INDUSTRIAL ATTACHMENT REPORT

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

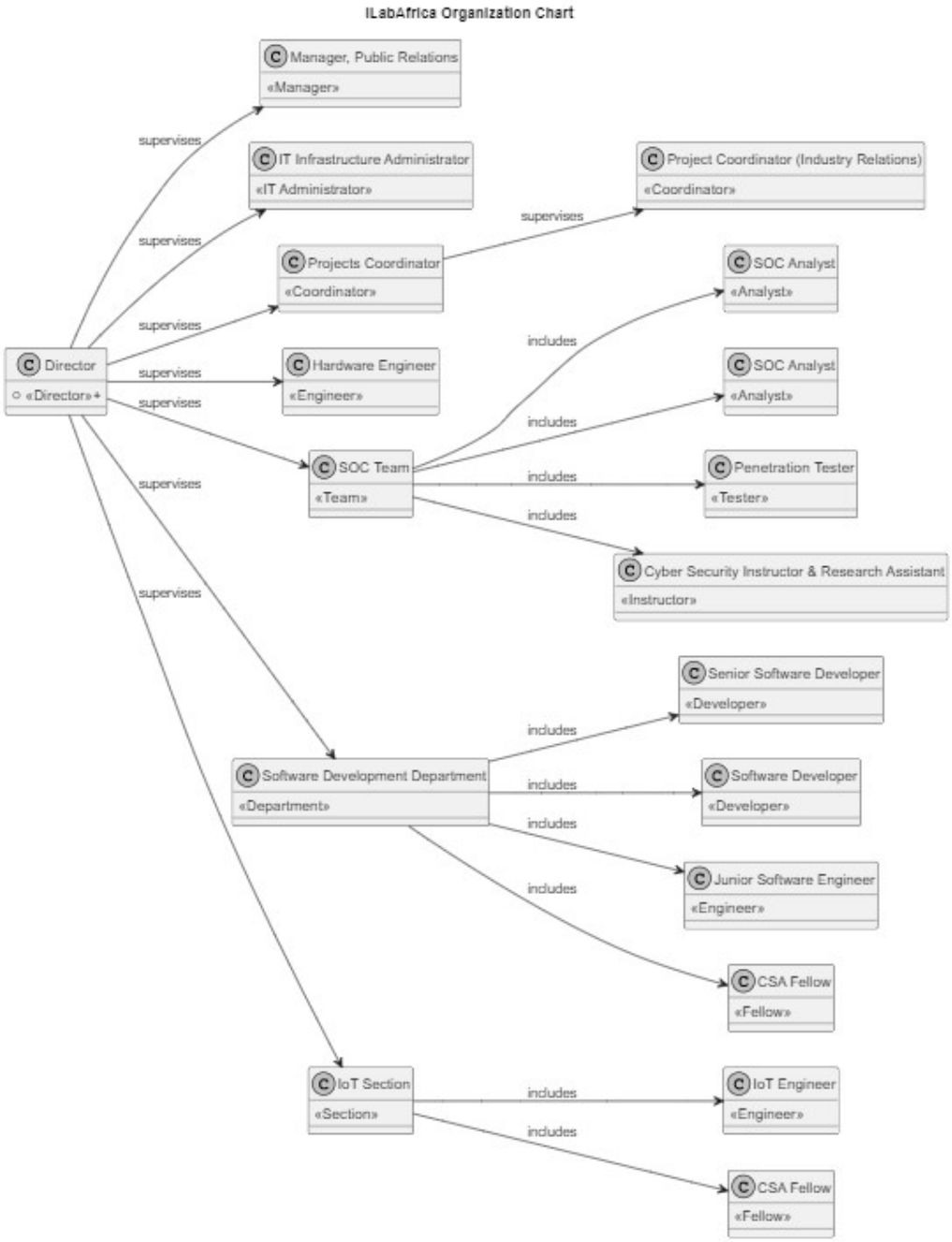
Industry-based Supervisor: Jayson Waigwa

Table of Contents

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, a centre of excellence in Information Communication Technology (ICT) innovation and development based at Strathmore University, was my chosen place of attachment. The centre's mission to innovate and provide ICT solutions that contribute towards societal development aligned with my personal aspirations, making it an ideal environment for my professional growth.



Organizational chart for iLab Africa

Prior to my attachment, I had high expectations. I anticipated a challenging yet rewarding experience where I would apply the theoretical knowledge I had gained from my coursework to real-world scenarios. I looked forward to working with experienced professionals who would guide me and provide insights into the ICT industry. As I embarked on this journey, I was eager to learn, adapt, and contribute to the best of my abilities.

