INTERNSHIP REPORT

Domain: Cybersecurity

Virtual Internship at

Allama Iqbal Open University (AIOU)

Directorate of ICT – Networks and Data Centre

SUBMITTED BY:

NAME: **Roonaq Imtiaz**

REG NO: **FA23-BCS-150**

PROGRAM: **Cybersecurity Intern**

Winter 2026

SUBMISSION: **24 February 2026**

COMSATS University Islamabad, Abbottabad Campus

Declaration Form

I, **Roonaq Imtiaz**, Registration No. **FA23-BCS-150**, enrolled in the **BS Computer Science**, hereby declare that I have successfully completed an online internship of **6 weeks** through **Allama Iqbal Open University (AIOU) Directorate of ICT – Networks and Data Centre**. This report has been prepared based on the tasks and experiences gained during the internship period. The internship was carried out under the supervision of External Supervisor **Ms. Laiba Bukhari** and Faculty Advisor **Sir Mukhtiar Zamin**. I affirm that this report is original work and has not been submitted elsewhere for academic credit.

Student: _Roonaq Imtiaz_ **Signature:**

1. Acknowledgement

All praise is due to Allah Almighty, whose blessings and guidance made this internship and report possible. I sincerely thank my Faculty Supervisor, **Mr. Mukhtiar Zamin**, for his continuous guidance and constructive feedback throughout the internship period.

I am deeply grateful to my External Supervisor, **Ms. Laiba Bukhari**, from the **Directorate of ICT - Networks and Data Centre at AIOU**, for her invaluable support, structured task assignments, and professional guidance during the six weeks of the virtual internship. I also thank the AIOU ICT department team for creating a welcoming and productive virtual learning environment, and the TryHackMe and Coursera platforms for their structured and high-quality cybersecurity resources.

Finally, my deepest appreciation goes to my family for their unwavering support and encouragement throughout this journey. This experience would not have been possible without their love and patience.

---

2. Executive Summary

This report documents the six-week virtual cybersecurity internship completed by Roonaq Imtiaz (FA23-BCS-150) at Allama Iqbal Open University (AIOU), Directorate of ICT – Networks and Data Centre, from January 13 to February 23, 2026, under the supervision of Ms. Laiba Bukhari and Mr. Mukhtiar Zamin. The internship followed a structured weekly curriculum covering foundational cybersecurity concepts, the Cyber Kill Chain framework (presented via Google Meet), Linux essentials and Bash command-line practice on Ubuntu VM, SQL basics for security analysis, and vulnerability assessment principles. The final project, CyberFolio — a professional cybersecurity portfolio website built using HTML, CSS, and JavaScript — was successfully developed and deployed in Week 5. Five Coursera/Cisco certifications were earned throughout the internship. The experience significantly strengthened technical knowledge in cybersecurity, Linux, SQL, and web development, while also developing professional skills in documentation, presentation, and independent learning.

---

3. Table of Contents

Contents

PART 1

4. Introduction to Virtual Internship

4.1 Importance of Virtual Internships

Virtual internships have become an essential component of professional development, particularly in technology-driven fields like cybersecurity, where most work is conducted remotely. They allow students to engage with industry professionals and real-world tasks without geographical constraints, closely mirroring actual industry conditions. Beyond technical exposure, virtual internships build critical digital workplace skills remote communication, self-discipline, online collaboration, and independent learning, all of which are highly valued by cybersecurity employers.

4.2 Objective of the Internship

The primary objective was to gain practical exposure to cybersecurity concepts, tools, and frameworks in a professional environment. Specifically, the internship aimed to strengthen knowledge of networking fundamentals, cyber threats, security frameworks, Linux administration, SQL, and risk management, while bridging the gap between academic study and industry application through structured assignments, guided courses, and a final project.

4.3 Overview of the Organization and Platform

This internship was hosted by Allama Iqbal Open University (AIOU) within its Directorate of ICT – Networks and Data Centre, which manages the university's networking, data management, and system security infrastructure. The internship was conducted virtually, using Google Meet for the meeting and the presentation, email and WhatsApp is used for task assignment and reporting, and TryHackMe and Coursera as the primary structured learning platforms.

