**QUESTION 1** The PRIMARY purpose of operations security is

A. Protect the system hardware from environment damage.

B. Monitor the actions of vendor service personnel.

C. Safeguard information assets that are resident in the system.

D. Establish thresholds for violation detection and logging.

**Section:** (none)

**Explanation/Reference:**

**QUESTION 2**

Which of the following is not a component of a Operations Security "triples"?

A. ) Asset

B. ) Threat

C. ) Vulnerability

D. ) Risk

**Section:** (none)

**Explanation/Reference:**

**QUESTION 3**

A periodic review of user account management should not determine:

A. ) Conformity with the concept of least privilege

B. ) Whether active accounts are still being used

C. ) Strength of user-chosen passwords

D. ) Whether management authorizations are up-to-date

**QUESTION 4**

Which of the following functions is less likely to be performed by a typical security administrator?

A. ) Setting user clearances and initial passwords

B. ) Adding and removing system users

C. ) Setting or changing file sensitivity labels

D. ) Reviewing audit data

**QUESTION 5**

Who is responsible for setting user clearances to computer-based information?

A. ) Security administrators

B. ) Operators

C. ) Data owners

D. ) Data custodians

**QUESTION 6**

Who is the individual permitted to add users or install trusted programs?

A. Database Administrator

B. Computer Manager

C. Security Administrator

D. Operations Manager

Typical system administrator or enhanced operator functions can include the following Installing system

software

Starting up (booting) and shutting down a system

Adding and removing system users

Performing back-ups and recovery

Handling printers and managing print queues -Ronald Krutz The CISSP PREP Guide (gold edition) pg 305-

304

**QUESTION 7**

In Unix, which file is required for you to set up an environment such that every used on the other host is a

trusted user that can log into this host without authentication?

A. /etc/shadow

B. /etc/host.equiv

C. /etc/passwd

D. None of the choices.

**Section:** (none)

**Explanation/Reference:**

Explanation:

The /etc/hosts.equiv file is saying that every user on the other host is a trusted user and allowed to log into

this host without authentication (i.e. NO PASSWORD). The only thing that must exist for a user to log in to

this system is an /etc/passwd entry by the same login name the user is currently using. In other words, if there

is a user trying to log into this system whose login name is "bhope", then there must be a "bhope" listed in

the /etc/passwd file.

**QUESTION 8**

For what reason would a network administrator leverage promiscuous mode?

A. To screen out all network errors that affect network statistical information.

B. To monitor the network to gain a complete statistical picture of activity.

C. To monitor only unauthorized activity and use.

D. To capture only unauthorized internal/external use.

**Section:** (none)

**QUESTION 9**

Which of the following questions is less likely to help in assessing controls over hardware and software

maintenance?

A. ) In access to all program libraries restricted and controlled?

B. ) Are integrity verification programs used by applications to look for evidences of data tampering, errors,

and omissions?

C. ) Is there version control?

D. ) Are system components tested, documented, and approved prior to promotion to production?

**Section:** (none)

**QUESTION 10**

Which of the following correctly describe "good" security practice?

A. Accounts should be monitored regularly.

B. You should have a procedure in place to verify password strength.

C. You should ensure that there are no accounts without passwords.

D. All of the choices.

**Section:** (none)

**Explanation/Reference:**

Explanation:

In many organizations accounts are created and then nobody ever touches those accounts again. This is a

very poor security practice. Accounts should be monitored regularly, you should look at unused accounts and

you should have a procedure in place to ensure that departing employees have their rights revoke prior to

leaving the company. You should also have a procedure in place to verify password strength or to ensure that

there are no accounts without passwords.

**QUESTION 11**

Access to the \_\_\_\_\_\_\_\_\_ account on a Unix server must be limited to only the system administrators that

must absolutely have this level of access.

A. Superuser of inetd.

B. Manager or root.

C. Fsf or root

D. Superuser or root.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Access to the superuser or root account on a server must be limited to only the system administrators that

must absolutely have this level of access. Use of programs such as SUDO is recommended to give limited

and controlled root access to administrators that have a need for such access.

**QUESTION 12**

Which of the following files should the security administrator be restricted to READ only access?

A. ) Security parameters

B. ) User passwords

C. ) User profiles

D. ) System log

**Section:** (none)

**QUESTION 13**

Root login should only be allowed via:

A. Rsh

B. System console

C. Remote program

D. VNC

**Section:** (none)

**Explanation/Reference:**

Explanation:

The root account must be the only account with a user ID of 0 (zero) that has open access to the UNIX shell. It

must not be possible for root to sign on directly except at the system console. All other access to the root

account must be via the 'su' command.

**QUESTION 14**

What does "System Integrity" mean?

A. ) The software of the system has been implemented as designed.

B. ) Users can't tamper with processes they do not own

C. ) Hardware and firmware have undergone periodic testing to verify that they are functioning properly

D. ) Design specifications have been verified against the formal top-level specification

**Section:** (none)

**QUESTION 15**

Operations Security seeks to primarily protect against which of the following?

A. ) object reuse

B. ) facility disaster

C. ) compromising emanations

D. ) asset threats

**Section:** (none)

**QUESTION 16**

In order to avoid mishandling of media or information, you should consider using:

A. Labeling

B. Token

C. Ticket

D. SLL

**Section:** (none)

**Explanation/Reference:**

Explanation:

In order to avoid mishandling of media or information, proper labeling must be used. All tape, floppy disks,

and other computer storage media containing sensitive information must be externally marked with the

appropriate sensitivity classification. All tape, floppy disks, and other computer storage media containing

unrestricted information must be externally marked as such.

All printed copies, printouts, etc., from a computer system must be clearly labeled with the proper

classification.

**QUESTION 17**

In order to avoid mishandling of media or information, which of the following should be labeled?

A. All of the choices.

B. Printed copies

C. Tape

D. Floppy disks

**Section:** (none)

**Explanation/Reference:**

Explanation:

In order to avoid mishandling of media or information, proper labeling must be used. All tape, floppy disks,

and other computer storage media containing sensitive information must be externally marked with the

appropriate sensitivity classification. All tape, floppy disks, and other computer storage media containing

unrestricted information must be externally marked as such.

All printed copies, printouts, etc., from a computer system must be clearly labeled with the proper

classification.

As a rule of thumb, you should have an indication of the classification of the document. The classification is

based on the sensitivity of information. It is usually marked at the minimum on the front and back cover, title,

and first pages.

**QUESTION 18**

Compact Disc (CD) optical media types is used more often for:

A. ) very small data sets

B. ) very small files data sets

C. ) larger data sets

D. ) very aggregated data sets

**Section:** (none)

**QUESTION 19**

At which temperature does damage start occurring to magnetic media?

A. ) 100 degrees

B. ) 125 degrees

C. ) 150 degrees

D. ) 175 degrees

**Section:** (none)

**QUESTION 20**

Which of the following statements pertaining to air conditioning for an information processing facility is

correct?

