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

The security team wants to detect connections that can compromise credentials by sending them in plaintext across the wire. Which of the following rules should they enable on their IDS sensor?

A. alert tcp any 22 any 22 (msg:SSH connection; class type:misc-attack;sid: 122:rev:1;)

B. alert tcp any any any 6000: (msg:X-Windows session; flow:from_server,established;nocase;classtype:misc-attack;sid:101;rev:1;)

C. alert tcp any 23 any 23 (msg:Telnet shell; class type:misc-attack;sid:100; rev:1;)

D. alert udp any any any 5060 (msg:VOIP message; classtype:misc-attack;sid:113; rev:2;)

Correct Answer: C

QUESTION 2

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 3

How does data classification help protect against data loss?

A. DLP systems require classification in order to protect data

B. Data at rest is easier to protect than data in transit

C. Digital watermarks can be applied to sensitive data

D. Resources and controls can be appropriately allocated

Correct Answer: A

QUESTION 4

A compromised router is reconfigured by an attacker to redirect SMTP email traffic to the attacker\\'s server before sending packets on to their intended destinations. Which IP header value would help expose anomalies in the path outbound SMTP/Port 25 traffic takes compared to outbound packets sent to other ports?

A. Checksum

B. Acknowledgement number

C. Time to live

D. Fragment offset

Correct Answer: C

Explanation: In a case study of a redirect tunnel set up on a router, some anomalies were noticed while watching network traffic with the TCPdump packet sniffer. Packets going to port 25 (Simple Mail Transfer Protocol [SMTP] used by mail servers and other Mail Transfer Agents [MTAs] to send and receive e-mail) were apparently taking a different network path. The TLs were consistently three less than other destination ports, indicating another three network hops were taken.

Other IP header values listed, such as fragment offset. The acknowledgement number is a TCP, not IP, header field.

QUESTION 5

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.