Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

BAGONG PILIPINAS

NIDSToKnow: A Web-Based Network Intrusion Detection System (NIDS) Learning and Simulation Platform Using Cowrie Honeypot

Proponents:

Danlie Ken B. Gregory

Hanz Hendrick R. Lacsi

Angel Bless M. Mendoza

INTRODUCTION

The increasing prevalence of global cyber threats underscores the need for cybersecurity education at all levels, including within Higher Education Institutions (HEIs), as it is essential for building a more informed and secure digital society, as noted by Maraj et al. (2021). Vikram (2024) of Kanan.co reported that the United States of America (USA), United Kingdom (UK), and Australia topped the list of the best countries to study cybersecurity. The International Business Machines Corporation (IBM) in the USA has targeted 3 million individuals, including college students, by developing the Cyber Campus, a comprehensive Software-as-a-Service (SaaS) platform that simulates real-world networks and cyberattacks for training, testing, and research purposes (Koehler et al., 2024).

In contrast, inadequate cybersecurity education in developing regions, especially in Southeast Asia, creates a skills gap that hinders effective defense against rising digital security threats (Lavrova, 2025). According to the Global Cybersecurity Index (2023), the Philippines remains at the 61st rank out of 182 countries. While in the National Cybersecurity Index (2023), it dropped to 48th from 43rd out of 195 countries. Xiao et al. (2023) emphasized the cybersecurity challenges faced by HEIs in the new era, including a lack of innovation in embracing rapid technological iteration, lack of immersion or practicality over theory, lack of interaction or focus on a student-centered approach and collaboration, and lack of comprehensiveness, meaning HEIs are too dependent on teaching materials and therefore need to provide new learning methods.

The Philippine government has taken steps to address cybersecurity threats through national initiatives such as the Cybercrime Prevention Act of 2012 or Republic Act 10175 (Republic of the Philippines, 2012) and the National Cybersecurity Plan 2022 (Department of Information and Communications Technology [DICT], 2022). Recognizing the growing demand for skilled professionals, the Commission on Higher Education (CHED) has endorsed efforts to integrate cybersecurity education into the curricula of State Universities and Colleges (SUCs) and private institutions. especially the Information Technology (IT) majors. In support of this, CHED collaborated with the DICT to implement capacity-building programs such as the webinars, seminars, and training aimed at producing qualified cybersecurity professionals (De Ramos & Esponilla, 2022).

However, as De Ramos and Esponilla (2022) point out, the current implementation of cybersecurity education in Philippine HEIs remains limited. While programs and partnerships have been introduced, many institutions still face gaps in infrastructure, skilled faculty, and hands-on training environments. These challenges hinder the development of comprehensive, practice-based learning experiences that can prepare students to respond to real-world cyber threats.

One of the main topics in IT courses is Network Intrusion Detection Systems (NIDS), which are important to study in schools to help protect digital networks. NIDS is used to find and stop possible cyberattacks, so it’s a key subject for students who want to work in cybersecurity. But simulating cybersecurity including NIDS through hands-on activities can be hard because trying real attacks can harm the network (Song et al., 2022) and hard to understand since attacks usually come from the Linux environment (Jain & Singh, 2011). This makes it difficult for students to see how NIDS works in real situations. Even so, learning the ideas behind NIDS is still very important, because it helps students understand how to build and manage safe networks in real life while also learning how to handle risks properly (Jain & Waoo, 2023).

Meanwhile, Cowrie is a honeypot system that simulates fake Secure Shell (SSH) and Teletype network (Telnet) services used to trap hackers, creating a safe environment that looks like a real server. It allows attackers to interact with it, trying to log in or run commands in the Linux operating system, without causing harm to actual systems (S & Chakkaravarthy, 2023). Cowrie records detailed logs of these activities, which helps in understanding how attackers behave and what methods they use (Carrillo-Mondejar et al., 2024). For example, it often captures brute-force attempts and commands like uname -a that check system information (Setianto et al., 2021).

