CYBERSECURITY INTERNSHIP REPORT

IN SKILLDZIRE TECHNOLOGIES

An Industrial Internship report submitted in partial fulfillment of the requirement for the award of the degree of

BACHELOR OF TECHNOLOGY

By

ANIL SINTHU

22VV5A1273

Internship Mentor

Mrs. Madhumita Chanda

Assistant Professor (c)

Department of Information Technology

DEPARTMENT OF INFORMATION TECHNOLOGY

Jawaharlal Nehru Technological University Gurajada Vizianagaram

College of Engineering Vizianagaram (Autonomous)

Dwarapudi, Vizianagaram-535003, Andhra Pradesh, India

2023-2024

Declaration

I, **ANIL SINTHU**, Reg. No. **22VV5A1273**, of the Department of Information Technology at JNTUGV-CEV(A), do hereby declare that I have completed the mandatory internship from 15-05-2024 to 15-07-2024 in SKILLDZIRE Technologies Pvt. Ltd. under the Faculty Guideship of Mrs. Madhumita Chanda, Assistant Professor (c), Department of IT, JNTUGV-CEV(A).

Signature

DEPARTMENT OF INFORMATION TECHNOLOGY
Jawaharlal Nehru Technological University Gurajada Vizianagaram
College of Engineering Vizianagaram (Autonomous)
Dwarapudi, Vizianagaram _ 535003 Andhra Pradesh, India
2023_2024

Website: https://jntugvcev.edu.in

Subject Name: SUMMER INTERNSHIP **Regulation: R20**
Academic Year: 2024

CO'S

Course Outcomes

Course Outcomes	
CO1	Apply appropriate workplace behaviors in a professional setting.
CO2	Demonstrate content knowledge appropriate to job assignment.
CO3	Exhibit evidence of increased content knowledge gained through practical experience.
CO4	Describe the nature and function of the organization in which the internship experience takes place.
CO5	Explain how the internship placement site fits into their broader career field.
CO6	Evaluate the internship placement experience in terms of their personal, educational and career needs.

CO-PO Mapping

Mapping of Course Outcomes (COs) with Program Outcomes (POs)

Course Outcomes	Program Outcomes(POs)														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	1	2	1	2	1	-	-	-	3	3	2	3	3	2	2
CO2	3	3	2	2	2	-	-	-	2	3	3	2	3	2	2
CO3	3	3	2	1	3	-	-	1	2	2	3	3	3	3	2
CO4	2	3	1	2	2	-	-	1	2	3	2	2	2	3	1
CO5	3	2	2	3	1	-	-	-	2	3	1	3	1	2	1
CO6	1	2	3	2	1	2	2	3	1	2	3	2	2	1	3

Enter correlation levels 1,2 and 3 as defined below:
1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High) If there is no correlation, put "-"

Signature of internship mentor

Acknowledgement

This acknowledgement transcends the reality of formality when I express deep gratitude and respect to all those people behind the screen who inspired and helped us in completion of this project work.

With great pleasure and privilege, I wish to express my heartfelt sense of gratitude and Special thanks to **Mrs. Madhumita Chanda**, Assistant Professor(c), Department of Information Technology, for her continuous support during my internship.

With great pleasure and privilege, I wish to express my heartfelt sense of gratitude and indebtedness to **Dr. Ch.Bindu Madhuri**, Head of Department of Information Technology, JNTUGV Vizianagaram, for her supervision.

I extend heartfelt thanks to our principal Prof. **Dr. R.Rajeswara Rao** for providing intensive support throughout my dissertation.

I am also thankful to all the Teaching and Non-Teaching staff of Information Technology Department, JNTUG - Vizianagaram, for their direct and indirect help provided to me in completing the dissertation.

I am also thankful to the entire team at **SkillDzire** Technologies for offering me the opportunity to gain hands-on experience.

I also extend my sincere appreciation to my family and friends for their continuous encouragement throughout this journey.

ANIL SINTHU

(22VV5A1273)

Certificate from Intern Organization

SkillDzire

CERTIFICATE OF INTERNSHIP

This is to Certify that Mr./Ms

Sinthu Anil

Enrolled in the **Information Technology - 22VV5A1273**

From College **JNTUK-University College of Engineering Vizianagaram**

of university **JNTUGV, Vizianagaram**

has Successfully Completed short-term Internship programme titled

Cyber Security

under SkillDzire for 2 Months.Organized By **SkillDzire** in collaboration with **Andhra Pradesh State Council of Higher Education**.

Certificate ID:
SDST-14555

Issued On:
28-Jun-2024

Approved By AICTE

Authorized Signature

Contents

Contents

ABSTRACT

This report presents the key findings, activities, and skills developed during a two-month internship at **SkillDzire Technologies Pvt. Ltd.**, an organization specializing in providing cybersecurity solutions and training. The primary objective of the internship was to gain hands-on experience in the field of cybersecurity, particularly focusing on web application security, penetration testing, and the implementation of cybersecurity policies aligned with industry standards.

Throughout the internship, I actively participated in various projects, which involved configuring and deploying **Web Application Firewalls (WAF)**, performing vulnerability assessments using tools like **OWASP ZAP**, and conducting penetration tests to identify and mitigate security risks. The tasks undertaken were aimed at improving the security posture of the organization's web applications and ensuring compliance with cybersecurity frameworks such as **ISO/IEC 27001**.

In addition to technical skills, this internship provided an opportunity to enhance soft skills such as communication, teamwork, and project management. Regular interactions with the cybersecurity team and feedback from mentors helped me gain a deeper understanding of the challenges and best practices in the industry.

This report outlines the detailed learning outcomes, challenges faced, and solutions implemented during the internship. It also highlights the significance of adopting advanced security techniques, such as **Zero-Trust Architecture** and **Intrusion Detection Systems (IDS)**, to safeguard organizational assets from emerging cyber threats.

The internship has not only expanded my technical expertise but has also reinforced my interest in pursuing a long-term career in cybersecurity. The knowledge and skills acquired will be instrumental in navigating the rapidly evolving landscape of information security.

Keywords: Web Application Security, Penetration Testing, OWASP ZAP, Cybersecurity Policies, Intrusion Detection Systems, ISO/IEC 27001, Zero-Trust Architecture, SkillDzire Technologies.

CHAPTER 1: Executive Summary

SkillDzire Technologies Private Limited was founded in **October 2020** by **Sreedhar Thokala and Srikanth Muppalla**. SkillDzire is India's largest real-time learning platform, offering students opportunities to be trained by industry experts, with certifications and placement assistance. The company's mission is to bridge the skills gap for engineering graduates, equipping them with industry-relevant skills to secure employment. With flexible class timings and experienced faculty, SkillDzire contributes to India's workforce development.

In addition to training, **SkillDzire Technologies Pvt Ltd** provides innovative solutions in software development, digital marketing, and data analytics. Their goal is to empower businesses with cutting-edge technologies that enhance their competitiveness in the global market. The company's team consists of highly skilled professionals catering to clients from various industries, delivering quality services that foster growth and innovation.

