# Free Questions for CS0-002

## Shared by Hughes on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

Question Type: MultipleChoice

An analyst needs to provide recommendations based on a recent vulnerability scan:

| Plug-in name | Family |
|---|---|
| SMB use domain SID to enumerate users | Windows : User management |
| SYN scanner | Port scanners |
| SSL certificate cannot be trusted | General |
| Scan not performed with admin privileges | Settings |

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?

## Options:

A- SMB use domain SID to enumerate users
B- SYN scanner
C- SSL certificate cannot be trusted
D- Scan not performed with admin privileges

## Answer:

D

## Explanation:

This should be addressed to ensure potential vulnerabilities are identified because it indicates that the vulnerability scan was not able to access some resources or perform some actions that require higher privileges on the target system. This could result in missing or inaccurate findings, as some vulnerabilities may not be detected or verified.

# Question 2

Question Type: MultipleChoice

During a risk assessment, a senior manager inquires about what the cost would be if a unique occurrence would impact the availability of a critical service. The service generates $1 ,000 in

revenue for the organization. The impact of the attack would affect 20% of the server's capacity to perform jobs. The organization expects that five out of twenty attacks would succeed during the year. Which of the following is the calculated single loss expectancy?

## Options:

A- $200
B- $800
C- $5,000
D- $20,000

## Answer:

A

## Explanation:

The single loss expectancy (SLE) is a measure of the monetary loss associated with a single occurrence of a risk. The SLE can be calculated by multiplying the asset value (AV) by the exposure factor (EF), which is the percentage of loss that the asset would suffer if the risk occurred. In this case, the asset value is the revenue generated by the service, which is $1,000. The exposure factor is the impact of the attack on the server's capacity, which is 20%.Therefore, the SLE is $1,000 x 0.2 = $2001.

# Question 3

Question Type: MultipleChoice

A security analyst scans the company's external IP range and receives the following results from one of the hosts:

| Port: | Protocol: | State: |
|---|---|---|
| 17 | tcp/udp | close |
| 21 | udp | close |
| 22 | tcp | open |
| 25 | tcp | close |
| 23 | udp | close |
| 53 | udp | open |
| 80 | tcp/udp | close |
| 139 | tcp | close |
| 389 | tcp | close |
| 443 | tcp | close |
| 3389 | tcp | close |
| 8080 | tcp/udp | close |
| 8443 | tcp/udp | close |

Which of the following best represents the security concern?

## Options:

A- A remote communications port is exposed.
B- The FTP port should be using TCP only.
C- Microsoft RDP is accepting connections on TCP.
D- The company's DNS server is exposed to everyone.

A A remote communications port is exposed is not correct. A remote communications port is a generic term for any port that allows remote access or communication with a host. There are many types of remote communications ports, such as SSH, Telnet, FTP, or RDP, and each one has its own security implications. The results do not specify which remote communications port is exposed, so this answer is too vague and inaccurate.

B The FTP port should be using TCP only is not correct. FTP stands for File Transfer Protocol, and it is a protocol that allows users to transfer files between hosts. FTP uses TCP ports 20 and 21 by default, and these ports are closed on the host according to the results.However, FTP can also use UDP ports 20 and 21 for data transfer in some cases, such as when using passive mode or extended passive mode2. Therefore, it is not true that FTP should be using TCP only, and this answer does not represent a security concern.

D) The company's DNS server is exposed to everyone is not correct. DNS stands for Domain Name System, and it is a system that translates domain names into IP addresses. DNS uses UDP port 53 by default, and this port is open on the host according to the results. This indicates that the host is providing DNS services to anyone on the internet, which may or may not be a security concern depending on the configuration and purpose of the host. For example, if the host is a

public DNS server that is intended to serve DNS queries from anyone, then this answer does not represent a security concern. However, if the host is a private DNS server that is meant to serve DNS queries only from authorized users or devices, then this answer could represent a security concern.
1:What Is Remote Desktop Protocol (RDP)?2:FTP - File Transfer Protocol: [What Is Domain Name System (DNS)?]

## Answer:

C

## Explanation:

The correct answer is C. Microsoft RDP is accepting connections on TCP. Microsoft RDP stands for Microsoft Remote Desktop Protocol, and it is a protocol that allows users to remotely access and control a Windows computer or server. RDP uses TCP port 3389 by default, and this port is open on the host according to the results. This indicates that the host is allowing RDP connections from anyone on the internet, which poses a security concern.An attacker could exploit vulnerabilities in RDP or use brute force attacks to gain unauthorized access to the host and compromise its data or resources1.

