GNSA Q&As

GIAC Systems and Network Auditor

Pass GIAC GNSA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gnsa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

Which of the following commands will you use to watch a log file /var/adm/messages while the log file is updating continuously?

A. less -g /var/adm/messages

B. tail /var/adm/messages

C. cat /var/adm/messages

D. tail -f /var/adm/messages

Correct Answer: D

The tail command is used to display the last few lines of a text file or piped data. It has a special command line option -f (follow) that allows a file to be monitored. Instead of displaying the last few lines and exiting, tail displays the lines and then monitors the file. As new lines are added to the file by another process, tail updates the display. This is particularly useful for monitoring log files. The following command will display the last 10 lines of messages and append new lines to the display as new lines are added to messages: tail -f /var/adm/messages Answer: B is incorrect. The tail command will display the last 10 lines (default) of the log file. Answer: C is incorrect. The concatenate (cat) command is used to display or print the contents of a file. Syntax: cat filename For example, the following command will display the contents of the /var/log/dmesg file: cat /var/log/dmesg Note: The more command is used in conjunction with the cat command to prevent scrolling of the screen while displaying the contents of a file. Answer: A is incorrect. The less command is used to view (but not change) the contents of a text file, one screen at a time. It is similar to the more command. However, it has the extended capability of allowing both forward and backward navigation through the file. Unlike most Unix text editors/viewers, less does not need to read the entire file before starting; therefore, it has faster load times with large files. The command syntax of the less command is as follows: less [options] file_name Where,

QUESTION 2

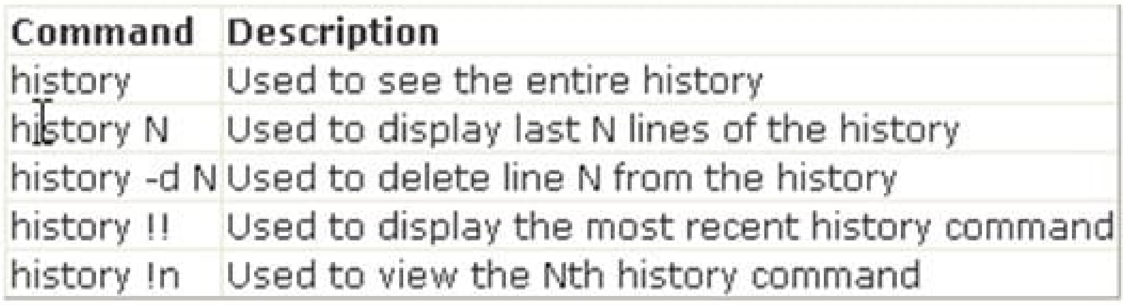
Fill in the blank with the appropriate command.

You want to search the most recent command that starts with the string \\'user\\'. For this, you will enter the ________ command to get the desired result.

A. history !user

Correct Answer: A

Here, you will use the history !user command to search the most recent command that starts with the string \\'user\\'. In the bash shell, the history command is used to view the recently executed commands. History is on by default. A user can turn off history using the command set +o history and turn it on using set -o history. An environment variable HISTSIZE is used to inform bash about how many history lines should be kept. The following commands are frequently used to view and manipulate history:



Command	Description
history	Used to see the entire history
history N	Used to display last N lines of the history
history -d N	Used to delete line N from the history
history !!	Used to display the most recent history command
history !n	Used to view the Nth history command

QUESTION 3

Which of the following statements about data integrity of a container are true? (Choose two)

A. It ensures that a hacker cannot alter the contents of an HTTP message while it is in transit from a container to a client.

B. Data integrity ensures that information is made available to users who are authorized to access it.

C. Data integrity ensures that information has not been modified by a third party while it is in transit.

D. It ensures that an eavesdropper cannot read an HTTP message being sent from a client to a container.

Correct Answer: AC

Data integrity ensures that information has not been modified, altered, or destroyed by a third party while it is in transit. Data integrity ensures that the data received is same as the data that was sent. Moreover, no one can tamper with the

data during transmission from source to destination.

It also ensures that a hacker cannot alter the contents of an HTTP message while it is in transit from the container to the client. This will be accomplished through the use of HTTPS. The HTTPS stands for Hypertext Transfer Protocol over

Secure Socket Layer. The HTTPS encrypts and decrypts the page requests and page information between the client browser and the Web server using a Secure Socket Layer.

Answer: D is incorrect. This answer option describes confidentiality.

Answer: B is incorrect. This answer option also describes confidentiality.

QUESTION 4

You work as a Network Auditor for XYZ CORP. The company has a Windows-based network. You use DumpSec as an auditing and reporting program for security issues.

Which of the following statements is true about DumpSec? (Choose three)

A. It obtains the DACLs for the registry.

B. It dumps user and group information.

C. It collates the DACLs for the file system.

D. It kills the running services in the Windows environment.

Correct Answer: ABC

DumpSec, a program launched by Somarsoft, is a security auditing and reporting program for Microsoft Windows. It collates and obtains the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers, and shares in

a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group, and replication information, policies, as well as services (Win32) and kernel drivers loaded on the system. It can also report

the current status of services (running or stopped) in the Windows environment.

Answer: D is incorrect. It cannot kill running services. It can only report the current status of services (running or stopped) in the Windows environment.

QUESTION 5

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to identify the secure terminals from where the root can be allowed to log in.

Which of the following Unix configuration files can you use to accomplish the task?

A. /etc/services

B. /etc/ioports

C. /proc/interrupts

D. /etc/securetty

Correct Answer: D

In Unix, the /etc/securetty file is used to identify the secure terminals from where the root can be allowed to log in.

Answer: B is incorrect. In Unix, the /etc/ioports fileshows which I/O ports are in use at the moment.

Answer: A is incorrect. In Unix, the /etc/services file is the configuration file that lists the network services that the system supports. Answer: C is incorrect. In Unix, the /proc/interrupts file is the configuration file that shows the interrupts in use

and how many of each there has been.