



# ECSS<sup>Q&As</sup>

EC-Council Certified Security Specialist Practice Test

**Pass EC-COUNCIL ECSS Exam with 100% Guarantee**

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

<https://www.geekcert.com/ecss.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

John works as a professional Ethical Hacker. He has been assigned a project to test the security of [www.we-are-secure.com](http://www.we-are-secure.com). He performs Web vulnerability scanning on the We-are-secure server. The output of the scanning test is as follows:

```
C:\whisker.pl -h target_IP_address-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - - - - - == Host:
target_IP_address= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
```

```
+ 200 OK: HEAD /cgi-bin/printenv
```

John recognizes `/cgi-bin/printenv` vulnerability (`\\Printenv\\` vulnerability) in the `We_are_secure` server. Which of the following statements about `\\Printenv\\` vulnerability are true? Each correct answer represents a complete solution. Choose all that apply.

- A. This vulnerability helps in a cross site scripting attack.
- B. `\\Printenv\\` vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.
- C. With the help of `\\printenv\\` vulnerability, an attacker can input specially crafted links and/or other malicious scripts.
- D. The countermeasure to `\\printenv\\` vulnerability is to remove the CGI script.

Correct Answer: ACD

---

### QUESTION 2

In which of the following techniques does an attacker take network traffic coming towards a host at one port and forward it from that host to another host?

- A. Firewalking
- B. Snooping
- C. Port redirection
- D. UDP port scanning

Correct Answer: C

---

### QUESTION 3

Maria works as a Desktop Technician for PassGuide Inc. She has received an e-mail from the MN

Compensation Office with the following message:

Dear Sir/Madam,

My name is Edgar Rena, the director of compensation here at the MN Compensation Office in Chicago. We receive so



many complaints about fraudulent activities that have been taking place in your region for the past few years. Due to the

high volume loss of money, the MN compensation department has had an agreement with the appropriate authority to compensate each victim with a sum of USD\$500,000.00.

You were selected among the list of people to be paid this sum. To avoid any imperative mood by intending scammers, your payment has been transmuted into an International bank draft which can be cashed at any local bank in your

country.

Please fill the below details and send it to our secretary for your compensation bank draft.

Full name:

Address:

Tel:

Fill and Send to:

Dr. Michael Brown

MN Compensation Office, IL

Tel: +1-866-233-8434

Email: micbrown@live.com

Further instructions shall be given to you by our secretary as soon as you contact him. To avoid losing your compensation, you are requested to pay the sum of \$350 for Insurance Premium to our secretary.

Thanks and God bless.

If Maria replies to this mail, which of the following attacks may she become vulnerable to?

- A. Phishing attack
- B. SYN attack
- C. CookieMonster attack
- D. Mail bombing

Correct Answer: A

---

#### QUESTION 4

Which of the following attacks is used to hack simple alphabetical passwords?

- A. Man-in-the-middle attack
- B. Dictionary-based attack
- C. Black hat attack



D. Sniffing

Correct Answer: B

---

#### QUESTION 5

You work as a Network Security Administrator for NetPerfect Inc. The company has a Windowsbased network. You are incharge of the data and network security of the company. While performing a threat log analysis, you observe that one of the database administrators is pilfering confidential data. What type of threat is this?

A. Malware

B. External threat

C. Internal threat

D. Zombie

Correct Answer: C

[Latest ECSS Dumps](#)

[ECSS Study Guide](#)

[ECSS Exam Questions](#)