A. ) The AC units must be controllable from outside the area

B. ) The AC units must keep negative pressure in the room so that smoke and other gases are forced out of

the room

C. ) The AC units must be n the same power source as the equipment in the room to allow for easier

shutdown

D. ) The AC units must be dedicated to the information processing facilities

**Section:** (none)

**QUESTION 21**

Removing unnecessary processes, segregating inter-process communications, and reducing executing

privileges to increase system security is commonly called

A. Hardening

B. Segmenting

C. Aggregating

D. Kerneling

**Section:** (none)

**Explanation/Reference:**

What is hardening? Naturally, there is more than one definition, but in general, one tightens control using

policies which affect authorization, authentication and permissions. Nothing happens by default. You only give

out permission after thinking about it, something like "deny all" to everyone, then "allow" with justification.

Shut off everything, then only turn on that which must be turned on. It is not unlike locking every single door,

window and access point in your house, then unlocking only those that need to be. It is quite common for

users to take all the defaults when their new system gets turned on making for instant vulnerability. A major

problem is trying to figure out where all those details are that need to be turned off, without making the system

unusable.

**QUESTION 22**

RAID levels 3 and 5 run:

A. ) faster on hardware

B. ) slower on hardware

C. ) faster on software

D. )at the same speed on software and hardware

**Section:** (none)

**QUESTION 23**

Which of the following RAID levels functions as a single virtual disk?

A. ) RAID Level 7

B. ) RAID Level 5

C. ) RAID Level 10

D. ) RAID Level 2

**Section:** (none)

**QUESTION 24**

Which of the following takes the concept of RAID 1 (mirroring) and applies it to a pair of servers?

A. ) A redundant server implementation

B. ) A redundant client implementation

C. ) A redundant guest implementation

D. ) A redundant host implementation

**Section:** (none)

**QUESTION 25**

Which of the following enables the drive array to continue to operate if any disk or any path to any disk fails?

A. ) RAID Level 7

B. ) RAID Level 1

C. ) RAID Level 2

D. ) RAID Level 5

**Section:** (none)

**Explanation/Reference:**

"RAID Level 7 is a variation of RAID 5 wherein the array functions as a single virtual disk in the hardware.

This is sometimes simulated by software running over a RAID level 5 hardware implementation, which

enables the drive array to continue to operate if any disk or any path to any disk fails. It also provides parity

protection." Pg 91 Krutz: CISSP Prep Guide: Gold Edition.

**QUESTION 26**

Depending upon the volume of data that needs to be copied, full backups to tape can take:

A. ) an incredible amount of time

B. ) a credible amount of time

C. ) an ideal amount of time

D. ) an exclusive amount of time

**Section:** (none)

**QUESTION 27**

Which one of the following entails immediately transmitting copies of on-line transactions to a remote

computer facility for backup?

A. Archival storage management (ASM)

B. Electronic vaulting

C. Hierarchical storage management (HSM)

D. Data compression

**Section:** (none)

**Explanation/Reference:**

"Electronic vaulting makes an immediate copy of a changed file or transaction and sends it to a remote

location where the original backup is stored....Another technology used for automated backups is hierarrchial

storage management (HSM). In this situation, the HSM system dynamically manages the storage and covery

of files, which are copied to storage media devices that vary in speed and cost. The faster media hold the

data that is accessed more often and the seldom-useed files are stored on the slower devices, or near-line

devices. The different storage media rang from optical disk, magnetic disks, and tapes.

Pg. 619 Shon Harris CISSP All-In-One Certification Exam Guide

**QUESTION 28**

When continuous availability (24 hours-a-day processing) is required, which one of the following provides a

good alternative to tape backups?

A. Disk mirroring

B. Backup to jukebox

C. Optical disk backup

D. Daily archiving

**Section:** (none)

**Explanation/Reference:**

Hierarchical Storage Management (HSM). HSM provides continuous on-line backup by using optical or tape

'jukeboxes,' similar to WORMs. It appears as an infinite disk to the system, and can be configured to provide

the closest version of an available real-time backup. This is commonly employed in very large data retrieval

systems." Pg. 71 Krutz:

The CISSP Prep Guide.

**QUESTION 29**

Zip/Jaz drives are frequently used for the individual backups of small data sets of:

A. ) specific application data

B. ) sacrificial application data

C. ) static application data

D. ) dynamic application data

**Section:** (none)

**QUESTION 30**

With non-continuous backup systems, data that was entered after the last backup prior to a system crash will

have to be:

A. ) recreated

B. ) created

C. ) updated

D. ) deleted

**Section:** (none)

**QUESTION 31**

The alternate processing strategy in a business continuity plan can provide for required backup computing

capacity through a hot site, a cold site, or

A. A dial-up services program.

B. An off-site storage replacement.

C. An online backup program.

D. A crate and ship replacement.

**Section:** (none)

**Explanation/Reference:**

What I believe is being wanted here is not the other data center backup alternatives but transaction

redundancy implementation.

The CISSP candidate should understand the three concepts used to create a level of fault tolerance and

redundancy in transaction processing. While these processes are not used solely for disaster recovery, they

are often elements of a larger disaster recovery plan. If one or more of these processes are employed, the

ability of a company to get back online is greatly enhanced. -Ronald Krutz The CISSP PREP Guide (gold

edition) pg 394 (they are Electronic Vaulting, Remote journaling, and Database shadowing)

**QUESTION 32**

The 8mm tape format is commonly used in Helical Scan tape drives, but was superseded by:

A. ) Digital Linear Tape (DLT)

B. ) Analog Linear Tape (ALT)

C. ) Digital Signal Tape (DST)

D. ) Digital Coded Tape (DCT)

**Section:** (none)

**Explanation/Reference:**

"8mm Tape. This format was commonly used in Helical Scan tape drives, but was superseded by Digital

Linear Tape (DLT)." Pg 95 Krutz: CISSP Prep Guide: Gold Edition.

**QUESTION 33**

The spare drives that replace the failed drives are usually hot swappable, meaning they can be replaced on

the server in which of the following scenarios?

A. ) system is up and running

B. ) system is quiesced but operational

C. ) system is idle but operational

D. ) system is up and in single-user-mode

**Section:** (none)

**QUESTION 34**

Primarily run when time and tape space permits, and is used for the system archive or baselined tape sets is

the:

A. ) full backup method

B. ) Incremental backup method

C. ) differential backup method

D. ) tape backup method

**Section:** (none)

**QUESTION 35**

This backup method makes a complete backup of every file on the server every time it is run by:

A. ) full backup method

B. ) incremental backup method

C. ) differential backup method

D. ) tape backup method

**Section:** (none)

**QUESTION 36**

A backup of all files that are new or modified since the last full backup is

A. In incremental backup

B. A father/son backup

C. A differential backup

D. A full backup

**Section:** (none)

**Explanation/Reference:**

"Incremental backup -A procedure that backs up only those files that have been modified since the previous

backup of any sort. It does remove the archive attribute. Differential backup - A procedure that backs up all

files that have been modified since the last full backup. It does not remove the archive attribute." - Shon

Harris All-in-one CISSP Certification Guide pg 618

**QUESTION 37**

What two factors should a backup program track to ensure the serviceability of backup tape media?