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.

Main Content

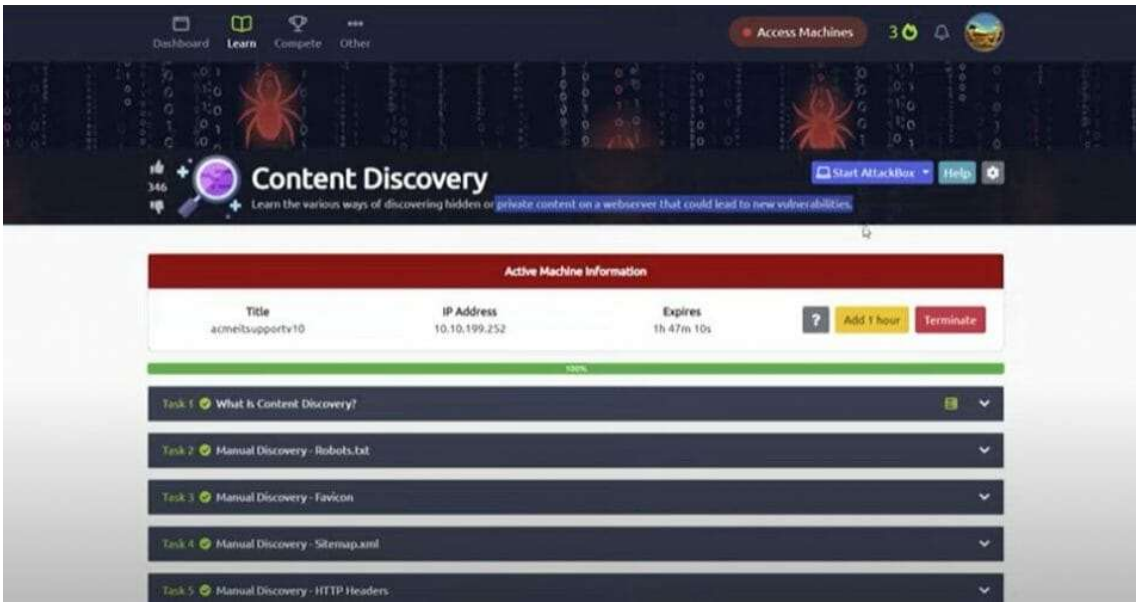
Overview of Activities

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

During my first week, I was introduced to the Cybersecurity training department, a team of five dedicated professionals. My primary task was to assist in populating the iCPT course timetable, a responsibility that required meticulousness and a deep understanding of the course structure. This task was crucial as it facilitated the smooth running of the course, ensuring that all topics were adequately covered within the stipulated time. Additionally, I learned the importance of time management and effective communication, as I had to coordinate with different instructors and adjust the timetable based on their availability.

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.



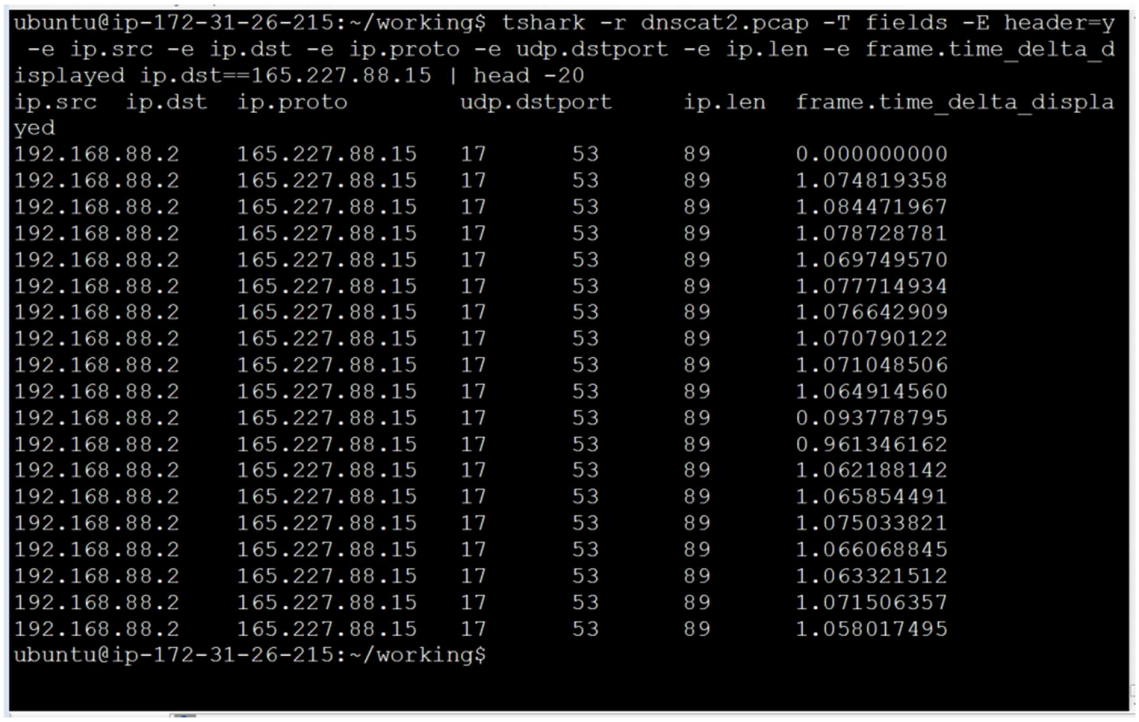
A screenshot of the TryHackme platform with the content discovery room.

