Dragon

by

Riley Kittle, Daniel Leonard, and Katelyn Murphy

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

Riley Kittle	*4/12/2021*
Riley Kittle	Date
Daniel Leonard	*4/12/2021*
Daniel Leonard	Date
Katelyn Murphy	*4/12/2021*
Katelyn Murphy	Date
Tony Iacobelli	*4/12/2021*
Tony Iacobelli, Faculty Advisor	Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2021

TABLE OF CONTENTS

List of Illustrations

TABLES

FIGURES

ACRONYMS AND ABBREVIATIONS

Nmap	**Network Mapper**
ISPs	**Internet service providers**
PHP	**Hypertext Preprocessor**
PM2	**Process Manager 2**
TMUX	**Terminal Multiplexer**
USB	**Universal Serial Bus**

ABSTRACT

Due to the COVID-19 pandemic, many people have had to adjust their daily routines and turn their home into their workplace and classroom. With an increased amount of people utilizing their home networks for a wide range of activities, some of which may include potentially sensitive information, it is important to ensure that users' home networks are secure, now more than ever. Dragon delivers a convenient and affordable device that provides users with the ability to stay informed about their network health and devices, and equips users with the necessary information to fix network security risks that are identified. Features include port and device scanning, file sanitization, and Wi-Fi password testing. By equipping users with this knowledge, Dragon will assist them in increasing the security of their home network.

1. INTRODUCTION

1.1 Introduction

When the COVID-19 pandemic hit, the world had to adapt to many changes. One of these changes is that people were spending much more time at home than before the pandemic (Ritchie, n.d.). Since the beginning of the pandemic, the average amount of time that people in the United States spent in places of work dropped 38%, and the average amount of time that people spent at home increased 20%, according to Our World in Data (Ritchie, n.d.). Because of this increase in time spent at home, people used their home network more often, whether for work, school, or personal use (Vogels et al., 2020). With an increased amount of people that utilized their home networks for a wide range of activities, some of which may have included potentially sensitive information, it was important to ensure that a user's home network was secure, more than ever before.

1.2 Problem Statement

During that time, when people were spending more time at home, "87% of adults say the Internet has been important for them personally during the coronavirus outbreak," and approximately "two-thirds of adults under the age of 50 say the Internet has been essential for them during the outbreak," as reported by Pew Research (Vogels et al., 2020). In fact, many people had to share their home network with other people in their household who were also working or learning from home. The New York Times reported that most people are "experiencing slower overall speeds in the wake of the pandemic," due to an increase in home Internet usage that Internet service providers (ISPs) have not experienced before (Chen, 2020). Because home Internet access remained vital to many people, it was also important to ensure that users were not unknowingly contributing to their slow home Internet speeds. Therefore, it was

crucial for home users to ensure that they did not have any unknown devices sitting on their network, silently using and sending out data.

Because users were utilizing their home network more often, the risk of a potential security threat became more detrimental. The areas of network and computer security are "often considered as hard to understand and manage by the average, non-technical user," (Karvonen, Vesterinen, & Manner, n.d.). As such, the average person had little experience with knowing how secure their home network is, and users would likely have no idea if their network was at risk or if it had been compromised. Users would also be unaware of security vulnerabilities, such as if there were any open ports on their network, if their Wi-Fi password was easily guessable, or even if it was still set to the default password. In fact, Techno-Crime Institute cited that "46% of consumers and 30% of technology professionals never change their default router passwords," (Manning, 2020). In order to create a better and more secure home network environment, users needed to be equipped with the ability to manage their network devices, and the tools to ensure that their home network was not vulnerable to security risks.

1.3 Problem Solution

Dragon presented as an affordable solution for home users that provided an all-in-one device with useful features to improve users' home network environment. Dragon was aimed toward any user who wanted to make their network more secure. Dragon would ensure that a user's network was secure from external parties and attacks, and did not have any ports open that should not have been. Dragon alerted the user if their Wi-Fi password was easily guessable or was still set to the default password. Users were informed of all devices that were on their network. If the user found an unknown device that should not have been on their network, Dragon then informed them how to remove the device from the network.

Additionally, Dragon featured a Universal Serial Bus (USB) sanitizer option, which allowed users to check the files on a USB flash drive before they connected it to their personal computers. Overall, Dragon delivered a convenient and affordable device that equipped users with the ability to stay informed about their network devices, and ensured they had taken the necessary steps to secure their home network, as well as provided information that helped it remained secure. Dragon provided users with the necessary tools to support their work from home and personal use needs.

1.4 Project Goals

One of the primary goals of Dragon was to equip users with tools that made their home network as secure as was possible, since people were spending an increased amount of time at home using their network. Dragon incorporated several technologies into an affordable Raspberry Pi device. Once the device was connected to a power source, it automatically ran scripts to scan the user's network and reported the results. This aligned with another main goal of Dragon: to provide a user-friendly device that did not require any setup beyond connecting a couple of cords. Dragon aimed to accomplish that with features such as port and device scanning, file sanitization, and Wi-Fi password testing. Another aspect of Dragon was a supplemental webpage. The webpage enhanced the user experience by providing general information about Dragon and its features.

1.5 Overview

The purpose of this report was to provide a detailed outline and discussion of how the project was completed. The following sections were included: design objectives, methodology, budget, timeline, problems encountered, and future recommendations.

2. DISCUSSION

2.1 Project Concept

The concept for Dragon stemmed from researching general network security improvements for family members. Many of these components were confusing to set up or run through solo, especially for the average non-technical user. The team decided to offer several such security improvement components in an all-in-one device to any user, technical or non-technical. The idea focused on creating and developing an affordable network security package that allowed the user the confidence that their home network was secure from common vulnerabilities. The device did not require any setup beyond connecting it to a power source, which made it a suitable choice for any user, regardless of technical experience. With network scanning scripts that automatically ran upon device startup, Dragon helped provide users with an overview of their home network security.

2.2 Design Objectives

The design objectives of Dragon changed since the idea's inception. The original objective was to provide users with an all-in-one device with features built in that would improve their work from home experience, such as a Wi-Fi extender, ad blocker, cloud storage, and VPN and print servers. The team realized this objective would be difficult because of the varying technologies that would be required to implement such features, as well as the fact that user input would be needed in order for some of these features to run. If user input was required, it would not be possible to retain the goal of a device that was convenient for both technical and non-technical users to utilize.

The team continued research on network-related features and decided on features that supported home network security instead. The features included the development and automation of scripts that gathered information about the security of the network and produced the results to the user, as well as provided a supplemental webpage with general information about Dragon's features and common results. The scripts employed the use of automated port scanning, Wi-Fi cracking, and file sanitizing commands. The automation of the scripts allowed for an accessible and straightforward device that anyone could use.

2.3 Methodology and Technical Approach

The team's project solution consisted of a Linux-based package hosted on a Raspberry Pi. This affordable and convenient package solution utilized multiple tools that improved the security of the user's home network. Technologies used included Raspberry Pi, Linux, Apache web server, GitHub, bash scripts, Aircrack, Shodan, PHP (Hypertext Preprocessor), Nmap (Network mapper), tmux (Terminal Multiplexer), and PM2 (Process Manager 2).