To address these limitations in cybersecurity education, particularly the lack of practical, hands-on experiences in understanding real-world network threats, this study’s goal is to NIDSToKnow, a web-based network intrusion detection system (NIDS) learning and simulation platform using cowrie honeypot.. This platform aims to enhance learning by simulating three NIDS methods: signature-based, anomaly-based, and hybrid detection. By integrating Cowrie, a honeypot system that can mimic SSH and Telnet services, the project creates a safe and interactive environment where IT students can observe and analyze simulated attacks typically originating from Linux-based systems. This simulation-based approach not only mitigates risks associated with live testing but also enables a deeper understanding of NIDS concepts, bridging the gap between theoretical learning and real-world cybersecurity applications.

General Objectives

This study aims to create a web-based platform entitled "NIDSToKnow: A Web-Based Network Intrusion Detection System (NIDS) Learning and Simulation Platform Using Cowrie Honeypot."

Specific Objectives:

1. To develop a web-based Network Intrusion Detection System (NIDS) Learning and Simulation Platform Using Cowrie Honeypot with the following features:

    1.1. Theoretical and practical activities focused on the three NIDS three methods:

        1.1.1. Signature-based

        1.1.2. Anomaly-based

        1.1.3. Hybrid

    1.2. Simulated attacks through the Cowrie honeypot to detect and examine malicious activities.

    1.3. Interactive learning modules covering fundamental and advanced NIDS.

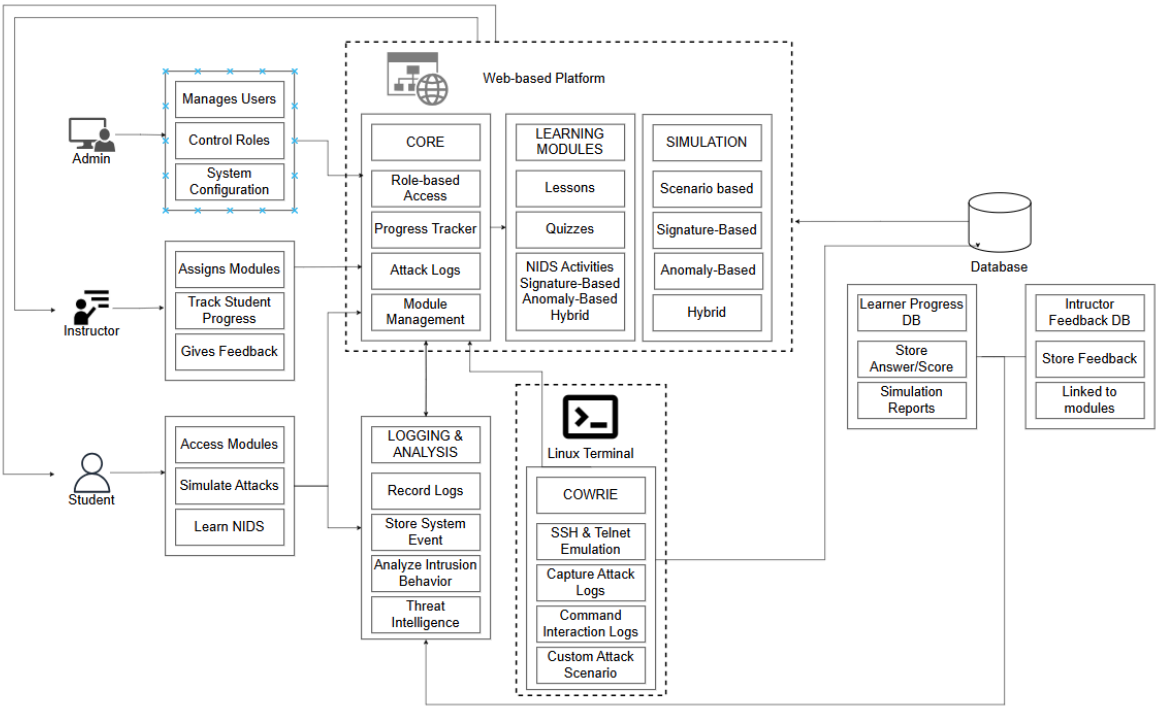
    1.4. Progress tracker to monitor learner advancement through the modules.

