**Threats and Attacks on Endpoints**

**Key Contributors: Briah Graves**



**26 September 2022**

This project and the preparation of this report were funded in part by ….through an agreement with the University of the Incarnate Word.

Cyber Security Systems and the University of the Incarnate Word

EXECUTIVE SUMMARY

This report explains the different types of threats and attacks on endpoints and how to protect against them, and what can be done to prevent them from happening in the future. In order to present this information, I will be using a Gantt chart to show the progress along with a Trello and Github.

Project Milestones: E.g. Major steps required to complete your project.

1. Milestone 1: Different threats and attacks that can happen to endpoints
2. Milestone 2: How to protect against aforementioned threats and attacks
3. Milestone 3: How to prevent it from happening in the future

Materials List:

1. Item 1: Github
2. Item 2: Gaokao

Deliverables: E.g. Report, Deployed architecture, other project outcomes etc.

1. Deliverable 1: Trello
2. Deliverable 2: Github

Professional Accomplishments: E.g. New skills that you developed

1. Accomplishment 1: Learned how to detect threats and attacks on a computer
2. Accomplishment 2: Figured out how to exploit them
3. Accomplishment 3: How to prevent them from happening in the future

# PROJECT SCHEDULE MANAGEMENT

Create a Gantt chart with the application of your choice and replace it with the picture presented below.

Project Management Board Link (QR Code Only). Send invite to user: @gdparra

Qr code

Description automatically generated

Trello link: <https://trello.com/b/2znASH6T/f22-bg-threats-and-attacks-on-endpoints>

Create a Github Project Repository and add the user “cyberknowledge” as a contributor.

<https://github.com/04bri17/css-final-project>

# TABLE OF CONTENTS

Executive Summary [2]

Deliverables [3]

Milestones [5]

Implementation [8]

Resources [12]

Milestones

Different types of threats and attacks on endpoints

There are numerous types of threats and attacks on endpoints, but the main and   
popular ones are as follows: malware, ransomware, imprison, launch, snoop, deceive,   
and evade. Malware is a software that enters a computer system without the user’s   
knowledge or consent and then performs an unwanted and harmful action. [3]

Ransomware prevents a user’s endpoint from properly and fully functioning well until fee is paid; some ransomware pretends to come from a law enforcement agency while others pretend to come from a software vendor and displays a fictitious warning that a license has expired. [3]

You also have viruses, worms, and bots. There are two types of viruses: file-based virus (attached to a file that reproduces itself on the same computer without human interaction) and fileless virus (does not attach itself to a file but takes advantage of native services and processes that are part of the OS to avoid detection and carry out its attacks). [3]

How to protect against aforementioned threats and attacks

Back up your important data is the most important thing to do when it comes to protecting your information and systems. It’s important to always have more than one copy of your most important data so if your information happens to get stolen or lost, you have an extra copy and you are able to restore it. [1]

Limit sensitive personal info on social media. Basically, all this means is that if there’s no need to share more than just the basic information, then don’t. By] oversharing, it puts you at a higher risk of threats and attacks. [1]

Enable privacy and security settings; find out what privacy and security settings are available not just on your system, but on the social media sites as well and enable them. By doing this will give you another layer of protection. [1]

Lastly, use a password manager that helps keep track of all your passwords and the age of all of them. BY doing so, it allows you to determine which passwords are old and need to be replaced, and which ones are too similar to other websites. [1]

How to prevent these from happening in the future

First, you must secure the perimeter by using Next-Generation firewalls, integrate Advanced Malware Protection, Next-Generation Prevention Systems, etc. [2]

Second, protect users wherever they work because nowadays, 50% of employees are mobile and are working wherever they want and wherever they can get an internet connection by using a mobile device. Use VPNs and user verification and device trust so that whoever is using the device can verify it’s really them. [2]

Lastly, find and control problems fast. Breaches will happen so it’s important to identify and remove them as fast as possible. This requires extensive visibility and control as well as a well-prepared IT staff. [2]



**Attacks and Threats on Endpoints**

**Briah Graves**  
**26 September 2022**

This project and the preparation of this report were funded in part by monies provided by CPS Energy through an agreement with The University of Texas at San Antonio.

©CPS Energy and the University of Texas at San Antonio

**-----------------------------------------------------------------------------------------------------------------------------**

**EXECUTIVE SUMMARY**

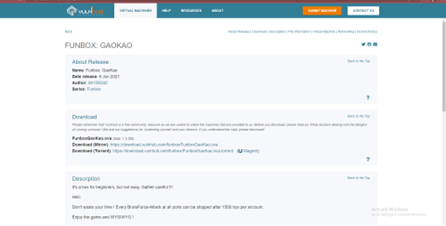
This report explains the different threats and attacks on endpoints and how to   
protect against them, and what can be done to prevent them from happening again in the   
future. In order to present this information, I will be using a Gantt chart to show the   
progress of this report along with a Trello board and Github.

