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

A security device processes the first packet from 10.62.34.12 destined to 10.23.10.7 and recognizes a malicious anomaly. The first packet makes it to 10.23.10.7 before the security devices sends a TCP RST to 10.62.34.12. What type of security device is this?

A. Host IDS

B. Active response

C. Intrusion prevention

D. Network access control

Correct Answer: B

An active response device dynamically reconfigures or alters network or system access controls, session streams, or individual packets based on triggers from packet inspection and other detection devices. Active response happens after the event has occurred, thus a single packet attack will be successful on the first attempt and blocked in future attempts. Network intrusion prevention devices are typically inline devices on the network that inspect packets and make decisions before forwarding them on to the destination. This type of device has the capability to defend against single packet attacks on the first attempt by blocking or modifying the attack inline.

QUESTION 2

An internal host at IP address 10.10.50.100 is suspected to be communicating with a command and control whenever a user launches browser window. What features and settings of Wireshark should be used to isolate and analyze this network traffic?

A. Filter traffic using ip.src = = 10.10.50.100 and tcp.srcport = = 80, and use Expert Info

B. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 53, and use Expert Info

C. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 80, and use Follow TCP stream

D. Filter traffic using ip.src = = 10.10.50.100, and use Follow TCP stream

Correct Answer: C

QUESTION 3

Which of the following attacks would use ".." notation as part of a web request to access restricted files and directories, and possibly execute code on the web server?

A. URL directory

B. HTTP header attack

C. SQL injection

D. IDS evasion

E. Cross site scripting

Correct Answer: A

QUESTION 4

What would the output of the following command help an incident handler determine? cscript manage-bde . wsf –status

A. Whether scripts can be run from the command line

B. Which processes are running on the system

C. When the most recent system reboot occurred

D. Whether the drive has encryption enabled

Correct Answer: D

QUESTION 5

An outside vulnerability assessment reveals that users have been routinely accessing Gmail from work for over a year, a clear violation of this organization\\'s security policy. The users report "it just started working one day". Later, a network administrator admits he meant to unblock Gmail for just his own IP address, but he made a mistake in the firewall rule.

Which security control failed?

A. Access control

B. Authentication

C. Auditing

D. Rights management

Correct Answer: C

Explanation: Audits are used to identify irregular activity in logged (after-the-fact) records. If this activity went unnoticed or uncorrected for over a year, the internal audits failed because they were either incomplete or inaccurate. Authentication, access control and managing user rights would not apply as a network admin could be expected to have the ability to configure firewall rules.