

312-50V9^{Q&As}

Certified Ethical Hacker Exam V9

**Pass EC-COUNCIL 312-50V9 Exam with 100%
Guarantee**

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

<https://www.leads4pass.com/312-50v9.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

(Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.). Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal? What is odd about this attack? Choose the best answer.

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP TTL:44 TOS:0x10 ID:242
```

```
***FRP** Seq: OXA1D95 Ack: 0x53 Win: 0x400
```

```
...
```

```
05/20-17:06:58.685879 192.160.13.4:31337 ->
```

```
172.16.1.101:1024
```

```
TCP TTL:44 TOS:0x10 ID:242
```

```
***FRP** Seq: OXA1D95 Ack: 0x53 Win: 0x400
```

- A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
- B. This is back orifice activity as the scan comes from port 31337.
- C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.
- D. These packets were crafted by a tool, they were not created by a standard IP stack.

Correct Answer: B Section: (none)

QUESTION 2

What is not a PCI compliance recommendation?

- A. Limit access to card holder data to as few individuals as possible.
- B. Use encryption to protect all transmission of card holder data over any public network.
- C. Rotate employees handling credit card transactions on a yearly basis to different departments.
- D. Use a firewall between the public network and the payment card data.

Correct Answer: C Section: (none)

QUESTION 3

You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.

```
route add 10.0.0.0 mask 255.0.0.0 10.0.0.1 route add 0.0.0.0 mask 255.0.0.0 199.168.0.1
```

What is the main purpose of those static routes?

- A. Both static routes indicate that the traffic is external with different gateway.
- B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
- C. Both static routes indicate that the traffic is internal with different gateway.
- D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

Correct Answer: D Section: (none)

QUESTION 4

Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.

What do you think Tess King is trying to accomplish? Select the best answer.

- A. A zone harvesting
- B. A zone transfer
- C. A zone update
- D. A zone estimate

Correct Answer: B Section: (none)

QUESTION 5

When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

- A. Network tap
- B. Layer 3 switch
- C. Network bridge
- D. Application firewall

Correct Answer: A Section: (none)

[312-50V9 PDF Dumps](#)

[312-50V9 Study Guide](#)

[312-50V9 Braindumps](#)