GCED$^{Q\&As}$

GIAC Certified Enterprise Defender Practice Test

QUESTION 1

Michael, a software engineer, added a module to a banking customer\\'s code. The new module deposits small amounts of money into his personal bank account. Michael has access to edit the code, but only code reviewers have the ability to commit modules to production. The code reviewers have a backlog of work, and are often willing to trust the software developers\\' testing and confidence in the code.

Which technique is Michael most likely to engage to implement the malicious code?

A. Denial of Service

B. Race Condition

C. Phishing

D. Social Engineering

Correct Answer: C

QUESTION 2

Which type of attack could be used to obtain IOS router configuration files without a valid user password?

A. ARP cache poisoning

B. CDP sniffing

C. SNMP man in the middle

D. TFTP brute force

Correct Answer: D

Explanation: TFTP is a protocol to transfer files and commonly used with routers for configuration files, IOS images, and more. It requires no authentication. To download a file you need only know (or guess) its name. CDP, SNMP and ARP are not used for accessing or transferring IOS configuration files.

QUESTION 3

Which statement below is the MOST accurate about insider threat controls?

A. Classification of information assets helps identify data to protect.

B. Security awareness programs have a minimal impact on reducing the insider threat.

C. Both detective and preventative controls prevent insider attacks.

D. Rotation of duties makes an insider threat more likely.

E. Separation of duties encourages one employee to control a great deal of information.

Correct Answer: A

A company needs to classify its information as a key step in valuing it and knowing where to focus its protection. Rotation of duties and separation of duties are both key elements in reducing the scope of information access and the ability to conceal malicious behavior. Separation of duties helps minimize "empire building" within a company, keeping one individual from controlling a great deal of information, reducing the insider threat. Security awareness programs can help other employees notice the signs of an insider attack and thus reduce the insider threat. Detection is a reactive method and only occurs after an attack occurs. Only preventative methods can stop or limit an attack.

QUESTION 4

Requiring background checks for employees who access protected data is an example of which type of data loss control?

A. Mitigation

B. Prevention

C. Monitoring

D. Identification

Correct Answer: B

Explanation: Once sensitive data is identified and classified, preventive measures can be taken. Among these are software-based controls, such as auditing and access control, as well as human controls such as background checks, psychological examinations, and such.

QUESTION 5

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

Correct Answer: B

QUESTION 6

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 7

When attempting to collect data from a suspected system compromise, which of the following should generally be collected first?

A. The network connections and open ports

B. The contents of physical memory

C. The current routing table

D. A list of the running services

Correct Answer: B

QUESTION 8

Which tool uses a Snort rules file for input and by design triggers Snort alerts?

A. snot

B. stick

C. Nidsbench

D. ftester

Correct Answer: C

QUESTION 9

At the start of an investigation on a Windows system, the lead handler executes the following commands after inserting a USB drive. What is the purpose of this command? C:\ >dir / s / a dhsra d: \ > a: \ IRCD.txt

A. To create a file on the USB drive that contains a listing of the C: drive

B. To show hidden and archived files on the C: drive and copy them to the USB drive

C. To copy a forensic image of the local C: drive onto the USB drive

D. To compare a list of known good hashes on the USB drive to files on the local C: drive

Correct Answer: C

Explanation: This command will create a text file on the collection media (in this case you would probably be using a USB flash drive) named IRCD.txt that should contain a recursive directory listing of all files on the desk.

QUESTION 10

How does data classification help protect against data loss?

A. DLP systems require classification in order to protect data

B. Data at rest is easier to protect than data in transit

C. Digital watermarks can be applied to sensitive data

D. Resources and controls can be appropriately allocated

Correct Answer: A

QUESTION 11

Which of the following would be used in order to restrict software form performing unauthorized operations, such as invalid access to memory or invalid calls to system access?

A. Perimeter Control

B. User Control

C. Application Control

D. Protocol Control

E. Network Control

Correct Answer: C

QUESTION 12

In order to determine if network traffic adheres to expected usage and complies with technical standards, an organization would use a device that provides which functionality?