2. To implement role-based access control for learners, instructors, and administrators to manage access to platform features based on user roles.

3. To provide instructors with tools to assign modules, monitor learner engagement, and give personalized feedback.

4. To assess the usability, engagement, and educational effectiveness of the platform through pilot testing with IT learners and feedback from educators.

Conceptual Framework



The conceptual framework of NIDSToKnow, a cybersecurity learning and simulation platform, comprises five core components: the Linux Terminal and Attack Scenario, the Cowrie Honeypot, the Database, the NIDS Engine, and the Web-Based Interface. These components are integrated to simulate attacks, capture data, perform intrusion detection analysis, and facilitate learning in a practical educational context. The system is designed to offer a safe and interactive environment to study cyber threats through honeypot technology and three specific NIDS detection methods.

The process begins with the *Linux Terminal and Attack Scenario*, which serves as the origin point for simulated attacks. Here, learners can set up custom attack scenarios targeting SSH or Telnet protocols to simulate real-world malicious activities.

These actions are then directed to the *Cowrie Honeypot*, an interactive system that captures logs of attacker interactions—recording crucial details such as IP addresses, usernames, passwords, commands, statuses, and timestamps. By doing so, a safe and detailed environment is given.

The captured data is stored and organized in a centralized *Database*. It manages learner progress data, instructor feedback, and activity logs, all crucial for driving the educational component of the platform.

Next in line is the *NIDS Engine*, which analyses the data in the Database using 3 intrusion detection methods *Signature, Anomaly, and Hybrid.* The analyzed results are then passed onto the web interface.

The *Web-Based Interface* provides a user-friendly environment for authorized users (Admin, Instructor, and Students) to interact with the system. Students access learning modules and progress metrics, while instructors can track student activities and progress and give feedback, and administrators manage the system.

Together, these components form a cohesive, learning platform and ensure effective training in NIDS and practical cybersecurity skills. This holistic design enhances students' resilience to network systems and future threats.

Scope and Limitation of the Study

This study focuses on the development and implementation of a web-based Network Intrusion Detection System (NIDS) Learning and Simulation Platform using the Cowrie Honeypot. The platform is designed specifically for IT instructors and learners who are studying network security. It will cover the three core methods of Network Intrusion Detection: signature-based, anomaly-based, and hybrid methods. The platform will use the Cowrie Honeypot in a Linux terminal to simulate fake attacks, specifically targeting the SSH and Telnet protocols. This will allow users to engage in hands-on activities and analyze these real-world attack scenarios. The system is accessible via desktop or laptop devices. The platform will also feature interactive learning modules and progress tracking to enhance the learning experience.

The platform will only use the Cowrie Honeypot in a Linux terminal to simulate fake attacks based on SSH and Telnet protocols, allowing users to analyze real-world scenarios. It will not simulate attacks based on other protocols, such as HTTP, FTP, or DDoS attacks. The system is not accessible via mobile devices (smartphones or tablets). Furthermore, while the platform allows for the analysis of simulated attacks, it does not provide real-time detection or mitigation of actual cyber threats. The system's performance may also be affected by high network traffic or multiple concurrent users, potentially impacting the user experience.

Literature Review

Cyberattacks

The increasing number and complexity of cyberattacks show how important NIDS are in protecting digital infrastructure (Eniodunmo & Al-Aqtash, 2023). Advanced machine learning techniques, like self-normalizing neural networks (SNNs), have shown promise in improving NIDS by allowing them to detect intrusions accurately and in real-time (Alawida et al., 2024). Eniodunmo and Al-Aqtash (2023) showed that SNNs work better than traditional methods like K-Nearest Neighbors and Support Vector Machines in detecting cyber threats, showing how NIDS are evolving to meet modern needs (Back et al., 2018). As cyber threats become more varied, such as phishing and denial of service attacks, it is essential for NIDS to use both spatial and temporal analytics to identify attack patterns

(Alawida et al., 2024)

Cyberattacks also play an important role in modern warfare by targeting critical infrastructure and disrupting supply chains (Korda & Dapaah, 2023). This highlights the need for advanced NIDS with the ability to predict and detect attacks, as pointed out by Korda and Dapaah (2023) and Yeboah-Ofori et al. (2021). The rise of Internet of Things (IoT) devices adds more challenges to cybersecurity, as these devices are often targeted in distributed denial of service attacks (Gudimetla & Kotha, 2024). To help with this, artificial intelligence, especially machine learning, provides useful tools for analyzing large amounts of network data to find threats (Gudimetla & Kotha, 2024). As networks grow and cyber threats become more complex, AI-powered NIDS are essential for keeping cybersecurity systems strong and responsive in both civilian and military areas (Yeboah-Ofori et al., 2021).

