[Mar-2024 The Best CompTIA Security+ Study Guide for the SY0-601 Exam [Q114-Q137

[Mar-2024] The Best CompTIA Security+ Study Guide for the SY0-601 Exam
SY0-601 certification guide Q&A from Training Expert TopExamCollection QUESTION 114

Which of the following test describes the risk that is present once mitigations are applied?
* Control risk
* Residual risk
* Inherent risk
* Risk awareness

Explanation

Residual risk is the risk that remains after applying risk mitigation measures, such as controls, policies, or procedures. It reflects the level of uncertainty and potential impact that cannot be completely eliminated by risk management efforts. Residual risk is calculated by subtracting the risk reduction from the inherent risk, or by multiplying the inherent risk by the risk control effectiveness. Residual risk should be compared to the acceptable level of risk to determine if further action is needed or if the risk can be accepted by the management. References: CompTIA Security+ SY0-601 Certification Study Guide, Chapter 10: Summarizing Risk Management Concepts, page 456; Residual risk – Wikipedia; Residual risk definition and why it’s important – Advisera

QUESTION 115

A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```


Which of the following can the security analyst conclude?
* A replay attack is being conducted against the application.
* An injection attack is being conducted against a user authentication system.
* A service account password may have been changed, resulting in continuous failed logins within the application.
* A credentialed vulnerability scanner attack is testing several CVEs against the application.

QUESTION 116

Which of the following is a reason why an organization would define an AUP?
* To define the lowest level of privileges needed for access and use of the organization’s resources
* To define the set of rules and behaviors for users of the organization’s IT systems
* To define the intended partnership between two organizations
* To define the availability and reliability characteristics between an IT provider and consumer

QUESTION 117

An employee’s company account was used in a data breach Interviews with the employee revealed:

* The employee was able to avoid changing passwords by using a previous password again.

* The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.

Which of the following can be implemented to prevent these issues from reoccuring? (Select TWO)
* Geographic dispersal
* Password complexity
* Password history
* Geotagging
* Password lockout
* Geofencing

Explanation

two possible solutions that can be implemented to prevent these issues from reoccurring are password history and geofencing12. Password history is a feature that prevents users from reusing their previous passwords1. This can enhance password security by forcing users to create new and unique passwords periodically1. Password history can be configured by setting a policy that specifies how many previous passwords are remembered and how often users must change their passwords Geofencing is a feature that

restricts access to a system or network based on the geographic location of the user or device2. This can enhance security by preventing unauthorized access from hostile or foreign regions2

. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries2.

QUESTION 118

A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?
* Predictability
* Key stretching
* Salting
* Hashing
https://www.techtarget.com/searchsecurity/definition/salt

QUESTION 119

Which of the following serves to warn users against downloading and installing pirated software on company devices?
* AUP
* NDA
* ISA
* BPA

QUESTION 120

A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?
* RA1D 0
* RAID1
* RAID 5
* RAID 10
https://techgenix.com/raid-10-vs-raid-5/

