VISAKHA
INSTITUTE OF ENGINEERING & TECHNOLOGY
Approved by AICTE NEW DELHI
(Affiliated to JNTUGV, VIZIANAGARAM)
88th Division, Narava, GVMC, Visakhapatnam-530027
DIPLOMA | ENGINEERING | MANAGEMENT

NAAC
NATIONAL ASSESSENT AND ACCREDITATION COUNCIL
'A' GRADE

ISO
9001:2015

COLLEGE CODE
VSPT

VISAKHA INSTITUTE OF ENGINEERING &TECHNOLOGY

COMPUTER SCIENCE AND ENGINEERING

Name: THIVANANA BALA BHARATHI
Year: III BTECH
Semester: II
Roll No: 21NT1A0574
Internship: CYBER SECURITY

AN INTERNSHIP PROJECT REPORT
ON

Cyber security

Carried out by EXCELR

A report submitted in the partial full fill of the requirements under

internship project for the award of

BACHELOR OF TECHNOLOGY IN

COMPUTER SCIENCE ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

(2021 – 2025)

VISAKHA INSTITUTE OF ENGINEERING AND TECHNOLOGY

(Approved by AICTE New Delhi & Recognized by JNTUG, VIZINAGARAM)

88th Division, NARAVA, GVMC Visakhapatnam -530027

INTERNSHIP 6 WEEKS REPORT 2024

Andhra Pradesh State Council of Higher Education

(A Statutory Body of Govt. of Andhra Pradesh)

EXCELR

Raising Excellence

INTERNSHIP PERIOD

DURING 2024

VISAKHA INSTITUTE OF ENGINEERING & TECHNOLOGY
Approved by AICTE NEW DELHI
(Affiliated to JNTUGV, VIZIANAGARAM)
88th Division, Narava, GVMC, Visakhapatnam-530027
DIPLOMA | ENGINEERING | MANAGEMENT
NAAC NATIONAL ASSESSENT AND ACCREDITATION COUNCIL 'A' GRADE
ISO 9001:2015
COLLEGE CODE VSPT

CERTIFICATE OF INTERNSHIP

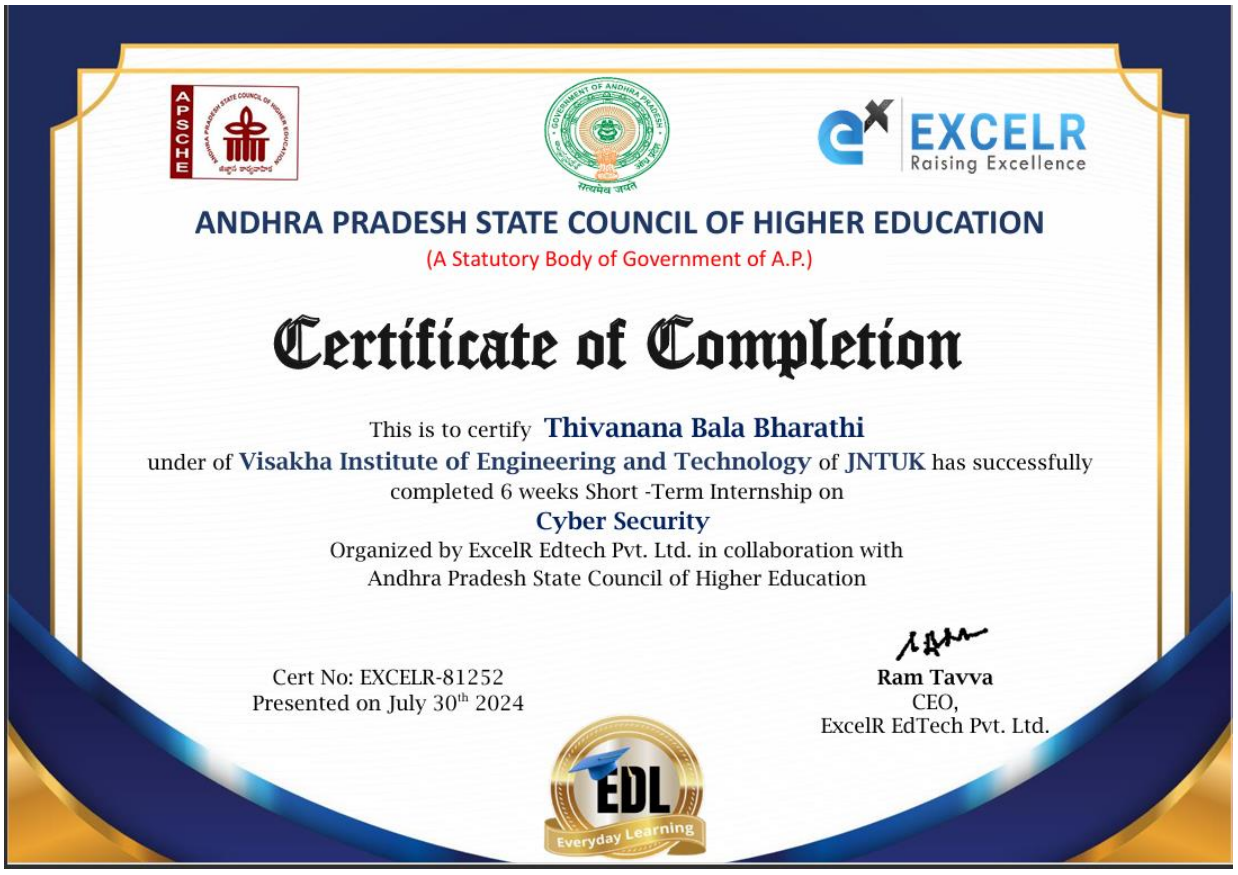
This is to certify that the "**Cyber Security**" submitted by NAME: THIVANANA BALA BHARATHI (Regd. No: 21NT1A0574) is work done by her/his and submitted during 2023 – 2024 for 6 WEEKS in this academic year, in partial fulfilment of the requirements for the award of the degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING, at EXCELR, APSCHE.

