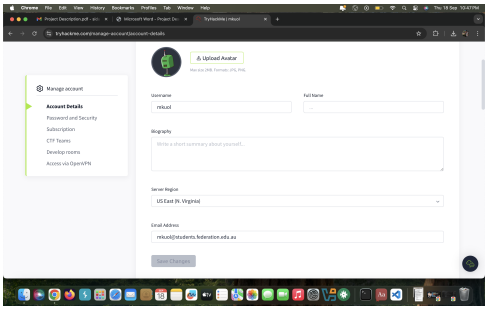

ITECH1502: Cybersecurity Fundamentals

Final Project Report

Forensic Log Analysis: Juicy Details

Michael Kuol
30339511

Platform Used: TryHackMe

September 18, 2025

Contents

1 Summary

This report details the forensic analysis of a simulated security incident conducted on the TryHackMe platform within the "Juicy Details" room. The objective was to act as a Security Operations Center (SOC) Analyst, tasked with investigating a set of server logs to understand the scope of a network intrusion. Through methodical log analysis, the attacker's tools, exploited vulnerabilities, and exfiltrated data were successfully identified. The investigation revealed a multi-stage attack involving reconnaissance (Nmap), brute-forcing (Hydra), SQL injection (SQLmap), directory brute-forcing (Feroxbuster), and data exfiltration via FTP. This project serves as a practical application of core cybersecurity concepts in log analysis and incident response.

2 Introduction

TryHackMe is a prominent online platform that provides hands-on cybersecurity training through interactive labs known as "rooms". It is widely used by students and professionals to develop practical skills in a safe, gamified environment. For this project, the "Juicy Details" room was selected due to its direct relevance to the unit topics of incident response and forensics. The room provides a realistic scenario where an analyst must sift through log files—a fundamental skill for any cybersecurity role—to piece together the narrative of a cyberattack. My registration on the platform, verified with my Federation University email, is shown in Figure 1.

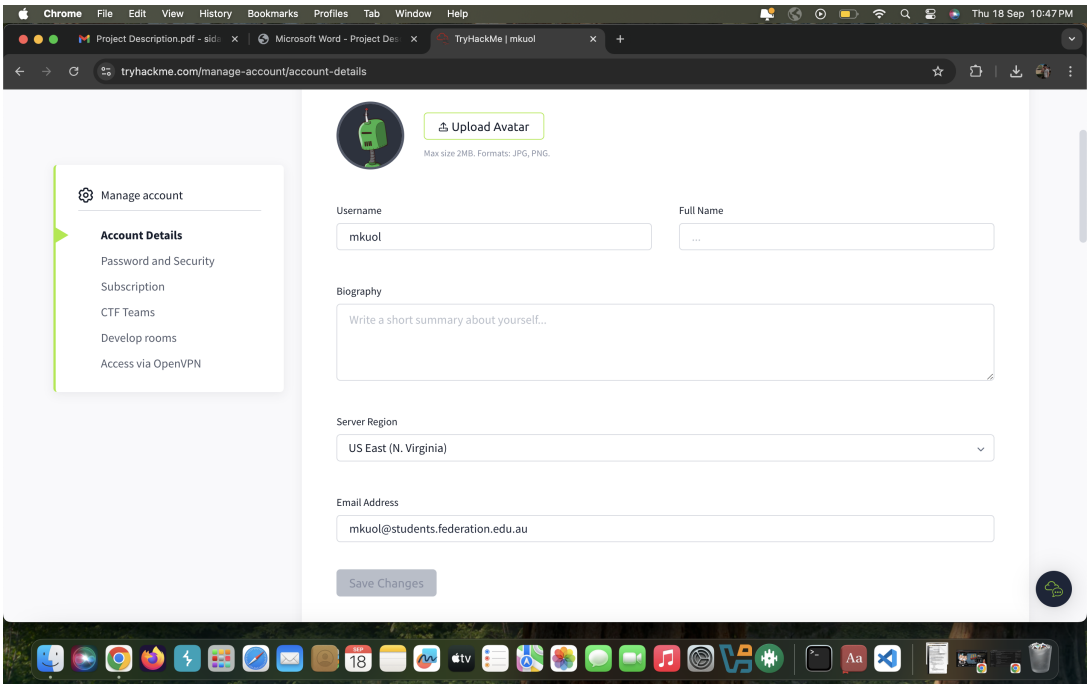

Figure 1: Account verification with FedUni email on TryHackMe.