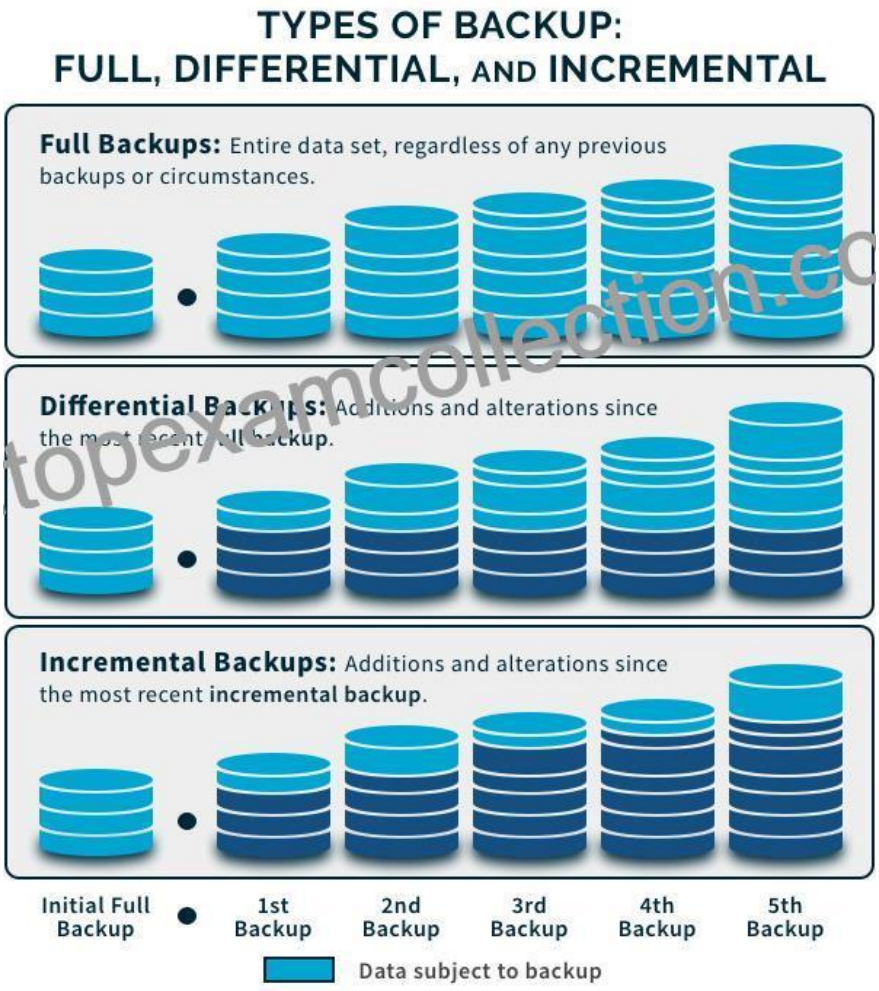
QUESTION 121

A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?
* Snapshot
* Differential
* Full
* Tape
Explanation

There are mainly three types of backup: full, differential, and incremental.

Let’s dive in to know more about the types of backup, the difference between them and which one would be the best fit for your business.

A basic graphic displaying the difference between full backup, differential backup, and incremental backup.



Full Backup

A full backup is the most complete type of backup where you clone all the selected data. This includes files, folders, SaaS applications, hard drives and more. The highlight of a full backup is the minimal time it requires to restore data. However, since as everything is backed up in one go, it takes longer to backup compared to other types of backup.

The other common issue with running full backups is that it overloads storage space. That’s why most businesses tend to run a full backup and occasionally follow it up with differential or incremental backup. This reduces the burden on the storage space, increasing backup speed.

Differential Backup

A differential backup straddles the line between a full and an incremental backup. This type of backup involves backing up data that was created or changed since the last full backup. To put it simply, a full backup is done initially, and then subsequent backups are run to include all the changes made to the files and folders.

It lets you restore data faster than full backup since it requires only two backup components: an initial full backup and the latest differential backup.

Let’s see how a differential backup works:

Day 1 – Schedule a full backup

Day 2 – Schedule a differential backup. It will cover all the changes that took place between Day 1 and Day 2 Day 3 – Schedule a differential backup. It will make a copy of all the data that has changed from Day

2 (this includes the full backup on Day 1 + differential backup) and Day 3.

Incremental Backup

The first backup in an incremental backup is a full backup. The succeeding backups will only store changes that were made to the previous backup. Businesses have more flexibility in spinning these types of backups as often as they want, with only the most recent changes stored.

Incremental backup requires space to store only the changes (increments), which allows for lightning-fast backups.

Difference Between Full, Differential and Incremental Backups

Full

Differential

Incremental

Storage Space

High

Medium to High

Low

Backup Speed

Slowest

Fast

Fastest

Restoration Speed

Fastest

Fast

Slowest

Media Required for Recovery

Most recent backup only

Most recent full backup & most recent differential backup

Most recent full backup & all incremental backups since full backup

Duplication

Stores a lot of duplicate files

Stores duplicate files

No duplicate files

QUESTION 122

A security analyst is tasked with classifying data to be stored on company servers. Which of the following should be classified as proprietary?
* Customers’ dates of birth
* Customers’ email addresses
* Marketing strategies
* Employee salaries

QUESTION 123

Entering a secure area requires passing through two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?
* Cameras

B: Faraday cage
* Access control vestibule
* Sensors
* Guards

QUESTION 124

A security architect is designing the new outbound internet for a small company. The company would like all 50 users to share the same single Internet connection. In addition, users will not be permitted to use social media sites or external email services while at work. Which of the following should be included in this design to satisfy these requirements? (Select TWO).
* DLP
* MAC filtering
* NAT
* VPN
* Content filler
* WAF

NAT (Network Address Translation) is a technology that allows multiple devices to share a single IP address, allowing them to access the internet while still maintaining security and privacy. VPN (Virtual Private Network) is a technology that creates a secure, encrypted tunnel between two or more devices, allowing users to access the internet and other network resources securely and

privately. Additionally, VPNs can also be used to restrict access to certain websites and services, such as social media sites and external email services.