During my **two-month internship** with SkillDzire, I worked with the cybersecurity team on tasks including vulnerability assessments, threat modeling, and penetration testing. I gained hands-on experience with tools such as **Wireshark**, **Nmap**, and **Metasploit**. I also conducted network security audits and web application vulnerability scanning, developing an in-depth understanding of cybersecurity frameworks, tools, and methodologies.

Chapter 2: Overview of SKILLDZIRE Technologies

SkillDzire Technologies Private Limited, based in Hyderabad, is an educational technology company that provides real-time learning platforms. The company focuses on bridging the gap between academia and industry by offering practical training and certification programs.

Key Features and Services:

- **Real-time Learning Platform:** An interactive platform offering live classes, recorded sessions, and project-based assignments, led by industry experts.
- **Industry-Relevant Courses:** Comprehensive courses tailored to current industry demands, covering topics such as cybersecurity, data science, PCB design, electric vehicles, embedded systems, IoT, and building planning.
- **Certifications and Placements:** SkillDzire provides industry-recognized certifications and placement assistance upon successful completion of its programs.
- **Experienced Faculty:** Courses are taught by professionals with significant industry experience, providing students with practical insights and mentorship.

SkillDzire has established partnerships with leading universities and corporate clients. These collaborations aim to upskill professionals through hands-on training. The company's clients include organizations in sectors such as finance, healthcare, and information technology.

2.1 Introduction of the Organization

SkillDzire Technologies was founded in October 2020 by Sreedhar Thokala and Srikanth Muppalla. Since its inception, the company has aimed to be a leader in real-time learning in India. SkillDzire offers a platform where students can access industry-focused courses, get certified, and benefit from placement support. The platform is designed to equip engineering graduates with the skills needed to succeed in their respective fields.

The company's training programs focus on high-demand skills such as cybersecurity, data science, embedded systems, IoT, and more. The organization prides itself on collaborating with industry professionals to deliver high-quality, practical learning experiences.

2.2 Vision, Mission, and Values of the Organization

Vision: To be the largest real-time learning platform in India that prepares students for a dynamic job market with industry-relevant skills.

Mission: SkillDzire's mission is to bridge the skill gap for engineering students, enabling them to gain hands-on experience in emerging technologies through industry-focused training. The company's goal is to help students secure meaningful employment opportunities by providing them with the necessary skills and industry certifications.

Values: The company upholds the values of innovation, integrity, and excellence in its training programs. It focuses on offering personalized learning experiences, ensuring flexibility in class timings, and providing mentorship from experienced faculty.

2.3 Policy of the Organization, in Relation to the Intern Role

SkillDzire Technologies emphasizes providing its interns with a rich learning experience. The organization follows a structured internship policy aimed at providing students with hands-on training and exposure to real-world challenges. Interns are integrated into key projects where they can apply their theoretical knowledge to practical tasks.

Interns working at SkillDzire in the field of cybersecurity, for example, participate in tasks such as vulnerability assessments, penetration testing, and threat modeling. The organization ensures that interns are guided by experienced professionals, providing feedback and opportunities for growth. This policy aligns with SkillDzire's overarching mission of skill development and real-world readiness.

2.4 Performance of the Organization in Terms of Turnover, Profits, Market Reach, and Market Value

As a fast-growing company, SkillDzire Technologies has seen significant growth since its founding. The company has expanded its reach across multiple industries, including finance, healthcare, and information technology, providing skill development and training services to professionals and students alike.

In terms of market reach, SkillDzire has partnered with over 100 universities and several corporate clients, contributing to its strong presence in the ed-tech sector. The company's focus on emerging technologies and continuous innovation has contributed to steady growth in revenue, with increasing enrollments in its certification programs. SkillDzire's investment in quality education and partnerships has further enhanced its market value, positioning the company as a trusted player in the educational technology space.

CHAPTER 3: INTERNSHIP PART

This section provides a comprehensive overview of the tasks, projects, and activities undertaken during the two-month internship at SkillDzire Technologies. The internship focused on real-time cybersecurity challenges, allowing me to engage in hands-on projects such as network security audits, vulnerability scanning, and penetration testing. This section presents the weekly activity logs in tabular form, followed by detailed weekly reports to offer a clear understanding of the work completed, the tools used, and the outcomes achieved.

Projects Overview:

- **Project 1: Network Security Audit** – Conducted a comprehensive audit of SkillDzire's internal network. This involved scanning for vulnerabilities, analyzing network traffic, and securing network devices using industry-standard tools such as **Wireshark**, **Nmap**, and **Metasploit**.
- **Project 2: Web Application Vulnerability Scanning** – Performed vulnerability scanning for SkillDzire's web applications using tools like **OWASP ZAP** and **Burp Suite**, identifying potential security threats and recommending mitigation measures.
- **Project 3: Penetration Testing on Simulated Networks** – Conducted penetration testing on simulated environments to identify security loopholes and test the effectiveness of defenses. Tools such as **Metasploit** and **Kali Linux** were used to simulate attacks and validate security controls.
- **Project 4: Incident Response and Threat Management** – Participated in a mock incident response scenario, where I worked alongside the cybersecurity team to detect, analyze, and mitigate security incidents in real-time.

These projects were instrumental in developing a practical understanding of cybersecurity practices, including risk management, threat modeling, and defensive techniques.

Chapter 4: Activity log and weekly reports

4.1.1 Activity log for First Week

Day & Date	**Brief Description of the Daily Activity**	**Learning Outcome**	**Internship Mentor Signature**
Day 1 15-05-2024	Introduction to cybersecurity and team orientation	Basic understanding of cybersecurity concepts and team structure	
Day 2 16-05-2024	Installation and configuration of cybersecurity tools (Wireshark, Nmap)	Learned tool setup and basic network scanning techniques	
Day 3 17-05-2024	Conducted a vulnerability assessment on internal network	Learned how to identify potential network vulnerabilities using Nmap	
Day 4 18-05-2024	Introduction to penetration testing; explored Metasploit framework	Gained knowledge of penetration testing and use of Metasploit	
Day 5 19-05-2024	Analyzed network traffic with Wireshark; packet capturing and analysis	Learned packet analysis techniques for detecting network anomalies	

4.1.2 Weekly Report

WEEK – 1 (From Dt 15-05-2024 to Dt 19-05-2024)

Objective of the Activity Done:

The primary objective was to get familiarized with the basic concepts of cybersecurity, network analysis, and setting up cybersecurity tools.

Detailed Report:

During the first week of my internship, I was introduced to the fundamental concepts of cybersecurity and the structure of SkillDzire's cybersecurity team. I learned how to set up and configure essential cybersecurity tools like **Wireshark** and **Nmap**, which are used for network traffic analysis and vulnerability scanning. These tools provided me with hands-on experience in monitoring network activities and identifying potential vulnerabilities.

I also participated in network vulnerability assessments on internal systems, where I applied basic network scanning techniques to discover open ports and security loopholes. This week laid a strong foundation by introducing me to the **Metasploit** framework, which is widely used for penetration testing. Additionally, I gained a working knowledge of packet capturing and analysis using Wireshark, which helped me understand how to detect suspicious activities within network traffic.

