# Review Test Submission: Homework1

| | |
|---|---|
| User | Hong Zhang |
| Course | ITMS-448_IT-S-448-Parent.16S |
| Test | Homework1 |
| Started | 1/19/16 9:41 PM |
| Submitted | 1/24/16 12:08 PM |
| Due Date | 1/24/16 11:59 PM |
| Status | Completed |
| Attempt Score | 105 out of 120 points |
| Time Elapsed | 110 hours, 26 minutes |
| Results Displayed | Submitted Answers, Correct Answers, Feedback, Incorrectly Answered Questions |

## Question 1

30 out of 30 points

Download the HW1_Lab_Instructions from the Lab Instructions folder in Blackboard. Complete all of the steps in the lab and submit the requested screenshot from step 45 to answer this question.

Selected Answer: Capture.JPG

Response Feedback: [None Given]

## Question 2

41 out of 50 points View Rubric

Read the following whitepaper:

https://www.sans.org/reading-room/whitepapers/casestudies/breach-simulating-detecting-common-attack-36157

Pick two information security related items (these two items can be technical topics, concepts, or tools) in the whitepaper that you are not currently familiar with but find interesting. Research those two items and write a short 1.5 to 3 page double spaced 12pt font paper explaining what you learned about each one. No title or abstract pages are necessary. Upload the paper in .doc, .docx, or pdf format to answer this question. This paper should be completely in your own words. Therefore, do not use direct quotes from external sources. Please include a Bibliography page (on a separate page from your 1.5 to 3 pages of paper content) that lists the sources you used in your research. Wikis will not be considered valid research sources for this course. No screenshots or images may be used in this paper. As I am mainly concerned with your paper content, you do not need to format your Biblography in any specific format and do not need to include in-text citations for this particular paper.

Click the "View Rubric" button to view my grading structure for this assignment.

Selected Answer: ITMS - 448 _ HW1_Short Paper _ Hong Zhang.docx

Response Feedback: [None Given]

### Question 3

5 out of 5 points

✓ 1. Define confidentiality.

2. Provide three real world examples of attacks against confidentiality. (Don't use any of the examples from the lecture.)

Selected Answer:

Confidentiality: it is one principle of three core security principles. Confidentiality prevents unauthorized disclosure of information through Authentication / Access Controls / Authorization, or Cryptography /Encryption. It protects privacy of personal information, proprietary company information and health information (HIPAA).

Real world examples of attacks against confidentiality**:**

1. Heartland Payment Systems: It happened in March 2008. The impact was 134 million credit cards exposed through SQL injection to install spyware on Heartland's data systems.

2. ESTsoft: It happened between July-August 2011. The impact was the personal information of 35 million South Koreans was exposed after hackers breached the security of a popular software provider. South Korean news outlets reported that attackers with Chinese IP addresses uploaded malware to a server used to update ESTsoft's ALZip compression application.

3. *Dangdang.com*, one of China's biggest e-commerce websites: In April 2012, *Dangdang.com* declared their database was hacked. Form October 2011 to March 2012, More than 12 million users' information was leaked. Some users deposited some e-money in their accounts and hackers had taken the money out.

Correct Answer:

- Prevents unauthorized disclosure of information through:
  - Authentication/Access Controls/Authorization
  - Cryptography / Encryption
- Protects:
  - Privacy of personal information
  - Proprietary company information
  - Health information (HIPAA)

✓ Provide examples.

