GISF Q&As

GIAC Information Security Fundamentals

Pass GIAC GISF Exam with 100% Guarantee

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

Which of the following processes is responsible for low risk, frequently occurring low cost changes?

A. Incident Management

B. IT Facilities Management

C. Request Fulfillment

D. Release Management

Correct Answer: C

QUESTION 2

Hardening a system is one of the practical methods of securing a computer system. Which of the following techniques is used for hardening a computer system?

A. Disabling all user accounts

B. Applying egress filtering

C. Applying Access Control List (ACL)

D. Applying a patch to the OS kernel

Correct Answer: D

QUESTION 3

You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

A. Containment

B. Preparation

C. Recovery

D. Identification

Correct Answer: A

QUESTION 4

Based on the case study, to implement more security, which of the following additional technologies should you implement for laptop computers?

(Click the Exhibit button on the toolbar to see the case study.) Each correct answer represents a complete

solution. Choose two.

A. Encrypted Data Transmissions

B. Digital certificates

C. Two-factor authentication

D. PAP authentication

E. Encrypting File System (EFS)

Correct Answer: BE

QUESTION 5

Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

A. Physical

B. Administrative

C. Automatic

D. Technical

Correct Answer: ABD

QUESTION 6

Which of the following combines the characteristics of a bridge and a router?

A. Firewall

B. Brouter

C. Switch

D. Hub

E. Repeater

Correct Answer: B

QUESTION 7

You work as a security manager for Qualxiss Inc. Your Company involves OODA loop for resolving and deciding over company issues. You have detected a security breach issue in your company.

Which of the following procedures regarding the breach is involved in the observe phase of the OODA loop?

A. Follow the company security guidelines.

B. Decide an activity based on a hypothesis.

C. Implement an action practically as policies.

D. Consider previous experiences of security breaches.

Correct Answer: A

QUESTION 8

Which of the following protocols implements VPN using IPSec?

A. SLIP

B. PPTP

C. PPP

D. L2TP

Correct Answer: D

QUESTION 9

You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project.

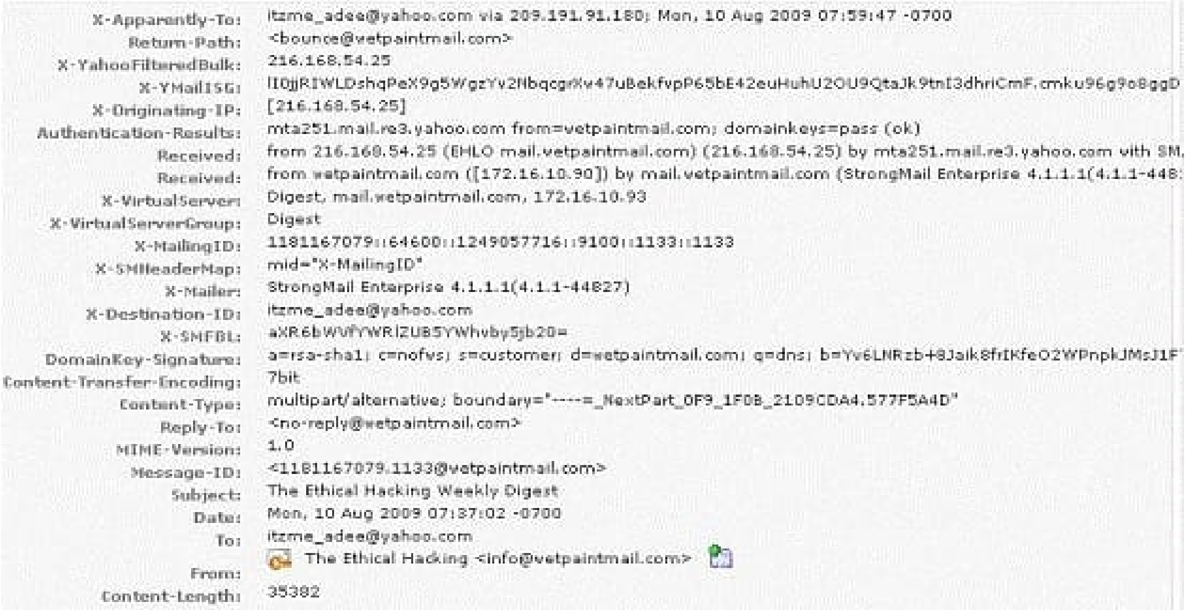
Now, you want to know the IP address of the sender so that you can analyze various information such as

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@vetpaintmail.com>
       X-YahooFilteredBulk:  216.168.54.25
               X-YMailISG:  II0jjRIWLDshqPeX9g5WgzYv2NbqcgrKv47uBekfvpP65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.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.vetpaintmail.com) (216.168.54.25) by mta251.mail.re3.yahoo.com with SM,
                 Received:  from vetpaintmail.com ([172.16.10.90]) by mail.vetpaintmail.com (StrongMail Enterprise 4.1.1.1(4.1.1-448:
          X-VirtualServer:  Digest, mail.vetpaintmail.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=vetpaintmail.com; q=dns; b=Yv6LNRzb+8Jaik8frIKfeO2WPnpkJMsJ1F
Content-Transfer-Encoding:  7bit
            Content-Type:  multipart/alternative; boundary="----=_NextPart_0F9_1F08_2109CDA4.577F5A4D"
                Reply-To:  <no-reply@vetpaintmail.com>
            MIME-Version:  1.0
              Message-ID:  <1181167079.1133@vetpaintmail.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@vetpaintmail.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

QUESTION 10

A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. IPChains

B. OpenSSH

C. Stunnel

D. IPTables

Correct Answer: D

QUESTION 11

You are responsible for virus protection for a large college campus. You are very concerned that your antivirus solution must be able to capture the latest virus threats. What sort of virus protection should you implement?

A. Network Based

B. Dictionary

C. Heuristic

D. Host based

Correct Answer: C

QUESTION 12

The Incident handling process implemented in an enterprise is responsible to deal with all the incidents regarding the enterprise. Which of the following procedures will be involved by the preparation phase of the Incident handling process?

A. Organizing a solution to remove an incident

B. Building up an incident response kit

C. Working with QA to validate security of the enterprise

D. Setting up the initial position after an incident

Correct Answer: B

QUESTION 13

Which of the following network connectivity devices translates one protocol into another and is used to connect dissimilar network technologies?

A. Hub

B. Firewall

C. Bridge

D. Gateway

Correct Answer: D

QUESTION 14

How should you configure the Regional Centers\\' e-mail, so that it is secure and encrypted? (Click the Exhibit button on the toolbar to see the case study.)

A. Use EFS.

B. Use IPSec.

C. Use S/MIME.

D. Use TLS.

Correct Answer: C

QUESTION 15

Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. Configuration Management is used for which of the following?

1.

To account for all IT assets

2.

To provide precise information support to other ITIL disciplines

3.

To provide a solid base only for Incident and Problem Management

4.

To verify configuration records and correct any exceptions

A. 2 and 4 only

B. 1, 3, and 4 only

C. 1, 2, and 4 only

D. 2, 3, and 4 only

Correct Answer: C

GISF VCE Dumps GISF Practice Test GISF Exam Questions