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

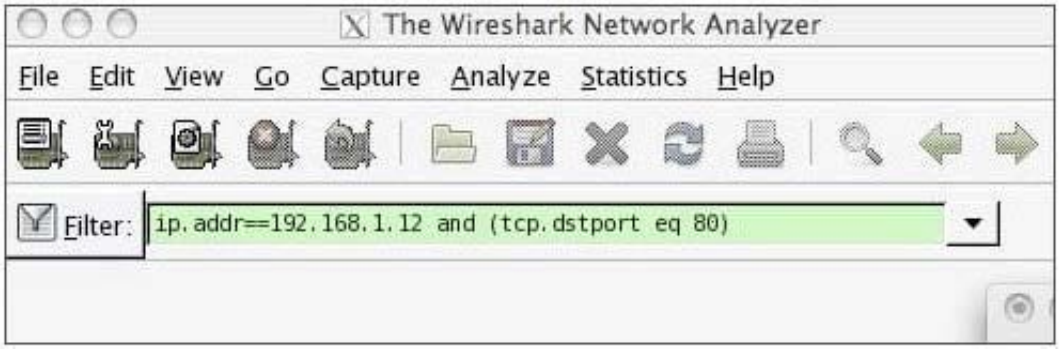
100% Passing Guarantee
100% Money Back Assurance

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

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 2

Which of the following tools is the most capable for removing the unwanted add-on in the screenshot below?

A. ProcessExplorer

B. Taskkill

C. Paros

D. Hijack This

Correct Answer: B

QUESTION 3

Which of the following is an operational security control that is used as a prevention mechanism?

A. Labeling of assets

B. Heat detectors

C. Vibration alarms

D. Voltage regulators

Correct Answer: A

Explanation: The following are considered operational security prevention controls: Security gates, guards, and dogs; Heating, ventilation, and air conditioning (HVAC); Fire suppressant; Labeling of assets (classification and responsible agents); Off-site storage (recovery); Safes and locks. The other distractors are considered operational security detection controls.

QUESTION 4

Which of the following would be included in a router configuration standard?

A. Names of employees with access rights

B. Access list naming conventions

C. Most recent audit results

D. Passwords for management access

Correct Answer: B

QUESTION 5

An incident response team investigated a database breach, and determined it was likely the result of an internal user who had a default password in place. The password was changed. A week later, they discover another loss of database records. The database admin provides logs that indicate the attack came from the front-end web interface. Where did the incident response team fail?

A. They did not eradicate tools left behind by the attacker

B. They did not properly identify the source of the breach

C. They did not lock the account after changing the password

D. They did not patch the database server after the event

Correct Answer: D