3 Problem and Objectives

3.1 Problem/Challenge

The challenge places the user in the role of a SOC Analyst for a company named "Juice Shop". An attacker has breached the network, and the only available evidence is a zip file containing three server logs: 'access.log' (web server), 'auth.log' (authentication), and 'vsftpd.log' (FTP server), as shown in Figure 2. The task is to analyze these logs to retrospectively identify the attacker's full methodology.

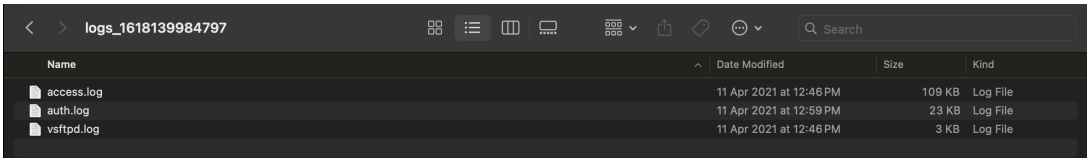

Figure 2: The provided log files for the investigation.

3.2 Project Goal/Objectives

The primary goal was to successfully complete the TryHackMe room by answering all investigative questions correctly. The specific objectives were to:

- Identify the sequence of tools used by the attacker for reconnaissance and exploitation.
- Determine which system endpoints were vulnerable to specific attacks like brute-force and SQL injection.
- Trace the attacker's actions to identify what sensitive data was accessed and stolen.
- Apply command-line tools for efficient log file analysis.

4 Methodology

The investigation was conducted by systematically analyzing the three provided log files. The primary tool used for analysis was the 'grep' command to filter and search for specific keywords and patterns within the logs.

4.1 Phase 1: Reconnaissance and Tool Identification

The first step was to analyze the 'access.log' to identify the tools used by the attacker, which are often revealed in the User-Agent string of HTTP requests.

- **Nmap, Curl, Feroxbuster:** Searching the log for these tool names revealed their usage for initial scanning and directory discovery.
- **Hydra:** Filtering the log for "Hydra" showed a large volume of requests to a login endpoint, indicating a brute-force attack (Figure 3).
- **SQLmap:** Filtering for "sqlmap" revealed automated SQL injection attempts against a search parameter (Figure 4).

The order of occurrence in the log was determined to be: nmap, hydra, curl, sqlmap, feroxbuster.

4.2 Phase 2: Vulnerability Analysis

Based on the tool identification, the logs were further analyzed to pinpoint specific vulnerabilities.

- The Hydra traffic was exclusively directed at the `/rest/user/login` endpoint, identifying it as the target of the brute-force attack. A successful login was confirmed by searching for a request from Hydra that received a HTTP 200 OK status code.
- The SQLmap traffic targeted the `/rest/products/search` endpoint, using the 'q' parameter for the injection.

This analysis successfully answered the questions in the reconnaissance task, as confirmed in Figure 7.

4.3 Phase 3: Stolen Data Investigation

The final phase focused on what data the attacker successfully exfiltrated.

- By searching 'access.log' for keywords, it was found that the attacker scraped user email addresses from the `/rest/products/reviews` endpoint (Figure 5).
- The 'vsftpd.log' was analyzed to investigate FTP activity. It showed a successful anonymous login and the download of two backup files: 'coupons$_2$013.*md.bak*'*and*'*www−data.bak*'(*Figure*6).
- The 'auth.log' file was examined for shell access attempts, which revealed a successful SSH login for the user 'www-data'.

