EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : **GCED**

Title : GIAC Certified Enterprise Defender

Version : DEMO

1.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
Answer: A

2.Why would an incident handler acquire memory on a system being investigated?
A. To determine whether a malicious DLL has been injected into an application
B. To identify whether a program is set to auto-run through a registry hook
C. To list which services are installed on they system
D. To verify which user accounts have root or admin privileges on the system
Answer: C

3.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
Answer: A
Explanation:
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).

4.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
Answer: B
Explanation:
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.

5.Which tool uses a Snort rules file for input and by design triggers Snort alerts?
A. snot
B. stick
C. Nidsbench
D. ftester
Answer: C