

AN INTERNSHIP REPORT ON
CYBER SECURITY

Submitted in the partial fulfilment of the requirement for the award of degree of

BACHELOR OF TECHNOLOGY
In
COMPUTER SCIENCE AND ENGINEERING

Submitted by

Thumu Tejaswini(21471A05L0)

Under the esteemed guidance of

Mr. K.V.Narasimha Reddy B.Tech, M.Tech.

Assistant Professor



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NARASARAOPETA ENGINEERING COLLEGE: NARASAROPET
(AUTONOMOUS)

Accredited by NAAC with A+ Grade and NBA under Tyre -1

NIRF rank in the band of 201-300 and an ISO 9001:2015 Certified

Approved by AICTE, New Delhi, Permanently Affiliated to JNTUK, Kakinada
KOTAPPAKONDA ROAD, YALAMANDA VILLAGE, NARASARAOPET- 522601
2024-2025

NARASARAOPETA ENGINEERING COLLEGE: NARASARAOPET

(AUTONOMOUS)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



CERTIFICATE

This is certify that the Internship report entitled as “**CYBER SECURITY**” is a bonafide work done by **Thumu Tejaswini (21471A05L0)** in partial fulfilment of the requirements for the award of the degree of **BACHELOR OF TECHONOLOGY** in the Department of **COMPUTER SCIENCE AND ENGINEERING** during 2024-2025.

INTERNSHIP GUIDE

Mr.K.V.Narasimha Reddy M.Tech
Assistant Professor

HEAD OF THE DEPARTMENT

Dr.S.N.Tirumala RaoM.Tech, Ph.D
Professor & HOD

EXTERNAL EXAMINER

Program Book For Long-Term Internship

Name of the Student : Thumu Tejaswini
Name of the College : Narasaraopeta Engineering College
Registration Number : 21471A05L0
Period of Internship : From: 03- 02-2025 to 18-03-2025
Name of the : Black Bucks
Internship Organization

An Internship Report On

Cyber Security

Submitted in accordance with the requirement for the degree of B.Tech

Name of the Student : Thumu Tejaswini
Name of the College : Narasaraopeta Engineering College
Department : Computer Science and Engineering
Name of the Supervisor : Mr. K.V.Narasimha Reddy
Duration of the : From: 03-02, 2025 to 18-03-2025
Internship

Programme of Study : B.Tech -CSE
Year of Study : IV Year
Register Number : 21471A05L0
Date of Submission :

Declaration of Student



I, Thumu Tejaswini, student of **B.Tech- Computer Science And Engineering**, bearing Regd.No. **21471A05L0** of the department of CSE, Narasaraopeta Engineering College, do hereby declare that I have completed the Internship in Cyber Security organized by BlackBucks Technologies Pvt. Ltd., Hyderabad, from 03-02-2025 to 18-03-2025, under the faculty guideship of Mr. K.V.Narasimha Reddy, Assistant Professor, Department of CSE.

Endorsements

Internship Guide

Head of the Department

Certificate from Intern Organization




ANDHRA PRADESH STATE COUNCIL OF HIGHER EDUCATION
(A Statutory Body of the Government of A.P.)

Certificate of Completion



Certificate Id: **BBAPSCHDE2025LTIN002837**

This is to certify that **Thumu Tejaswini**, bearing Reg. No: **21471A05L0**, from **Narasaraopeta Engineering College**, has successfully completed a **Long-term internship for 240 hours** on **Cyber Security** in the year **2025**. This internship was organized by **Blackbuck Engineers**, in association with the **Andhra Pradesh State Council of Higher Education (APSCE)**.



Anuradha Thota
Chief Executive Officer
Blackbuck Engineers Pvt. Ltd.

Date: 17/03/2025
Place: Hyderabad

ACKNOWLEDGEMENT

We wish to express our thanks to various personalities who are responsible for the completion of the Internship. We are extremely thankful to our beloved chairperson **Sri M.V. Koteswara Rao** B.Sc., who took keen interest on us in every effort throughout this course. We owe our gratitude to our principal **Dr. S. Venkateswarlu** M. Tech., Ph.D., for his kind attention and valuable guidance throughout the course.

We express our deep-felt gratitude to **Dr. S. N. Tirumala Rao** M. Tech, Ph.D., Professor & Head, Department of CSE and also to our guide, **Mr. K.V.Narasimha Reddy**, Assistant Professor, Department of CSE, for extending their valuable guidance and encouragement. Their profound knowledge and willingness have been a constant source of inspiration for us throughout this internship.

We extend our sincere thanks to all other Teaching and Non-Teaching staff to department for their cooperation and encouragement during our B.Tech degree. we have no words to acknowledge the warm affection, constant inspiration, and encouragement that we receive from our parents.

We affectionately acknowledge the encouragement received from our friends and those who involved in giving valuable suggestions had clarifying out doubts, which had really helped us in successfully completing our internship.

SUBMITTED BY

T.Tejaswini

(21471A05L0)



INSTITUTE VISION AND MISSION

INSTITUTION VISION

To emerge as a Centre of excellence in technical education with a blend of effective student centric teaching learning practices as well as research for the transformation of lives and community.

INSTITUTION MISSION

M1: Provide the best class infra-structure to explore the field of engineering and research

M2: Build a passionate and a determined team of faculty with student centric teaching, imbining experiential, innovative skills

M3: Imbibe lifelong learning skills, entrepreneurial skills and ethical values in students for addressing societal problems



DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

VISION OF THE DEPARTMENT

To become a centre of excellence in nurturing the quality Computer Science & Engineering professionals embedded with software knowledge, aptitude for research and ethical values to cater to the needs of industry and society.

MISSION OF THE DEPARTMENT

The department of Computer Science and Engineering is committed to

M1: Mould the students to become Software Professionals, Researchers and Entrepreneurs by providing advanced laboratories.

M2: Impart high quality professional training to get expertize in modern software tools and technologies to cater to the real time requirements of the Industry.

M3: Inculcate team work and lifelong learning among students with a sense of societal and ethical responsibilities.



Program Specific Outcomes (PSO's)

PSO1: Apply mathematical and scientific skills in numerous areas of Computer Science and Engineering to design and develop software-based systems.

PSO2: Acquaint module knowledge on emerging trends of the modern era in Computer Science and Engineering

PSO3: Promote novel applications that meet the needs of entrepreneur, environmental and social issues.



