**RIPHAH INTERNATIONAL UNIVERSITY**

|  |
| --- |
|  |

**Faculty of Computing**

**FINAL YEAR PROJECT PROPOSAL & PLAN**

**Phish Net - Phishing Simulation Toolkit**

**Project Team**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Full Name of Student** | **SAP Id** | **Program** | **Contact Number** | **Email Address** |
| Ali Kayani | 37539 | BSCY | 0334-8141448 | 37539@students.riphah.edu.pk |
| Umar Waqar | 27668 | BSCY | 0312-0204073 | 27668@students.riphah.edu.pk |
|  |  |  |  |  |

**Dr. Jawaid Iqbal**

Asst. Professor

**Phish Net – Phishing Simulation Toolkit**

**Change Record**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Author(s)** | **Version** | **Date** | **Notes** | **Supervisor’s Signature** |
| Ali Kayani & Umar Waqar | 1.0 | Feb 21st, 25 | Original Draft |  |
| Ali Kayani & Umar Waqar | 2.0 | Feb 27th, 25 | Changes Based on Feedback From Supervisor |  |
| Ali Kayani & Umar Waqar | 2.0 | Feb 27th, 25 | Changes Based on Feedback From Faculty |  |
|  |  |  | Added Project Plan |  |
|  |  |  | Changes Based on Feedback From Supervisor |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Project Proposal**

**Phish Net – Phishing Simulation Toolkit:**

**Introduction and Background**: Phish Net is the need of the hour for the Pakistan’s Technology Industry. Having not much input in the Cyber Security domain and especially the Phishing dilemma. This project would be the revolution the industry starves. With numerous phishing attempts being made from High-level VIP victims, to private companies, public institutions, military organizations and education & healthcare institutions.

In today’s digital era, cyber threats are evolving at an alarming rate, yet Pakistan’s technology sector has limited resources dedicated to tackling one of the most pressing issues phishing attacks. These attacks don’t just target individuals; they compromise VIPs, private companies, government institutions, military organizations, and even hospitals and universities. Despite this growing threat, there’s a significant gap in cybersecurity education and industry precautions/mitigations across the country.

Right now, most businesses rely on foreign cybersecurity solutions, leaving them dependent on international providers and vulnerable to external policies. Without a homegrown solution, Pakistan remains exposed to financial losses, data breaches, and operational disruptions caused by cybercriminals.

**Existing Systems**: Phishing is the major cyber security threat to be reported inside and outside of Pakistan. Targeting individuals, private companies, and multiple genres of public and private institutions. The National Cyber Security Policy 2021 has highlighted the urgent need for improved cybersecurity measures. Yet most organizations still rely on foreign tools and haphazard sluggish measures that couldn’t stand against the rapidly advancing threat landscape.

After careful market analysis we studied that there is literally no domestic solution tailored to our technological landscape. Additionally, international security awareness platforms like KnowBe4 and Cofense help in training but not to our work force’ caliber. The country also lacks in threat intelligence system for effective threat intel perception/study and analytics plus reporting. Also, there’s a need for meticulously constructed phishing campaign modules and the simulations need more perfection for a more seamless and realistic experience. This demonstrates the current state in cybersecurity and helps identify gaps that our project will address.

Furthermore, there is a need to introduce behavior analytics for better understanding the employe’s thinking/actions. The lack of a real-time phishing database would better guide institution executives in enforcing stringent actions and policies. There is also the need for Automated Phishing to greatly improve timely campaign initiations, the user practical experience and overall planning leverage in teaching by example and practices.

**Problem Statement:**Lack of a home-grown phishing system with real-time analytical database for threat perception. No profound reporting and alerting system/mechanism while having the need to inculcate email notifications and analytical techniques for a streamlined and profound information study. Need for meticulously constructed campaign modules for hard to differ emails and attacks. While having the need for realistic phishing simulations. The desire for a comprehensive cyber test range. Lacking the grant of customizations and control the target audience would like to make it and exercise as they implement in their environments. Detailed and comprehensive analytics with proper charts, graphs and other analytical components. Furthermore, there are a lot of other small perks offered by each phishing platform but all lacking in one or the other. Thus, needing to add each of these tools’ perks in an evolved tool with a touch of refinement added to it. Lack of abidance with international standards and regulations and no knowledge of everyday cyber practices. Need to make our institutions internationally recognizable.

