Strathmore University

@iLabAfrica Centre

INDUSTRIAL ATTACHMENT REPORT

Attachment Duration: January 30th, 2023 - March 24th, 2023

Name: Ian Peter

Registration Number: SCT211-0036/2018

Degree: BSc. Computer Science

Name and Address of the Company/Institution Attached: iLab Africa, Strathmore University, Nairobi

Industry-based Supervisor: Jayson Waigwa

Introduction

This report provides a comprehensive overview of my industrial attachment at iLab Africa, Strathmore University, Nairobi, which took place from January 30th to March 24th, 2023. The purpose of this attachment was to gain practical experience in the field of Computer Science, complementing the theoretical knowledge acquired during my BSc. Computer Science course at Jomo Kenyatta University of Agriculture and Technology.

iLab Africa is a leading technology hub that provides an ideal environment for innovation, research, and development in Information and Communication Technology (ICT). It offers a wide range of services and opportunities, including cybersecurity training, digital forensics, and performance testing, among others. This made it an excellent setting for my industrial attachment, allowing me to apply and enhance my skills in a real-world context.

The objective of this report is to detail the activities I was involved in, the new skills I acquired, the challenges I encountered, and the solutions I implemented during my attachment period. This report also aims to provide a reflection on my learning experience, demonstrating how the practical knowledge gained complements my academic studies.

The report is structured to provide a detailed account of my weekly tasks, a comparison of the challenges faced with the content taught in my course, and a discussion of the new skills learned. It also includes my suggestions for improving the program to enhance the learning experience for future students.

Thank you for providing the structure. Here is the revised content for the "Main Content" section of your report:

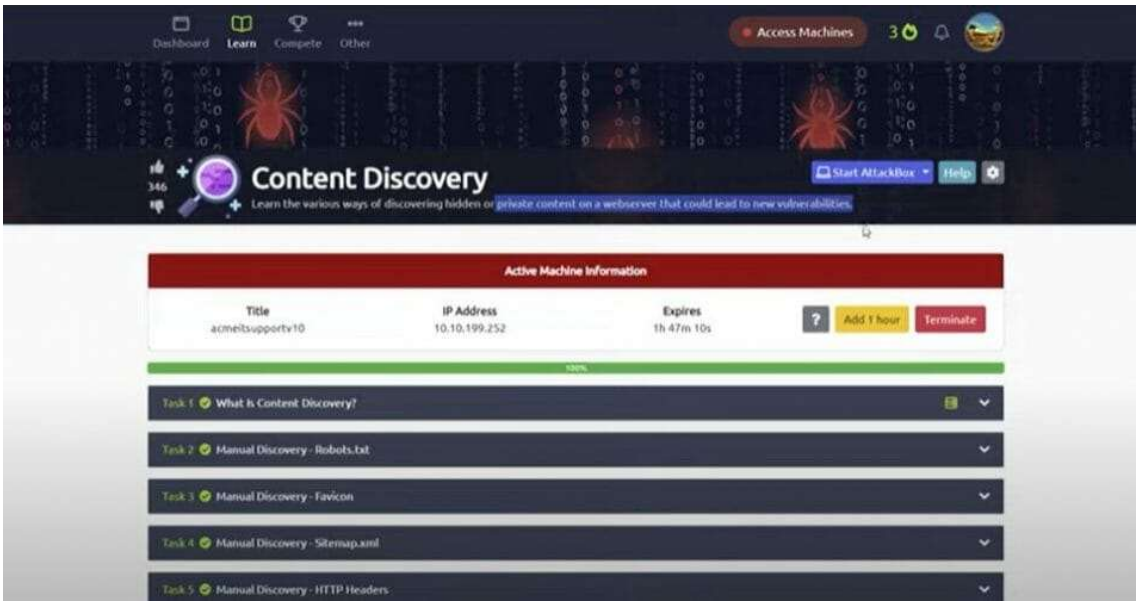
Main Content

Overview of Activities

During my attachment at iLab Africa, Strathmore University, I was involved in a variety of tasks and activities that allowed me to apply and expand my knowledge in cybersecurity. These activities ranged from assisting in teaching cybersecurity courses, developing guidelines for a Digital Forensics Lab, working on performance testing projects, to setting up a Wazuh server for SIEM solutions.