QUESTION 125

During an incident response process involving a laptop, a host was identified as the entry point for malware.

The management team would like to have the laptop restored and given back to the user. The cybersecurity analyst would like to continue investigating the intrusion on the host. Which of the following would allow the analyst to continue the investigation and also return the laptop to the user as soon as possible?
* dd
* memdump
* tcpdump
* head

QUESTION 126

Which of the following must be in place before implementing a BCP?
* SLA
* AUP
* NDA
* BIA
To create an effective business continuity plan, a firm should take these five steps:

Step 1: Risk Assessment

This phase includes:

Evaluation of the company’s risks and exposures

Assessment of the potential impact of various business disruption scenarios

Determination of the most likely threat scenarios

Assessment of telecommunication recovery options and communication plans

Prioritization of findings and development of a roadmap

Step 2: Business Impact Analysis (BIA)

During this phase we collect information on:

Recovery assumptions, including Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO)

Critical business processes and workflows as well as the supporting production applications

Interdependencies, both internal and external

Critical staff including backups, skill sets, primary and secondary contacts

Future endeavors that may impact recovery

Special circumstances

Pro tip: Compiling your BIA into a master list can be helpful from a wholistic standpoint, as well as helpful in identifying pain points throughout the organization.

Step 3: Business Continuity Plan Development

This phase includes:

Obtaining executive sign-off of Business Impact Analysis

Synthesizing the Risk Assessment and BIA findings to create an actionable and thorough plan

Developing department, division and site level plans

Reviewing plan with key stakeholders to finalize and distribute

Step 4: Strategy and Plan Development

Validate that the recovery times that you have stated in your plan are obtainable and meet the objectives that are stated in the BIA. They should easily be available and readily accessible to staff, especially if and when a disaster were to happen. In the development phase, it’s important to incorporate many perspectives from various staff and all departments to help map the overall company feel and organizational focus. Once the plan is developed, we recommend that you have an executive or management team review and sign off on the overall plan.

Step 5: Plan Testing & Maintenance

The final critical element of a business continuity plan is to ensure that it is tested and maintained on a regular basis. This includes:

Conducting periodic table top and simulation exercises to ensure key stakeholders are comfortable with the plan steps

Executing bi-annual plan reviews

Performing annual Business Impact Assessments

QUESTION 127

A user downloaded an extension for a browser, and the user’s device later became infected. The analyst who is investigating the incident saw various logs where the attacker was hiding activity by deleting data. The following was observed running:

```
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C| Format-Volume -DriveLetter C - FileSystemLabel "New
NTFS - Full -Force -Confirm:$false |
```

Which of the following is the malware using to execute the attack?

* PowerShell
* Python
* Bash
* Macros

QUESTION 128

Which of the following would satisfy three-factor authentication requirements?
* Password, PIN, and physical token
* PIN, fingerprint scan, and ins scan
* Password, fingerprint scan, and physical token
* PIN, physical token, and ID card
Explanation

Three-factor authentication combines three types of authentication methods: something you know (password), something you have (physical token), and something you are (fingerprint scan). Option C satisfies these requirements, as it uses a password (something you know), a physical token (something you have), and a fingerprint scan (something you are) for authentication.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom Note: There could be other options as well that could satisfy the three-factor authentication requirements as per the organization’s security policies.

QUESTION 129

A security administrator has discovered that workstations on the LAN are becoming infected with malware.

The cause of the infections appears to be users receiving phishing emails that are bypassing the current email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?
* Forward proxy
* HIDS
* Awareness training
* A jump server
* IPS
Explanation

Awareness training should be implemented to educate users on the risks of clicking on malicious URLs.