**Objectives**: Our system aims to achieve the following milestones:

* Train and educate employees through interactive phishing simulations and awareness programs
* Teach through practical experiences and brain triggering exercises
* Introducing lab environments for safer learning grounds for the target audience
* Help organizations comply with international standards and regulations
* Informing the target audience of recent cyber security norms and practices
* Establish a real-time threat intelligence database for better analytics and risk detection
* Improve incident response strategies and minimize financial losses caused by phishing
* Provide a cyber test range
* Provide a proper cyber framework to the Pakistani market
* Reducing the foreign dependence for tools and services
* Provide user friendly, meticulously crafted and customizable system

**Proposed Solution**: We plan to develop a Phishing Simulation Toolkit. The system design, architecture and functionalities are properly explained via diagrams and charts. Deliberately in the appendices attached to this document. For better project understanding and evaluation. Through deliberately made phishing campaigns, template engine, automated simulations and realistic simulation experience – we would help train the work force through teach by experience motto. While also maintaining a local attack database and a detail-oriented analytics and reporting mechanisms Moreover, incorporating convenient notification mechanism and introducing multiple minor quality-of-life improvements. Not only that our system will also introduce customization ability to help each firm make a bespoke system perfect for their work environment.

**Methodology**: In the development of our project, we will be utilizing **React** for the frontend due to its component-based architecture, which ensures scalability, reusability, and efficient state management. For the backend, we will integrate **Express.js** with **PostgreSQL**, providing a secure, reliable, and high-performance database solution that supports complex queries and data integrity. **Node.js** will act as an intermediary for handling API requests efficiently, ensuring smooth communication between the frontend and backend.

Our approach follows an **Agile Development Model**, incorporating iterative development cycles, continuous integration, and user feedback to refine the system. This method allows flexibility in adapting to changes and ensures incremental improvements throughout the project lifecycle.

The APIs to be integrated in the project include:

* **Gophish API** – Facilitates phishing campaign automation, email tracking, and real-time user response monitoring.
* **Google reCAPTCHA API** – Enhances authentication security by preventing automated bot attacks.
* **Email Validation API** – Ensures user email legitimacy before launching phishing campaigns.
* **IP Geolocation API** – Helps in tracking phishing engagement patterns based on geographic data.

All these components will correlate seamlessly: the frontend will interact with the backend through RESTful APIs, which in turn will fetch or store data in PostgreSQL. Gophish APIs will handle campaign execution, while security measures like reCAPTCHA will be integrated at authentication points. The combination of these technologies will ensure that PhishNet is a robust, scalable, and efficient phishing simulation toolkit.

**Implementation Plan**: Keeping into consideration the nature of our project, the following modules and milestones will be undertaken to achieve a timely production of our product. Definite timelines are set with minor room for leeway to tackle unforeseen hurdles along the way:

