

ECSS^{Q&As}

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.leads4pass.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

Which of the following protocols of the TCP/IP suite is used in the application layer of the OSI model?

- A. DCAP
- B. OSPF
- C. ARP
- D. Telnet

Correct Answer: D

QUESTION 2

Which of the following Trojans opens a very large number of Web browser windows?



- A. Backdoor.Zagaban
- B. Wmpscfgs.exe
- C. Back Orifice
- D. JS.WindowsBomb

Correct Answer: D

QUESTION 3

You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below: What is the IP address of the sender of this email?

```

X-Apparently-To: itzme_adee@yahoo.com via 209.191.91.180; Mon, 10 Aug 2009 07:59:47 -0700
Return-Path: <bounce@wetpaintmail.com>
X-YahooFilteredBulk: 216.168.54.25
X-YMailISG: lI0jRIWLDshqPeX9g5WgzYv2NbqcgrXw47uBekfvpP65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.cmku96g9o8ggD
X-Originating-IP: [216.168.54.25]
Authentication-Results: mta251.mail.re3.yahoo.com from=wetpaintmail.com; domainkeys=pass (ok)
Received: from 216.168.54.25 (EHLO mail.wetpaintmail.com) (216.168.54.25) by mta251.mail.re3.yahoo.com with SMTP
Received: from wetpaintmail.com ([172.16.10.90]) by mail.wetpaintmail.com (StrongMail Enterprise 4.1.1.1(4.1.1-448:
X-VirtualServer: Digest, mail.wetpaintmail.com, 172.16.10.93
X-VirtualServerGroup: Digest
X-MailingID: 1181167079::64600::1249057716::9100::1133::1133
X-SMHeaderMap: mid="X-MailingID"
X-Mailer: StrongMail Enterprise 4.1.1.1(4.1.1-44827)
X-Destination-ID: itzme_adee@yahoo.com
X-SMFBL: aXR6bWVfYWRLZUB5YWhvby5jb20=
DomainKey-Signature: a=rsa-sha1; c=noofs; s=customer; d=wetpaintmail.com; q=dns; b=Yv6LNRzb+8Jaik8frIKfeO2WPnPkJMsJ1F
Content-Transfer-Encoding: 7bit
Content-Type: multipart/alternative; boundary="-----_NextPart_0F9_1F0B_2109CDA4,577F5A4D"
Reply-To: <no-reply@wetpaintmail.com>
MIME-Version: 1.0
Message-ID: <1181167079.1133@wetpaintmail.com>
Subject: The Ethical Hacking Weekly Digest
Date: Mon, 10 Aug 2009 07:37:02 -0700
To: itzme_adee@yahoo.com
From:  The Ethical Hacking <info@wetpaintmail.com> 
Content-Length: 35382
    
```

- A. 209.191.91.180
- B. 216.168.54.25
- C. 172.16.10.90
- D. 141.1.1.1

Correct Answer: B

QUESTION 4

Fill in the blank with the appropriate name of the attack. takes best advantage of an existing authenticated connection

Correct Answer: session hijacking

QUESTION 5

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

Which of the following tools is John using to crack the wireless encryption keys?

A. Cain

B. Kismet

C. PsPasswd

D. AirSnort

Correct Answer: D

[Latest ECSS Dumps](#)

[ECSS VCE Dumps](#)

[ECSS Braindumps](#)