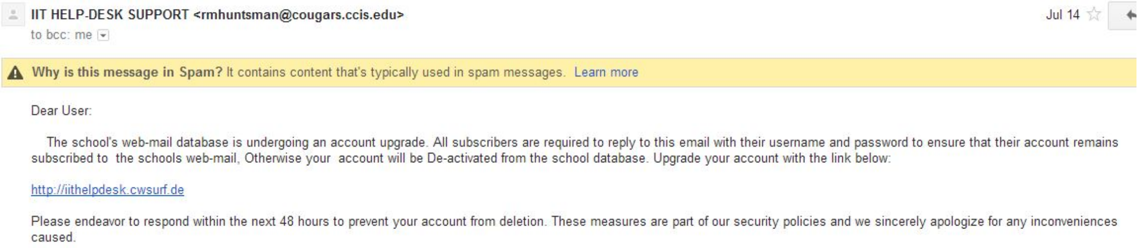
Response Feedback: [None Given]

## Question 4

5 out of 5 points

✓ Below is an email with headers. Is this a phishing email? If so, provide at least 4 reasons why you think it is.

Email:



IIT HELP-DESK SUPPORT <rmhuntsman@cougars.ccis.edu>

to bcc: me

Jul 14

Why is this message in Spam? It contains content that's typically used in spam messages. Learn more

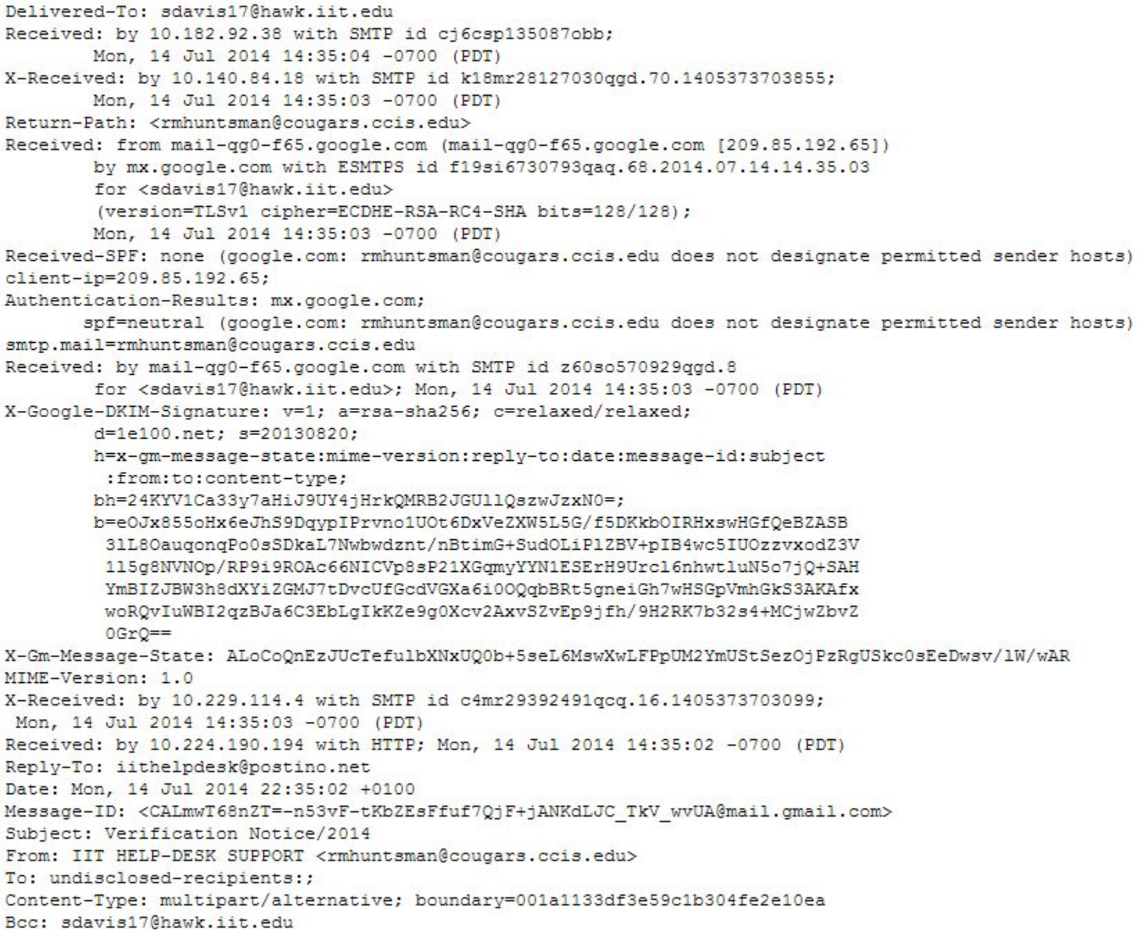
Dear User:

The school's web-mail database is undergoing an account upgrade. All subscribers are required to reply to this email with their username and password to ensure that their account remains subscribed to the schools web-mail, Otherwise your account will be De-activated from the school database. Upgrade your account with the link below:

http://iithelpdesk.cwsurf.de

Please endeavor to respond within the next 48 hours to prevent your account from deletion. These measures are part of our security policies and we sincerely apologize for any inconveniences caused.

Headers:



```
Delivered-To: sdavis17@hawk.iit.edu
Received: by 10.182.92.38 with SMTP id cj6csp135087obb;
        Mon, 14 Jul 2014 14:35:04 -0700 (PDT)
X-Received: by 10.140.84.18 with SMTP id k18mr28127030qgd.70.1405373703855;
        Mon, 14 Jul 2014 14:35:03 -0700 (PDT)
Return-Path: <rmhuntsman@cougars.ccis.edu>
Received: from mail-qg0-f65.google.com (mail-qg0-f65.google.com [209.85.192.65])
        by mx.google.com with ESMTPS id f19si6730793qaq.68.2014.07.14.14.35.03
        for <sdavis17@hawk.iit.edu>
        (version=TLSv1 cipher=ECDHE-RSA-RC4-SHA bits=128/128);
        Mon, 14 Jul 2014 14:35:03 -0700 (PDT)
Received-SPF: none (google.com: rmhuntsman@cougars.ccis.edu does not designate permitted sender hosts)
client-ip=209.85.192.65;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: rmhuntsman@cougars.ccis.edu does not designate permitted sender hosts)
smtp.mail=rmhuntsman@cougars.ccis.edu
Received: by mail-qg0-f65.google.com with SMTP id z60so570929qgd.8
        for <sdavis17@hawk.iit.edu>; Mon, 14 Jul 2014 14:35:03 -0700 (PDT)
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20130820;
        h=x-gm-message-state:mime-version:reply-to:date:message-id:subject
         :from:to:content-type;
        bh=24KYV1Ca33y7aHiJ9UY4jHrkQMRB2JGUllQszwJzxN0=;
        b=eOJx855oHx6eJhS9DqypIPrvno1UOt6DxVeZXW5L5G/f5DKkbOIRHxswHGfQeBZASB
         31L8OauqonqPo0sSDkaL7Nwbwdznt/nBtimG+SudOLiPlZBV+pIB4wc5IUOzzvxodZ3V
         115g8NVNOp/RP9i9ROAc66NICVp8sP21XGqmyYYN1ESErH9Urcl6nhwtluN5o7jQ+SAH
         YmBIZJBW3h8dXYiZGMJ7tDvcUfGcdVGXa6i0OQqbBRt5gneiGh7wHSGpVmhGkS3AKAfx
         woRQvIuWBI2qzBJa6C3EbLgIkKZe9g0Xcv2AxvSZvEp9jfh/9H2RK7b32s4+MCjwZbvZ
         0GrQ==
X-Gm-Message-State: ALoCoQnEzJUcTefulbXNxUQ0b+5seL6MswXwLFPpUM2YmUStSezOjPzRgUSkc0sEeDwsv/1W/wAR
MIME-Version: 1.0
X-Received: by 10.229.114.4 with SMTP id c4mr29392491qcq.16.1405373703099;
 Mon, 14 Jul 2014 14:35:03 -0700 (PDT)
Received: by 10.224.190.194 with HTTP; Mon, 14 Jul 2014 14:35:02 -0700 (PDT)
Reply-To: iithelpdesk@postino.net
Date: Mon, 14 Jul 2014 22:35:02 +0100
Message-ID: <CALmwT68nZT=-n53vF-tKbZEsFfuf7QjF+jANKdLJC_TkV_wvUA@mail.gmail.com>
Subject: Verification Notice/2014
From: IIT HELP-DESK SUPPORT <rmhuntsman@cougars.ccis.edu>
To: undisclosed-recipients:;
Content-Type: multipart/alternative; boundary=001a1133df3e59c1b304fe2e10ea
Bcc: sdavis17@hawk.iit.edu
```

Selected
Answer:

It is a phishing email.