Program Educational Objectives (PEO's)

The graduates of the programme are able to:

PEO1: Apply the knowledge of Mathematics, Science and Engineering fundamentals to identify and solve Computer Science and Engineering problems.

PEO2: Use various software tools and technologies to solve problems related to academia, industry and society.

PEO3: Work with ethical and moral values in the multi-disciplinary teams and can communicate effectively among team members with continuous learning.

PEO4: Pursue higher studies and develop their career in software industry.



Program Outcomes

PO1: Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2: Problem analysis: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3: Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6: The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7: Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9: Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11: Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12: Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Internship Course Outcomes (CO'S):

Student is able to

CO421.1: Construct the company profile by compiling the brief history, management structure, products / services offered, key achievements and market performance for his / her organization of internship.

CO421.2: Assess its Strengths, Weaknesses, Opportunities and Threats (SWOT) organization of internship

CO421.3: Determine the challenges and future potential for his / her internship organization in particular and the sector in general.

CO421.4: test the theoretical learning in practical situations by accomplishing the tasks assigned during the internship period.

CO421.5: Apply various soft skills such as time management, positive attitude and communication skills during performance of the tasks assigned in internship organization.

CO421.6: Analyse the functioning of internship organization and recommend changes for improvement in processes and prepare the project Documentation and present the Report using appropriate method.

Course Outcomes – Program Outcomes mapping

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
C421.1		✓											✓		
C421.2	✓		✓		✓								✓		
C421.3				✓		✓	✓	✓					✓		
C421.4			✓			✓	✓	✓					✓	✓	
C421.5					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C421.6									✓	✓	✓		✓	✓	

Course Outcomes – Program Outcome correlation

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
C421.1	2	3											2		
C421.2			2		3								2		
C421.3				2		2	3	3					2		
C421.4			2			1	1	2					3	2	
C421.5					3	3	3	2	3	2	2	1	3	2	1
C421.6									3	2	1		2	3	

Note: The values in the above table represent the level of correlation between CO's and PO's:

1. Low level

2. Medium level

3. High level

Internship mapping with various courses of Curriculum with Attained PO's:

Name of the course from which principles are applied in this project	Description of the device	Attained PO
CC2204	Gathering the requirements and defining the problem, plan to develop a Medical Inventory Management system	PO1, PO3
CC2204	Each and every requirement is critically analyzed, the process model is identified and divided into four modules	PO2, PO3
CC2204,CC12L12	Logical design is done by using the unified modelling language which involves individual team work	PO3, PO5, PO9
CC2204,CC12L12,CC2203	Each and every module is tested, integrated, and evaluated in our project	PO1, PO5
CC12L13	Documentation is done by all our four members in the form of a group	PO10
CC2204	Each and every phase of the work is presented periodically	PO10, PO11
CC12L13,CC2203	Implementation is done and the project will be handled by the Medical Inventory Management system and in future updates in our project can be done based on 360digiTMG.	PO4, PO7
CC12L13,CC2203	The physical web page design includes software components like jupyter,Phthon,Mysql	PO5, PO6

INDEX

S.NO	CONTENTS	PAGE NO
1	Executive Summary	
2	Internship Part	
3	Week 1: Introduction to Cyber Security, Information security, CIA and ethical Hacking	
4	Week 2: Types of Pentesting, Scanning Networks, Advanced Network Scanning, Scanning IDS/IPS	
5	Week 3: Types of Enumeration, System Hackin, Vulnerability Analysis,	
6	Week 4: GenAI in Cybersecurity, Vulnerability Assessment & System Hacking, Cloud Service Providers, VPC, WAF and Cloud	
7	Week 5: Executive Summary: Provide a high-level overview of cybersecurity threats and assessments.	
8	Week 6: Introduction about the project, Details about Abstract	
9	Week 7: Abstract and System Requirements Submission	
10	Week 8: Design and implementation of project	
11	Outcome Description	
12	Photos	
13	Student Self Evaluation of the Short-Term Internship	
14	Evaluation by the Supervisor of the Intern Organization	

1. EXECUTIVE SUMMARY

BlackBucks is a company that offers virtual assistant services to individuals and businesses. Their virtual assistants are trained professionals who can handle a wide range of tasks, including scheduling appointments, managing email, conducting research, and more. The company is based in the United States and has a team of experienced managers and support staff who are dedicated to ensuring that their virtual assistants meet the high standards of quality and efficiency. BlackBucks has a reputation for providing excellent customer service and consistently delivering high-quality work. We strongly believe that Job is the byproduct of our skill sets. If we have relevant industry skills automatically it will lead to multiple opportunities. That's exactly what we designed for engineering graduates. Our goal is to specifically help bring changes happen in the country in a programmed & faster manner.

2. INTERNSHIP PART

Cyber Security tutorial covers basic and advanced concepts, specially designed to cater to both students and experienced working professionals. This Cyber Security tutorial helps you gain a solid introduction to the fundamentals of Cyber Security and explore a wide range of techniques, including penetration, vulnerability, and Reverse Engineering.

Cyber Security is the practice of protecting systems, networks, and data from unauthorized access, theft, and damage. With the rapid evolution of technology, artificial intelligence (AI) has emerged as a vital tool in strengthening cybersecurity defenses. AI refers to systems or machines that mimic human intelligence, enabling them to perform tasks such as decision-making, problem-solving, and pattern recognition.

One of the key advantages of AI in cybersecurity is its ability to adapt and learn from new attack methods. By processing and analyzing data in real-time, AI systems can identify emerging threats and implement countermeasures more quickly than traditional methods. Additionally, AI can predict vulnerabilities in systems, helping organizations to strengthen their defenses proactively.

However, the use of AI in cybersecurity also introduces challenges. Cybercriminals are leveraging AI to create sophisticated attacks, such as AI-generated phishing emails or automated hacking tools. Furthermore, AI systems rely heavily on data, raising concerns about privacy and the ethical use of information.

To maximize the benefits of AI in cybersecurity, organizations must strike a balance between technological advancements and ethical considerations. They should implement secure data handling practices, ensure transparency in AI systems, and invest in continuous training for cybersecurity professionals. By harnessing the potential of AI, the cybersecurity industry can enhance its ability to detect, prevent, and respond to threats, ensuring the safety of critical assets in an increasingly digital world.

Features of Cyber Security

- Identifying potential security threats such as malware, phishing attacks, and unauthorized access.
- Safeguarding sensitive information through encryption, access controls, and Secure storage.