Week 1: Introduction and Orientation

I was introduced to the team and the various projects they were working on. I was assigned to the Cybersecurity training department with a team of five other people. I was involved in populating the iCPT course timetable and researching extensively on courses offered at iLab Africa in preparation for the open day. I also completed the content discovery room on TryHackme, a platform that provides an interactive, hands-on environment for learning cybersecurity, where I learned ways of discovering hidden content on a webserver.



A screenshot of the TryHackme platform with the content discovery room.

Week 2: Digital Forensics and Penetration Testing

I worked with a team to develop guidelines for a Digital Forensics Lab and completed the Overpass 2 – Hacked on TryHackme, where I learned PCAP analysis. I also learned how to detect and exploit SQL injection vulnerabilities and how to use tshark for PCAP analysis. Tshark is a network protocol analyser that captures and interactively browses the traffic running on a computer network.

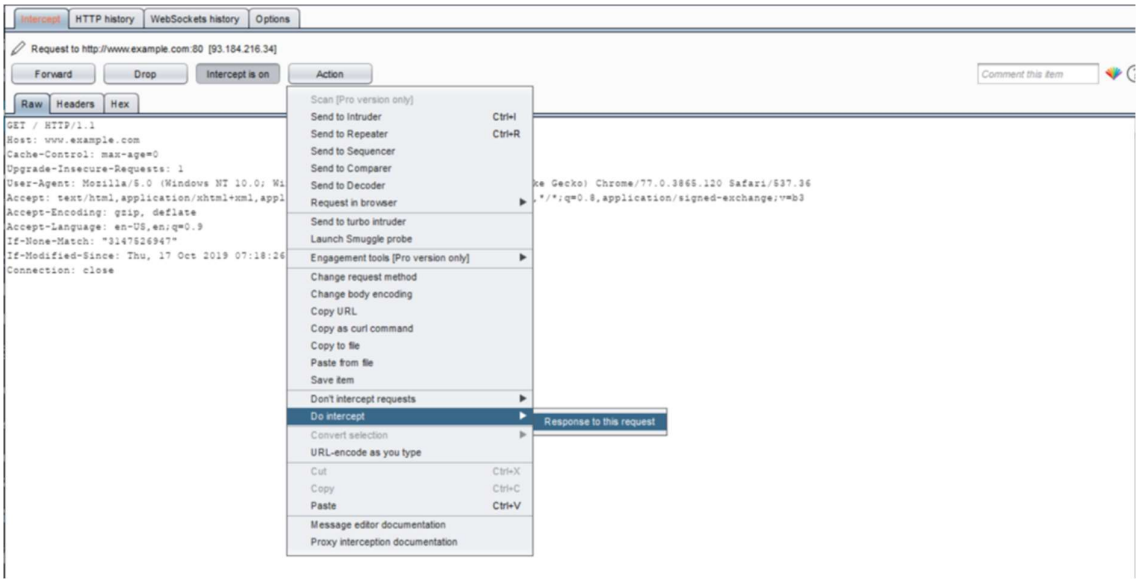
I was assigned to a team of four other mentees to develop various labs for the Digital Forensics module.

```
ubuntu@ip-172-31-26-215:~/working$ tshark -r dnscat2.pcap -T fields -E header=y
 -e ip.src -e ip.dst -e ip.proto -e udp.dstport -e ip.len -e frame.time_delta_d
isplayed ip.dst==165.227.88.15 | head -20
ip.src  ip.dst  ip.proto        udp.dstport     ip.len  frame.time_delta_displa
yed
192.168.88.2    165.227.88.15   17      53      89      0.000000000
192.168.88.2    165.227.88.15   17      53      89      1.074819358
192.168.88.2    165.227.88.15   17      53      89      1.084471967
192.168.88.2    165.227.88.15   17      53      89      1.078728781
192.168.88.2    165.227.88.15   17      53      89      1.069749570
192.168.88.2    165.227.88.15   17      53      89      1.077714934
192.168.88.2    165.227.88.15   17      53      89      1.076642909
192.168.88.2    165.227.88.15   17      53      89      1.070790122
192.168.88.2    165.227.88.15   17      53      89      1.071048506
192.168.88.2    165.227.88.15   17      53      89      1.064914560
192.168.88.2    165.227.88.15   17      53      89      0.093778795
192.168.88.2    165.227.88.15   17      53      89      0.961346162
192.168.88.2    165.227.88.15   17      53      89      1.062188142
192.168.88.2    165.227.88.15   17      53      89      1.065854491
192.168.88.2    165.227.88.15   17      53      89      1.075033821
192.168.88.2    165.227.88.15   17      53      89      1.066068845
192.168.88.2    165.227.88.15   17      53      89      1.063321512
192.168.88.2    165.227.88.15   17      53      89      1.071506357
192.168.88.2    165.227.88.15   17      53      89      1.058017495
ubuntu@ip-172-31-26-215:~/working$
```

A screenshot of tshark in action, showing the analysis of network traffic.

