# GIAC Foundational Cybersecurity Technologies Practice Test (Sample)

## Study Guide


**Everything you need from our exam experts!**

# Questions

**1. What type of exploit allows an attacker to execute arbitrary code remotely, as described in CVE-2019-9874?**

**A. Remote Code Execution (RCE)**

**B. Heap corruption**

**C. Information disclosure**

**D. Buffer over-read**

**2. In what scenario is symmetric encryption most effective?**

**A. When data is shared among many users**

**B. When a single shared secret key can be securely managed**

**C. When secure document signing is required**

**D. When data needs to be publicly available**

**3. What could occur as a result of a successful Directory Traversal attack?**

**A. Improved application performance**

**B. Unlimited access to the server's filesystem**

**C. A reduction in web traffic**

**D. Increased data integrity**

**4. What does the acronym UAC stand for in cybersecurity?**

**A. User Access Control**

**B. Universal Access Control**

**C. Unauthorized Access Control**

**D. User Authentication Control**

**5. What is a common method for securing passwords in storage?**

**A. Plain text storage**

**B. Encryption**

**C. Base64 encoding**

**D. Hashing**

**6. If you run the command "Python" on a Linux system, what will happen?**

- **A. Python will list all currently installed libraries and modules**
- **B. The computer will run Python in the background upon reboot**
- **C. The operating system will prompt you for a Python code file to open**
- **D. An interactive console will open for writing simple Python code**

**7. What protocol is commonly used to access email on a server?**

- **A. IMAP**
- **B. SSH**
- **C. ICMP**
- **D. BGP**

**8. How do prepared statements help prevent SQL injection attacks?**

- **A. Query parameters are sent in the body of a POST request**
- **B. Queries are appended with an authorization token**
- **C. Query language is kept separate from user supplied data**
- **D. Queries submitted by users are HTML entity encoded**

**9. In Python, what type of structure is `cast_list` if it is defined with curly braces?**

- **A. Dictionary**
- **B. Tuple**
- **C. Array**
- **D. List**

**10. What file attribute is the penetration tester looking to find using the command below? find / -perm -4000 -user root -type f -print 2>/dev/null**

- **A. SUID set**
- **B. SGID set**
- **C. World writable**
- **D. Sticky bit set**

# Answers

1. A
2. B
3. B
4. A
5. D
6. D
7. A
8. C
9. A
10. A

# Explanations

## 1. What type of exploit allows an attacker to execute arbitrary code remotely, as described in CVE-2019-9874?

**A. Remote Code Execution (RCE)**

**B. Heap corruption**

**C. Information disclosure**

**D. Buffer over-read**

**The reason Remote Code Execution (RCE) is the correct answer is that it specifically refers to the ability of an attacker to execute arbitrary code on a target system from a remote location. In the context of CVE-2019-9874, this vulnerability is characterized by an attacker exploiting a flaw to run their own malicious code without requiring direct access to the victim's machine. RCE vulnerabilities are particularly severe because they allow attackers to take control of systems, steal sensitive information, or even disrupt services. The other options do not apply to this scenario. Heap corruption involves issues with memory management that can lead to various security problems but does not inherently imply the execution of arbitrary code by an attacker. Information disclosure refers to vulnerabilities that expose sensitive data without necessarily allowing code execution. Buffer over-read entails reading more data than allocated, which could result in sensitive information being exposed but does not allow for arbitrary code execution like an RCE does. Thus, the key aspect of RCE is the ability to execute malicious code remotely, making it the most fitting classification for the exploit in question.**

## 2. In what scenario is symmetric encryption most effective?

**A. When data is shared among many users**

**B. When a single shared secret key can be securely managed**

**C. When secure document signing is required**

**D. When data needs to be publicly available**

**Symmetric encryption is most effective when a single shared secret key can be securely managed because it relies on that single key for both encryption and decryption processes. In scenarios where the same key is utilized by authorized parties to access data, the efficiency and speed of symmetric algorithms come into play. This method is advantageous in environments where there is a trusted way to distribute the key to all concerned parties, ensuring that only those individuals can encrypt or decrypt the data. The performance benefits are also significant; symmetric encryption algorithms typically require less computational power and are faster than their asymmetric counterparts, which is vital for processing large volumes of data quickly. In contrast, sharing data among many users complicates key management, as multiple keys would be required for each user, which can increase the chances of key exposure or misuse. Secure document signing usually necessitates asymmetric encryption, which provides non-repudiation and integrity for the data. A scenario requiring data to be publicly available would not benefit from encryption in the first place, as the purpose of encryption is to protect data confidentiality, not to make it publicly accessible. Therefore, the scenario in which symmetric encryption shines is when a single shared secret key can be effectively managed and utilized.**