- Ensuring the confidentiality, integrity, and availability (CIA triad) of data.
- Securing networks through firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).
- Assessing potential risks to systems and data, and implementing measures to reduce these risks.
- Implementing access controls, encryption, and secure configurations specific to cloud platforms.

ACTIVITY LOG FOR FIRST WEEK
WEEK -1: From 03-02-2025 To 07-02-2025

S.NO	DATE	DESCRIPTION	SIGN
1	03/02/2025 Monday	Introduction to Cyber Security	
2	04/02/2025 Tuesday	Assessment test-01 on Cyber Security	
3	05/02/2025 Wednesday	CIA Triad, Information Security, Case Study, Firewalls	
4	06/02/2025 Thursday	Assessment test-02 on CIA, Information Security, Case Study, Firewalls	
5	07/02/2025 Friday	Phases of Ethical Hacking, Network Security Overview	
6	07/02/2025 Saturday	Cloud security Overview, Hackers Mindset	

Week 1: Introduction to Cyber Security

Topic Covered: Introduction to Cyber Security.

Description: In Cybersecurity is the practice of protecting systems, networks, and data from digital threats. It encompasses a wide range of technologies, processes, and practices designed to defend against attacks like malware, phishing, ransomware, and unauthorized access. In an increasingly connected world, cybersecurity is crucial for individuals, organizations, and governments to safeguard sensitive information and maintain operational continuity. It is a dynamic field that evolves alongside emerging technologies and threats, requiring constant vigilance and adaptation.

The significance of cybersecurity lies in its ability to prevent financial loss, data breaches, and reputational damage. For instance, a cyberattack on a business can result in stolen customer data, disrupted operations, and legal liabilities. By implementing measures such as encryption, access controls, and secure coding practices, cybersecurity aims to address these challenges proactively.

To tackle evolving threats, cybersecurity integrates various tools and strategies, including antivirus software, firewalls, intrusion detection systems, and incident response plans. Awareness and education play an equally critical role, as human error is a leading cause of security breaches. Together, these efforts help build resilient systems capable of withstanding cyber threats.

The session covered the three pillars of cybersecurity: **Confidentiality**, which ensures data privacy and restricts unauthorized access; **Integrity**, which maintains the accuracy and trustworthiness of data; and **Availability**, which ensures data and systems are accessible when needed. Real-world examples were discussed to illustrate each pillar's significance. Information security strategies and tools, including data encryption, access controls, and secure storage practices, were explored to protect sensitive information from breaches.

A case study on a major cybersecurity breach, such as Target's 2013 data breach, was analyzed to highlight lessons learned and preventive measures. Additionally, firewalls were introduced as a critical network security component, with discussions on types of firewalls (hardware, software, and cloud-based) and their functions. The session provided participants with a deeper understanding of core cybersecurity principles and practical applications of firewalls in securing networks.

The session introduced the five phases of ethical hacking: **Reconnaissance** (gathering information about the target), **Scanning** (identifying vulnerabilities), **Gaining Access**

(exploiting vulnerabilities), **Maintaining Access** (establishing a persistent presence), and **Covering Tracks** (erasing evidence). A comprehensive overview of network security tools and techniques was provided, including firewalls, intrusion detection/prevention systems (IDS/IPS), and VPNs, to protect networks from unauthorized access, misuse, or destruction. Cloud security was also discussed, focusing on securing data, applications, and infrastructure in cloud environments, while addressing challenges like shared responsibility, data privacy, and access management. Additionally, the hackers' mindset was explored to understand attackers' thought processes, highlighting the differences between black hat, white hat, and gray hat hackers. Participants gained an appreciation for the strategic approach required in ethical hacking and valuable insights into securing modern networks and cloud systems.

ACTIVITY LOG FOR SECOND WEEK
WEEK -2: From 10-02-2025 To 15-02-2025

S.NO	DATE	DESCRIPTION	SIGN
1	10/02/2025 Monday	Types of Pentesting , Info sec Laws & Standards, Information Gathering / Foot printing & Reconnaissance	
2	11/02/2025 Tuesday	Assignment 01, Assessment test-3,4 on cyber security and types of pentesting.	
3	12/02/2025 Wednesday	Scanning Networks, Network Scanning Basics, Nmap Scanning Commands, Port Scanning, Countermeasures for Scanning Attacks, IDS/IPS Role in Network Scanning.	
4	13/02/2025 Thursday	Assignment test-05,06 on scanning network and ids/ips	
5	14/02/2025 Friday	Advanced Network Scanning Scanning IDS/IPS Fragmentation Techniques	
6	15/02/2025 Saturday	Slow Scan Techniques Firewall Evasion Techniques	

Week 2: Types of Pentesting

Topic Covered: Types of Pentesting, Scanning Networks, Advanced Network Scanning, Scanning IDS/IPS, Scanning Networks, Advanced Network Scanning

Description: Penetration testing (pentesting) is a simulated attack on a system, network, or application to identify vulnerabilities before malicious actors can exploit them. Different types of pentesting include **Black Box Testing** (testing with no prior knowledge of the system), **White Box Testing** (full knowledge of the system is provided), and **Gray Box Testing** (limited knowledge of the system). Pentesting helps organizations uncover security flaws, evaluate their defenses, and improve their overall cybersecurity posture.

Information security laws and standards provide a framework for ensuring data protection and compliance. Laws like GDPR, HIPAA, and CCPA mandate how organizations should handle personal and sensitive data, while standards like ISO/IEC 27001 establish guidelines for implementing robust information security management systems. These regulations aim to safeguard privacy, mitigate risks, and ensure accountability.

Information gathering, also known as footprinting or reconnaissance, is the first step in ethical hacking. This process involves collecting data about a target to identify potential vulnerabilities. Techniques include open-source intelligence (OSINT), WHOIS lookups, DNS enumeration, and analyzing publicly available information. Reconnaissance is crucial for understanding the target environment and planning subsequent actions. Network scanning is the process of identifying active hosts, open ports, and services in a network to detect potential vulnerabilities. Tools like **Nmap** (Network Mapper) are widely used for this purpose. Nmap scanning commands help identify open ports, determine operating systems, and map network structures. Key types of scans include

TCP Connect Scans, SYN Scans, and UDP Scans.

