|  |  |
| --- | --- |
|  | CIS-1290 Principles of Information Security |

Topic 2 Assignment 2

|  |  |
| --- | --- |
| To: | Mike MacDonald |
| From: | Christopher Sigouin |
| Date: | January 30, 2015 |
| Subject: | Exercises 1 and 4 from the end of Chapter 2 |
|  |  |

The following exercises from chapter 2 of the textbook “Principles of Information Security” are listed below in bold. Answers to the specified exercises follow each one.

**Exercise #1: Consider the statement: an individual threat agent, like a hacker, can be a factor in more than one threat category. If a hacker hacks into a network, copies a few files, defaces the Web page, and steals credit card numbers, how many different threat categories does this attack fall into?**

In accordance with the statement: If a hacker hacks into a network, copies a few files, defaces the Web page, and steals credit card numbers, I believe that it would fall within 13 categories. The category and a brief explanation why is listed below:

* Compromises to intellectual property

*It is fairly clear that this category should be included as the statement specifies he “copies files“. The files are property of the particular organization.*

* Software attacks

*Again, it is very clear that this category should be included. The statement specifies that he “hacks” into the network. Utilization of software to produce the hack*

* Deviation in quality of service

*An ISP may have issues with their own network allowing private information about their clients to be accessible. This could increase the likelihood of the hack occurring. (WAN usernames or passwords)*

* Espionage or trespass

*The statement specifies that he “copies files” as well as “steals credit card numbers”.*

* Forces of nature

*Certain conditions (ie. Lightning) may affect an organizations networking equipment and could be the resulting factor of the hack.*

* Human error or failure

*People are a security threat. Someone within an organization stating something they should not have could profit a hacker and provide easy network access.*

* Information extortion

*Since the statement specifies that he “steals credit card numbers” would lead me to believe he may disclose, ransom or use blackmail type procedures*

* Missing, inadequate, or incomplete controls

*An organizations security technologies may not be functioning as they should and may be the resulting factor of the hack into the network.*

* Sabotage or vandalism

*The statement specifies that he “defaces the webpage” therefore this category counts.*

* Theft

*The statement specifies that the hacker “copies files” and “steals credit card numbers” therefore this category is included.*

* Technical hardware failures or errors

*Hardware failures could be the resulting factor of the hack occurring.*

* Technical software failures or errors

*Software failures could be the resulting factor of the hack occurring.*

* Technological obsolescence

*Outdated technologies that may have known vulnerabilities could be the resulting factor of the hack if not upgraded or updated.*

The category “Missing, inadequate, or incomplete” is the only one I could not construct a reason why the attack would fall under it. This category is directed towards loss of data due to technology failures.

**Exercise #4: The chapter discussed many threats and vulnerabilities to information security. Using the Web, find at least two other sources of information on threats and vulnerabilities. Begin with www.securityfocus.com and use a keyword search on "threats".**

Two sources of information for threats and vulnerabilities I located are listed below:

Open Source Vulnerability Database - <http://www.osvdb.org/>

OSVDB is an independent and open sourced web-based vulnerability database created for the security community. The goal of the project is to provide accurate, detailed, current, and unbiased technical information on security vulnerabilities. The project hopes to provide a truly comprehensive vulnerability database with extended features to better facilitate searching, information classification, and references. (Quoted from http://www.osvdb.org/about)

Common Vulnerabilities and Exposures - <https://cve.mitre.org/>

Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities. CVE’s common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization’s security tools. If a report from one of your security tools incorporates CVE Identifiers, you may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem. (Quoted from https://cve.mitre.org/)