A. The initial usage data of the media and the number of uses.

B. The physical characteristics and rotation cycle of the media.

C. The manufactured and model number of the tape media.

D. The frequency of usage and magnetic composition.

**Section:** (none)

**Explanation/Reference:**

The answer should be B. The physical charecteristics (what type of tape drive) and rotation cyle. (Frequency

of backup cycles and retention timE.)

**QUESTION 38**

Which of the following virus types changes some of its characteristics as it spreads?

A. ) boot sector

B. ) parasitic

C. ) stealth

D. ) polymorphic

**Section:** (none)

**QUESTION 39**

Which one of the following is a good defense against worms?

A. Differentiating systems along the lines exploited by the attack.

B. Placing limits on sharing, writing, and executing programs.

C. Keeping data objects small, simple, and obvious as to their intent.

D. Limiting connectivity by means of well-managed access controls.

**Section:** (none)

**Explanation/Reference:**

Take as general information regarding worms

"Although the worm is not technically malicious, opening the attachment allows the file to copy itself to the

user's PC Windows folder and then send the .pif-based program to any e-mail address stored on the hard

drive.

Ducklin said the huge risks associated with accepting program files such as .pif, .vbs (visual basic script) or

the more common .exe (executable) as attachments via e-mail outweighs the usefulness of distributing such

files in this manner. "There's no business sense for distributing programs via e-mail," he said. To illustrate the

point, Ducklin said six of the top 10 viruses reported to Sophos in April spread as Windows programs inside emails."

http://security.itworld.com/4340/030521stopworms/page\_1.html

**QUESTION 40**

An active content module, which attempts to monopolize and exploits system resources is called a

A. Macro virus

B. Hostile applet

C. Plug-in worm

D. Cookie

**Section:** (none)

**Explanation/Reference:**

This applet can execute in the network browser and may contain malicious code. The types of downloadable

programs are also known as mobile code. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 361

"ActiveX Controls are Microsoft's answer to Sun's Java applets. They operate in a very similar fashion, but

they are implemented using any on of a variety of languages, including Visual Basic, C, C++ and Java. There

are two key distinctions between Java applets and ActiveX controls. First, ActiveX controls use proprietary

Microsoft technology and, therefore, can only execute on systems running Microsoft operating systems.

Second, ActiveX controls are not subject to the sandbox restrictions placed on Java applets. They have full

access to the Windows operating environment and can perform a number of privileged actions. Therefore,

special precautions must be taken when deciding which ActiveX controls to download and execute. Many

security administrators have taken the somewhat harsh position of prohibiting the download of any ActiveX

content from all but a select handful of trusted sites." Pg. 214 Tittel: CISSP Study Guide

**QUESTION 41**

Macro viruses written in Visual Basic for Applications (VDA) are a major problem because

A. Floppy disks can propagate such viruses.

B. These viruses can infect many types of environments.

C. Anti-virus software is usable to remove the viral code.

D. These viruses almost exclusively affect the operating system.

**Section:** (none)

**QUESTION 42**

What is the term used to describe a virus that can infect both program files and boot sectors?

A. Polymorphic

B. Multipartite

C. Stealth

D. Multiple encrypting

**Section:** (none)

**QUESTION 43**

Why are macro viruses easy to write?

A. Active contents controls can make direct system calls

B. The underlying language is simple and intuitive to apply.

C. Only a few assembler instructions are needed to do damage.

D. Office templates are fully API compliant.

**Section:** (none)

**Explanation/Reference:**

Macro Languages enable programmers to edit, delete, and copy files. Because these languages are so easy

to use, many more types of macro viruses are possible. - Shon Harris All-in-one CISSP Certification Guide pg

785

**QUESTION 44**

Which one of the following traits alow macro viruses to spread more effectively than other types?

A. They infect macro systems as well as micro computers.

B. They attach to executable and batch applications.

C. They can be transported between different operating systems.

D. They spread in distributed systems without detection

**Section:** (none)

**Explanation/Reference:**

Macro virus is a virus written in one of these programming languages and is platform independent. They infect

and replicate in templates and within documents. - Shon Harris All-in-one CISSP Certification Guide pg 784

**QUESTION 45**

In what way could Java applets pose a security threat?

A. ) Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by

removing SSL and S-HTTP

B. ) Java interpreters do not provide the ability to limit system access that an applet could have on a client

system

C. ) Executables from the Internet may attempt an intentional attack when they are downloaded on a client

system

D. ) Java does not check the bytecode at runtime or provide other safety mechanisms for program isolation

from the client system.

**Section:** (none)

**Explanation/Reference:**

Explanation:

"Java Security

Java applets use a security scheme that employs a sandbox to limit the applet's access to certain specific

areas within the user's system and protects the system from malicious or poorly written applets. The applet is

supposed to run only within the sandbox. The sandbox restricts the applet's environment by restricting access

to a user's hard drives and system resources. If the applet does not go outside the sandbox, it is considered

safe. However, as with many other things in the computing world, the bad guys have figured out how to

escape their confines and restrictions. Programmers have figured out how to write applets that enable the

code to access hard drives and resources that are supposed to be protected by the Java security scheme.

This code can be malicious in nature and cause destruction and mayhem to the user and her system.

Java employs a sandbox in its security scheme, but if an applet can escape the confines of the sandbox, the

system can be easily compromised." Pg 726 Shon Harris: All-In-One CISSP Certification Guide.

**QUESTION 46**

What setup should an administrator use for regularly testing the strength of user passwords?

A. ) A networked workstation so that the live password database can easily be accessed by the cracking

program

B. ) A networked workstation so the password database can easily be copied locally and processed by the

cracking program

C. ) A standalone workstation on which the password database is copied and processed by the cracking

program

D. ) A password-cracking program is unethical; therefore it should not be used.

**Section:** (none)

**QUESTION 47**

On UNIX systems, passwords shall be kept:

A. In any location on behalf of root.

B. In a shadow password file.

C. In the /etc/passwd file.

D. In root.

**Section:** (none)

**Explanation/Reference:**

Explanation:

When possible, on UNIX systems, passwords shall not be kept in the /etc/passwd file, but rather in a shadow

password file which can be modified only by root or a program executing on behalf of root.

**QUESTION 48**

Which of the following would constitute the best example of a password to use for access to a system by a

network administrator?

A. ) holiday

B. ) Christmas12

C. ) Jenny&30

D. ) TrZc&45g

**Section:** (none)

**QUESTION 49**

Which of the following is not a media viability control used to protect the viability of data storage media?

A. ) clearing

B. ) marking

C. ) handling

D. ) storage

**Section:** (none)

**Explanation/Reference:**

Reference: pg 315 Krutz: CISSP Study Guide: Gold Edition

**QUESTION 50**

Which of the following refers to the data left on the media after the media has been erased?

A. ) remanence

B. ) recovery

C. ) sticky bits

D. ) semi-hidden

**Section:** (none)

**QUESTION 51**

What is the main issue with media reuse?

