# 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**

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

Correct Answer: A

**QUESTION 2**

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 3**

How does an Nmap connect scan work?

A. It sends a SYN, waits for a SYN/ACK, then sends a RST.

B. It sends a SYN, waits for a ACK, then sends a RST.

C. It sends a SYN, waits for a ACK, then sends a SYN/ACK.

D. It sends a SYN, waits for a SYN/ACK, then sends a ACK

Correct Answer: A

Explanation: An Nmap connect scan sends a SYN, waits for a SYN/ACK, then sends a ACK to complete the three-way handshake. A Nmap half-open scan sends a SYN, waits for a SYN/ACK, then sends a RST.

**QUESTION 4**

A company classifies data using document footers, labeling each file with security labels "Public", "Pattern", or "Company Proprietary". A new policy forbids sending "Company Proprietary" files via email. Which control could help security analysis identify breaches of this policy?

A. Monitoring failed authentications on a central logging device

B. Enforcing TLS encryption for outbound email with attachments

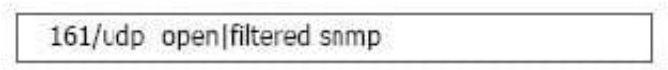
C. Blocking email attachments that match the hashes of the company\\'s classification templates

D. Running custom keyword scans on outbound SMTP traffic from the mail server

Correct Answer: D

**QUESTION 5**

When running a Nmap UDP scan, what would the following output indicate?




A. The port may be open on the system or blocked by a firewall

B. The router in front of the host accepted the request and sent a reply

C. An ICMP unreachable message was received indicating an open port

D. An ACK was received in response to the initial probe packet

Correct Answer: A

Explanation: When Nmap shows an "open filtered" response for the scan results, this indicates a couple of different reasons. The port could be open but a firewall could be blocking the use ACK flags; only TCP

packets do.