## 3. What could occur as a result of a successful Directory Traversal attack?

**A. Improved application performance**

**B. Unlimited access to the server's filesystem**

**C. A reduction in web traffic**

**D. Increased data integrity**

**A successful Directory Traversal attack allows an attacker to manipulate the URL or input parameters in such a way that they can navigate outside the intended directories of a web application. By exploiting this vulnerability, the attacker gains the ability to access restricted areas of the server's filesystem, thereby achieving unlimited access to the server's filesystem. This means that the attacker could potentially view, modify, or download sensitive files that should not be accessible to unauthorized users, including configuration files, user data, and other critical resources. This type of attack is particularly concerning because it can lead to further exploitation of the server or application, as the attacker may then gain more information about the server's structure, access sensitive data, or install malicious software. Therefore, the risk posed by a successful Directory Traversal attack should be treated with a high level of urgency in cybersecurity practices.**

## 4. What does the acronym UAC stand for in cybersecurity?

**A. User Access Control**

**B. Universal Access Control**

**C. Unauthorized Access Control**

**D. User Authentication Control**

**The acronym UAC stands for User Access Control in cybersecurity. This term refers to a security feature designed to prevent unauthorized changes to the operating system by prompting users for permission or an administrator password before allowing actions that could affect the operating system or other users. It is particularly important in the context of Windows operating systems, where it helps mitigate the risk of malware and protect system integrity by ensuring that only authorized users can make significant changes. User Access Control enhances security by enforcing the principle of least privilege, which means users operate with the minimum permissions necessary for their tasks. This helps in reducing the likelihood of accidental or malicious changes to system settings and software installations, safeguarding both user data and the overall system stability. While other options might refer to certain security concepts, they do not reflect the recognized standard meaning of the UAC acronym in cybersecurity. User Authentication Control, for instance, focuses on verifying user identities, which is a different area of security than access control.**

## 5. What is a common method for securing passwords in storage?

**A. Plain text storage**

**B. Encryption**

**C. Base64 encoding**

**D. Hashing**

**Hashing is a widely accepted method for securing passwords during storage. It converts the original password into a fixed-length string of characters, which appears random. This transformation is one-way, meaning it cannot easily be reversed to retrieve the original password. This is crucial for protecting user data; even if an attacker gains access to the storage where hashed passwords are kept, they cannot easily retrieve the original passwords. Additionally, reputable hashing algorithms include a process called salting, where a unique value is added to each password before hashing, further increasing security by defending against precomputed attacks, such as rainbow tables. In contrast, options like plain text storage leave passwords vulnerable and unprotected, while encryption, although secure, requires additional steps for key management. Base64 encoding is merely an encoding scheme and doesn't provide real security, as it can be easily decoded. Hashing represents an industry-standard approach that emphasizes both security and efficiency.**

## 6. If you run the command "Python" on a Linux system, what will happen?

**A. Python will list all currently installed libraries and modules**

**B. The computer will run Python in the background upon reboot**

**C. The operating system will prompt you for a Python code file to open**

**D. An interactive console will open for writing simple Python code**

**When you run the command "Python" on a Linux system, it initiates the Python interpreter in an interactive mode. This is why the correct answer indicates that an interactive console will open for writing simple Python code. In this console, users can type Python code directly and execute it line-by-line. This feature is particularly useful for testing code snippets, calculations, and learning Python programming in real-time. The interactive console creates a dynamic environment where developers can experiment with code without the need to create a separate script file. The other options do not accurately describe what happens when you execute the command. For instance, while Python does have a library management system, running the command won't automatically list installed libraries and modules. Additionally, Python doesn't run in the background upon reboot simply by being invoked through this command; it requires explicit processes for that functionality. Lastly, invoking Python does not prompt users to open a specific Python code file, instead it provides a shell for immediate code execution.**

## 7. What protocol is commonly used to access email on a server?

**A. IMAP**

**B. SSH**

**C. ICMP**

**D. BGP**

**The protocol commonly used to access email on a server is IMAP, which stands for Internet Message Access Protocol. IMAP allows users to access and manipulate their email messages directly on the mail server. It is particularly useful because it enables users to organize their messages into folders, view messages without downloading them, and maintain the same state across multiple devices. This means that whether you check your email on a phone, a tablet, or a computer, the experience remains consistent. Other protocols for email access include POP3, which downloads messages to a client and typically removes them from the server, but the focus here is on IMAP due to its versatility. SSH is primarily used for secure remote administration and file transfer, ICMP serves diagnostic or control purposes on networks, and BGP is a routing protocol used for exchanging routing information. Therefore, IMAP stands out as the appropriate choice for accessing email hosted on a server.**

## 8. How do prepared statements help prevent SQL injection attacks?

**A. Query parameters are sent in the body of a POST request**

**B. Queries are appended with an authorization token**

**C. Query language is kept separate from user supplied data**

**D. Queries submitted by users are HTML entity encoded**

**Prepared statements help prevent SQL injection attacks by keeping the query language separate from user-supplied data. When a prepared statement is used, the structure of the SQL query is defined first, and placeholders are used for any variables. This means that when user input is provided, it is treated purely as data, without altering the structure of the SQL command itself. By doing so, the risk of an attacker injecting malicious SQL code through user input is significantly minimized. The database interprets the command and the data separately, ensuring that any harmful SQL injection attempts are not executed in the context of the original SQL command. This separation effectively mitigates potential security vulnerabilities associated with dynamic SQL queries that directly incorporate user input without any validation or parameterization. The other options, while potentially relevant to data handling and security, do not address the core mechanism of how prepared statements work in relation to SQL injection specifically. For example, sending query parameters in the body of a POST request or appending authorization tokens do not inherently abstract user input from the query language itself. Likewise, HTML entity encoding is a technique used primarily in web applications to prevent cross-site scripting (XSS) and does not protect against SQL injection attacks.**

## 9. In Python, what type of structure is `cast_list` if it is defined with curly braces?

**A. Dictionary**

**B. Tuple**

**C. Array**

**D. List**

**When `cast_list` is defined using curly braces in Python, it is a dictionary. In Python, curly braces `{}` are used to create dictionaries, which are unordered collections of key-value pairs. Each key must be unique, and it is associated with a value that can be of any data type. Dictionaries are versatile and allow for fast lookups, additions, and deletions of items based on keys. The structure is particularly useful for situations where you want to associate certain values with specific identifiers. In contrast, a tuple is created using parentheses `()`, a list is defined with square brackets `[]`, and an array is typically created using the array module or libraries such as NumPy, which do not use curly braces at all. This distinction in the syntax and key characteristics of these different data structures helps clarify why defining `cast_list` with curly braces results in a dictionary.**

## 10. What file attribute is the penetration tester looking to find using the command below? find / -perm -4000 -user root -type f -print 2>/dev/null

**A. SUID set**

**B. SGID set**

**C. World writable**

**D. Sticky bit set**

**The command provided is designed to search for files on a Unix/Linux system that have specific characteristics. The use of `-perm -4000` is particularly significant because it indicates that the command is searching for files that have the "Set User ID" (SUID) permission set. When a file has the SUID attribute set, it allows users to execute the file with the permissions of the file's owner—which in this case is specified as "root." This is particularly important in penetration testing, as SUID files can pose security risks if not properly monitored or controlled, potentially allowing unauthorized users to gain elevated privileges. In the context of penetration testing, finding SUID files helps identify possible vulnerabilities that could be exploited to gain unauthorized access or to escalate privileges. Thus, identifying files with the SUID bit set is crucial for assessing the security posture of a system. The other attributes mentioned do not correspond to the characteristics being searched for in this command: - The SGID (Set Group ID) allows files to run with the permissions of the group that owns the file, which is not indicated by the `-4000` permission. - A world writable file allows any user to write to the file, denoted by `-222`, which**