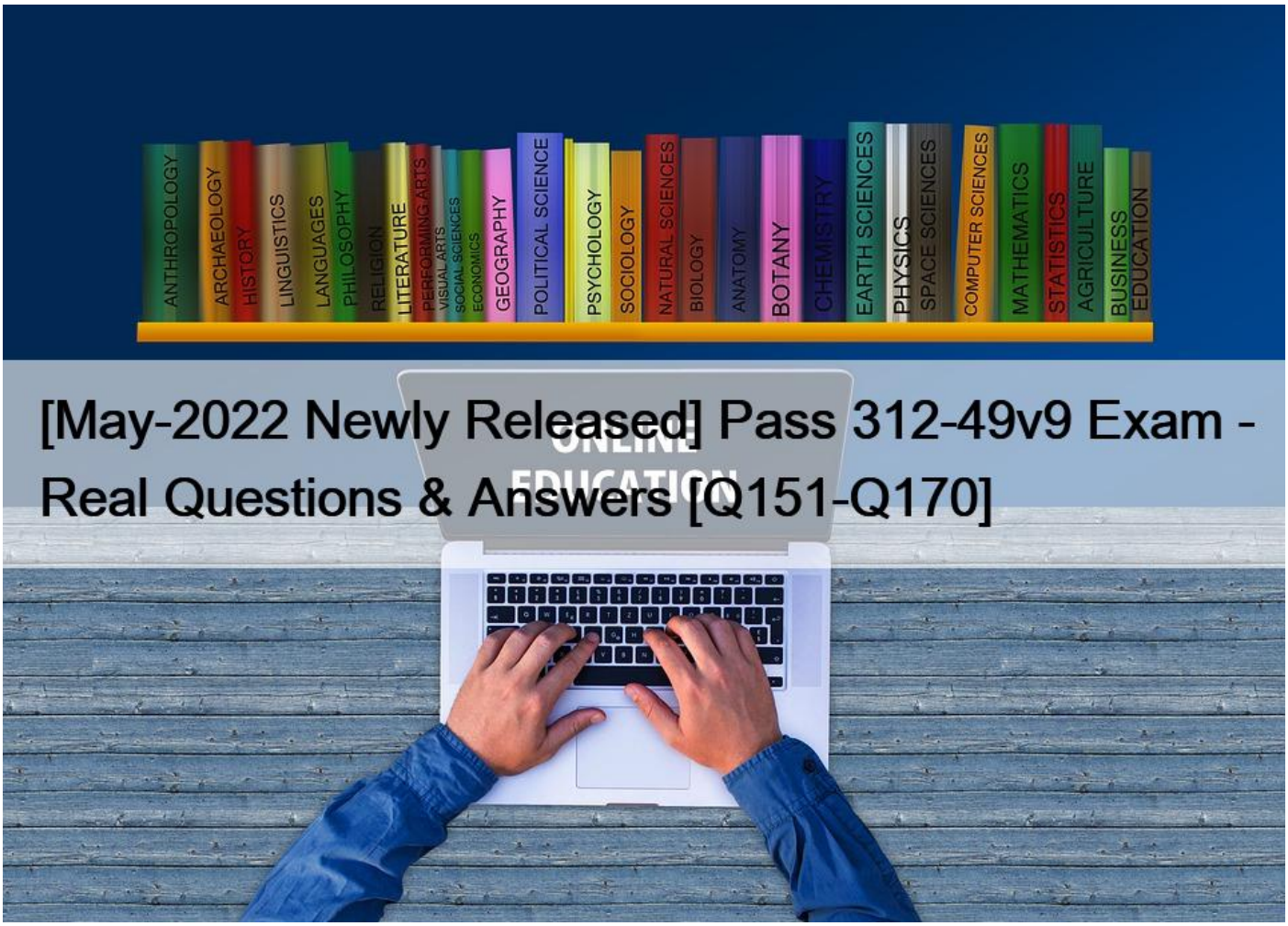
[May-2022 Newly Released Pass 312-49v9 Exam - Real Questions & Answers [Q151-Q170



[May-2022 Newly Released] Pass 312-49v9 Exam - Real Questions and Answers
Pass 312-49v9 Review Guide, Reliable 312-49v9 Test Engine

NEW QUESTION 151

What type of attack sends SYN requests to a target system with spoofed IP addresses?
* SYN flood
* Ping of death
* Cross site scripting
* Land

NEW QUESTION 152

Computer forensics report provides detailed information on complete computer forensics investigation process. It should explain how the incident occurred, provide technical details of the incident and should be clear to understand. Which of the following

attributes of a forensics report can render it inadmissible in a court of law?
* It includes metadata about the incident
* It includes relevant extracts referred to In the report that support analysis or conclusions
* It is based on logical assumptions about the incident timeline
* It maintains a single document style throughout the text

NEW QUESTION 153

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux.