Network Scan

One goal of Dragon was to find all devices that were on a user's network. A second goal was to determine the ports that were open on the network. Dragon required connection to a user's Wi-Fi network so that the automated scripts properly scanned the network. Aside from the connection of the device to a power source, the one other task required of the user was the authentication of Dragon to their home Wi-Fi network. From there, the scripts used Nmap commands and scanned for any devices on the network, as well as identified any open ports on the network. The user was then shown a list of the devices that were currently sitting on their

network, which allowed the user to determine if there were any unknown devices connected to their network. The user was also shown a list of any open ports that were on their network.

Wi-Fi Password

Another goal of Dragon was to check a user's Wi-Fi password strength. The scripts attempted to crack the user's home Wi-Fi password using Aircrack commands. This performed a dictionary attack, which used a wordlist that generated possible passwords. If the user's Wi-Fi password was cracked, the password was shown on the screen. This informed the user that their password was easily guessable, and that it was beneficial if they considered changing it to something more difficult and secure. If the user's password could not be cracked, a "Not Found" message appeared, which informed the user that their password was not easily guessable.

USB Sanitizer

The USB sanitizer feature provided a solution to another goal of Dragon: it encouraged the user and engaged them to be active in security best practices. The sanitizer feature provided a way for the user to scan the contents of any USB flash drive before it was connected to their computer. Once a USB flash drive was inserted into Dragon, the sanitizer script then found the directory of the USB flash drive. Once the directory was found, the script moved into the directory and showed its contents. Then it performed a sanity check and asked the user for confirmation to delete the files that were shown. If the user confirmed the action, the script would run the removal command. Finally, an empty directory with the files removed would be shown. This allowed the user to feel confident since it provided them the opportunity to be engaged in keeping their home computer and network safe. This was especially beneficial for a non-technical user, as they may have been influenced by the process and thus considered security measures in their future daily actions.

Webpage

The user was able to navigate to the webpage associated with Dragon and learned more information about their next steps. For example, the webpage showed the user how to remove any network devices and close any ports they wanted to close, if applicable. The webpage provided general information and best practice recommendations about common outputs and results that the user compared their own results to.

Security

Dragon and its features presented several security considerations. As a home network security device that was for both technical and non-technical users, a user likely did not possess sufficient technical knowledge to know what processes and scripts were running on Dragon. However, users could be confident that their information and data was not stored, sold, or stolen. Dragon was not equipped with any ability to write or send data outside of the device. Dragon ran locally on the user's home network, which prevented any data from being extracted from the physical device itself. This eliminated the possibility of possessing sensitive information about a user's home network and any of its vulnerabilities that may have been found.

2.4 User Profile

Dragon was designed for any end user, regardless of whether they were a technical or non-technical user. One user group was identified as potential users of Dragon: the end user. The User Profile of the end user was shown in Figure 1. This user group encompassed anyone who wanted to secure their home network, no matter their level of technical expertise. The features and characteristics of that user profile guided the team in Dragon's creation and development so that the device was both accessible and beneficial for its users.

User Profile Form 1

Project: Dragon

Dragon was created with the intention of being easy to use, regardless of the user's technical experience or level of technical knowledge. Because an increasing number of people were using their home networks much more often than they were before the COVID-19 pandemic, people wanted to make their home networks more secure, and looked for a convenient and affordable option to do so.

Potential Users:

- Technical users who wanted to secure their home network
- Nontechnical users who wanted to secure their home network

Software, Interface, and Related Experience:

Individuals who used Dragon have had experience in looking at a monitor screen and reading the content that is displayed.

Users have had experience in using the Internet to navigate to a website. Users also know how to use their mouse to interact with a website, click page links, and scroll to read the contents of the webpage.

Experience with Similar Applications:

It was beneficial for the user to have basic experience with launching and using browsers such as Internet Explorer, Microsoft Edge, Mozilla Firefox, or Google Chrome.

The user needed to be generally familiar with search engines like Google, Yahoo, or Bing.

Task Experience:

The user needed the ability to plug in provided cables, such as a power cord, and the knowledge of how to connect a device to their home Wi-Fi network.

The user needed to know how to plug in a USB drive and SD card into appropriate port slots.

Most users had general experience plugging in power cords. Nontechnical users likely had experience that was limited to plugging in cell phones, appliances, or similar items. Technical

users typically had far more experience with using power cords and cables and connecting them to the correct devices. No matter what the user's experience level is, they were easily able to use Dragon.

Frequency of Use:

Users utilized Dragon at least once in order to check the security of their home network. Users continued to use Dragon any time that they wanted to view and monitor their home network security.

At any time, users were able to navigate to the webpage that provided details on Dragon.

Users used Dragon any time they wanted to:

- Check the security of their home network Wi-Fi password
- View and close any open ports on their network
- See a list of all devices connected to the network
- Clean files on flash drives

Users used Dragon's webpage any time they wanted to:

- Look up information about how to use Dragon
- Find FAQs about what some commonly displayed security results mean

Key Interface Design Requirements that the Profile Suggests:

- Clear display output of network information to the user
- Necessary cables to use Dragon are provided for convenience
- Locally hosted on the user's own network to prevent information security issues
- Minimalistic webpage design
- Clean and easy to use UI

Figure 1: User Profile

2.5 Use Case Diagram

The primary use case for Dragon involved the end user, the Raspberry Pi, the provided cables, and the webpage. In the use case diagram, the user engaged in the initial set up of Dragon, which was the Raspberry Pi device. The user connected Dragon to a power source with

the provided power cable, then proceeded to connect the device to the user's home Wi-Fi network. After these two steps were completed, Dragon automatically scanned the user's network. The user viewed the results of the network scan, which included a list of devices and open ports on the network, and the Wi-Fi password strength. To sanitize a USB flash drive, the user simply inserted the drive into Dragon. The user also navigated to a webpage to view general information about Dragon. Figure 2: Use Case Diagram, shown below, demonstrated the interactions between the end user, the Raspberry Pi, the setup steps, and the webpage.

