# 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.certbus.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



**QUESTION 1**

Andie, a network administrator, suspects unusual network services running on a windows system. Which of the following commands should he use to verify unusual network services started on a Windows system?

A. net serv

B. netmgr

C. lusrmgr

D. net start

Correct Answer: D

**QUESTION 2**

What is the size value of a nibble?

A. 0.5 kilo byte

B. 0.5 bit

C. 0.5 byte

D. 2 bits

Correct Answer: C

**QUESTION 3**

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 4**

A computer forensic report is a report which provides detailed information on the complete forensics investigation process.

A. True

B. False

Correct Answer: A

**QUESTION 5**

Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

A. Statement of personal or family history

B. Prior statement by witness

C. Statement against interest

D. Statement under belief of impending death

Correct Answer: D

**QUESTION 6**

Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive? 22,164 cylinders/disk 80 heads/cylinder 63 sectors/track

A. 53.26 GB

B. 57.19 GB

C. 11.17 GB

D. 10 GB

Correct Answer: A

**QUESTION 7**

The police believe that Mevin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions. They also suspect that he has been stealing, copying, and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspect door and searching his home and seizing all of his computer equipment if they haveis preventing the police from breaking down the suspect? door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

A. The USA Patriot Act

B. The Good Samaritan Laws

C. The Federal Rules of Evidence

D. The Fourth Amendment

Correct Answer: D

**QUESTION 8**

Smith, as a part his forensic investigation assignment, has seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data the mobile device. Smith found that the SIM was protected by a Personal identification Number (PIN) code but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He unsuccessfully tried three PIN numbers that blocked the SIM card. What Jason can do in this scenario to reset the PIN and access SIM data?

A. He should contact the device manufacturer for a Temporary Unlock Code (TUK) to gain access to the SIM

B. He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN

C. He should again attempt PIN guesses after a time of 24 hours

D. He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM

Correct Answer: D

**QUESTION 9**

Identify the attack from following sequence of actions? Step 1: A user logs in to a trusted site and creates a new session Step 2: The trusted site stores a session identifier for the session in a cookie in the web browser Step 3: The user is tricked to visit a malicious site Step 4: the malicious site sends a request from the user\\'s browser using his session cookie

A. Web Application Denial-of-Service (DoS) Attack

B. Cross-Site Scripting (XSS) Attacks

C. Cross-Site Request Forgery (CSRF) Attack

D. Hidden Field Manipulation Attack

Correct Answer: C

**QUESTION 10**

Which of the following is an iOS Jailbreaking tool?

A. Kingo Android ROOT

B. Towelroot

C. One Click Root

D. Redsn0w

Correct Answer: D

**QUESTION 11**

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 12**

Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

A. Search warrant

B. Subpoena

C. Wire tap

D. Bench warrant

Correct Answer: A

**QUESTION 13**

Attackers can manipulate variables that reference files with "dot-dot-slash (./)" sequences and their variations such as http://www.juggyDoy.corn/GET/process.php././././././././etc/passwd.

Identify the attack referred.

A. Directory traversal

B. SQL Injection

C. XSS attack

D. File injection

Correct Answer: A

**QUESTION 14**

When dealing with the powered-off computers at the crime scene, if the computer is switched off, turn it on

A. True

B. False

Correct Answer: B

**QUESTION 15**

When conducting computer forensic analysis, you must guard against _____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

A. Hard Drive Failure

B. Scope Creep

C. Unauthorized expenses

D. Overzealous marketing

Correct Answer: B