Week 3: Web Application Security and Penetration Testing

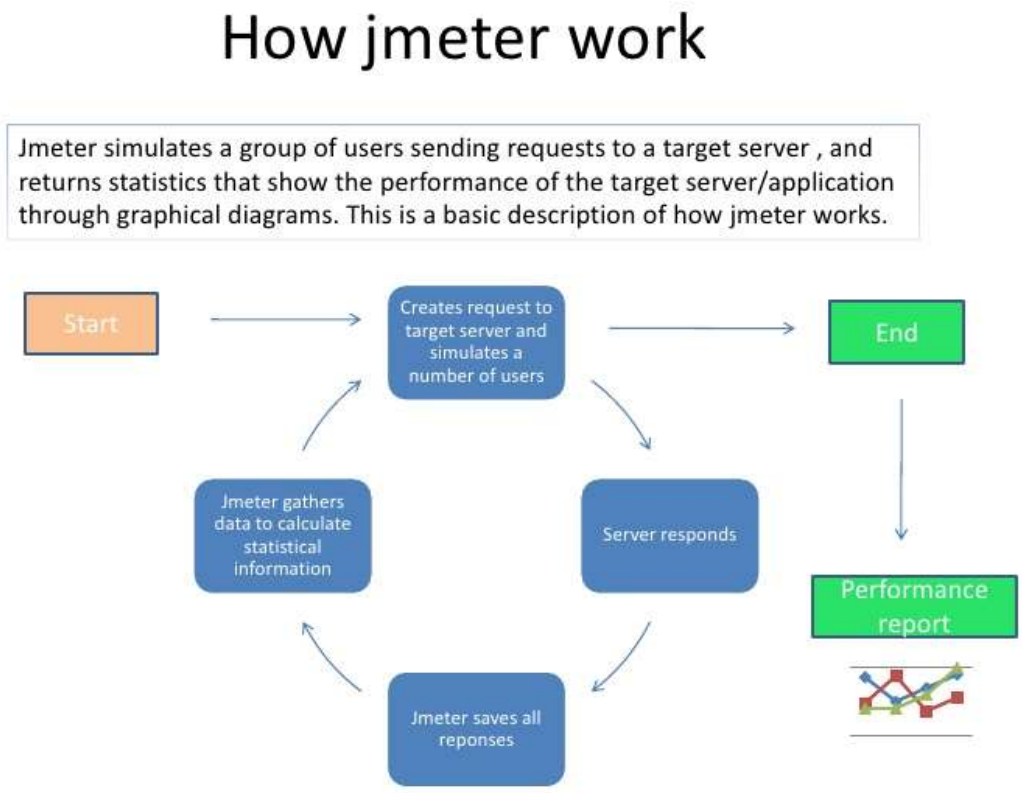
The third week was focused on web application security. I learned how to use Burp suite, a graphical tool for testing web application security, to alter intercepted requests and completed two more reports on the penetration test. I also learned to use ZAP proxy to spider a website and enumerate as much information as possible.



A screenshot of Burp Suite, showing how it can be used to alter intercepted requests.

