Exam Report: 9.12.10 Practice Questions

Date: 1/28/2020 7:30:23 pm
Time Spent: 2:22

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 47%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

What is the primary security feature that can be designed into a network's infrastructure to protect and support availability?

○ Switches instead of hubs

○ Fiber optic cables

○ Periodic backups

➡ ● Redundancy

Explanation

Redundancy is the primary security feature that can be designed into a network's infrastructure to protect and support availability, since it identifies single points of failure.

Periodic backups are better than no backups, but real-time and off-site backups are better protections for availability. Fiber optic cables are not a real protection for a network's availability, as they only provide the security benefit of eavesdropping protection. Switches are better than hubs, but there are infrastructure security measures that provide more significant protections for availability.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_01]

Question 2: Incorrect

Which form of alternate site is the cheapest, but may not allow an organization to recover before reaching their maximum tolerable downtime?

● ~~Warm site~~

○ Service bureau

➡ ○ Reciprocal agreement

○ Hot site

Explanation

A reciprocal agreement is a contract between two organizations that states in the event of a disaster they will aid each other by sharing their IT processing capabilities. Reciprocal agreements have no initial cost related to them. However, most organizations can barely support their own IT needs, much less the needs of an entire second organization.

A hot site, warm site, and service bureau contracts are all costly alternatives, but offer reasonable if not reliable assurance of recovery in the event of a disaster.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_02]

▼ Question 3: Correct

You manage a website for your company. The website uses three servers configured in a cluster. Incoming requests are distributed automatically between the three servers. All servers use a shared storage device that holds the website contents. Each server has a single network connection and a single power supply.

Considering the availability of your website, which component represents a single point of failure?

○ Network adapter

➡ ● Website storage

○ Web server

○ Power supply

Explanation

In this scenario, the shared storage is a single point of failure. A single point of failure means that failure in one component will cause the entire website to be unavailable. If the storage unit fails, then the website content will be unavailable.

Failure in a single network card, power supply, or even in a single server will not make the website unavailable. Any of these failures will take one server offline. But because of the server cluster, other servers will still be available to process incoming requests.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_07]

▼ Question 4: Correct

You manage your company's website. The Web1 server hosts the website. This server has the following configuration:

- Dual core processor
- Dual power supplies
- RAID 5 volume
- One RAID controller
- Two 1000 Mbps network adapters

Which component is a single point of failure for the website?

○ Disk storage

➡ ● Disk controller

○ Power supply

○ Network adapter

Explanation

A single point of failure means that failure in one component will cause the entire website to be unavailable. In this scenario, the disk controller is a single point of failure. If the disk controller fails, content for the website will be unavailable.

To prevent a single point of failure, provide redundant components. Dual power supplies, multiple network connections, and fault tolerant volumes (RAID 1, RAID 5, or RAID 0 + 1) can all sustain a failure in one component and continue to function.

References

LabSim for Security Pro, Section 9.12.

[All Questions SecPro2017_v6.exm REDUNDANCY_08]

▼ **Question 5:** Incorrect

Which of the following disk configurations might sustain losing two disks? (Select two.)

➡ □ RAID 0+1

☑ ~~RAID 5~~

➡ ☑ RAID 1+0

□ RAID 1

Explanation

RAID 1+0 combines disk mirroring (1) and disk striping (0). Multiple disks are configured into two mirrored arrays, which are then striped across the other set. RAID 1+0 can sustain multiple drive losses as long as no mirror loses all its drives. RAID 0+1 can also continue to work if both failed disks are in the same set; if a set in each disk fails, data is unavailable.

RAID 5 and RAID 1 can only sustain a loss of a single disk.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_09]

▼ **Question 6:** Correct

You have been asked to implement a RAID 5 solution for your network. What is the minimum number of hard disks that can be used to configure RAID 5?

○ 2

➡ ● 3

○ 4

○ 5

○ 6

Explanation

A RAID 5 array stripes data and parity information across multiple hard disks. To complete a RAID 5 array, a minimum of three hard disks is required.

RAID 0 and RAID 1 can both be implemented with a minimum of two hard disks.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_10]

▼ **Question 7:** Incorrect

What option is an advantage RAID 5 has over RAID 1?

