GCED Q&As

GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

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

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

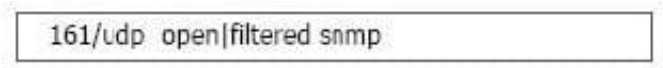
100% Passing Guarantee
100% Money Back Assurance

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

When running a Nmap UDP scan, what would the following output indicate?



A. The port may be open on the system or blocked by a firewall

B. The router in front of the host accepted the request and sent a reply

C. An ICMP unreachable message was received indicating an open port

D. An ACK was received in response to the initial probe packet

Correct Answer: A

Explanation: When Nmap shows an "open filtered" response for the scan results, this indicates a couple of different reasons. The port could be open but a firewall could be blocking the use ACK flags; only TCP

packets do.

QUESTION 2

What would be the output of the following Google search? filetype:doc inurl:ws_ftp

A. Websites running ws_ftp that allow anonymous logins

B. Documents available on the ws_ftp.com domain

C. Websites hosting the ws_ftp installation program

D. Documents found on sites with ws_ftp in the web address

Correct Answer: D

QUESTION 3

Why would the pass action be used in a Snort configuration file?

A. The pass action simplifies some filtering by specifying what to ignore.

B. The pass action passes the packet onto further rules for immediate analysis.

C. The pass action serves as a placeholder in the snort configuration file for future rule updates.

D. Using the pass action allows a packet to be passed to an external process.

E. The pass action increases the number of false positives, better testing the rules.

Correct Answer: A

Explanation: The pass action is defined because it is sometimes easier to specify the class of data to ignore rather than the data you want to see. This can cut down the number of false positives and help keep down the size of log data. False positives occur because rules failed and indicated a threat that is really not one. They should be minimized whenever possible. The pass action causes the packet to be ignored, not passed on further. It is an active command, not a placeholder.

QUESTION 4

What is the BEST sequence of steps to remove a bot from a system?

A. Terminate the process, remove autoloading traces, delete any malicious files

B. Delete any malicious files, remove autoloading traces, terminate the process

C. Remove autoloading traces, delete any malicious files, terminate the process

D. Delete any malicious files, terminate the process, remove autoloading traces

Correct Answer: A

QUESTION 5

What is the most common read-only SNMP community string usually called?

A. private

B. mib

C. open

D. public

Correct Answer: D

QUESTION 6

From a security perspective, how should the Root Bridge be determined in a Spanning Tree Protocol (STP) environment?

A. Manually selected and defined by the network architect or engineer.

B. Defined by selecting the highest Bridge ID to be the root bridge.

C. Automatically selected by the Spanning Tree Protocol (STP).

D. All switch interfaces become root bridges in an STP environment.

Correct Answer: B

QUESTION 7

Which of the following is an SNMPv3 security feature that was not provided by earlier versions of the protocol?

A. Authentication based on RSA key pairs

B. The ability to change default community strings

C. AES encryption for SNMP network traffic

D. The ability to send SNMP traffic over TCP ports

Correct Answer: C

QUESTION 8

The creation of a filesystem timeline is associated with which objective?

A. Forensic analysis

B. First response

C. Access control

D. Incident eradication

Correct Answer: A

QUESTION 9

What feature of Wireshark allows the analysis of one HTTP conversation?

A. Follow UDP Stream

B. Follow TCP Stream

C. Conversation list > IPV4

D. Setting a display filter to `tcp\\'

Correct Answer: B

Explanation: Follow TCP Stream is a feature of Wireshark that allows the analysis of a single TCP conversation between two hosts over multiple packets. Filtering packets using tcp in the filter box will return all TCP packets, not grouping by a single TCP conversation. HTTP is TCP not UDP, so you cannot follow a HTTP stream over UDP.

QUESTION 10

Why might an administrator not be able to delete a file using the Windows del command without specifying additional

command line switches?

A. Because it has the read-only attribute set

B. Because it is encrypted

C. Because it has the nodel attribute set

D. Because it is an executable file

Correct Answer: A

QUESTION 11

An internal host at IP address 10.10.50.100 is suspected to be communicating with a command and control whenever a user launches browser window. What features and settings of Wireshark should be used to isolate and analyze this network traffic?

A. Filter traffic using ip.src = = 10.10.50.100 and tcp.srcport = = 80, and use Expert Info

B. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 53, and use Expert Info

C. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 80, and use Follow TCP stream

D. Filter traffic using ip.src = = 10.10.50.100, and use Follow TCP stream

Correct Answer: C

QUESTION 12

What would the output of the following command help an incident handler determine? cscript manage-bde . wsf –status

A. Whether scripts can be run from the command line

B. Which processes are running on the system

C. When the most recent system reboot occurred

D. Whether the drive has encryption enabled

Correct Answer: D

QUESTION 13

Who is ultimately responsible for approving methods and controls that will reduce any potential risk to an organization?

A. Senior Management

B. Data Owner

C. Data Custodian

D. Security Auditor

Correct Answer: D

QUESTION 14

Which of the following is the best way to establish and verify the integrity of a file before copying it during an investigation?

A. Write down the file size of the file before and after copying and ensure they match

B. Ensure that the MAC times are identical before and after copying the file

C. Establish the chain of custody with the system description to prove it is the same image

D. Create hash of the file before and after copying the image verifying they are identical

Correct Answer: D

QUESTION 15

Which type of attack could be used to obtain IOS router configuration files without a valid user password?

A. ARP cache poisoning

B. CDP sniffing

C. SNMP man in the middle

D. TFTP brute force

Correct Answer: D

Explanation: TFTP is a protocol to transfer files and commonly used with routers for configuration files, IOS images, and more. It requires no authentication. To download a file you need only know (or guess) its name. CDP, SNMP and ARP are not used for accessing or transferring IOS configuration files.