIDS
* EDR
* UEFI

Explanation

Detailed Explanation: Data Loss Prevention (DLP) can help prevent employees from stealing data by monitoring and controlling access to sensitive data. DLP can also detect and block attempts to transfer sensitive data outside of the organization, such as via email, file transfer, or cloud storage.

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 10: Managing Identity and Access, p.465

NO.150 Which of the following employee roles is responsible for protecting an organization’s collected personal information?
* CTO
* DPO
* CEO
* DBA

Explanation

Many companies also have a data protection officer or DPO. This is a higher-level manager who is responsible for the organization

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/#:~:text=M

The CompTIA SY0-601 exam itself consists of 90 multiple-choice and performance-based questions. SY0-601 exam duration is 90 minutes, and the passing score is 750 out of 900. SY0-601 exam can be taken at any Pearson VUE test center or online. The cost of the exam is $370, and it is valid for three years. After three years, the certification can be renewed by earning continuing education credits or by retaking the exam.

Practice SY0-601 Questions With Certification guide Q&A from Training Expert ValidExam:
https://www.validexam.com/SY0-601-latest-dumps.html]