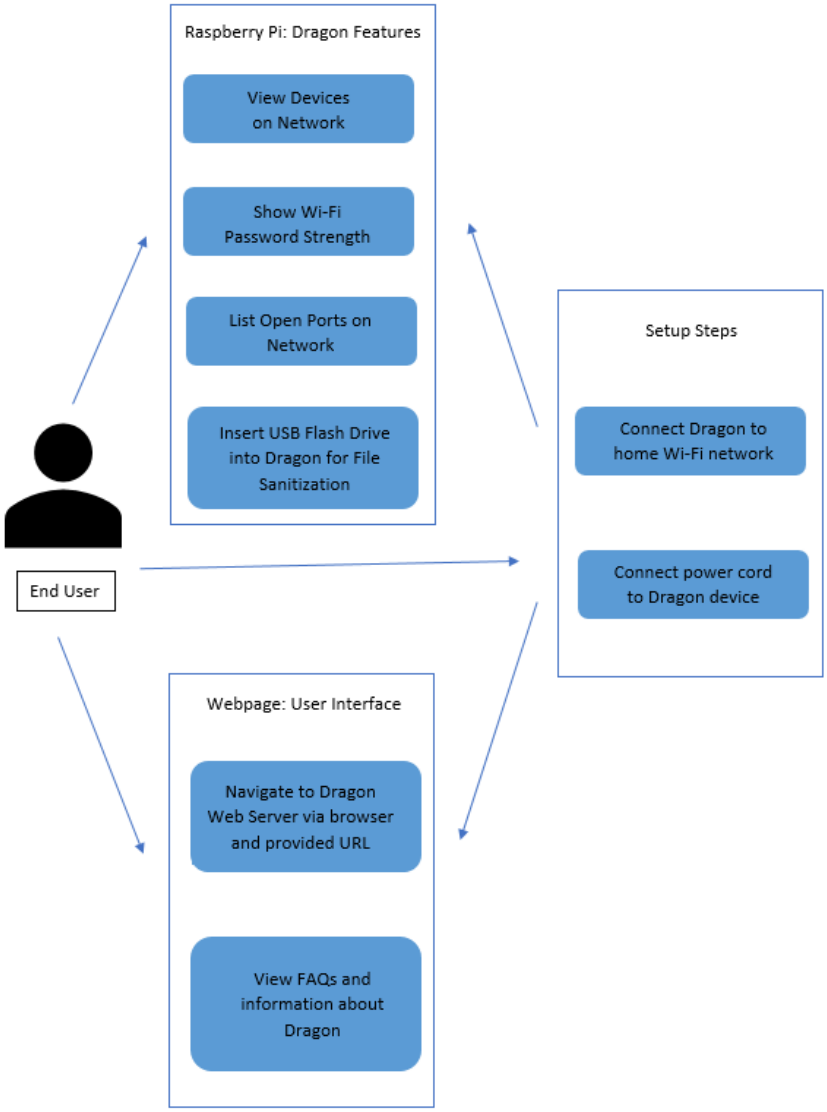

Figure 2: Use Case Diagram

2.6 Technical Architecture

The technical architecture of Dragon can be shown in the supplemental webpage that displays all script results.

Figure 3: Home Page below provided an overview of Dragon, how it worked and why it was beneficial to the user.

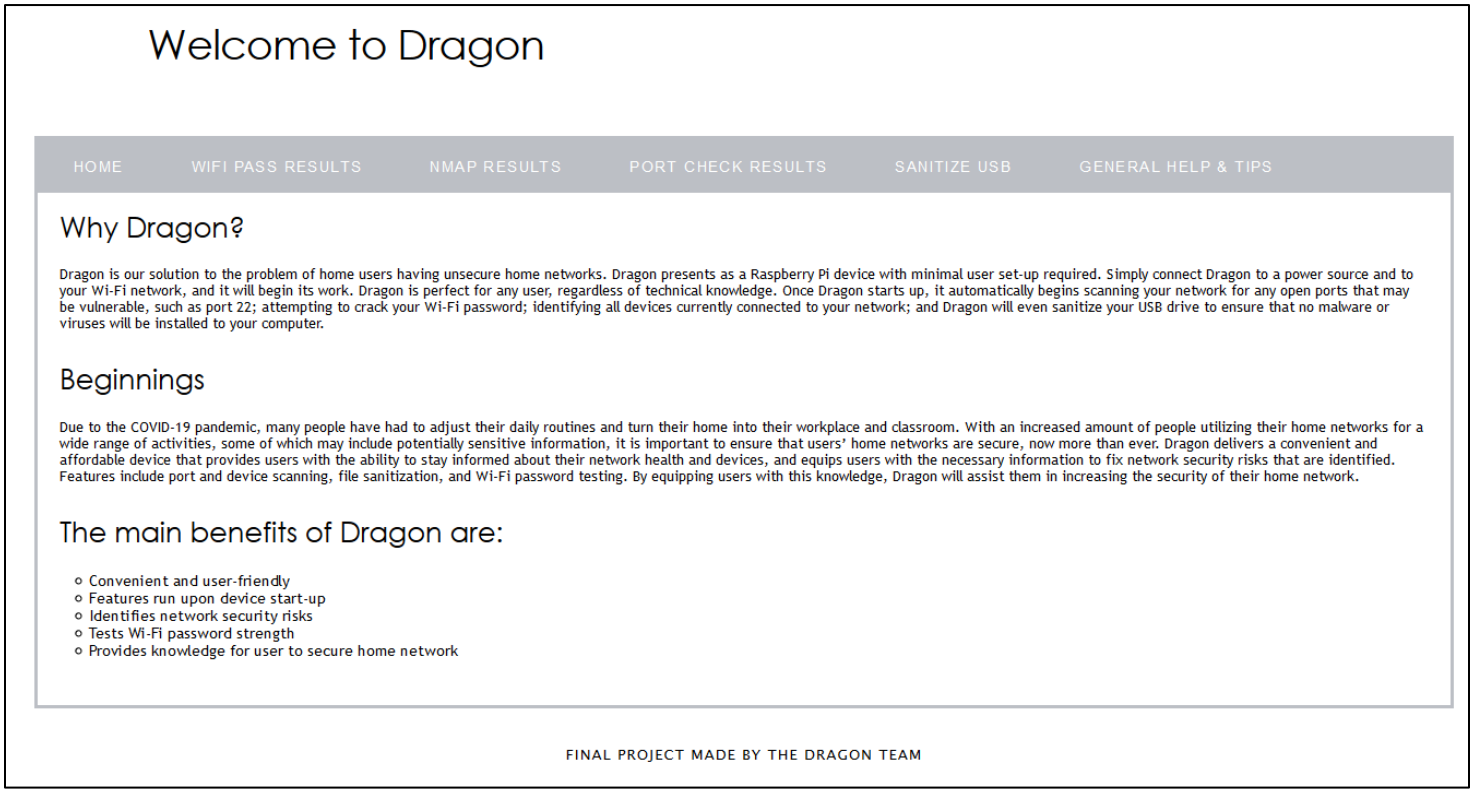

Figure 3: Home Page

Figure 4: Wi-Fi Password Page, below, showed the results of the Wi-Fi password script that ran upon Dragon's startup. The script also ran upon clicking the "WiFi Pass Results" tab, which acted as a button to manually kick off the Wi-Fi password cracking feature.