A. ) Degaussing

B. ) Data remanence

C. ) Media destruction

D. ) Purging

**Section:** (none)

**QUESTION 52**

What should a company do first when disposing of personal computers that once were used to store

confidential data?

A. ) Overwrite all data on the hard disk with zeroes

B. ) Delete all data contained on the hard disk

C. ) Demagnetize the hard disk

D. ) Low level format the hard disk

**Section:** (none)

**QUESTION 53**

Which of the following is not a critical security aspect of Operations Controls?

A. ) Controls over hardware

B. ) data media used

C. ) Operations using resources

D. ) Environment controls

**Section:** (none)

**Explanation/Reference:**

Reference: pg 311 Krutz: CISSP Prep Guide: Gold Edition

Section 2, Attack Response (8 Questions)

**QUESTION 54**

What tool is being used to determine whether attackers have altered system files of executables?

A. File Integrity Checker

B. Vulnerability Analysis Systems

C. Honey Pots

D. Padded Cells

**Section:** (none)

**Explanation/Reference:**

Explanation:

Although File Integrity Checkers are most often used to determine whether attackers have altered system files

or executables, they can also help determine whether vendor-supplied bug patches or other desired changes

have been applied to system binaries. They are extremely valuable to those conducting a forensic

examination of systems that have been attacked, as they allow quick and reliable diagnosis of the footprint of

an attack. This enables system managers to optimize the restoration of service after incidents occur.

**QUESTION 55**

A system file that has been patched numerous times becomes infected with a virus. The anti-virus software

warns that disinfecting the file can damage it. What course of action should be taken?

A. ) Replace the file with the original version from master media

B. ) Proceed with automated disinfection

C. ) Research the virus to see if it is benign

D. ) Restore an uninfected version of the patched file from backup media

**Section:** (none)

**QUESTION 56**

In an on-line transaction processing system, which of the following actions should be taken when erroneous or

invalid transactions are detected?

A. ) The transactions should be dropped from processing

B. ) The transactions should be processed after the program makes adjustments

C. ) The transactions should be written to a report and reviewed

D. ) The transactions should be corrected and reprocessed

**Section:** (none)

**QUESTION 57**

Which of the following is a reasonable response from the intrusion detection system when it detects Internet

Protocol (IP) packets where the IP source address is the same as the IP destination address?

A. Allow the packet to be processed by the network and record the event.

B. Record selected information about the item and delete the packet.

C. Resolve the destination address and process the packet.

D. Translate the source address and resend the packet.

**Section:** (none)

**Explanation/Reference:**

RFC 1918 and RFC 2827 state about private addressing and ip spoofing using the same source address as

destination address. Drop the packet.

**QUESTION 58**

Which of the following is not a good response to a detected intrusion?

A. ) Collect additional information about the suspected attack

B. ) Inject TCP reset packets into the attacker's connection to the victim system

C. ) Reconfigure routers and firewalls to block packets from the attacker's apparent connection

D. ) Launch attacks or attempt to actively gain information about the attacker's host

**Section:** (none)

**QUESTION 59**

Once an intrusion into your organizations information system has been detected, which of the following

actions should be performed first?

A. ) Eliminate all means of intruder access

B. ) Contain the intrusion

C. ) Determine to what extent systems and data are compromised

D. ) Communicate with relevant parties

**Section:** (none)

**QUESTION 60**

After an intrusion has been contained and the compromised systems having been reinstalled, which of the

following need not be reviewed before bringing the systems back to service?

A. ) Access control lists

B. ) System services and their configuration

C. ) Audit trails

D. ) User accounts

**Section:** (none)

**QUESTION 61**

Which of the following includes notifying the appropriate parties to take action in order to determine the extent

of the severity of an incident and to remediate the incident's effects?

A. ) Intrusion Evaluation (IE) and Response

B. ) Intrusion Recognition (IR) and Response

C. ) Intrusion Protection (IP) and Response

D. ) Intrusion Detection (ID) and Response

**Section:** (none)

**Explanation/Reference:**

"Intrusion Detection (ID) and Response is the task of monitoring systems for evidence of an intrusion or an

inappropriate usage. This includes notifying the appropriate parties to take action in order to determine the

extent of the severity of an incident and to remediate the incident's effects." Pg 86 Krutz: CISSP Prep Guide:

Gold Edition.

Section 3, Violation Monitoring (63 Questions)

**QUESTION 62**

Which of the following is used to monitor network traffic or to monitor host audit logs in order to determine

violations of security policy that have taken place?

A. ) Intrusion Detection System

B. ) Compliance Validation System

C. ) Intrusion Management System

D. )Compliance Monitoring System

**Section:** (none)

**QUESTION 63**

Which of the following is not a technique used for monitoring?

A. ) Penetration testing

B. ) Intrusion detection

C. ) Violation processing (using clipping levels)

D. ) Countermeasures testing

**Section:** (none)

**QUESTION 64**

Which one of the following is NOT a characteristic of an Intrusion Detection System? (IDS)

A. Determines the source of incoming packets.

B. Detects intruders attempting unauthorized activities.

C. Recognizes and report alterations to data files.

D. Alerts to known intrusion patterns.

**Section:** (none)

**Explanation/Reference:**

Explanation: Software employed to monitor and detect possible attacks and behaviors that vary from the

normal and expected activity. The IDS can be network-based, which monitors network traffic, or host-based,

which monitors activities of a specific system and protects system files and control mechanisms. - Shon Harris

All-in-one CISSP Certification Guide pg 932

**QUESTION 65**

An IDS detects an attach using which of the following?

A. ) an event-based ID or a statistical anomaly-based ID

B. ) a discrete anomaly-based ID or a signature-based ID

C. ) a signature-based ID or a statistical anomaly-based ID

D. ) a signature-based ID or an event-based ID

**Section:** (none)

**QUESTION 66**

Which of the following monitors network traffic in real time?

A. ) network-based IDS

B. ) host-based IDS

C. ) application-based IDS

D. ) firewall-based IDS

**Section:** (none)

**QUESTION 67**

What technology is being used to detect anomalies?

A. IDS

B. FRR

C. Sniffing

D. Capturing

**Section:** (none)

**Explanation/Reference:**

Explanation:

Intrusion Detection is a quickly evolving domain of expertise. In the past year we have seen giant steps

forward in this area. We are now seeing IDS engines that will detect anomalies, and that have some built-in

intelligence. It is no longer a simple game of matching signatures in your network traffic.

**QUESTION 68**

IDSs verify, itemize, and characterize threats from:

A. Inside your organization's network.

B. Outside your organization's network.

C. Outside and inside your organization's network.

D. The Internet.

**Section:** (none)

**Explanation/Reference:**

Explanation:

IDSs verify, itemize, and characterize the threat from both outside and inside your organization's network,

assisting you in making sound decisions regarding your allocation of computer security resources. Using IDSs

in this manner is important, as many people mistakenly deny that anyone (outsider or insider) would be

interested in breaking into their networks. Furthermore, the information that IDSs give you regarding the

source and nature of attacks allows you to make decisions regarding security strategy driven by demonstrated

need, not guesswork or folklore.