* **Milestone #1** - Project Requirements – Planning – **March 15-17, 2025** (3 days)
* **Milestone #2** – Resource Allocation & Responsibilities – Planning – **March 18, 2025** (1 day)
* **Milestone #3** - Project Discussions – Planning – **March 19 - August 19, 2025** (5 months) – Faculty FYP Meetings
* **Milestone #4** – User Profiles – GUI – **August 20, 2025** (2 days)
* **Milestone #5** – Dashboard – GUI – **August 22, 2025** (3 days)
* **Milestone #6** – Login & Registration – GUI – **August 25, 2025** (3 days)
* **Milestone #7** – Registration Mechanism – Processing – **August 28, 2025** (2 days)
* **Milestone #8** – Functionalities – Functions – **August 30, 2025** (5 days)
* **Milestone #9** – Functionality Pages – Pages + Functions – **September 4, 2025** (5 days)
* **Milestone #10** – Functionality Sub Pages – Sub Pages – **September 9, 2025** (4 days)
* **Milestone #11** – User Management System – Development – **September 13, 2025** (3 days)
* **Milestone #12** – Notification Mechanism – Development – **September 16, 2025** (3 days)
* **Milestone #13** – Template Engine – Development – **September 19, 2025** (3 days)
* **Milestone #14** – Email Builder – Development – **September 22, 2025** (3 days)
* **Milestone #15** – Campaign Manager – Development – **September 25, 2025** (4 days)
* **Milestone #16** – Phishing Simulations – Cyber Development – **September 29, 2025** (5 days)
* **Milestone #17** – Analytics – Development + Back End – **October 4, 2025** (5 days)
* **Milestone #18** – Reporting Mechanism – Development + Back End – **October 9, 2025** (5 days)
* **Milestone #19** – Database – Back End Development – **October 14, 2025** (4 days)
* **Milestone #20** – Back End Linkage – Back End Development – **October 18, 2025** (5 days)
* **Milestone #21** – APIs – Back End Development – **October 23, 2025** (4 days)
* **Milestone #22** – Cybersecurity Features – Cyber – **October 27, 2025** (5 days)
* **Milestone #23** – Evaluation – Result – **November 1, 2025** (3 days)
* **Milestone #24** – Testing – QC – **November 4, 2025** (5 days)
* **Milestone #25** – Debugging – QA – **November 9, 2025** (5 days)
* **Milestone #26** – Project Defense – Formalities – **November 14, 2025** (2 days)
* **Milestone #27** – Implementation – Formalities – **November 16, 2025** (3 days)
* **Milestone #28** – Improvement – QA – **November 19, 2025** (4 days)
* **Milestone #29** – Documentation – Formalities – **November 23, 2025** (5 days)

PhishNet is being developed as a **phishing simulation and cyber awareness tool** for **corporate organizations** to train employees on cybersecurity threats. The stakeholders include **businesses, IT security teams, employees, and compliance regulators**, ensuring a secure and effective security awareness solution.

**Evaluation Plan**: Our project will be evaluated through rigorous test runs, incorporating both automated and manual **Quality Assurance (QA) and Quality Control (QC)** mechanisms. The evaluation process will focus on functionality, security, usability, and performance to ensure that PhishNet meets industry standards and user expectations.

Key evaluation methods include:

* **Automated Testing:** Unit tests, integration tests, and end-to-end tests using tools like Jest and Cypress to validate system performance.
* **Manual Testing:** QA teams will simulate real-world scenarios to identify potential bugs, UI/UX issues, and security vulnerabilities.
* **End-User Experience Monitoring:** Collecting real-time feedback from users regarding usability, effectiveness, and interface intuitiveness.
* **Self-Simulation:** The development team will conduct phishing simulations from an end-user perspective to evaluate campaign effectiveness and response accuracy.

**Success Criteria:**

* **Accuracy & Effectiveness:** The system should successfully execute phishing simulations, track user interactions, and provide meaningful insights through reports.
* **User Engagement & Learning Curve:** A user-friendly interface ensuring smooth navigation and ease of use for both administrators and trainees.
* **Security & Reliability:** The system must ensure secure authentication, data protection, and resistance against unauthorized access.
* **Scalability & Performance:** The platform should handle multiple concurrent phishing campaigns efficiently without performance degradation.
* **Compliance & Ethical Use:** Adherence to cybersecurity policies and ethical boundaries in phishing simulations.

**Project Scope/ Expected Outcomes**: After the successful development of PhishNet, we aim to provide the market with a deliberate and realistic phishing simulation system that offers meticulously constructed customizable phishing campaigns. This toolkit will simulate real-world phishing attacks while ensuring an interactive and immersive user experience for end users. Additionally, PhishNet will ensure compliance with international cybersecurity regulations and help organizations enhance their cybersecurity awareness programs.