Week 4: Performance Testing and Teaching Assistance

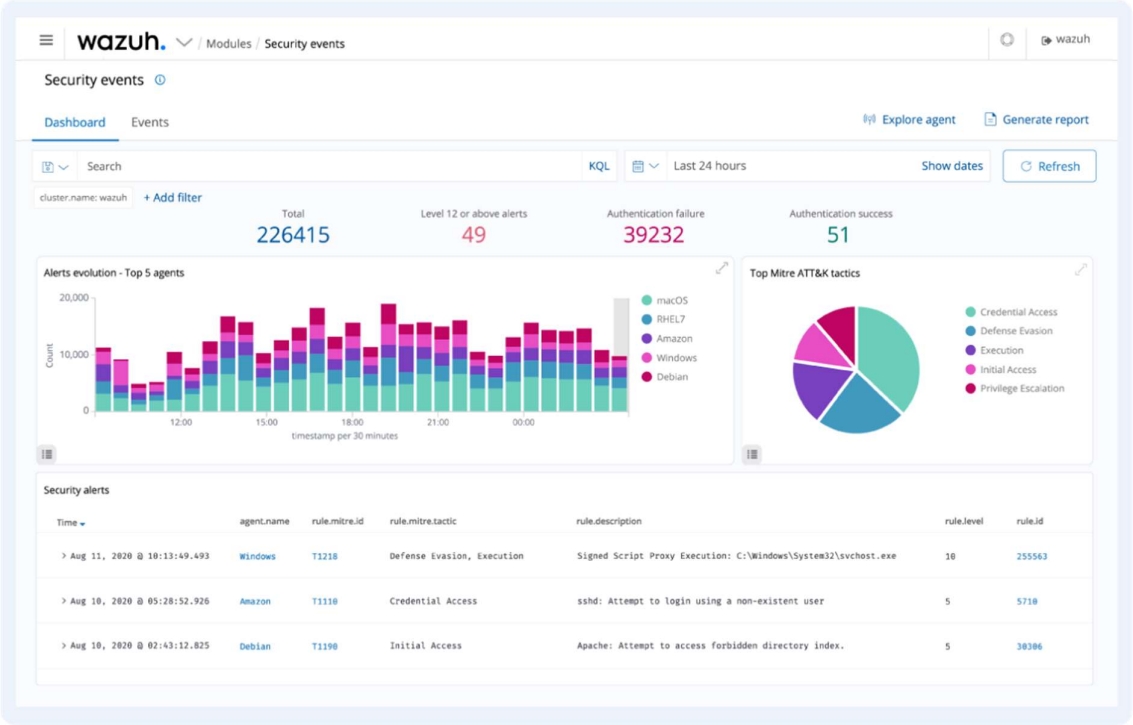
In the fourth week, I worked on a performance testing project that required logging with the Apache JMeter tool, an open-source software designed to load test functional behavior and measure performance. I also served as a teaching assistant in the iCPT class about Linux systems. I learned how to integrate a custom python script into the Apache JMeter tool to work on performance tests better.



Description of how JMeter works. Image Credits: https://octoperf.com/img/blog/jmeter-tutorial/how-jmeter-works.jpg

Week 5: Digital Forensics and Incidence Response

During the fifth week, I set up Wazuh server to work as a SIEM solution in conjunction with the iLab security team. Wazuh is a free and open-source platform used for threat detection, integrity monitoring, incident response, and compliance. I also tackled challenges on picoCTF with the team from iLab. I served as a teaching assistant in using Scripting for Security.