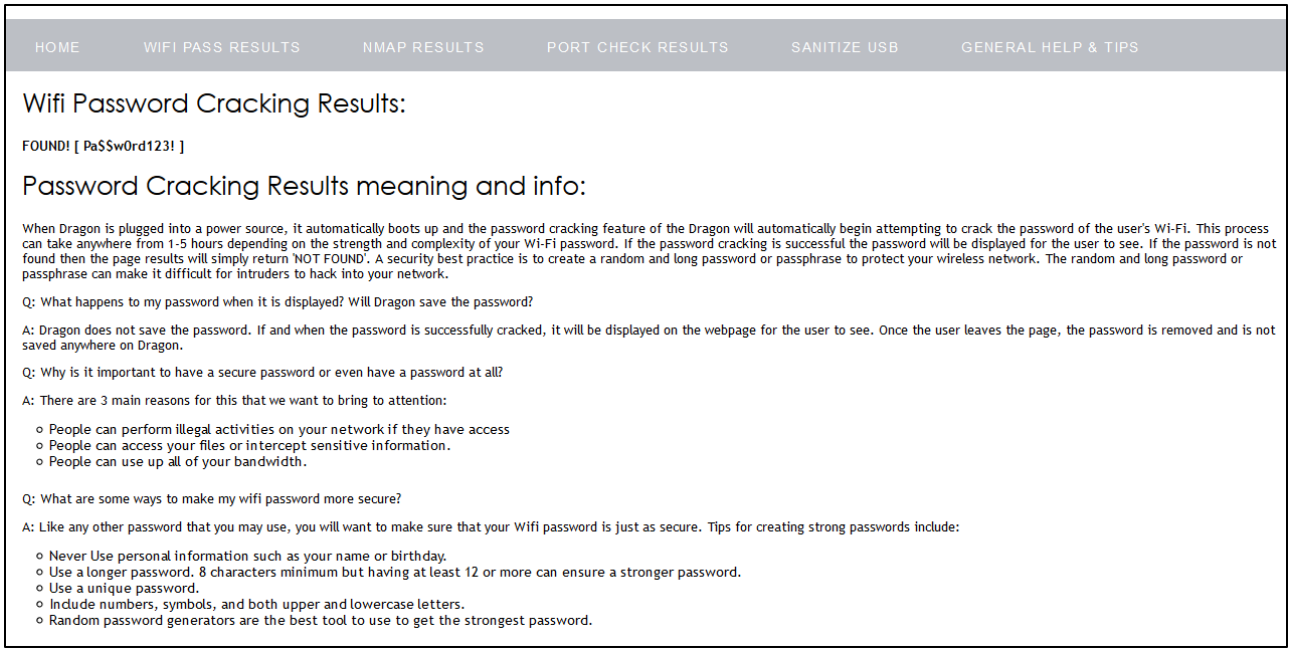

Figure 4: Wi-Fi Password Page

Figure 5: Network Device Page, below, showed the results of the network device script that ran upon Dragon's startup. The script also ran upon clicking the "Nmap Results" tab, which acted as a button to manually kick off the network device scanning feature.

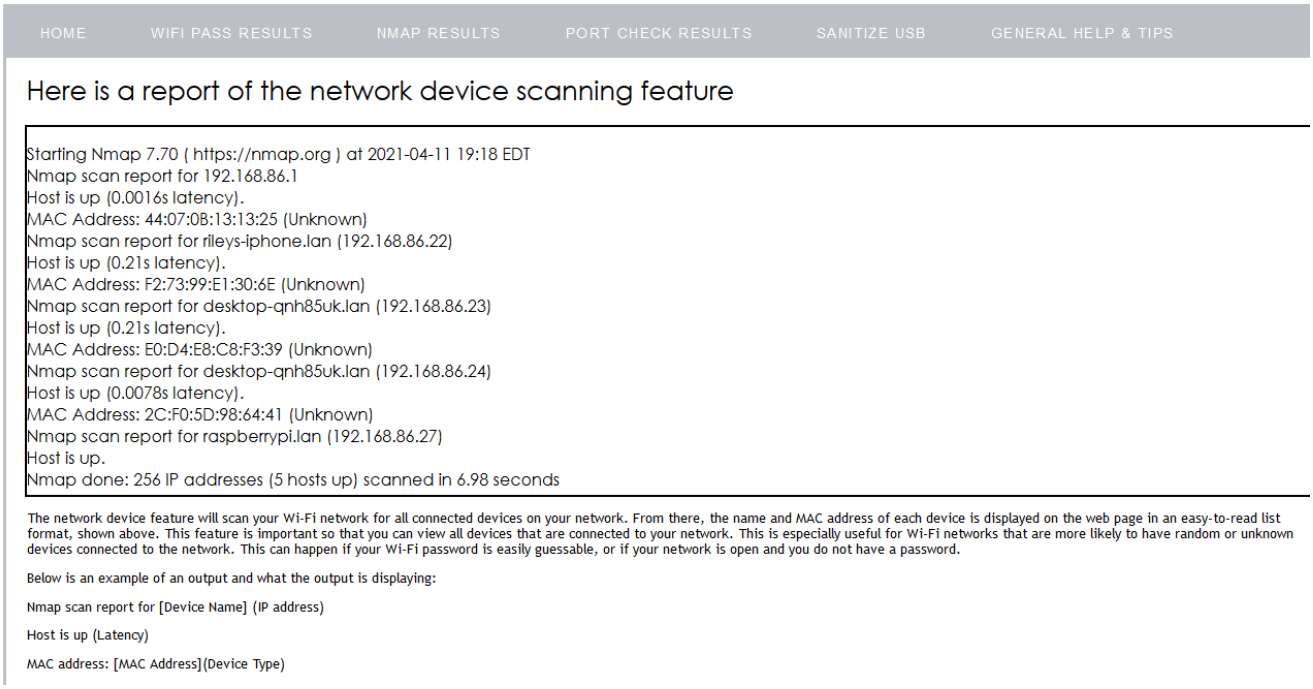

Figure 5: Network Device Page

Figure 6: Port Check Page, below, showed the open port results of the port scanning script that ran upon Dragon's startup. The script also ran upon clicking the "Port Check Results" tab, which acted as a button to manually kick off the port check scanning feature.