Countermeasures for scanning attacks involve implementing strong network security practices, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and monitoring tools. IDS/IPS systems play a critical role in detecting and preventing malicious activities during network scans. For instance, they can flag unusual traffic patterns and block attempts to exploit vulnerabilities. These measures help organizations secure their networks against reconnaissance efforts by attackers. Port scanning is a subset of network scanning that specifically targets network ports to determine their status (open, closed, or filtered). Open ports often represent potential entry points for attackers. Organizations mitigate these risks by restricting unnecessary open ports, deploying firewalls, and monitoring for suspicious scanning

activity. Advanced network scanning involves sophisticated methods to bypass security measures and gather more in-depth information. Techniques like **fragmentation** split packets into smaller fragments to evade detection by IDS/IPS systems. Slow scan techniques, such as sending packets at irregular intervals, are used to avoid raising alarms. These methods require careful analysis to detect and prevent.

Firewall evasion techniques are designed to bypass network defenses, enabling attackers to scan or penetrate systems without being detected. Common methods include spoofing IP addresses, tunneling traffic through trusted protocols, and using encrypted communication channels. Such techniques highlight the need for robust firewall configurations and continuous monitoring.

ACTIVITY LOG FOR THIRD WEEK
WEEK -3: From 17-02-2025 To 22-02-2025

S.NO	DATE	DESCRIPTION	SIGN
1	17/02/2025 Monday	Enumeration: What is Enumeration? Types of Enumeration Important Ports for Enumeration	
2	18/02/2025 Tuesday	Assessment test-07 on Enumeration and types of Enum	
3	19/02/2025 Wednesday	System Hacking: Gaining Access Password Cracking Techniques, Privilege Escalation, Maintaining Access, Clearing Tracks	
4	20/02/2025 Thursday	Assessment test-08 on System Hacking and Hacking System	
5	21/02/2025 Friday	Vulnerability Analysis: What is Vulnerability? Vulnerability Assessment Process, Active Assessment, Passive Assessment.	
6	21/02/2025 Saturday	External Assessment, Internal Assessment, Risk Assessment, Creating Baseline Report	

Week 3: Enumeration

Topic Covered: Enumeration, System Hacking, Vulnerability Analysis

Description: Enumeration is the process of actively gathering detailed information about a target system or network after gaining access during an attack or penetration test. It focuses on extracting data such as user accounts, network shares, system policies, and services. Unlike reconnaissance, which is passive, enumeration requires active interaction with the target system.

The main types of enumeration include NetBIOS Enumeration, SNMP Enumeration, LDAP Enumeration, DNS Enumeration, and SMB Enumeration. Each type focuses on a specific protocol or service, aiming to gather relevant information such as shared resources, user credentials, or domain details. For example, NetBIOS enumeration identifies shared directories and files, while DNS enumeration gathers details about domain names and subdomains.

System hacking involves exploiting vulnerabilities in a target system to gain unauthorized access and maintain control. The process typically includes gaining access, cracking passwords, escalating privileges, maintaining access, and clearing tracks to avoid detection. Password-cracking techniques include brute force, dictionary attacks, and rainbow tables, which systematically test combinations of passwords to find the correct one.

Privilege escalation involves exploiting vulnerabilities to gain higher-level permissions on a system. For instance, attackers may exploit misconfigurations or software flaws to move from a regular user account to an administrator account. Once access is gained, maintaining control ensures continued exploitation. Techniques include installing backdoors, rootkits, or creating new user accounts.

Clearing tracks is the final step in system hacking, ensuring that evidence of the attack is removed to evade detection. This involves deleting logs, clearing command history, or modifying timestamps. Understanding these techniques helps organizations build effective countermeasures, such as implementing logging tools, system hardening, and intrusion detection systems.

Vulnerability analysis is the systematic process of identifying, analyzing, and addressing weaknesses in a system, network, or application that could be exploited by attackers. A vulnerability is any flaw or misconfiguration that can be used to gain unauthorized access or disrupt services. The analysis helps organizations understand their risk exposure and prioritize mitigation efforts. Creating a baseline report is a critical step in vulnerability analysis, documenting existing security controls and known vulnerabilities. This report serves as a reference point for tracking improvements and ensuring compliance with security policies. By

addressing vulnerabilities proactively, organizations can reduce the likelihood of successful attacks and maintain a strong security posture.

ACTIVITY LOG FOR FOURTH WEEK
WEEK -4: From 24-02-2025 To 01-03-2025

S.NO	DATE	DESCRIPTION	SIGN
1	24/02/2025 Monday	GenAI in Cyber security, Defensive Usage of AI	
2	25/02/2025 Tuesday	Assessment test-09, Assignment test-03 on the GenAI and Cyber Security	
3	26/02/2025 Wednesday	Vulnerability Assessment & System Hacking Continued	
4	27/02/2025 Thursday	Assessment test-10 on vulnerability Assessment and System Hacking	
5	28/02/2025 Friday	Cloud Service Providers (AWS, GCP, Azure),	
6	28/02/2025 Saturday	VPC (Virtual Private Cloud)	

Week 4: GenAI in Cyber security

Topic Covered: GenAI in Cyber security, Defensive Usage of AI, Vulnerability Assessment & System Hacking Continued, Cloud Service Providers, VPC

Description: Generative AI (GenAI) has emerged as a powerful tool in cybersecurity, enhancing the ability to detect, prevent, and respond to cyber threats. In defensive applications, GenAI is used to identify patterns in vast datasets, enabling real-time anomaly detection and threat analysis. For example, AI-driven tools can analyze network traffic to identify potential intrusions or predict attack patterns by analyzing historical data.

Defensive AI can also automate vulnerability assessments, generate simulated attack scenarios, and provide recommendations for mitigation. Its ability to learn and adapt to new threats makes it an invaluable asset for cybersecurity teams. Additionally, GenAI-powered chatbots and virtual assistants help in responding to incidents, providing technical support, and educating users about best security practices.

Despite its benefits, the use of GenAI in cybersecurity also raises concerns about adversarial AI, where attackers use AI to develop sophisticated malware or bypass security measures. To counteract this, defensive AI must continually evolve, incorporating robust training data and deploying advanced algorithms to outsmart malicious actors. Vulnerability assessment continues to play a critical role in identifying security weaknesses in systems and networks. Techniques such as **active scanning**, **penetration testing**, and **risk assessment** are refined using AI-driven tools that enhance speed and accuracy. System hacking, as part of ethical hacking, involves advanced techniques for gaining access, escalating privileges, and maintaining control of a system while testing its defenses. Key methods in system hacking include advanced password-cracking techniques, social engineering, and exploiting zero-day vulnerabilities. Vulnerability assessments often involve creating a detailed baseline report, identifying internal and external threats, and recommending immediate countermeasures. By combining these practices, organizations can proactively secure their infrastructure against emerging threats. Cloud service providers like AWS, Google Cloud Platform (GCP), and Microsoft Azure are critical components of modern IT infrastructure, offering scalable and flexible solutions for organizations. Each provider offers a range of services, including compute, storage, machine learning, and database management, enabling businesses to optimize operations while reducing costs.

