Chp 12 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/19/2022 9:20:44 pm • Time spent: 06:27

Score: 100% Passing Score: 80%

Question 1: ✔ Correct

Your network performs a full backup every night. Each Sunday, the previous night's backup tape is archived.

On a Wednesday morning, the storage system fails. How many restore operations would you need to perform to recover all of the data?

- 1
- 2
- 3
- 4
- 5
- 6

EXPLANATION

You would need to perform a single restore procedure. You would simply restore the last full backup from Wednesday to restore all of the data.

The fact that you archive one backup each week is irrelevant to restoring the latest data. The archived copy is only used to restore something to a specific point in time. If you had used full and differential backups, you would restore the last full and last differential backups. If you had used full and incremental backups, you would restore the last full and each subsequent incremental backup.

REFERENCES

12.8.4 Backup Types and Storage Facts

q_bkp_stor_full_02_secp7.question.fex

Question 2: ✔ Correct

Which of the following is an important aspect of evidence-gathering?

- Monitor user access to compromised systems.
- ➡ Back up all log files and audit trails.
- Purge transaction logs.
- Restore damaged data from backup media.

EXPLANATION

When gathering evidence, it is important to make backup copies of all log files and audit trails. These files help reconstruct the events leading up to the security violation. They often include important clues to the intruder's identity.

Users should not have access to compromised systems while evidence-gathering is taking place. Along the same lines, damaged data should not be restored, nor transaction logs purged, while evidence-gathering is taking place.

REFERENCES

12.1.2 Incident Response Process Facts

q_incident_resp_log_02_secp7.question.fex

Question 3: ✔ Correct

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?

- Hot site
- ➡ Cold site
- Reciprocal agreement
- 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

12.7.2 Redundancy Facts

q_redundancy_cold_site_secp7.question.fex

Question 4: ✔ Correct

How can a criminal investigator ensure the integrity of a removable media device found while collecting evidence?

- Create a checksum using a hashing algorithm
- Enable write protection
- Reset the file attributes on the media to read-only
- Write a log file to the media

EXPLANATION

To protect or ensure the integrity of collected digital evidence, an investigator should create a checksum using a hashing algorithm. In the future, the same hashing algorithm can be used to create another checksum. Then the two values are compared. If the checksums are identical, the media was not altered.

Not all removable media has write-protection switches, and it is possible for software to circumvent these physical restrictions. Writing a new file to the media or altering the settings on files on the media is a direct violation of integrity.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_checksum_secp7.question.fex

Question 5: ✔ Correct

During a recent site survey, you found a rogue wireless access point on your network. Which of the following actions should you take first to protect your network while still preserving evidence?

- ➡ Disconnect the access point from the network.
- See who is connected to the access point and attempt to find the attacker.
- Connect to the access point and examine its logs for information.
- Run a packet sniffer to monitor traffic to and from the access point.

EXPLANATION

The first step in responding to an incident is to take actions to stop the attack and contain or limit the damage. For example, if an attack involves a computer system attached to the network, the first step might be to disconnect the system from the network. Although you want to preserve as much information as possible to assist in later investigations, it might be better to stop the attack, even if doing so alerts the attacker or results in the loss of evidence regarding the attack.

After containing a threat, a forensic investigation can be performed on computer systems to gather evidence and identify the methods used in the attack.

REFERENCES

12.1.2 Incident Response Process Facts

q_incident_resp_contain_secp7.question.fex

Question 6: ✔ 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?

- Hot spare
- ➡ Hot site
- Warm site
- 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

12.7.2 Redundancy Facts

q_redundancy_hot_site_secp7.question.fex

Question 7: ✔ Correct

Your company is about to begin litigation, and you need to gather information. You need to get emails, memos, invoices, and other electronic documents from employees. You'd also like to get printed, physical copies of documents. Which tool would you use to gather this information?

- Legal hold
- Chain of custody
- Timestamps
- Timeline of events

EXPLANATION

You would use a legal hold. The purpose behind a legal hold is to help ease the burden of the IT and legal teams when it comes to gathering evidentiary documentation. This notice instructs employees to retain any electronically stored information, or ESI.