➡ ○ RAID 5 improves performance over RAID 1.

○ RAID 5 provides redundancy for the disk controller.

● ~~RAID 5 continues to operate with a failure in two disks; RAID 1 can only operate with a failure of one disk.~~

○ RAID 5 provides redundancy; RAID 1 does not.

Explanation

RAID 5 provides both fault tolerance and improved performance. RAID 1 (mirroring) provides only fault tolerance with no performance benefit.

Both RAID 5 and RAID 1 can only sustain a loss of one disk in the set. Use multiple disk controllers to provide redundancy for the disk controller.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_11]

Question 8: Incorrect

You have a computer with three hard disks.

- A RAID 0 volume uses space on Disk 1 and Disk 2.
- A RAID 1 volume uses space on Disk 2 and Disk 3.

Disk 2 fails. Which of the following is true?

● ~~Data on the RAID 0 volume is accessible; data on the RAID 1 volume is not.~~

➡ ○ Data on the RAID 1 volume is accessible; data on the RAID 0 volume is not.

○ Data on both volumes is not accessible.

○ Data on both volumes is still accessible.

Explanation

In this scenario, Disk 2 is shared between both volumes. If Disk 2 fails, the RAID 1 volume is still accessible because RAID 1 (mirrored) volumes can sustain the loss of a single disk. The data on the RAID 0 volume is not accessible. RAID 0 uses striping, which distributes the data evenly between multiple disks. If a single disk fails, the entire volume is lost.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_12]

Question 9: Correct

You have a web server on your network that hosts the public website for your company. You want to make sure that the website will continue to be available even if a NIC, hard drive, or other problem prevents the server from responding.

Which solution should you implement?

○ NIC teaming

➡ ● Load balancing

○ QoS

○ Traffic shaping

Explanation

Load balancing configures a group of servers in a logical group (called a *server farm*). Incoming requests to the group are distributed to individual members within the group. Load balancing provides fault tolerance if the load balancing mechanism is able to detect when a specific farm member is unavailable, automatically distributing new requests to the available members.

With NIC teaming, two or more physical connections to the same network are logically grouped (or bonded). If one NIC fails, the second NIC with a connection to the same network can still be used. NIC teaming provides redundancy for a network adapter, but not for other components, such as hard drives.

A *traffic shaper* (also called a *bandwidth shaper*) is a device that is capable of modifying the flow of data through a network in response to network traffic conditions. Quality of Service (QoS) refers to a set of mechanisms that tries to guarantee timely delivery or minimal delay of important or time-sensitive communications. QoS is particularly important when implementing Voice over IP (VoIP), Video over IP, or online gaming where delay or data loss make the overall experience unacceptable.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_15]

▼ Question 10: Incorrect

You manage a server that runs your company website. The web server has reached its capacity, and the number of client requests is greater than the server can handle.

You would like to find a solution so that a second server can respond to requests for website content.

Which solution should you implement?

○ Traffic shaper

○ QoS

➡ ○ Load balancing

● ~~Ethernet bonding~~

Explanation

Load balancing configures a group of servers in a logical group (called a *server farm*). Incoming requests to the group are distributed to individual members within the group. Incoming requests can be distributed evenly between group members or unevenly based on additional criteria, such as server capacity. The primary goal of load balancing is to improve performance by configuring multiple devices to respond as one.

A *traffic shaper* (also called a *bandwidth shaper*) is a device that is capable of modifying the flow of data through a network in response to network traffic conditions. Quality of Service (QoS) refers to a set of mechanisms that tries to guarantee timely delivery or minimal delay of important or time-sensitive communications. QoS is particularly important when implementing Voice over IP (VoIP), Video over IP, or online gaming--programs in which delay or data loss make the overall experience unacceptable.

With Ethernet *bonding* (also called NIC *teaming*), two or more physical connections to the same network are logically grouped (or bonded). Data is divided and sent on multiple interfaces, effectively increasing the speed at which the device can send and receive on the network.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_16]

▼ Question 11: Incorrect

To prevent server downtime, which of the following components should be installed redundantly in a server system?