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 9

QUESTION 130

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?
* DLP
* CASB
* HIDS
* EDR
* UEFI
Explanation

The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data when accessing network shares. References:

* CompTIA Security+ Study Guide Exam SY0-601, Chapter 8

QUESTION 131

An organization recently discovered that a purchasing officer approved an invoice for an amount that was different than the original purchase order. After further investigation a security analyst determines that the digital signature for the fraudulent invoice is exactly the same as the digital signature for the correct invoice that had been approved Which of the following attacks MOST likely explains the behavior?
* Birthday
* Rainbow table
* Impersonation
* Whaling

QUESTION 132

A recent security audit revealed that a popular website with IP address 172.16.1.5 also has an FTP service that employees were using to store sensitive corporate dat

a. The organization’s outbound firewall processes rules top-down. Which of the following would permit HTTP and HTTPS, while denying all other services for this host?
* access-rule permit tcp destination 172.16.1.5 port 80

access-rule permit tcp destination 172.16-1-5 port 443

access-rule deny ip destination 172.16.1.5
* access-rule permit tcp destination 172.16.1.5 port 22

access-rule permit tcp destination 172.16.1.5 port 443

access-rule deny tcp destination 172.16.1.5 port 80
* access-rule permit tcp destination 172.16.1.5 port 21

access-rule permit tcp destination 172.16.1.5 port 80

access-rule deny ip destination 172.16.1.5
* access-rule permit tcp destination 172.16.1.5 port 80

access-rule permit tcp destination 172.16.1.5 port 443

access-rule deny tcp destination 172.16.1.5 port 21

QUESTION 133

Which of the following would BEST provide detective and corrective controls for thermal regulation?
* A smoke detector
* A fire alarm
* An HVAC system
* A fire suppression system
* Guards

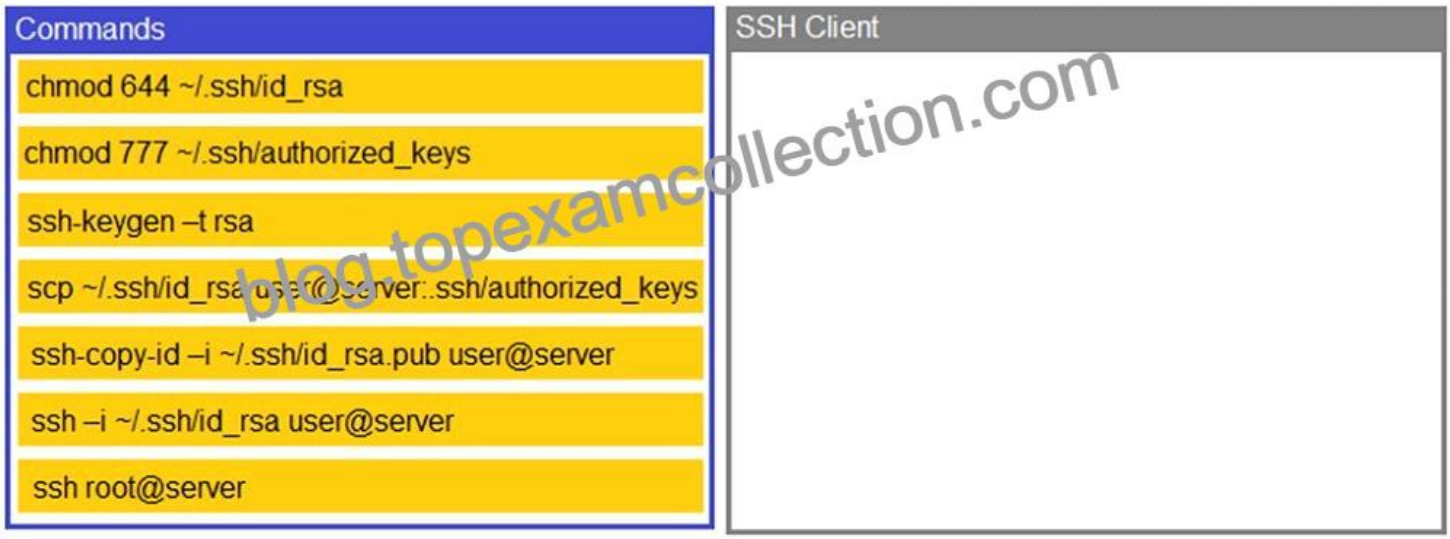
QUESTION 134

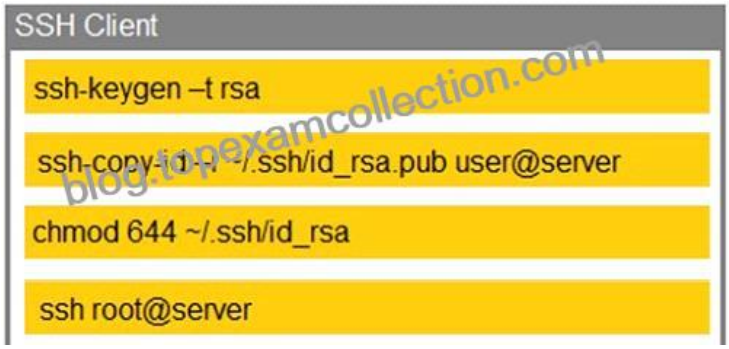
A security engineer is setting up passwordless authentication for the first time.