**Major Modules:**

* **Planning & Architecture Design:**

Meticulously planning the overall development agenda. Determining the key milestones and the finer details of each one of them. While also mapping the interconnection of each of the modules and the minutest of functionalities in every one of them.

* **Authentication & User Management:**

Secure login and registration system with role-based access control (RBAC) to ensure authorized access. Integration with Google reCAPTCHA for bot prevention and multi-factor authentication (MFA) for enhanced security. Furthermore, giving them user based functionalities.

* **Users’ Dashboards:**

Developing the in-depth user dashboards for all key user profiles with each with their role based functionalities that later divided to their functionality pages and later on broken into subsequent functionality operations and sub pages.

* **Phishing Campaign Manager:**

Allows administrators to create, customize, and schedule phishing campaigns. Includes email template management, campaign tracking, and automation for efficient campaign execution.

* **Notifications & Emails:**

Proper notification and system be enforced while having a meticulous email builder going hand in hand with the phishing email template engine for forwarding the phishing attempts.

* **Reports & Analytics Portal:**

Generates detailed phishing campaign reports with real-time insights. Provides metrics on user interactions, email open rates, link clicks, and form submissions, helping organizations assess employee security awareness.

* **Database & Backend:**

Secure and seamless integration of the front and back end with detailed and reliable databases for each key storage functionality. After being ensured through our agile testing and Quality Assurance practices. While using certain APIs for the back-end connectivity.

* **Testing & Evaluation:**

Evaluation through rigorous test runs, incorporating both automated and manual **Quality Assurance (QA) and Quality Control (QC)** mechanisms. The evaluation process will focus on functionality, security, usability, and performance to ensure that PhishNet meets industry standards and user expectations. Via Automated Testings, Manual Testings, End User Experience, Self Simulations. Unit Integration.

* **Debugging & Improvements:**

Rectifying our project’s setbacks and patching the issues via refinements and debugging runs. While also introducing quality of life improvements to the overall project’s working and everyday experience.

**Conclusion and Future Work**: In a nut shell, this project will provide a comprehensive and realistic phishing campaign and simulation system, that will provide a localized threat database for attack study and a meticulous template engine for customization and adaptability for every use case. Not only that this system would teach by example and practical demonstrations. While also giving a state-of-the-art user management system integrated into it along with proper reporting and analytical mechanisms implemented for optimal performance. All inside of a thoughtful and user-friendly architecture. Although there is a lot of work to be produced by this system but I think that the introduction of Artificial intelligence would further enhance its effectiveness. While the room for a detailed education system also feels to be available in the system

**Appendices**: In the attached documents you will come across a detailed functionality document providing a detailed insight to each aspect of the system along with their relevant operations. Moreover, the ERD and Class diagram will help guide the faculty about the overall project structure, architecture, inter dependencies, operational flow, components and their characteristics.

**List of Faculty Proposed Changes**

**Phis Net – Phishing Simulation Toolkit**

**Supervisor’s Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |
| --- | --- | --- |
| **Proposed Change** | **Proposed By** | **Supervisor’s Decision** |
|  | Name of Faculty Member(s) who proposed this change | Approved/Disapproved and/or Comments |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Project Plan**

**Work Breakdown Structure:** A work breakdown structure (WBS) is deliverable based decomposition of project scope. The WBS includes 100% of the work defined by the project scope and captures all deliverables – internal, external, interim – in terms of the work to be completed, including project management.

Sample WBS:

1. **Title Page:**
   * **Project Title:** Phish Net – Phishing Simulation Toolkit
   * **Author:** Ali Kayani & Umar Waqar
   * **University Name:** Riphah International University, Islamabad
   * **Department:** Department of Cyber Security
   * **Date:** March 10, 2025
2. **Abstract:**

**Summary of the Project:** Phish Net is the need of the hour for the Pakistan’s Technology Industry. Having not much input in the Cyber Security domain and especially the Phishing dilemma. This project would be the revolution the industry starves. With numerous phishing attempts being made from High-level VIP victims, to private companies, public institutions, military organizations and education & healthcare institutions.