**-----------------------------------------------------------------------------------------------------------------------------**

Implementation

Gaokao Funbox Simulator

[Figure 1] This is the site [www.vulnhub.com](http://www.vulnhub.com) where you can find the GAOKAO machine for users new to coding. [4]



PROCESS

The first step after installing GAOKAO is to identify the IP address of the target machine.

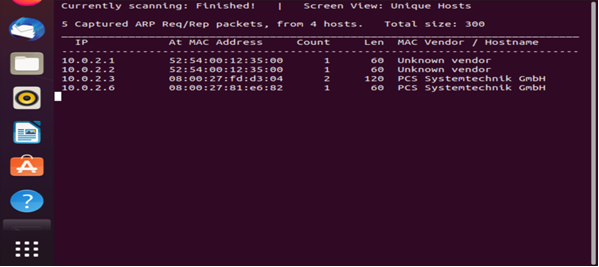
I installed netdiscover in order to find what I was looking for.

A picture containing text

Description automatically generated

[Figure 2]

After using the previous command, I was able to identify the machine I was looking for. You will know have found the correct target based on the range of the IP address



[Figure 3]

From here I know that the IP address of the target machine is 10.0.2.6.

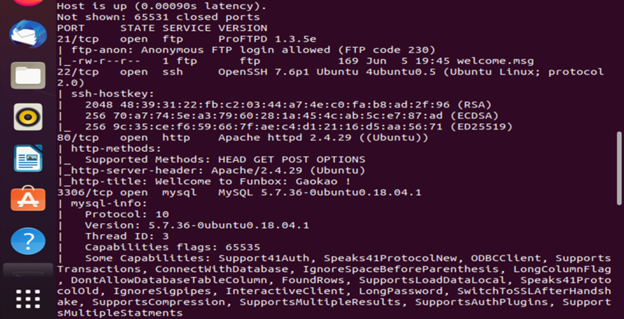
Then I used the nmap command to scan the IP address of the target machine. There I found a service or open ports that were exposed on the target machine.

[Figure 4]



This figure displays the completed scan achieved by using the command ‘sudo nmap’ which is a simple but thorough scan on your network.

[Figure 5]



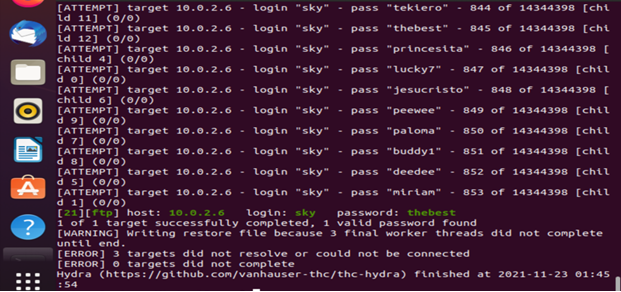
Above shows that I have discovered anonymous access to FTP servers, SSH servers, web servers, and mysql servers. Once you’re able to see all your servers you choose the best suited one for the machine. Here I logged in to 10.0.2.6 as an anonymous user. To do this, use the ‘ftp’ command.

[Figure 6]



At this point my machine read that the username I focused on was ‘Sky.’ There are different ways of using to bruteforce to uncover the password. The method I chose to use was by using the ‘hydra’ command. it’s pre-installed in Kali Linux, but you can use it to brute-force username and password. In the next figure, it will show that the command was successful because it will display in green the username ‘sky’ and the password ‘thebest.’

[Figure 7]



As a result, I retrieved the login information for the ftp server and logged in using this username and password.

[Figure 8]



In conclusion, this FunBox virtual program for new coding users showed the directory of the machine /home/sky. So, I realized that user.flag had a shell script, but unfortunately, it didn’t work, so I couldn’t proceed with that execution.

RESOURCES

* [10 Ways to protect yourself from Cyber Security Threats-https://moneyinc.com/10-ways-to-protect-yourself-from-cyber-security-threats/#:~:text=10%20Ways%20to%20Protect%20Yourself%20from%20Cyber%20Security,and%20Access%20to%20Social%20Media%20...%20More%20items](https://moneyinc.com/10-ways-to-protect-yourself-from-cyber-security-threats/) [1]
* Threat Prevention-How to stop Cyber Threats-https://www.cisco.com/c/en/us/products/security/what-is-threat-prevention.html#:~:text=Four%20steps%20for%20threat%20prevention%201%20Secure%20the,control%20problems%20fast%20Security%20breaches%20will%20happen.%20 [2]
* Module 3-Part 1(Lecture slides) [3]
* <https://www.Vulnhub.com> [4]