



GPPA^{Q&As}

GIAC Certified Perimeter Protection Analyst

Pass GIAC GPPA Exam with 100% Guarantee

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

<https://www.pass4itsure.com/gppa.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 are the Network Administrator and your company has recently implemented encryption for all emails. You want to check to make sure that the email packages are being encrypted.

What tool would you use to accomplish this?

- A. Password cracker
- B. Performance Monitor
- C. Packet sniffer
- D. Vulnerability analyzer

Correct Answer: C

QUESTION 2

Which of the following are the reasons that network administrators use Access Control Lists? Each correct answer represents a complete solution. (Choose two.)

- A. Removing weak user password
- B. Encrypting data to be routed
- C. Controlling VTY access into a router
- D. Filtering traffic as it passes through a router

Correct Answer: CD

QUESTION 3

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory-based single forest multiple domain IPv4 network. All the DNS servers on the network run Windows Server 2008. The users in the network use NetBIOS name to connect network application on the network. You have migrated the network to IPv6-enabled network. Now you want to enable DNS Server to perform lookups in GlobalNames Zone.

Which of the following commands will you use to accomplish the task?

- A. Dnscmd /config /enableglobalnames 1
- B. Dnscmd /config /globalnamesqueryorder 0
- C. Dnscmd /config /enableglobalnamesupport 1
- D. Dnscmd /config /enableglobalnamesupport 0

Correct Answer: C

**QUESTION 4**

An organization has a TCP/IP based network. It uses IPv6 addressing in its network. IPv6 tackles addressing and routing-table problems, and improves the protocol as well.

Which of the following statements is true about IPv6?

- A. It implements broadcasting.
- B. It eliminates the primary need for Network Address Translation (NAT).
- C. It uses symmetric key encryption.
- D. Its address is 32 bits in length.

Correct Answer: B

QUESTION 5

You work as a Network Administrator for NetTech Inc. Your manager needs to access a particular server on the network from outside the company network. You have a registered IP address assigned to a router on the company network.

Which of the following will be useful for accessing the server from outside the network?

- A. Overloading
- B. Switch
- C. Static NAT
- D. Dynamic VLAN

Correct Answer: C

QUESTION 6

Sam works as a Network Administrator for Gentech Inc. He has been assigned a project to develop the rules that define the IDP policy in the rulebase.

Which of the following will he define as the components of the IDP policy rule?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. IDP Profiler
- B. IDP rule notifications
- C. IDP rule IP actions
- D. IDP appliance deployment mode



Correct Answer: BC

QUESTION 7

You work as a Network Administrator for Net World Inc. You have configured a few routers on the company\\'s network. You are required to accomplish the following goals:

-

Encrypt all service passwords immediately.

-

Ensure that encryption is also applied on the passwords changed in the future.

You run the following command service password-encryption.

Which of the goals will this action accomplish?

A.

The action will accomplish neither of the goals.

B.

The action will encrypt all passwords immediately.

C.

The action will accomplish both the goals.

D.

The action will ensure that encryption is also applied on the passwords changed in the future.

Correct Answer: C

QUESTION 8

Which of the following types of firewall functions by creating two different communications, one between the client and the firewall, and the other between the firewall and the end server?

A. Stateful firewall

B. Proxy-based firewall

C. Endian firewall

D. Packet filter firewall

Correct Answer: B

**QUESTION 9**

In which of the following IDS evasion techniques does an attacker deliver data in multiple small sized packets, which makes it very difficult for an IDS to detect the attack signatures of such attacks?

- A. Insertion
- B. Fragmentation overlap
- C. Fragmentation overwrite
- D. Session splicing

Correct Answer: D

QUESTION 10

What is the easiest way to verify that name resolution is functioning properly on a TCP/IP network?

- A. Use the TRACERT command with the /pingname parameter.
- B. Ping the source host with its IP address.
- C. Ping the source host with its computer name.
- D. Check the IP statistics on the file server.

Correct Answer: C

QUESTION 11

Jain works as a Security Manager for ABC Inc. The company has a Windows-based network.

Jain has been assigned a project to detect the services used by an attack to access the network. For this purpose, he is required to use the predefined service objects of the rulebase. This predefined service object defines the services used in the attack to access the network.

Which of the following objects will he create when he finds that the attack is not defined in the predefined service objects?

- A. Custom service objects
- B. Compound attack objects
- C. Signature attack objects
- D. Protocol anomaly attack objects

Correct Answer: A

QUESTION 12



Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform a user must install a packet capture library.

What is the name of this library?

- A. SysPCap
- B. libpcap
- C. WinPCap
- D. PCAP

Correct Answer: C

QUESTION 13

Which of the following has a set of system-independent functions for packet capture and network analysis?

- A. WinDump
- B. WinPcap
- C. libpcap
- D. tcpdump

Correct Answer: C

QUESTION 14

In which of the following situations does legal and authorized traffic cause an intrusion detection system (IDS) to generate an alert and slow down performance?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. False alert
- B. False positives
- C. False generation
- D. False illusion

Correct Answer: AB

QUESTION 15

Which of the following intrusion detection systems (IDS) produces the false alarm because of the abnormal behavior of users and network?



- A. Host-based intrusion detection system (HIDS)
- B. Protocol-based intrusion detection system (PIDS)
- C. Network intrusion detection system (NIDS)
- D. Application protocol-based intrusion detection system (APIDS)

Correct Answer: A

[GPPA PDF Dumps](#)

[GPPA VCE Dumps](#)

[GPPA Study Guide](#)