This assignment has three goals:

1. Understanding the history and purpose of operational security (OPSEC)
2. Practice some basic procedures for operational security for an online investigation
3. Discuss how OPSEC can be used in everyday life

**What is Operations Security?**

We can define operational security (OPSEC) as a process of identifying the critical information that an adversary may want, and then protecting that information. Operations security is clearly important for the military, government, and businesses. Because of our networked world, it is becoming increasingly important for individuals as well. Individuals need to protect ourselves from cybercriminals.

This assignment will see you as someone preparing to do online investigations and needing to protect your critical information from the cybercriminals you are investigating. You will begin by reading a chapter from the book *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, by Jason Andress, and answering questions. Then you will do your own operations security – in effect securing \*your\* future operations as an investigator.

**Assignment Instructions**

This assignment is in three parts. Complete all parts on the same word document. Number each question and pay attention to the organization of your content so that it is readable and understandable. Use subheadings (Part I and Part II, etc). I personally put my screenshots in tables. You do not have to do this, but make sure that your screenshots are readable and organized.

**Part I – Reading and Critical Thinking (30 pts)**

Read the chapter “Operations Security”, by Jason Andress and answer these questions in a few sentences each.

1. **Describe how George Washington played a part in the origination of operations security?** **(5 pts.)** George Washington played a part in the origination of operations security by emphasizing that small items of information can potentially be beneficial once it is combined and creating an intelligence-gathering organization that executed its services privately.
2. **Describe how the first formal OPSEC methods arose?** **(5 pts.)** The First formal OPSEC methods arose during the Vietnam War when the United States conducted a study, Purple Dragon, to prevent their adversaries from obtaining details of their activities. The study mentioned two main ideas, which were first about the environment and spies. The second idea was that to solve a breach of information, a survey that inquiries about the information itself, vulnerability analysis, etc., must be performed. During this process, people administering the surveys created the phrase operations security.
3. **List the five stages of operational security.** **(5 pts.)** The five stages of operational security are the identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of countermeasures.
4. **What is the relationship between a threat, a vulnerability, and a risk?** **(5 pts.)** The relationship between a threat, a vulnerability, and a risk is that it will be considered a risk when there is a matching set of threats and vulnerabilities. This means that if there is an absence of one or both components, threats, and vulnerabilities, there will be no risks associated.
5. **Describe a threat, vulnerability, and risk that a college student may have.** **(5 pts.)** A hacker executing a phishing scam is sending an email to students specifically at ODU to recruit them for a potential internship, and to be considered for the internship, the students will need to disclose personal information. Threat: the hacker executing the phishing scam, the vulnerability: the student not being knowledgeable on phishing scams, and the risk: the personal information obtained by the hacker could be used to access your school account or for other nefarious purposes.

**Part II – Protecting Critical Information (60 pts)**

In this part of the assignment, you will go through a process of protecting the information that is critical to your operation as an investigator.  You will learn how to properly document images, and remove as many of your digital footprints as possible. They are equally important.  For this assignment, you will be using Firefox to browse the web and using Firefox add-ons to protect your information (you should also be able to use Chrome).

I would prefer that you download the portable version of Firefox onto your flash drive, and you can [use these instructions to do so.](https://docs.google.com/document/u/0/d/1c0LvAej0kZ5COVvF7mVt8T1fdzT2vutOxNP4seV-gss/edit) This will give you practice for using portable apps going forward. However, if you wish can use Firefox on your personal machine or the machine in the lab if it allows you.

Documenting Information by Using Nimbus

Nimbus is an excellent way of documenting what you do in your web browser. It cannot take screenshots of anything outside of your browser, but for documenting web evidence it is excellent. Install Nimbus by going to the icon to right of the address bar, clicking it and going to the “Add-ons and themes” link.  Search for Nimbus and add it to Firefox. If you are using the portable Firefox application, then your activity is being written to the USB (see image below).

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
|  |
| Graphical user interface, text, application  Description automatically generated |
| Graphical user interface, text, application, email  Description automatically generated |

Look for the Nimbus icon, click on it, and look for the “actions after capture” options and toggle to “edit” if it is not there already. Now, whenever you take a screenshot, you will automatically be sent to the edit screen where you can edit the shot.  The next few tasks are just practice with Nimbus.

1. Go to a website of your choosing. **(7.5 pts.)**

|  |
| --- |
| Graphical user interface, application  Description automatically generated |

* 1. Take a screenshot using the “visible part of page” (you may have to decrease the size of your web window before taking the screenshot to make sure all the information is recorded)
  2. Resize the picture so that the width is 2200 (keep the “proportional” box checked).
  3. Select two items on the page and write notes beside them. It does not matter what you write. It is just for practice.
  4. Number the notes using the number function.
  5. Save the screenshot and paste it into your assignment (under question 6)

1. Go to Amazon’s webpage **(7.5 pts.)**

|  |
| --- |
| A screenshot of a computer  Description automatically generated with low confidence |

* 1. Take a screenshot using “entire page” (you may have to decrease the size of your web window before taking the screenshot to make sure all the information is recorded)
  2. Resize the picture so that the width is 2200 (keep the “proportional” box checked).
  3. Blur the “Hello, Sign-In” section of the page
  4. Circle a product somewhere on the screen using a red pen. Write a note about the product.
  5. Save the screenshot and paste it into your assignment (under question 7)