Security features, such as identity and access management (IAM), encryption, and monitoring tools, ensure robust protection for cloud environments. Virtual Private Cloud (VPC)

is a key offering in cloud computing, allowing organizations to isolate their cloud resources within a private network. VPCs provide enhanced control over network configuration, enabling users to define subnets, set up firewalls, and establish secure connections through VPNs or Direct Connect. This isolation minimizes the risk of unauthorized access and enhances overall security.

ACTIVITY LOG FOR FIFTH WEEK
WEEK -5: From 03-03-2025 To 08-03-2025

S.NO	DATE	DESCRIPTION	SIGN
1	03/03/2025 Monday	Executive Summary: Provide a high-level overview of cybersecurity threats.	
2	04/03/2025 Tuesday	Assessment test on Threat Intelligence and IoCs.	
3	05/03/2025 Wednesday	Recommendations & Actionable Steps: Develop incident response strategies.	
4	06/03/2025 Thursday	Assessment test on SIEM tools, hands-on log analysis.	
5	07/03/2025 Friday	Step-by-step approach to forensic analysis using Autopsy & Volatility	
6	08/03/2025 Saturday	Review of security policies and compliance guidelines.	

Week 5: Cybersecurity Assessment and Incident Response Report

Topic Covered: Executive Summary: Provide a high-level overview of cybersecurity threats and assessments.

Description:

This summary provides a comprehensive overview of cybersecurity assessments conducted during the week. The activities focused on identifying, analyzing, and mitigating cybersecurity threats through structured evaluations, hands-on exercises, and compliance strategies. Key topics included:

1. Cybersecurity Threat Overview:

- Provided a high-level summary of modern cybersecurity threats, including malware, phishing, insider threats, and ransomware.
- Discussed strategies for proactive threat defense, including network security, access controls, and encryption.

2. Threat Intelligence and Incident Response:

- Conducted an assessment on the significance of threat intelligence in identifying potential cyber threats.
- Evaluated different intelligence sources such as SIEM logs, threat feeds, and real-time monitoring to detect malicious activities.

3. Incident Response Strategies and Best Practices:

- Developed actionable steps to handle security incidents, covering preparation, detection, containment, eradication, and recovery.
- Studied real-world cybersecurity incidents to understand response mechanisms and their effectiveness.

4. SIEM Tools and Log Analysis:

- Hands-on assessment on the use of SIEM (Security Information and Event Management) tools to analyze security logs.
- Implemented log monitoring techniques to detect anomalies and potential threats in an enterprise environment.

5. Forensic Analysis and Digital Investigations:

- Explored forensic analysis methodologies, including evidence collection, digital footprints, and legal considerations.
- Conducted forensic investigations using tools like Autopsy and FTK Imager to analyze digital evidence.

6. Security Policies and Compliance Guidelines:

- Reviewed key cybersecurity policies and compliance frameworks such as ISO 27001, GDPR, and HIPAA.
- Discussed the role of security policies in maintaining organizational security and preventing data breaches.

Throughout the week, participants gained practical experience in security analysis, incident response, and forensic investigations. By leveraging SIEM tools and forensic techniques, they developed skills to detect, investigate, and mitigate cybersecurity threats effectively. The assessments provided a deeper understanding of modern cybersecurity challenges, equipping participants with the knowledge and tools required to safeguard digital environments.

ACTIVITY LOG FOR FIFTH WEEK
WEEK -6: From 10-03-2025 To 15-03-2025

S.NO	DATE	DESCRIPTION	SIGN
1	10/03/2025 Monday	Executive Summary: Provide a high-level overview of the Projects, titles	
2	11/03/2025 Tuesday	Assessment test-11, on Cloud, VPC	
3	12/03/2025 Wednesday	Recommendations Actionable Steps: Detailed remediation guidance for each project	
4	13/03/2025 Thursday	Assessment test-12, Assignment test-04 on VPC, Azure and Cloud	
5	14/03/2025 Friday	Detailed over View at Step-by-step process in project.	
6	15/03/2025 Saturday	Steps in Project	

Week 6: Penetration Test Report

Topic Covered: Executive Summary: Provide a high-level overview of the Projects, titles

Description: During This summary provides a high-level overview of cyber security projects designed to strengthen system defenses, ensure data protection, and enhance compliance with industry standards. The projects addressed critical areas of cyber security, focusing on real-world challenges and practical solutions. Key project titles included:

Implementing Secure Network Architectures: Focused on designing and deploying firewalls, intrusion detection/prevention systems (IDS/IPS), and virtual private networks (VPNs) to protect organizational networks.

Vulnerability Assessment and Mitigation Strategies: Emphasized identifying, analyzing, and addressing security vulnerabilities through active and passive assessments, creating baseline reports, and performing risk analysis.

Cloud Security Best Practices: Highlighted securing data, applications, and infrastructure across cloud platforms like AWS, Azure, and GCP, including implementing Virtual Private Clouds (VPCs) and adhering to the shared responsibility model.

Ethical Hacking and Penetration Testing: Explored ethical hacking methodologies, including reconnaissance, scanning, exploitation, and reporting to identify and address weaknesses in systems and applications.

Incident Response and Threat Management: Covered strategies for identifying, mitigating, and recovering from cybersecurity incidents, focusing on real-time monitoring and response mechanisms. These projects collectively enhanced participants' understanding of core cybersecurity principles, tools, and practices, equipping them with the skills to secure modern IT environments against evolving threats. OpenVAS (Open Vulnerability Assessment System) is a robust open-source tool used to identify vulnerabilities in systems, applications, and networks. The first step in using OpenVAS is setting it up securely by installing it on a protected host, updating vulnerability feeds, and configuring appropriate scanning profiles, such as "Full and Fast," tailored to the project scope. To maintain security, the tool should have restricted access, and scans should be scheduled during low-traffic periods to minimize disruptions. When conducting vulnerability scans, define target systems within the authorized scope, select or customize scan configurations to check for common vulnerabilities like outdated software or misconfigurations, and execute the scan while monitoring its progress.

