

312-49^{Q&As}

ECCouncil Computer Hacking Forensic Investigator (V9)

Pass EC-COUNCIL 312-49 Exam with 100% Guarantee

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

<https://www.pass2lead.com/312-49.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

Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

- A. File fingerprinting
- B. Identifying file obfuscation
- C. Static analysis
- D. Dynamic analysis

Correct Answer: A

QUESTION 2

A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

- A. They examined the actual evidence on an unrelated system
- B. They attempted to implicate personnel without proof
- C. They tampered with evidence by using it
- D. They called in the FBI without correlating with the fingerprint data

Correct Answer: C

QUESTION 3

The newer Macintosh Operating System is based on: A. OS/2

- B. BSD Unix
- C. Linux
- D. Microsoft Windows

Correct Answer: B

QUESTION 4

You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk

contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

- A. Limited force and library attack
- B. Brute Force and dictionary Attack
- C. Maximum force and thesaurus Attack
- D. Minimum force and appendix Attack

Correct Answer: B

QUESTION 5

Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.

Which organization coordinates computer crimes investigations throughout the United States?

- A. Internet Fraud Complaint Center
- B. Local or national office of the U.S. Secret Service
- C. National Infrastructure Protection Center
- D. CERT Coordination Center

Correct Answer: B

QUESTION 6

You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm's employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

- A. Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned
- B. Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment
- C. Inform the owner that conducting an investigation without a policy is a violation of the employee's expectation of privacy
- D. Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

Correct Answer: C

QUESTION 7

George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

- A. Nessus is too loud
- B. Nessus cannot perform wireless testing
- C. Nessus is not a network scanner
- D. There are no ways of performing a "stealthy" wireless scan

Correct Answer: A

QUESTION 8

Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation?

- A. John Doe Search Warrant
- B. Citizen Informant Search Warrant
- C. Electronic Storage Device Search Warrant
- D. Service Provider Search Warrant

Correct Answer: C

QUESTION 9

Which one of the following is not a first response procedure?

- A. Preserve volatile data
- B. Fill forms
- C. Crack passwords
- D. Take photos

Correct Answer: C

QUESTION 10

The use of warning banners helps a company avoid litigation by overcoming an employee assumed _____. When connecting to the company's intranet, network or Virtual Private Network(VPN) and will allow the company's investigators to monitor, search and retrieve information stored within the network.

- A. Right to work
- B. Right of free speech
- C. Right to Internet Access
- D. Right of Privacy

Correct Answer: D

QUESTION 11

Smith, an employee of a reputed forensic investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in the hacking of the organization's DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry keys will Smith check to find the above information?

- A. TypedURLs key
- B. MountedDevices key
- C. UserAssist Key
- D. RunMRU key

Correct Answer: D

QUESTION 12

Which of the following tool captures and allows you to interactively browse the traffic on a network?

- A. Security Task Manager
- B. Wireshark
- C. ThumbsDisplay
- D. RegScanner

Correct Answer: B

QUESTION 13

One way to identify the presence of hidden partitions on a suspect's hard drive is to:

- A. Add up the total size of all known partitions and compare it to the total size of the hard drive
- B. Examine the FAT and identify hidden partitions by noting an H in the partition Type field
- C. Examine the LILO and note an H in the partition Type field

D. It is not possible to have hidden partitions on a hard drive

Correct Answer: A

QUESTION 14

Which code does the FAT file system use to mark the file as deleted?