5 Results and Outcomes

The methodical investigation yielded a complete picture of the attack and resulted in the successful completion of the room (Figure 8).

5.1 Evidence of Attacker Tools

The logs provided clear evidence of the tools used by the attacker.

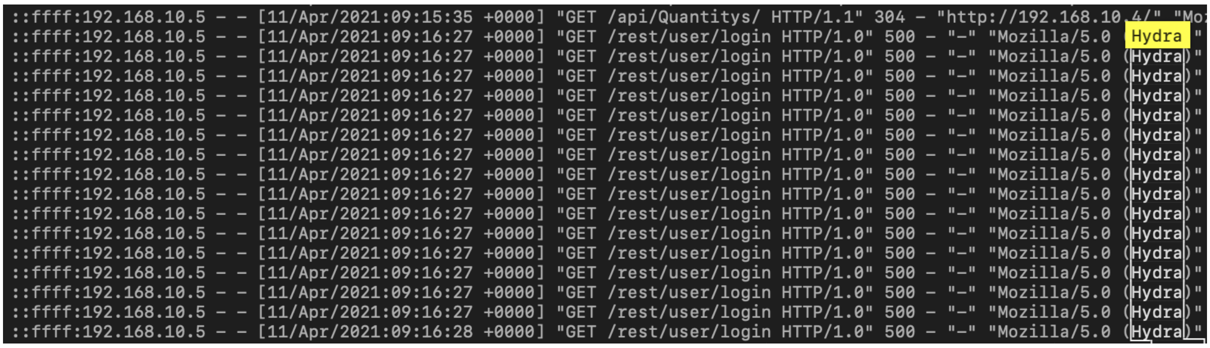

Figure 3: Evidence of a brute-force attack using Hydra in ‘access.log‘.

