



*Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.*



312-49v10 Dumps  
312-49v10 Braindumps  
312-49v10 Real Questions  
312-49v10 Practice Test  
312-49v10 Actual Questions



**EC-Council**

# 312-49v10

*Computer Hacking Forensic Investigator (CHFI-v10)*



### Question: 90

Kyle is performing the final testing of an application he developed for the accounting department.

His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command.

What is he testing at this point?

```
#include <stdio.h>
#include <string.h>
int main(int argc, char
```

```
*argv[]) {
    char buffer[10];
    if (argc < 2) {
        fprintf(stderr, "USAGE: %s stringn", argv[0]);
        return 1;
    }
```

```
    strcpy(buffer, argv[1]);
    return 0;
}
```

- A. Buffer overflow
- B. SQL injection
- C. Format string bug
- D. Kernel injection

**Answer: A**

### Question: 91

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet.

Why is that?

- A. Stateful firewalls do not work with packet filtering firewalls
- B. NAT does not work with stateful firewalls
- C. IPSEC does not work with packet filtering firewalls
- D. NAT does not work with IPSEC

**Answer: D**

### Question: 92

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and

passwords.

What tool could you use to get this information?

- A. Airsnort
- B. Snort
- C. Ettercap
- D. RaidSniff

**Answer:** C

**Question:** 93

What TCP/UDP port does the toolkit program netstat use?

- A. Port 7
- B. Port 15
- C. Port 23
- D. Port 69

**Answer:** B

**Question:** 94

Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server.

Why will Jonathan not succeed?

- A. Only an HTTPS session can be hijacked
- B. HTTP protocol does not maintain session
- C. Only FTP traffic can be hijacked
- D. Only DNS traffic can be hijacked

**Answer:** B

**Question:** 95

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers.

What type of firewall must you implement to abide by this policy?

- A. Packet filtering firewall
- B. Circuit-level proxy firewall
- C. Application-level proxy firewall
- D. Stateful firewall

**Answer:** D

### Question: 96

Printing under a Windows Computer normally requires which one of the following files types to be created?

- A. EME
- B. MEM
- C. EMF
- D. CME

**Answer: C**

### Question: 97

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related.

What organization should Frank submit the log to find out if it is a new vulnerability or not?

- A. APIPA
- B. IANA
- C. CVE
- D. RIPE

**Answer: C**

### Question: 98

Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces.

What could have prevented this information from being stolen from the laptops?

- A. EFS Encryption
- B. DFS Encryption
- C. IPS Encryption
- D. SDW Encryption

**Answer: A**

### Question: 99

This organization maintains a database of hash signatures for known software.

- A. International Standards Organization
- B. Institute of Electrical and Electronics Engineers
- C. National Software Reference Library
- D. American National standards Institute

**Answer: C**

**Question: 100**

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe.

What are you trying to accomplish here?

- A. Poison the DNS records with false records
- B. Enumerate MX and A records from DNS
- C. Establish a remote connection to the Domain Controller
- D. Enumerate domain user accounts and built-in groups

**Answer: D**



# SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

*Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:*

**Actual Exam Questions:** *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

**Exam Dumps:** *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

**Practice Tests:** *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

**Guaranteed Success:** *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

**Updated Content:** *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

**Technical Support:** *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>  
Kill your exam at First Attempt....Guaranteed!