○ Floppy disk drive

➡ ○ Power supply

● ~~RAM modules~~

○ CD or DVD drive

Explanation

To prevent server downtime, you should install redundant power supplies in a server system. If one fails, the other can immediately take over, allowing the server to remain running.

Because it isn't a critical component, a redundant CD or DVD drive probably isn't necessary. Unless data was shared from a disc in the drive, a failed CD or DVD drive probably won't affect the server's functionality. With most motherboards, there's no way to install redundant RAM modules. Like CD or

DVD drives, the floppy disk drive isn't a critical component. A failed floppy disk drive won't bring the server down.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_19]

Question 12: Incorrect

Match the recovery term on the right with the appropriate definition on the left.

MTTF

~~Identifies the average lifetime of a system or component.~~

Measures the average time to failure of a system or component.

MTD

~~Identifies the average amount of time necessary to repair a failed component or to restore operations.~~

Identifies the length of time an organization can survive with a specified service, asset, or process down.

MTTR

~~Identifies the length of time an organization can survive with a specified service, asset, or process down.~~

Identifies the average amount of time necessary to repair a failed component or to restore operations.

MTBF

~~Measures the average time to failure of a system or component.~~

Identifies the average lifetime of a system or component.

Explanation

Redundancy measurement parameters include the following:

- *Mean Time Between Failures* (MTBF) identifies the average lifetime of a system or component. Components should be replaced around the time that the MTBF is reached.
- *Mean Time To Failure* (MTTF) measures the average time to failure of a system or component. This metric assumes that the system or component is not repaired at any point in its lifetime, which would extend its useful life.
- *Mean Time To Repair* (MTTR) identifies the average amount of time to repair a failed component or restore operations. This is also referred to as Mean Time to Restore.
- *Maximum Tolerable Downtime* (MTD) combines the RPO, RTO, MTBF, and MTTR to identify the length of time an organization can survive with a specified service, asset, or process down.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_21]

Question 13: Correct

You have been asked to deploy a network solution that includes an alternate location where operational recovery is provided within minutes of a disaster. Which of the following strategies would you choose?

○ HSTG

➡ ● Hot site

○ Warm site

○ Hot spare

○ Cold site

Explanation

A hot site is a complete disaster recovery facility that could be fully operational within hours or minutes in the event of a disaster. This includes maintaining redundant hardware and up-to-date network data.

A warm site is a remote network location that maintains a backup of the data, but it is not always current. Data may be days or weeks old, depending on backup procedures. A cold site provides a space and sometimes hardware in an alternate location that can be configured when needed. Returning to an operational state may take days. A hot spare is a redundant hardware component used as a failover solution.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_05]

▼ **Question 14:** Correct

If your mission-critical services have a maximum tolerable downtime (MTD) (or a recovery time objective [RTO]) of 36 hours, what is the optimum form of recovery site?

○ Mobile

➡ ● Warm

○ Cold

○ Hot

Explanation

A warm site would be the most optimum. A warm site can often provide recovery within the stated time period, and it has the most reasonable cost for the situation.

With an MTD/RTO of 36 hours, a cold site is out of the question because recovery would take much longer than the allotted time. Obviously, a hot site would offer instant recovery, but at a significant financial, administrative, management, and security cost. Nothing about the scenario indicates that a mobile backup is needed or preferred.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_17]

▼ **Question 15:** Incorrect

Which of the following is a recovery site that may have electricity connected, but there are no servers installed and no high-speed data lines present?

○ Reciprocal agreement

➡ ○ Cold site

○ Hot site

● ~~Warm site~~

Explanation

A *cold site* is a recovery site that may have electricity connected, but there are no servers installed and no high-speed data lines present. A cold site does not offer an adequate route to recovery for most organizations.

A *hot site* is a real-time full mirror of the primary site. It is fully functional and ready for immediate use 24/7. A *warm site* is partially configured and may require days or weeks to bring up to production level. A *reciprocal agreement* is not a form of recovery site; instead, it is a non-enforceable agreement between two companies to assist each other in the event of a disaster.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_18]