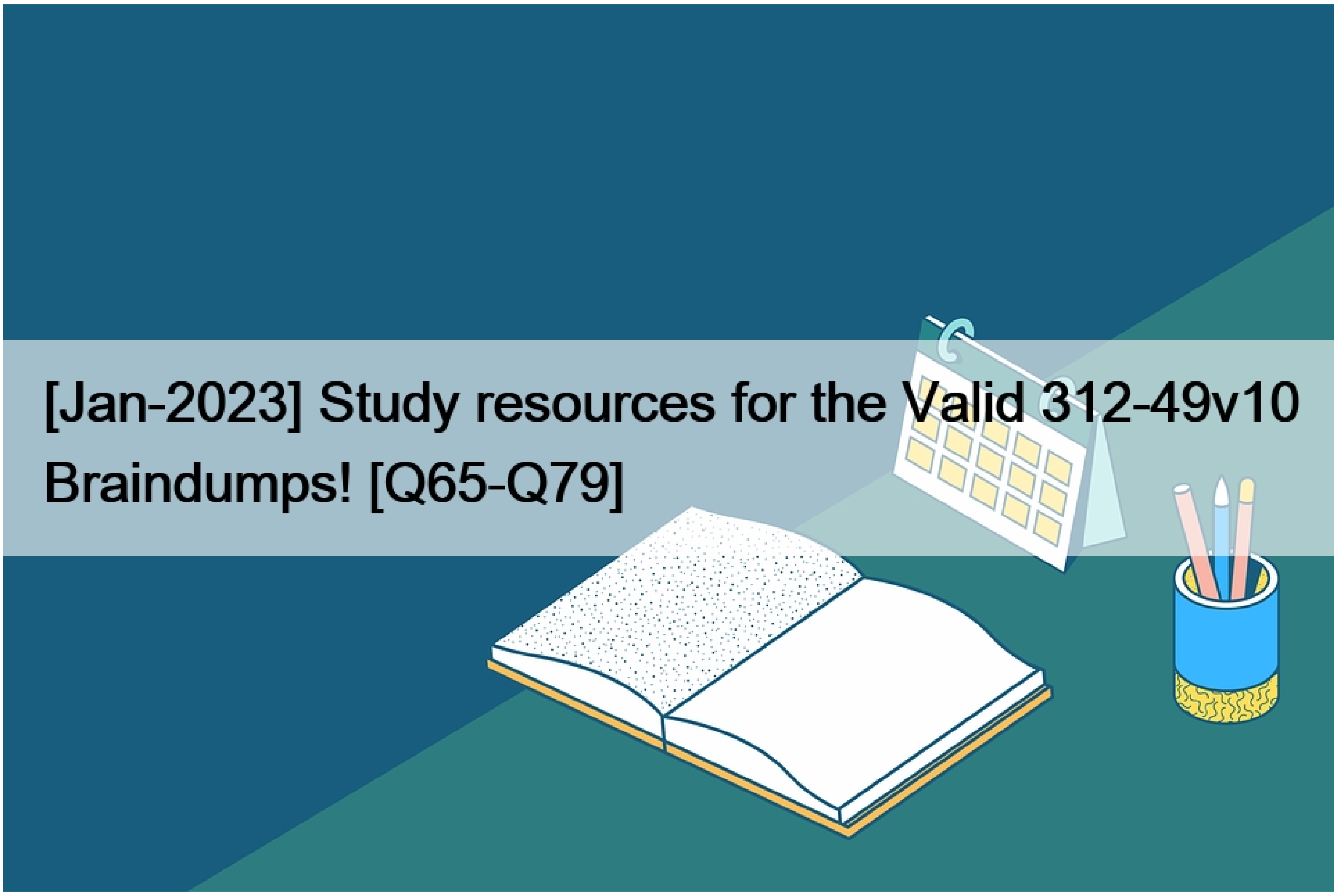
[Jan-2023 Study resources for the Valid 312-49v10 Braindumps! [Q65-Q79



[Jan-2023] Study resources for the Valid 312-49v10 Braindumps!
Updated 312-49v10 Tests Engine pdf - All Free Dumps Guaranteed!

