Exam Report: 7.8.8 Practice Questions

Date: 1/22/2020 7:35:52 pm
Time Spent: 48:07

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 73%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: 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 go to use them in the future?

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

Explanation

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

Storing logs offsite makes them harder to access and alter, and 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 will 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 copy that remains has not been altered.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_01]

Question 2: Correct

What does hashing of log files provide?

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

Explanation

Perform *hashing* of the log files to detect alteration. If a log file is altered, then 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. Time stamps 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

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_02]

Question 3: Correct

Over the past few days, a server has gone offline and rebooted automatically several times. You would like to see a record of when each of these restarts has occurred.

Which log type should you check?

- (selected) System
- Performance
- Firewall
- Security

Explanation

A system log records operating system, system, and hardware events. The system log will contain entries for when the system was shut down or started, when new hardware is added, and when new services are started.

A performance log records information about the use of system resources, such as the processor, memory, disk, or network utilization. A firewall log identifies traffic that has been allowed or denied through a firewall. A security log records information related to logons, such as incorrect passwords being used, and the use of user rights.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_03]

Question 4: Correct

You have heard about a Trojan horse program where the compromised system sends personal information to a remote attacker on a specific TCP port. You want to be able to easily tell whether any of your systems are sending data to the attacker.

Which log would you monitor?

- (selected) Firewall
- System
- Application
- Security

Explanation

A firewall log identifies traffic that has been allowed or denied through a firewall. You can identify traffic types used by computers on your network by looking at the outgoing ports. For example, you can identify servers that are running a specific service, or you can see computers that are communicating using ports that might indicate malicious software.

A system log records operating system, system, and hardware events. A security log records information related to logons, such as incorrect passwords being used, and the use of user rights. An application log records actions performed by an application. For each of these logs, the Trojan horse program will likely be written in a way that little or no logging will be recorded by the program, so examining these logs will not give you much information about the program on a system.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_04]

Question 5: Correct

Which of the following is a standard for sending log messages to a central logging server?

- OVAL
- LC4
- Nmap
- Syslog

Explanation

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).

The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system. LC4 (previously called LOphtcrack) is a password cracking tool. Nmap is a network mapping tool that performs ping and port scans.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_05]

Question 6: Correct

You suspect that some of your computers have been hijacked and are being used to perform denial of service attacks directed against other computers on the Internet.

Which log would you check to see if this is happening?

- Firewall
- System
- Application
- Security

Explanation

A firewall log identifies traffic that has been allowed or denied through a firewall. You can identify traffic types used by computers on your network by looking at the outgoing ports. For example, you can identify servers that are running a specific service, or you can see computers that are communicating using ports that might indicate malicious software.

A system log records operating system, system, and hardware events. A security log records information related to logons, such as incorrect passwords being used, and the use of user rights. An application log records actions performed by an application. For each of these logs, the Trojan horse program will likely be written in a way that little or no logging will be recorded by the program, so examining these logs will not give you much information about the program on a system.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_06]

Question 7: Incorrect

You suspect that your Web server has been the target of a denial of service attack. You would like to view information about the number of connections to the server over the past three days.

Which log would you most likely examine?

- Security
- System

~~Firewall~~

Performance

Explanation

A performance log records information about the use of system resources. For example, the performance log records processor, memory, disk, and network utilization. In addition, the performance log can record information related to the performance of a specific service, such as the number of connections to a Web server. You might also find this information in an application log for the service.

A security log records information related to logons, such as incorrect passwords being used, and the use of user rights. A system log records operating system, system, and hardware events. A firewall log identifies traffic that has been allowed or denied through a firewall.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_08]

Question 8: Incorrect

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 actions. Which of the following actions would best protect the log files?

Configure permissions on the log files to prevent access

Take a hash of the log files

Use syslog to send log entries to another server

~~Encrypt the log files~~

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 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 does not prevent the files from being deleted. Hashing of log files ensures integrity for the files to prove that the files have not been altered since they were created.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_09]

Question 9: Correct

You decide to use syslog to send log entries from multiple servers to a central logging server. Which of the following are the most important considerations for your implementation? (Select two.)