**QUESTION 69**

IDS can be described in terms of what fundamental functional components?

A. Response

B. Information Sources

C. Analysis

D. All of the choices.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Many IDSs can be described in terms of three fundamental functional components:

Information Sources - the different sources of event information used to determine whether an intrusion has

taken place. These sources can be drawn from different levels of the system, with network, host, and

application monitoring most common. Analysis - the part of intrusion detection systems that actually organizes

and makes sense of the events derived from the information sources, deciding when those events indicate

that intrusions are occurring or have already taken place. The most common analysis approaches are misuse

detection and anomaly detection.

Response - the set of actions that the system takes once it detects intrusions. These are typically grouped into

active and passive measures, with active measures involving some automated intervention on the part of the

system, and passive measures involving reporting IDS findings to humans, who are then expected to take

action based on those reports.

**QUESTION 70**

What are the primary goals of intrusion detection systems? (Select all that apply.)

A. Accountability

B. Availability

C. Response

D. All of the choices

C

**Section:** (none)

**Explanation/Reference:**

Explanation:

Although there are many goals associated with security mechanisms in general, there are two overarching

goals usually stated for intrusion detection systems. Accountability is the capability to link a given activity or

event back to the party responsible for initiating it. This is essential in cases where one wishes to bring

criminal charges against an attacker. The goal statement associated with accountability

is: "I can deal with security attacks that occur on my systems as long as I know who did it (and where to find

them.)" Accountability is difficult in TCP/IP networks, where the protocols allow attackers to forge the identity

of source addresses or other source identifiers. It is also extremely difficult to enforce accountability in any

system that employs weak identification and authentication mechanisms.

Response is the capability to recognize a given activity or event as an attack and then taking action to block

or otherwise affect its ultimate goal. The goal statement associated with response is "I don't care who attacks

my system as long as I can recognize that the attack is taking place and block it." Note that the requirements

of detection are quite different for response than for accountability.

**QUESTION 71**

What is the most common way to classify IDSs?

A. Group them by information source.

B. Group them by network packets.

C. Group them by attackers.

D. Group them by signs of intrusion.

**Section:** (none)

**Explanation/Reference:**

Explanation:

The most common way to classify IDSs is to group them by information source. Some IDSs

analyze network packets, captured from network backbones or LAN segments, to find attackers. Other IDSs

analyze information sources generated by the operating system or application software for signs of intrusion.

**QUESTION 72**

The majority of commercial intrusion detection systems are:

A. Identity-based

B. Network-based

C. Host-based

D. Signature-based

**Section:** (none)

**Explanation/Reference:**

Explanation:

The majority of commercial intrusion detection systems are network-based. These IDSs detect attacks by

capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS

can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby

protecting those hosts.

**QUESTION 73**

Which of the following is a drawback of Network-based IDSs?

A. It cannot analyze encrypted information.

B. It is very costly to setup.

C. It is very costly to manage.

D. It is not effective.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Network-based IDSs cannot analyze encrypted information. This problem is increasing as

more organizations (and attackers) use virtual private networks. Most network-based IDSs cannot tell whether

or not an attack was successful; they can only discern that an attack was initiated. This means that after a

network-based IDS detects an attack, administrators must manually investigate each attacked host to

determine whether it was indeed penetrated.

**QUESTION 74**

Host-based IDSs normally utilize information from which of the following sources?

A. Operating system audit trails and system logs.

B. Operating system audit trails and network packets.

C. Network packets and system logs.

D. Operating system alarms and system logs.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system

logs. Operating system audit trails are usually generated at the innermost (kernel) level of the operating

system, and are therefore more detailed and better protected than system logs. However, system logs are

much less obtuse and much smaller than audit trails, and are furthermore far easier to comprehend. Some

host-based IDSs are designed to support a centralized IDS management and reporting infrastructure that can

allow a single management console to track many hosts. Others generate messages in formats that are

compatible with network management systems.

**QUESTION 75**

When comparing host based IDS with network based ID, which of the following is an obvious advantage?

A. It is unaffected by switched networks.

B. It cannot analyze encrypted information.

C. It is not costly to setup.

D. It is not costly to manage.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Host-based IDSs are unaffected by switched networks. When Host-based IDSs operate on OS

audit trails, they can help detect Trojan horse or other attacks that involve software integrity breaches. These

appear as inconsistencies in process execution.

**QUESTION 76**

You are comparing host based IDS with network based ID. Which of the following will you consider as an

obvious disadvantage of host based IDS?

A. It cannot analyze encrypted information.

B. It is costly to remove.

C. It is affected by switched networks.

D. It is costly to manage.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Host-based IDSs are harder to manage, as information must be configured and managed for

every host monitored. Since at least the information sources (and sometimes part of the analysis engines) for

host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the

attack.

Host-based IDSs are not well suited for detecting network scans or other such surveillance that targets an

entire network, because the IDS only sees those network packets received by its host. Host-based IDSs can

be disabled by certain denial-of-service attacks.

**QUESTION 77**

Which of the following IDS inflict a higher performance cost on the monitored systems?

A. Encryption based

B. Host based

C. Network based

D. Trusted based

**Section:** (none)

**Explanation/Reference:**

Explanation:

Host-based IDSs use the computing resources of the hosts they are monitoring, therefore inflicting a

performance cost on the monitored systems.

**QUESTION 78**

Application-based IDSs normally utilize information from which of the following sources?

A. Network packets and system logs.

B. Operating system audit trails and network packets.

C. Operating system audit trails and system logs.

D. Application's transaction log files.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Application-based IDSs are a special subset of host-based IDSs that analyze the events transpiring within a

software application. The most common information sources used by application-based IDSs are the

application's transaction log files.

**QUESTION 79**

Which of the following are the major categories of IDSs response options?

A. Active responses

B. Passive responses

C. Hybrid

D. All of the choices.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Once IDSs have obtained event information and analyzed it to find symptoms of attacks, they generate

responses. Some of these responses involve reporting results and findings to a pre-specified location. Others

involve more active automated responses. Though researchers are tempted to underrate the importance of

good response functions in IDSs, they are actually very important. Commercial IDSs support a wide range of

response options, often categorized as active responses, passive responses, or some mixture of the two.

**QUESTION 80**

Alarms and notifications are generated by IDSs to inform users when attacks are detected. The most common

form of alarm is:

A. Onscreen alert

B. Email

C. Pager

D. Icq

**Section:** (none)

**Explanation/Reference:**

Explanation:

Alarms and notifications are generated by IDSs to inform users when attacks are detected. Most commercial

IDSs allow users a great deal of latitude in determining how and when alarms are generated and to whom they

are displayed.

The most common form of alarm is an onscreen alert or popup window. This is displayed on the IDS console

or on other systems as specified by the user during the configuration of the IDS. The information provided in

the alarm message varies widely, ranging from a notification that an intrusion has taken place to extremely

detailed messages outlining the IP addresses of the source and target of the attack, the specific attack tool

used to gain access, and the outcome of the attack. Another set of options that are of utility to large or

distributed organizations are those involving remote notification of alarms or alerts. These allow organizations

to configure the IDS so that it sends alerts to cellular phones and pagers carried by incident response teams or

system security personnel.

