

ExamsLabs

ExamsLabs

HOME

ALL VENDORS

GUARANTEE

FAQ

TESTIMONIALS

CART (0)

Pass Your Next Certification Exam Fast!

Everything you need to prepare, learn & pass your certification exam easily.

365 days free updates. First attempt guaranteed success.



Select a vendor...

Select an test...

Your email address

Free Download Demo

Try **Online Engine** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.

PDF format: Easy to read and print learning materials, our products are available in PDF file format.

Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.

What Client's Say

"I passed today with score 80%. I confirm that it's valid in UK. Focus on "Correct answer" and forget the "Answer X from real test". I had free new questions.



Sebastian
★★★★★

"Questions from this HPE0-S51 dump are 100% valid... not all answers. I passed this exam a few days ago (in France) and got these results.



Wayne
★★★★★

<http://www.examslabs.com/>

Latest Study Materials, Valid Dumps - ExamsLabs

Exam : **312-50v9**

Title : Certified Ethical Hacker v9
Exam

Vendor : EC-COUNCIL

Version : DEMO

NO.1 Perspective clients want to see sample reports from previous penetration tests. What should you do next?

- A. Share full reports, not redacted.
- B. Share full reports, with redacted.
- C. Decline but, provide references.
- D. Share reports, after NDA is signed.

Answer: B

NO.2 Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.

Which tool can be used to perform session splicing attacks?

- A. Hydra
- B. Burp
- C. Whisker
- D. Tcpsplice

Answer: C

NO.3 This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like Korek attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.

Which of the following tools is being described?

- A. Wifcracker
- B. WLAN-crack
- C. Airguard
- D. Aircrack-ng

Answer: D

NO.4 In Risk Management, how is the term "likelihood" related to the concept of "threat?"

- A. Likelihood is the probability that a vulnerability is a threat-source.
- B. Likelihood is a possible threat-source that may exploit a vulnerability.
- C. Likelihood is the likely source of a threat that could exploit a vulnerability.
- D. Likelihood is the probability that a threat-source will exploit a vulnerability.

Answer: D

NO.5 Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.

If a scanned port is open, what happens?

- A. The port will ignore the packets.
- B. The port will send an RST.
- C. The port will send an ACK.
- D. The port will send a SYN.

Answer: A

NO.6 Which method of password cracking takes the most time and effort?

- A. Rainbow Tables
- B. Shoulder surfing
- C. Bruce force
- D. Directory attack

Answer: C

NO.7 Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.

What should you do?

- A. Copy the data to removable media and keep it in case you need it.
- B. Ignore the data and continue the assessment until completed as agreed.
- C. Confront the client on a respectful manner and ask her about the data.
- D. Immediately stop work and contact the proper legal authorities.

Answer: D

NO.8 > NMAP -sn 192.168.11.200-215

The NMAP command above performs which of the following?

- A. A ping scan
- B. A trace sweep
- C. An operating system detect
- D. A port scan

Answer: A

NO.9 In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known wardriving.

Which algorithm is this referring to?

- A. Wired Equivalent Privacy (WEP)
- B. Temporal Key Integrity Protocol (TRIP)
- C. Wi-Fi Protected Access (WPA)
- D. Wi-Fi Protected Access 2(WPA2)

Answer: A

NO.10 An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to www.MyPersonalBank.com, that the user is directed to a phishing site.

Which file does the attacker need to modify?

- A. Hosts
- B. Networks
- C. Boot.ini

D. Sudoers

Answer: A

NO.11 Which of these options is the most secure procedure for strong backup tapes?

- A. In a climate controlled facility offsite
- B. Inside the data center for faster retrieval in a fireproof safe
- C. In a cool dry environment
- D. On a different floor in the same building

Answer: A

NO.12 Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

- A. Verify access right before allowing access to protected information and UI controls
- B. Use security policies and procedures to define and implement proper security settings
- C. Validate and escape all information sent over to a server
- D. Use digital certificates to authenticate a server prior to sending data

Answer: A