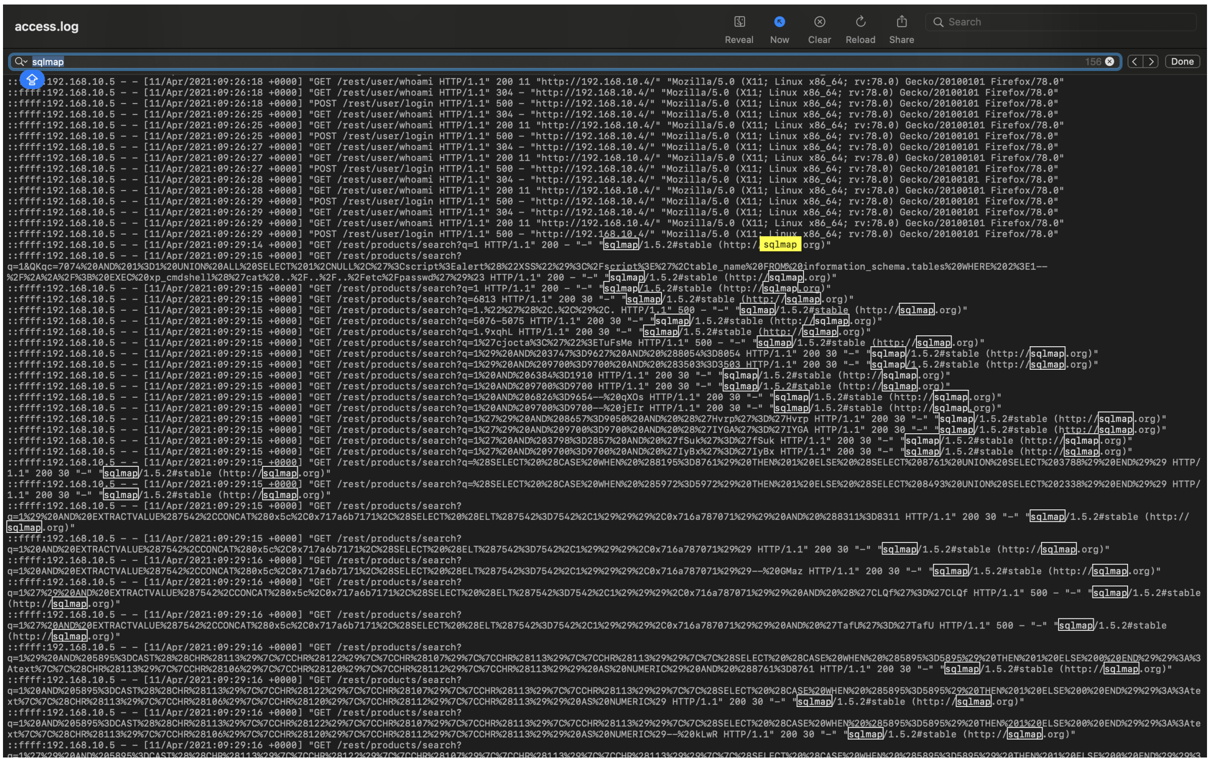

Figure 4: Evidence of SQL injection attempts using SQLmap in ‘access.log‘.

5.2 Evidence of Data Exfiltration

The investigation successfully identified multiple instances of data theft.

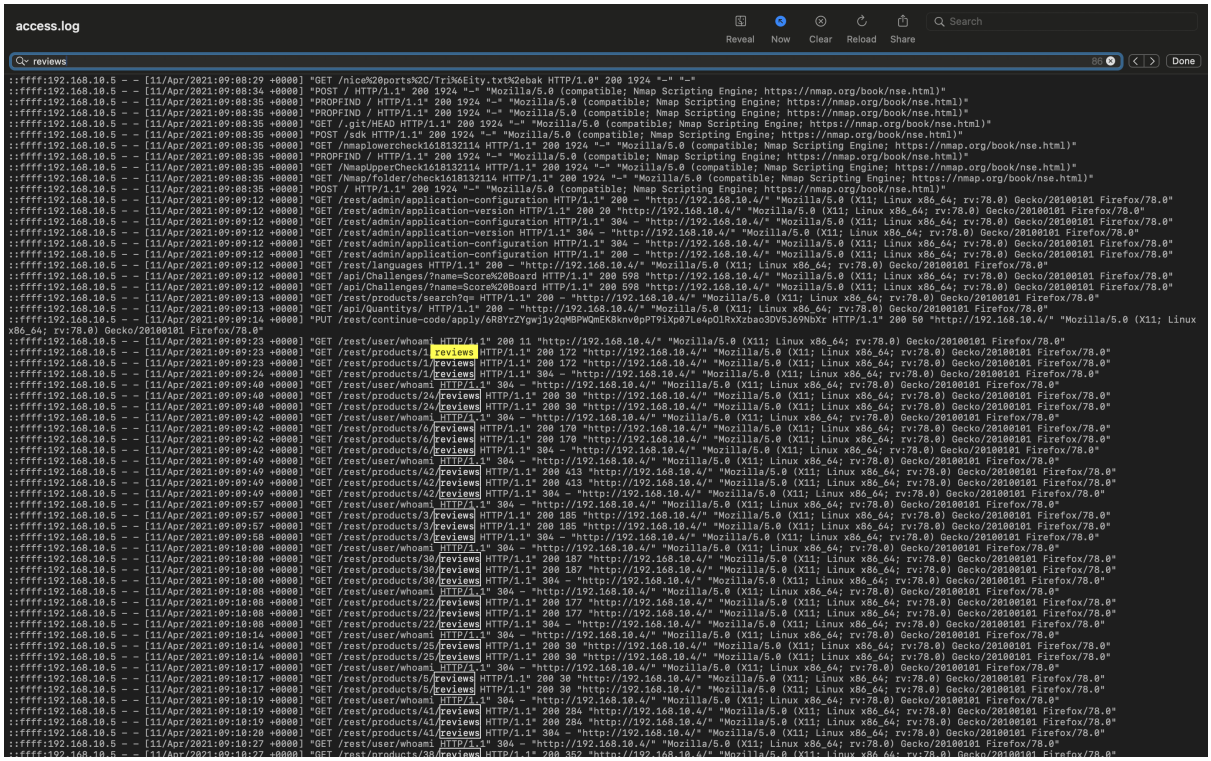

Figure 5: Log entries showing the scraping of user data from product reviews.