Week 2: Digital Forensics and Penetration Testing

In the second week, I was part of a team that developed guidelines for a Digital Forensics Lab. This task was both challenging and enlightening. It required a deep understanding of digital forensics principles and a keen eye for detail. The guidelines we developed would serve as a roadmap for digital forensics investigations, ensuring that all procedures were carried out correctly and efficiently. This experience gave me a deeper understanding of the importance of procedure and documentation in digital forensics.

I also 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.

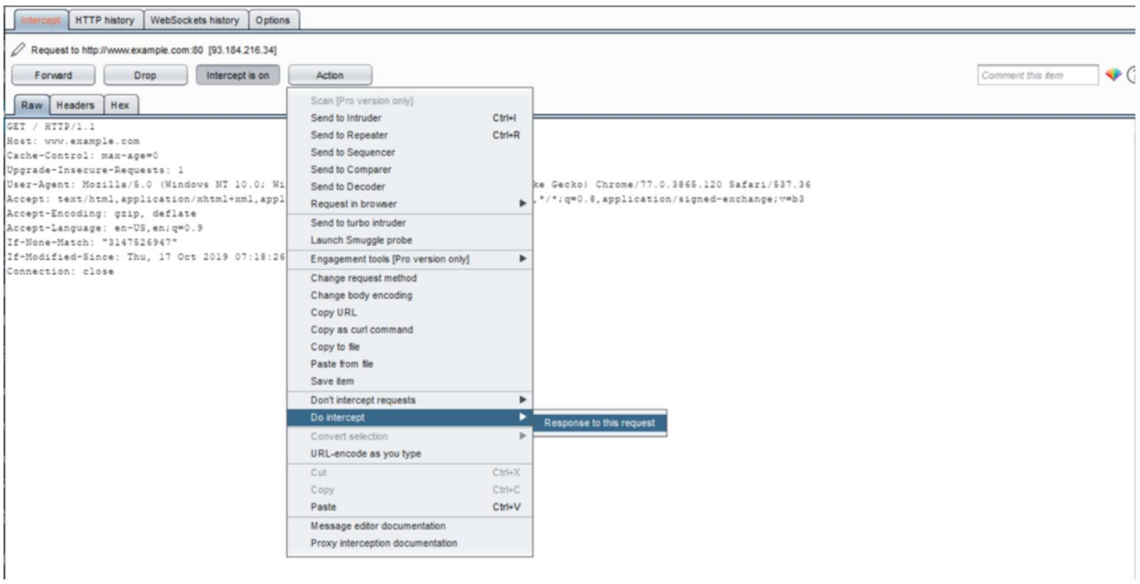


```
ubuntu@ip-172-31-26-215:~/working$ tshark -r dnscat2.pcap -T fields -E header=y
 -e ip.src -e ip.dst -e ip.proto -e udp.dstport -e ip.len -e frame.time_delta_d
isplayed ip.dst==165.227.88.15 | head -20
ip.src  ip.dst  ip.proto        udp.dstport     ip.len  frame.time_delta_displa
yed
192.168.88.2    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. These tools allowed me to intercept, inspect, and modify network requests, a crucial skill in identifying and exploiting vulnerabilities in web applications.



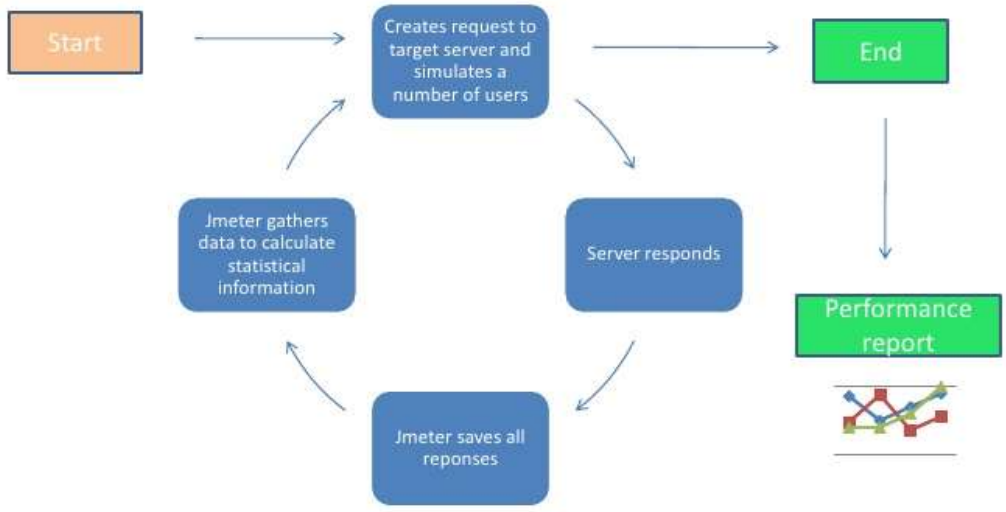
A screenshot of Burp Suite, showing how it can be used to alter intercepted requests.

Week 4: Performance Testing and Teaching Assistance

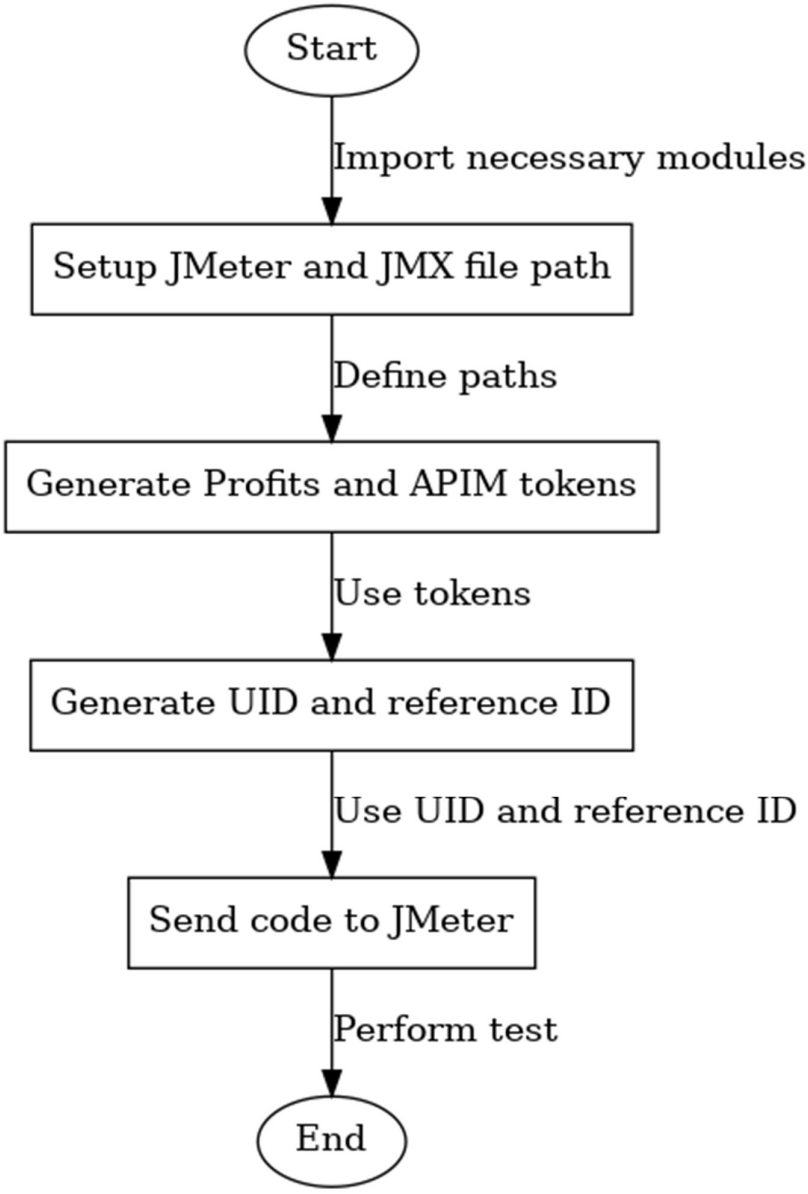
In the fourth week, I worked on a performance testing project that required logging with the Apache JMeter tool, an open-source software designed to load test functional behaviour and measure performance, a critical aspect in ensuring the reliability and efficiency of web applications. I also served 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.

