312-50V10^{Q&As}

Certified Ethical Hacker Exam (C|EH v10)

Pass EC-COUNCIL 312-50V10 Exam with 100% Guarantee

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

https://www.passapply.com/312-50v10.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

How can a policy help improve an employee\\'s security awareness?

A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security

B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees

C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line

D. By decreasing an employee\\'s vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

Correct Answer: A

QUESTION 2

An IT security engineer notices that the company\\\'s web server is currently being hacked. What should the engineer do next?

A. Unplug the network connection on the company\\\'s web server.

B. Determine the origin of the attack and launch a counterattack.

C. Record as much information as possible from the attack.

D. Perform a system restart on the company\\\'s web server.

Correct Answer: C

QUESTION 3

This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.

Which of the following organizations is being described?

A. Payment Card Industry (PCI)

B. Center for Disease Control (CDC)

C. Institute of Electrical and Electronics Engineers (IEEE)

D. International Security Industry Organization (ISIO)

Correct Answer: A

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back end storage and access of PII (personally identifiable information). References: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

QUESTION 4

Which of the following act requires employer\\'s standard national numbers to identify them on standard transactions?

A. SOX

B. HIPAA

C. DMCA

D. PCI-DSS

Correct Answer: B

QUESTION 5

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace

B. tcptraceroute

C. Nessus

D. OpenVAS

Correct Answer: A

tcptrace is a tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/Wireshark, snoop, EtherPeek, and Agilent NetMetrix.

References: https://en.wikipedia.org/wiki/Tcptrace

QUESTION 6

While performing ping scans into a target network you get a frantic call from the organization\\'s security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization\\'s IDS monitor.

How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.

B. Do not scan the broadcast IP.

C. Spoof the source IP address.

D. Only scan the Windows systems.

Correct Answer: B

QUESTION 7

Which set of access control solutions implements two-factor authentication?

A. USB token and PIN

B. Fingerprint scanner and retina scanner

C. Password and PIN

D. Account and password

Correct Answer: A

QUESTION 8

Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use a scan tool like Nessus

B. Use the built-in Windows Update tool

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Correct Answer: A

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and

Exposures architecture for easy cross-linking between compliant security tools.

The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix- or

Windows-based operating systems. Note: Significant capabilities of Nessus include:

References: http://searchnetworking.techtarget.com/definition/Nessus

QUESTION 9

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK

B. LOGIN, NICK

C. USER, PASS

D. LOGIN, USER

Correct Answer: A

QUESTION 10

Scenario: 1. Victim opens the attacker\\'s web site.

2.

Attacker sets up a web site which contains interesting and attractive content like \\'Do you want to make S100 In a day?\\',

3.

Victim clicks to the interesting and attractive content url.

4- Attacker creates a transparent iframe\\' in front of the url which victim attempt to click, so victim thinks that he/she clicks to the \\'Do you want to make $1000 in a day?\\' url but actually he/sne clicks to the content or url that exists in the transparent iframe\\' which is setup by the attacker.

What is the name of the attack which is mentioned in the scenario?

A. HTTP Parameter Pollution

B. HTML Injection

C. Session Fixation

D. ClickJacking Attack

Correct Answer: D

QUESTION 11

Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA is the recovery agent used to encrypt data when a user\\'s certificate is lost.

B. The root CA stores the user\\'s hash value for safekeeping.

C. The CA is the trusted root that issues certificates.

D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Correct Answer: C

QUESTION 12

Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?

A. Bootrom Exploit

B. iBoot Exploit

C. Sandbox Exploit

D. Userland Exploit

Correct Answer: D

QUESTION 13

A consultant has been hired by the V.P. of a large financial organization to assess the company\\'s security posture. During the security testing, the consultant comes across child pornography on the V.P.\\'s computer. What is the consultant\\'s obligation to the financial organization?

A. Say nothing and continue with the security testing.

B. Stop work immediately and contact the authorities.

C. Delete the pornography, say nothing, and continue security testing.

D. Bring the discovery to the financial organization\\\'s human resource department.

Correct Answer: B

QUESTION 14

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

A. Data items and vulnerability scanning

B. Interviewing employees and network engineers

C. Reviewing the firewalls configuration

D. Source code review

Correct Answer: A

QUESTION 15

Which of the following is a strong post designed to stop a car?

A. Gate

B. Fence

C. Bollard

D. Reinforced rebar

Correct Answer: C

Latest 312-50V10 Dumps	312-50V10 Study Guide	312-50V10 Exam Questions