Overall, this week provided a comprehensive introduction to the cybersecurity domain, focusing on both theory and practical hands-on tasks. By the end of the week, I had a strong understanding of key cybersecurity tools and basic network security measures.

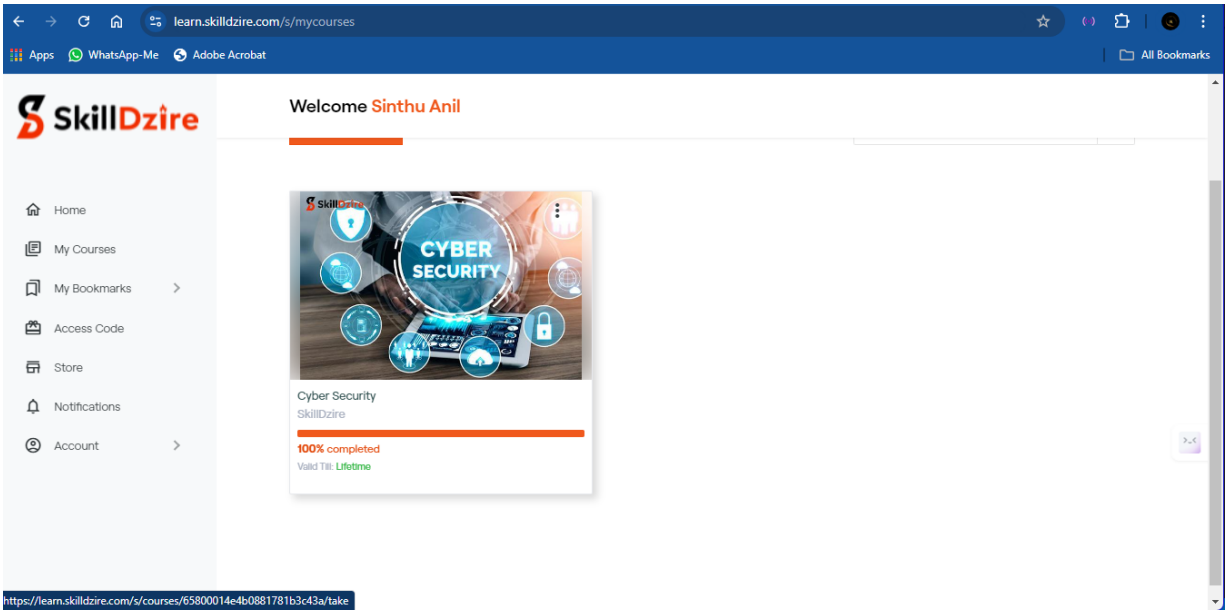

Figure: SkillDzire's learning Platform

Additionally, I participated in a session focused on cybersecurity frameworks, which included an overview of the **NIST Cybersecurity Framework** and **ISO/IEC 27001**. This laid the foundation for understanding how SkillDzire implements security controls.

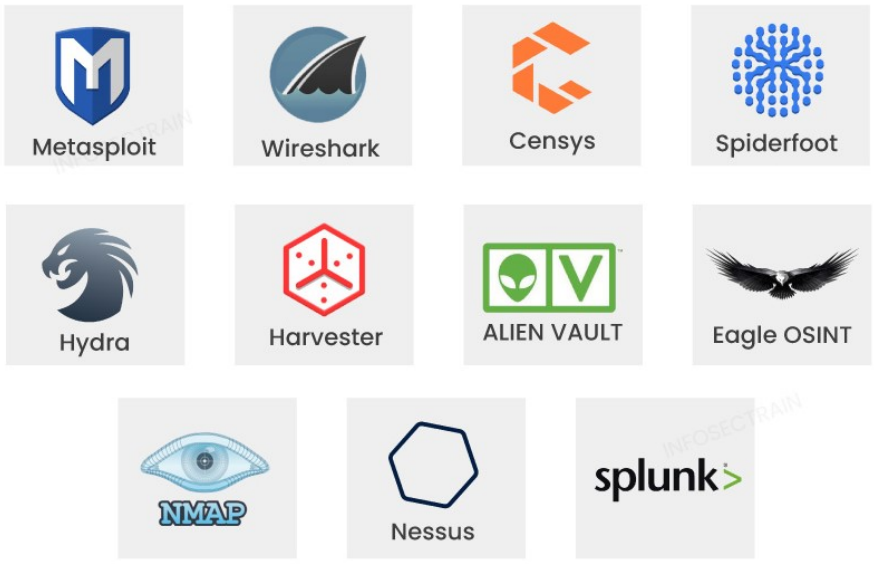

Figure: Network Traffic Analysis and Vulnerability Scanning Tools (Wireshark, Nmap)

4.2.1 Activity Log for Second Week

Day & Date	**Brief Description of the Daily Activity**	**Learning Outcome**	**Internship Mentor Signature**
Day 1 20-05-2024	Conducted network vulnerability scanning on a simulated network	Learned about different network vulnerabilities and scanning methods	
Day 2 21-05-2024	Threat modeling for web applications	Gained an understanding of identifying and mitigating web application threats	
Day 3 22-05-2024	Performed penetration test on a simulated web application using OWASP ZAP	Learned how to identify web vulnerabilities such as SQL injection and XSS	
Day 4 23-05-2024	Drafted a vulnerability assessment report for the web application	Developed skills in documenting vulnerabilities and proposed mitigations	
Day 5 24-05-2024	Participated in a session on cybersecurity frameworks (NIST, ISO 27001)	Gained knowledge of key cybersecurity frameworks and best practices	

4.2.2 Weekly Report

WEEK – 2 (From Dt 20-05-2024 to Dt 24-05-2024)

Objective of the Activity Done:

The primary objective was to explore web application security, including vulnerability scanning, penetration testing, and understanding common web security flaws.

Detailed Report:

In the second week, my focus shifted towards web application security. I used **OWASP ZAP** to perform vulnerability scans on a simulated web application, identifying common security flaws such as **SQL Injection** and **Cross-Site Scripting (XSS)**. This helped me understand how attackers exploit vulnerabilities in web applications and the importance of securing input fields.

Additionally, I participated in threat modeling sessions, where we analyzed potential security risks for web applications and how to mitigate them. I also learned how to draft vulnerability assessment reports that documented the findings and recommended security patches. This process improved my skills in communicating technical findings to non-technical stakeholders.

Moreover, this week included an introduction to **cybersecurity frameworks** such as **NIST** and **ISO 27001**, which provided a theoretical understanding of cybersecurity standards and their real-world applications in securing web platforms.