How jmeter work

Jmeter simulates a group of users sending requests to a target server , and returns statistics that show the performance of the target server/application through graphical diagrams. This is a basic description of how jmeter works.



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



A flowchart showing the steps involved in performance testing using Apache JMeter.

Week 5: Digital Forensics and Incidence Response

During the fifth week, I had the opportunity to delve deeper into the realm of digital forensics and incident response. One of the significant tasks I undertook was setting up a Wazuh server to function as a Security Information and Event Management (SIEM) solution in collaboration with the iLab security team. Wazuh is a free and open-source platform that provides a comprehensive suite of features for threat detection, integrity monitoring, incident response, and compliance.

The process of setting up the Wazuh server involved several steps. First, I had to install the Wazuh server software on a dedicated machine. This involved downloading the software, configuring the necessary settings, and ensuring that the server was properly connected to our network. Once the server was up and running, I then had to help in configuring it to collect and analyse security data from various sources within our network. This included setting up rules for detecting potential

threats, configuring alerts for specific events, and setting up dashboards for monitoring security events in real-time.

This task was instrumental in enhancing the security of our network environment. By implementing a SIEM solution, we were able to gain a more comprehensive view of our network's security posture. This allowed us to detect potential threats more quickly, respond to security incidents more effectively, and ensure that our network remained secure and compliant with relevant regulations.

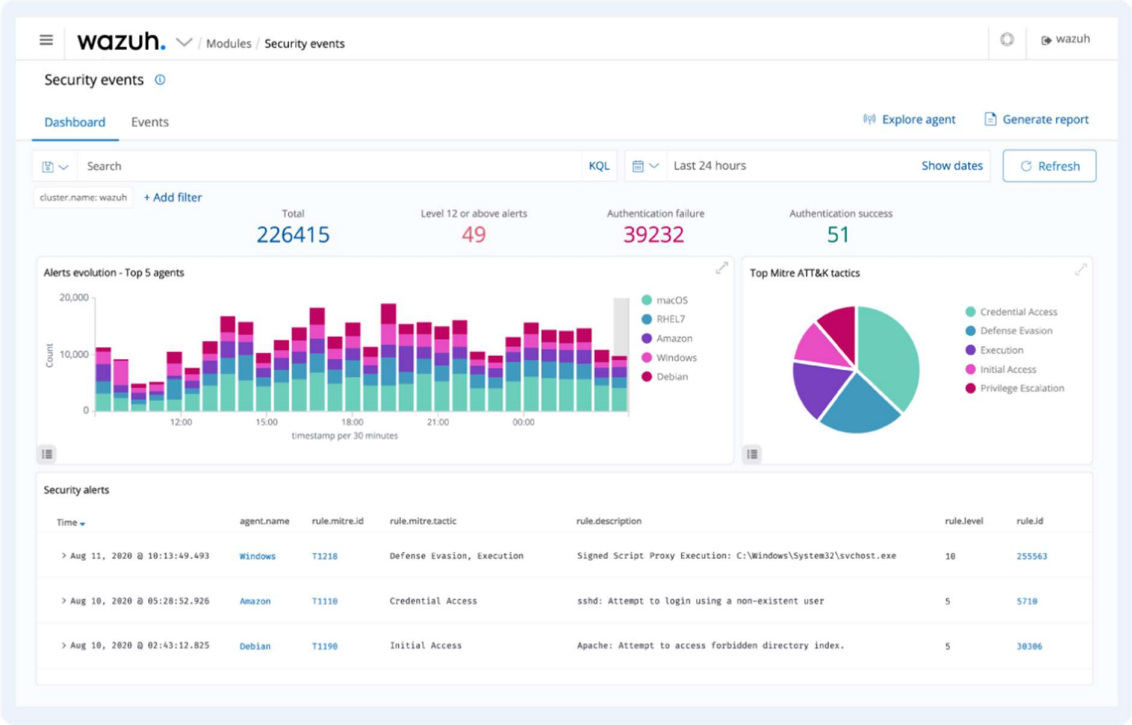
In addition to setting up the Wazuh server, I also tackled challenges on picoCTF, a free online platform that hosts cybersecurity competitions. These challenges allowed me to apply and refine my skills in various areas of cybersecurity, including cryptography, web exploitation, and reverse engineering. Working on these challenges with the team from iLab was a great learning experience, and it helped to further deepen my understanding of cybersecurity concepts and techniques.

Furthermore, I served as a teaching assistant in a course on Scripting for Security. This role allowed me to share my knowledge and experience with others and help them learn important skills in cybersecurity. The course covered both Bash and Python scripting, two powerful tools for automating tasks, analysing data, and solving problems in the field of cybersecurity.

In the Bash scripting classes, we covered the basics of Bash scripting, including variables, control structures, and functions. We also explored more advanced topics such as file manipulation, process management, and network communication. The students learned how to write Bash scripts to automate common tasks, analyze log files, and monitor system resources.