Clock synchronization between all devices

Retention policies on the syslog client

Disk space on the syslog server

A fast network connection

Explanation

A best practice to secure log files is to save the archived logs to a remote log server. Archived log server considerations include:

- The amount of disk space required to save the files on the server.
- Backup requirements on the server.

- Time stamping to ensure that the computer generating the event and the computer where the logs are saved have common system clocks.
- Integrity of the logs to ensure logs have not been modified.

Retention policies and disk space available for saving files is a consideration on the syslog server, not on the individual syslog clients. A fast network connection is not a requirement for using a remote logging solution.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_10]

Question 10: Correct

Which of the following best describes an *audit daemon*?

- (•) The trusted utility that runs a background process whenever auditing is enabled.
- ( ) The interface that allows the administrator to handle, set up, initialize, and modify subsystem parameters.
- ( ) The component that examines audit trails from current or previous audit sessions and reduces or compresses them for archival.
- ( ) The driver responsible for accepting audit records from the audit kernel.

Explanation

The *audit daemon* is the trusted utility that runs a background process whenever auditing is enabled. It is the sole reader of the audit device which in turn provides the daemon with blocks of records from the audit collection file.

The audit *device driver* is responsible for accepting audit records from the audit kernel. The audit *manager interface* allows the administrator to handle, set up, initialize, and modify subsystem parameters. The *data analysis and reduction* subsystem examines audit trails from current or previous audit sessions and reduces or compresses them for archival.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_11]

Question 11: Incorrect

Which of the following is **not** included in a system level audit event? (Select two.)

- [ ] Successful and unsuccessful logon attempts.
- [ ] The user name logging in.
- [ ] Activities performed on the system.
- [ ] Any actions performed by the user.
- [x] Names of accessed files.
- [ ] Beginning and ending times of access.

Explanation

The names of accessed files and actions performed by the user are both recorded in the *application level* audit event. A system level audit event tracks system-wide events including:

- Successful and unsuccessful logon attempts.
- The user name logging in.
- Beginning and ending times of access.
- Activities performed on the system.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_12]

Question 12: Incorrect

The auditing feature of an operating system serves as what form of control when users are informed that their actions are being monitored?

- Preventative
- ~~Detective~~
- Corrective
- Directive

Explanation

When users are being watched and they are aware of it, auditing is a preventative security control.

Auditing is never a corrective or directive security control. Auditing is detective when the audit logs are reviewed to locate the occurrence of security violating activities.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_13]

Question 13: Correct

What is the purpose of audit trails?

- Detect security-violating events
- Problem correction
- Restore systems to normal operations
- 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 a 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

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_14]

Question 14: Correct

Which of the following is a collection of recorded data that may include details about logons, object access, and other activities deemed important by your security policy that is often used to detect unwanted and unauthorized user activity?

- Audit trail
- CPS (certificate practice statement)
- Syslog
- Chain of custody

Explanation

An audit trail is a collection of recorded data that may include details about logons, object access, and

other activities deemed important by your security policy that is often used to detect unwanted and unauthorized user activity.

Syslog is a standard protocol for recording *system* events, not user events. The chain of custody is a document related to evidence gathering that contains details about personnel in possession and control of evidence from the time of discovery up through the time of presentation in court. CPS (Certificate Practice Statement) is a document written by a certificate authority outlining their certificate handling, management, and administration procedures.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_15]

Question 15: Correct

A recreation of historical events is made possible through?

- Penetration testing
- Incident reports
- Audit trails
- Audits

Explanation

The ability to recreate historical events is made possible through audit trails. Without the evidence in an audit trail, knowledge of activities that occurred in the past (minutes or longer) is fairly non-existent.

Audits are the security assessments performed by external auditors to check compliance with security policy and best business practices. Penetration testing is the use of hacker techniques and tools to assess security. An incident report is often produced from audit trails and is an example of the recreation of historical events rather than being the source that makes such reconstruction possible.

References

LabSim for Security Pro, Section 7.8.
[All Questions SecPro2017_v6.exm LOG_MGMT_16]