In today’s digital age, cyber threats are evolving at an alarming rate, yet Pakistan’s technology sector has limited resources dedicated to tackling one of the most pressing issues—phishing attacks. These attacks don’t just target individuals; they compromise VIPs, private companies, government institutions, military organizations, and even hospitals and universities. Despite this growing threat, there’s a significant gap in cybersecurity education and industry precautions/mitigations across the country.

Right now, most businesses rely on foreign cybersecurity solutions, leaving them dependent on international providers and vulnerable to external policies. Without a homegrown solution, Pakistan remains exposed to financial losses, data breaches, and operational disruptions caused by cybercriminals.

1. **Acknowledgments:**
   * Express heartfelt gratitude to the project supervisor, Professor Jawaid Iqbal, for their invaluable guidance and unwavering support throughout the research journey. Acknowledge her expertise, which played a pivotal role in shaping the direction and success of the project.
   * Extend thanks to colleagues and friends for their encouragement and assistance during the course of the project.
2. **Table of Contents:**
   * **Introduction**
     + 1.1 Background and Context
     + 1.2 Problem Statement
     + 1.3 Objectives and Scope
   * **Literature Review**
   * **Methodology**
     + 3.1 Research Design
     + 3.2 Tools and Technologies
   * **System Design**
     + 4.1 Architecture and Design
   * **Implementation**
     + 5.1 Implementation Details
   * **Testing and Evaluation**
     + 6.1 Testing Methods
     + 6.2 Results and Evaluation
   * **Results and Discussion**
     + 7.1 Presentation of Results
     + 7.2 Discussion of Findings
   * **Conclusion**
     + 8.1 Summary
     + 8.2 Achievements and Limitations
   * **Future Work**
   * **References**
   * **Appendices**
3. **Introduction:**
   * **Background and Context:** Phish Net is the need of the hour for the Pakistan’s Technology Industry. Having not much input in the Cyber Security domain and especially the Phishing dilemma. This project would be the revolution the industry starves. With numerous phishing attempts being made from High-level VIP victims, to private companies, public institutions, military organizations and education & healthcare institutions.

In today’s digital age, cyber threats are evolving at an alarming rate, yet Pakistan’s technology sector has limited resources dedicated to tackling one of the most pressing issues phishing attacks. These attacks don’t just target individuals; they compromise VIPs, private companies, government institutions, military organizations, and even hospitals and universities. Despite this growing threat, there’s a significant gap in cybersecurity education and industry precautions/mitigations across the country.

Right now, most businesses rely on foreign cybersecurity solutions, leaving them dependent on international providers and vulnerable to external policies. Without a homegrown solution, Pakistan remains exposed to financial losses, data breaches, and operational disruptions caused by cybercriminals

* **Problem Statement:** The project would eliminate the cyber threats targeted at companies w.r.t **Phishing Techniques** and lack of knowledge. Construct a domestic Phishing Simulation and Cyber Awareness Solution. Improvement in Cyber Measures, bridge the knowledge gap in our industry. Real-time phishing monitoring. Insider threat surveillance, Phishing Database for company’s self-evaluation and improvement tracking. While utilizing it for future Incident Response Plan and Mitigation Strategies. Through Training Modules, Cyber Test Range and Evaluation Mechanisms.
* **Objectives and Scope:** Our system aims to train and educate employees through interactive phishing simulations and awareness programs, enhancing their cybersecurity knowledge through practical experiences and brain-triggering exercises. By introducing lab environments, we provide a safer learning ground for the target audience, ensuring hands-on exposure to real-world cyber threats. Additionally, our platform helps organizations comply with international standards and regulations while keeping users informed about the latest cybersecurity norms and practices. To strengthen security measures, we aim to establish a real-time threat intelligence database for better analytics and risk detection, improving incident response strategies and minimizing financial losses caused by phishing attacks. Our system also includes a cyber test range and a structured cyber framework tailored to the Pakistani market, reducing dependence on foreign tools and services. Designed with user-friendliness in mind, our meticulously crafted and customizable system ensures accessibility and adaptability for organizations of all sizes. PhishNet is a phishing simulation and cyber awareness tool designed for corporate organizations to train employees on cybersecurity threats. It offers interactive simulations, real-time analytics, compliance tracking, and a cyber test range to enhance security awareness. Key features include a user management system, notification mechanisms, an email template engine, and a campaign manager for targeted training. With advanced threat intelligence, phishing simulations, and reporting, PhishNet helps businesses strengthen cybersecurity resilience. The stakeholders include organizations, IT security teams, employees, and compliance regulators, ensuring a secure, scalable, and locally tailored solution.

