



312-38^{Q&As}

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/312-38.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 policies to help define what users can and should do to use the network and organization of computer equipment?

- A. None
- B. IT policy
- C. user policy
- D. general policy
- E. remote access policy

Correct Answer: C

QUESTION 2

Fill in the blank with the appropriate term. is a protocol used to synchronize the timekeeping among the number of distributed time servers and clients.



Correct Answer: NTP

Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission.

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:



```
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: II0jRIWLDshqPeX9g5WgzYv2NbqcgrXv47uBekfvpP65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.cmkU96g9o8ggD
X-Originating-IP: [216.168.54.25]
Authentication-Results: mta251.mail.re3.yahoo.com from=vetpaintmail.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 SM
Received: from vetpaintmail.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-SMFBID: aXR6bWVfYWRIZUB5YWhvby5jb20=
DomainKey-Signature: a=rsa-sha1; c=noofs; s=customer; d=vetpaintmail.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. 209.191.91.180
- B. 141.1.1.1
- C. 172.16.10.90
- D. 216.168.54.25

Correct Answer: D

The IP address of the sender of this email is 216.168.54.25. According to the scenario, 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. Once you start to analyze the email header, you get an entry entitled as X-Originating-IP. You know that in Yahoo, the X-Originating-IP is the IP address of the email sender and in this case, the required IP address is 216.168.54.25. Answer options A, C, and B are incorrect. All these are the IP addresses of the Yahoo and Wetpaint servers.

QUESTION 4

Which of the following is a technique for gathering information about a remote network protected by a firewall?

- A. Firewalking
- B. Warchalking



C. Wardriving

D. Wardialing

Correct Answer: A

Fire walking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. If the firewall allows this crafted packet through, it forwards the packet to the next hop. On the next hop, the packet expires and elicits an ICMP "TTL expired in transit" message to the attacker. If the firewall does not allow the traffic, there should be no response, or an ICMP "administratively prohibited" message should be returned to the attacker. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall. The main drawback of this technique is that if an administrator blocks ICMP packets from leaving the network, it is ineffective. Answer option B is incorrect.

Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving. Answer option C is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources. Answer option D is incorrect. War dialing or wardialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers - hackers that specialize in computer security - for password guessing.

QUESTION 5

Which of the following is a device that provides local communication between the datalogger and a computer?

A. Controllerless modem

B. Optical modem

C. Acoustic modem

D. Short haul modem

Correct Answer: D

A short haul modem is a device that provides local communication between the datalogger and a computer with an RS-232 serial port. It transmits data up to 6.5 miles over a four-wire unconditioned line (two twisted pairs). Answer option B is incorrect. An optical modem is a device that is used for converting a computer's electronic signals into optical signals for transmission over optical fiber. It also converts optical signals from an optical fiber cable back into electronic signals. It provides higher data transmission rates because it uses extremely high capacity of the optical fiber cable for transmitting data. Answer option C is incorrect. An acoustic modem provides wireless communication under water. The optimum performance of a wireless acoustic modem system depends upon the speed of sound, water depth, existence of thermocline zones, ambient noise, and seasonal change. Answer option A is incorrect. A controllerless modem is a hardware-based modem that does not have the physical communications port controller circuitry. It is also known as WinModem or software modem. A controllerless modem is very inexpensive and can easily be upgraded with new software.



VCE & PDF

Pass4itSure.com

<https://www.pass4itsure.com/312-38.html>

2024 Latest pass4itsure 312-38 PDF and VCE dumps Download

[312-38 PDF Dumps](#)

[312-38 Practice Test](#)

[312-38 Exam Questions](#)