K. VIJAY
Department Internship Coordinator
Department of CSE

Dr. ASC.TEJASWINI KONE
Head the Department
Department of CSE

EXTERNAL SIGNATURE

CERTIFICATE FROM EXCELR ORGANIZATION



ANDHRA PRADESH STATE COUNCIL OF HIGHER EDUCATION

(A Statutory Body of Government of A.P.)

Certificate of Completion

This is to certify **Thivanana Bala Bharathi**
under of **Visakha Institute of Engineering and Technology** of **JNTUK** has successfully completed 6 weeks Short -Term Internship on

Cyber Security

Organized by ExcelR Edtech Pvt. Ltd. in collaboration with
Andhra Pradesh State Council of Higher Education

Cert No: EXCELR-81252
Presented on July 30th 2024

Ram Tavva
CEO,
ExcelR EdTech Pvt. Ltd.

DECLARATION

We hereby declare that work entitled “Internship Program 2024” submitted towards completion of summer training after 3rd year of BTech (CSE) At EXCELR comprises of our original work pursue under the guidance of DEPARTMENT OF CSE.

ACKNOWLEDGMENT

A project is a golden opportunity for learning and self-development. I consider myself very lucky and Honor to have so many wonderful people, lead me through, in completing of this project.

Our grateful thanks to DEPARTMENT OF CSE, in spite of being extraordinarily busy with their duties, took time out tohear, guide and keep us on the correct path. A humble ‘Thank you’.

We would like to thank Mrs. A.S.C Tejaswini Kone Madam Head Of The Department for all the help rendered. Thank you, Dear Madam we would like to thank you for your efforts and help provided to me to get such an excellent opportunity. Last but not the least there were so many who shared valuable information that helped in the successful completion of this project

THIVANANA BALA BHARATHI
21NT1A0574

CYBER SECURITY 6 WEEKS INTERNSHIP

EXCELR

ABSTRACT

Cyber Security internships provide a strategic entry point for aspiring professionals, offering an intensive introduction to the theoretical foundations and practical applications of information security.

Through participation in these programs, interns gain a comprehensive understanding of core cyber security principles. This includes the methodologies for securing systems against malware infiltration, phishing scams, and unauthorized access attempts. Furthermore, interns translate this knowledge into tangible action by engaging in projects that mirror real-world security challenges. This might involve tasks such as vulnerability assessments, participation in security incident response protocols, or even controlled ethical hacking simulations. These simulations serve the critical purpose of identifying and exploiting system vulnerabilities before malicious actors can leverage them.