1. Go to ODU’s webpage **(7.5 pts.)**

|  |
| --- |
| A screenshot of a video game  Description automatically generated |

* 1. Take a screenshot of any section of the page using “selected area”
  2. Point to something in that section using the “text arrow” option, and write something in the textbox. It doesn’t matter what you write.
  3. Save the screenshot and paste it into your assignment (under question 8)

Removing Digital Footprints by Using Firefox Multi-Account Containers

The Multi-Account Containers plug-in allows you to separate browsing sessions without needing to clear your history or using multiple browsers. Whatever you do in one container is not shared with another. This has several applications:

* You can log into several social media accounts at once (using different containers). This means you can browse social media with several different aliases.
* You can avoid being tracked with cookies. When you browse the web, you collect data and carry it with you. If you browse Amazon and then do a Google search, your information will be carried over to Google. You can open a separate container just for a particular website and keep that website’s cookie data separate.
* You can open links in separate containers as a form of “sandboxing” to protect your information. Links often contain scripts (small pieces of code) that can extract data about you. If, however, you use a container, the code can only extract what is in the container.

Install Multi-Account Containers and complete the tasks below (You may be asked to turn on sync. Ignore this.)

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

Create four separate containers called “OPSEC”, “Google”, “Alias”, and [A container of your choice.] Open the Multi-Account Containers menu and click the “Manage Containers” option. Then you can either delete each container or rename and customize the containers. Your containers before you modify them should look like below.

|  |
| --- |
| Graphical user interface, application  Description automatically generated |

1. Take a screenshot of your four customized containers. **(7.5 pts.)**

|  |
| --- |
| Graphical user interface, website  Description automatically generated |

Assign a specific website to a container so that the website always opens in that container. The most obvious use of this is for Google so that your Google search history is not shared with other websites.

* Go to Google, and then click the containers menu and select “Always open this site in….”
* You will know you have done this correctly when you see the fingerprint the color of your container.

|  |
| --- |
| Graphical user interface, application, Teams  Description automatically generated |

1. Take a screenshot of your Google container **(7.5 pts.)**

|  |
| --- |
| Graphical user interface, application  Description automatically generated |

User-Agent Switcher and Manager

User-Agent Switcher allows you to spoof your operating system and browser.

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
| Graphical user interface, website  Description automatically generated |

1. Install User-Agent Switcher. Spoof your browsing session with the browser and operating system of your choice and take a screenshot of the spoofed agent. **(7.5 pts.)**

|  |
| --- |
| Graphical user interface, text  Description automatically generated |

uBlock Origin

uBlock Origin protects you from invasive advertisements, tracking code, and malicious content. It is a wonderful plug-in that can tell you quite a bit about all the malicious or unwanted code – usually trackers and scripts, that run on a website. Trackers are often from advertising agencies. Scripts are pieces of code embedded on a website to perform certain tasks.

Here is what happens when ublock Origin is installed and one navigates to ODU’s website. 15 trackers or scripts were blocked.

|  |
| --- |
| Graphical user interface, application  Description automatically generated |

uBlock Origin is an outstanding plug-in with a broad range of functions. However, for this activity, I would like you to go to the settings tab and disable java-script. Java script is a common language that most website use. However, it is also a common vector for attacks and other malicious software. You may wish to block JavaScript when exploring some sites when doing an investigation.

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

Here is ODU’s entire homepage without JavaScript (captured by Nimbus).

|  |
| --- |
| A picture containing text, screenshot, different  Description automatically generated |

1. Navigate to a site of your choosing and take a screenshot of that site showing how many pieces of code were blocked. **(7.5 pts.)**

|  |
| --- |
| Graphical user interface, website  Description automatically generated |

1. Disable JavaScript, refresh the site, and take a screenshot of the entire page. **(7.5 pts.)**

|  |
| --- |
| A screenshot of a computer  Description automatically generated with medium confidence |

**Part III – Critical Thinking**

Now that you have completed this assignment, reflect on what you have done. Describe in 2 - 3 paragraphs how operational security is important for an investigator. Also, describe how these specific strategies you practiced in this assignment can make an investigation more secure.  **(15 pts)**

Operational security is a methodology that is utilized to protect against stolen information. Throughout this process, organizations/groups will have to specify what needs to be protected, what is required to protect itself from, and what countermeasures should be in place. This process is beneficial for investigators because it enables them to analyze and gather information. While investigators are trying to conduct an investigation, they may unknowingly be compromised by hackers too. They can collect information by executing an attack or other malicious methods over the internet. Operational security will aid in preventing hackers from obtaining sensitive information on the investigator and allow them to perform their duties discreetly.

Throughout part two of the lab, I practiced several methods that I will utilize to protect critical information. For instance, utilizing the web browser, Firefox will aid in investigations since it is private. The application Nimbus will allow for the documentation of information collected throughout the investigation and enable investigators to highlight and add notes without compromising the evidence. Multi-Account containers will help investigators browse in separate sessions and get rid of tracking. Containers will protect the investigator's personal information since the container limits the proliferation of information that hackers could potentially use since the investigator only searches one website. Also, once the user-agent switcher is installed, investigators can disguise the user-agent to a specific domain preventing websites from obtaining information on their browsing. Finally, utilizing UBlock will intercept intrusive advertisements, and disabling JavaScript will block trackers. Thus, each of the methods practiced throughout the lab will ensure safe intelligence gathering and protect hackers from obtaining sensitive information from investigators.