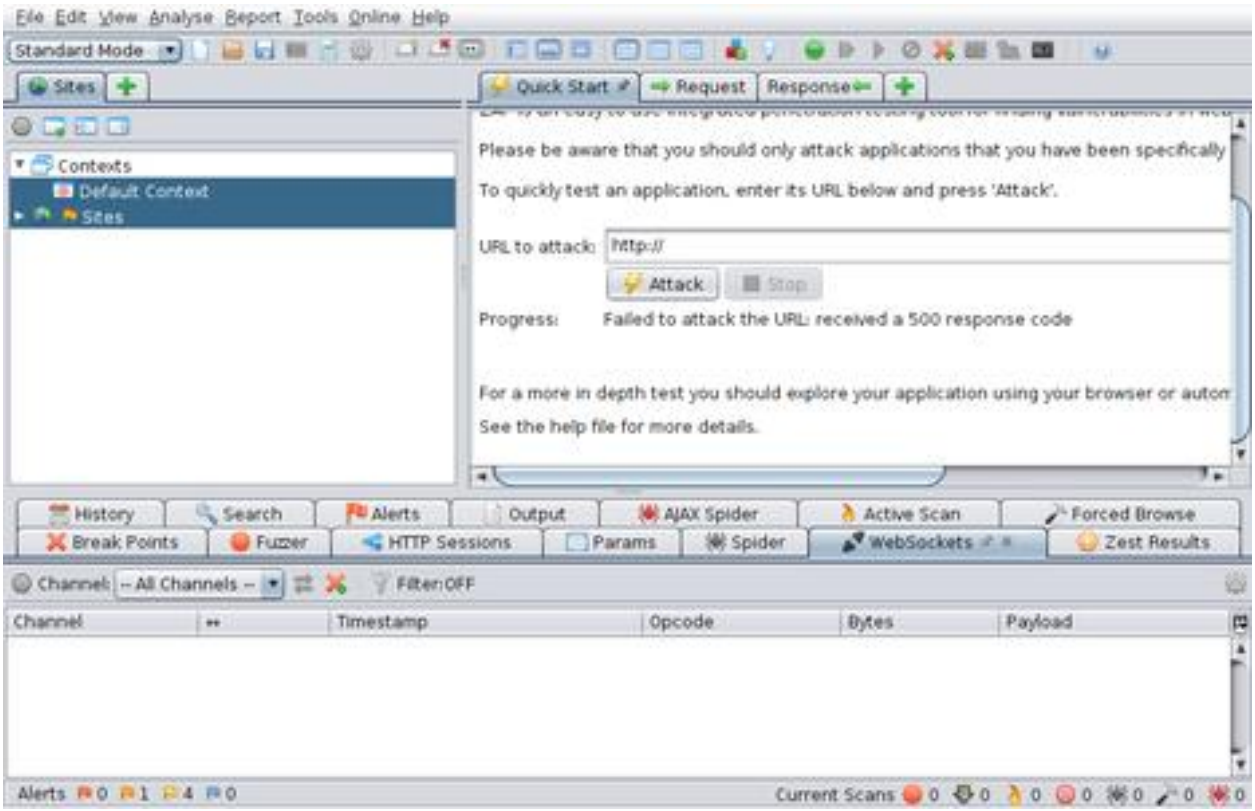

Figure: Web Application Vulnerability Scanning with OWASP ZAP

4.3.1 Activity log for Third Week

Day & Date	**Brief Description of the Daily Activity**	**Learning Outcome**	**Internship Mentor Signature**
Day 1 27-05-2024	Explored advanced penetration testing techniques using Metasploit	Learned to exploit advanced vulnerabilities and write exploit scripts	
Day 2 28-05-2024	Analyzed web application security using OWASP Top 10 guidelines	Learned to classify and mitigate common web application vulnerabilities	
Day 3 29-05-2024	Conducted network traffic analysis for security anomalies using Wireshark	Improved skills in real-time network traffic monitoring and threat detection	
Day 4 30-05-2024	Implemented incident response for a simulated network breach	Gained practical experience in incident detection and response strategies	
Day 5 31-05-2024	Assisted in drafting incident response documentation	Learned the process of documenting incident response and recovery	

4.3.2 Weekly Report

WEEK – 3 (From Dt 27-05-2024 to Dt 31-05-2024)

Objective of the Activity Done:

The objective this week was to perform advanced penetration testing and network traffic analysis, along with incident response planning.

Detailed Report:

This week, I expanded my penetration testing skills by utilizing the **Metasploit** framework to simulate more advanced attacks on a simulated network. I practiced writing custom exploit scripts and learned to exploit vulnerabilities in a controlled environment. This hands-on experience with Metasploit deepened my understanding of how attackers can gain unauthorized access to networks and systems.

In addition to penetration testing, I focused on network traffic analysis using **Wireshark**. I analyzed real-time network traffic to detect security anomalies and suspicious activities. This helped me gain practical skills in monitoring network events and recognizing patterns that indicate potential threats.

Towards the end of the week, I participated in an **incident response** simulation, where I learned about the steps involved in detecting, responding to, and recovering from security breaches. This exercise enhanced my understanding of the role of incident response in mitigating the damage caused by cyberattacks.

