312-50V12 Q&As

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/312-50v12.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

A. Have the network team document the reason why the rule was implemented without prior manager approval.

B. Monitor all traffic using the firewall rule until a manager can approve it.

C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.

D. Immediately roll back the firewall rule until a manager can approve it

Correct Answer: D

QUESTION 2

What does a firewall check to prevent particular ports and applications from getting packets into an organization?

A. Transport layer port numbers and application layer headers

B. Presentation layer headers and the session layer port numbers

C. Network layer headers and the session layer port numbers

D. Application layer port numbers and the transport layer headers

Correct Answer: A

QUESTION 3

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers

manually to get more precise results than if using web vulnerability scanners.

What proxy tool will help you find web vulnerabilities?

A. Maskgen

B. Dimitry

C. Burpsuite

D. Proxychains

Correct Answer: C

QUESTION 4

Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

A. LDAP Injection attack

B. Cross-Site Scripting (XSS)

C. SQL injection attack

D. Cross-Site Request Forgery (CSRF)

Correct Answer: B

QUESTION 5

An ethical hacker has been tasked with assessing the security of a major corporation\\'s network. She suspects the network uses default SNMP community strings. To exploit this, she plans to extract valuable network information using SNMP enumeration. Which tool could best help her to get the information without directly modifying any parameters within the SNMP agent\\'s management information base (MIB)?

A. snmp-check (snmp_enum Module) to gather a wide array of information about the target

B. Nmap, with a script to retrieve all running SNMP processes and associated ports

C. Oputits, are mainly designed for device management and not SNMP enumeration

D. SnmpWalk, with a command to change an OID to a different value

Correct Answer: A

snmp-check (snmp_enum Module) is the best tool to help the ethical hacker to get the information without directly modifying any parameters within the SNMP agent\\'s MIB. snmp-check is a tool that allows the user to enumerate SNMP devices and extract information from them. It can gather a wide array of information about the target, such as system information, network interfaces, routing tables, ARP cache, installed software, running processes, TCP and UDP services, user accounts, and more. snmp-check can also perform brute force attacks to discover the SNMP community strings, which are the passwords used to access the SNMP agent. snmp-check is available as a standalone tool or as a module (snmp_enum) within the Metasploit framework. The other options are not as effective or suitable as snmp-check for the ethical hacker\\'s task. Nmap is a network scanning and enumeration tool that can perform various types of scans and probes on the target. It can also run scripts to perform specific tasks, such as retrieving SNMP information. However, Nmap may not be able to gather as much information as snmp-check, and it may also trigger alerts or blocks from firewalls or intrusion detection systems. Oputils is a network monitoring and management toolset that can perform various functions, such as device discovery, configuration backup, bandwidth monitoring, IP address management, and more. However, Oputils is mainly designed for device management and not SNMP enumeration, and it may not be able to extract valuable network information from the SNMP agent. SnmpWalk is a tool that allows the user to retrieve the entire MIB tree of an SNMP agent by using SNMP GETNEXT requests. However, SnmpWalk is not suitable for the ethical hacker\\'s task, because it requires the user to change an OID (object identifier) to a different value, which may modify the parameters within the SNMP agent\\'s MIB and affect its functionality or security. References: snmp-check - The SNMP enumerator SNMP Enumeration | Ethical Hacking - GreyCampus SNMP Enumeration - GeeksforGeeks Nmap - the Network Mapper - Free Security Scanner OpUtils - Network Monitoring and Management Toolset SnmpWalk - SNMP MIB Browser

QUESTION 6

Which definition among those given below best describes a covert channel?

A. A server program using a port that is not well known.

B. Making use of a protocol in a way it is not intended to be used.

C. It is the multiplexing taking place on a communication link.

D. It is one of the weak channels used by WEP which makes it insecure

Correct Answer: B

QUESTION 7

Attacker Rony installed a rogue access point within an organization\\'s perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by johnson in the above scenario?

A. Host-based assessment

B. Wireless network assessment

C. Application assessment

D. Distributed assessment

Correct Answer: B

Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner.This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment.It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses.Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

QUESTION 8

Which method of password cracking takes the most time and effort?

A. Dictionary attack

B. Shoulder surfing

C. Rainbow tables

D. Brute force

Correct Answer: D

Brute-force attack when an attacker uses a set of predefined values to attack a target and analyze the response until he succeeds. Success depends on the set of predefined values. It will take more time if it is larger, but there is a better probability of success. In a traditional brute-force attack, the passcode or password is incrementally increased by one letter/number each time until the right passcode/password is found.

QUESTION 9

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext. Which file do you have to clean to clear the password?

A. .X session-log

B. .bashrc

C. .profile

D. .bash_history

Correct Answer: D

File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are

executed.BASH_HISTORY files are hidden files with no filename prefix. They always use the filename .bash_history.NOTE:

Bash is that the shell program employed by Apple Terminal.Our goal is to assist you understand what a file with a *.bash_history suffix is and the way to open it.The Bash History file type, file format description, and Mac and Linux programs

listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we\\'ve tested and validated.