Beyond technical expertise, cybersecurity internships foster the development of essential soft skills. Interns hone their problem-solving acumen by meticulously dissecting complex security issues and implementing effective solutions. Collaborative projects with experienced professionals strengthen communication skills, as interns learn to articulate technical concepts to a diverse range of audiences. Perhaps most significantly, interns gain a profound understanding of ethical hacking principles. This empowers them to adopt an attacker's mentality, proactively thwarting cyberattacks by anticipating and preempting their strategies.

Interns benefit from invaluable mentorship throughout the program. Seasoned cybersecurity professionals provide industry insights, share best practices, and offer guidance on navigating a dynamic and fulfilling career path in information security.

ACTIVITY LOG FOR THE 1st WEEK

S.no	Week	Day	Content
1	Week-1	Day-1	Introduction to Cyber security
2		Day-2	Introduction to Networking
3		Day-3	Python for Hacking
4		Day-4	Cryptographic Failures
5		Day-5	OWASP Category & API Hacking

1st WEEK REPORT

INTRODUCTION TO CYBER SECURITY

- Introduction to Cyber security: This topic serves as the gateway into the vast world of protecting digital systems and data from unauthorized access, cyberattacks, and breaches. It encompasses understanding the fundamental concepts of cyber security, such as threat landscape analysis, risk management, security policies, compliance frameworks, and various defense mechanisms like firewalls, antivirus software, intrusion detection systems, and encryption protocols.

- Introduction to Networking: Networking forms the backbone of modern technology infrastructure, enabling communication and data exchange between devices and systems. This topic delves into the basics of networking protocols, architectures, devices (routers, switches, modems), addressing schemes (IPv4, IPv6), network topologies, and the OSI (Open Systems Interconnection) model. Understanding networking fundamentals is crucial for comprehending how data flows across interconnected systems and for implementing secure network configurations.

- Python for Hacking: Python's versatility and extensive libraries make it a popular choice for cybersecurity professionals and hackers alike. This topic explores how Python can be used for various hacking techniques, including network scanning, vulnerability assessment, exploitation, password cracking, and writing custom hacking scripts/tools.

- Cryptographic Failures: Cryptography plays a pivotal role in safeguarding sensitive information by encrypting data to prevent unauthorized access or tampering. However, cryptographic failures can lead to severe security breaches and data compromises. This topic examines common cryptographic vulnerabilities and weaknesses, such as weak key generation, flawed implementations, side-channel attacks, cryptographic protocol flaws, and the impact of quantum computing on current encryption algorithms.

- OWASP Categories & API Hacking: The Open Web Application Security Project (OWASP) provides a framework for identifying and mitigating security risks in web applications. This topic focuses on OWASP's top security risks, including injection attacks, broken authentication, sensitive data exposure, XML External Entities (XXE), and security misconfigurations. Additionally, participants will explore the emerging threat landscape surrounding API (Application Programming Interface) security, covering topics such as API authentication, authorization, input validation, and common API vulnerabilities like Insecure Direct Object References (IDOR) and API rate limiting bypasses.

ACTIVITY LOG FOR THE 2nd WEEK

S.no	Week	Day	Content
1	Week-2	Day-1	FootPrinting and Reconnaissance
2		Day-2	Introduction to Linux
3		Day-3	Linux Installation
4		Day-4	Linux Bash Commands
5		Day-5	Linux Tools Meta Splloit, Salmap Categories

2nd WEEK REPORT

- **Footprinting and Reconnaissance:** Footprinting and reconnaissance are essential initial steps in the process of ethical hacking and penetration testing. This topic involves gathering information about a target system or network to identify potential vulnerabilities and weaknesses. It includes passive reconnaissance techniques like gathering publicly available information from sources such as social media, search engines, and company websites, as well as active reconnaissance techniques like network scanning, port scanning, and footprinting tools to map out the target's infrastructure and discover potential entry points for exploitation.

- Introduction to Linux: Linux is a widely used open-source operating system renowned for its stability, security, and flexibility. This topic provides an overview of Linux, including its history, architecture, distributions (such as Ubuntu, CentOS, and Debian), and the philosophy of the open-source community. Participants will gain an understanding of the Linux command-line interface (CLI) and basic system administration tasks, laying the groundwork for further exploration of Linux-based cybersecurity tools and techniques.