1. **Existing Systems:**
   * **Review of Existing Systems:** After careful market analysis we studied that there is literally no domestic solution tailored to our technological landscape. Additionally, international security awareness platforms like KnowBe4 and Cofense help in training but not to our work force’ caliber. The country also lacks in threat intelligence system for effective threat intel perception/study and analytics plus reporting. Also, there’s a need for meticulously constructed phishing campaign modules and the simulations need more perfection for a more seamless and realistic experience. This demonstrates the current state in cybersecurity and helps identify gaps that our project will address. Furthermore, there is a need to introduce behavior analytics for better understanding the employe’s thinking/actions. The lack of a real-time phishing database would better guide institution executives in enforcing stringent actions and policies. There is also the need for Automated Phishing to greatly improve timely campaign initiations, the user practical experience and overall planning leverage in teaching by example and practices.
2. **Methodology:**
   * **Research Design:** Our research follows a structured approach, focusing on the evaluation of phishing tools like SafeTitan, Cofense, KnowBe4, and similar platforms to assess their architecture, user experience, and effectiveness. Through a comparative analysis, we identified gaps and opportunities for improvement, aiming to create a more interactive and scalable solution. Insights from market research and industry trends drive the development of a customizable phishing awareness platform designed specifically for human detection and cybersecurity training.
   * **Tools and Technologies:** The project will leverage modern web technologies and cybersecurity tools to create an effective phishing simulation environment. The frontend will be developed using React with Vite for fast rendering and modularity. The backend will use Node.js integrated with Gophish APIs to simulate phishing campaigns. PostgreSQL will serve as the database for managing user interactions and campaign data. For security analytics, machine learning algorithms such as Random Forest and Decision Trees may be incorporated to analyze phishing response trends. Additional security features will include reCAPTCHA, JWT authentication, and role-based access control (RBAC). Jest and Cypress will be used for automated testing to ensure code quality and security compliance.
3. **System Design:**
   * **Architecture and Design:** Illustrate the architectural framework of your machine learning-based cyber security system. Utilize diagrams or flowcharts to enhance comprehension.
4. **Implementation:**
   * **Implementation Details:** The project will be implemented in phases:
   * **Phase 1 – Setup & Core Modules:**

• Configure development environment, version control, and CI/CD pipelines.  
 • Implement user authentication (login/registration) and API connectivity.

* + **Phase 2 – Dashboard & Campaign Manager:**

• Develop the admin dashboard, including campaign management and reporting modules.  
• Create dynamic email template management and scheduling features.

* + **Phase 3 – User & Organization Management:**

• Integrate user management, role-based access, and organizational segmentation.  
• Build settings and preferences modules for enhanced user customization.

* + **Phase 4 – Testing, Evaluation & Refinement:**

• Conduct unit, integration, and end-to-end testing across all modules.  
• Optimize performance based on test results and user feedback.

* + **Phase 5 – Documentation & Deployment:**

• Finalize the end – user (customer) and technical detailed documentation.  
• Deploy the toolkit in a staging environment for pilot testing before production rollout.