In the Python scripting classes, we delved into the Python programming language, which is widely used in cybersecurity due to its simplicity and versatility. We covered topics such as data types, control structures, functions, and modules. We also explored Python libraries that are particularly useful in cybersecurity, such as Scapy for network analysis and Beautiful Soup for web scraping. The students learned how to write Python scripts to automate tasks, analyze network traffic, and extract information from web pages.

Overall, the fifth week was a highly productive and enriching experience that allowed me to apply and expand my skills in digital forensics, incident response, and cybersecurity education.



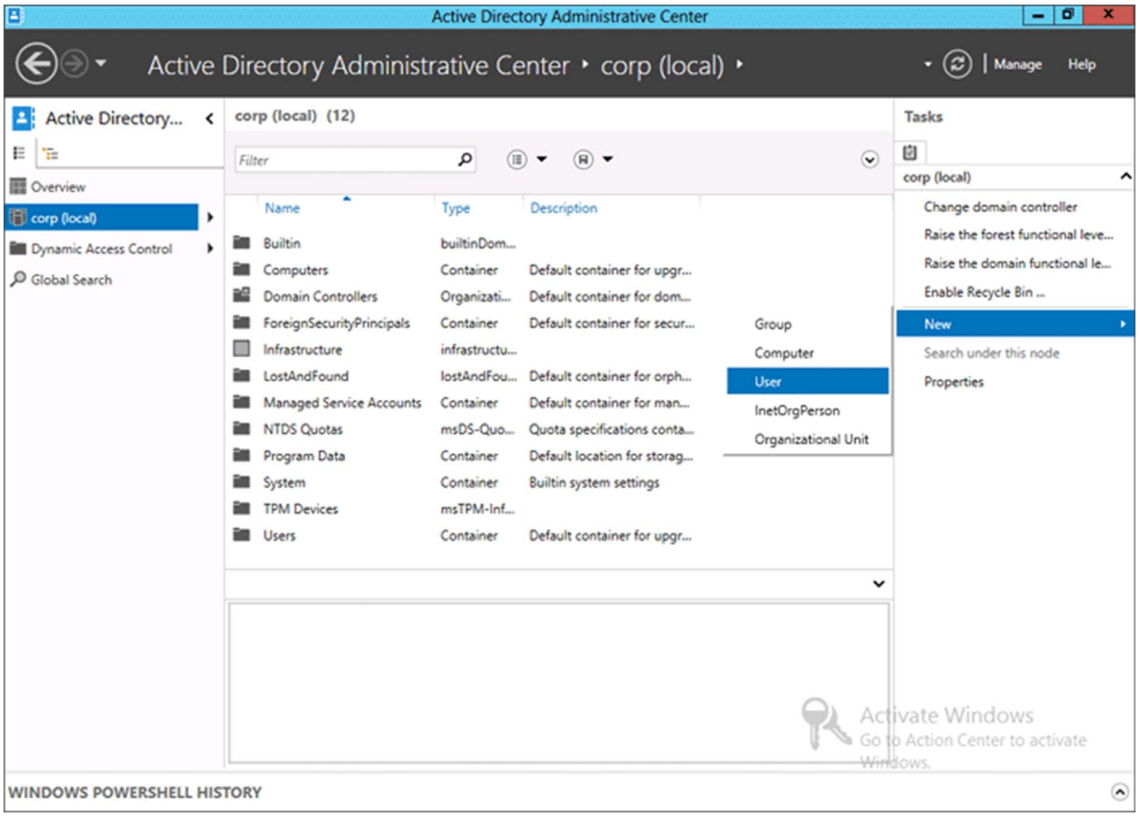
A screenshot of the Wazuh platform, showing how it can be used for threat detection and incident response.

Week 6: Active Directory and Teaching Assistance

The sixth week of my attachment was dedicated to understanding and teaching about Windows Active Directory. Active Directory (AD) is a Microsoft technology used to manage computers and other devices on a network. It is a directory service that uses the LDAP (Lightweight Directory Access Protocol) to communicate with other devices on the network. It provides a centralized system for managing and storing data and network resources, and it plays a crucial role in the security and accessibility of these resources.

As a teaching assistant, I was involved in an online class focusing on Enumerating Active Directory. Enumeration is a process in cybersecurity that involves extracting usernames, machine names, network resources, shares, and services from a system. In the context of Active Directory, enumeration can provide valuable information about the network's structure and its assets. This information can be used to identify potential vulnerabilities or misconfigurations that could be exploited by an attacker.

