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.geekcert.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

In an 802.1x deployment, which of the following would typically be considered a Supplicant?

A. A network switch

B. A perimeter firewall

C. A RADIUS server

D. A client laptop

Correct Answer: D

QUESTION 2

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 3

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

Correct Answer: C

Explanation: The FWSnort utility functions as a transport layer inline IPS.

QUESTION 4

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.

QUESTION 5

Which of the following applies to newer versions of IOS that decrease their attack surface?

A. Telnet cannot be enabled or used

B. The Cisco Discovery Protocol has been removed

C. More services are disabled by default

D. Two-factor authentication is default required

Correct Answer: C

Explanation: Recent versions of IOS have less services enabled by default, older versions vary but generally have more services (even those not needed) enabled by default; this increases the attack surface on the device.