INFO6003 Lab-02 Gathering Information

For this lab the student will explore the information available on security vulnerabilities from a variety of sources. Students need to record their answers and observations in the Word document associated with the Dropbox.

Not all links will work in this Lab. Answer all questions and number your answers.

Provide references to the web pages you use on a reference page.

If I ask you to describe, explain or summarize, that needs to be in your own words. If I just ask you for the recommended workaround for a specific vulnerability, copy and paste is fine.

Note: when copying and pasting, only copy the **relevant** information

Common Vulnerabilities and Exposures (CVE)

- Navigate to the **http://cve.mitre.org** web site.

- Read the statement provided on the main page regarding CVEs.

- On the left side under the heading About CVE, click on the Terminology link and read the definition of Vulnerability and Exposure.

1. **In the word document, summarize a Vulnerability and an Exposure, in your own words.**

- Back on the Mitre **home page**, in the body of the page, under the heading, “Wide Spread use of CVE” click on the **Vulnerability Management** Link.

- Click on the Organizations link in the table. This will give you an idea of the number of corporations using the CVE database in their commercial products.

- Go back to the previous table and click on the Product column, then find and select the item:
- **Symantec Security Response Web Site**

- This will link you to the Symantec Security Response Web Site: **http://www.symantec.com/security_response/**

- Take a look at the different security response tabs.

- Navigate to the Vulnerabilities Tab:

2. **For the first 20 vulnerabilities in the list, identify the organization, platform or group of organizations whose products are affected. (example below, you could have more or less)**
    - # are Microsoft vulnerabilities
    - # are Multi-Vendor vunlerabilities
    - # are Webkit vulnerabilities
    - # are Adobe vulnerabilities
    - Provide lots of detail in your answer regarding the various software versions.

Note: depending on when you do this, all the vulnerabilities could be from one company. Especially if it is close to patch Tuesday.

3. **Give a brief description of the first vulnerability in the list and then list the recommended actions**

Microsoft Security Bulletins

- Navigate to the **http://technet.microsoft.com/en-us/security/bulletin** web site.
- Scroll down to the "search by bulletin, KB, or CVE number" field then search for the Security Bulletin for **MS15-004**
- Click on the link and read the Executive Summary.
- Scroll down to see the Operating Systems / Application Versions affected by this bulletin.
- Scroll down further to the Vulnerability Information section.
  - Read a more detailed explanation of the vulnerability and the reference to the CVE bulletin that addresses this vulnerability.

4. **What vulnerability is addressed in this bulletin?**

Note: Provide the common name and the CVE identifier (hint: Vulnerability Information)

5. **What action does Microsoft recommend?**

(Recommendations and / or Workarounds) Provide specific instructions.

Repeat the steps above for MS15-002 to answer the next two questions

6. **What vulnerability is addressed in this bulletin?**

Note: Provide the common name and the CVE identifier (hint: Vulnerability Information)

7. **What action does Microsoft recommend?**

(Recommendations and / or Workarounds)

SANS Top Cyber Security Risks

Navigate to the **http://isc.sans.edu** web site

8. **What is the current Threat Level?** (If you don't see it right away, look harder)

9. **If you click on the current threat level you can view historical changes. What was the most recent event to trigger a threat level of Yellow?**

10. **(a) What event in April of 2014 triggered a threat level of Yellow? Click through and determine what you should do if you are vulnerable?**

As a last step, go the https://www.microsoft.com/en-us/msrc/technical-security-notifications site and investigate this offering.

- **(b) Try to sign up for your own** Email: **Security Notification Service** **using your FOL email account**. Is Microsoft going to let you?

  I would highly suggest setting yourself up with a Microsoft account if you don’t have one, so you can try this tool.