QUESTION 10

What does the following command in netcat do? nc -l -u -p55555

A. logs the incoming connections to /etc/passwd file

B. loads the /etc/passwd file to the UDP port 55555

C. grabs the /etc/passwd file when connected to UDP port 55555

D. deletes the /etc/passwd file when connected to the UDP port 55555

Correct Answer: C

QUESTION 11

Which results will be returned with the following Google search query? site:target.com site:Marketing.target.com accounting

A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.

B. Results matching all words in the query.

C. Results for matches on target.com and Marketing.target.com that include the word "accounting"

D. Results matching "accounting" in domain target.com but not on the site Marketing.target.com

Correct Answer: D

QUESTION 12

Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (GHDB) with an emphasis on VPN footprinting. Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

A. intitle: This operator restricts results to only the pages containing the specified term in the title

B. location: This operator finds information for a specific location

C. inur: This operator restricts the results to only the pages containing the specified word in the URL

D. link: This operator searches websites or pages that contain links to the specified website or page

Correct Answer: B

The location: operator is the least useful in providing the attacker with sensitive VPN-related information, because it does not directly relate to VPN configuration, credentials, or vulnerabilities. The location: operator finds information for a specific location, such as a city, country, or region. For example, location:paris would return results related to Paris, France. However, this operator does not help the attacker to identify or access VPN servers or clients, unless they are specifically named or indexed by their location, which is unlikely. The other operators are more useful in providing the attacker with sensitive VPN-related information, because they can help the attacker to find pages or files that contain VPN configuration, credentials, or vulnerabilities. The intitle: operator restricts results to only the pages containing the specified term in the title. For example, intitle:vpn would return pages with VPN in their title, which may include VPN guides, manuals, or tutorials. The inurl: operator restricts the results to only the pages containing the specified word in the URL. For example, inurl:vpn would return pages with VPN in their URL, which may include VPN login portals, configuration files, or directories. The link: operator searches websites or pages that contain links to the specified website or page. For example, link:vpn.com would return pages that link to vpn.com, which may include VPN reviews, comparisons, or recommendations. References: Google Search Operators: The Complete List (44 Advanced Operators) Footprinting through search engines Module 02: Footprinting and Reconnaissance

QUESTION 13

Why containers are less secure that virtual machines?

A. Host OS on containers has a larger surface attack.

B. Containers may full fill disk space of the host.

C. A compromise container may cause a CPU starvation of the host.

D. Containers are attached to the same virtual network.

Correct Answer: A

QUESTION 14

You are a cybersecurity specialist at CloudTech Inc., a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?

A. Use the cloud service provider\\'s encryption services but store keys on-premises.

B. Use the cloud service provider\\'s default encryption and key management services.

C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.

D. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.

Correct Answer: D

The best practice to meet the client\\'s requirement is to encrypt data client- side before uploading to the cloud and retain control of the encryption keys. This practice is also known as client-side encryption or end-to-end encryption, and it involves encrypting the data on the client\\'s device using a software or hardware tool that generates and manages the encryption keys. The encrypted data is then uploaded to the cloud service, where it remains encrypted at rest. The encryption keys are never shared with the cloud service provider or any third party, and they are only used by the client to decrypt the data when needed. This way, the client can maintain full control over the encryption keys and the security of the data, even when the data is stored on a public cloud service12. The other options are not as optimal as option D for the following reasons:

A. Use the cloud service provider\\'s encryption services but store keys on- premises: This option is not feasible because it contradicts the client\\'s requirement of maintaining full control over the encryption keys. Using the cloud service provider\\'s encryption services means that the client has to rely on the cloud service provider to generate and manage the encryption keys, even if the keys are stored on-premises. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data. Moreover, storing the keys on-premises may introduce additional challenges, such as key distribution, synchronization, backup, and recovery3. B. Use the cloud service provider\\'s default encryption and key management services: This option is not desirable because it violates the client\\'s requirement of maintaining full control over the encryption keys. Using the cloud service provider\\'s default encryption and key management services means that the client has to trust the cloud service provider to encrypt and decrypt the data on the server-side, using the cloud service provider\\'s own encryption keys and mechanisms. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data. Furthermore, the cloud service provider\\'s default encryption and key management services may not meet the regulatory requirements or the security standards of the client4. C. Rely on Secure Sockets Layer (SSL) encryption for data at rest: This option is not sufficient because SSL encryption is not designed for data at rest, but for data in transit. SSL encryption is a protocol that encrypts the data as it travels over the internet between the client and the server, using certificates and keys that are exchanged and verified by both parties. SSL encryption can protect the data from being intercepted or modified by unauthorized parties, but it does not protect the data from being accessed or decrypted by the cloud service provider or any third party who has access to the server. Moreover, SSL encryption does not provide the client with any control over the encryption keys or the security of the data. References:

1: Client-side encryption - Wikipedia

2: What is Client-Side Encryption? | Definition, Benefits and Best Practices | Kaspersky

3: Cloud Encryption Key Management: What You Need to Know | Thales

4: Cloud Encryption: How It Works and How to Use It | Comparitech : What is SSL Encryption and How Does it Work? | Norton

QUESTION 15

Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files. What is the type of injection attack Calvin\\'s web application is susceptible to?

A. Server-side template injection

B. Server-side JS injection

C. CRLF injection

D. Server-side includes injection

Correct Answer: D