5. Internship Details

5.1 Duration and Timeline

The internship commenced on January 13, 2026, and concluded on February 24, 2026, spanning six weeks with approximately 35 hours committed per week to self-directed learning, assignments, platform-based courses, and project development. Each week had defined objectives and deliverables ensuring measurable progress.

Week	Dates	Focus Area
Week 1	13 Jan – 19 Jan 2026	Cybersecurity Fundamentals & Terminology
Week 2	20 Jan – 26 Jan 2026	Cyber Kill Chain & Presentation
Week 3	27 Jan – 02 Feb 2026	Linux Essentials & Hands-on Practice
Week 4	03 Feb – 09 Feb 2026	Linux CLI, Bash & SQL Basics
Week 5	10 Feb – 16 Feb 2026	Assets/Threats/Vulnerabilities & Final Project
Week 6	17 Feb – 24 Feb 2026	Course Completion & Report Writing

5.2 Nature of Work

The internship covered a progressive range of cybersecurity tasks. Week 1 focused on a terminology-based research assignment covering networking concepts (LAN, WAN, NAT, DNS, OSI model, TCP/UDP) and cybersecurity fundamentals (CIA triad, OWASP Top 10, phishing, malware, ransomware). Week 2 involved in-depth study and delivery of a formal presentation on the Cyber Kill Chain framework. Weeks 3 and 4 were dedicated to Linux essentials, hands-on command-line practice on an Ubuntu Virtual Machine, Bash scripting, and SQL fundamentals. Week 5 covered assets, threats, and vulnerabilities, alongside the design and deployment of the CyberFolio portfolio website. Week 6 completed the final Coursera course and report preparation.

5.3 Supervisor Interaction

Regular communication was maintained with site supervisor throughout the internship. Weekly progress reports were submitted documenting tasks, learning outcomes, and certificates. Formal interaction via Google Meet took place in Week 2 for the Cyber Kill Chain presentation.

Ms. Laiba Bukhari provided task assignments, reviewed submissions, and guided course selection, while email was used for submitting reports and certificates. This structured communication model ensured consistent accountability and focus.

5.4 Tools & Technologies Used

The internship utilized TryHackMe for interactive cybersecurity learning (SOC Level 1, Cyber Kill Chain, Cyber Defence Frameworks), Coursera and Cisco Networking Academy for structured certifications, Ubuntu Virtual Machine for Linux hands-on practice, and Bash shell for command-line tasks including file management, permissions, and scripting. SQL was studied for security-oriented database querying. HTML, CSS, and JavaScript were used to build and deploy the CyberFolio website. Google Meet facilitated virtual meeting and the presentation.

PART 2

6. Work Samples / Project Summaries

6.1 Week 1 Assignment – Cybersecurity Terminology & Threat Landscape

Task Requirements:

The external supervisor assigned a terminology-based research and documentation task requiring consolidation of foundational cybersecurity and networking concepts into a structured written assignment.

Approach and Tools Used:

Research was conducted using TryHackMe's introductory modules, Google, YouTube, and the Coursera Google Cybersecurity Certificate. Topics covered included networking terms (LAN, WAN, NAT, DNS, TCP vs UDP, IPv4/IPv6, OSI 7-layer model), security concepts (OWASP Top 10, SOC, MSSP, penetration testing, sandboxing), attack types (phishing, social engineering, malware, ransomware, password attacks), and the CIA triad. The Coursera module on risk management and security frameworks was also completed.

Outcomes Achieved:

A comprehensive assignment was submitted covering all required topics. Coursera and TryHackMe progress were certified, and a strong foundational understanding of cybersecurity was established, serving as the base for all subsequent learning.

6.2 Week 2 – Cyber Kill Chain Presentation

Task Requirements:

The supervisor assigned a deep-dive study of the Cyber Kill Chain framework followed by a formal presentation delivered via Google Meet, requiring understanding of all seven stages and their defensive significance.