NO.65 NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DDR). Which of the following is not a part of DDF?
* Encrypted FEK
* Checksum
* EFS Certificate Hash
* Container Name

NO.66 You have used a newly released forensic investigation tool, which doesn&#8217;t meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?
* The tool hasn&#8217;t been tested by the International Standards Organization (ISO)
* Only the local law enforcement should use the tool
* The total has not been reviewed and accepted by your peers
* You are not certified for using the tool

NO.67 You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.

What method would be most efficient for you to acquire digital evidence from this network?
* create a compressed copy of the file with DoubleSpace
* create a sparse data copy of a folder or file
* make a bit-stream disk-to-image file
* make a bit-stream disk-to-disk file

NO.68 What does ICMP Type 3/Code 13 mean?
* Host Unreachable
* Administratively Blocked
* Port Unreachable
* Protocol Unreachable

NO.69 Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?
* Safari
* Mozilla Firefox
* Microsoft Edge
* Google Chrome

NO.70 While collecting Active Transaction Logs using SQL Server Management Studio, the query Select * from ::fn_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, assigning NULL values implies?
* Start and end points for log sequence numbers are specified
* Start and end points for log files are not specified
* Start and end points for log files are specified
* Start and end points for log sequence numbers are not specified

NO.71 You should make at least how many bit-stream copies of a suspect drive?
* 1
* 2
* 3
* 4

NO.72 Which command can provide the investigators with details of all the loaded modules on a Linux-based system?
* list modules -a
* lsmod
* plist mod -a
* lsof -m

NO.73 An investigator wants to extract passwords from SAM and System Files. Which tool can the Investigator use to obtain a list of users, passwords, and their hashes In this case?
* PWdump7
* HashKey
* Nuix
* FileMerlin

NO.74 How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?
* 128
* 64

* 32
* 16

NO.75 An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?
* Smurf
* Ping of death
* Fraggle
* Nmap scan

NO.76 Which OWASP loT vulnerability talks about security flaws such as lack of firmware validation, lack of secure delivery, and lack of anti-rollback mechanisms on loT devices?
* Lack of secure update mechanism
* Use of insecure or outdated components
* Insecure default settings
* Insecure data transfer and storage

NO.77 Which of the following statements is TRUE about SQL Server error logs?
* SQL Server error logs record all the events occurred on the SQL Server and its databases
* Forensic investigator uses SQL Server Profiler to view error log files
* Error logs contain IP address of SQL Server client connections
* Trace files record, user-defined events, and specific system events

NO.78 Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri&#8217;s duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company&#8217;s switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?
* Trick the switch into thinking it already has a session with Terri&#8217;s computer
* Poison the switch&#8217;s MAC address table by flooding it with ACK bits
* Crash the switch with a DoS attack since switches cannot send ACK bits
* Enable tunneling feature on the switch

NO.79 During an Investigation. Noel found a SIM card from the suspect&#8217;s mobile. The ICCID on the card is

8944245252001451548.

What does the first four digits (89 and 44) In the ICCID represent?
* TAC and industry identifier
* Country code and industry identifier
* Industry identifier and country code
* Issuer identifier number and TAC

EC-COUNCIL 312-49v10 Exam Syllabus Topics:

TopicDetailsTopic 1- Defeating Anti-Forensics Techniques- Malware ForensicsTopic 2- Computer Forensics Investigation Process- Dark Web Forensics- Mobile ForensicsTopic 3- Data Acquisition and Duplication- Linux and Mac Forensics

312-49v10 Dumps Updated Practice Test and 705 unique questions:
https://www.validbraindumps.com/312-49v10-exam-prep.html]