Reasons:

1. Sender’s email address of IIT Help-Desk Support rmhuntsman@cougars.ccis.edu: It said this address from IIT Help-Desk Support but its address is not ending as @iit.edu or @hawk.iit.edu, some kind of official company email address. Usually, this kind of company email should use official company email address to send email.
2. Received: from mail-qg0-f65.googel.com (mail-qg0-f65.googel.com [209.85.192.65]): apparently, this email address is not IIT’s email and is a Google email account address. When I check the IP address for 209.85.192.65, it belongs to Google Company.
3. Received-SPF: none (googel.com: rmhuntsman@cougars.ccis.edu does not designate permitted sender hosts): it shows rmhuntsman@cougars.ccis.edu is not the sender’s real email address. None means the domain does not have an SPF record or the SPF record does not evaluate to a result.
4. spf = neutral (googel.com: rmhuntsman@cougars.ccis.edu does not designate permitted sender hosts): it proves the sender uses a fake email address. Neutral means the SPF record specifies explicitly that nothing can be said about validity.
5. Received: by mail-qg0-f65.googel.com with SMTP id z60so570929qgd.8: It shows the sender's email address.

Correct Answer: ✓ Yes, it is a phishing email.

1. "From:" field does not have iit.edu domain listed.
2. "Received: from field" is not an iit.edu domain or an ip address associated to iit.edu.
3. The message fails the SPF checks by the incoming mail server.
4. The link in the body of the message does not have an iit.edu domain and is from a foreign country.
5. The body of the message asks the user to send their username and password.

Response Feedback: [None Given]

## Question 5

5 out of 5 points

You should generally test and analyze malware samples on a computer used in a production system with full access to the corporate local area network. True or False?

Selected Answer: ✓ False

Correct Answer: ✓ False

Response Feedback: You should never test malware on a production system with network access to the local area network. A worm for example could easily spread and affect the entire organization. All malware should be tested in an isolated environment.

## Question 6

0 out of 5 points

✗ Explain what Defense in Depth means and why it is important.

Selected Answer:

Defense in Depth (also known as Castle Approach) is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. It means multiple layers protection for the system which includes perimeter firewall, IDS/IPS, UTM/Gateway Antivirus, department firewall, host firewall & antivirus and security patches/ limited privileges on the Host. These layers' logs will go to a computer for analyst monitoring.

Defense in Depth is important because it creates policy and hardens your network/systems. It can monitor your system and give you alert if hackers attack your system.

Correct Answer: ✓

An organization should never rely on a single method of security. For example, a company that only uses network antivirus such as on a UTM firewall but doesn't use client antivirus would risk malware getting past the network device and into the client systems. Defense in depth relies on using multiple levels of defense such as:
Perimeter Firewall
IDS/IPS
UTM/Gateway A/V
Department Firewall
Host Firewall & A/V
Security Patches / Limited Privileges on Host

Response Feedback: Your first sentence was plagiarized from Wikipedia. Since you did not plagiarize your entire answer, I will give you a warning this one time. If this happens again, I will need to submit an academic dishonesty report to the Dean's office and you will receive a zero for that entire assignment.

## Question 7

5 out of 5 points

✓ You are a security administrator for a Fortune 500 company. Your boss just heard about the heartbleed vulnerability and wants you to determine if any of your servers are affected. Your environment has Windows, Linux and Unix servers. How would you determine which servers were vulnerable and what would you do to fix them?

