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

Which could be described as a Threat Vector?

A. A web server left6 unpatched and vulnerable to XSS

B. A coding error allowing remote code execution

C. A botnet that has infiltrated perimeter defenses

D. A wireless network left open for anonymous use

Correct Answer: A

A threat vector is the method (crafted packet) that would be used to exercise a vulnerability (fragmentation to bypass IDS signature). An unpatched web server that is susceptible to XSS simply describes a vulnerability (unpatched) paired with a specific threat (XSS) and does not touch on the method to activate the threat. Similarly, the coding error that allows remote code execution is simply describing the pairing of a vulnerability with a threat, respectively. The botnet is an unspecified threat; there is no indication of how the threat was activated (or it\\'s intention/capabilities; the threat).

QUESTION 2

Which type of media should the IR team be handling as they seek to understand the root cause of an incident?

A. Restored media from full backup of the infected host

B. Media from the infected host, copied to the dedicated IR host

C. Original media from the infected host

D. Bit-for-bit image from the infected host

Correct Answer: A

Explanation: By imaging the media with tools such as dd or Ghost and analyzing the copy, you preserve the original media for later analysis so that the results can be recreated by another competent examiner if necessary.

QUESTION 3

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 4

When an IDS system looks for a pattern indicating a known worm, what type of detection method is it using?

A. Signature-based

B. Anomaly-based

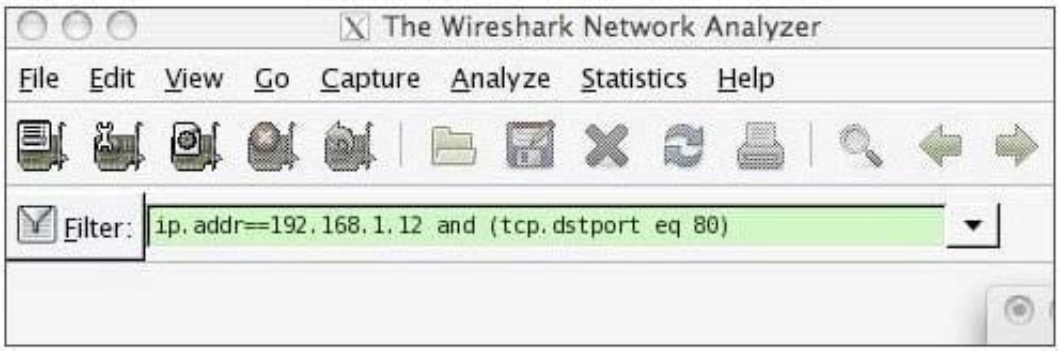
C. Statistical

D. Monitored

Correct Answer: A

QUESTION 5

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