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.pass2lead.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

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.

QUESTION 2

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to impose some special access restrictions on users.

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

A. /var/run/utmp

B. /etc/terminfo

C. /etc/usertty

D. /etc/termcap

Correct Answer: C

In Unix, the /etc/usertty file is used to impose some special access restrictions on users.

Answer: B is incorrect. In Unix, the /etc/terminfo file contains the details for the terminal I/O.

Answer: A is incorrect. In Unix, the /var/run/utmp file is the configuration file that contains information about the currently logged in users. Mostly, the \\'Who\\' and \\'w\\' commands use this file.

Answer: D is incorrect. In Unix, the /etc/termcap file works as a terminal capability database.

QUESTION 3

You work as a Web Developer for XYZ CORP. The company has a Windows-based network. You have been assigned the task to secure the website of the company. To accomplish the task, you want to use a website monitoring service.

What are the tasks performed by a website monitoring service?

A. It checks the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network.

B. It checks SSL Certificate Expiry.

C. It checks HTTP pages.

D. It checks Domain Name Expiry.

Correct Answer: BCD

Website monitoring service can check HTTP pages, HTTPS, FTP, SMTP, POP3, IMAP, DNS, SSH, Telnet, SSL, TCP, PING, Domain Name Expiry, SSL Certificate Expiry, and a range of other ports with great variety of check intervals from every four hours to every one minute. Typically, most website monitoring services test a server anywhere between once-per hour to once-per-minute. Advanced services offer in-browser web transaction monitoring based on browser add-ons such as Selenium or iMacros. These services test a website by remotely controlling a large number of web browsers. Hence, it can also detect website issues such a JavaScript bugs that are browser specific. Answer: A is incorrect. This task is performed under network monitoring. Network tomography deals with monitoring the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network/ Internet.

QUESTION 4

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

A. Incontrovertible

B. Corroborating

C. Direct

D. Circumstantial

Correct Answer: D

Circumstantial evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person. Answer: B is incorrect. Corroborating evidence is evidence that tends to support a

proposition that is already supported by some evidence. Answer: A is incorrect. Incontrovertible evidence is a colloquial term for evidence introduced to prove a fact that is supposed to be so conclusive that there can be no other truth as to the

matter; evidence so strong, it overpowers contrary evidence, directing a fact-finder to a specific and certain conclusion.

Answer: C is incorrect. Direct evidence is testimony proof for any evidence, which expressly or straight-forwardly proves the existence of a fact.

QUESTION 5

Adam works as a Security Analyst for Umbrella Inc. He is retrieving large amount of log data from syslog servers and network devices such as Router and switches. He is facing difficulty in analyzing the logs that he has retrieved. To solve this problem, Adam decides to use software called Sawmill. Which of the following statements are true about Sawmill?

A. It incorporates real-time reporting and real-time alerting.

B. It is used to analyze any device or software package, which produces a log file such as Web servers, network devices (switches and routers etc.), syslog servers etc.

C. It is a software package for the statistical analysis and reporting of log files.

D. It comes only as a software package for user deployment.

Correct Answer: ABC

Sawmill is a software package for the statistical analysis and reporting of log files, with dynamic contextual filtering, \\'live\\' data zooming, user interface customization, and custom calculated reports. Sawmill incorporates real-time reporting and real-time alerting. Sawmill also includes a page tagging server and JavaScript page tag for the analysis of client side clicks (client requests) providing a total view of visitor traffic and on-site behavioral activity. Sawmill Analytics is offered in three forms, as a software package for user deployment, as a turnkey on-premise system appliance, and as a SaaS service. Sawmill analyzes any device or software package producing a log file and that includes Web servers, firewalls, proxy servers, mail servers, network devices (switches and routers etc.), syslog servers, databases etc. Its range of potential uses by knowledge workers is essentially limitless. Answer: D is incorrect. Sawmill Analytics software is available in three different forms; as a software package for user deployment, as a turnkey on-premise system appliance, and as a SaaS service.