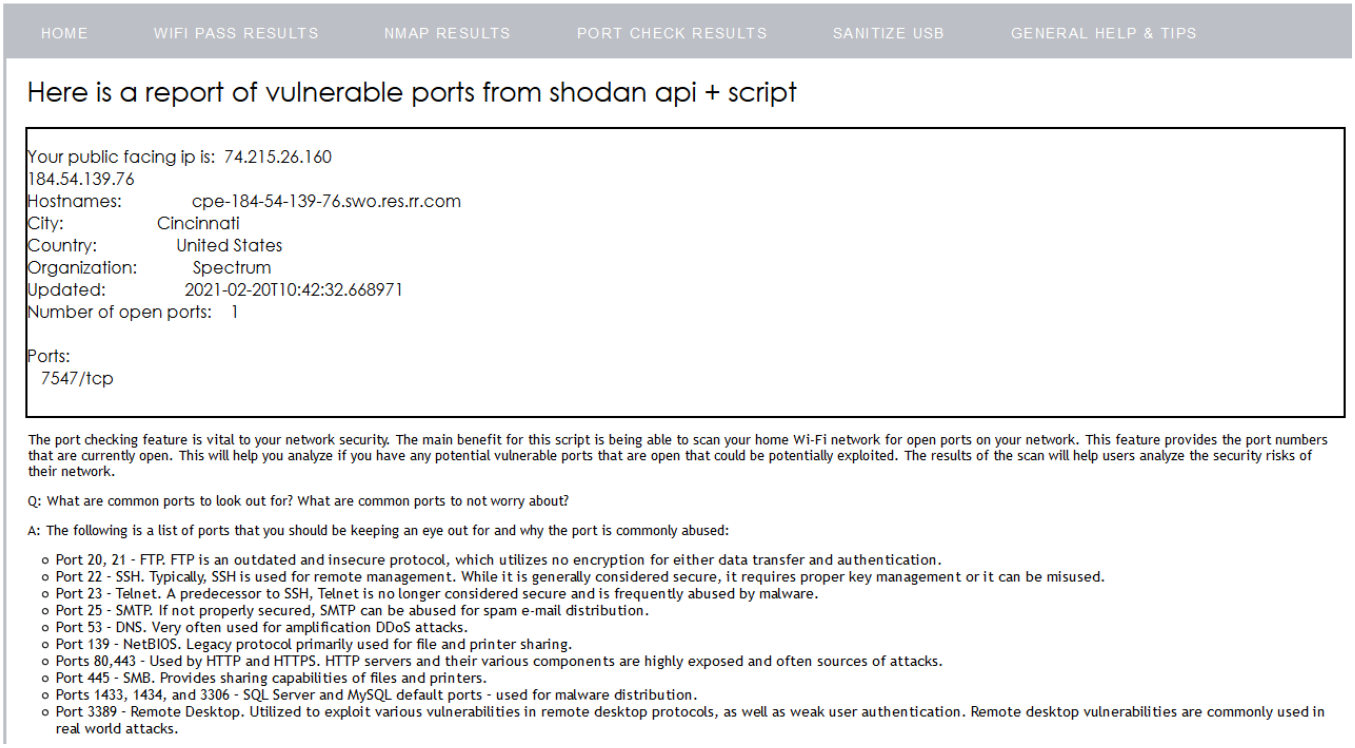

Figure 6: Port Check Page

Figure 7: USB Sanitization Page, shown below, displayed the initial page of the USB sanitizing script, which ran only upon user confirmation. In order to proceed, the user inserted a USB device into Dragon, and confirmed that they would like the USB to be sanitized, before proceeding to the actual sanitization. The user was informed that this could not be reverted. The script ran only by clicking the "USB Sanitization" button, which then proceeded to wipe the USB drive.

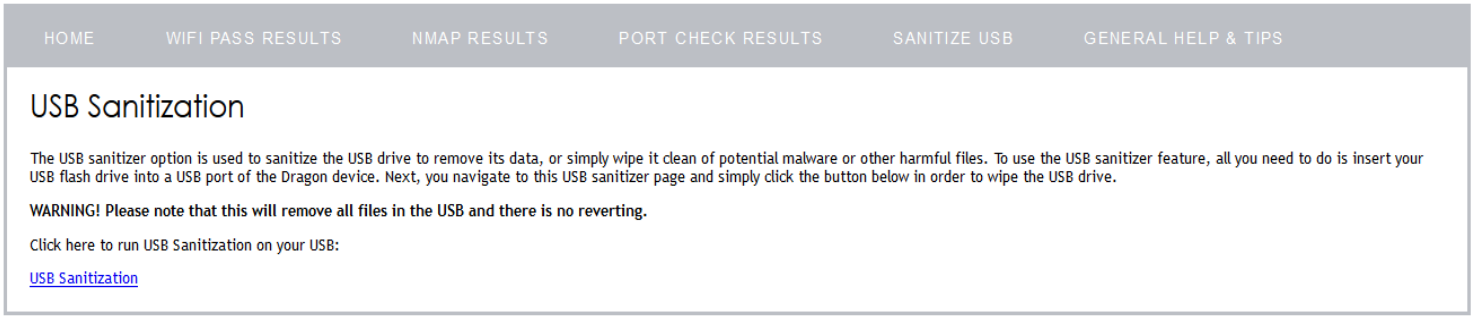

Figure 7: USB Sanitization Page

Figure 8: USB Wiped, was presented after the user confirmed the USB sanitization. This validated that the USB drive was completely wiped.

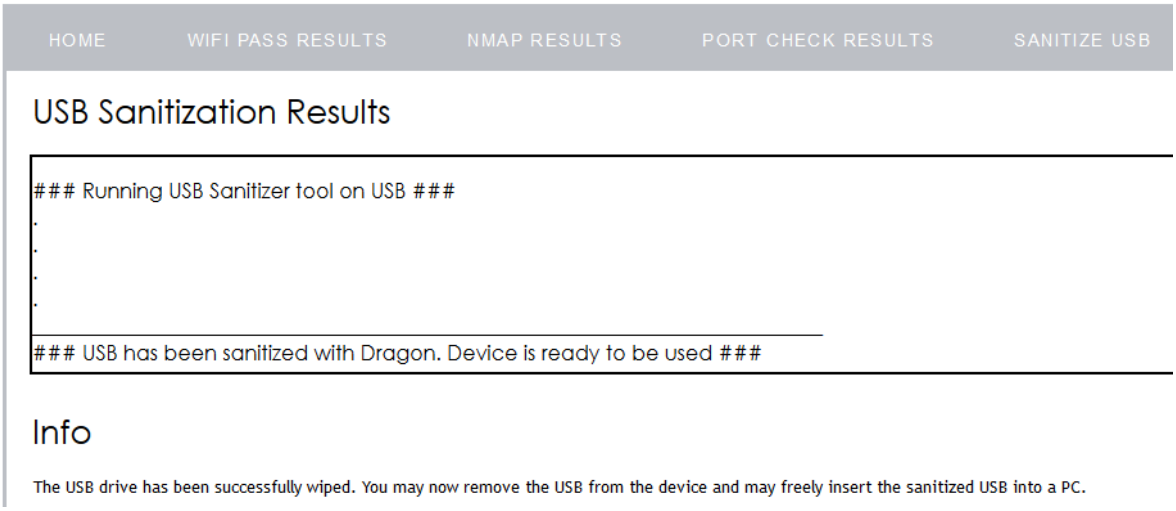

Figure 8: USB Wiped

The webpage was created with HTML and CSS and used Apache webserver to host it. The webpage acted as a supplement to Dragon and provided a user-friendly option for viewing Dragon's scan results. As shown in Figures 4-8, the results of the user's individual Wi-Fi network scan were displayed on each feature page. Below the results, the webpage also explained to the user what each feature did and helpful information to secure their network.

2.7 Testing

Testing Overview

This section outlined the steps that were taken to test Dragon's functionality, as well as its feasibility as a user-friendly device. Testing was an important part of a project's development and impacted a target user's experience. Details on testing Dragon's use cases and features were included in this section as well. Finally, user feedback was also provided in this section.