After the scan, review the report to prioritize vulnerabilities based on their severity and potential impact. Address vulnerabilities by applying software updates, reconfiguring systems to align with best practices, and implementing strong password policies or multifactor authentication for critical systems. Post-remediation, continuous monitoring is essential. Regularly schedule scans with OpenVAS to keep assessments up-to-date and use its reporting features to track trends and recurring issues. For better integration, combine OpenVAS with security tools like SIEM for centralized monitoring and incident response. Additionally, educating administrators and stakeholders about common vulnerabilities and creating a comprehensive vulnerability management plan can further enhance the security posture. By following these steps, organizations can effectively use OpenVAS to identify, address, and monitor vulnerabilities, significantly reducing the risk of cyber threats.

ACTIVITY LOG FOR SEVENTH WEEK
WEEK -7: From 17-03-2025 To 22-02-2025

S.NO	DATE	DESCRIPTION	SIGN
1	17/03/2025 Monday	Explaining each and every round present in the project and clarifying doubts	
2	18/03/2025 Tuesday	Explained about the round 1 of the project and its PDF format	
3	19/03/2025 Wednesday	Overview details about the Round 2 System Requirements and its pdf format	
4	20/02/2025 Thursday	Abstract Submission and System requirement Submission Of the project	
5	21/03/2025 Friday	Implementation and process on how it worked	
6	22/03/2025 Saturday	Testing	

Week 7: Abstract and System Requirements Submission

Topic Covered: Abstract Submission and System requirement Submission

Description: In the ever-evolving digital landscape, where data drives innovation and decision-making, the need for automated and intelligent data extraction tools is more vital than ever. Manually collecting information from websites is time-consuming, inefficient, and prone to errors. As online content grows rapidly, especially in domains like news, research, and academia, it becomes essential to use tools that can systematically extract and analyze insights from web data. This project aims to develop an Intelligent Web Scraper and Text Analyzer — a solution that not only scrapes content from webpages but also performs natural language processing (NLP) to assess sentiment and readability. The system focuses on extracting blog articles or similar content from specified URLs and analyzing their tone, complexity, and structure. Built using Python, it uses requests for handling HTTP connections and BeautifulSoup to parse HTML, enabling accurate content extraction. The extracted text is then tokenized using NLTK. Sentiment is evaluated using the Afinn library, while readability is assessed using textstat, which computes scores like the Flesch Reading Ease. Unlike traditional scrapers that only collect raw data, this tool adds an analytical layer, allowing users to interpret emotional tone and readability. Structured output is supported using pandas, enabling tabular display and export to formats like CSV or Excel. The scraper also offers flexibility — users can input various URLs and adapt to different article structures with minimal changes. The project workflow begins with the user providing a URL. The system then connects to the webpage, extracts the main content, analyzes the text, and finally displays or stores the sentiment and readability scores. Integrating web scraping with NLP transforms unstructured content into actionable insights, making the tool both powerful and practical.

Abstract:

In today's data-driven world, where timely access to accurate information defines strategic advantage, manual data collection from websites is increasingly inefficient and impractical. This project introduces a Web Scraper for Information Gathering, an intelligent and automated system developed using Python to efficiently extract, process, and structure web-based data from a variety of online sources. Utilizing libraries such as BeautifulSoup, Selenium, and Requests, the tool is capable of retrieving content from both static and dynamic websites. Designed to recognize patterns, handle JavaScript-rendered pages, and bypass basic anti-scraping mechanisms, the system ensures high adaptability across diverse platforms like e-commerce sites, news portals, and government databases. The extracted content is cleaned, filtered, and organized into a structured format, enabling seamless integration with data analytics tools or machine learning pipelines. In contrast to traditional, time-consuming data collection methods, this solution automates web crawling and content analysis, significantly improving accuracy, scalability, and efficiency. Real-world applications include tracking market trends, monitoring cybersecurity threats, extracting academic research content, and gathering product intelligence. By streamlining the web data collection process and enabling real-time information access, the Web Scraper for Information Gathering enhances informed decision-making and supports a wide range of analytical and research-based initiatives across industries.

System Requirements and Specifications

1. Hardware Components

To effectively run the Web Scraper for Information Gathering, the following hardware specifications are recommended:

- **Processor:** Intel Core i5 or higher (or AMD Ryzen equivalent)
- **RAM:** Minimum 8 GB for smooth multitasking and data processing
- **Storage:** At least 256 GB of available storage space for storing scraped data and libraries
- **Display:** Standard monitor with 1024x768 resolution or higher
- **Input Devices:** Standard keyboard and mouse for user interaction

2. Software Tools and Versions Used

The project utilizes the following software components and libraries:

- **Operating System:** Compatible with Windows 10/11, macOS, and major Linux distributions
- **Programming Language:** Python 3.8 or above
- **Libraries and Tools:**
 - requests – For handling HTTP requests and fetching web content
 - BeautifulSoup – For parsing and extracting HTML data from webpages
 - pandas – For structuring and storing extracted data in tabular formats
 - textstat – For analyzing and assessing the readability of scraped textual content
 - afinn – For basic sentiment analysis of textual data
 - nmap – For performing simple network scanning tasks if required

3. Network and Other Dependencies

- **Internet Connectivity:** Required for accessing target websites, APIs, and downloading dependencies
- **Python Environment:** Must be properly configured with all necessary libraries installed via pip
- **Security and Compliance:** Ensure that the web scraper adheres to ethical scraping practices, including compliance with websites' robots.txt policies
- **Proxy Support:** Should be available for scraping websites with request limitations

4. Troubleshooting and Special Considerations

- **Blocked Requests:** Use appropriate headers, user-agent strings, and proxy rotation to avoid detection and blocking by websites
- **Data Storage:** Ensure sufficient disk space for storing large volumes of scraped data in CSV or database formats
- **Network Issues:** Verify internet connectivity and check proxy/firewall settings if errors occur during scraping

Conclusion

The **Web Scraper for Information Gathering** is a lightweight, efficient, and versatile tool designed to automate web data collection with minimal system requirements. Its compatibility across major platforms and support for essential Python libraries make it ideal for researchers and analysts. With proper setup and ethical usage, this scraper ensures reliable data extraction and contributes to faster, smarter decision-making.

ACTIVITY LOG FOR THE EIGHTH WEEK

WEEK -8: 24-03-2025 TO 30-03-2025

S.NO	DATE	DESCRIPTION	SIGN
1	25/03/2025 Monday	Conducted security analysis of password generation techniques to ensure strong encryption and randomness.	
2	26/03/2025 Tuesday	Implemented additional features such as password strength validation and clipboard functionality incidents.	
3	27/03/2025 Wednesday	Performed system testing, including edge case analysis, to ensure secure and reliable password generation.	
4	28/02/2025 Thursday	Reviewed compliance with cybersecurity standards (ISO 27001, NIST) and ensured cryptographic best practices.	
5	29/03/2025 Friday	Conducted performance optimization and finalized the user interface for improved usability.	
6	30/03/2025 Saturday	Prepared a detailed project report, presented findings, and discussed key learnings with mentors.	

Week 8: Advanced Cybersecurity Strategies and Final Project Review

Topic Covered: Final Implementation and Project Presentation

Description: During the eighth and final week of the internship, the primary focus was on completing, testing, and presenting the Web Scraper for Information Gathering project. This phase emphasized refining all functionalities, optimizing data extraction efficiency, and ensuring the reliability and ethical compliance of the scraping mechanisms. The week began with a comprehensive review of the web scraping pipeline, ensuring smooth handling of static and dynamic websites, structured data formatting, and consistent results across various sources.

Key improvements were made to the scraper, including better error handling, dynamic content processing using Selenium, and enhancements in text readability assessment using textstat and sentiment analysis with afinn. The system was tested against diverse web platforms, verifying its ability to extract meaningful information such as articles, product listings, and metadata. Edge case testing was conducted to evaluate scenarios like broken links, missing HTML tags, blocked access, or unexpected redirects. Strategies such as rotating headers, using proxies, and complying with robots.txt were implemented to prevent scraping blocks and ensure ethical data collection practices.

Security and legal compliance were prioritized by incorporating measures to respect website terms of service and privacy policies, aligning with frameworks like GDPR and ethical data handling principles. In addition, performance tuning was done to improve scraping speed, reduce memory usage, and ensure the scalability of the system for large-scale data collection.

A detailed project report was compiled, highlighting the project objectives, technical architecture, scraping techniques used, libraries and tools (like requests, BeautifulSoup, pandas, and nmap), challenges encountered, and future enhancement possibilities. The documentation emphasized real-world applications such as market trend analysis, academic research, and cybersecurity threat monitoring through automated data collection.

The final presentation included a live demo showcasing the scraper's capabilities—extracting structured data from a live website, cleaning it, and exporting it into a user-friendly format (CSV or JSON). The demonstration focused on the scraper's flexibility, support for different data types, and accuracy of extraction. Feedback from mentors and evaluators was positive, with

suggestions including integrating natural language processing for deeper insights, incorporating real-time monitoring, and building a dashboard for visualization.

This concluding phase reinforced skills in Python programming, automation, web technologies, and ethical data extraction. It deepened understanding in areas such as data preprocessing, real-time information gathering, and dealing with anti-scraping mechanisms. By the end of the internship, the web scraper was fully functional, efficient, and ready for deployment in various domains. The internship overall strengthened analytical thinking, scripting capabilities, and a responsible approach to data mining, paving the way for future advancements in information retrieval, data science, and cybersecurity.

OUTCOMES DESCRIPTION

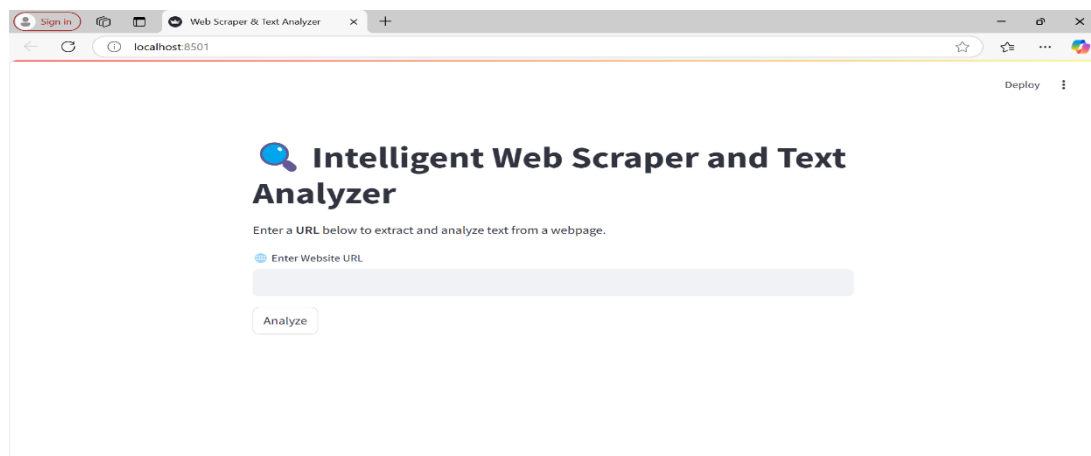
In the Cybersecurity Internship at Blackbucks, the overall outcomes I have learned include:

1. **Enhanced Threat Detection:** Gained expertise in identifying and analyzing cyber threats using tools like OpenVAS, CVE search engines, and SIEM solutions.
2. **Improved Incident Response Skills:** Developed the ability to create and implement incident response plans, minimizing damage and recovery time in case of security breaches.
3. **Stronger Vulnerability Management:** Learned how to assess and prioritize vulnerabilities using the Common Vulnerability Scoring System (CVSS) and industry best practices.
4. **Practical Hands-on Experience:** Worked with real-world cybersecurity tools such as Kali Linux, OpenVAS, and penetration testing frameworks, enhancing my technical skills.
5. **Better Compliance Understanding:** Understood security auditing practices and compliance standards such as ISO 27001, NIST, and GDPR, ensuring regulatory adherence.
6. **Proficiency in Penetration Testing:** Gained knowledge of ethical hacking methodologies and penetration testing techniques to identify and mitigate security weaknesses.
7. **Automated Security Implementation:** Explored security automation using SIEM tools and AI-driven security solutions to improve threat monitoring and response.
8. **Project-Based Learning:** Applied cybersecurity concepts in a final project, which involved conducting a security audit, performing penetration testing, and securing a system.
9. **Critical Thinking & Problem-Solving:** Developed analytical skills to assess risks, implement security measures, and respond to cyber threats effectively.
10. **Industry-Ready Skills:** Strengthened my knowledge in cybersecurity fundamentals, preparing me for real-world cybersecurity roles and certifications.

