GCED$^{\text{Q\&As}}$

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.passapply.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

Which of the following is a major problem that attackers often encounter when attempting to develop or use a kernel mode rootkit?

A. Their effectiveness depends on the specific applications used on the target system.

B. They tend to corrupt the kernel of the target system, causing it to crash.

C. They are unstable and are easy to identify after installation

D. They are highly dependent on the target OS.

Correct Answer: B

QUESTION 2

Who is ultimately responsible for approving methods and controls that will reduce any potential risk to an organization?

A. Senior Management

B. Data Owner

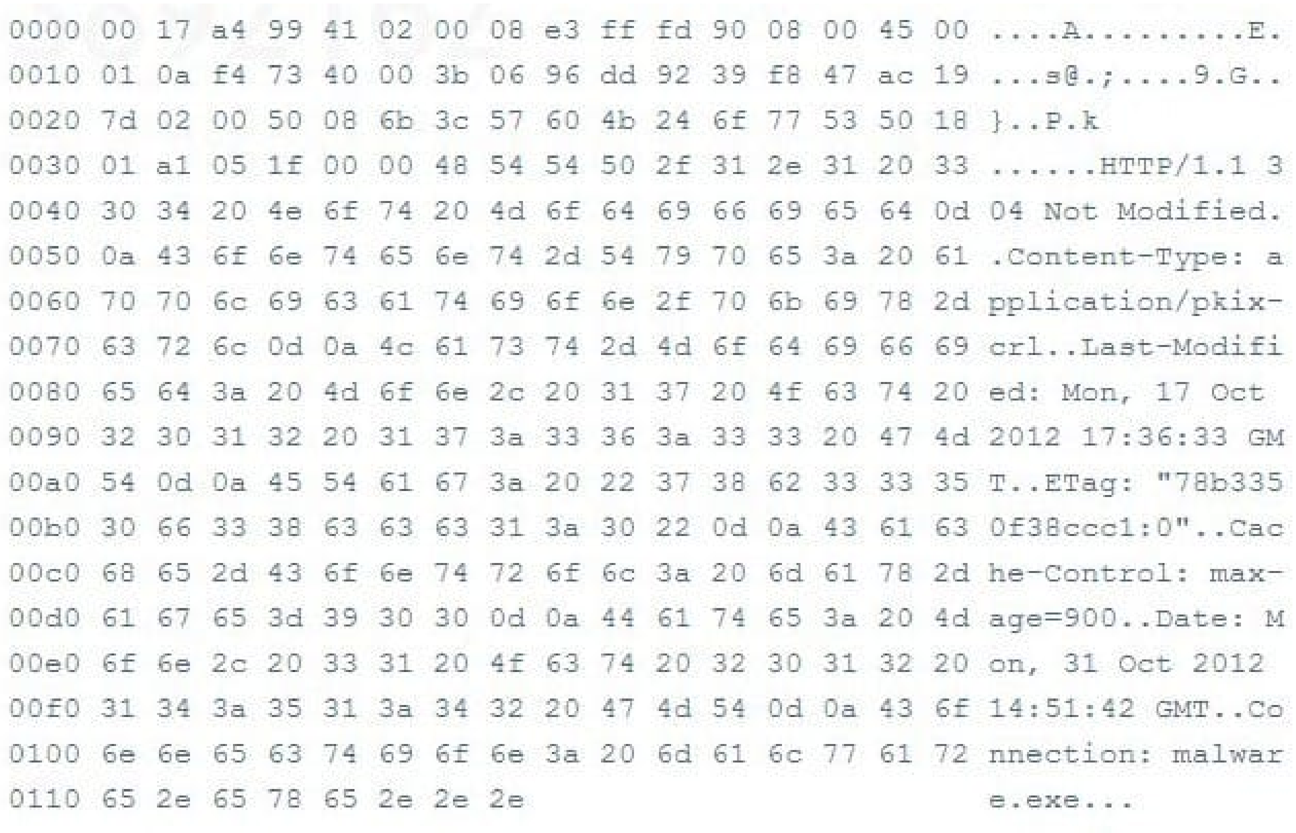
C. Data Custodian

D. Security Auditor

Correct Answer: D

QUESTION 3

Although the packet listed below contained malware, it freely passed through a layer 3 switch. Why didn\\'t the switch detect the malware in this packet?



```
0000 00 17 a4 99 41 02 00 08 e3 ff fd 90 08 00 45 00 ....A.........E.
0010 01 0a f4 73 40 00 3b 06 96 dd 92 39 f8 47 ac 19 ...s@.;....9.G..
0020 7d 02 00 50 08 6b 3c 57 60 4b 24 6f 77 53 50 18 }..P.k
0030 01 a1 05 1f 00 00 48 54 54 50 2f 31 2e 31 20 33 ......HTTP/1.1 3
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not Modified.
0050 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 .Content-Type: a
0060 70 70 6c 69 63 61 74 69 6f 6e 2f 70 6b 69 78 2d pplication/pkix-
0070 63 72 6c 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 crl..Last-Modifi
0080 65 64 3a 20 4d 6f 6e 2c 20 31 37 20 4f 63 74 20 ed: Mon, 17 Oct
0090 32 30 31 32 20 31 37 3a 33 36 3a 33 33 20 47 4d 2012 17:36:33 GM
00a0 54 0d 0a 45 54 61 67 3a 20 22 37 38 62 33 33 35 T..ETag: "78b335
00b0 30 66 33 38 63 63 63 31 3a 30 22 0d 0a 43 61 63 0f38ccc1:0"..Cac
00c0 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d he-Control: max-
00d0 61 67 65 3d 39 30 30 0d 0a 44 61 74 65 3a 20 4d age=900..Date: M
00e0 6f 6e 2c 20 33 31 20 4f 63 74 20 32 30 31 32 20 on, 31 Oct 2012
00f0 31 34 3a 35 31 3a 34 32 20 47 4d 54 0d 0a 43 6f 14:51:42 GMT..Co
0100 6e 6e 65 63 74 69 6f 6e 3a 20 6d 61 6c 77 61 72 nnection: malwar
0110 65 2e 65 78 65 2e 2e 2e                         e.exe...
```

A. The packet was part of a fragmentation attack

B. The data portion of the packet was encrypted

C. The entire packet was corrupted by the malware

D. It didn\\'t look deeply enough into the packet

Correct Answer: D

Explanation: Routers, layer 3 switches, some firewalls, and other gateways are packet filtering devices that use access control lists (ACLs) and perform packet inspection. This type of device uses a small subset of the packet to make filtering decisions, such as source and destination IP address and protocol. These devices will then allow or deny protocols based on their associated ports. This type of packet inspection and access control is still highly susceptible to malicious attacks, because payloads and other areas of the packet are not being inspected. For example, application level attacks that are tunneled over open ports such as HTTP (port 80) and HTTPS (port 443).

QUESTION 4

Which tool keeps a backup of all deleted items, so that they can be restored later if need be?

A. ListDLLs

B. Yersinia

C. Ettercap

D. ProcessExplorer

E. Hijack This

Correct Answer: E

Explanation: After selecting "fix it!" with Hijack This you can always restore deleted items, because Hijack This keeps a backup of them.

QUESTION 5

What piece of information would be recorded by the first responder as part of the initial System Description?

A. Copies of log files

B. System serial number

C. List of system directories

D. Hash of each hard drive

Correct Answer: B