Testing Methodology

The testing methodology that was performed consisted of a combination of integration testing and usability/user acceptance testing. The integration testing approach was used because there were multiple team members contributing to the project. Therefore, it was only prudent to test the various components of Dragon each time a team member's part was completed and added to the project.

The use of integration testing was employed and ensured that all components flowed and worked seamlessly together. For example, if a component had issues upon integration, the team was able to troubleshoot and remedy the situation in a more time efficient manner, since it was known which component was the one that caused the product issues. Otherwise, the route of putting all the components together and only testing at the end would have caused efficiency issues. If the product was not working, each component needed to be analyzed and tested for the cause of the problem, which would have required additional time and effort for the team members.

Testing throughout the duration of the project had the potential to avoid encountering any larger issues, and instead allowed sufficient time for mitigation of issues upon discovery and

initial integration. Therefore, the team employed the approach of testing throughout the duration of the project, in order to make use of members' valuable time and effort in the most efficient manner.

In addition, user acceptance testing was also used in the testing of this project. Since Dragon was geared toward the average user, the team wanted to make sure that the average user could indeed use the product, as well as identified any issues that a user may have encountered or found confusing. In order to conduct user acceptance testing, family and friends were recruited to test and interact with Dragon.

Scope of Testing

For the scope of testing, the team chose the main use case of the project to use in the user acceptance testing: the average user, regardless of any technical expertise. The scope of this testing included the minimal user set-up of the device and navigation to Dragon's supplemental web page, as well as the user's overall ability to use Dragon.

Several users were recruited to perform test cases. The purpose of these test cases was observation and confirmation of the average user's success in using Dragon and its supplemental web page. This included testing three main features and their corresponding procedures: the user connecting Dragon to the user's own home Wi-Fi network via the provided Wi-Fi dongle, connecting Dragon to a power source, and using their own PC where they navigated and interacted with the web page.

The three above features were chosen because they were the only steps the user need to take on their end in order to successfully use Dragon. The other aspects of Dragon ran automatically upon device startup, so the user did not need to be involved in testing the behind-

the-scenes hardware and software portions.

Objectives

The team's objective was to ensure that Dragon's features were user-friendly, as they were designed to be, as well to validate Dragon's overall functionality as a product. Each user was given instructions on how to proceed in the initial set-up, as well as directions on how to see their individual network scan results. Each step that the user went through was given a "pass" or "fail" rating. The rating was determined by whether or not the procedure worked for them, based on the instructions given.

Overall, the purpose of this testing was to ensure that Dragon functioned as it was intended: as a user-friendly product for even the most non-technical users. The end goal was to have Dragon be as easy to use as possible, while still maintaining its efficacy and value. The team's objectives were outlined below.

1. All initial set-up requirements were successfully performed
    a. Connect Dragon to user's home Wi-Fi network via provided Wi-Fi dongle
    b. Connect Dragon to a power source (wall outlet, etc.) via provided power cable
2. All script outputs were displayed on Dragon's webpage
    a. The user must navigate to Dragon's webpage via own local IP address
    b. The user's individual network scan results must populate on Dragon's webpage for easy viewing
3. All performance issues must be resolved before IT Expo

a. Any user feedback must be considered, and any changes must be implemented in a timely fashion before the IT Expo

Test Logs and Procedures

The procedures consisted of:

1. Communicated to the user to log in to a PC that was already connected to their home Wi-Fi network
2. Had user insert provided Wi-Fi dongle into a USB port on their PC
3. Instructed user to navigate to the Wi-Fi and network settings on their PC
    a. Made sure user selects “Wi-Fi 2” from dropdown menu that appears
        i. Otherwise, user would not be able to connect to the provided Wi-Fi dongle
    b. Connected Wi-Fi dongle to user’s Wi-Fi network with their own Wi-Fi credentials (they must know this information)
4. Directed user to remove Wi-Fi dongle from PC and insert it into USB port on Dragon
5. Had user connect the provided power cord to Dragon and to a power source (most likely a wall outlet)
    a. Upon connection to power, Dragon would automatically startup and its features ran without any further user input or action
6. Told user to wait approximately five minutes to ensure Dragon collected all information and scan results
7. Had user then navigate to the web server on their PC
    a. This was Dragon’s supplemental webpage and it loaded and displayed the user’s network results

8. Ensured the user can see that all scan results are accounted for
    a. This included the Wi-Fi password crack, network device and port scanning, and confirmation of successful USB sanitization

The testing results are outlined in Table 1, shown below.

Record #	Test case #	Input	Expected output	Actual output	Pass/ Fail	Reason for failure/success	Date
1	1A	Ally K.	Network scan results displayed	Network scan results displayed	P	Successful initial connection to user's Wi-Fi network	2/3/21
2	1B	Ally K.	Wi-Fi password results displayed	Wi-Fi password results displayed	P	Successful initial connection to user's Wi-Fi network	2/3/21
3	1C	Ally K.	Port scan results displayed	Port scan results displayed	P	Successful initial connection to user's Wi-Fi network	2/3/21
4	1D	Ally K.	USB drive sanitized	USB drive sanitized	P	Successfully inserted USB drive	2/3/21
5	2A	Mark L.	Network scan results displayed	No scan results displayed	F	Unsuccessful initial connection to user's Wi-Fi network	2/5/21
6	2B	Mark L.	Wi-Fi password results displayed	No scan results displayed	F	Unsuccessful initial connection to user's Wi-Fi network	2/5/21
7	2C	Mark L.	Port scan results displayed	No scan results displayed	F	Unsuccessful initial connection to user's Wi-Fi network	2/5/21
8	2D	Mark L.	USB drive sanitized	USB drive sanitized	P	Successfully inserted USB drive	2/5/21
9	3A	Matthew M.	Network scan results displayed	Network scan results displayed	P	Successful initial connection to user's Wi-Fi network	2/6/21

10	3B	Matthew M.	Wi-Fi password results displayed	Wi-Fi password results displayed	P	Successful initial connection to user's Wi-Fi network	2/6/21
	3C	Matthew M.	Port scan results displayed	Port scan results displayed	P	Successful initial connection to user's Wi-Fi network	2/6/21
	3D	Matthew M.	USB drive sanitized	USB drive sanitized	P	Successfully inserted USB drive	2/6/21

Table 1. Testing Logs

Review

After the team conducted this testing process, a few valuable lessons were learned. This testing process helped ensure all team members realized that the average user tended to have very little technical experience. The users' feedback and experiences highlighted this, as the team learned that some of Dragon's features or procedures were difficult or confusing for the average user understand. This was beneficial and eye-opening for all members, as the team previously thought the set-up and procedures were more straightforward and self-explanatory, even for non-technical users.

This feedback was useful in reworking the instructions and procedures that were provided to the user. It also assisted in ensuring that any future instructions and procedures written by the team were easily understood by even the most non-technical user.

