Demo Questions

GIAC GCED Exam

GIAC Certified Enterprise Defender

Thank you for downloading GCED Exam PDF

Question #1 ***Topic 1***

Which type of media should the IR team be handling as they seek to understand the root cause of an incident?

- A. Restored media from full backup of the infected host
- B. Media from the infected host, copied to the dedicated IR host
- C. Original media from the infected host
- D. Bit-for-bit image from the infected host

Correct Answer: *A*

By imaging the media with tools such as dd or Ghost and analyzing the copy, you preserve the original media for later analysis so that the results can be recreated by another competent examiner if necessary.

Question #2 ***Topic 1***

An incident response team is handling a worm infection among their user workstations. They created an IPS signature to detect and block worm activity on the border IPS, then removed the worms artifacts or workstations triggering the rule. Despite this action, worm activity continued for days after. Where did the incident response team fail?

- A. The team did not adequately apply lessons learned from the incident
- B. The custom rule did not detect all infected workstations
- C. They did not receive timely notification of the security event
- D. The team did not understand the worm's propagation method

Correct Answer: *B*

Identifying and scoping an incident during triage is important to successfully handling a security incident. The detection methods used by the team didnt detect all the infected workstations.

Question #3_Topic 1_

A legacy server on the network was breached through an OS vulnerability with no patch available. The server is used only rarely by employees across several business units. The theft of information from the server goes unnoticed until the company is notified by a third party that sensitive information has been posted on the Internet. Which control was the first to fail?

- A. Security awareness
- B. Access control
- C. Data classification
- D. Incident response

Correct Answer: *C*

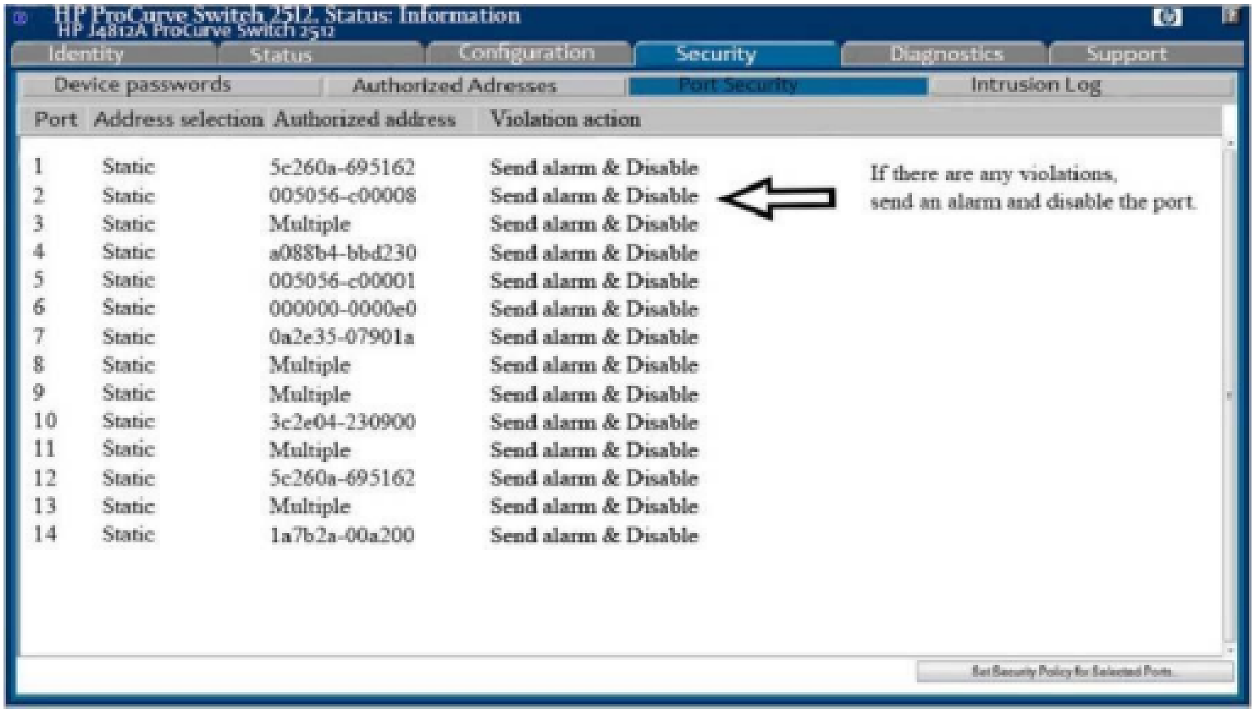
The legacy system was not properly classified or assigned an owner. It is critical that an organization identifies and classifies information so proper controls and measures should be put in place. The ultimate goal of data classification is to make sure that all information is properly protected at the correct level.

This was not a failure of incident response, access control or security

awareness training.

Question #4*Topic 1*

Analyze the screenshot below. Which of the following attacks can be mitigated by these configuration settings?



Port	Address selection	Authorized address	Violation action
1	Static	5c260a-695162	Send alarm & Disable
2	Static	005056-c00008	Send alarm & Disable
3	Static	Multiple	Send alarm & Disable
4	Static	a088b4-bbd230	Send alarm & Disable
5	Static	005056-c00001	Send alarm & Disable
6	Static	000000-0000e0	Send alarm & Disable
7	Static	0a2e35-07901a	Send alarm & Disable
8	Static	Multiple	Send alarm & Disable
9	Static	Multiple	Send alarm & Disable
10	Static	3c2e04-230900	Send alarm & Disable
11	Static	Multiple	Send alarm & Disable
12	Static	5c260a-695162	Send alarm & Disable
13	Static	Multiple	Send alarm & Disable
14	Static	1a7b2a-00a200	Send alarm & Disable

If there are any violations, send an alarm and disable the port.

- A. A Denial-of-Service attack using network broadcasts
- B. A Replay attack
- C. An IP masquerading attack
- D. A MAC Flood attack

Correct Answer: *D*

Both BPDU Guard and Root Guard are used to prevent a new switch from becoming the Root Bridge. They are very similar but use different mechanisms.

Rootguard allows devices to use STP, but if they send superior BDPUs (i.e. they attempt to become the Root Bridge), Root Guard disables the port until the offending BPDUs cease. Recovery is automatic.

If Portfast is enabled on a port, BPDU Guard will disable the port if a BPDU is received. The port stays disabled until it is manually re-enabled. Devices behind such ports cannot use STP, as the port would be disabled as soon as they send BPDUs (which is the default behavior of switches).

Question #5*Topic 1*

Of the following pieces of digital evidence, which would be collected FIRST from a live system involved in an incident?

- A. Event logs from a central repository
- B. Directory listing of system files
- C. Media in the CDrom drive
- [✓ D. Swap space and page files]

Correct Answer: *D*

Best practices suggest that live response should follow the order of volatility, which means that you want to collect data which is changing the most rapidly. The order of volatility is:

Memory -

Swap or page file -

Network status and current / recent network connections

Running processes -

Open files