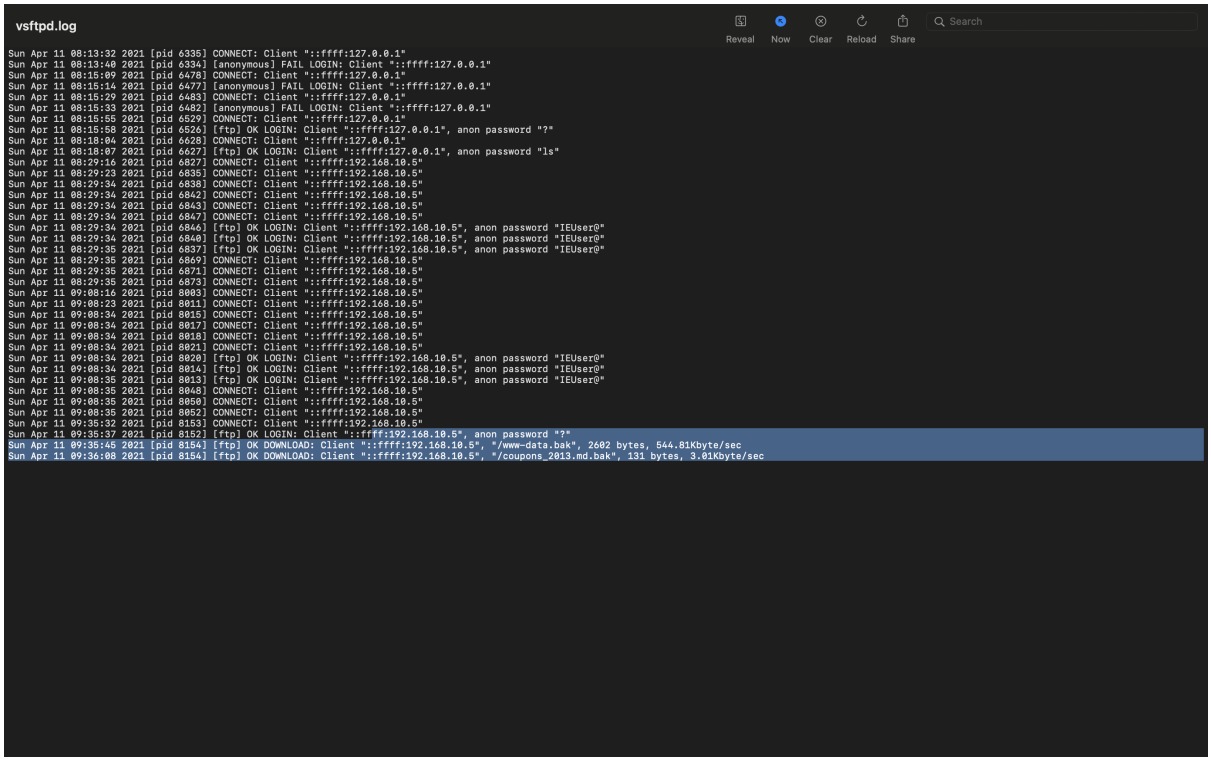

Figure 6: The ‘vsftpd.log‘ shows the attacker downloading backup files via anonymous FTP.

5.3 Project Completion

All tasks were successfully completed, demonstrating a full understanding of the attacker's path.

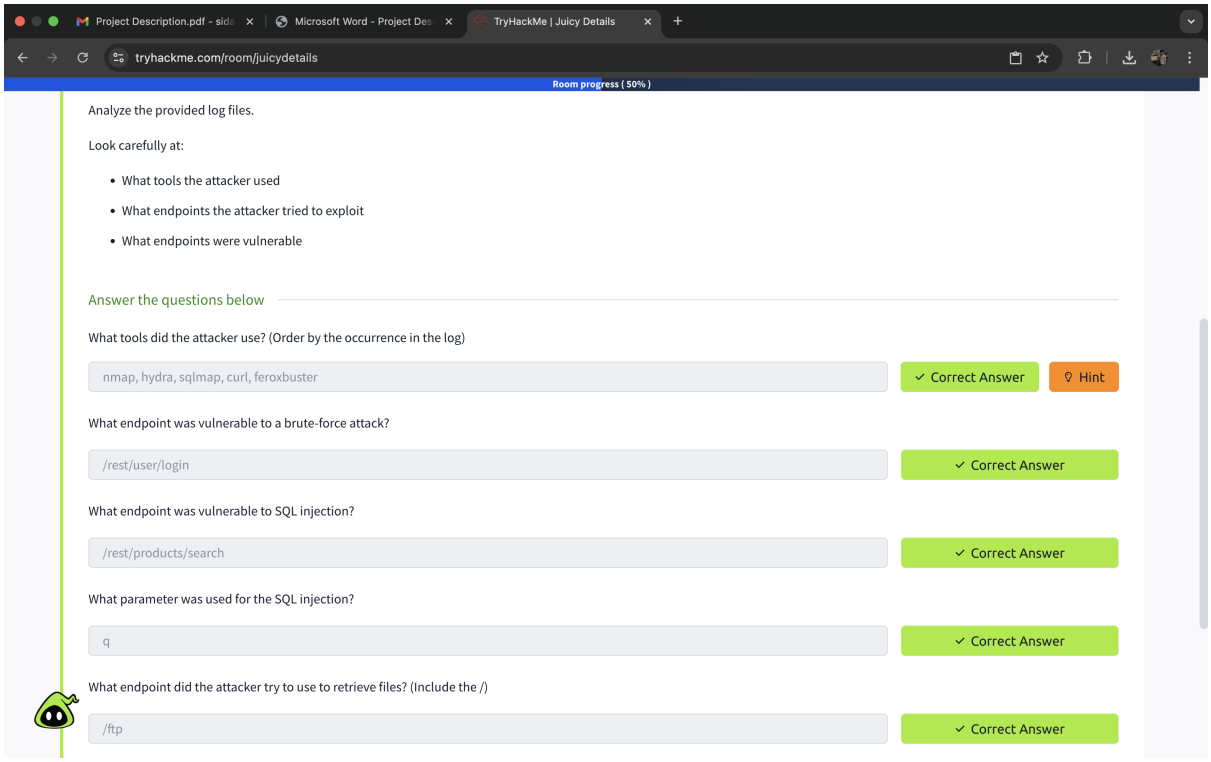

Figure 7: Successful completion of the Reconnaissance section.