2.8 Budget

In order to determine the budget for Dragon, several factors were considered. Required hardware consisted of one Raspberry Pi and one Wi-Fi adapter for each team member, in order to complete assigned roles and responsibilities. The sole software component was a GitHub

account for each team member. GitHub was chosen in order to provide version control and to serve as a backup of all necessary files and code, in case of accidental code changes or Raspberry Pi failure. Finally, the labor costs were broken down into three different areas. The webpage build required moderate effort and expertise, and was completed by all three team members. While the development work was also completed by all three team members, it was more demanding than the webpage build, in terms of effort, expertise, and price. Finally, the research and modifications involved a significant portion of each team member's time and effort, as this work was done to improve the project and its feasibility. Therefore, the price was adjusted to be paid hourly, in order to accurately reflect the intensive labor involved in the research and modifications portion. Table 2, shown below, provides a visual breakdown of the project budget.

Dragon Budget				
NO.	**ITEM**	**UNIT**	**UNIT PRICE**	**TOTAL**
HARDWARE				
1	**Raspberry Pi**	**3**	**$35**	**$105**
2	**Wi-Fi Adapter**	**3**	**$10**	**$30**
SOFTWARE				
3	**GitHub Account**	**3**	**$0 per account**	**$0**
			Subtotal	**$135**
LABOR				
4	**Webpage Build**	**3**	**$100 (flat fee)**	**$300**
5	**Development Work**	**3**	**$300 (flat fee)**	**$900**

6	**Research and Modifications**	**3**	**$15/hr/per person**	**$450**
			Subtotal	**$1650**
	Total			**$1785**

Table 2. Project Budget

2.9 Project Timeline

The project timeline was broken down into five different sections. First, the project management assignments and deliverables were identified, as well as their respective due dates. The second section was the research phase, which took place during the first month of the fall semester. The third section contained the environment set-up of necessary software and hardware components, which was completed within one week. The fourth section focused on the development phase, with one month dedicated to development completed in the fall semester and one month set aside for development to be completed in the spring semester. The final section outlined the testing phase, with the goal of being completed within the first month of the spring semester. This was done to allow sufficient time for any issues to arise and for preparation for the IT Expo. Table 2, shown below, presents a detailed project timeline.

Task Name	Duration	Start	Finish
Dragon	246 days	8/24/20	4/27/21
1.0 Project Milestones/Deliverables	246 days	8/24/20	4/27/21
1.1 Research Potential Ideas	7 days	8/24/20	8/31/20
1.2 Fall Assignment 0: Team Members and Project Title	1 day	8/24/20	8/24/20

1.3 Develop problem statement and solution	7 days	8/24/20	8/31/20
1.4 Fall Assignment 1: Team Contract	8 days	8/24/20	9/1/20
1.4.1 Get project approval from advisor	10 days	8/24/20	9/4/20
1.4.2 Meet with advisor to discuss project idea	1 day	8/31/20	8/31/20
1.5 Fall Assignment 2: Project Abstract	14 days	9/28/20	10/12/20
1.6 Fall Assignment 3: Team Contract Resubmission	14 days	9/28/20	10/12/20
1.7 Fall Assignment 4: User Profile Report and Table	6 days	10/13/20	10/19/20
1.8 Fall Assignment 5: Use Case Diagram	6 days	10/13/20	10/19/20
1.9 Fall Assignment 6: Draft Report	20 days	10/20/20	11/9/20
1.10 Fall Assignment 7: Final Fall Semester Presentation	13 days	11/10/20	11/23/20
1.11 Fall Assignment 8: Final Fall Semester Report	27 days	11/10/20	12/7/20
1.12 Spring Assignment 1: Testing Plan	14 days	1/25/21	2/8/21
1.13 Spring Assignment 2: IT Expo Abstract	7 days	2/8/21	2/15/21
1.14 Spring Assignment 3: First Draft of Tech Expo Poster	14 days	2/15/21	3/1/21
1.15 Spring Assignment 4: Tech Expo Poster Due	14 days	3/1/21	3/15/21
1.16 Spring Assignment 5: Final Report	91 days	1/11/21	4/12/21
1.17 Spring Assignment 6: Course Final Presentations	84 days	1/11/21	4/5/21
1.17 Spring Assignment 7: Plagiarism Review Final Report	91 days	1/11/21	4/12/21
1.18 Spring Assignment 8: IT Tech Expo	57 days	2/15/21	4/13/21
1.19 Spring Assignment 8: Final Library Copy of Report	14 days	4/12/21	4/26/21

2.0 Research Phase	30 days	9/2/20	10/2/20
2.1 Network Requirements	20 days	9/2/20	10/2/20
2.1.1 Select operating system: Raspbian vs Ubuntu	7 days	9/2/20	9/9/20
2.1.2 Select network scanning features	10 days	9/2/20	9/12/20
2.1.3 Research Wi-Fi adapters for monitor mode	2 days	9/5/20	9/7/20
2.2 Hardware Requirements	5 days	9/8/20	9/13/20
2.2.1 Select Raspberry Pi device version to be used	2 days	9/8/20	9/10/20
2.2.2 Research cables/cords to provide with device	2 days	9/11/20	9/13/20
2.3 Security Requirements	7 days	9/14/20	9/21/20
2.3.1 Research possible device storage	3 days	9/14/20	9/17/20
2.3.2 Evaluate security implications of device	3 days	9/18/20	9/21/20
2.4 Other Research	7 days	9/21/20	9/28/20
2.4.1 Determine practicality of desired features	3 days	9/21/20	9/24/20
2.4.1 Determine feasibility of implementing the multiple selected features onto one device	3 days	9/25/20	9/28/20
3.0 Set-Up Environments	8 days	9/29/20	10/7/20
3.1 Setup GitHub Repository	4 days	9/29/20	10/3/20
3.3 Purchase Raspberry Pi for each team member	7 days	9/29/20	10/6/20
3.3 Purchase and set up Wi-Fi adapter on Raspberry Pi	4 days	9/29/20	10/3/20
3.3 Test Wi-Fi adapter functionality	3 days	10/4/20	10/7/20
4.0 Development Phase	52 days	10/1/20	10/30/20

4.1 Write network device scanning script	14 days	10/1/20	10/15/20
4.1.1 Automate network device scanning script	14 days	10/16/20	10/30/20
4.2 Write port scanning script	14 days	10/1/20	10/15/20
4.2.1 Automate port scanning script	14 days	10/16/20	10/30/20
4.3 Write Wi-Fi password cracking script	14 days	10/1/20	10/15/20
4.3.1 Automate Wi-Fi password cracking script	14 days	10/16/20	10/30/20
4.4 Write USB sanitizing script	14 days	10/1/20	10/15/20
4.4.1 Automate USB sanitizing script	14 days	10/16/20	10/30/20
4.5 Design general information webpage	28 days	1/11/21	2/8/21
4.5.1 Add information about common results	10 days	1/11/21	1/21/21
4.5.2 Add “next steps” instructions	10 days	1/21/21	1/31/21
4.5.3 Clean up webpage formatting	9 days	1/31/21	2/8/21
4.5.4 Provide security recommendations and best practices	10 days	2/8/21	2/18/21
5.0 Testing Phase	93 days	10/31/20	2/1/21
5.1 Test and run each script	10 days	10/31/20	11/10/20
5.2 Fix bugs or issues found in scripts	26 days	11/11/20	12/7/20
5.3 Add additional commands to supplement scripts and features	68 days	11/11/20	1/18/21
5.4 Run demo tests of each script with group	5 days	1/18/21	2/1/21

Table 3. Project Timeline

2.10 Problems Encountered and Analysis of Problems Solved

The team encountered several problems that hindered the project's progress. The magnitude of the problems encountered ranged in severity. Some problems were more severe, like project feasibility issues, while others were less severe, such as scheduling conflicts and delayed communication between team members.