**QUESTION 81**

Which of the following is a valid tool that complements IDSs?

A. All of the choices.

B. Padded Cells

C. Vulnerability Analysis Systems

D. Honey Pots

**Section:** (none)

**Explanation/Reference:**

Explanation:

Several tools exist that complement IDSs and are often labeled as intrusion detection products by vendors

since they perform similar functions. They are Vulnerability Analysis Systems, File Integrity Checkers, Honey

Pots, and Padded Cells.

"IDS-Related Tools

Intrusion detection systems are often deployed in concert with several other components. These IDS-related

tools expand the usefulness and capabilities of IDSs and make IDSs more efficient and less prone to false

positives. These tools include honey pots, padded cells, and vulenerability scanners." Pg. 46 Tittel: CISSP

Study Guide

**QUESTION 82**

A problem with a network-based ID system is that it will not detect attacks against a host made by an intruder

who is logged in at which of the following?

A. ) host's terminal

B. ) guest's terminal

C. ) client's terminal

D. ) server's terminal

**Section:** (none)

**QUESTION 83**

When the IDS detect attackers, the attackers are seamlessly transferred to a special host. This method is

called:

A. Vulnerability Analysis Systems

B. Padded Cell

C. Honey Pot

D. File Integrity Checker

**Section:** (none)

**Explanation/Reference:**

Explanation:

Padded cells take a different approach. Instead of trying to attract attackers with tempting data, a padded cell

operates in tandem with traditional IDS. When the IDS detect attackers, it seamlessly transfers then to a

special padded cell host.

**QUESTION 84**

Which of the following is a weakness of both statistical anomaly detection and pattern matching?

A. Lack of ability to scale.

B. Lack of learning model.

C. Inability to run in real time.

D. Requirement to monitor every event.

**Section:** (none)

**Explanation/Reference:**

Explanation: Disadvantages of Knowledge-based ID systems:

This system is resources-intensive; the knowledge database continually needs maintenance and updates

New, unique, or original attacks often go unnoticed.Disadvantages of Behavior-based ID systems:

The system is characterized by high false alarm rates. High positives are the most common failure of ID

systems and can create data noise that makes the system unusable. The activity and behavior of the users

while in the networked system might not be static enough to effectively implement a behavior-based ID

system. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 88

**QUESTION 85**

The two most common implementations of Intrusion Detection are which of the following?

A. ) They commonly reside on a discrete network segment and monitor the traffic on that network segment

B. ) They commonly will not reside on a discrete network segment and monitor the traffic on that network

segment

C. ) They commonly reside on a discrete network segment but do not monitor the traffic on that network

segment

D. ) They commonly do not reside on a discrete network segment and monitor the traffic on that network

segment

**Section:** (none)

**QUESTION 86**

What are the primary approaches IDS takes to analyze events to detect attacks?

A. Misuse detection and anomaly detection.

B. Log detection and anomaly detection.

C. Misuse detection and early drop detection.

D. Scan detection and anomaly detection.

**Section:** (none)

**Explanation/Reference:**

Explanation:

There are two primary approaches to analyzing events to detect attacks: misuse detection and anomaly

detection. Misuse detection, in which the analysis targets something known to be "bad", is the technique used

by most commercial systems.

Anomaly

detection, in which the analysis looks for abnormal patterns of activity, has been, and continues to be, the

subject of a great deal of research. Anomaly detection is used in limited form by a number of IDSs. There are

strengths and weaknesses associated with each approach, and it appears that the most effective IDSs use

mostly misuse detection methods with a smattering of anomaly detection components.

**QUESTION 87**

Misuse detectors analyze system activity and identify patterns. The patterns corresponding to know attacks

are called:

A. Attachments

B. Signatures

C. Strings

D. Identifications

**Section:** (none)

**Explanation/Reference:**

Explanation:

Misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern

of events that describe a known attack. As the patterns corresponding to known attacks are called signatures,

misuse detection is sometimes called "signature-based detection." The most common form of misuse

detection used in commercial products specifies each pattern of events corresponding to an attack as a

separate signature. However, there are more sophisticated approaches to doing misuse detection (called

"state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.

**QUESTION 88**

Which of the following is an obvious disadvantage of deploying misuse detectors?

A. They are costly to setup.

B. They are not accurate.

C. They most be constantly updated with signatures of new attacks.

D. They are costly to use.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Misuse detectors can only detect those attacks they know about - therefore they must be constantly updated

with signatures of new attacks. Many misuse detectors are designed to use tightly defined signatures that

prevent them from detecting variants of common attacks. State-based misuse detectors can overcome this

limitation, but are not commonly used in commercial IDSs.

**QUESTION 89**

What detectors identify abnormal unusual behavior on a host or network?

A. None of the choices.

B. Legitimate detectors.

C. Anomaly detectors.

D. Normal detectors.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Anomaly detectors identify abnormal unusual behavior (anomalies) on a host or network. They function on the

assumption that attacks are different from "normal" (legitimate) activity and can therefore be detected by

systems that identify these differences. Anomaly detectors construct profiles representing normal behavior of

users, hosts, or network connections. These profiles are constructed from historical data collected over a

period of normal operation. The detectors then collect event data and use a variety of measures to determine

when monitored activity deviates from the norm.

**QUESTION 90**

A network-based IDS is which of the following?

A. ) active while it acquires data

B. ) passive while it acquires data

C. ) finite while it acquires data

D. ) infinite while it acquires data

**Section:** (none)

**QUESTION 91**

Which of the following usually provides reliable, real-time information without consuming network or host

resources?

A. ) network-based IDS

B. ) host-based IDS

C. ) application-based IDS

D. ) firewall-based IDS

**Section:** (none)

**Explanation/Reference:**

"A network-based IDS has little negative affect on overall network performance, and because it is deployed on

a single-purpose system, it doesn't adversely affect the performance of any other computer." Pg 34 Krutz:

CISSP Prep Guide: Gold Edition.

**QUESTION 92**

Which of the following would assist in intrusion detection?

A. ) audit trails

B. ) access control lists

C. ) security clearances

D. ) host-based authentication

**Section:** (none)

**QUESTION 93**

Using clipping levels refers to:

A. ) setting allowable thresholds on reported activity

B. ) limiting access to top management staff

C. ) setting personnel authority limits based on need-to-know basis

D. ) encryption of data so that it cannot be stolen

**Section:** (none)

**QUESTION 94**

In what way can violation clipping levels assist in violation tracking and analysis?

A. ) Clipping levels set a baseline for normal user errors, and violations exceeding that threshold will be

recorded for analysis of why the violations occurred

B. ) Clipping levels enable a security administrator to customize the audit trail to record only those violations

which are deemed to be security relevant

C. ) Clipping levels enable the security administrator to customize the audit trail to record only actions for

users with access to usercodes with a privileged status

D. ) Clipping levels enable a security administrator to view all reductions in security levels which have been

made to usercodes which have incurred violations

**Section:** (none)

**QUESTION 95**

When establishing a violation tracking and analysis process, which one of the following parameters is used to

keep the quantity of data to manageable levels?