Cybersecurity

As highlighted by Azizan et al. (2021), the continuous evolution of cyber threats has made it necessary to improve the way networks are protected. One of the widely used tools in the field of cybersecurity is the network intrusion detection system, which monitors network traffic to detect suspicious activities in real time. Integrating machine learning techniques into such systems has proven effective, as algorithms like Support Vector Machines and Random Forests can identify abnormal patterns with higher accuracy (Ibraheem, 2022). To further refine detection, Abdulhammed et al. (2019) emphasized the importance of dimensionality reduction techniques, such as Principal Component Analysis, which reduce noise and help the system focus on the most significant indicators of intrusion.

Deep learning has also become a significant part of strengthening cybersecurity measures. For instance, Laghrissi et al. (2021) found that Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) models performed well in recognizing complex intrusion patterns, especially in large and high-dimensional datasets. Hybrid approaches, which combine traditional machine learning with deep learning, have shown promise in achieving more generalized and adaptive detection systems (Farooq et al., 2023). However, the dynamic nature of cyber threats remains a challenge. Duan et al. (2020) argue that continuous learning is critical because systems must be able to update and retrain on new data to maintain effectiveness over time.

Network Intrusion Detection System

Building NIDS is very important for keeping networks safe in different organizations. NIDS consists of three methods which are signature-based, anomaly-based, and hybrid detection. Signature-based looks for unknown patterns like or “signatures” in network traffic. Anomaly-based watches for anything unusual compared to normal behavior. The hybrid method combines both signature-based and anomaly-based methods to be more accurate. These systems usually have three main parts: sensors to watch the network traffic, servers to analyze the data, and consoles to manage everything (Sayed & Taha, 2023). Thanks to new technology like artificial intelligence (AI) and machine learning (ML), NIDS are now much better at finding threats. For example, ML methods such as decision trees, naïve Bayes, and support vector machines help the system learn from past data and spot attacks in the future (Jain & Waoo, 2023). These tools make it easier for NIDS to detect both common and new types of cyberattacks while making fewer mistakes (Vanin et al., 2022).

Even with these improvements, using NIDS can still be hard because hackers are always coming up with new tricks. Old methods that look for specific, known attack patterns (called signature-based detection) don’t work well against brand-new attacks (Banik & Peña, 2015). Because of this, experts are now focusing on finding unusual behavior in the network, which might show a threat even if it hasn’t been seen before (Sivanantham et al., 2023). Some systems also use data mining to find hidden patterns that could mean someone is trying to break in (Sivanantham et al., 2023). Newer approaches like deep learning, especially with convolutional neural networks, and smart ways of picking which data to focus on, help make these systems more accurate and quicker to react (Qi et al., 2019; Ho et al., 2021).

Cowrie Honeypot

Cowrie is a medium-interaction honeypot designed to capture malicious behavior, offering insights into how attackers operate without compromising real systems. By emulating vulnerable SSH and Telnet services, it deceives intruders into revealing their methods, which are then recorded for analysis. Morić et al. (2024) highlight its growing use in both professional and academic environments, where it helps analyze intrusion techniques and supports hands-on cybersecurity training. Data collected from Cowrie can improve machine learning models used in intrusion detection, allowing these systems to identify and respond to threats more effectively (Tinnaluri & Shaik, 2024).

