Homework1:

3. Confidentiality: it is one core security principle. 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 c**onfidentiality:**

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.

4. It is a phishing email.

Reasons:

1. Sender’s email address for IIT Help-Desk Support [rmhuntsman@cougars.ccis.edu](mailto: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](mailto:rmhuntsman@cougars.ccis.edu) does not designate permitted sender hosts): it shows [rmhuntsman@cougars.ccis.edu](mailto: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](mailto: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

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. False

6. 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.

7. 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 | grepopenssl

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

1. Take server offline
2. 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

1. Bring server online
2. Revoke old certificates
3. Force password changes for users on server
4. Invalidate session keys

8. Explain the difference between Authenticity and Authorization.

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.

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. 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.

10. 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?

|  |  |  |
| --- | --- | --- |
|  |  | Source IP address of tor user |
|  |  | IP address of tor entry node |
|  |  | IP address of tor exit node |
|  |  | IP address of tor directory server |