A. Quantity baseline

B. Maximum log size

C. Circular logging

D. Clipping levels

**Section:** (none)

**Explanation/Reference:**

To make violation tracking effective, clipping levels must be established. A clipping level is a baseline of user

activity that is considered a routine level of user errors. When a clipping level is exceeded, a violation record

is then produced. Clipping levels are also used for variance detection. -Ronald Krutz The CISSP PREP Guide

(gold edition) pg 318

**QUESTION 96**

Audit trails based upon access and identification codes establish...

A. intrustion detection thresholds

B. individual accountability

C. audit review critera

D. individual authentication

**Section:** (none)

**Explanation/Reference:**

Accountability is another facet of access control. Individuals on a system are responsible for their actions. This

accountability property enables system activities to be traced to the proper individuals. Accountability is

supported by audit trails that record events on the system and on the network. Audit trails can be used for

intrusion detection and for the reconstruction of past events. -Ronald Krutz The CISSP PREP Guide (gold

edition) pg

**QUESTION 97**

The primary reason for enabling software audit trails is which of the following?

A. ) Improve system efficiency

B. ) Improve response time for users

C. ) Establish responsibility and accountability

D. ) Provide useful information to track down processing errors

**Section:** (none)

**Explanation/Reference:**

"Auditing capabilities ensure that users are accountable for their actions, verify that the security polices are

enforced, and are used as investigation tools." Pg 161 Shon Harris:

All-in-One CISSP Certification

**QUESTION 98**

Tracing violations, or attempted violations of system security to the user responsible is a function of?

A. authentication

B. access management

C. integrity checking

D. accountability

**Section:** (none)

**Explanation/Reference:**

Auditing capabilities ensure that users are accountable for their actions, verify that the security policies are

enforced, worked as a deterrent to improper actions, and are used as investigation tools. - Shon Harris All-inone

CISSP Certification Guide pg 182

**QUESTION 99**

According to the Minimum Security Requirements (MSR) for Multi-User Operating Systems (NISTIR 5153)

document, which of the following statements pertaining to audit data recording is incorrect?

A. ) The system shall provide end-to-end user accountability for all security-relevant events

B. ) The system shall protect the security audit trail from unauthorized access

C. ) For maintenance purposes, it shall be possible to disable the recording of activities that require

privileges.

D. ) The system should support an option to maintain the security audit trail data in encrypted format

**Section:** (none)

**QUESTION 100**

Which of the following questions is less likely to help in assessing controls over audit trails?

A. ) Does the audit trail provide a trace of user actions?

B. ) Are incidents monitored and tracked until resolved?

C. ) Is access to online logs strictly controlled?

D. ) Is there separation of duties between security personnel who administer the access control function and

those who administer the audit trail?

**Section:** (none)

**QUESTION 101**

You should keep audit trail on which of the following items?

A. Password usage.

B. All unsuccessful logon.

C. All of the choices.

D. All successful logon.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Keep audit trail of password usage; log all Successful logon, Unsuccessful logon, Date, Time, ID, Login name.

Control maximum logon attempt rate where possible.Where possible

users must be automatically logged off after 30 minutes of inactivity.

**QUESTION 102**

In addition to providing an audit trail required by auditors, logging can be used to

A. provide backout and recovery information

B. prevent security violations

C. provide system performance statistics

D. identify fields changed on master files.

**Section:** (none)

**Explanation/Reference:**

Auditing tools are technical controls that track activity within a network on a network device or on a specific

computer. Even though auditing is not an activity that will deny an entity access to a network or computer, it

will track activities so a network administrator can understand the types of access that took place, identify a

security breach, or warn the administrator of suspicious activity. This can be used to point out weakness of

their technical controls and help administrators understand where changes need to be made to preserve the

necessary security level within the environment. . - Shon Harris All-in-one CISSP Certification Guide pg 179-

180

**QUESTION 103**

Which of the following should NOT be logged for performance problems?

A. CPU load.

B. Percentage of use.

C. Percentage of idle time.

D. None of the choices.

**Section:** (none)

**Explanation/Reference:**

Explanation:

The level of logging will be according to your company requirements. Below is a list of items that could be

logged, please note that some of the items may not be applicable to all operating systems. What is being

logged depends on whether you are looking for performance problems or security problems. However you

have to be careful about performance problems that could affect your security.

**QUESTION 104**

Which of the following should be logged for security problems?

A. Use of mount command.

B. Percentage of idle time.

C. Percentage of use.

D. None of the choices.

**Section:** (none)

**Explanation/Reference:**

Explanation:

The level of logging will be according to your company requirements. Below is a list of items that could be

logged, please note that some of the items may not be applicable to all operating systems. What is being

logged depends on whether you are looking for performance problems or security problems. However you

have to be careful about performance problems that could affect your security.

**QUESTION 105**

Which of the following services should be logged for security purpose?

A. bootp

B. All of the choices.

C. sunrpc

D. tftp

**Section:** (none)

**Explanation/Reference:**

Explanation:

Request for the following services should be logged: systat, bootp, tftp, sunrpc, snmp, snmp-trap, nfs.

**QUESTION 106**

The auditing method that assesses the extent of the system testing, and identifies specific program logic that

has not been tested is called

A. Decision process analysis

B. Mapping

C. Parallel simulation

D. Test data method

**Section:** (none)

**Explanation/Reference:**

"Testing of software modules or unit testing should be addressed when the modules are being designed.

Personnel separate from the programmers should conduct this testing. The test data is part of the

specifications. Testing should not only check the modules using normal and valid input data, but it should also

check for incorrect types, out-of-range values, and other bounds and/or conditions. Live or actual field data is

not recommended for use in the testing procedures because both data types might not cover out-of-range

situations and the correct outputs of the test are unknown. Special test suites of data that exercise all paths of

the software to the fullest extent possible and whose corrected resulting outputs are known beforehand should

be used." Pg. 345 Krutz: The CISSP Prep Guide: Gold Edition.

**QUESTION 107**

Who should NOT have access to the log files?

A. Security staff.

B. Internal audit staff.

C. System administration staff.

D. Manager's secretary.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Logs must be secured to prevent modification, deletion, and destruction. Only authorized persons should have

access or permission to read logs. A person is authorized if he or she is a member of the internal audit staff,

security staff, system administration staff, or he or she has a need for such access to perform regular duties.

**QUESTION 108**

Which of the following correctly describe the use of the collected logs?

A. They are used in the passive monitoring process only.

B. They are used in the active monitoring process only.

C. They are used in the active and passive monitoring process.

D. They are used in the archiving process only.

**Section:** (none)

**Explanation/Reference:**

Explanation:

All logs collected are used in the active and passive monitoring process. All logs are kept on archive for a

period of time. This period of time will be determined by your company policies. This allows the use of logs for

regular and annual audits if retention is longer then a year. Logs must be secured to prevent modification,

deletion, and destruction.