1. **Testing and Evaluation:**
   * **Testing Methods:** The effectiveness of PhishNet’s phishing simulations will be evaluated using multiple testing methods, including unit testing, integration testing, and user acceptance testing. Automated tests using Jest and Cypress will ensure that each component functions correctly. Simulated phishing campaigns will be executed within controlled environments to measure user responses, interaction rates, and system performance.
   * **Results and Evaluation:** Performance will be analyzed by collecting real-time metrics such as email open rates, link clicks, credential submissions, and response times. The system’s ability to detect anomalies, such as repeated phishing attempts from the same user group, will be evaluated. A comparative analysis against industry benchmarks (e.g., KnowBe4) will validate PhishNet’s effectiveness. The overall impact on cybersecurity awareness will be measured through post-campaign surveys and behavioral analytics. Success will be defined by increased phishing detection rates and enhanced security practices among end-users.
2. **Results and Discussion:**
   * **Presentation of Results:** Showcasing the outcomes of our project, highlighting successful instances of perfect phishing simulations ran on the targeted users, without any discrimination or suspicion by the end user.
   * **Discussion of Findings:** The results from PhishNet's phishing simulations reveal key insights into user behavior and organizational cybersecurity readiness. The data collected from simulated campaigns demonstrate common phishing susceptibility patterns, highlighting specific vulnerabilities within different user groups. Trends indicate that users are more likely to click on phishing links in emails that appear urgent or impersonate internal communications. The effectiveness of training interventions was also evaluated, showing that repeated exposure to phishing simulations significantly improves employee recognition of suspicious emails. Additionally, the integration of behavioral analytics allowed for deeper insights into response patterns. Organizations using PhishNet observed measurable improvements in cybersecurity awareness, with decreased click-through rates on phishing emails over multiple simulation rounds. The real-time threat intelligence gathered from campaigns provided critical feedback for enhancing organizational security policies. These findings underscore the importance of continuous security awareness programs and demonstrate the necessity for adaptive phishing simulations in mitigating cyber threats.
3. **Conclusion:**
   * **Summary:** The PhishNet Phishing Simulator Toolkit successfully addresses the growing need for cybersecurity awareness by providing organizations with a dynamic and realistic phishing simulation platform. Through automated phishing campaigns, real-time analytics, and behavioral tracking, the toolkit enhances security training and strengthens defenses against social engineering attacks. Our findings demonstrate that repeated exposure to phishing simulations improves user awareness and reduces susceptibility to attacks. The integration of customizable templates, automated reporting, and organization-specific configurations ensures that PhishNet can be tailored to various industries and security frameworks. The project has bridged the gap between traditional training methods and modern, data-driven security awareness solutions.
   * **Achievements and Limitations:** One of the major accomplishments of PhishNet is its ability to provide a scalable, open-source phishing simulation framework that aligns with real-world attack methodologies. The system's modular design allows seamless integration into existing cybersecurity infrastructures, while its automated reporting and analytics enable organizations to measure the effectiveness of their security training. The use of behavioral analytics further enhances security awareness by identifying patterns in user responses. However, the project does have some limitations. The effectiveness of phishing simulations is dependent on user engagement, and some employees may not take training seriously unless mandated by their organization. Additionally, while PhishNet provides a realistic simulation environment, it does not replicate the full complexity of sophisticated phishing campaigns conducted by advanced threat actors. Future enhancements will focus on integrating AI-driven phishing detection, real-time threat intelligence feeds, and deeper behavioral analysis to further refine the toolkit’s capabilities.
4. **Future Work:**
   * **Suggestions for Future Enhancements:** Following iterations if made could greatly enhance the overall system’s performance and its practical effectiveness. Though, the timelines for those additions would not be attained within time and grossly naïve to be considered achievable.
5. **Appendices:**
   * **Additional Material:** Including supplementary materials, such as Class Diagram, ERD Diagram, UML Diagram, Data Flow Diagram, GAP Analysis and Comparison Table or additional information supporting the main content of the report.