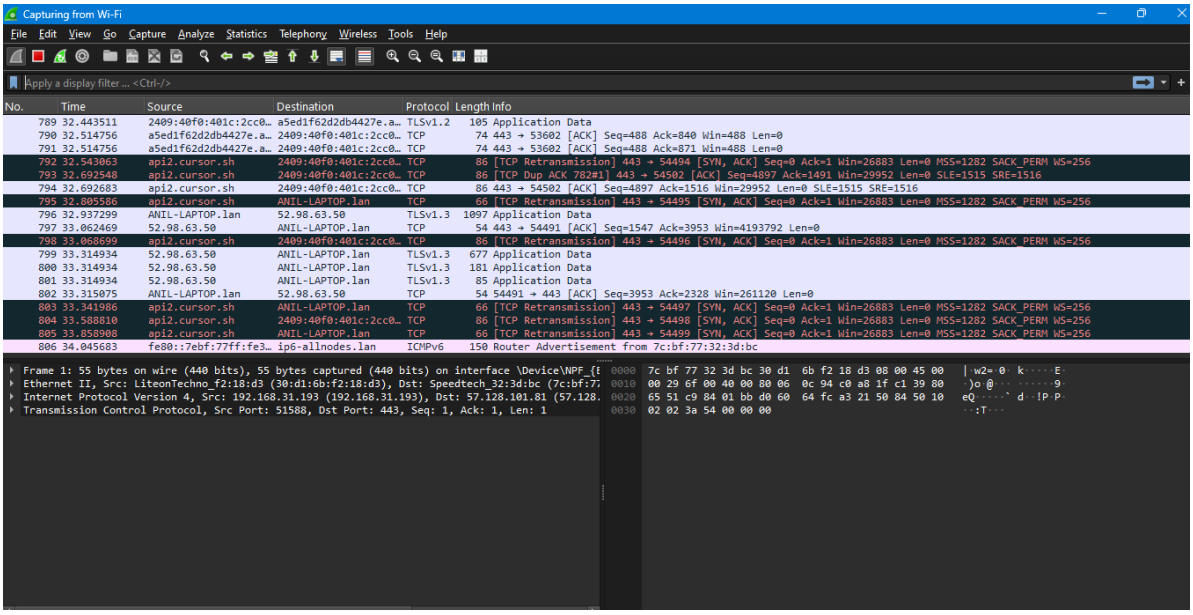

Figure: Network Traffic Monitoring and Anomaly Detection using Wireshark

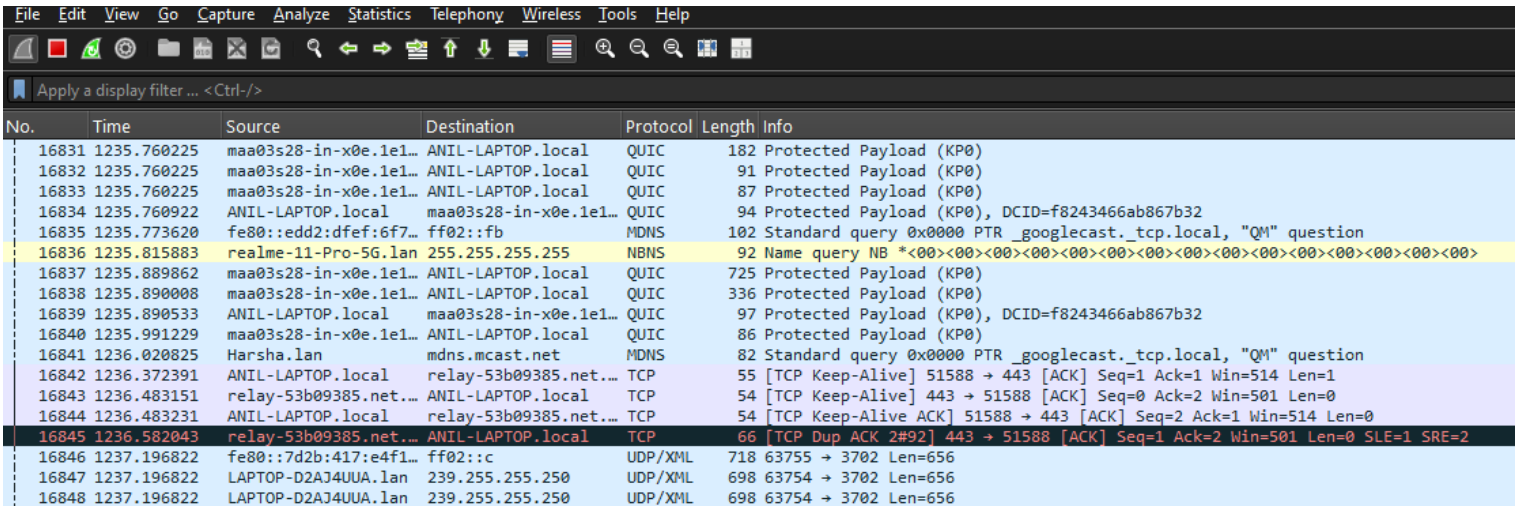

Figure: Network Traffic Monitoring and Anomaly Detection using Wireshark 2

4.4.1 Activity log for Fourth Week

Day & Date	**Brief Description of the Daily Activity**	**Learning Outcome**	**Internship Mentor Signature**
Day 1 03-06-2024	Participated in a mock cybersecurity incident response drill	Hands-on experience in reacting to and mitigating simulated cyberattacks	
Day 2 04-06-2024	Studied intrusion detection systems (IDS) and explored Snort IDS tool	Learned how IDS tools function and how to configure Snort for network monitoring	
Day 3 05-06-2024	Worked on configuring firewalls and access control lists (ACLs)	Learned about firewall rules and how to implement ACLs for network security	
Day 4 06-06-2024	Performed a full network security audit and prepared a report	Completed a full audit cycle and report, enhancing understanding of audit procedures	
Day 5 07-06-2024	Explored cloud security measures for AWS environments	Learned about securing cloud infrastructures and best practices in AWS security	

4.4.2 Weekly Report

WEEK – 4 (From Dt 03-06-2024 to Dt 07-06-2024)

Objective of the Activity Done:

The objective this week was to simulate incident response drills and configure Intrusion Detection Systems (IDS).

Detailed Report:

In Week 4, I participated in a mock cybersecurity incident response drill. This exercise provided practical experience in reacting to simulated cyberattacks, where I was required to identify security breaches, contain the attack, and begin recovery processes. This drill improved my decision-making and teamwork skills in a high-pressure scenario.

I also learned about **Intrusion Detection Systems (IDS)**, specifically **Snort**. I configured Snort on a test network to detect potential threats and analyze the logs generated by the IDS. This task deepened my understanding of how to monitor networks for malicious activity.

Additionally, I explored firewall configurations and **Access Control Lists (ACLs)** to protect internal networks from unauthorized access. This was followed by conducting a full network security audit, where I reviewed network security configurations, identified potential weaknesses, and recommended improvements.