A. Stateful packet filtering

B. Signature matching

C. Protocol anomaly detection

D. CRC checking

E. Forward error correction

Correct Answer: C

Explanation: In addition to standards compliance, Protocol Anomaly Detection determines whether data within the protocol adheres to expected usage. Even if a communication stream complies with a protocol standard, the way in which the protocol is being used may be inconsistent with what is expected. Perimeter devices that perform protocol anomaly detection contain in-depth knowledge of protocol standards and expected usage and are able to detect traffic that does not comply with those guidelines.

QUESTION 13

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

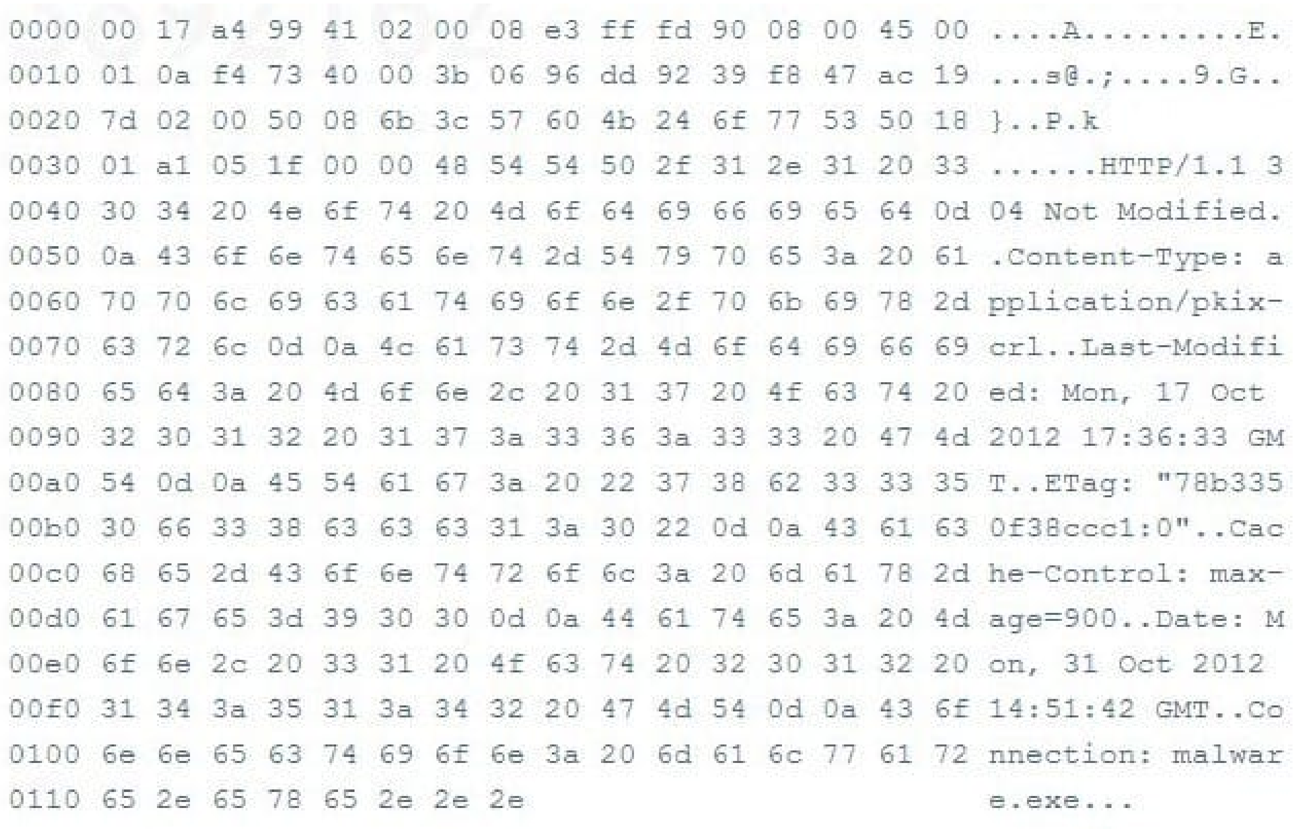
C. Statistical

D. Monitored

Correct Answer: A

QUESTION 14

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 15

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