- Linux Installation: Installing Linux is often the first practical step for individuals interested in exploring the operating system or using it for cybersecurity purposes. This topic covers the process of installing Linux on various hardware platforms, including desktops, laptops, virtual machines, and cloud instances. Participants will learn about different installation methods, partitioning schemes, bootloader configuration, and post-installation tasks to ensure a smooth and functional Linux environment.

- Linux Bash Commands: The Bash shell (Bourne Again Shell) is the default command-line interpreter for most Linux distributions. This topic delves into the essential Bash commands and syntax for navigating the file system, managing files and directories, manipulating text, executing programs, and performing system administration tasks. Participants will learn how to leverage Bash scripting to automate repetitive tasks and streamline their workflow in Linux environments.

- Linux Tools: Metasploit: Metasploit is a powerful penetration testing framework that enables security professionals to discover, exploit, and validate vulnerabilities in target systems. This topic introduces participants to Metasploit's extensive set of modules and functionalities for network reconnaissance, vulnerability scanning, payload generation, exploit development, and post-exploitation activities.

- OWASP Categories: The Open Web Application Security Project (OWASP) provides a comprehensive list of security risks and vulnerabilities commonly found in web applications. This topic explores OWASP's Sensitive Data Exposure, Injection, Broken Authentication, and other categories, detailing the techniques used to exploit these vulnerabilities and the best practices for mitigating them. By understanding OWASP categories, security professionals can proactively identify and address security flaws in web applications to protect against data breaches and unauthorized access.

ACTIVITY LOG FOR THE 3rd WEEK

S.no	Week	Day	Content
1	Week-3	Day-1	Cloud Computing
2		Day-2	Cryptography in CEH
3		Day-3	Cloud Backing & SQL Injections
4		Day-4	System Hacking & Cryptography Hacking
5		Day-5	System Hacking Methodology & Network Defence Technology

3rd WEEK REPORT

- Cloud Computing: Cloud computing revolutionizes the way businesses and individuals access and manage computing resources over the internet. This topic provides an in-depth exploration of cloud computing models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Participants will learn about cloud deployment models (public, private, hybrid), cloud service providers (such as AWS, Azure, Google Cloud), cloud architecture principles, scalability, elasticity, virtualization technologies, and the benefits and challenges of adopting cloud computing in various industries.

- Cryptography in CEH: Cryptography is a cornerstone of cybersecurity, and its applications are fundamental to the Certified Ethical Hacker (CEH) certification. This topic delves into the role of cryptography in CEH, covering cryptographic algorithms (symmetric, asymmetric), encryption techniques, digital signatures, cryptographic protocols (SSL/TLS), hashing algorithms (MD5, SHA), steganography, and cryptographic attacks (brute force, cryptanalysis). Participants will learn how cryptography is used to secure data, communications, and authentication mechanisms in ethical hacking scenarios.

- Cloud Backup & SQL Injections: Cloud backup services provide an efficient and reliable way to store and protect data in cloud environments. This topic explores the principles of cloud backup solutions, including backup strategies, data retention policies, disaster recovery plans, encryption mechanisms, and the importance of data integrity and availability. Additionally, participants will learn about SQL injections, a prevalent web application security vulnerability, and how attackers exploit these vulnerabilities to execute malicious SQL queries and manipulate databases. Techniques for detecting, preventing, and mitigating SQL injection attacks in cloud-based applications will also be covered.

- System Hacking & Cryptography Hacking: System hacking involves unauthorized access and manipulation of computer systems and networks to exploit vulnerabilities and gain privileged access. This topic delves into the techniques and methodologies used by hackers to bypass security controls, escalate privileges, and compromise systems. Participants will learn about common system hacking techniques, including password cracking, privilege escalation, rootkits, backdoors, and malware propagation. Additionally, cryptography hacking explores

the vulnerabilities and weaknesses in cryptographic implementations and protocols, such as key management flaws, padding oracle attacks, and side-channel attacks. Participants will learn how attackers exploit cryptographic weaknesses to compromise confidentiality, integrity, and authentication mechanisms.