The chain of custody proves that no tampering has occurred in gathering evidence.

Timestamps provide an exact date and time of an event and must be accurate to be admissible.

A timeline of events is required for digital forensic evidence to be admissible and to prove who is most responsible for what occurred.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_lglhold_secp7.question.fex

Question 8: ✔ Correct

You wish to configure collector-initiated event subscriptions. On the collector computer, in which program do you configure a subscription?

- Device Manager
- Local Group Policy
- Computer Management
- Event Viewer

EXPLANATION

Event Viewer is used to configure collector-initiated subscriptions.

Collector-initiated event subscriptions are not configured using Group Policy like source-initiated subscriptions.

Device Manager offers no settings to configure event subscriptions.

Computer Management offers no settings to configure event subscriptions.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_viewer_secp7.question.fex

Question 9: ✔ Correct

You would like to simulate an attack on your network so you can test defense equipment and discover vulnerabilities in order to mitigate risk. Which tool would you use to simulate all the packets of an attack?

- TCPDump
- Etherflood
- TCPReplay
- Wireshark

EXPLANATION

You would use TCPReplay. You could use TCPDump or Wireshark to capture the packets, but you would use TCPReplay to actually replay and simulate the attack.

Etherflood is a tool that can flood a switched network with random MAC addresses.

REFERENCES

12.6.7 Packet Capture Facts

q_capturepkt_tcprelay_secp7.question.fex

Question 10: ✔ Correct

You want to store your computer-generated audit logs in case they are needed in the future for examination or to be used as evidence in the event of a security incident. Which method can you use to ensure that the logs you put in storage have not been altered when you use them in the future?

- Create a hash of each log.
- Encrypt the logs.
- Make two copies of each log and store each copy in a different location.
- Store the logs in an offsite facility.

EXPLANATION

Use a hash to verify that the contents of a log have not been altered. When you analyze the logs, take another hash and compare the new hash to the original one. If the hashes match, the logs have not been altered.

Storing logs offsite makes them harder to access and alter, and this prevents a disaster at your main location from destroying the logs. Encrypting the logs protects the log confidentiality but does not prevent them from being altered, nor can it prove that the logs have not been altered. Creating two copies of the logs ensures that a single disaster does not destroy the logs. Comparing both logs to make sure they match does not guarantee that someone didn't alter both copies. In addition, if a disaster destroys one copy of the logs, you would not have a way to verify that the remaining copy has not been altered.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_hashing_01_secp7.question.fex

Question 11: ✔ Correct

You suspect a bad video driver is causing a user's system to randomly crash and reboot. Where would you go to identify and confirm your suspicions?

- SIP logs
- Dump files
- Syslog
- Application logs

EXPLANATION

You would choose dump files. Dump files are created when an application, OS, or other computer function stops abruptly. These files help IT admins perform root-cause analysis and can also give clues as to the crash's origin. This could be something as commonplace as a bad driver or hardware component. Or, unfortunately, it may prove to be the result of a malicious act.

Syslog is a protocol that defines how log messages are sent from one device to a logging server on an IP network. The sending device sends a small text message to the syslog receiver (the logging server).

App logs show application access, crashes, updates, and any other relevant information that could be valuable in determining root-cause analysis.

Session Information Protocol (SIP) logs contain key information about where a phone call was initiated and what the communication's intent was.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_dump_secp7.question.fex

Question 12: ✔ Correct

When you conduct a forensic investigation, which of the following initial actions is appropriate for preserving evidence?

- Turn off the system.
- Stop all running processes.
- Remove the hard drive.
- ➡ Document what is on the screen.

EXPLANATION

Preserving evidence while conducting a forensic investigation is a trade-off. Any attempt to collect evidence may actually destroy the very data necessary to identify an attack or attacker. Of the choices given, documenting what is on the screen is the least intrusive and the least likely to destroy critical evidence. Halting, disassembling, or stopping running processes may erase the data you need to track the intruder.

REFERENCES

12.1.2 Incident Response Process Facts

q_incident_resp_identify_02_secp7.question.fex

Question 13: ✔ Correct

The chain of custody is used for which purpose?

- Retaining evidence integrity
- Identifying the owner of the evidence
- Detailing the timeline between creation and discovery of evidence
- ➡ Listing people coming into contact with the evidence

EXPLANATION

The chain of custody is used to track the people who came in contact with the evidence. The chain of custody starts at the moment evidence is discovered and lists the identity of the person who discovered, logged, gathered, protected, transported, stored, and presented the evidence. The chain of custody helps to ensure the admissibility of evidence in court.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_chain_02_secp7.question.fex

Question 14: ✔ Correct

Which of the following components are the SIEM's way of letting the IT team know that a pre-established parameter is not within the acceptable range?

- Sensors
- Trends
- Dashboard
- Alerts

EXPLANATION

Alerts are the SIEM's way of letting the IT team know that a pre-established parameter is not within the acceptable range. An alert is intended to get the attention of the IT person, or persons, monitoring the network. A best practice in this area is 24-hour monitoring.

Sensors are set up at critical endpoints, services, and other vulnerable locations. These sensors are programmed to send customized alerts to the SIEM if certain parameters are not within the acceptable range.

The dashboard consists of customizable information screens that show real-time security and network information.

Trends are patterns of activity discovered and reported to the SIEM.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_alert_secp7.question.fex

Question 15: ✔ Correct

For some reason, your source computers are not communicating properly with the collector. Which tool would you use to verify communications?

- Run **winrm qc -q**
- Event Viewer System log
- Run **wecutil qc**
- Runtime Status

EXPLANATION

You would choose Runtime Status to verify communications after you have created a subscription.

The **wecutil qc** command would simply run the Windows Event Collector service.

The **winrm qc -q** command would initiate the Windows Remote Management service.

The Event Viewer System log would not verify current communications.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_runtime_secp7.question.fex

Question 16: ✔ Correct

What is the purpose of audit trails?

- To restore systems to normal operations.
- ➡ To detect security-violating events.
- To correct system problems.
- To prevent security breaches.

EXPLANATION

The purpose of audit trails is to detect security-violating events or actions.

Auditing itself is used to prevent security breaches, and audit trails are used for detective control. Neither auditing nor audit trails correct problems or restore systems to normal operations. That is done by the IT staff that inspects the contents of audit trails and creates a solution that is then implemented into the environment via the security policy.

REFERENCES

12.1.2 Incident Response Process Facts

q_incident_resp_incident_02_secp7.question.fex

Question 17: ✔ Correct

For some reason, when you capture packets as part of your monitoring, you aren't seeing much traffic. What could be the reason?

- Your machine is set to only capture HTTP packets.
- ➡ You forgot to turn on promiscuous mode for the network interface.
- Your NIC is set to broadcasting instead of receiving.
- You have multiple MAC addresses associated with one NIC.

EXPLANATION

The most likely reason is that you forgot to turn on promiscuous mode for your network interface. Turning on promiscuous mode gives the interface permission to grab every frame that comes its way, even if the frame is addressed to someone else.

REFERENCES

12.6.7 Packet Capture Facts

q_capturepkt_promis_secp7.question.fex

Question 18: ✔ Correct

You suspect cache poisoning or spoofing has occurred on your network. Users are complaining of strange web results and being redirected to undesirable sites. Which log would help you determine what is going on?

- Network logs
- Application logs
- Security logs
- DNS logs

EXPLANATION

You would take a look at the DNS logs for DNS cache poisoning. After this, you can begin monitoring DNS query traffic.

Network logs cannot help you with spoofed host name resolution.

Application logs do not help you determine DNS poisoning.

Security logs do little to help you identify spoofing.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_dnslogs_secp7.question.fex

Question 19: ✔ Correct

You would like to make sure users are not accessing inappropriate content online at work. Which endpoint security strategy would you employ?

- Firewall rules
- ➡ Content filtering
- Mobile device management (MDM)
- URL filters

EXPLANATION

You would choose content filtering. Online URL filtering is based on selected objectionable content.

MDM doesn't provide content filtering.

Firewall rules usually pertain to data, not necessarily inappropriate content.

URL filters are for whitelisting and blacklisting sites. They are not used for filtering content.

REFERENCES

12.2.2 Reconfigure and Protect Endpoints Facts

q_endpoint_prot_content_secp7.question.fex

Question 20: ✔ Correct

You need to find the text string New Haven in 100 documents in a folder structure on a Linux server. Which command would you use?

- **tail**
- **grep**
- **head**
- **chmod**

EXPLANATION

You would choose the **grep** command. This command searches through files for a specified character string. By default, **grep** is context-sensitive and displays the string in the context of the line containing the string.

The **chmod** command assigns or removes permissions to users, groups, or others.

The **head** command shows the first few lines of a file.

The **tail** command shows the last few lines of a file.

REFERENCES

12.6.2 Manipulating Files Facts

q_file_manipulate_grep_secp7.question.fex

Question 21: ✔ Correct

You need to limit the impact of a security breach for a particular file server with sensitive company data. Which strategy would you employ?

- Segmentation
- Isolation
- SOAR
- Containment

EXPLANATION

You would choose segmentation. You can segment using VLANs, software-defined networks, switches, subnetting, or even physical segmentation.

Isolation limits the ability of a compromised process or application to do more harm to the network or its assets.

Containment is the first step after an event has been detected and identified. Segmentation is preventative.

SOAR is a platform to compile security data generated by different security endpoints.

REFERENCES

12.2.4 Isolate and Containment Facts

q_isolate_contain_segmentation_secp7.question.fex

Question 22: ✔ Correct

You are concerned that an attacker can gain access to your web server, make modifications to the system, and alter the log files to hide his or her actions. Which of the following actions would best protect the log files?

- Encrypt the log files.
- Take a hash of the log files.
- Use syslog to send log entries to another server.
- Configure permissions on the log files to prevent access.

EXPLANATION

The best protection is to save log files to a remote server. In this way, compromise of a system does not provide access to the log files for that system.

Configuring permissions on the log files would allow access for only the specified user accounts. However, if an attacker has gained access to the system, he or she might also have access to the user accounts that have been given access to the log files. Encrypting the log files protects the contents from being read, but this does not prevent the files from being deleted. Hashing of log files ensures integrity and that the files have not been altered since they were created.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_syslog_02_secp7.question.fex

Question 23: ✔ Correct

This application endpoint-protection rule implicitly denies unless added to the rule. Which of the following processes describes this?

- Blacklisting
- Quarantining
- Content filtering
- ➡ Whitelisting

EXPLANATION

You would choose whitelisting. Whitelisting allows an IT admin to control the applications, IP addresses, URLs, and email addresses that are allowed onto the network. Whitelisting might mistakenly fail to list a needed application and interrupt workflow. Remember, whitelisting denies access until the item is added to the whitelist. This is called implicit deny. This is part of access control and is more strict than blacklisting.

Blacklisting lists the applications, IP addresses, URLs, email addresses, etc. that are to be blocked from the network.

Quarantining occurs when antivirus software finds a malicious item and quarantines it. This means that the item is placed in a folder where it cannot cause any damage to the network.

Content filtering is a strategy to keep employees from accessing unauthorized content on the web. Online URL filtering is based on selected objectionable content.

REFERENCES

12.2.2 Reconfigure and Protect Endpoints Facts

q_endpoint_prot_whitelisting_secp7.question.fex

Question 24: ✔ Correct

Which of the following are backed up during an incremental backup?

- Only files that have changed since the last full or differential backup.
- ➡ Only files that have changed since the last full or incremental backup.
- Only files that are new since the last full or incremental backup.
- Only files that have changed since the last full backup.

EXPLANATION

An incremental backup only captures files that have changed since the last full or incremental backup. The primary attraction to this backup plan is that it requires less storage space and processing time to complete. Restoration starts from the last full backup and then requires the loading of each subsequent incremental backup for a full restoration.

REFERENCES

12.8.4 Backup Types and Storage Facts

q_bkp_stor_increment_01_secp7.question.fex

Question 25: ✔ Correct

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

- Fiber optic cables
- ➡ Redundancy
- Switches instead of hubs
- Periodic backups

EXPLANATION

Redundancy is the primary security feature that can be designed into a network's infrastructure to protect and support availability. This is because 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

12.7.2 Redundancy Facts

q_redundancy_redundancy_secp7.question.fex

Question 26: ✔ Correct

You need to remotely wipe an android phone for one of your rogue users. Which endpoint tool would you use?

- Quarantining
- Mobile application management (MAM)
- Mobile device management (MDM)
- MAM-WE

EXPLANATION

You would choose mobile device management (MDM). MDM offers a way to easily monitor and manage mobile devices. This includes updates, data encryption, and remote wipes of a compromised device.

MAM lets a system administrator publish, push, configure, secure, monitor, and update mobile apps. It does not provide options to remotely wipe a device.

MAM-WE is the same as MAM, but it includes enrollment into a third-party enterprise mobility management (EMM) provider. Sensitive data can be managed on any device, including personal devices.

Quarantining has to do with antivirus software finding a malicious item and isolating it or a network endpoint.

REFERENCES

12.2.2 Reconfigure and Protect Endpoints Facts

q_endpoint_prot_mdm_secp7.question.fex

Question 27: ✔ Correct

You are in charge of making sure the IT systems of your company survive in case of any type of disaster in any of your locations. Your document should include organizational charts, phone lists, and order of restore. Each business unit should write their own policies and procedures with guidelines from corporate management. Which of the following documents should you create for this purpose?

- Incident-response team charter
- ➡ Business continuity plan
- Communication plan
- Disaster recovery plan

EXPLANATION

You would make a business continuity plan. More detailed and longer than a disaster recover plan, a business continuity plan has procedures and policies for each business unit. The policies and procedures are written by each business unit with guidelines from corporate management. This document includes organizational charts, phone lists, order of restore, and vendor contact information.

A disaster recovery plan is similar and is used for documenting a plan for policies and procedures that are executed in the event of a disruption of business. However, this type of plan is much less involved than the business continuity plan.

A communication plan is written to effectively communicate important company information in the case of an emergency.

An incident-response team charter simply describes the creation and function of a specialized team trained to identify malicious actions against a network.

REFERENCES

12.1.4 Incident Response Frameworks and Management Facts

13.2.6 Business Continuity Planning Facts

q_incident_resp_plan_01_secp7.question.fex

Question 28: ✔ Correct

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

- [x] RAID 0+1
- [ ] RAID 1
- [x] RAID 1+0
- [ ] RAID 0
- [ ] RAID 5

EXPLANATION

RAID 1+0 combines disk mirroring (1) and disk striping (0). Multiple disks are configured into two mirrored arrays that 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. But if a set in each disk fails, data is unavailable.

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

RAID 0 is disk striping, but RAID 0 by itself is not fault tolerant.

REFERENCES

12.7.5 RAID Facts

q_raid_raid.secp7.question.fex

Question 29: ✔ Correct

You have detected and identified a security event. What's the first step you should complete?

- Containment
- Playbook
- Segmentation
- Isolation

EXPLANATION

You would choose containment. Containment is the first step to complete after an event has been detected and identified.

Isolation limits the ability of a compromised process or application to do more harm to the network or its assets.

Segmentation is a strategic network design. The concept is simple: keep the sections of a network separated so that malicious actors cannot pivot within a network.

Playbooks are part of an incident-response plan. Playbooks can automate responses.

REFERENCES

12.2.4 Isolate and Containment Facts

q_isolate_contain_containment_secp7.question.fex

Question 30: ✔ Correct

!= or <> refers to Not Equal in which scripting language?