**QUESTION 109**

All logs are kept on archive for a period of time. What determines this period of time?

A. Administrator preferences.

B. MTTR

C. Retention polices

D. MTTF

**Section:** (none)

**Explanation/Reference:**

Explanation:

All logs collected are used in the active and passive monitoring process. All logs are kept on archive for a

period of time. This period of time will be determined by your company policies. This allows the use of logs for

regular and annual audits if retention is longer then a year. Logs must be secured to prevent modification,

deletion, and destruction.

**QUESTION 110**

Logs must be secured to prevent:

A. Creation, modification, and destruction.

B. Modification, deletion, and initialization.

C. Modification, deletion, and destruction.

D. Modification, deletion, and inspection.

**Section:** (none)

**Explanation/Reference:**

Explanation:

All logs collected are used in the active and passive monitoring process. All logs are kept on archive for a

period of time. This period of time will be determined by your company policies. This allows the use of logs for

regular and annual audits if retention is longer then a year. Logs must be secured to prevent modification,

deletion, and destruction.

**QUESTION 111**

To ensure dependable and secure logging, all computers must have their clock synchronized to:

A. A central timeserver.

B. The log time stamp.

C. The respective local times.

D. None of the choices.

**Section:** (none)

**Explanation/Reference:**

Explanation:

The following pre-requisite must be met to ensure dependable and secure logging:

All computers must have their clock synchronized to a central timeserver to ensure accurate time on events

being logged.

If possible all logs should be centralized for easy analysis and also to help detect patterns of abuse across

servers.

Logging information traveling on the network must be encrypted if possible. Log files are stored and protected

on a machine that has a hardened shell. Log files must not be modifiable without a trace or record of such

modification.

**QUESTION 112**

To ensure dependable and secure logging, logging information traveling on the network should be:

A. Stored

B. Encrypted

C. Isolated

D. Monitored

**Section:** (none)

**Explanation/Reference:**

Explanation:

The following pre-requisite must be met to ensure dependable and secure logging:

All computers must have their clock synchronized to a central timeserver to ensure accurate time on events

being logged.

If possible all logs should be centralized for easy analysis and also to help detect patterns of abuse across

servers.

Logging information traveling on the network must be encrypted if possible. Log files are stored and protected

on a machine that has a hardened shell. Log files must not be modifiable without a trace or record of such

modification.

**QUESTION 113**

The activity that consists of collecting information that will be used for monitoring is called:

A. Logging

B. Troubleshooting

C. Auditing

D. Inspecting

**Section:** (none)

**Explanation/Reference:**

Explanation:

Logging is the activity that consists of collecting information that will be used for monitoring and auditing.

Detailed logs combined with active monitoring allow detection of security issues before they negatively affect

your systems.

**QUESTION 114**

How often should logging be run?

A. Once every week.

B. Always

C. Once a day.

D. During maintenance.

**Section:** (none)

**Explanation/Reference:**

Explanation:

Usually logging is done 24 hours per day, 7 days per week, on all available systems and services except

during the maintenance window where some of the systems and services may not be available while

maintenance is being performed.

**QUESTION 115**

Which of the following are security events on Unix that should be logged?

A. All of the choices.

B. Use of Setgid.

C. Change of permissions on system files.

D. Use of Setuid.

**Section:** (none)

**Explanation/Reference:**

Explanation:

The following file changes, conditions, and events are logged:

.rhosts.

UNIX Kernel.

/etc/password.

rc directory structure.

bin files.

lib files.

Use of Setuid.

Use of Setgid.

Change of permission on system or critical files.

**QUESTION 116**

Which of the following are potential firewall problems that should be logged?

A. Reboot

B. All of the choices.

C. Proxies restarted.

D. Changes to configuration file.

**Section:** (none)

**Explanation/Reference:**

Explanation:

The following firewall configuration problem are logged:

Reboot of the firewall.

Proxies that cannot start (e.g. Within TIS firewall).

Proxies or other important services that have died or restarted.

Changes to firewall configuration file.

A configuration or system error while firewall is running.

**QUESTION 117**

Which of the following is required in order to provide accountability?

A. ) Authentication

B. ) Integrity

C. ) Confidentiality

D. ) Audit trails

**Section:** (none)

**Explanation/Reference:**

Reference: pg 5 Tittel: CISSP Study Guide

**QUESTION 118**

The principle of accountability is a principle by which specific action can be traced back to:

A. A policy

B. An individual

C. A group

D. A manager

**Section:** (none)

**Explanation/Reference:**

Explanation:

The principle of accountability has been described in many references; it is a principle by which specific action

can be traced back to an individual. As mentioned by Idrach, any significant action should be traceable to a

specific user. The definition of "Significant" is entirely dependant on your business circumstances and risk

management model. It was also mentioned by Rino that tracing the actions of a specific user is fine but we

must also be able to ascertain that this specific user was responsible for the uninitiated action.

**QUESTION 119**

The principle of \_\_\_\_\_\_\_\_\_ is a principle by which specific action can be traced back to anyone of your users.

A. Security

B. Integrity

C. Accountability

D. Policy

**Section:** (none)

**Explanation/Reference:**

Explanation:

The principle of accountability has been described in many references; it is a principle by which specific action

can be traced back to an individual. As mentioned by Idrach, any significant action should be traceable to a

specific user. The definition of "Significant" is entirely dependant on your business circumstances and risk

management model. It was also mentioned by Rino that tracing the actions of a specific user is fine but we

must also be able to ascertain that this specific user was responsible for the uninitiated action.

**QUESTION 120**

According to the principle of accountability, what action should be traceable to a specific user?

A. Material

B. Intangible

C. Tangible

D. Significant

**Section:** (none)

**Explanation/Reference:**

Explanation:

The principle of accountability has been described in many references; it is a principle by which specific action

can be traced back to an individual. As mentioned by Idrach, any significant action should be traceable to a

specific user. The definition of "Significant" is entirely dependant on your business circumstances and risk

management model. It was also mentioned by Rino that tracing the actions of a specific user is fine but we

must also be able to ascertain that this specific user was responsible for the uninitiated action.

**QUESTION 121**

Which of the following best ensures accountability of users for actions taken within a system or domain?

A. ) Identification

B. ) Authentication

C. ) Authorization

D. ) Credentials

**Section:** (none)

**Explanation/Reference:**

"Identification is the process by which a subject professes an identify and accountability is initiated." Pg 149

Tittel: CISSP Study Guide

"Identification and authentication are the keystones of most access control systems. Identification is the act of

a user professing an identify to a system, usually in the form of a log-on ID to the system. Identification

establishes user accountability for the actions on the system. Authentication is verification that the user's

claimed identity is valid and is usually implemented through a user password at log-on time." Pg 36 Krutz: The

CISSP Prep Guide

**QUESTION 122**

Individual accountability does not include which of the following?

A. ) unique identifiers

B. ) policies & procedures

C. ) access rules

D. ) audit trails

**Section:** (none)