- System Hacking Methodology & Network Defense Technology: System hacking methodology provides a structured approach for ethical hackers and cybersecurity professionals to assess and mitigate security risks in computer systems and networks. This topic covers the various phases of the system hacking process, including reconnaissance, scanning, enumeration, gaining access, maintaining access, and covering tracks. Participants will learn about the tools, techniques, and best practices for conducting ethical system hacking assessments and improving overall system security. Additionally, network defense technology explores the tools and technologies used to defend against cyber threats and attacks in networked environments. This includes intrusion detection and prevention systems (IDS/IPS), firewalls, network segmentation, honeypots, security information and event management (SIEM) systems, and threat intelligence platforms. Participants will gain insights into proactive defense strategies and tactics for identifying, mitigating, and responding to network security incidents and breaches.

ACTIVITY LOG FOR THE 4th WEEK

S.no	Week	Day	Content
1	Week-4	Day-1	Social Engineering & Security Vulnerabilities
2		Day-2	Session Hijacking
3		Day-3	Python for Hacking
4		Day-4	SQL Injection
5		Day-5	Network Scanning Concepts

4th WEEK REPORT

- Social Engineering & Security Vulnerabilities: Social engineering is a psychological manipulation technique used by cyber attackers to trick individuals into divulging confidential information, performing actions, or compromising security controls. This topic delves into the various forms of social engineering attacks, including phishing, pretexting, baiting, tailgating, and spear phishing. Participants will explore real-world examples of social engineering attacks and the psychological principles behind them. Additionally, the topic examines security vulnerabilities exploited by social engineering attacks, such as human factors, lack of awareness, weak authentication mechanisms, and organizational culture issues. Participants will learn strategies for mitigating social engineering risks through security awareness training, policies, procedures, and technical controls.

- Cybersecurity with AI: Artificial Intelligence (AI) and machine learning are increasingly being integrated into cybersecurity solutions to enhance threat detection, response, and prediction capabilities. This topic explores the intersection of cybersecurity and AI, covering AI-driven security analytics, anomaly detection, behavior analysis, predictive modeling, and automated incident response. Participants will learn about AI-powered security tools and technologies used to detect and mitigate cyber threats, such as malware, phishing attacks, and insider threats. Additionally, ethical considerations and challenges associated with AI in cybersecurity, such as data privacy, bias, and adversarial attacks, will be discussed.

- Session Hijacking: Session hijacking is a type of cyber attack where an attacker intercepts and takes control of an authenticated session between a user and a web application or network service. This topic delves into the various methods used by attackers to hijack sessions, including session fixation, session prediction, session sniffing, and session replay attacks. Participants will learn about the security vulnerabilities and weaknesses that enable session hijacking, such as weak session management, insecure communication channels, and insufficient session token protection. Additionally, participants will explore countermeasures and best practices for preventing and detecting session hijacking attacks, including strong session management practices, encryption, and multi-factor authentication.

- SQL Injection: SQL injection is a common web application security vulnerability that allows attackers to manipulate SQL queries executed by a web application's backend database. This topic provides an in-depth exploration of SQL injection attacks, including SQL injection techniques such as union-based injection, error-based injection, blind injection, and out-of-band injection. Participants will learn about the security risks posed by SQL injection vulnerabilities, including unauthorized data access, data manipulation, and database compromise. Additionally, participants will explore techniques for identifying, preventing, and mitigating SQL injection vulnerabilities in web applications, including input validation, parameterized queries, and web application firewalls.

- Network Scanning Concepts: Network scanning is the process of identifying and mapping out devices, services, and vulnerabilities within a network infrastructure. This topic covers the fundamentals of network scanning, including active and passive scanning techniques, port scanning, host discovery, service enumeration, and vulnerability scanning. Participants will learn about popular network scanning tools and utilities, such as Nmap, Wireshark, and Nessus, and how they can be used to gather information about networked systems and identify potential security risks. Additionally, participants will explore best practices for conducting network scans ethically and responsibly, minimizing disruption to network operations, and interpreting scan results to prioritize remediation efforts.

