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

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to find out when a particular user was last logged in. To accomplish this, you need to analyze the log configuration files.

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

A. /var/log/btmp

B. /var/log/messages

C. /var/log/lastlog

D. /var/log/wtmp

Correct Answer: C

In Unix, the /var/log/lastlog file is used by the finger to find when a user was last logged in.

Answer: D is incorrect. In Unix, the /var/log/wtmp file stores the binary info of users that have been logged on. Answer: A is incorrect. In Unix, the /var/log/btmp file is used to store information about failed logins.

Answer: B is incorrect. In Unix, the /var/log/messages is the main system message log file.

QUESTION 2

Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system.

Which of the following are the most likely threats to his computer? (Choose two)

A. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.

B. Attacker can use the Ping Flood DoS attack if WZC is used.

C. Attacker by creating a fake wireless network with high power antenna cause Victor\'s computer to associate with his network to gain access.

D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

Correct Answer: AC

Wireless Zero Configuration (WZC), also known as Wireless Auto Configuration, or WLAN AutoConfig is a wireless connection management utility included with Microsoft Windows XP and later operating systems as a service that dynamically selects a wireless network to connect to based on a user\'s preferences and various default settings. This can be used instead of, or in the absence of, a wireless network utility from the manufacturer of a computer\'s wireless networking device. The drivers for the wireless adapter query the NDIS Object IDs and pass the available network names to the service. WZC also introduce some security threats, which are as follows: WZC will probe for networks that are already connected. This information can be viewed by anyone using a wireless analyzer and can be used to set up fake access points to connect. WZC attempts to connect to the wireless network with the strongest signal. Attacker can create fake wireless networks with high- power antennas and cause computers to associate with his access point. Answer: D is incorrect. WZC does not interfere in the configuration of encryption and MAC filtering. Answer: B is

![Pass2Lead](https://Pass2Lead.com)
incorrect. In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping -f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs.

QUESTION 3

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to set some terminal characteristics and environment variables.

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

A. /etc/sysconfig/routed

B. /proc/net

C. /etc/sysconfig/network-scripts/ifcfg-interface

D. /etc/sysconfig/init

Correct Answer: D

In Unix, the /etc/sysconfig/init file is used to set terminal characteristics and environment variables.

Answer: B is incorrect. In Unix, the /proc/net file contains status information about the network protocols.

Answer: C is incorrect. In Unix, the /etc/sysconfig/network-scripts/ifcfg-interface file is the configuration file used to define a network interface.

Answer: A is incorrect. In Unix, the /etc/sysconfig/routed file is used to set up the dynamic routing policies.

QUESTION 4

Mark works as the Network Administrator for XYZ CORP. The company has a Unix-based network. Mark wants to scan one of the Unix systems to detect security vulnerabilities. To accomplish this, he uses TARA as a system scanner.

What can be the reasons that made Mark use TARA?

A. It has a very specific function of seeking paths to root.

B. It is composed mostly of bash scripts

C. It works on a wide variety of platforms.

D. It is very modular.

Correct Answer: BCD

Tiger Analytical Research Assistant (TARA) is a set of scripts that scans a Unix system for security problems. Following are the pros and cons of using TARA.

Pros:

It is open source.

It is very modular.

It can work on a wide variety of platforms.

It is composed mostly of bash scripts; hence, it can run on any Unix platform with little difficulty.

Cons:

It has a very specific function of seeking paths to root.

Answer: A is incorrect. It is a limitation of TARA that reduces its flexibility to be used for different purposes.

QUESTION 5

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He wants to break a dat a.txt file, 200MB in size, into two files in which the size of the first file named data.txt.aa should be 150MB and that of the second file named data.txt.ab should be 50MB. To accomplish his task and to further delete the data.txt file, he enters the following command: split --verbose -b 150m data.txt data.txt. ; rm -vf data.txt

Which of the following commands can John use to join the splitted files into a new data.txt file?

A. vi data.txt.* > data.txt

B. less data.txt.* > data.txt

C. vi data.txt.*

D. cat data.txt.* > data.txt

Correct Answer: D

The cat data.txt.* command will display both the splitted files, and the > command will redirect the output into a new data.txt file.

[Latest GNSA Dumps](#)   [GNSA PDF Dumps](#)   [GNSA VCE Dumps](#)