DUMPSBOSS.COM

GIAC Certified Enterprise Defender

GIAC GCED

Version Demo

Total Demo Questions: 10

Total Premium Questions: 88

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

QUESTION NO: 1

The creation of a filesystem timeline is associated with which objective?

A. Forensic analysis

B. First response

C. Access control

D. Incident eradication

ANSWER: A

QUESTION NO: 2

Which of the following is an outcome of the initial triage during incident response?

A. Removal of unnecessary accounts from compromised systems

B. Segmentation of the network to protect critical assets

C. Resetting registry keys that vary from the baseline configuration

D. Determining whether encryption is in use on in scope systems

ANSWER: B

QUESTION NO: 3

Monitoring the transmission of data across the network using a man-in-the-middle attack presents a threat against which type of data?

A. At-rest

B. In-transit

C. Public

D. Encrypted

ANSWER: B

QUESTION NO: 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.

QUESTION NO: 5

You are responding to an incident involving a Windows server on your company's network. During the investigation you notice that the system downloaded and installed two files, iexplorer.exe and iexplorer.sys. Based on the behavior of the system you suspect that these files are part of a rootkit. If this is the case what is the likely purpose of the .sys file?

A. It is a configuration file used to open a backdoor

B. It is a logfile used to collect usernames and passwords

C. It is a device driver used to load the rootkit

D. It is an executable used to configure a keylogger

ANSWER: C

QUESTION NO: 6

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

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.

QUESTION NO: 7

From a security perspective, how should the Root Bridge be determined in a Spanning Tree Protocol (STP) environment?

A. Manually selected and defined by the network architect or engineer.

B. Defined by selecting the highest Bridge ID to be the root bridge.

C. Automatically selected by the Spanning Tree Protocol (STP).

D. All switch interfaces become root bridges in an STP environment.

ANSWER: B

QUESTION NO: 8

Which tasks would a First Responder perform during the Identification phase of Incident Response?

A. Verify the root cause of the incident and apply any missing security patches.

B. Install or reenable host-based firewalls and anti-virus software on suspected systems.

C. Search for sources of data and information that may be valuable in confirming and containing an incident.

D. Disconnect network communications and search for malicious executables or processes.

ANSWER: C

QUESTION NO: 9

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

ANSWER: D

QUESTION NO: 10

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

ANSWER: D