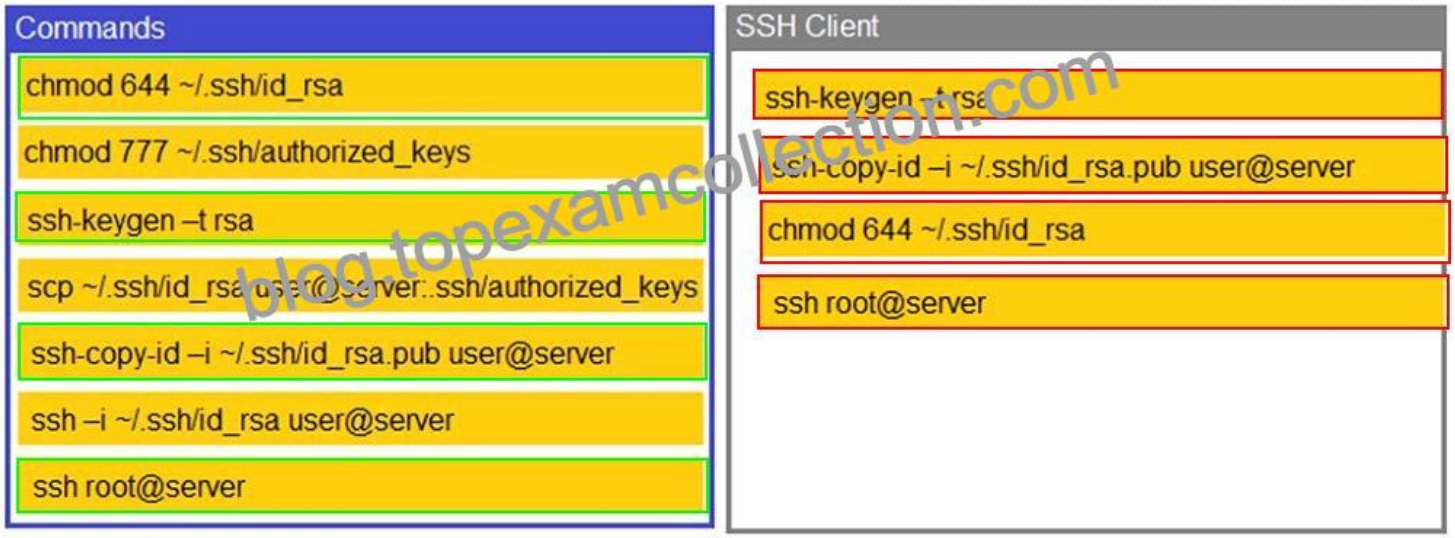
INSTRUCTIONS

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.







QUESTION 135

A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.

Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)
* DoS
* SSL stripping
* Memory leak
* Race condition
* Shimming
* Refactoring

“According to its self-reported version, the Cisco IOS software running on the remote device is affected by a denial of service vulnerability in the Session Initiation Protocol (SIP) gateway implementation due to improper handling of malformed SIP messages. An unauthenticated, remote attacker can exploit this, via crafted SIP messages, to cause memory leakage, resulting in an eventual reload of the affected device.”

QUESTION 136

During an asset inventory, several assets, supplies, and miscellaneous items were noted as missing. The security manager has been asked to find an automated solution to detect any future theft of equipment. Which of the following would be BEST to implement?
* Badges
* Fencing
* Access control vestibule
* Lighting
* Cameras

QUESTION 137

Which of the following models offers third-party-hosted, on-demand computing resources that can be shared with multiple organizations over the internet?
* Public cloud
* Hybrid cloud
* Community cloud
* Private cloud

There are three main models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)12. Each model represents a different part of the cloud computing stack and provides different levels of control, flexibility, and management.

According to one source1, a public cloud is a type of cloud deployment where the cloud resources (such as servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet. A public cloud can be shared with multiple organizations or users who pay for the service on a subscription or pay-as-you-go basis.

The Best CompTIA SY0-601 Study Guides and Dumps of 2024:
https://www.topexamcollection.com/SY0-601-vce-collection.html]