Approach and Tools Used:

Research was conducted using TryHackMe's Cyber Kill Chain and SOC Level 1 modules, YouTube, and supplementary Coursera materials. The seven stages — Reconnaissance,

Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives — were studied with corresponding defensive strategies. A structured presentation was created and delivered live to the supervisory team.

Outcomes Achieved:

The presentation was successfully delivered and evaluated. A structured understanding of how cyberattacks progress through distinct phases was developed, along with improved confidence in communicating complex technical concepts professionally.

6.3 Final Project – CyberFolio: A Cybersecurity Portfolio Website

Task Requirements:

The final project required developing and deploying a professional digital artifact documenting the cybersecurity learning journey in a publicly accessible format.

Approach and Tools Used:

CyberFolio was built using HTML for structure, CSS for styling and responsive layout, and JavaScript for dynamic content. Sections covered OS fundamentals, Linux, SQL, threats and vulnerabilities, an internship timeline, and a personal reflection. The website was deployed via Vercel, making it publicly accessible online.

Outcomes Achieved:

The website was successfully completed and deployed by end of Week 5. It serves as a comprehensive digital portfolio of the internship journey and was well-received by the supervisory team as a tangible, professional deliverable combining cybersecurity knowledge with practical web development.

PART 3

7. Learning Experiences

7.1 Knowledge Acquired

The internship substantially expanded theoretical and practical cybersecurity knowledge. Networking fundamentals (OSI model, TCP/UDP, NAT, DNS), the CIA triad, and OWASP Top 10 from Week 1 directly reinforced content from the Computer Networks and Information Security courses at CUI. The Cyber Kill Chain framework in Week 2 applied attack methodology concepts from the Information Security course to real-world scenarios. Linux fundamentals; file navigation, user management, permissions, Bash scripting complemented the Operating Systems course with hands-on Unix experience. SQL querying for security analysis connected directly to the Database Systems course. Week 5 and 6 introduced structured knowledge of asset classification, threat identification, and vulnerability assessment, reinforcing information security management foundations.

7.2 Skills Learned

Technically, Linux command-line proficiency improved significantly through consistent Ubuntu VM practice, Bash scripting enabled task automation, and SQL skills were applied to security-relevant database queries. Web development skills in HTML, CSS, and JavaScript were practically applied through the CyberFolio project. Professionally, preparing six detailed weekly progress reports strengthened technical writing and structured documentation. The Week 2 presentation developed the ability to research, synthesize, and communicate complex material to a professional audience. Independent learning and problem-solving were also significantly strengthened given the self-directed virtual format.

7.3 Observed Attitudes and Values

Consistency and discipline emerged as the most critical values maintaining a structured daily learning schedule was essential to meeting weekly deliverables without in-person supervision. Attention to detail proved vital across all tasks, from network protocol analysis to Linux permission management and website debugging. Curiosity and a growth mindset demonstrated

by independently completing additional TryHackMe rooms and supplementary Cisco coursework significantly deepened learning beyond assigned tasks. Professionalism in written and verbal communication with supervisors was observed as a foundational workplace value.

7.4 The Most Challenging Task Performed

The most challenging task was the design and deployment of the CyberFolio website in Week 5. The challenge was threefold: synthesizing five weeks of learning into coherent, publicly readable sections; resolving multiple CSS responsiveness and JavaScript debugging issues during development; and troubleshooting web hosting and deployment configuration areas not fully covered in academic coursework. These were overcome through systematic problem-solving, iterative testing, and consulting web development documentation. Completing and deploying the site within a single week while simultaneously finishing a Coursera course was the internship's most demanding and rewarding achievement.