ACTIVITY LOG FOR THE 5th WEEK

S.no	Week	Day	Content
1	Week-5	Day-1	Knowledge Sessions on GitHub
2		Day-2	Vulnerabilities of Authorization issue Cross-site

5th WEEK REPORT

- Knowledge Sessions on GitHub: GitHub has evolved beyond being just a version control system; it has become a central platform for collaboration, knowledge sharing, and project management in the software development community. This topic explores how GitHub can be leveraged to facilitate knowledge sessions, including workshops, code reviews, collaborative coding sessions, and knowledge sharing sessions. Participants will learn about GitHub's features and functionalities for organizing and sharing educational materials, such as repositories, wikis, issues, pull requests, and GitHub Pages. Additionally, participants will explore best practices for creating, managing, and participating in knowledge sessions on GitHub, including effective use of branching and versioning, code documentation, and community engagement.

- SOC Introduction: A Security Operations Center (SOC) is a centralized unit responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents in real-time. This topic provides a comprehensive introduction to SOC operations, covering the roles, functions, and workflows involved in operating a SOC. Participants will learn about the key components of a SOC, including people, processes, and technology, and how they work together to defend against cyber threats. Additionally, participants will explore the various types of SOC models, such as in-house SOC, managed SOC, and virtual SOC, and the factors to consider when establishing or outsourcing SOC capabilities. Furthermore, participants will delve into the SOC lifecycle, from incident detection and triage to incident response and recovery, as well as the tools and technologies commonly used in SOC environments, such as Security Information and Event Management (SIEM) systems, threat intelligence platforms, and incident response automation tools. Through case studies and practical examples, participants will gain insights into SOC operations and learn how to effectively detect, respond to, and mitigate cybersecurity threats in real-world scenarios.

ACTIVITY LOG FOR THE 6th WEEK

S.no	Week	Day	Content
1	Week-6	Day-1	Hands on practice Projects
2		Day-2	Oracle VM Virtual Manager

6th WEEK REPORT

- Hands-on Practice Projects: Hands-on practice projects provide invaluable opportunities for individuals to apply theoretical knowledge and develop practical skills in real-world scenarios. This topic explores the importance of hands-on learning and its role in reinforcing concepts, enhancing problem-solving abilities, and fostering experiential learning. Participants will learn about the benefits of hands-on practice projects, including improved retention of information, increased confidence, and the ability to troubleshoot and debug issues effectively. Additionally, participants will explore various types of hands-on practice projects, such as coding exercises, simulations, case studies, and lab assignments, and how they can be tailored to different learning objectives and skill levels. Through hands-on practice projects, participants can gain practical experience, build portfolios, and prepare for careers in fields such as software development, cybersecurity, data science, and more.

- Oracle VM Virtual Manager: Oracle VM Virtual Manager is a comprehensive virtualization management solution that enables organizations to deploy and manage virtualized environments efficiently. This topic provides an in-depth exploration of Oracle VM Virtual Manager, covering its features, capabilities, and deployment options. Participants will learn about the benefits of virtualization technology, including resource optimization, workload consolidation, and improved scalability and flexibility. Additionally, participants will explore the architecture of Oracle VM Virtual Manager, including components such as Oracle VM Server, Oracle VM Manager, and Oracle VM Agent, and how they work together to create and manage virtual machines. Through hands-on exercises and practical examples, participants will gain experience with installing, configuring, and managing virtualized environments using Oracle VM Virtual Manager, including tasks such as creating virtual machines, allocating resources, configuring networking, and monitoring performance.

PROJECT OVERVIEW

Understanding Cyber Threats: Exploring Nessus and Beyond

- This project delves into the ever-growing realm of cyber threats and explores the critical role of vulnerability scanning tools in fortifying your organization's security posture. We'll take a deep dive into Nessus, a popular and powerful vulnerability scanner, while also venturing beyond to explore other valuable tools in the cybersecurity landscape.

- The digital age has brought immense benefits, but it has also introduced a plethora of cyber threats that organizations must constantly be vigilant against. These threats can originate from various sources, including:

- Malicious Actors: Hackers, cybercriminals, and state-sponsored attackers actively seek vulnerabilities in systems to steal data, disrupt operations, or extort money.

- Botnets: Networks of compromised devices controlled by attackers can launch large-scale denial-of-service attacks or distribute malware.

- Social Engineering: Deceptive tactics like phishing emails or phone calls can trick users into divulging sensitive information or clicking malicious links.

- Insider Threats: Disgruntled employees, contractors, or third-party vendors with access to a system can pose a serious security risk.

- The consequences of a cyberattack can be devastating, leading to financial losses, reputational damage, data breaches, and operational disruptions.

