GIAC Foundational Cybersecurity Technologies Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **Which of the following is a Windows Database of settings for both the operating system and applications?**

   A. Group Policy

   B. User Access Control

   C. PowerShell

   D. Registry

2. **What is the name of the file that instructs search engines to avoid certain locations on a website?**

   A. robots.txt

   B. my.conf

   C. index.html

   D. admin.php

3. **Which of the following best describes encryption?**

   A. A transformation process that ensures the confidentiality of data

   B. A technique for data compression

   C. A method used only in secure communications

   D. A process that adds redundancy to data

4. **Which of the following is an effective way to mitigate a Cross Site Request Forgery?**

   A. Make sure every request is submitted from the same IP address

   B. Use a Cross Site Request Forgery Token that is required for every form

   C. Limit the number of requests submitted in a session

   D. Disable cookies during transfers

5. **Which C:\Windows\System32 subdirectory may provide stored credentials from unattended installs?**

   A. Restore

   B. Boot

   C. Sysprep

   D. Dism

6. What does a stack canary protect in a stack?

A. A value that sits after the return pointer

B. A value that sits before the return pointer of the stack

C. A security flag used in hardware

D. A variable used for stack management

7. When debugging a program with pwndbg, what is the significance of the 's' in the command x/s 0x80484ef?

A. Tells the command to step into the address 0x80484ef

B. Identifies the output format for data at address 0x80484ef

C. Tells the command to stop after the address 0x80484ef

D. Identifies the next breakpoint is address 0x80484ef

8. Which of the following is a likely source of logs for HTTP network traffic data?

A. Layer 2 switch

B. Firewall

C. DNS Server

D. Active Directory Server

9. Which approach is most effective for identifying unauthorized access in a system?

A. Regularly scheduled audits

B. Ad-hoc checks

C. Monitoring user access logs

D. Installing antivirus software

10. Which security method can reduce risks associated with file uploads?

A. Allow all file types

B. Implement strict file type validation

C. Use a single upload directory

D. Automatically process every file uploaded

Answers

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

Explanations

1. Which of the following is a Windows Database of settings for both the operating system and applications?

A. Group Policy

B. User Access Control

C. PowerShell

D. Registry

The Registry is a hierarchical database used in Windows operating systems to store low-level settings for the operating system and for applications that opt to use the Registry. This database contains information, settings, and options for both hardware and software, including device drivers, system services, user settings, and application configurations. Windows uses the Registry to manage various system functions and configurations, allowing for centralized control over the settings that govern the behavior of the OS and the associated applications. This includes managing user profiles, application preferences, and system policies, among others. The other options represent distinct components or functionalities within Windows. Group Policy is a feature that allows for centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment, but it doesn't serve as a database. User Access Control is a security component that helps prevent unauthorized changes to the operating system by requiring administrative approval for certain actions, rather than a storage database. PowerShell is a task automation framework consisting of a command-line shell and a scripting language, but it is not a database for settings. Thus, the Registry is the correct choice for a database of settings in Windows.

2. What is the name of the file that instructs search engines to avoid certain locations on a website?

A. robots.txt

B. my.conf

C. index.html

D. admin.php

The file that instructs search engines to avoid certain locations on a website is known as robots.txt. This file is placed in the root directory of a website and is part of the Robots Exclusion Protocol. It allows webmasters to inform search engine crawlers and bots which pages or sections of the site should not be processed or scanned. By specifying directives within this file, website owners can effectively manage how their content is crawled and indexed by search engines, facilitating better control over their site's visibility and search engine optimization strategies. The other options are not used for this purpose. For example, my.conf is typically a configuration file for applications or services but is unrelated to web crawling or indexing. Index.html is a standard file that serves as the homepage or main entry point of a website, containing the HTML content, but does not influence how bots interact with the site. Admin.php is a script file that usually handles administrative functions on a website but does not serve to communicate with search engine bots regarding crawling permissions.

3. Which of the following best describes encryption?

A. A transformation process that ensures the confidentiality of data

B. A technique for data compression

C. A method used only in secure communications

D. A process that adds redundancy to data

Encryption is fundamentally a transformation process that ensures the confidentiality of data. It involves converting plain text into a coded format, making it unreadable to unauthorized users. By employing encryption algorithms, sensitive information is protected from potential threats and data breaches, ensuring that only those with the appropriate decryption keys can access the original data. In contrast, the other options do not accurately describe encryption. While data compression is aimed at reducing the size of data, it does not concern itself with making the data confidential. The third option suggests that encryption is used only in secure communications, which is misleading, as encryption can also be applied to data at rest, stored in databases, or in various applications beyond just communication. Lastly, the option indicating that encryption adds redundancy to data is incorrect; encryption actually aims to make the data more secure and typically does not add extra data that would lead to redundancy.

4. Which of the following is an effective way to mitigate a Cross Site Request Forgery?

A. Make sure every request is submitted from the same IP address

B. Use a Cross Site Request Forgery Token that is required for every form

C. Limit the number of requests submitted in a session

D. Disable cookies during transfers

Using a Cross Site Request Forgery (CSRF) Token is an effective way to mitigate CSRF attacks because it incorporates an additional layer of verification for web requests. When a user requests a particular action (like submitting a form), the server generates a unique token and attaches it to the form. This token is then included with the form submission. When the server receives a request, it checks for the presence and validity of this token. If the token is absent or does not match the expected value, the server can reject the request. This mechanism ensures that the request is legitimate and originated from the authorized user, not from a third-party site trying to perform actions on behalf of the user, which is the fundamental issue with CSRF vulnerabilities. Other options lack effectiveness in addressing the specific nature of CSRF. For instance, restricting requests by IP addresses can lead to false negatives, especially for legitimate users who may change networks or use dynamic IP addresses. Limiting the number of requests in a session does not effectively prevent unauthorized requests, as it could inadvertently restrict legitimate user actions. Disabling cookies may resolve some session-related issues, but it does not address how CSRF exploits operate, as an attacker can still trigger requests without directly relying on cookies.

5. Which C:\Windows\System32 subdirectory may provide stored credentials from unattended installs?

A. Restore

B. Boot

C. Sysprep

D. Dism

The correct answer is C. Sysprep. This directory is associated with the system preparation tool used in Windows environments to prepare an installation of Windows for imaging and deployment. During an unattended installation, Sysprep can store credentials and other customization information needed for the installation to proceed without user intervention. This is particularly useful in environments where systems are set up in bulk, ensuring that the necessary settings and configurations are automatically applied. The other directories mentioned, such as Restore, Boot, and Dism, serve different purposes. The Restore directory is related to the system recovery functions, primarily used for restoring Windows to a previous state. The Boot directory contains files necessary for the system boot process and configurations, while Dism is associated with the Deployment Image Servicing and Management tool, used for managing Windows image files rather than storing installation credentials. Therefore, the Sysprep directory is specifically focused on preparing Windows installations, making it the right choice for stored credentials from unattended installs.

6. What does a stack canary protect in a stack?

A. A value that sits after the return pointer

B. A value that sits before the return pointer of the stack

C. A security flag used in hardware

D. A variable used for stack management

A stack canary is a specific security mechanism that helps protect against stack buffer overflow attacks. It typically involves placing a known value (the canary) right before the return pointer on the stack. The main purpose of the stack canary is to detect any alterations to the return pointer caused by a buffer overflow, which could allow an attacker to hijack the control flow of a program. When a program uses a stack canary, it checks the canary's value before executing a return instruction. If the value has changed, it indicates that there has been an overflow or an unauthorized alteration, prompting the program to terminate or take additional protective measures. This mechanism is essential for maintaining the integrity of the execution flow and preventing exploitable vulnerabilities. The other options pertain to different aspects of security and stack management but do not accurately describe the role or placement of the stack canary in relation to the return pointer. Thus, the correct understanding of the stack canary's position—right before the return pointer—is crucial for grasping its function in stack protection.

7. When debugging a program with pwndbg, what is the significance of the 's' in the command x/s 0x80484ef?

A. Tells the command to step into the address 0x80484ef

B. Identifies the output format for data at address 0x80484ef

C. Tells the command to stop after the address 0x80484ef

D. Identifies the next breakpoint is address 0x80484ef

The command `x/s 0x80484ef` in pwndbg is significant because the 's' indicates that the command should interpret the data at the specified memory address (0x80484ef) as a string. This means that when using this command, pwndbg will display the contents of the address as a null-terminated string, allowing the user to read textual data stored at that location in memory. This is particularly useful when debugging programs that may output strings or have important textual information at specific memory addresses. Understanding the context of the command helps clarify its use in debugging. Other formats can be specified with different letters, such as 'i' for instructions or 'x' for hexadecimal representation, but in this case, the 's' is specifically for string representation. This feature is instrumental in diagnosing issues within the program by allowing the debugger to present the data in a human-readable format, thereby aiding the developer in analyzing and resolving potential problems related to string handling or data corruption.

8. Which of the following is a likely source of logs for HTTP network traffic data?

A. Layer 2 switch

B. Firewall

C. DNS Server

D. Active Directory Server

The selection of a firewall as a likely source of logs for HTTP network traffic data is appropriate as firewalls are specifically designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. They often maintain logs that capture data about HTTP requests and responses, including details like source and destination IP addresses, ports, and protocols used, which are critical for understanding web traffic patterns and identifying potential security threats. A firewall inspects the content of the HTTP traffic, providing insights into which websites are being accessed and which users are generating that traffic. This capability makes firewalls an integral part of network security, as they help in detecting and logging suspicious activities that could indicate malicious behavior, such as unauthorized access attempts or data exfiltration. In contrast, the other options do not serve primarily as sources of HTTP traffic logging. A Layer 2 switch primarily operates at the data link layer, managing data frames and does not log the higher-level protocols such as HTTP. A DNS Server is focused on resolving domain names to IP addresses, not tracking HTTP traffic directly. Similarly, an Active Directory Server primarily handles authentication and directory services and does not log HTTP traffic as part of its core functions. Hence, firewalls stand out as the most relevant source for HTTP network traffic

9. Which approach is most effective for identifying unauthorized access in a system?

A. Regularly scheduled audits

B. Ad-hoc checks

C. Monitoring user access logs

D. Installing antivirus software

Monitoring user access logs is the most effective approach for identifying unauthorized access in a system because it allows for real-time tracking of all user activity within that environment. By regularly reviewing access logs, an organization can detect unusual patterns or anomalies that may indicate unauthorized access, such as access attempts by unfamiliar users, access at odd hours, or operations performed that deviate from a user's normal behavior. This method provides critical insights into who accessed what, when, and what actions were taken. Automated alerts can also be set up for certain activities, enabling quicker responses to potential security incidents. In contrast, while regularly scheduled audits can help with the overall assessment of security posture, they may not catch unauthorized access in a timely manner. Ad-hoc checks provide a less systematic approach and might miss ongoing unauthorized activities. Although antivirus software is crucial for preventing malware and other malicious software, it does not specifically focus on unauthorized access at the user level. Therefore, monitoring user access logs remains the most targeted and effective method for identifying potential security breaches related to unauthorized access.

10. Which security method can reduce risks associated with file uploads?

A. Allow all file types

B. Implement strict file type validation

C. Use a single upload directory

D. Automatically process every file uploaded

Implementing strict file type validation is crucial in reducing the risks associated with file uploads. This method involves checking the type of file that a user is attempting to upload and ensuring it conforms to a predetermined list of acceptable file types. By validating the file types against a whitelist of safe formats (such as images or documents), organizations can significantly minimize the risk of malicious files being uploaded to their systems. Allowing all file types can expose the system to various threats, such as uploading executable files that could contain malware. Using a single upload directory might help organize files, but it doesn't address potential risks associated with the file contents themselves. Automatically processing every file uploaded can lead to security vulnerabilities, as malicious files may be executed or further processed without adequate checks. By enforcing strict validations, organizations can protect themselves from common file upload vulnerabilities, such as remote code execution, file inclusion attacks, and other security threats that could arise from processing untrusted files. This proactive approach is essential in maintaining the integrity and security of the overall system.