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.passapply.com/ecss.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Which of the following tools combines the functionality of the traceroute and ping programs in a single network diagnostic tool?

A. Conky

B. Mtr

C. Ntop

D. Cacti

Correct Answer: B

QUESTION 2

Adam works as a Security Analyst for Umbrella Inc. He is retrieving large amount of log data from syslog servers and network devices such as Router and switches. He is facing difficulty in analyzing the logs that he has retrieved. To solve this problem, Adam decides to use software called Sawmill. Which of the following statements are true about Sawmill?

Each correct answer represents a complete solution. Choose all that apply.

A. It is used to analyze any device or software package, which produces a log file such as Web servers, network devices (switches and routers etc.), syslog servers etc.

B. It incorporates real-time reporting and real-time alerting.

C. It comes only as a software package for user deployment.

D. It is a software package for the statistical analysis and reporting of log files.

Correct Answer: ABD

QUESTION 3

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

QUESTION 4

Which of the following Trojans is used by attackers to modify the Web browser settings?

A. Trojan.Lodear

B. Win32/Pacex.Gen

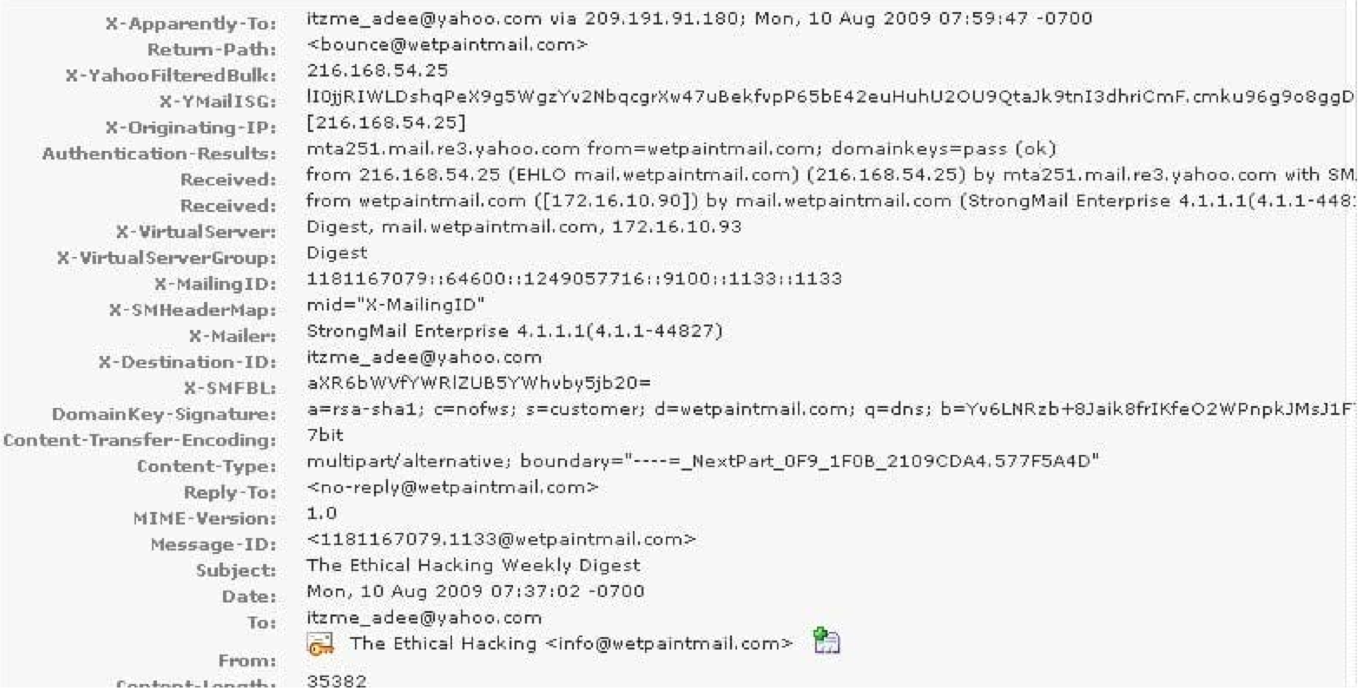
C. WMA/TrojanDownloader.GetCodec

D. Win32/FlyStudio

Correct Answer: D

QUESTION 5

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:  lI0jjRIWLDshqPeX9g5WgzYv2NbqcgrXw47uBekfvpP65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.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 SM
                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=nofws; 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
                           The Ethical Hacking <info@wetpaintmail.com>
                    From:
          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 6

Which of the following password cracking attacks is implemented by calculating all the possible hashes for a set of characters?

A. Rainbow attack

B. Dictionary attack

C. Brute force attack

D. SQL injection attack

Correct Answer: A

QUESTION 7

RRD Job World wants to upgrade its network. The company decides to implement a TCP/IP- based network. According to the case study, RRD Job World is concerned about security. Which of the following methods should the on-site employees use to communicate securely with the headquarters?

(Click the Exhibit button on the toolbar to see the case study.)

A. Basic (Clear Text) authentication using SSL

B. DNS security and group policies

C. L2TP over IPSec

D. Windows NT Challenge/Response (NTLM) authentication

Correct Answer: A

QUESTION 8

Sam, a malicious hacker, targets the electric power grid of Umbrella Inc. and gains access to the electronic control systems. Which of the following types of cybercrime has Sam performed?

A. Cyber defamation

B. Cybertrespass

C. Cyberterrorism

D. Cybertheft

Correct Answer: C

QUESTION 9

Burp Suite is a Java application for attacking web applications. This tool includes a proxy server, a spider, an intruder, and a repeater. Which of the following can be used to perform stress testing?

A. Repeater

B. Spider

C. Intruder

D. Proxy Server

Correct Answer: A

QUESTION 10

John works as a professional Ethical Hacker. He has been assigned a project to test the security of 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 11

Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

A. Digital certificates

B. Twofish

C. Public key

D. RSA

Correct Answer: AC

QUESTION 12

You work as a Network Administrator for ABC Inc. The company uses a secure wireless network.

John complains to you that his computer is not working properly. What type of security audit do you need to conduct to resolve the problem?

A. Independent audit

B. Operational audit

C. Non-operational audit

D. Dependent audit

Correct Answer: A

QUESTION 13

Firewalking is a technique that can be used to gather 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. Which of the following are pre-requisites for an attacker to conduct firewalking?

Each correct answer represents a complete solution. Choose all that apply.

A. ICMP packets leaving the network should be allowed.

B. An attacker should know the IP address of the last known gateway before the firewall.

C. There should be a backdoor installed on the network.

D. An attacker should know the IP address of a host located behind the firewall.

Correct Answer: ABD

QUESTION 14

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 15

Which of the following honeypots is a low-interaction honeypot and is used by companies or corporations for capturing limited information about malicious hackers?

A. Production honeypot

B. Research honeypot

C. Honeynet

D. Honeyfarm

Correct Answer: A

Latest ECSS Dumps ECSS Practice Test ECSS Braindumps