The most severe problems that were encountered were that that the team's first and second project ideas had to be scratched, which resulted in six weeks of lost time. The team was worried about falling behind, and were proactive in reaching out to the advisor for guidance. This allowed for the development of a new project idea that was solid and feasible. All members worked with tenacity to get the project up and running and were able to successfully get the team back on track.

Another problem encountered was communication. All team members work full-time so it was difficult to make contact with one another at some points and responses were sometimes delayed. This caused minor issues with scheduling meetings, particularly when work sessions were needed for troubleshooting issues. To solve this problem, the team decided to dedicate at least one block of time a week, outside of class time, that all members would be free and available to regroup and work together. This allowed for troubleshooting issues to be resolved more efficiently.

Finally, the last problem that was encountered was associated with the Wi-Fi password cracking script. In order for the Wi-Fi password script to run, it had to disconnect Dragon from the Wi-Fi network and then reconnect. This characteristic made it difficult to implement a button on the webpage that the user could click to manually run the Wi-Fi password script. The team wanted the user to have the option to manually run all of the script features without having to

reboot Dragon each time. However, due to the required disconnection from and reconnection to the Wi-Fi network, the Wi-Fi password feature would not cooperate with a button. The team wanted all features to have a button but could not figure out a workaround for the Wi-Fi password feature to have a button. However, the team finally discovered tmux as a potential technology that would allow for the Wi-Fi password to have a button. After many trials and errors, the team was able to understand tmux and how to integrate it into the Wi-Fi password script. This allowed the Wi-Fi password feature to successfully have a button so that the user could run the script manually. Once this was accomplished, the team's project was completed.

2.11 Future Recommendations

After working on Dragon for the last two semesters, there are a couple things the team would do differently. If there was more time, the team would have made the webpage more colorful and aesthetically pleasing, as well as included more details and recommendations on how to make the user's network more secure. There would also be video demonstrations embedded in the webpage that would give more in-depth insight into various outputs and results the user might see. This would allow the user to compare different potential results because each individual's network and results would differ and it can be hard for the team to predict what the user would see for their outputs.

As a result, if the team had to complete the project all over again, there would be greater focus on video demonstrations that showed multiple results for each team member's network, as well as test volunteers. A potential idea that others had suggested was adding real-life scenarios and testimonies where individuals experienced security threats due to weak home network security. However, after the spring semester has ended, there are no plans to continue Dragon.

3. CONCLUSION

The fall semester was both challenging and rewarding for all team members. In the beginning of the semester, there were several obstacles that hindered the project's progress, but these were overcome due to the team's determination and tenacity. As a result, many lessons about communication, teamwork, and project management were learned. The project also allowed for all team members to develop their current skills and learn new technologies. This learning and skill development continued into the spring semester as the team focused on the webpage.

The team gained more insight into HTML and CSS during the spring semester when creating the webpage. During the spring semester, the team also learned a new technology called tmux. Tmux allowed for the integration of buttons on the webpage. The user clicked those buttons to manually start the various scripts if Dragon was already booted up. The team also was able to practice and hone their presentation and communication skills during the spring semester. As a result, the spring semester proved to be rewarding for all team members.

3.1 Lessons Learned

The team learned several valuable lessons during the project's timeframe. One lesson was that there should have been more time and thought spent on developing the project idea. The team would likely have avoided changing project ideas if more consideration had been put into the original project ideas. This was due to the original ideas being more software development-based, while all team members were on either the cybersecurity or networking track. The overall lesson learned here was to pick a project idea that works for all members' skills and abilities. Another lesson learned was that it was of high importance to communicate thoughts and feelings to one another, as everyone's input was valuable and helped shape and develop the project and

kept it on track.

3.2 Abilities and Skills Developed

The team developed and honed several skills throughout this project. All members further developed their scripting abilities, and all team members' co-op employers were impressed and appreciative of this skill. Knowing and understanding how to script is an important skill to have in one's career and made a person more marketable.

The team was also introduced to new technologies during this project. None of the members had ever worked with GitHub before, but it is a popular and valuable repository to have experience with. The team also had little prior experience with password cracking, so being exposed to Aircrack as a way to perform a dictionary attack was highly insightful for a group of cybersecurity and networking track students. Finally, tmux was the last new technology that the team learned. It was not until the spring semester that tmux was discovered, understood and used, but it was extremely useful in assisting in the final development and integration of the features into the webpage.

4. References

Amal, R. (2016, October 01). Learn to Hack WIFI password with Ubuntu (WPA/WPA2). Retrieved November 10, 2020, from https://www.learn2crack.com/2013/07/learn-to-hack-wifi-password-with-ubuntu.html

Chen, B. (2020, March 18). The Tech Headaches of Working From Home and How to Remedy Them. Retrieved October 12, 2020, from https://www.nytimes.com/2020/03/18/technology/personaltech/working-from-home-problems-solutions.html

Encarnacion, L. (2016). How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng. Retrieved November 10, 2020, from http://lewiscomputerhowto.blogspot.com/2014/06/how-to-hack-wpawpa2-wi-fi-with-kali.html

Karvonen, K., Vesterinen, P., & Manner, J. (n.d.). Easy-to-Use Firewall Management for Home Users. Retrieved December 04, 2020, from https://cups.cs.cmu.edu/soups/2007/workshop/Firewall_Management_for_Home_Users

Manning, W. (2020, September 09). Do You Know Whether Somebody Has Already Hacked Your Home Network? - Techno-Crime Institute. Retrieved December 04, 2020, from https://technocrime.com/know-whether-somebody-already-hacked-home-network/

Ritchie, H. (n.d.). Google Mobility Trends: How has the pandemic changed the movement of people around the world? Retrieved October 12, 2020, from https://ourworldindata.org/covid-mobility-trends

Tucakov, D. (2020, September 10). 17 Best Nmap Command Examples in Linux for System Administrators. Retrieved November 10, 2020, from https://phoenixnap.com/kb/nmap-command-linux-examples

Vogels, E., Perrin, A., Rainie, L., & Anderson, M. (2020, May 31). 53% of Americans Say the Internet Has Been Essential During the COVID-19 Outbreak. Retrieved October 12, 2020, from https://www.pewresearch.org/internet/2020/04/30/53-of-americans-say-the-internet-has-been-essential-during-the-covid-19-outbreak/