

312-49V10^{Q&As}

ECCouncil Computer Hacking Forensic Investigator (V10)

Pass EC-COUNCIL 312-49V10 Exam with 100% Guarantee

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

<https://www.pass2lead.com/312-49v10.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

Which of the following tool creates a bit-by-bit image of an evidence media?

- A. Recuva
- B. FileMerlin
- C. AccessData FTK Imager
- D. Xplico

Correct Answer: C

QUESTION 2

Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

- A. Phreaking
- B. Squatting
- C. Crunching
- D. Pretexting

Correct Answer: A

QUESTION 3

Study the log given below and answer the following question: Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169 Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482 Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53 Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21 Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53 Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111 Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80 Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53 Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53 Apr 26 06:44:25 victim7 PAM_pwd[12509]: (login) session opened for user simple by (uid=0) Apr 26 06:44:36 victim7 PAM_pwd[12521]: (su) session opened for user simon by simple(uid=506)

Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

- A. Disallow UDP 53 in from outside to DNS server
- B. Allow UDP 53 in from DNS server to outside
- C. Disallow TCP 53 in from secondaries or ISP server to DNS server
- D. Block all UDP traffic

Correct Answer: A

QUESTION 4

What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

- A. Copyright
- B. Design patent
- C. Trademark
- D. Utility patent

Correct Answer: D

QUESTION 5

An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: DiskandVen_Best_BuyandProd_Geek_Squad_U3andRev_6.15. What does the "Geek_Squad" part represent?

- A. Product description
- B. Manufacturer Details
- C. Developer description
- D. Software or OS used

Correct Answer: A