Selected Answer: Because Heartbleed vulnerability is in OpenSSL, it affects any OS or device with vulnerable version of OpenSSL which include Linux, Unix, OSX, etc. I will check these servers using OpenSSL.
The method for checking if system vulnerable is opening a terminal and run the command:

```
dpkg -l | grep openssl
```

By the way, if OpenSSL 's Version is 1.0.1k, it is not vulnerable.
Fixing steps as follows:
1. Upgrade version of OpenSSL to 1.0.1g or above.
The commands are:

```
apt-get update
apt-get install openssl
```

2. Take server offline
3. Generate new private/public keys

- Submit new public keys to certificate authority
- Install new certificate on server
- Ensure old key pairs are no longer being used

4. Bring server online
5. Revoke old certificates
6. Force password changes for users on server
7. Invalidate session keys

Correct Answer: ✓
Only servers using OpenSSL are vulnerable to heartbleed. Most are Linux and Unix servers running Apache and nginx web servers. Generally, Windows servers do not use OpenSSL. Once you located Linux and Unix servers running OpenSSL, you would need to look at the version. The OpenSSL 1.0.1g patch released in April 2014 fixes the bug. OpenSSL 1.0.1 though 1.0.1f are vulnerable and should be patched. You would also want to change keys, reissue certificates, and ask users to change their passwords if passwords were stored on that server.

Response Feedback: [None Given]

## Question 8

5 out of 5 points

Explain the difference between Authenticity and Authorization.

Selected Answer: Authentication is the process of confirming the identity of individuals requesting access to a secure environment. It is done by verifying the login and credentials match those created within that environment.
Authorization is the process of applying permissions to a user which ensures users requesting access have permission to do so. It is determined prior to a user obtaining authentication credentials. It can choose the most appropriate privileges for each user.

Generally, authentication is the process of verifying the identity of a user attempting to access a resource, whereas authorization is the process of verifying the user's permission to access a resource.

Correct ✓

Answer: A trusted individual can authenticate to a system with resources. Once authenticated, the invidual can only access resources they are authorized for.

Response Feedback: Again, make sure everything is completely in your own words.

## Question 9

4 out of 5 points

1. How does tor provide anonymity to the user? 2. What are some potential ways that the user's IP address may be leaked?

Selected Answer:

1. The solution is using tor. When you use tor, your delivering data packet will not have the regular header which like the normal network and do not offer the sender’s address. At the same time, tor encrypts this packet and picks a random encrypted path to destination server. If you go to another website, tor will help you choose another random encrypted path. Actually, tor hides the content of Internet traffic.

2. When the client use normal network to deliver data packet, the packet will include IP addresses from the client and the server in the header. Hence, when you check email header, use Web Real Time Communication (WebRTC) or wireshark (a network protocol analyzer), you can find the user's IP address.

Correct Answer: ✓

1. Tor sends traffic through various nodes in a random path to connect to a destination server. Your ISP can only see that you connected to the entrance node. Ultimately, the destination server only collects the IP address of the exit node, not the user's source IP address. Therefore, your ISP is not able to identify what websites you are browsing to and websites on the Internet you visit are not about to identify you by your IP address.
2. Active content such as Java, JS, Flash, Shockware, QuickTime, RealAudio, ActiveX Controls, and VBScript may be able to ignore configured tor proxy settings and share information (such as your IP address) directly to sites on the Internet. Active content services may also be able to store their own cookies which they may pass information directly to sites on the Internet.

Response Feedback: Only certain packets such as email would allow the revealing of the user's public IP. Regular http or https traffic would not.

## Question 10

5 out of 5 points

A user connects their browser to tor and browses to the web server at www.doge2048.com. Which IP address will the web server capture?

Selected Answer: ✓ IP address of tor exit node

Correct Answer: ✓ IP address of tor exit node

Thursday, February 18, 2016 9:13:04 AM CST

← OK