# Question 4

Question Type: MultipleChoice

During a routine security review, anomalous traffic from 9.9.9.9 was observed accessing a web server in the corporate perimeter network. The server is mission critical and must remain accessible around the world to serve web content. The Chief Information Security Officer has directed that improper traffic must be restricted. The following output is from the web server:

```
netstat -an

Active Connections
Proto          Local address      Foreign address      State
TCP            0.0.0.0:135        0.0.0.0:0            LISTENING
TCP            0.0.0.0:445        0.0.0.0:0            LISTENING
TCP            0.0.0.0:80         0.0.0.0:0            LISTENING
TCP            0.0.0.0:443        0.0.0.0:0            LISTENING
TCP            10.0.1.5:445       9.9.9.9:44251        ESTABLISHED
TCP            10.0.1.5.443       9.9.9.9:44252        ESTABLISHED
TCP            10.0.1.5:135       10.0.1.20:53243      ESTABLISHED
```

Which of the following is the best method to accomplish this task?

## Options:

A- Adjusting the IDS to block anomalous activity
B- Implementing port security
C- Adding 9.9.9.9 to the blocklist
D- Adjusting the firewall

## Answer:

D

## Explanation:

Based on the output of the ''netstat -an'' command, it seems that the web server is listening on port 80 for HTTP traffic and port 443 for HTTPS traffic. The anomalous traffic from 9.9.9.9 is accessing the web server on port 443, which means it is using a secure connection.

The best method to accomplish the task of restricting improper traffic from 9.9.9.9 isD. Adjusting the firewall. A firewall is a device or software that controls the flow of network traffic based on predefined rules. By adjusting the firewall rules, you can block or allow specific IP addresses, ports, protocols, or domains from accessing your web server.

# Question 5

Question Type: MultipleChoice

A security analyst is reviewing the following DNS logs as part of security-monitoring activities:

FROM 192.168.1.20 A www.google.com 67.43.45.22

FROM 192.168.1.20 AAAA www.google.com 2006:67:AD:1FAB::102

FROM 192.168.1.43 A www.mail.com 193.56.221.99

FROM 192.168.1.2 A www.company.com 241.23.22.11

FROM 192.168.1.211 A www.uewiryfajfchfaerwfj.co 32.56.32.122

FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53

FROM 192.168.1.93 ARAA www.nbc.com 2002:10:976::1

FROM 192.168.1.78 A www.comptia.org 122.10.31.87

Which of the following most likely occurred?

## Options:

A- The attack used an algorithm to generate command and control information dynamically.
B- The attack attempted to contact www.google.com to verify internet connectivity.
C- The attack used encryption to obfuscate the payload and bypass detection by an IDS.
D- The attack caused an internal host to connect to a command and control server.

## Answer:

A

## Explanation:

This is a technique that is commonly used by malware to evade detection and blocking by security tools. The malware generates random domain names that are used to communicate with the command and control server, which can change its IP address frequently. The domain names are usually long and nonsensical, such as www.uewiryfajfchfaerwfj.co in the log.The malware uses a predefined algorithm or a seed value to generate the same domain names as the server, so that they can find each other on the internet12.

# Question 6

Question Type: MultipleChoice

A security analyst is reviewing a new Internet portal that will be used for corporate employees to obtain their pay statements. Corporate policy classifies pay statement information as confidential, and it must be protected by MF

## Options:

A- Which of the following would best fulfill the MFA requirement while keeping the portal accessible from the internet?
A- Obtaining home public IP addresses of corporate employees to implement source IP restrictions and requiring a username and password
B- Requiring the internet portal to be accessible from only the corporate SSO internet endpoint and requiring a smart card and PIN
C- Moving the internet portal server to a DMZ that is only accessible from the corporate VPN and requiring a username and password
D- Distributing a shared password that must be provided before the internet portal loads and requiring a username and password

## Answer:

B

## Explanation:

Requiring the internet portal to be accessible from only the corporate SSO internet endpoint and requiring a smart card and PIN. This option provides the best MFA requirement because it uses two factors of authentication: something you have (smart card) and something you know (PIN). It also restricts access to the portal from a trusted source (corporate SSO internet endpoint).