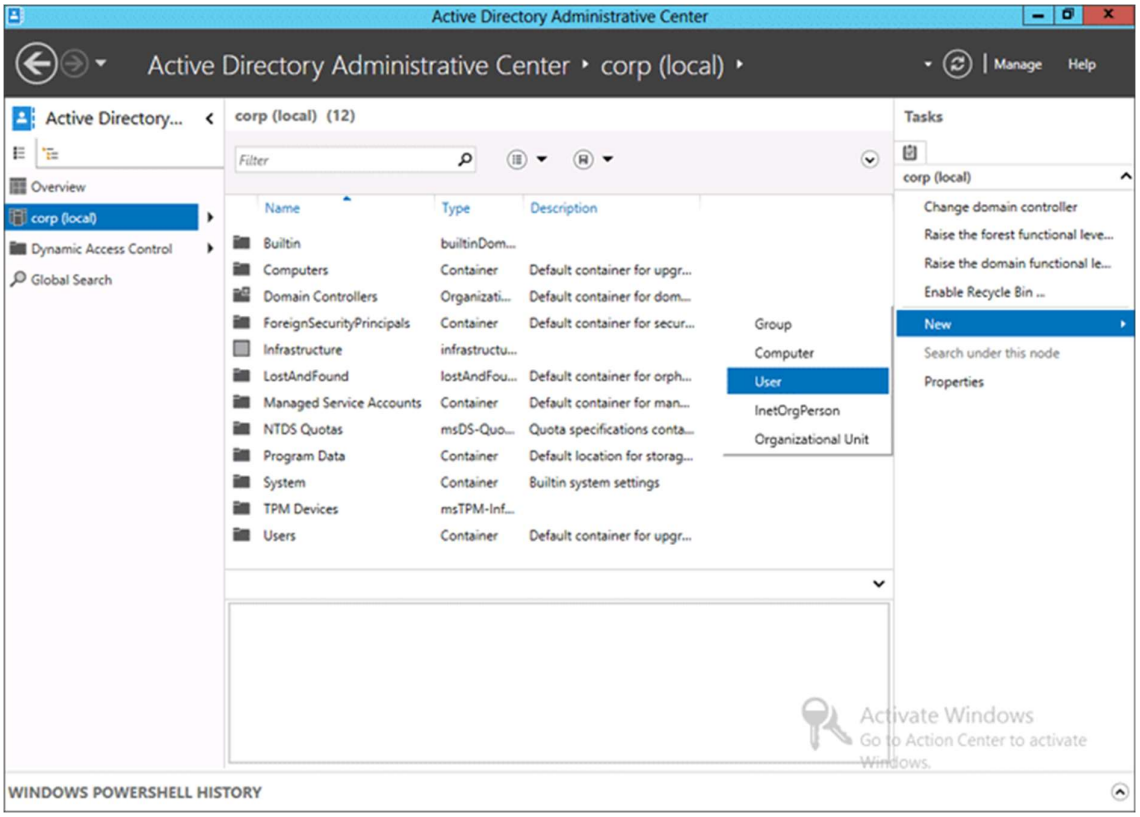


A screenshot of the Wazuh platform, showing how it can be used for threat detection and incident response.

Week 6: Active Directory and Teaching Assistance

In the sixth week, I served as a teaching assistant in an online Windows Active Directory class on Enumerating Active Directory. Active Directory (AD) is a Microsoft technology used to manage computers and other devices on a network.

I also taught a class on Windows Active Directory dealing with Active Directory Exploitation.

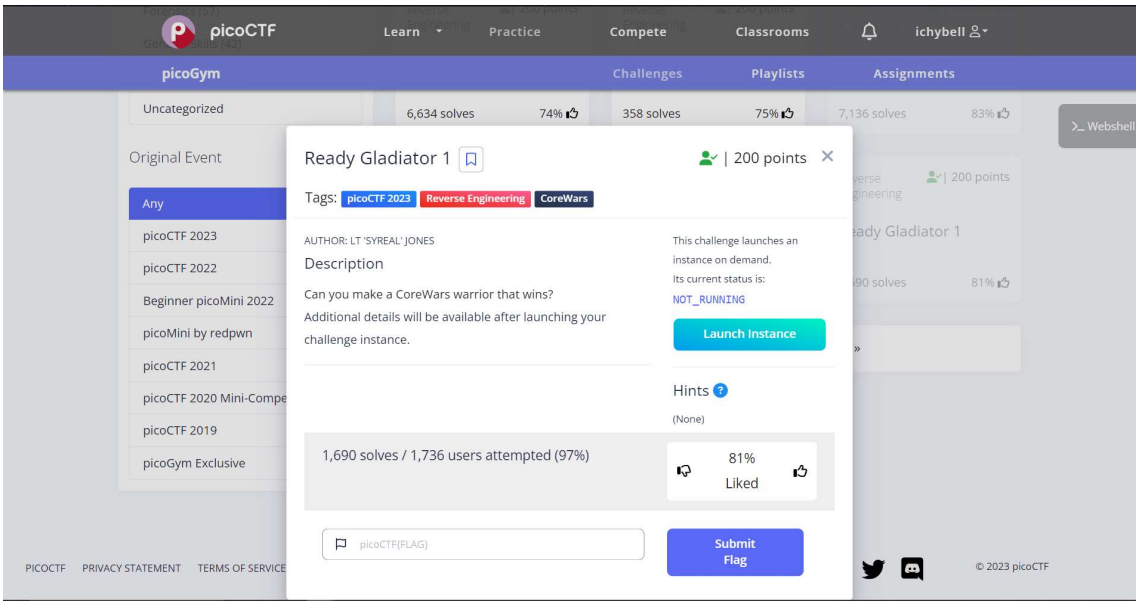


A screenshot of the Windows Active Directory interface.

Week 7: Cryptography and Reverse Engineering

The seventh week was heavily focused on learning new skills in cryptography and reverse engineering by use of picoCTF. PicoCTF is a free, online cybersecurity competition hosted by Carnegie Mellon University where participants must solve a variety of challenges to earn points.

I successfully completed a CTF challenge on Reverse Engineering using Ghidra to disassemble code and exploit flaws.



A screenshot of the picoCTF platform, showing a challenge being solved.