In addition to assisting in the class, I also taught a session on Active Directory Exploitation. This session focused on how an attacker might exploit vulnerabilities in an Active Directory environment to gain unauthorized access or escalate their privileges. We discussed various techniques and tools used in AD exploitation, such as Pass-the-Hash, Kerberoasting, and Golden Ticket attacks. Teaching this class allowed me to deepen my understanding of these complex topics and develop my skills as an educator.

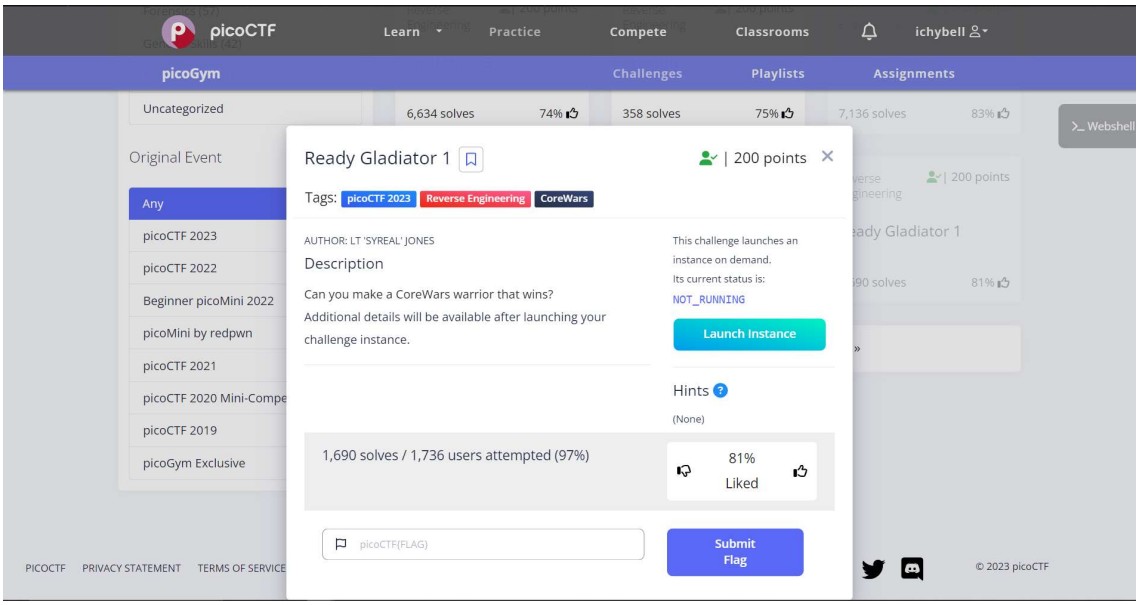


A screenshot of the Windows Active Directory interface.

Week 7: Cryptography and Reverse Engineering

The seventh week was heavily focused on learning new skills in cryptography and reverse engineering. These are two fundamental areas in cybersecurity, and they are often involved in Capture The Flag (CTF) competitions, such as picoCTF. PicoCTF is a free, online cybersecurity competition hosted by Carnegie Mellon University. The competition involves a variety of challenges that test participants' skills in areas such as cryptography, web exploitation, binary exploitation, and reverse engineering.

One of the highlights of this week was successfully completing a CTF challenge on Reverse Engineering using Ghidra. Ghidra is a software reverse engineering (SRE) framework developed by the National Security Agency's Research Directorate. It helps analysts to disassemble, decompile, and analyze malicious code. In this challenge, I used Ghidra to disassemble a piece of code, understand its functionality, and identify any potential flaws that could be exploited.