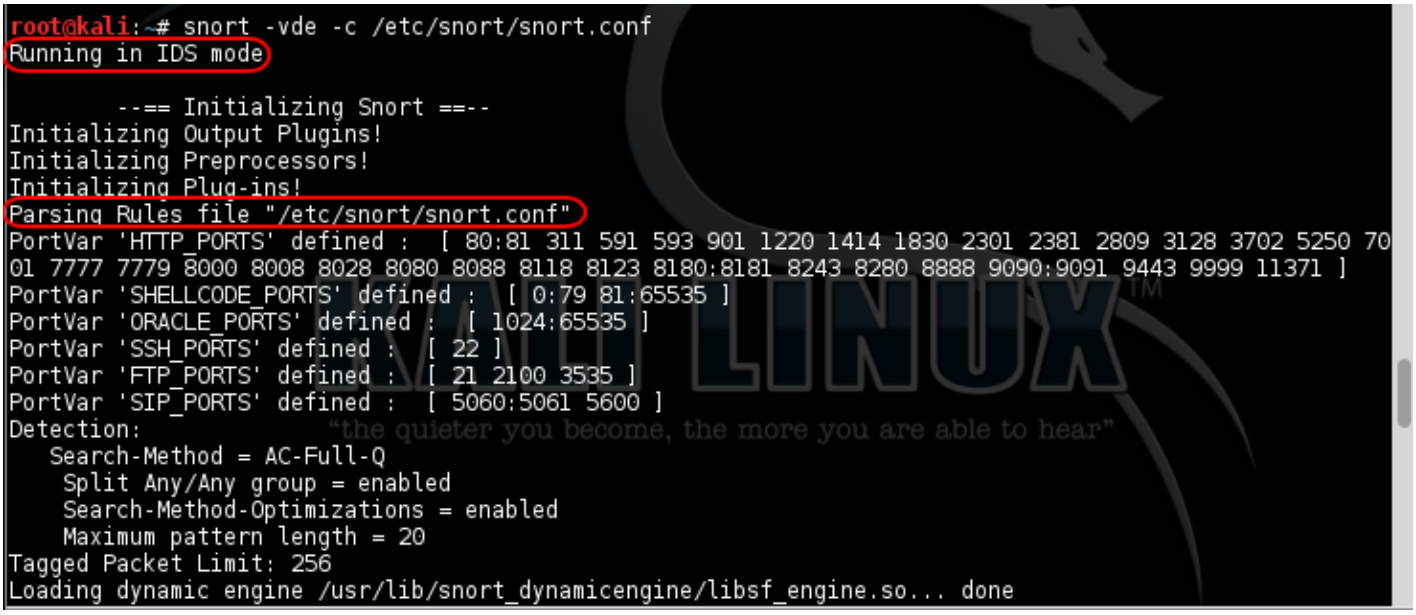

Figure: Incident Response Drill and IDS Configuration using Snort

4.5.1 Activity log for Fifth Week

Day & Date	**Brief Description of the Daily Activity**	**Learning Outcome**	**Internship Mentor Signature**
Day 1 10-06-2024	Attended a session on zero-trust architecture and its implementation	Gained insight into zero-trust models and security best practices	
Day 2 11-06-2024	Conducted penetration testing on cloud environments using Kali Linux	Gained practical experience in cloud penetration testing	
Day 3 12-06-2024	Drafted a security review for the cloud penetration test	Learned how to summarize cloud security vulnerabilities and recommend mitigations	
Day 4 13-06-2024	Reviewed case studies on recent cybersecurity attacks	Gained knowledge on the latest cybersecurity threats and defensive strategies	
Day 5 14-06-2024	Assisted in updating SkillDzire's cybersecurity policy documentation	Learned about policy updates and security compliance requirements	

4.5.2 Weekly Report

WEEK – 5 (From Dt 10-06-2024 to Dt 14-06-2024)

Objective of the Activity Done:

The focus this week was on implementing a Zero-Trust Architecture and performing cloud-based penetration testing.

Detailed Report:

This week, I focused on studying and implementing **Zero-Trust Architecture**, which is a modern security model that assumes that no entity (internal or external) can be trusted by default. I reviewed case studies of successful Zero-Trust implementations and learned how to apply these principles to improve internal network security.

I then conducted a penetration test on a cloud environment using **Kali Linux**. The objective was to identify vulnerabilities in the cloud infrastructure, including access control weaknesses and improper configuration of security settings. This gave me hands-on experience in cloud security, which is critical for securing cloud-based applications.

At the end of the week, I drafted a report summarizing the vulnerabilities discovered during the cloud penetration test, recommending mitigation strategies to protect cloud environments from future attacks.

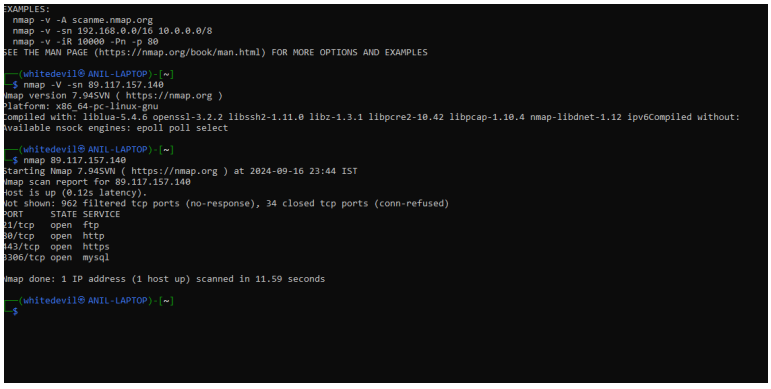

Figure: Cloud Penetration Testing with Kali Linux

4.6.1 Activity Log for Sixth Week

Day & Date	**Brief Description of the Daily Activity**	**Learning Outcome**	**Internship Mentor Signature**
Day 1 17-06-2024	Discussion on ISO/IEC 27001	Understood compliance frameworks and their importance in securing sensitive data	
Day 2 18-06-2024	Reviewed and contributed to SkillDzire's cybersecurity policies	Developed skills in updating security policies based on industry standards	
Day 3 19-06-2024	Participated in a policy documentation session on cloud security	Gained insight into the unique challenges and solutions in cloud security	
Day 4 20-06-2024	Case study analysis of recent cybersecurity breaches	Learned how companies handle security breaches and their post-incident recovery strategies	
Day 5 21-06-2024	Drafted sections of updated cybersecurity policy for network and incident response	Gained experience in creating actionable security policies	

4.6.2 Weekly Report

WEEK – 6 (From Dt 17-06-2024 to Dt 21-06-2024)

Objective of the Activity Done:

The goal this week was to enhance my understanding of cybersecurity compliance, review real-world breach case studies, and contribute to policy updates.

Detailed Report:

During Week 6, I participated in detailed discussions on cybersecurity compliance frameworks, including **ISO/IEC 27001**. This helped me understand the regulatory requirements that organizations must follow to secure sensitive data and maintain compliance.

I also contributed to updating SkillDzire's cybersecurity policies, focusing on sections related to network security and incident response. This experience provided practical insights into drafting effective security policies that align with industry standards. Additionally, I attended a policy session focused on cloud security, which introduced me to the challenges faced in protecting cloud infrastructures.

Furthermore, I reviewed case studies of recent cybersecurity breaches, analyzing what went wrong and how companies recovered. This provided me with a solid understanding of incident response, which would be applied in future projects.

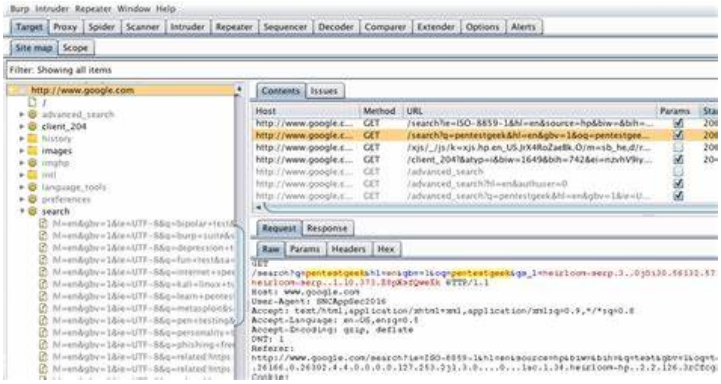

Figure: Cybersecurity Policy Discussion and Updates

4.7.1 Activity Log for Seventh Week

Day & Date	**Brief Description of the Daily Activity**	**Learning Outcome**	**Internship Mentor Signature**
Day 1 24-06-2024	Session on implementing secure network architectures	Learned how to design and implement secure network topologies	
Day 2 25-06-2024	Configured firewalls and access control lists (ACLs) on the network	Gained practical experience in securing networks by configuring firewalls	
Day 3 26-06-2024	Conducted a full security audit of SkillDzire's internal network	Developed skills in performing comprehensive security audits	
Day 4 27-06-2024	Implemented advanced IDS configurations using Snort	Enhanced knowledge of IDS setup and tuning to detect potential threats	
Day 5 28-06-2024	Reviewed audit findings and prepared a report on security improvements	Learned how to communicate audit results effectively and recommend fixes	

4.7.2 Weekly Report

WEEK – 7 (From Dt 24-06-2024 to Dt 28-06-2024)

Objective of the Activity Done:

This week focused on configuring network security tools, conducting internal security audits, and implementing advanced intrusion detection techniques.