PHOTOS

```
1 import streamlit as st
2 import requests
3 from bs4 import BeautifulSoup
4 from afinn import Affin
5 import textstat
6 # Set up Streamlit UI
7 st.set_page_config(page_title="Web Scraper & Text Analyzer", layout="centered")
8 st.title("🔍 Intelligent Web Scraper and Text Analyzer")
9 st.markdown("Enter a **URL** below to extract and analyze text from a webpage.")
10 # Input field
11 url = st.text_input("🌐 Enter Website URL, ")
12 # Process on button click
13 if st.button("Analyze"):
14     if url.strip() == "":
15         st.warning("Please enter a valid URL.")
16     else:
17         try:
18             # Step 1: Fetch the webpage
19             response = requests.get(url, timeout=10)
20             soup = BeautifulSoup(response.text, 'html.parser')
21             # Step 2: Extract main paragraph/text
22             paragraphs = soup.find_all('p')
23             text = " ".join([p.get_text() for p in paragraphs])
24
25             if not text.strip():
26                 st.error("No readable content found on the page.")
27             else:
28                 # Step 3: Sentiment Analysis
29                 afinn = Affin()
30                 sentiment_score = afinn.score(text)
31                 sentiment = "Positive" if sentiment_score > 0 else "Negative" if sentiment_score < 0 else "Neutral"
32                 # Step 4: Readability
33                 flesch_score = textstat.flesch_reading_ease(text)
34                 # Output Results
35                 st.subheader("📊 Analysis Results")
36                 st.success(f"**Sentiment**": {sentiment} (Score: {sentiment_score:.2f})")
37                 st.info(f"**Readability (Flesch Reading Ease)**": {flesch_score:.2f}")
38         except Exception as e:
39             st.error(f"Error fetching or processing the URL: {str(e)}")
40
```

Fig 1: Code of the Web Scraper for Information Gathering



The screenshot shows a web browser window with the title "Web Scraper & Text Analyzer". The address bar shows "localhost:8501". The page has a white background with a blue magnifying glass icon and the title "Intelligent Web Scraper and Text Analyzer" in bold. Below the title, there is a subtitle "Enter a URL below to extract and analyze text from a webpage." and a text input field with a blue magnifying glass icon and the placeholder text "Enter Website URL". Below the input field is a button labeled "Analyze". In the top right corner, there is a "Deploy" button with a dropdown arrow.

Fig 2 : Web Scraper & Text Analyzer - Input Screen

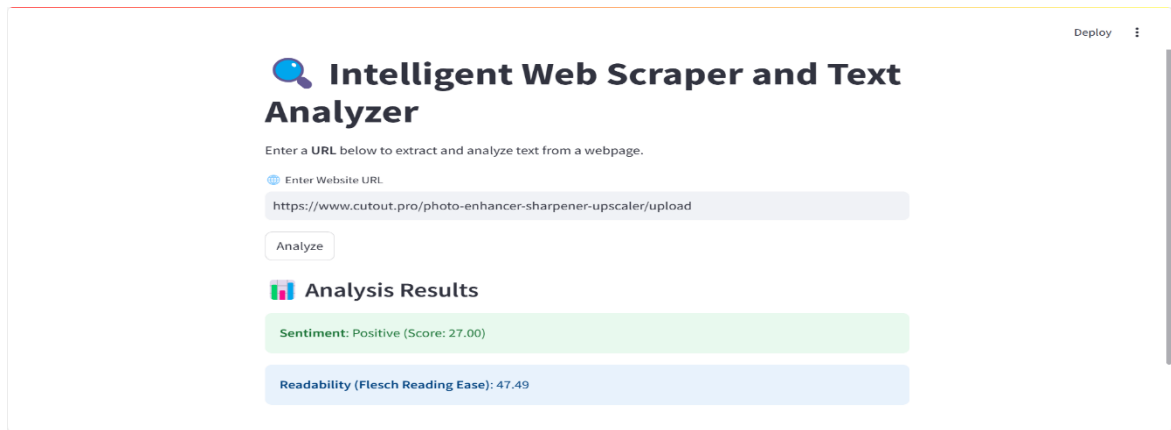


Fig 3 : Web Scraper & Text Analyzer - Output Screen

Student Self Evaluation of the Short-Term Internship

Student Name: T.Tejaswini

Roll Number: 21471A05L0

Term of Internship: From 03-02-2025 to 14-03-2025

Date of Evaluation:

Organization Name: BlackBucks Technologies Pvt. Ltd., Hyderabad

Name & Address of the Supervisor with Mobile Number:

K.V.Narasimha Reddy, Assistant Professor, Dept of CSE, Narasaraopeta Engineering College. Ph. No: 9177435922

Please rate your performance in the following areas:

Rating Scale: Letter grade of CGPA calculation to be provided

1	Oral communication					
2	Written communication	1	2	3	4	5
3	Initiative	1	2	3	4	5
4	Interaction with staff	1	2	3	4	5
5	Attitude	1	2	3	4	5
6	Dependability	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Planning 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	1	2	3	4	5
12	Productivity	1	2	3	4	5
13	Progress of learning	1	2	3	4	5
14	Adaptability to organization's culture/policies	1	2	3	4	5
15	OVERALL PERFORMANCE	1	2	3	4	5

Signature of the Student

Evaluation by the Supervisor of the Intern Organization

Student Name: Thumu Tejaswini

Roll Number: 21471A05L0

Term of Internship: From 03-02-2025 to 14-03-2025

Date of Evaluation:

Organization Name: BlackBucks Technologies Pvt. Ltd., Hyderabad

Name &Address of the Supervisor with Mobile Number:

K.V.Narasimha Reddy, Assistant Professor, Dept of CSE, Narasaraopeta Engineering College. Ph. No: 9177435922

Please rate Student's performance in the following areas:

Please note that your evaluation shall be done independent of the student's self- evaluation.

Rating Scale: Letter grade of CGPA calculation to be provided

1	Oral communication					
2	Written communication	1	2	3	4	5
3	Initiative	1	2	3	4	5
4	Interaction with staff	1	2	3	4	5
5	Attitude	1	2	3	4	5
6	Dependability	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Planning 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	1	2	3	4	5
12	Productivity	1	2	3	4	5
13	Progress of learning	1	2	3	4	5
14	Adaptability to organization's culture/policies	1	2	3	4	5
15	OVERALL PERFORMANCE	1	2	3	4	5

Signature of the Supervisor