Week 8: Conclusion and Final Reflections

In the final week, I continued to serve as a teaching assistant and worked on several challenges on picoCTF. I also assisted in setting up a Windows Active Directory on AWS environment. AWS, or Amazon Web Services, is a cloud services platform that provides computing power, database storage, and other functionality.

Full Coverage of the Course

The attachment at iLab Africa allowed me to apply and practice the knowledge and skills I've learned from my course. The tasks I was involved in directly related to the courses I had taken, such as Introduction to Computer Systems, Computer Organisation, Introduction to Computer Programming, Introduction to Systems Programming, Object Oriented Programming, Data Structures and Algorithms, and Discrete Structures.

Problems Encountered

During the attachment, I encountered a few challenges. One of the main challenges was understanding and applying complex cybersecurity concepts during the development of the cybersecurity training module and the digital forensics lab. However, I was able to overcome this challenge by conducting extensive research, practicing on platforms like TryHackme, and seeking guidance from my supervisor and colleagues.

Another challenge was managing multiple tasks simultaneously. Balancing between assisting in teaching, working on performance testing projects, and setting up a Wazuh server required effective time management and prioritization. I was able to overcome this challenge by developing a detailed work plan and regularly updating it to reflect my progress and priorities.

New Skills Learned

During my attachment, I acquired a variety of new skills that will be beneficial for my future studies and career. These include:

1. **Advanced Cybersecurity Techniques:** I gained hands-on experience with advanced cybersecurity tools and techniques. For instance, I learned how to use Burp Suite for web application security testing. This tool allowed me to intercept, inspect, and modify network requests, which is crucial for identifying and exploiting vulnerabilities in web applications. I also learned to use tshark for PCAP analysis, which involved inspecting network traffic to detect anomalies or potential security threats. Furthermore, I learned to set up and use a Wazuh server for Security Information and Event Management (SIEM). This experience gave me a practical understanding of how to monitor and analyse security alerts in a network environment.
2. **Performance Testing**: I developed skills in performance testing through my work with Apache JMeter. This involved designing and executing tests to evaluate the speed, responsiveness, and stability of web applications under different workloads. I also learned to integrate custom Python scripts into JMeter, which allowed me to create more flexible and powerful testing scenarios.
3. **Teaching Assistance**: Serving as a teaching assistant provided me with valuable experience in communicating complex technical concepts in a clear and understandable manner. This not only reinforced my own understanding of these concepts but also helped me develop essential communication and presentation skills.
4. **Working in a Team**: Working on various projects with a team at iLab Africa helped me enhance my teamwork and collaboration skills. I learned how to coordinate tasks, share knowledge, and work towards common goals effectively with others.
5. **Project Management**: Managing multiple tasks and projects simultaneously taught me valuable lessons in time management, prioritization, and project planning. These skills will be invaluable in any future academic or professional endeavours.

Conclusion

Reflecting on my attachment at iLab Africa, Strathmore University, I can confidently say that it was a transformative experience that significantly enriched my academic journey. The opportunity to apply theoretical knowledge from my coursework in a practical, real-world setting was invaluable. It not only reinforced my understanding of key concepts but also highlighted the relevance and applicability of what I've learned.

The new skills I acquired, from advanced cybersecurity techniques to performance testing, from teaching assistance to teamwork, have broadened my skill set and prepared me for future challenges in the field of Computer Science. These skills are not just limited to technical knowledge; they also encompass essential soft skills like communication, teamwork, and time management, which are crucial for any professional setting.

Moreover, the experience of working in a professional environment allowed me to observe and learn from experienced professionals in my field of interest. It provided me with insights into the workings of the industry, the challenges faced, and the innovative solutions being developed.

In conclusion, the attachment was more than just a requirement for my course; it was a steppingstone into the professional world. It has equipped me with the skills, experience, and confidence to face future academic and professional challenges. I am grateful for this experience and look forward to applying what I've learned in my future endeavours.

References

1. TryHackme. (2023). Content Discovery Room. Retrieved from https://tryhackme.com
2. Wireshark. (2023). Tshark Documentation. Retrieved from https://www.wireshark.org/docs/man-pages/tshark.html
3. Apache JMeter. (2023). User Manual. Retrieved from https://jmeter.apache.org/usermanual/index.html
4. Wazuh. (2023). Documentation. Retrieved from https://documentation.wazuh.com/current/
5. PicoCTF. (2023). About PicoCTF. Retrieved from https://picoctf.com/about

Appendices

Please refer to the attached documents for additional information, including my weekly progress charts from my logbook.