Detailed Report:

During Week 7, I gained practical experience in securing internal networks. The week began with a session on secure network architectures, where I learned about the best practices for designing secure network infrastructures. I configured **firewalls** and **Access Control Lists (ACLs)** to control network traffic and prevent unauthorized access.

Additionally, I conducted a full security audit of SkillDzire's internal network, which involved reviewing network configurations, identifying potential weaknesses, and implementing improvements. I also configured **Snort**, an open-source **Intrusion Detection System (IDS)**, to monitor the network for suspicious activities. This task improved my understanding of IDS setup, tuning, and effective threat detection.

At the end of the week, I reviewed the audit findings and prepared a report that included recommendations for improving network security. This provided me with experience in documenting technical findings and communicating them clearly.

4.8.1 Activity Log for Eighth Week

Day & Date	**Brief Description of the Daily Activity**	**Learning Outcome**	**Internship Mentor Signature**
Day 1 01-07-2024	Explored web application firewall (WAF) configurations. Completed daily assessment exam on the topic of Web Application Firewalls on learn.skilldzire.com	Gained knowledge on securing web applications using WAFs	
Day 2 02-07-2024	Configured WAF to protect SkillDzire's web applications. Completed daily assessment exam on firewall configuration at learn.skilldzire.com	Gained hands-on experience in configuring and managing WAFs	
Day 3 03-07-2024	Performed a vulnerability scan using OWASP ZAP on web applications. Took an assessment on OWASP security principles on learn.skilldzire.com	Learned to identify and mitigate common web application vulnerabilities	
Day 4 04-07-2024	Documented vulnerabilities and prepared mitigation strategies. Completed assessment exam on vulnerability mitigation techniques	Improved skills in vulnerability documentation and threat mitigation	
Day 5 05-07-2024	Conducted a penetration test on web applications. Took the final exam for web security assessment on learn.skilldzire.com	Gained hands-on experience in testing web applications for security flaws	

4.8.2 Weekly Report

WEEK – 8 (From Dt 01-07-2024 to Dt 05-07-2024)

Objective of the Activity Done:

The main focus this week was securing web applications, including firewall configuration, vulnerability scanning, penetration testing, and daily assessment exams on the learn.skilldzire.com platform.

Detailed Report:

In Week 8, my primary focus was on securing SkillDzire's web applications. This involved configuring a **Web Application Firewall (WAF)**, which provided protection against common web application attacks such as SQL injections and cross-site scripting (XSS). Alongside this practical work, I completed daily assessments on the **learn.skilldzire.com** platform to reinforce the concepts I was learning.

On **Day 1**, I explored WAF configurations and took an assessment exam on firewall basics. **Day 2** involved configuring the WAF to protect SkillDzire's applications, followed by an exam on WAF deployment.

Throughout the week, I conducted a vulnerability scan on SkillDzire's web applications using **OWASP ZAP**. The daily assessments helped me better understand the OWASP security principles, which I applied in practice. I documented identified vulnerabilities and created mitigation strategies based on assessment feedback.

At the end of the week, I performed a **penetration test** on the web applications to validate the security measures implemented. The final exam on **learn.skilldzire.com** for web security assessment provided an opportunity to test my understanding of the overall security framework, from firewall management to vulnerability detection and remediation.