# Question 7

Question Type: MultipleChoice

An organization is performing a risk assessment to prioritize resources for mitigation and remediation based on impact. Which of the following metrics, in addition to the CVSS for each CVE, would best enable the organization to prioritize its efforts?

## Options:

A- OS type

B- OS or application versions
C- Patch availability
D- System architecture
E- Mission criticality

## Answer:

C

## Explanation:

A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect an organization's assets, operations, or objectives.A risk assessment matrix is a tool that can help prioritize the risks based on their likelihood and impact1.

The CVSS (Common Vulnerability Scoring System) is a standard framework for rating the severity of vulnerabilities in software systems.The CVSS provides a numerical score from 0 to 10, as well as a qualitative rating from Low to Critical, based on the characteristics and consequences of the vulnerability2.

However, the CVSS score alone may not be sufficient to determine the priority of mitigation and remediation actions for each vulnerability. Other factors that may influence the decision include:

Patch availability: This metric indicates whether there is a fix or update available for the vulnerability from the vendor or developer. Patch availability can affect the urgency and feasibility of remediation, as well as the risk exposure and potential damage of exploitation.For example, a vulnerability with a high CVSS score but with a readily available patch may be less critical than a vulnerability with a lower CVSS score but with no patch available3.

Mission criticality: This metric reflects the importance and value of the asset or system affected by the vulnerability to the organization's mission, goals, or functions. Mission criticality can affect the impact and priority of remediation, as well as the risk tolerance and acceptance level of the organization.For example, a vulnerability with a high CVSS score but affecting a non-essential system may be less critical than a vulnerability with a lower CVSS score but affecting a core system4.

OS type: This metric indicates the operating system (OS) of the asset or system affected by the vulnerability. OS type can affect the likelihood and complexity of exploitation, as well as the availability and compatibility of patches or mitigations.For example, a vulnerability with a high CVSS score but affecting an uncommon or unsupported OS may be less critical than a vulnerability with a lower CVSS score but affecting a widely used or supported OS3.

OS or application versions: This metric indicates the specific version of the OS or application affected by the vulnerability. OS or application versions can affect the applicability and relevance of the vulnerability, as well as the availability and compatibility of patches or mitigations.For

example, a vulnerability with a high CVSS score but affecting an outdated or obsolete version may be less critical than a vulnerability with a lower CVSS score but affecting a current or popular version3.

System architecture: This metric indicates the design and configuration of the asset or system affected by the vulnerability. System architecture can affect the exposure and accessibility of the vulnerability, as well as the effectiveness and efficiency of patches or mitigations.For example, a vulnerability with a high CVSS score but affecting an isolated or segmented system may be less critical than a vulnerability with a lower CVSS score but affecting an interconnected or integrated system3.

Therefore, to best enable the organization to prioritize its efforts based on impact, patch availability is one of the most important metrics to consider in addition to the CVSS score for each CVE (Common Vulnerabilities and Exposures). Patch availability can directly influence the risk level and remediation strategy for each vulnerability.

# Question 8

Question Type: MultipleChoice

A company is required to monitor for unauthorized changes to baselines on all assets to comply with industry regulations. Two of the remote units did not recover after scans were performed on the assets. An analyst needs to recommend a solution to prevent recurrence. Which of the following is the best way to satisfy the regulatory requirement without impacting the availability to similar assets and creating an unsustainable process?

## Options:

A- Manually review the baselines daily and document the results in a change history log
B- Document exceptions with compensating controls to demonstrate the risk mitigation efforts.
C- Implement a new scanning technology to satisfy the monitoring requirement and train the team.
D- Purchase new remote units from other vendors with a proven ability to support scanning requirements.

A) Manually review the baselines daily and document the results in a change history log is not correct. This option would not prevent the recurrence of the problem, as it does not address the root cause of why the remote units did not recover after scans were performed. Moreover, this option would create an unsustainable process, as it would require a lot of time and resources to manually review and document the baselines of all assets on a daily basis.
C) Implement a new scanning technology to satisfy the monitoring requirement and train the team is not correct. This option would not guarantee that the problem would not recur, as it is possible that the new scanning technology would also cause issues with the remote units or other

assets. Furthermore, this option would incur additional costs and efforts to acquire, deploy, and maintain the new scanning technology and train the team on how to use it.
D) Purchase new remote units from other vendors with a proven ability to support scanning requirements is not correct. This option would not be feasible or cost-effective, as it would require replacing all the remote units with new ones from different vendors. This option would also introduce new risks and challenges, such as compatibility, interoperability, or vendor lock-in.

### Answer:

B

### Explanation:

The correct answer is B. Document exceptions with compensating controls to demonstrate the risk mitigation efforts. Compensating controls are alternative or additional controls that are implemented when the primary or required controls are not feasible or effective.Compensating controls can help to reduce the risk to an acceptable level and satisfy the regulatory requirements, as long as they are documented and justified1.

## Question 9

Question Type: MultipleChoice

Which of the following is the best method to ensure secure boot UEFI features are enabled to prevent boot malware?

### Options:

A- Enable secure boot in the hardware and reload the operating system.
B- Reconfigure the system's MBR and enable NTFS.
C- Set I-JEFI to legacy mode and enable security features.
D- Convert the legacy partition table to UEFI and repair the operating system.
B) Reconfigure the system's MBR and enable NTFS is not correct. MBR stands for Master Boot Record, and it is a legacy partitioning scheme that stores information about the partitions and the boot loader on a disk. NTFS stands for New Technology File System, and it is a file system that supports features such as encryption, compression, and access control. Reconfiguring the system's MBR and enabling NTFS would not enable secure boot UEFI features, as they are not related to UEFI or secure boot.Moreover, MBR is incompatible with UEFI, as UEFI requires a different partitioning scheme called GPT (GUID Partition Table)3.
C) Set UEFI to legacy mode and enable security features is not correct. Legacy mode is a compatibility mode that allows UEFI systems to boot using legacy BIOS methods. Legacy mode

disables some of the features and benefits of UEFI, such as secure boot, faster boot time, or larger disk support. Setting UEFI to legacy mode would not enable secure boot UEFI features, but rather disable them.
D) Convert the legacy partition table to UEFI and repair the operating system is not correct. Converting the legacy partition table to UEFI means changing the partitioning scheme from MBR to GPT, which is required for UEFI systems to boot. However, this alone would not enable secure boot UEFI features, as it also depends on the firmware settings and the operating system support. Repairing the operating system may or may not fix any issues caused by converting the partition table, but it would not necessarily enable secure boot either.
1:What Is Secure Boot?2:How to Enable Secure Boot3:MBR vs GPT: Which One Is Better for You?: [UEFI vs Legacy BIOS -- The Ultimate Comparison Guide]

## Answer:

A

## Explanation:

The correct answer is A. Enable secure boot in the hardware and reload the operating system. Secure boot is a feature of UEFI that ensures that only trusted and authorized code can execute during the boot process.Secure boot can prevent boot malware, such as rootkits or bootkits, from compromising the system before the operating system loads1. To enable secure boot, the hardware must support UEFI and have a firmware that implements the secure boot protocol. The operating system must also support UEFI and have a digital signature that matches the keys stored in the firmware. If the operating system was installed in legacy mode or does not have a valid signature, it may not boot with secure boot enabled.Therefore, it may be necessary to reload the operating system after enabling secure boot in the hardware2.

# Question 10

Question Type: MultipleChoice

An employee contacts the SOC to report a high-severity bug that was identified in a new, internally developed web application, which went live in production last week. The SOC staff did not receive contact details or escalation procedures to follow. Which of the following stages of the SDLC

process was overlooked?

## Options:

A- Input validation
B- Planning
C- Implementation and integration
D- Operations and maintenance

## Answer:

B

## Explanation:

The planning stage of the SDLC process is when the project scope, objectives, requirements, risks, and deliverables are defined and agreed upon by all stakeholders.This stage also involves creating a project plan that outlines the tasks, resources, schedule, budget, and communication channels for the project.

The planning stage is crucial for ensuring that the project is aligned with the business goals and customer needs, and that the project team has a clear vision and direction for the development process. By overlooking this stage, the SOC staff did not receive contact details or escalation procedures to follow in case of a high-severity bug, which could have serious consequences for the security and functionality of the web application.

# Question 11

Question Type: MultipleChoice

During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

## Options:

A- strings
B- head
C- fsstat
D- dd

## Answer:

A

## Explanation:

The strings command is a Linux utility that can extract human-readable content from any file or partition3.It can be used to analyze a Linux swap partition by finding text strings that may indicate malicious activity or compromise4. The head command (B) can only display the first few lines of a file or partition, which may not contain any useful information. The fsstat command can only display file system statistics such as size, type, and layout, which may not reveal any human-readable content. The dd command (D) can only copy or convert a file or partition, which may not extract any human-readable content.