- Vulnerability scanning is a crucial component of any cybersecurity strategy. It involves using automated tools to identify weaknesses in systems, networks, and applications. These weaknesses, often referred to as vulnerabilities, can be exploited by attackers to gain unauthorized access or compromise a system's integrity.

Regular vulnerability scanning offers several key benefits:

- Proactive Security: By identifying vulnerabilities before attackers do, organizations can prioritize patching and remediation efforts, significantly reducing their attack surface.

- Improved Security Posture: Vulnerability scanning provides a comprehensive view of an organization's security posture, enabling them to allocate resources effectively and focus on the most critical risks.

- Compliance with Regulations: Many regulations mandate regular vulnerability scanning to ensure organizations are taking adequate steps to protect sensitive data.

Nessus: A Leading Vulnerability Scanner

- Nessus, developed by Tenable, is a widely recognized and powerful vulnerability scanner. It offers a comprehensive suite of features, including:

- Extensive Vulnerability Database: Nessus boasts a vast database of vulnerabilities, regularly updated to reflect the latest threats.

- Multiple Scanning Techniques: Nessus employs various scanning techniques, including network-based scanning, agent-based scanning, and credentialed scanning, to provide a deeper level of analysis.

- Reporting and Remediation: Nessus generates detailed reports that clearly identify vulnerabilities, their severity levels, and recommended remediation steps.

- Integration Capabilities: Nessus integrates seamlessly with other security tools, streamlining security workflows and enhancing overall threat detection and response capabilities.

Beyond Nessus: Exploring Other Vulnerability Scanners

- While Nessus is a dominant player, there are other noteworthy vulnerability scanners available, each with its own strengths and use cases. Here are a few examples:

- OpenVAS: A free and open-source vulnerability scanner offering a wide range of features and extensive community support.

- Avira Free Antivirus: While primarily an antivirus solution, Avira offers basic vulnerability scanning capabilities for personal use.

- Qualys VMDR: A cloud-based vulnerability management platform that provides comprehensive scanning, prioritization, and remediation functionalities.

- Rapid7 Nexpose: A robust vulnerability scanner that offers asset discovery, vulnerability assessment, and risk scoring capabilities.

Choosing the Right Vulnerability Scanner

- The selection of the most suitable vulnerability scanner depends on various factors, including:

- Organization Size and Needs: Larger organizations with complex IT environments may require a more comprehensive solution like Nessus or Qualys VMDR, while smaller businesses might find OpenVAS or a basic antivirus solution sufficient.

- Budget: OpenVAS offers a free option, while commercial solutions like Nessus typically require paid subscriptions.

- Ease of Use: Some scanners are more user-friendly than others, and the level of technical expertise available within the organization should be considered.

- Integration Capabilities: Compatibility with existing security tools can significantly enhance efficiency.

Project Activities

- This project will involve a series of activities to gain a thorough understanding of vulnerability scanning and its role in cybersecurity:

- 1. In-Depth Exploration of Nessus: This will involve a deep dive into Nessus's features, functionalities, and user interface. Tutorials, documentation, and hands-on practice will be utilized to gain practical experience with the tool.

- 2. Comparative Analysis of Vulnerability Scanners: Research and evaluate other prominent vulnerability scanners like OpenVAS, Qualys VMDR, and Rapid7 Nexpose. Compare their features, pricing, and suitability for different organizational needs.

- 3. Scenario-Based Vulnerability Scanning: Simulate real-world scenarios by conducting vulnerability scans on test environments. This will involve identifying vulnerabilities.

Conclusion

Understanding cyber threats is crucial in today's interconnected digital landscape, where organizations and individuals are constantly at risk of cyber attacks. From data breaches to ransomware infections, cyber threats pose significant risks to data security, privacy, and business continuity. Therefore, it is essential to have a comprehensive understanding of the various types of cyber threats and the tools and techniques available to mitigate them.

One powerful tool in the cybersecurity arsenal is vulnerability scanning software, such as Nessus and beyond. These scanning tools play a critical role in identifying weaknesses and vulnerabilities within systems, networks, and applications before malicious actors can exploit them. By scanning for known vulnerabilities, misconfigurations, and security weaknesses, organizations can proactively address security issues and strengthen their cyber defenses.