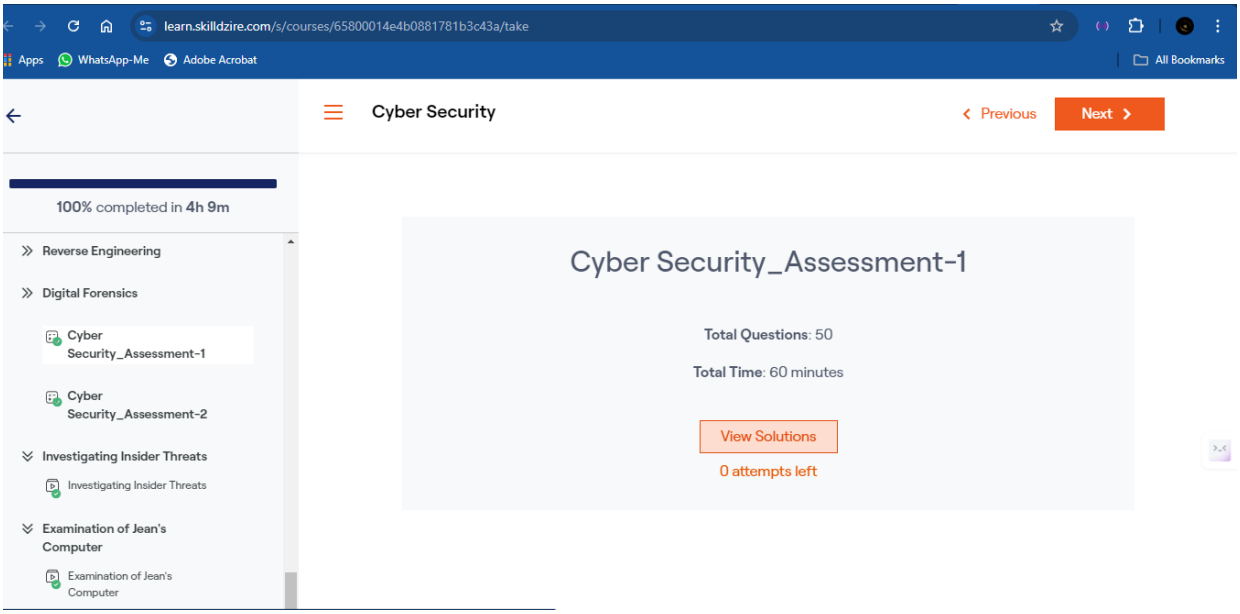

Figure: Assessment portal of SkillDzire

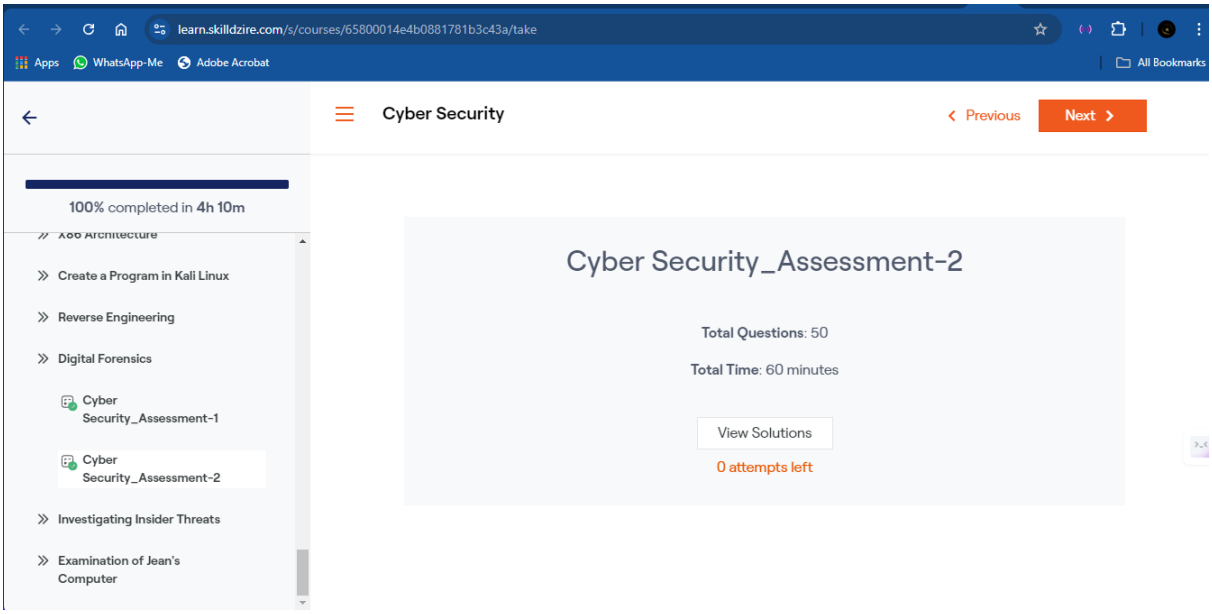

Figure: Assessment portal of SkillDzire

Chapter 5: Outcomes Description

5.1 Describe the work environment you have experienced

The work environment at **SkillDzire Technologies** has been both collaborative and innovative, fostering a strong culture of continuous learning. The team's structure is flat, ensuring open communication between junior staff, interns, and senior management. My immediate supervisor was always approachable, offering guidance on both technical challenges and career development.

The cybersecurity team worked in an agile environment with daily stand-up meetings to discuss ongoing projects, challenges, and goals. Weekly knowledge-sharing sessions focused on the latest cybersecurity developments, encouraging active participation and independent exploration.

5.2 Describe the Real-Time Technical Skills You Have Acquired

During the internship, I acquired several real-time technical skills in cybersecurity:

- **Network Security Auditing**: Hands-on experience with tools like **Nmap** and **Wireshark** for vulnerability assessments and network traffic analysis.
- **Penetration Testing**: Used **Metasploit** to simulate penetration tests, exploit known vulnerabilities, and assess security controls.
- **Web Application Security**: Worked with **OWASP ZAP** and **Burp Suite** to identify and mitigate risks like SQL injection and cross-site scripting (XSS).
- **Incident Response**: Participated in mock drills using **Snort** for Intrusion Detection, learning how to detect and respond to security breaches.

5.3 Describe the Managerial Skills You Have Acquired

In addition to technical skills, I developed critical managerial skills, including:

- **Task Prioritization**: Learned to prioritize cybersecurity tasks based on their impact and urgency.
- **Project Management**: Took ownership of projects such as conducting security audits and writing vulnerability reports.
- **Team Collaboration**: Participated in team meetings and discussions, enhancing my communication and teamwork abilities.
- **Decision-Making**: Gained experience in making quick decisions during incident response scenarios.

5.4 Describe How You Could Improve Your Communication Skills

While I improved my communication skills, there are areas I could further develop:

- **Technical Writing**: I need to work on simplifying complex technical information for non-technical stakeholders.
- **Public Speaking**: I could improve my confidence when presenting technical concepts in front of large audiences.
- **Active Listening**: Enhancing my active listening skills will help me better understand different perspectives during team discussions.
- **Clarifying Technical Jargon**: I could improve in translating technical terms into plain language when working with cross-functional teams.

5.5 Describe the Technological Developments You Have Observed and Relevant to the Subject Area of Training

During my internship, I observed several key technological developments in the field of cybersecurity:

- **Zero-Trust Architecture**: Adoption of the Zero-Trust model, which assumes that no entity can be trusted by default, improving overall security.
- **Cloud Security**: Increased emphasis on securing cloud environments using tools like **AWS Shield** and **Azure Security Center**.
- **Automation in Cybersecurity**: Tools like **SIEM** (Security Information and Event Management) automate repetitive tasks, improving efficiency in threat detection and incident response.
- **Machine Learning in Threat Detection**: Machine learning algorithms are increasingly being used to detect anomalies and patterns in large datasets, improving threat detection capabilities.

6.Annexure

All the signed weekly reports are enclosed here

Student Self Evaluation of the short-Term Internship

Student Name: SINTHU ANIL	**Registration No:22VV5A1273**
Term of Internship: 2 months	**From: May To : July**
Date of Evaluation:	
Organization Name : SkillDzire Technologies	

Please rate your performance in the following areas:

Rating Scale: Letter grade of CGPA calculation to be provided

1	Oral communication	1	2	3	4	5
2	Written communication	1	2	3	4	5
3	Proactiveness	1	2	3	4	5
4	Interaction ability with community	1	2	3	4	5
5	Positive Attitude	1	2	3	4	5
6	Self-confidence	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Work Plan and organization	1	2	3	4	5
9	Professionalism	1	2	3	4	5
10	Creativity	1	2	3	4	5
11	Quality of work done	1	2	3	4	5
12	Time Management	1	2	3	4	5
13	Understanding the Community	1	2	3	4	5
14	Achievement of Desired Outcomes	1	2	3	4	5
15	**OVERALLPERFORMANCE**	**1**	**2**	**3**	**4**	**5**

Date: Signature of the Student

Evaluation by the Internship Mentor

Student Name: SINTHU ANIL	**Registration No: 22VV5A1273**
Term of Internship: 2 months	**From: May To : July**
Date of Evaluation:	
Organization Name : SkillDzire Technologies	

Please rate your performance in the following areas:

Rating Scale: Letter grade of CGPA calculation to be provided

1	Oral communication	1	2	3	4	5
2	Written communication	1	2	3	4	5
3	Proactiveness	1	2	3	4	5
4	Interaction ability with community	1	2	3	4	5
5	Positive Attitude	1	2	3	4	5
6	Self-confidence	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Work Plan and organization	1	2	3	4	5
9	Professionalism	1	2	3	4	5
10	Creativity	1	2	3	4	5
11	Quality of work done	1	2	3	4	5
12	Time Management	1	2	3	4	5
13	Understanding the Community	1	2	3	4	5
14	Achievement of Desired Outcomes	1	2	3	4	5
15	**OVERALL PERFORMANCE**	**1**	**2**	**3**	**4**	**5**

Date: Signature of the Mentor

Internal Assessment Statement

Name of the Student : SINTHU ANIL

Programme of Study : B Tech

Year Of Study : IV year

Branch : INFORMATION TECHNOLOGY

Register No/H.T. No : 22VV5A1273

Name of the College : JNTUGV COLLEGE OF ENGINEERING,VIZIANAGARAM

University : JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY GURAJADA VIZIANAGARAM

Sl.No	Evaluation Criteria	Maximum Marks	Marks Awarded
1.	Report	20	
2.	Oral presentation	30	
	Grand Total	50	

Certified by

Signature of the Mentor **Signature of the Head of the Department**

seal: