Vendor:GIAC

Exam Code:GCED

Exam Name:GIAC Certified Enterprise Defender Practice Test

Version: Demo

QUESTION 1

Why would a Cisco network device with the latest updates and patches have the service config setting enabled, making the device vulnerable to the TFTP Server Attack?

A. Disabling telnet enables the setting on the network device.

B. This setting is enabled by default in the current Cisco IOS.

C. Allowing remote administration using SSH under the Cisco IOS also enables the setting.

D. An attack by Cisco Global Exploiter will automatically enable the setting.

E. This older default IOS setting was inherited from an older configuration despite the upgrade.

Correct Answer: B

Explanation: Enabling the service config setting causes a Cisco router to be vulnerable to the TFTP Server Attack since it will actively try to retrieve a new configuration file from the nearest TFTP server. An attacker can insert a malicious update file in this process to compromise the Cisco router.

The service config setting was disabled by default in the Cisco IOS in version 12.0, but had been enabled by default in the 11.x series of the IOS trains. This feature is often enabled in later versions since organizations don\\'t always realize the risk of this setting and will leave it enabled as the migrate through multiple IOS upgrades.

The other items listed don\\'t enable the service config setting.

QUESTION 2

What is the most common read-only SNMP community string usually called?

A. private

B. mib

C. open

D. public

Correct Answer: D

QUESTION 3

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 4

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.

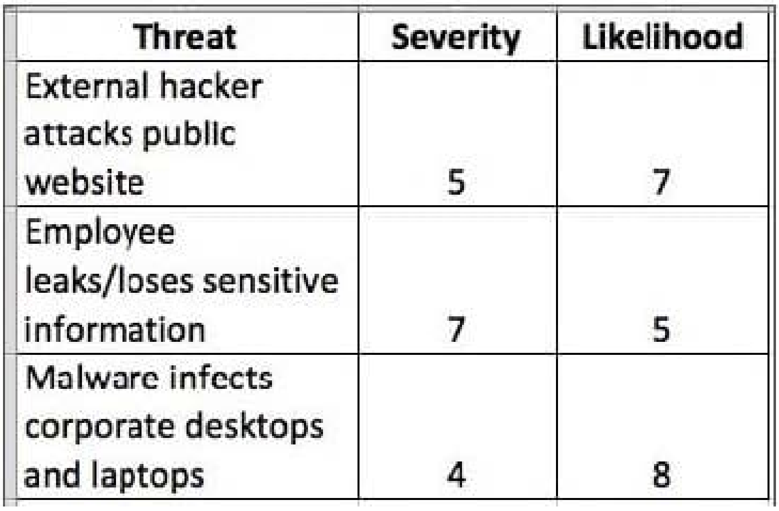
C. Automatically selected by the Spanning Tree Protocol (STP).

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

Correct Answer: B

QUESTION 5

The matrix in the screen shot below would be created during which process?



Threat	Severity	Likelihood
External hacker attacks public website	5	7
Employee leaks/loses sensitive information	7	5
Malware infects corporate desktops and laptops	4	8

A. Risk Assessment

B. System Hardening

C. Data Classification

D. Vulnerability Scanning

Correct Answer: A

QUESTION 6

Network administrators are often hesitant to patch the operating systems on CISCO router and switch operating systems, due to the possibility of causing network instability, mainly because of which of the following?

A. Having to rebuild all ACLs

B. Having to replace the kernel

C. Having to re-IP the device

D. Having to rebuild ARP tables

E. Having to rebuild the routing tables

Correct Answer: B

Explanation: Many administrators are hesitant to upgrade the IOS on routers based on past experience with the code introducing instability into the network. It is often difficult to completely test an IOS software upgrade in a production environment because the monolithic kernel requires that the IOS be replaced before the device can be tested. Because of these reasons, IOS upgrades to resolve security flaws are often left undone in many organizations.

QUESTION 7

Which Windows CLI tool can identify the command-line options being passed to a program at startup?

A. netstat

B. attrib

C. WMIC

D. Tasklist

Correct Answer: C

QUESTION 8

Which command is the Best choice for creating a forensic backup of a Linux system?

A. Run form a bootable CD: tar cvzf image.tgz /

B. Run from compromised operating system: tar cvzf image.tgz /

C. Run from compromised operating system: dd if=/ dev/hda1 of=/mnt/backup/hda1.img

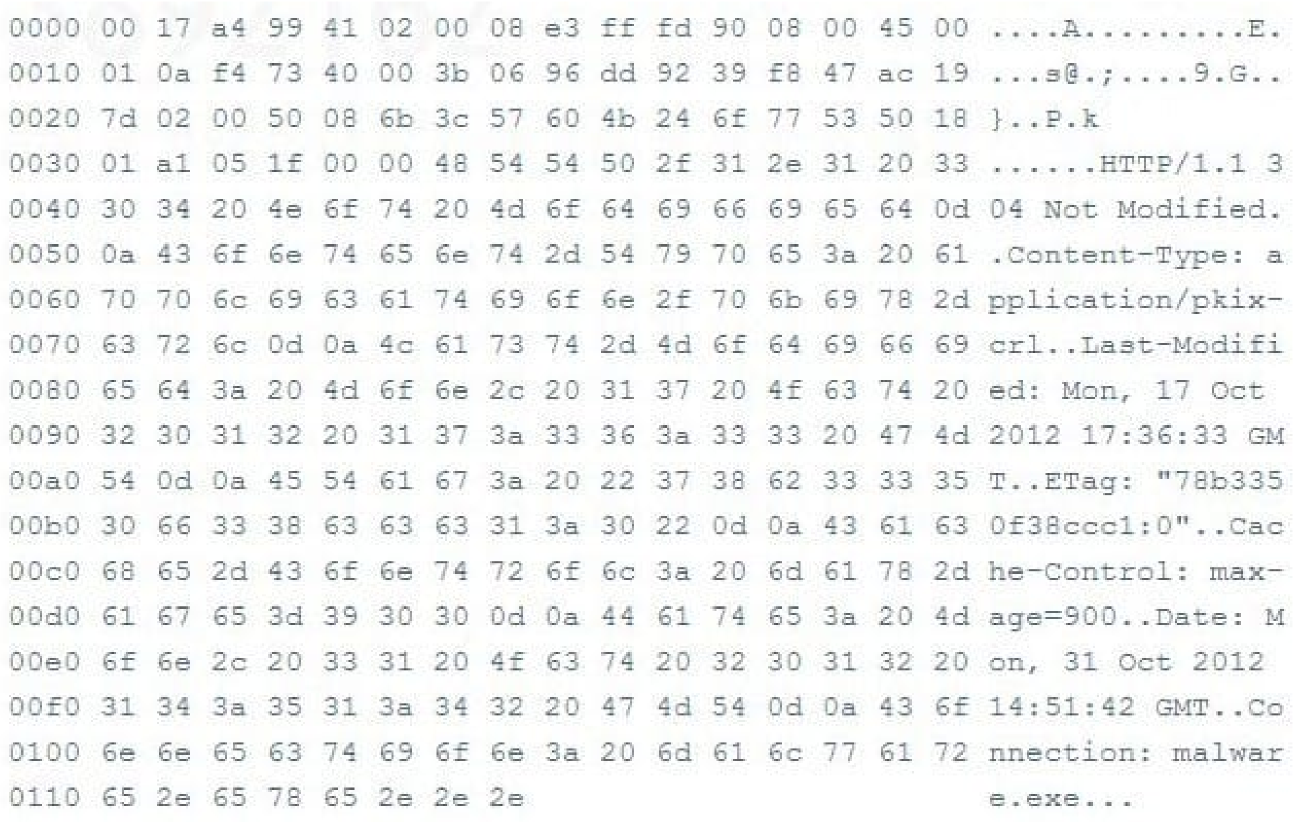
D. Run from a bootable CD: dd if=/dev/hda1 of=/mnt/backup/hda1.img

Correct Answer: D

Explanation: Using dd from a bootable CD is the only forensically sound method of creating an image. Using tar does not capture slack space on the disk. Running any command from a compromised operating system will raise integrity issues.

QUESTION 9

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 10

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 11

An incident response team investigated a database breach, and determined it was likely the result of an internal user who had a default password in place. The password was changed. A week later, they discover another loss of database records. The database admin provides logs that indicate the attack came from the front-end web interface. Where did the incident response team fail?

A. They did not eradicate tools left behind by the attacker

B. They did not properly identify the source of the breach

C. They did not lock the account after changing the password

D. They did not patch the database server after the event

Correct Answer: D

QUESTION 12

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.