8. Challenges Faced & Solutions

Several challenges were encountered during the six-week virtual internship, each requiring practical problem-solving. The most persistent challenge was the self-directed nature of the virtual environment; without in-person colleagues or immediate support, maintaining focus and meeting weekly deadlines required a structured daily schedule and personal sub-deadlines within each week. During the Linux practice weeks (Weeks 3 and 4), unexpected system behaviour from certain commands and permission configurations on the Ubuntu VM was resolved by consulting official Linux documentation, community forums, and supplementary YouTube tutorials, a process that ultimately deepened understanding beyond course material alone. In Week 5, CSS responsiveness issues and JavaScript debugging during CyberFolio development required multiple iterations and systematic incremental fixes, while parallel course completion and project development demanded careful day-by-day task prioritization. Each of these challenges, though demanding, contributed meaningfully to technical growth and professional resilience.

9. Reflection & Conclusion

The six-week virtual cybersecurity internship at AIOU has been a genuinely transformative experience. Beginning with foundational concepts and progressing through the Cyber Kill Chain, Linux administration, SQL, vulnerability assessment, and culminating in the CyberFolio website each week built meaningfully upon the last, forming a cohesive and comprehensive learning journey. The most significant realization from this experience is that cybersecurity demands continuous hands-on practice and adaptability, not just theoretical knowledge. The practical exposure through TryHackMe, Ubuntu VM exercises, SQL, and web development reinforced this in ways that classroom learning alone cannot replicate.

The internship also reinforced the value of virtual work environments. Skills developed in managing remote communication, maintaining accountability without physical supervision, and leveraging digital learning tools are directly applicable to modern cybersecurity careers. Academically, the experience served as a powerful bridge concepts from Operating Systems, Database Systems, Computer Networks, and Information Security were encountered and applied

repeatedly in practical contexts, strengthening confidence in the foundation provided by COMSATS University Abbottabad.

Looking ahead, this internship has solidified the intention to pursue a career in cybersecurity, particularly in network security, vulnerability assessment, and ethical hacking. Future goals include obtaining CompTIA Security+ and CEH certifications and advancing through Hack The Box challenges for practical penetration testing skills. The CyberFolio website will continue to grow as a living portfolio. Overall, this internship has been a foundational and defining step in a professional cybersecurity journey.

10. Appendices

Appendix A – Coursera Certificates

The following Coursera Cybersecurity courses were completed during the internship:

- Play It Safe: Manage Security Risks (Week 1)
- Connect and Protect: Networks and Network Security (Week 2)
- Linux Essentials with Shawn Powers (Week 3)
- Tools of the Trade: Linux and SQL (Week 4)
- Introduction to Cybersecurity – Cisco Networking Academy (Week 5)
- Assets, Threats, and Vulnerabilities (Week 6)

Certificate links:

Week 1: https://coursera.org/share/57e50fd5b2c58626f4684455fe24205c

Week 2: https://coursera.org/share/5603db6945ffd7bc4411a22250d0efa9

Week 4: https://coursera.org/share/836cb973028ec9549515c6083d515e94

Week 5: https://www.credly.com/badges/dda975a7-2999-4cf2-95b4-234e59eb7e5c/public_url