- A. ESH
- B. 5EH
- C. H5E
- D. E5H

Correct Answer: D

QUESTION 15

A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

```
2007-06-14 13:59:05 192.168.254.1 action=Permit sent=16369 rcvd=180962 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 13:59:06 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 13:59:07 192.168.254.1 action=Permit sent=844 rcvd=486 src=24.119.229.125 dst=10.120.10.123 src_port=38660 d
2007-06-14 13:59:07 192.168.254.1 action=Permit sent=545 rcvd=404 src=192.168.254.80 dst=208.186.166.68 src_port=15113
2007-06-14 13:59:07 192.168.254.1 action=Permit sent=545 rcvd=404 src=192.168.254.80 dst=208.186.166.68 src_port=14857
2007-06-14 13:59:07 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 13:59:09 192.168.254.1 action=Permit sent=13365 rcvd=149662 src=70.185.198.247 dst=10.120.10.122 src_port=61
2007-06-14 13:59:09 192.168.254.1 action=Permit sent=691 rcvd=415 src=70.185.198.247 dst=10.120.10.123 src_port=48392 d
2007-06-14 13:59:09 192.168.254.1 action=Permit sent=12219 rcvd=140495 src=70.185.206.122 dst=10.120.10.122 src_port=51
2007-06-14 13:59:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 13:59:10 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 18:34:04 192.168.254.1 action=Permit sent=3038 rcvd=34134 src=70.185.198.247 dst=10.120.10.122 src_port=4480
2007-06-14 18:34:05 192.168.254.1 action=Permit sent=795 rcvd=6686 src=70.185.198.247 dst=10.120.10.122 src_port=46344
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2780 rcvd=18874 src=70.185.198.247 dst=10.120.10.122 src_port=4532
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2737 rcvd=8922 src=24.119.169.162 dst=10.120.10.122 src_port=2689
2007-06-14 18:34:09 192.168.254.1 action=Permit sent=2054 rcvd=23150 src=70.185.198.247 dst=10.120.10.122 src_port=4695
2007-06-14 18:34:11 192.168.254.1 action=Permit sent=2632 rcvd=68608 src=70.185.198.247 dst=10.120.10.122 src_port=4711
2007-06-14 18:34:12 192.168.254.1 action=Permit sent=4121 rcvd=71135 src=24.119.169.162 dst=10.120.10.122 src_port=1665
2007-06-14 18:34:13 192.168.254.1 action=Permit sent=644 rcvd=1803 src=70.185.198.247 dst=10.120.10.122 src_port=47368
2007-06-14 11:47:20 192.168.254.1 action=Permit sent=725 rcvd=1115 src=70.185.198.247 dst=10.120.10.122 src_port=48136
2007-06-14 11:47:30 192.168.254.1 action=Permit sent=766 rcvd=415 src=70.185.206.122 dst=10.120.10.123 src_port=62212 d
2007-06-14 11:47:33 192.168.254.1 action=Permit sent=5054 rcvd=81723 src=24.119.169.162 dst=10.120.10.122 src_port=8959
2007-06-14 11:47:37 192.168.254.1 action=Permit sent=26296 rcvd=233409 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 11:47:40 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:47:41 192.168.254.1 action=Permit sent=18221 rcvd=210841 src=216.97.160.253 dst=10.120.10.122 src_port=49
2007-06-14 11:47:42 192.168.254.1 action=Permit sent=5741 rcvd=102596 src=24.119.169.162 dst=10.120.10.122 src_port=379
2007-06-14 11:47:43 192.168.254.1 action=Permit sent=2982 rcvd=24075 src=24.119.169.162 dst=10.120.10.122 src_port=641
2007-06-14 11:47:46 192.168.254.1 action=Permit sent=2557 rcvd=28655 src=24.119.169.162 dst=10.120.10.122 src_port=1600
2007-06-14 11:47:49 192.168.254.1 action=Permit sent=844 rcvd=461 src=24.119.169.162 dst=10.120.10.123 src_port=13185 d
2007-06-14 11:47:53 192.168.254.1 action=Permit sent=3348 rcvd=18192 src=24.119.169.162 dst=10.120.10.122 src_port=4737
2007-06-14 11:47:55 192.168.254.1 action=Permit sent=3760 rcvd=34120 src=24.119.169.162 dst=10.120.10.122 src_port=3713
2007-06-14 11:47:57 192.168.254.1 action=Permit sent=3664 rcvd=30265 src=24.119.169.162 dst=10.120.10.122 src_port=6785
2007-06-14 11:47:58 192.168.254.1 action=Permit sent=3406 rcvd=39223 src=24.119.169.162 dst=10.120.10.122 src_port=5761
2007-06-14 11:47:59 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:04 192.168.254.1 action=Permit sent=545 rcvd=404 src=192.168.254.42 dst=208.186.166.68 src_port=7696 d
2007-06-14 11:48:05 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:10 192.168.254.1 action=Permit sent=407 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=260 dst_po
2007-06-14 11:48:13 192.168.254.1 action=Permit sent=1040 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=41216 dst
2007-06-14 11:48:15 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:16 192.168.254.1 action=Deny sent=0 rcvd=11264 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
```

What can the investigator infer from the screenshot seen below?

- A. A smurf attack has been attempted
- B. A denial of service has been attempted

C. Network intrusion has occurred

D. Buffer overflow attempt on the firewall.

Correct Answer: C

[Latest 312-49 Dumps](#)

[312-49 PDF Dumps](#)

[312-49 VCE Dumps](#)