In addition, Cowrie’s open-source nature encourages ongoing development and integration with threat intelligence platforms. According to Naik et al. (2020), the honeypot has successfully captured a variety of attacks, from brute-force logins to the deployment of malicious scripts. This adaptability makes Cowrie an invaluable tool for real-time threat detection and analysis, as it continuously evolves with emerging attack methods. Studies have also shown that the data collected by Cowrie, when analyzed, can provide key insights into attacker behavior and techniques, which can then be used to improve cybersecurity models and predict future threats (Mispriatin et al., 2022). Furthermore, Cowrie's integration with other security systems, such as Intrusion Prevention Systems ( ), allows for a more proactive defense mechanism, where the system can not only capture attacks but also mitigate them in real-time (Susanti et al., 2022).

Theoretical Activities

The concept of theoretical activities in education acts an important role in deepening students' understanding and applying knowledge in real-world contexts. Al-Balushi and Martin-Hansen (2019) highlight how active learning, such as discussions and debates, enhances students' understanding of scientific models. Their research emphasizes the influence of Vygotsky's frameworks in shaping classroom interactions to improve students' conceptual understanding. In vocational education, Ferm (2021) shows that students bridge the gap between theory and practice by applying theoretical knowledge in real-world situations, which boosts their confidence in practical skills.

The integration of theoretical activities also supports the development of specific skills, such as in mathematics. Ledezma et al. (2022) argue that using theoretical tools in mathematical tasks helps students connect theory with practice. In a similar vein, Thanh (2020) demonstrates how self-assessment and reflection enhance independent learning, improving students' self-esteem and engagement. The versatility of theoretical frameworks across different educational contexts is further illustrated by Helmer (2021), who uses humorous instructions in driving education to facilitate learning, showcasing the broad application of these activities.

Practical Activities

Practical activities in education are vital for experiential learning, allowing students to apply theoretical knowledge to real-world contexts. Neves et al. (2017) emphasize the effectiveness of home-based versus laboratory-based practical activities in physiology, noting that such experiences help students grasp complex theoretical content. This engagement not only enhances comprehension but also fosters interest, crucial for academic and professional success. Similarly, Bernhardsson et al. (2017) explore work-integrated learning (WIL), where they describe how the integration of practical activities with theoretical learning helps develop the necessary skills for professional success, encouraging students to become proactive and engaged learners.

Experiential learning further serves a key function in motivating students and developing essential skills. Project-based learning significantly boosts student interest and motivation, as it allows them to see the direct application of their learning (Tsoy et al., 2023). Additionally, Vauderwange et al. (2019) suggest that integrating research projects into university curricula improves knowledge transfer, making the learning process more relevant to real-world contexts. Mäkelä et al. (2018) advocate for collaborative, practice-oriented learning to address educational challenges. Repeated testing of practical tasks leads to better performance and retention, reinforcing that practical activities are foundational to effective learning (Begley et al., 2013).

Learning Modules

Learning modules are essential tools in education, helping to structure content and engage students in meaningful learning. Research by Masaguni et al. (2023) highlights the effectiveness of science modules based on project-based learning (PBL) for middle school students. Their study found that these modules increased both student activity and learning outcomes, especially in understanding substances like addictive and additive chemicals.

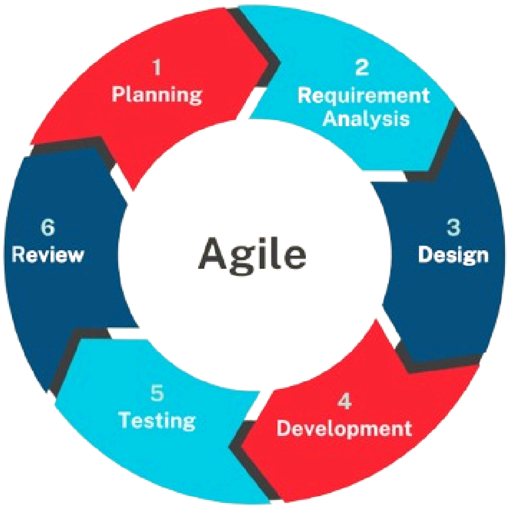
Learning modules should encourage intrinsic motivation, not just focus on assessments (Croft, 2018). Additionally, studies by Az-Zahra et al. (2023) stress the importance of well-structured modules to support student-centered activities, which align with modern educational trends that encourage more active student involvement.

