

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.certbus.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 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

QUESTION 2

Which of the following password cracking attacks does not use any software for cracking e-mail passwords? Each correct answer represents a complete solution. Choose all that apply.

- A. Brute force attack
- B. Shoulder surfing
- C. Social engineering
- D. Dictionary attack

Correct Answer: BC

QUESTION 3

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 4

Which of the following is a transport layer circuit-level proxy server?

- A. Bastion host
- B. UDP proxy
- C. SOCKS
- D. Forced proxy

Correct Answer: C

QUESTION 5

Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?

- A. Initial analysis, request for service, data collection, data reporting, data analysis
- B. Request for service, initial analysis, data collection, data reporting, data analysis
- C. Request for service, initial analysis, data collection, data analysis, data reporting
- D. Initial analysis, request for service, data collection, data analysis, data reporting

Correct Answer: C

QUESTION 6

Peter works as a professional Computer Hacking Forensic Investigator for eLaw-Suit law firm. He is working on a case of a cyber crime. Peter knows that the good investigative report should not only communicate the relevant facts, but also present expert opinion. This report should not include the cases in which the expert acted as a lay witness. Which of the following type of witnesses is a lay witness?

- A. One who can give a firsthand account of something seen, heard, or experienced.
- B. One with special knowledge of the subject about which he or she is testifying.
- C. One who observes an event.
- D. One who is not qualified as an expert witness.

Correct Answer: D

QUESTION 7

Which of the following organizations is dedicated to computer security research and information sharing?

- A. NIPC
- B. FBI
- C. Honeynet Project
- D. IEEE

Correct Answer: C

QUESTION 8

Which of the following protocols is used the most by web servers?

- A. COM
- B. FTP
- C. HTTP
- D. ORG

Correct Answer: C

QUESTION 9

You work as a Network Administrator for Infonet Inc. The company's office has a wireless network. Wireless access point on the network works as a router and DHCP server. You want to configure a laptop to connect to the wireless network. What will you configure on the laptop to accomplish the task?

- A. Service Set Identifier
- B. Internet service provider's DNS server address
- C. Demilitarized zone
- D. I/O address

Correct Answer: A

QUESTION 10

Which of the following components are usually found in an Intrusion detection system (IDS)?

Each correct answer represents a complete solution. Choose two.

- A. Modem
- B. Console
- C. Sensor

D. Gateway

E. Firewall

Correct Answer: BC

QUESTION 11

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

A. Cyber law

B. Copyright law

C. Trademark law

D. Espionage law

Correct Answer: C

QUESTION 12

Which of the following functions does the RSA Digital Signature combine with public key algorithm to create a more secure signature?

A. %

B. \$


C. #

D. *

Correct Answer: C

QUESTION 13

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:

```
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: IIOjRIWLDshqPeX9g5WgzYv2NbcqgrXw47uBekfvpP65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.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: aXR6bWVfYWRIZUB5YWhvby5jb20=
DomainKey-Signature: a=rsa-sha1; c=noaws; 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
```

What is the IP address of the sender of this email?

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

Correct Answer: A

QUESTION 14

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. AirSnort
- B. Kismet
- C. PsPasswd
- D. Cain

Correct Answer: A

QUESTION 15

Which of the following attacks is used by attackers to access a company's internal network through its remote access system?

- A. Trojan horse
- B. Land attack
- C. War dialer
- D. Denial-of-Service (DoS) attack

Correct Answer: C

[Latest ECSS Dumps](#)

[ECSS PDF Dumps](#)

[ECSS Exam Questions](#)