Figure 1: Coursera Certificate - Play It Safe

Figure 2: Coursera Certificate – Connect and Protect

Figure 3: Coursera Certificate – Tools of the Trade

Figure 4: CISCO – Introduction to Cybersecurity

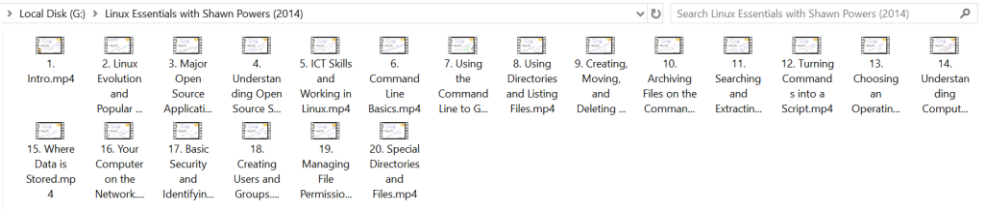
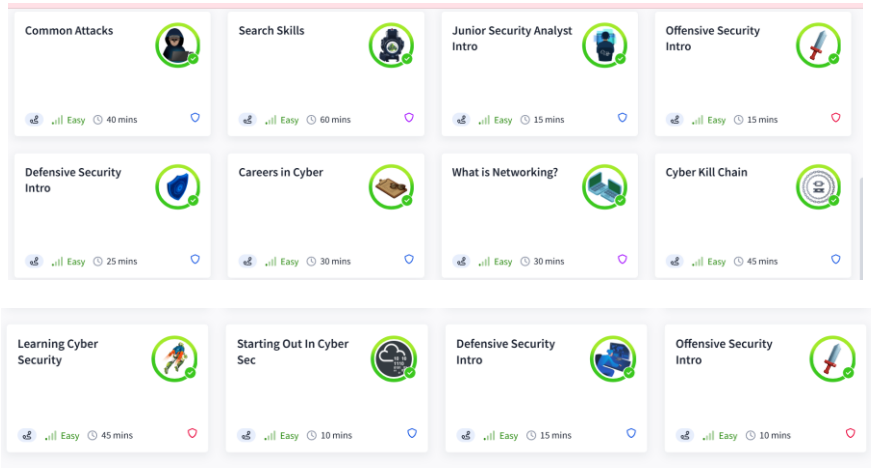


Figure 5: Linux Essentials with Shawn Powers

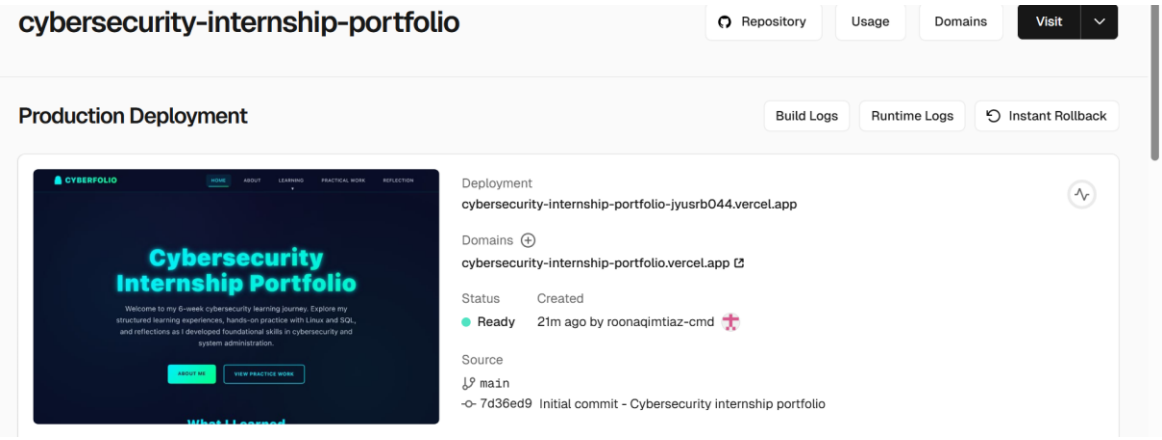
Appendix B – TryHackMe Progress

TryHackMe modules completed during the internship include: Introduction to Cybersecurity, Pre-Security Path, SOC Level 1, Cyber Defense Frameworks, and Cyber Kill Chain. Screenshots of TryHackMe progress are available upon request.



Appendix C – CyberFolio Project

The CyberFolio website was designed and deployed as the final internship project in Week 5. It serves as a professional digital portfolio documenting all cybersecurity learning from the internship. The website includes structured sections on OS fundamentals, Linux, SQL, threats and vulnerabilities, and personal reflection. The deployed website can be viewed at the URL provided to the supervisory team upon submission.



Link: https://cybersecurity-internship-portfolio.vercel.app/

Appendix D – Weekly Progress Reports

Six weekly progress reports (Weeks 1–6) were submitted to both supervisors throughout the internship, documenting objectives, tasks completed, learning outcomes, and certificates. These are available as supporting documentation upon request.

-------End of Report-------