**Roles & Responsibility Matrix:**

The purpose of roles & responsibility matrix is to identify who will do what.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **WBS #** | **WBS Deliverable** | **Activity #** | **Activity to Complete the Deliverable** | **Duration**  **(# of Days)** | **Responsible Team Member(s) & Role(s)** |
| 1 | Architecture Design | 1 | Designing ERD & Class Diagrams | 3 | Ali Kayani & Umar Waqar |
| 2 | Methodology Development | 2 | Pondering on the approach | 5 | Ali Kayani & Umar Waqar |
| 3 | Project Planning | 3 | Developing the work roadmap | 2 | Ali Kayani & Umar Waqar |
| 4 | Login Page | 4 | Constructing Login Page | 3 | Ali Kayani & Umar Waqar |
| 4 | Registration Page | 5 | Constructing Registration Page | 1 | Ali Kayani & Umar Waqar |
| 4 | Registration Mechanism | 6 | Database & Page Linkage + Proc. | 2 | Ali Kayani & Umar Waqar |
| 5 | User Management System | 7 | Employee Handling Interface | 3 | Ali Kayani & Umar Waqar |
| 5 | User Profiles | 8 | Creating profile variations along with their privileges | 2 | Ali Kayani & Umar Waqar |
| 5 | Dashboards | 9 | Constructing Landing Page | 3 | Ali Kayani & Umar Waqar |
| 5 | Functionalities | 10 | Developing key dashboard functionalities | 5 | Ali Kayani & Umar Waqar |
| 5 | Functionality Pages | 11 | Further developing their subsequent redirections | 5 | Ali Kayani & Umar Waqar |
| 6 | Notification Mechanism | 12 | Notification System + Email Integration | 3 | Ali Kayani & Umar Waqar |
| 7 | Template Engine | 13 | Email Building Mechanism | 3 | Ali Kayani & Umar Waqar |
| 8 | Email Builder | 14 | Phishing Emails | 3 | Ali Kayani & Umar Waqar |
| 9 | Campaign Manager | 15 | Building the Campaign Mastermind | 2 | Ali Kayani & Umar Waqar |
| 9 | Campaign Tracker | 16 | Creating Tracking Mechanism | 3 | Ali Kayani & Umar Waqar |
| 10 | Phishing Simulations | 17 | End Product Experiences | 7 | Ali Kayani & Umar Waqar |
| 11 | Analytics | 18 | Data Charts and Numbers | 5 | Ali Kayani & Umar Waqar |
| 12 | Reporting | 19 | Alerting & feedbacks | 5 | Ali Kayani & Umar Waqar |
| 13 | User Evaluation & Enlistment | 20 | User Marking System & Enrollment Mechanism | 4 | Ali Kayani & Umar Waqar |
| 14 | Database | 21 | Developing the required Databases | 10 | Ali Kayani & Umar Waqar |
| 15 | Back End Linkage | 22 | Linking front and back end | 5 | Ali Kayani & Umar Waqar |
| 15 | APIs & Codes | 23 | Integrating APIS & Codes | 3 | Umar Waqar |
| 16 | Cyber Features | 24 | Implementing other Cyber features for security etc. | 3 | Umar Waqar |
| 17 | Evaluation | 25 | Product qualifying its commitments | 6 | Ali Kayani |
| 18 | Testing | 26 | Running Test Runs on the product | 10 | Ali Kayani |
| 19 | Debugging | 27 | Sorting Product Issues | 10 | Ali Kayani & Umar Waqar |
| 20 | Implementation | 28 | Implementing the system in real life environment | 4 | Ali Kayani & Umar Waqar |
| 21 | Interface Improvements | 29 | Improving the system GUI | 10 | Ali Kayani & Umar Waqar |
| 22 | Quality of Life Improvements | 30 | Making minor efficiency improvements | 10 | Ali Kayani & Umar Waqar |
| 23 | Documentation | 31 | Developing the Paper Work | 10 | Ali Kayani & Umar Waqar |

**Approval**

|  |  |
| --- | --- |
| **Project Supervisor** | |
| **Comments\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

|  |  |
| --- | --- |
| **Project Coordinator** | |
| **Comments\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |