



Vendor: GIAC

Exam Code: GCED

Exam Name: GIAC Certified Enterprise Defender

Version: DEMO

QUESTION 1

At the start of an investigation on a Windows system, the lead handler executes the following commands after inserting a USB drive. What is the purpose of this command?

```
C:\ >dir / s / a dhsra d:\ > a: \ IRCD.txt
```

- A. To create a file on the USB drive that contains a listing of the C: drive
- B. To show hidden and archived files on the C: drive and copy them to the USB drive
- C. To copy a forensic image of the local C: drive onto the USB drive
- D. To compare a list of known good hashes on the USB drive to files on the local C: drive

Answer: C

Explanation:

This command will create a text file on the collection media (in this case you would probably be using a USB flash drive) named IRCD.txt that should contain a recursive directory listing of all files on the desk.

QUESTION 2

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

Answer: A

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.

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

On which layer of the OSI Reference Model does the FWSnort utility function?

- A. Physical Layer

- B. Data Link Layer
- C. Transport Layer
- D. Session Layer
- E. Application Layer

Answer: C

Explanation:

The FWSnort utility functions as a transport layer inline IPS.

QUESTION 5

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'

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 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.

Answer: B

QUESTION 7

Which tasks would a First Responder perform during the Identification phase of Incident Response?

- A. Verify the root cause of the incident and apply any missing security patches.
- B. Install or reenable host-based firewalls and anti-virus software on suspected systems.
- C. Search for sources of data and information that may be valuable in confirming and containing an incident.
- D. Disconnect network communications and search for malicious executables or processes.

Answer: C

QUESTION 8

What should happen before acquiring a bit-for-bit copy of suspect media during incident

response?

- A. Encrypt the original media to protect the data
- B. Create a one-way hash of the original media
- C. Decompress files on the original media
- D. Decrypt the original media

Answer: B

QUESTION 9

How does the Cisco IOS IP Source Guard feature help prevent spoofing attacks?

- A. Filters traffic based on IP address once a DHCP address has been assigned
- B. Prevents unauthorized MAC addresses from receiving an IP address on the network
- C. Blocks unsolicited ARP packets after a client has received an IP address
- D. Rate limits client traffic to prevent CAM table flooding

Answer: A

QUESTION 10

Which control would BEST help detect a potential insider threat?

- A. Mandatory approval process for executive and administrative access requests.
- B. Providing the same access to all employees and monitoring sensitive file access.
- C. Multiple scheduled log reviews of all employee access levels throughout the year
- D. Requiring more than one employee to be trained on each task or job duty.

Answer: A

QUESTION 11

How would an attacker use the following configuration settings?

```
interface Tunnel0
ip address 192.168.55.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 192.17.250.2
```

- A. A client based HIDS evasion attack
- B. A firewall based DDoS attack
- C. A router based MITM attack
- D. A switch based VLAN hopping attack

Answer: C

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



10% Discount Coupon Code: ASTR14