In professional development, learning modules are also a major part e in transforming educators' practices. Holmgren et al. (2019) found that teachers who engaged in structured learning modules were more reflective and willing to adapt their teaching methods to better suit adult learners. In the e-learning realm, Lee and Sen (2018) emphasized the need to design modules that match students' learning styles, ensuring greater success in digital education. Suratnu (2023) also supports the use of the Analyze, Design, Develop, Implement, and Evaluate (ADDIE) model in module design, which ensures that educational content is both thorough and user-friendly. Furthermore, Project-based learning modules can develop creativity and problem-solving skills, contributing to holistic learning in the classroom (Cruz & Rivera, 2022).

METHODOLOGY

The proponents utilized the Agile Software Development Methodology in developing the web-based platform. Agile Methodology consists of Planning, Requirement Analysis, Design, Development, Testing, and Review. Most of the platforms use this model because it doesn't focus on prototypes. It can be presented once it is completed. Agile methodology represents a transformative approach to software development that prioritizes adaptability, collaboration and customer- relationship (Safwan, 2013).

Agile Software Development Model



The proponents implemented the Agile Software Development Model for NIDStoKnow to guide the creation of the web-based platform. This approach emphasizes flexibility, collaboration, and continuous improvement, allowing the development team to adapt swiftly to changing requirements and stakeholder feedback. By employing Agile, the proponents can iteratively develop and enhance NIDStoKnow, incorporating changes and adjusting features based on suggestions and comments from the IT learners, teachers, and adviser.

Planning

After identifying the issues related to their major in Network Administration, the proponents will begin with an initial conceptualization of the solution in NIDStoKnow. Once NIDStoKnow and its concept is approved, proponents will have a close coordination with their adviser to ensure a thorough understanding of the system's goals and objectives. The proponents will then proceed to outline a clear, structured plan, breaking down the necessary steps for the development of the system. To organize the project efficiently, they will establish a detailed timeline using a Gantt Chart, which will allocate specific resources and set milestones for each phase of development.

The first stage of the project involves gathering essential data and information to analyze the requirements. After this, the proponents will start to design the system's interfaces. During the second semester of their third year, the proponents are expected to accomplish key milestones, including the colloquium presentation and the completion of 50-70% of the system's development. This will provide an opportunity to review progress and make adjustments as needed.

By the first semester of their fourth year, the proponents should aim to complete the documentation covering chapter 1 to 5 and the entire system, ensuring it meets all defined objectives. The system will test in terms of its usability, engagement, and educational effectiveness of the platform through pilot testing with IT learners and educators. After the testing, the proponent will ask feedback or reviews from the users to have quality assurance and to make changes if necessary.

Requirements Analysis

The NIDSToKnow platform is designed to serve as an educational and simulation tool for teaching NIDS using a honeypot-based approach. The functional requirements of the system center around three major user roles: learners, instructors, and administrators. The platform must support user registration, authentication, and role-based access control to ensure that users only interact with the features appropriate to their role. Learners must be able to access both theoretical and practical learning modules, which will cover fundamental and advanced NIDS concepts, including signature-based, anomaly-based, and hybrid detection methods. These modules should include interactive content, hands-on simulations using Cowrie honeypot, quizzes, and progress tracking features.

To simulate real-world attacks in a controlled environment, the platform will integrate Cowrie honeypot, enabling learners to observe how intrusion attempts, particularly those mimicking SSH and Telnet attacks from Linux-based systems, are detected and logged. The system must provide detailed logs and analysis tools to help learners understand attacker behavior and detection mechanisms. Instructors must be given tools to assign modules, monitor student engagement and progress, and offer personalized feedback. Meanwhile, administrators must be able to manage the overall platform, including user accounts, content modules, and system logs.

In terms of non-functional requirements, the platform must be secure, particularly since it involves simulated attacks and sensitive data such as user information and performance records. The user interface must be intuitive and user-friendly to support engagement and learning efficiency. Scalability is also important, as the platform must accommodate growing numbers of users and increasing simulation data without performance degradation. Compatibility with modern web browsers and responsiveness across various devices (e.g., laptops, tablets) are also essential.