- Python
- Bash
- PowerShell
- PuTTY

EXPLANATION

!= or <> refers to Not Equal in the Python scripting language.

-ne refers to Not Equal in the Bash scripting language.

ne refers to Not Equal in the PowerShell scripting language.

PuTTY is an SSH and Telnet client that was originally developed for the Windows platform.

REFERENCES

12.6.4 Shells and Scripting Facts

q_shells_scripting_python_secp7.question.fex

Question 31: ✔ Correct

Which of the following drive configurations is fault tolerant?

- RAID 0
- Disk striping
- Expanded volume set
- ➡ RAID 5

EXPLANATION

The only fault-tolerant drive configuration in this list of selections is RAID 5, or disk striping with parity. Disk striping, or RAID 0, offers no fault tolerance. It only offers performance improvements. An expanded volume set offers not fault tolerance, either. An expanded volume set is a volume that spans more than one hard drive. In fact, an expanded volume set is more susceptible to problems than a single standalone hard drive.

REFERENCES

12.7.5 RAID Facts

q_raid_raid5_01_secp7.question.fex

Question 32: ✔ Correct

What does the hashing of log files provide?

- Prevention of log files being altered or overwritten
- Confidentiality to prevent unauthorized reading of the files
- Sequencing of files and log entries to recreate a timeline of events
- Prevention of the system running when the log files are full
- ➡ Proof that the files have not been altered

EXPLANATION

Perform hashing of the log files to detect alteration. If a log file is altered, the hash of that file will be different. If the current hash is the same, you can assume that the file has not been altered.

Hashing can detect alteration, but does not prevent it; users can still alter or delete a file. Encryption prevents unauthorized users from viewing the file contents. Timestamps on logs and log entries identify when events occur so you can reconstruct a timeline of events. Audit policies and retention policies control how log files are saved and what the system does when a log cannot be created or when disk space is full.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_hashing_02_secp7.question.fex

Question 33: ✔ Correct

A conditional statement that selects the statements to run depending on whether an expression is true or false is known as which of the following?

- If statement
- Else statement
- If else statement
- Else if statement

EXPLANATION

An *if else* statement is a conditional statement that selects the statements to run depending on whether an expression is true or false.

An *if* statement is a conditional statement that, if proven true, performs a function or displays information.

Else is a conditional statement that, if previous conditions are not true, displays alternate information or performs alternate commands.

Else if is a conditional statement performed after an if statement that, if true, performs a function.

REFERENCES

12.6.4 Shells and Scripting Facts

q_shells_ifelse_constant_secp7.question.fex

Question 34: ✔ Correct

You are configuring a source-initiated subscription on the collector computer in Event Viewer. Which of the following do you need to specify?

- Computer
- Computer group
- System log
- Content filter

EXPLANATION

You would choose the computer group for a source-initiated subscription.

Selecting a computer would be for the collector-initiated subscription.

The Forwarded Events log is selected, not the System log.

Content filtering is a strategy to keep employees from accessing unauthorized content on the web.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_group_secp7.question.fex

Question 35: ✔ Correct

A system failure has occurred. Which of the following restoration processes would result in the fastest restoration of all data to its most current state?

- Restore the full backup and all differential backups
- Restore the full backup and all incremental backups
- Restore the full backup and the last incremental backup
- Restore the full backup and the last differential backup

EXPLANATION

The fastest method for restoring data to its most current state is to restore the full backup and then the last differential backup. Differential backups include all changes since the last full backup (or other backup method that resets the archive bit).

Restoring the full backup and the last incremental backup is an incomplete restore because all of the incremental backups must be used. However, restoring several backup sets rather than a single set is slower. Only the last differential backup set needs to be used.

REFERENCES

12.8.4 Backup Types and Storage Facts

q_bkp_stor_diff_01_secp7.question.fex

Question 36: ✔ Correct

Your network uses the following backup strategy:

- Full backups every Sunday night
- Differential backups Monday night through Saturday night

On Thursday morning, the storage system fails. How many restore operations would you need to perform to recover all of the data?

