**Review Test Submission: Homework1**

### Question 3

1.  Define confidentiality.

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

•Prevents unauthorized disclosure of information through:

§Authentication/Access Controls/Authorization

§Cryptography / Encryption

•Protects:

§Privacy of personal information

§Proprietary company information

§Health information (HIPAA)

### Question 4

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

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.

### Question 5

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? False

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

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

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

### Question 7

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?

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.

### Question 8

Explain the difference between Authenticity and Authorization.

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

### Question 9

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

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.

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