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.leads4pass.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

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

Correct Answer: C

QUESTION 2

Of the following pieces of digital evidence, which would be collected FIRST from a live system involved in an incident?

A. Event logs from a central repository

B. Directory listing of system files

C. Media in the CDrom drive

D. Swap space and page files

Correct Answer: D

Explanation: Best practices suggest that live response should follow the order of volatility, which means that you want to collect data which is changing the most rapidly. The order of volatility is: Memory Swap or page file Network status and current / recent network connections Running processes Open files

QUESTION 3

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 4

If a Cisco router is configured with the "service config" configuration statement, which of the following tools could be used by an attacker to apply a new router configuration?

A. TFTPD

B. Hydra

C. Ettercap

D. Yersinia

Correct Answer: A

QUESTION 5

What piece of information would be recorded by the first responder as part of the initial System Description?

A. Copies of log files

B. System serial number

C. List of system directories

D. Hash of each hard drive

Correct Answer: B

QUESTION 6

Network administrators are often hesitant to patch the operating systems on CISCO router and switch operating systems, due to the possibility of causing network instability, mainly because of which of the following?

A. Having to rebuild all ACLs

B. Having to replace the kernel

C. Having to re-IP the device

D. Having to rebuild ARP tables

E. Having to rebuild the routing tables

Correct Answer: B

Explanation: Many administrators are hesitant to upgrade the IOS on routers based on past experience with the code introducing instability into the network. It is often difficult to completely test an IOS software upgrade in a production environment because the monolithic kernel requires that the IOS be replaced before the device can be tested. Because

of these reasons, IOS upgrades to resolve security flaws are often left undone in many organizations.

QUESTION 7

Following a Digital Forensics investigation, which of the following should be included in the final forensics report?

A. An executive summary that includes a list of all forensic procedures performed.

B. A summary of the verified facts of the incident and the analyst\\'s unverified opinions.

C. A summary of the incident and recommended disciplinary actions to apply internally.

D. An executive summary that includes high level descriptions of the overall findings.

Correct Answer: D

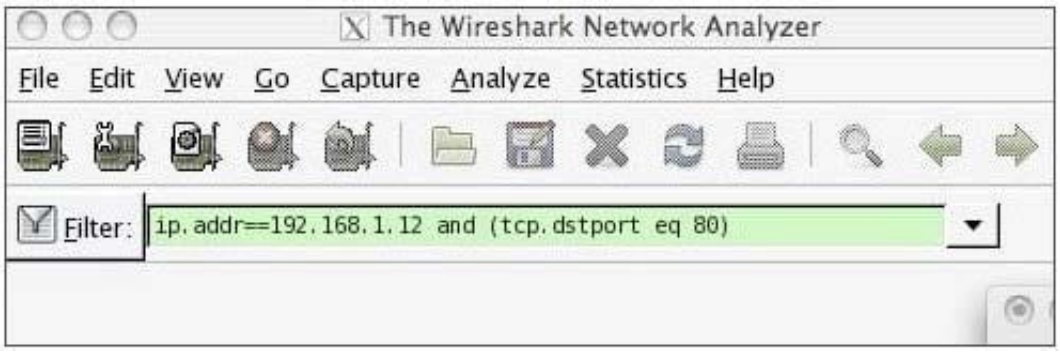
Explanation: A professional forensic report should include an executive summary, including a description of the incident and the overall findings.

The written report needs to be factually accurate and free from speculation or bias, meaning that an analyst\\'s unverified or unsubstantiated opinions should not be included in the report. Beyond the executive summary, the detailed report should include a description of the data preserved, a detailed explanation of the procedures performed, and a summary of the facts. Disciplinary action, if needed, would be addressed

through other channels and not included in the forensic analyst\\'s report.

QUESTION 8

What information would the Wireshark filter in the screenshot list within the display window?



A. Only HTTP traffic to or from IP address 192.168.1.12 that is also destined for port 80

B. Only traffic to or from IP address 192.168.1.12 and destined for port 80 C. Only traffic with a source address of 192.168.1.12 to or from port 80

D. Only traffic with a destination address of 192.168.1.12 to or from port 80

Correct Answer: B

QUESTION 9

Monitoring the transmission of data across the network using a man-in-the-middle attack presents a threat against which type of data?

A. At-rest

B. In-transit

C. Public

D. Encrypted

Correct Answer: B

QUESTION 10

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 11

Enabling port security prevents which of the following?

A. Using vendors other than Cisco for switching equipment as they don\\'t offer port security

B. Spoofed MAC addresses from being used to cause a Denial of Service condition

C. Legitimate MAC addresses from being used to cause a Denial of Service condition

D. Network Access Control systems from functioning properly

Correct Answer: C

QUESTION 12

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

A. private

B. mib

C. open

D. public

Correct Answer: D

QUESTION 13

Requiring criminal and financial background checks for new employees is an example of what type of security control?

A. Detective Support Control

B. Detective Operational Control

C. Detective Technical Control

D. Detective Management Control

Correct Answer: D

Explanation: Management Controls include: Policies, guidelines, checklists, and reporting.

Detective management controls include personnel security. As a detective control, we are referring to

indepth background investigations, clearances, and rotation of duties.

QUESTION 14

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 15

You have been tasked with searching for Alternate Data Streams on the following collection of Windows partitions; 2GB FAT16, 6GB FAT32, and 4GB NTFS. How many total Gigabytes and partitions will you need to search?

A. 4GBs of data, the NTFS partition only.

B. 12GBs of data, the FAT16, FAT32, and NTFS partitions.

C. 6GBs of data, the FAT32 partition only.

D. 10GBs of data, both the FAT32 and NTFS partitions.

Correct Answer: C