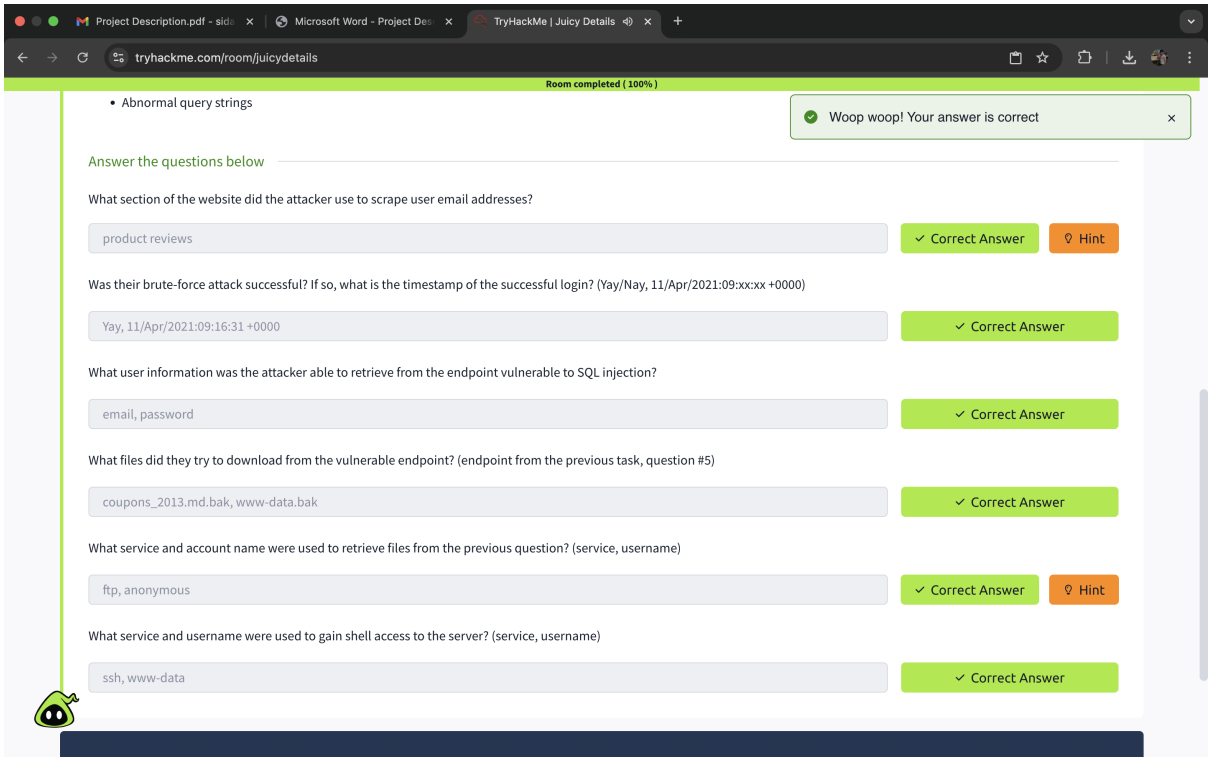

Figure 8: 100% completion of the Juicy Details room on TryHackMe.

6 Reflection

6.1 What I Learned

This exercise provided significant hands-on experience in forensic log analysis. I learned how different attack tools leave distinct fingerprints in common server logs, such as the User-Agent strings left by Nmap and SQLmap or the repetitive requests from Hydra. I became more proficient with using command-line tools like ‘grep‘ to quickly parse thousands of log entries for critical evidence. Most importantly, I learned how to connect disparate pieces of information across different logs (‘access‘, ‘auth‘, ‘vsftpd‘) to build a cohesive timeline of an attack.

6.2 Contribution to Professional Growth

This project directly simulates the day-to-day responsibilities of a SOC Analyst or Digital Forensics investigator. The skills practiced here—attention to detail, methodical analysis, and evidence correlation—are foundational for any defensive cybersecurity role. Having a documented project like this in my portfolio serves as tangible proof of my ability to apply theoretical knowledge to a practical, real-world challenge, which will be invaluable when applying for internships or entry-level positions.

6.3 What I Would Do Differently

If I were to repeat this task, I would try to leverage more advanced command-line tools to make the analysis even more efficient. For instance, I could use a combination of ‘awk‘, ‘sort‘, and ‘uniq‘ to quickly summarize the top attacked endpoints or source IP addresses instead of manually scrolling through ‘grep‘ results. I would also spend more time researching the specific versions of the tools mentioned in the logs to understand if their signatures have changed over time, which would be relevant in a real-world investigation.

7 Conclusion

The ”Juicy Details” challenge was successfully completed by methodically analyzing the provided logs. The investigation revealed that an attacker used a sequence of common hacking tools to identify and exploit vulnerabilities in a web application, ultimately leading to the theft of sensitive user data and credentials. This project effectively demonstrated the critical role of log analysis in post-incident forensics and reinforced the practical skills required to deconstruct a cyberattack.

8 Portfolio Link

A summary of this project is included in my professional cybersecurity portfolio, which is maintained on GitHub.

- **GitHub Portfolio:** https://github.com/mkuol2022/Portfolio-Setup/