



# 312-50V8<sup>Q&As</sup>

Certified Ethical Hacker v8

## Pass NetApp 312-50V8 Exam with 100% Guarantee

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

<https://www.passapply.com/312-50v8.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by NetApp  
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



**QUESTION 1**

Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

- A. Truecrypt
- B. Sub7
- C. Nessus
- D. Clamwin

Correct Answer: C

---

**QUESTION 2**

A common technique for luring e-mail users into opening virus-launching attachments is to send messages that would appear to be relevant or important to many of their potential recipients. One way of accomplishing this feat is to make the virus-carrying messages appear to come from some type of business entity retailing sites, UPS, FEDEX, CITIBANK or a major provider of a common service.

Here is a fraudulent e-mail claiming to be from FedEx regarding a package that could not be delivered. This mail asks the receiver to open an attachment in order to obtain the FEDEX tracking number for picking up the package. The attachment contained in this type of e-mail activates a virus.



#### Fake E-mail

From: FEDEX Packet Service  
Subject: FEDEX Packet N0328795951

Dear Sir/Madam,

Unfortunately we were not able to deliver postal package you sent on July the 1st in time because the recipient's address is not correct.

Please print out the invoice copy attached and collect the package at our office.

Your Sincerely FEDEX

[File Attached: Fedex-Tracking-number.zip]

#### Legit E-mail

Be alert for fraudulent e-mails claiming to be from FedEx regarding a package that could not be delivered. These e-mails ask the receiver to open an attachment in order to obtain the airbill or invoice for picking up the package. The attachment contained in this type of e-mail activates a virus. DO NOT OPEN the attachment. Instead, delete the e-mail immediately.

These fraudulent e-mails are the unauthorized actions of third parties not associated with FedEx. When FedEx sends e-mails with tracking updates for undeliverable packages, we do not include attachments.

FedEx does not request, via unsolicited mail or e-mail, payment or personal information in return for goods in transit or in FedEx custody. If you have received a fraudulent e-mail that claims to be from FedEx, you can report it by forwarding it to [abuse@fedex.com](mailto:abuse@fedex.com).

If you have any questions or concerns about services provided by FedEx, please review our services at [fedex.com/us/services](http://fedex.com/us/services) or contact FedEx Customer Service at 1.800.GoFedEx 1.800.463.3339.

Vendors send e-mails like this to their customers advising them not to open any files attached with the mail, as they do not include attachments.

Fraudulent e-mail and legit e-mail that arrives in your inbox contain the fedex.com as the sender of the mail.

How do you ensure if the e-mail is authentic and sent from fedex.com?

- A. Verify the digital signature attached with the mail, the fake mail will not have Digital ID at all
- B. Check the Sender ID against the National Spam Database (NSD)
- C. Fake mail will have spelling/grammatical errors
- D. Fake mail uses extensive images, animation and flash content

Correct Answer: A



### QUESTION 3

A specific site received 91 ICMP\_ECHO packets within 90 minutes from 47 different sites.

77 of the ICMP\_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP\_ECHO packets had an ICMP ID:0 and Seq:0.

What can you infer from this information?

- A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
- B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
- C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
- D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Correct Answer: B

---

### QUESTION 4

Blane is a security analyst for a law firm. One of the lawyers needs to send out an email to a client but he wants to know if the email is forwarded on to any other recipients. The client is explicitly asked not to resend the email since that would be a violation of the lawyer's and client's agreement for this particular case.

What can Blane use to accomplish this?

- A. He can use a split-DNS service to ensure the email is not forwarded on.
- B. A service such as HTTrack would accomplish this.
- C. Blane could use MetaGoofil tracking tool.
- D. Blane can use a service such as ReadNotify tracking tool.

Correct Answer: D

---

### QUESTION 5

How does traceroute map the route a packet travels from point A to point B?

- A. Uses a TCP timestamp packet that will elicit a time exceeded in transit message
- B. Manipulates the value of the time to live (TTL) within packet to elicit a time exceeded in transit message
- C. Uses a protocol that will be rejected by gateways on its way to the destination
- D. Manipulates the flags within packets to force gateways into generating error messages

Correct Answer: B

---



VCE & PDF

PassApply.com

<https://www.passapply.com/312-50v8.html>

2024 Latest passapply 312-50V8 PDF and VCE dumps Download

---

[312-50V8 Practice Test](#)

[312-50V8 Study Guide](#)

[312-50V8 Braindumps](#)