Identify the Apache error log from the following logs.
* 127.0.0.1 – frank [10/0ct/2000:13:55:36 -0700]”GET I apache_pb.gif HTTP/ 1.0″ 200 2326
* [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/ home/live/ap/htdocs/test
* http://victim.com/scripts/..%c0%af../..%cOo/oaf

../..%c0%af../..%c0%af../..%c0%af../..

%c0%af../ ..

%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:Winntsystem32LogfilesW3S VC1
* 127.0.0.1 – – [10/Apr/2007:1 0:39:11 +0300]] [error] “GET I apache_pb.gif HTTP/ 1.0” 200

2326

NEW QUESTION 154

Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where “x” represents the

_____.
* Drive name
* Original file name’s extension
* Sequential number
* Original file name

NEW QUESTION 155

Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?
* ParentIDPrefix
* LastWrite
* UserAssist key
* MRUListEx key

NEW QUESTION 156

Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?
* Identifying File Dependencies
* Strings search

* Dynamic analysis
* File obfuscation

NEW QUESTION 157

Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?
* HIPAA
* GLBA
* SOX
* FISMA

NEW QUESTION 158

You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?
* To control the room temperature
* To strengthen the walls, ceilings, and floor
* To avoid electromagnetic emanations
* To make the lab sound proof

NEW QUESTION 159

CAN-SPAM Act requires that you:
* Don’t tell the recipients where you are located
* Don’t identify the message as an ad
* Don’t use deceptive subject lines
* Don’t use true header information

NEW QUESTION 160

What is the smallest physical storage unit on a hard drive?
* Track
* Cluster
* Sector
* Platter

NEW QUESTION 161

In a Linux-based system, what does the command “Last -F” display?
* Recently opened files
* Login and logout times and dates of the system
* Last functions performed
* Last run processes

NEW QUESTION 162

When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called “INF02” in the Recycled folder. If the INF02 file is deleted, it is re-created when you_____.
* Restart Windows

* Kill the running processes in Windows task manager
* Run the antivirus tool on the system
* Run the anti-spyware tool on the system

NEW QUESTION 163

Which of the following commands shows you all of the network services running on Windowsbased servers?
* Net start
* Net config
* Net Session
* Net use

NEW QUESTION 164

After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?
* PRIV.STM
* PUB.EDB
* PRIV.EDB
* PUB.STM

NEW QUESTION 165

If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?
* The system files have been copied by a remote attacker
* The system administrator has created an incremental backup
* The system has been compromised using a t0rn rootkit
* Nothing in particular as these can be operational files

NEW QUESTION 166

When collecting evidence from the RAM, where do you look for data?
* Swap file
* SAM file
* Data file
* Log file

NEW QUESTION 167

If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?
* The system has been compromised using a t0rnrootkit
* The system administrator has created an incremental backup
* The system files have been copied by a remote attacker
* Nothing in particular as these can be operational files

NEW QUESTION 168

At what layer does a cross site scripting attack occur on?
* Presentation
* Application

* Session
* Data Link

NEW QUESTION 169

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?
* Passwords of 14 characters or less are broken up into two 7-character hashes
* A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
* Networks using Active Directory never use SAM databases so the SAM database pulled was empty
* The passwords that were cracked are local accounts on the Domain Controller

NEW QUESTION 170

Task list command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.

Which of the following task list commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?
* tasklist/s
* tasklist/u
* tasklist/p
* tasklist/V

EC-COUNCIL 312-49v9 Exam Syllabus Topics:

TopicDetailsTopic 1- InvestigatTopic 2- Data Acquisition and DuplicationTopic 3- Computer Forensics Investigation ProcessTopic 4 - Network Forensics