Nessus, for instance, is a widely used vulnerability scanning tool known for its comprehensive coverage of vulnerabilities across a wide range of assets, including servers, workstations, network devices, and web applications. It provides automated vulnerability assessment capabilities, enabling organizations to quickly identify and prioritize security risks based on severity and impact. Additionally, Nessus offers advanced features such as compliance auditing, configuration assessment, and malware detection, empowering organizations to maintain compliance with industry standards and regulations and safeguard against emerging threats.

Beyond Nessus, there are other scanning tools and techniques that organizations can leverage to enhance their cybersecurity posture. These tools may include open-source solutions, commercial products, or custom-built scripts tailored to specific environments and requirements. Some examples include Qualys, OpenVAS, Rapid7, and Nmap.

However, it is essential to recognize that vulnerability scanning is just one aspect of a comprehensive cybersecurity strategy. To effectively defend against cyber threats, organizations must adopt a multi-layered approach that combines vulnerability management with other security measures such as patch management, network segmentation, access

control, intrusion detection, and incident response.

In conclusion, understanding cyber threats and employing effective scanning tools like Nessus and beyond are essential components of a proactive cybersecurity strategy. By continuously monitoring for vulnerabilities and weaknesses, organizations can reduce the likelihood of successful cyber attacks and minimize the impact of security breaches on their operations and reputation.

Internal & External Evaluation for Semester Internship

Objectives:

- Explore career alternatives prior to graduation.
- To assess interests and abilities in the field of study.
- To develop communication, interpersonal and other critical skills in the future job.
- To acquire additional skills required for the world of work.
- To acquire employment contacts leading directly to a full-time job following graduation from college.

Assessment Model:

- There shall be both internal evaluation and external evaluation
- The Faculty Guide assigned is in-charge of the learning activities of the students and for the comprehensive and continuous assessment of the students.
- The assessment is to be conducted for 200 marks. Internal Evaluation for 50 marks and External Evaluation for 150 marks
- The number of credits assigned is 12. Later the marks shall be converted into grades and grade points to include finally in the SGPA and CGPA.
- The weightings for Internal Evaluation shall be:
    - Activity Log 10 marks
    - Internship Evaluation 30 marks
    - Oral Presentation 10 marks

- The weightings for External Evaluation shall be:
    - Internship Evaluation 100 marks
    - Viva-Voice 50 marks

- The External Evaluation shall be conducted by an Evaluation Committee comprising of the Principal, Faculty Guide, Internal Expert and External Expert nominated by the affiliating University. The Evaluation Committee shall also consider the grading given by the Supervisor of the Intern Organization.

- Activity Log is the record of the day-to-day activities. The Activity Log is assessed on an individual basis, thus allowing for individual members within groups to be assessed this way.

- While evaluating the student's Activity Log, the following shall be considered -

  a. The individual student's effort and commitment.

  b. The originality and quality of the work produced by the individual

  c. The student's integration and co-operation with the work assigned.

  d. The completeness of the Activity Log.

- The Internship Evaluation shall include the following components and based on Weekly Reports and Outcomes Description

  a. Description of the Work Environment.

  b. Real Time Technical Skills acquired.

  c. Managerial Skills acquired.

  d. Improvement of Communication Skills.

  e. Team Dynamics

  f. Technological Developments recorded.

INTERNAL ASSESSMENT STATEMENT

Name of the Student:

Program of Study:

Year of Study:

Group:

Register No/H.T. No:

Name of the College:

University:

SL.NO	Evaluation criterion	Maximum Marks	Marks Awarded
1	Activity Log	10	
2	Internship Evaluation	30	
3	Oral Presentation	10	
	GRAND TOTAL	50	

Date: **Signature of the Faculty Guide**

EXTERNAL ASSESSMENT STATEMENT

Name of the Student:

Program of Study:

Year of Study:

Group:

Register No/H.T. No:

Name of the College:

University:

SL.NO	Evaluation criterion	Maximum Marks	Marks Awarded
1	Internship Evaluation	80	
2	For the grading giving by the supervisor of the Intern Organization	20	
3	Viva-Voce	50	
	TOTAL	150	
GRAND TOTAL (EXT.50M + INT.100M)		**200**	

Signature of the Faculty Guide

Signature of the Internal Expert

Signature of the External Expert

Signature of the Principal with Seal