- 1
- 2
- 3
- 4
- 5

EXPLANATION

You would need to perform two restore procedures:

1. Restore the full backup from Sunday

2. Restore the differential backup from Wednesday

If you did a full backup every night, you would restore only a single backup (Wednesday's backup). If you did full backups with incremental backups, you would restore the last full backup along with each incremental backup.

REFERENCES

12.8.4 Backup Types and Storage Facts

q_bkp_stor_diff_06_secp7.question.fex

Question 37: ✔ Correct

You have a large number of source computers in your IT environment. Which subscription type would be most efficient to employ?

- Event forwarding
- HTTP or HTTPS
- Collector-initiated
- ➡ Source-initiated

EXPLANATION

You would choose source-initiated since there are a large number of source computers.

Collector-initiated is more efficient if you have a limited number of source computers.

Event forwarding uses HTTP to transfer the events from the source to the collector.

HTTP or HTTPS makes setup relatively easy because most firewalls are already configured for HTTP and HTTPS traffic.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_source_02_secp7.question.fex

Question 38: ✔ Correct

Your disaster recovery plan calls for backup media to be stored at a different location. The location is a safe deposit box at the local bank. Because of this, the disaster recovery plan specifies that you choose a method that uses the least amount of backup media, but also allows you to quickly back up and restore files.

Which backup strategy would BEST meet the disaster recovery plan?

- ➡ Perform a full backup once per week and a differential backup the other days of the week.
- Perform a full backup each day of the week.
- Perform a full backup once per year and a differential backup for the rest of the days in the year.
- Perform a full backup once per week and an incremental backup the other days of the week.
- Perform a full backup once per month and an incremental backup the other days of the month.

EXPLANATION

Performing a full backup once per week and a differential backup the other days of the week would best meet this disaster recovery plan. The full backup backs up all files, usually to one tape. But the backup process can be time consuming. The differential backup backs up all files since the last full backup.

Performing a full backup each day would meet the requirement of using as few tapes as possible, but that backup process would be very time consuming each day.

Performing a full backup once per week and an incremental backup the other days of the week would be one of the fastest methods for backing up files, but it would require many tapes to complete the restore. The incremental backup only backs up files added or changed since the last backup. Because of this, in order to do a complete restore of the file system, you would need a tape for each day of the week on which an incremental backup ran.

Performing a full backup once per month and an incremental backup the other days of the month would be the fastest method to backup files, but it would require many tapes to complete the restore. The incremental backup only backs up files added or changed since the last backup. Because of this, in order to do a complete restore of the file system, you would need a tape for each day of the month on which an incremental backup ran.

Performing a full backup once per year with a differential backup for the rest of the days in the year would only require two tapes for a complete file system restore, but backing up the file system would become very time consuming. The differential backup would back up everything since the last full backup.

REFERENCES

12.8.4 Backup Types and Storage Facts

q_bkp_stor_diff_04_secp7.question.fex

Question 39: ✔ Correct

Which log file type is one of the most tedious to parse but can tell you exactly when users log onto your site and what their location is?

- System logs
- Event logs
- Web server logs
- Authentication logs

EXPLANATION

Web server logs are one of the most tedious of all logs to parse. However, these logs can tell you exactly when users log onto your site and what their location is.

Authentication logs are vital to a network's security. Authentication servers may be Active Directory-based or OpenLDAP depending on your network structure.

System logs are produced by an operating system.

Event logs show application access, crashes, updates, and any other relevant information that could be valuable in determining root-cause analysis.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_web_secp7.question.fex

Question 40: ✔ Correct

By default, events received from the source computers in Event Subscription are saved in which log?

- Security log
- Application log
- System log
- ➡ Forwarded Events log

EXPLANATION

By default, events received from source computers are saved in the Forwarded Events log.

There are application security logs, event security logs, and security logs for specialty applications, such as IDS/IPS, endpoints, firewalls, routers, and switches.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_event_secp7.question.fex