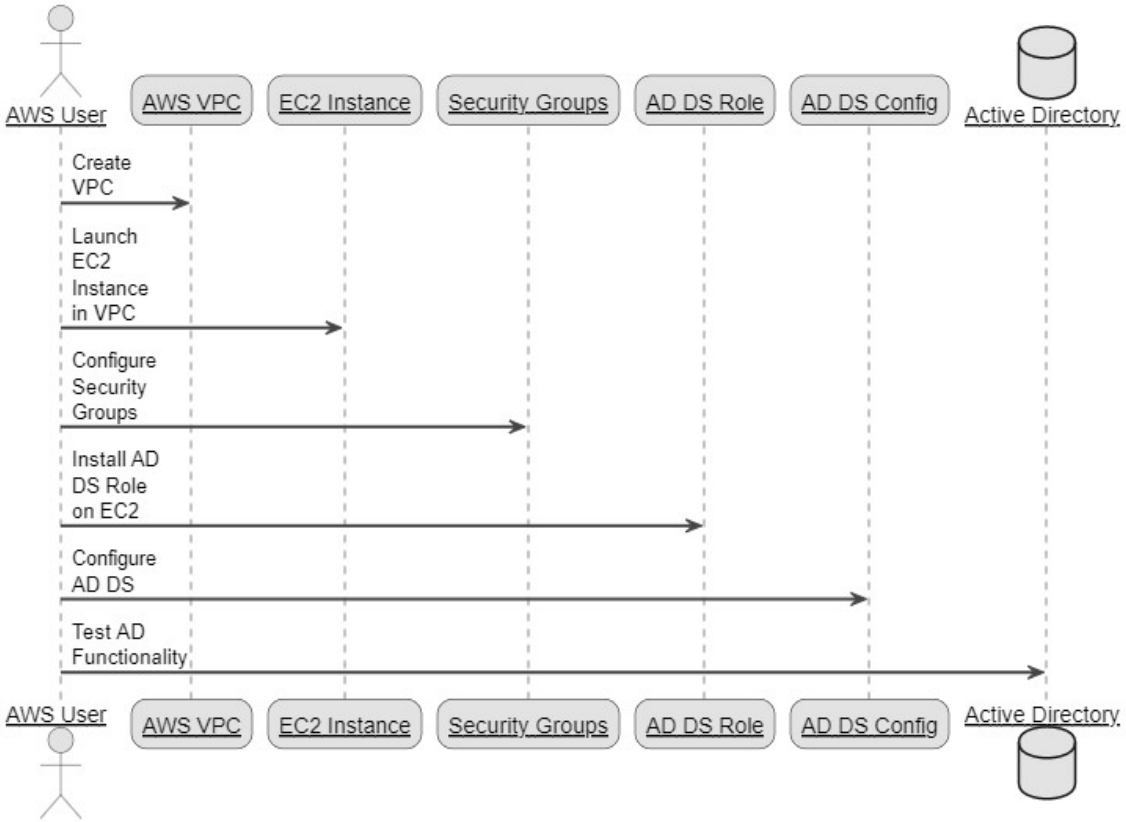
A screenshot of the picoCTF platform, showing a challenge being solved.

Week 8: Conclusion and Final Reflections

In the final week of my attachment, I continued to serve as a teaching assistant and worked on several challenges on picoCTF. These challenges allowed me to apply the skills and knowledge I had gained over the course of my attachment, and they provided a fun and engaging way to test my abilities.

One of the significant tasks I undertook during this week was assisting in setting up a Windows Active Directory on an AWS environment. Amazon Web Services (AWS) is a cloud services platform that provides a range of services, including computing power, database storage, and other functionality. Setting up an Active Directory on AWS involved creating a virtual private cloud (VPC), launching an EC2 instance, and installing and configuring the Active Directory Domain Services role. This task allowed me to gain practical experience with cloud computing and understand how traditional IT infrastructure can be migrated to the cloud.

Throughout these weeks, I was able to gain a deeper understanding of various cybersecurity concepts, enhance my technical skills, and develop my abilities as a teacher and mentor. The experience was both challenging and rewarding, and it has significantly contributed to my growth as a cybersecurity professional.



Process of setting up a Windows Active Directory on an AWS environment

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.