To test the platform, the proponents will validate it with cybersecurity experts and IT educators before it becomes accessible to students. This user acceptance testing phase aims to assess the system's functionality, usability, and educational effectiveness from both professional and pedagogical perspectives. By engaging experts prior to student deployment, the proponents ensure that the platform's simulated attacks, NIDS methodologies, and learning modules are technically accurate, instructionally sound, and aligned with real-world cybersecurity practices. Feedback collected during this phase will guide refinements and improvements, ensuring a secure and effective learning experience.

Design

After gathering data and requirements, the proponents will test different color palettes to find the most suitable one for the website. The NIDSToKnow design changes iteratively, with each sprint responding to feedback from the adviser and panel. This process began with identifying key features and user stories, such as implementing the Cowrie honeypot to detect and record security risks, creating an easy-to-use dashboard for visualizing data, and implementing an alert system for notifying administrators of detected attacks. Early design focused on developing a versatile architecture integrated with the Cowrie honeypot, enabling real-time monitoring and reporting, and providing interactive learning content to create a hands-on student centered environment that promotes learning by doing. Preliminary wireframes for the dashboard, instructor tools, and user interface were developed to map out user interactions.

Design was enhanced during each sprint. The proponent's constant cooperation and input from system admins, instructors, and IT learners ensured it remained user-centric and aligned with end-users' needs. Early input led to design changes, particularly in the dashboard's layout. Metrics, such as attack frequency and threat score, were given priority to make it easier for users to understand real-time data. The alerting system was revised to add configurable notification options, such as email and SMS notifications, to increase its efficacy. Only the most important elements required for each sprint were described in the design documentation, which remained fluid and lean throughout iterations.

The integration of third-party services AbuseIPDB and the MySQL database was enhanced as the design process went along. Design changes were made to enhance database performance under increased loads to ensure it continues to function effectively in real-world settings after testing.

The Agile methodology made sure that the design phase was flexible and sensitive to user input and technological difficulties. By reviewing and modifying design decisions made at each sprint, the team was able to adapt to changing requirements, and solve problems related to the user interface, system architecture, or backend integrations. NIDSToKnow has developed into a complete, easy-to-use platform with a well-organized backend and a robust alerting system.

Development

During NIDSToKnow's development phase, the proponents focused on the iterative implementation of core features for the cybersecurity learning platform. Their primary goal was to develop and test each component—such as the Cowrie honeypot integration, the interactive NIDS training modules, and the user interface with intuitive dashboards—incrementally within short sprints. Each sprint, typically lasting two to four weeks, focused on completing specific features as prioritized in the product backlog. The proponents worked closely together, with constant communication between developers, cybersecurity experts, and educators. This collaborative approach ensured that features aligned with the project's educational goals and user requirements.

The development process included coding the backend using Flask for API creation, data processing, and integration with the MySQL database, while the frontend was developed to create a learning-friendly and intuitive dashboard for NIDS monitoring. Real-time data visualizations, including threat analytics and student performance metrics, were integrated. Each sprint delivered a working version of the dashboard, which was capable of pulling data and providing learning modules that included quizzes and educational materials. Developers also worked on building secure log exporting and archiving, ensuring that the system could securely store and export logs for future analysis.

At the same time, the proponents integrated AbuseIPDB to provide threat intelligence and IP reputation checks, strengthening the system's ability to proactively defend against potential attacks. Continuous integration and unit testing were conducted to ensure that new code did not interfere with existing features, and each new feature was functional, secure, and educational. By adopting Agile practices, the proponents rapidly identified and fixed issues, iterating on the codebase to improve the functionality, security, and educational value of NIDSToKnow.

Every sprint also included sprint reviews where the newly developed features were demonstrated to stakeholders for feedback. This feedback was crucial for refining the system, guaranteeing that the final product met usability and security standards. With each sprint, the system became more robust and comprehensive. By the end of the development phase, NIDSToKnow was capable of supporting real-time NIDS learning with hands-on simulations, incorporated instructor tools, a user-friendly learning interface, and a safe log management system. Testing and verification ensured smooth operation in a production environment.

Testing

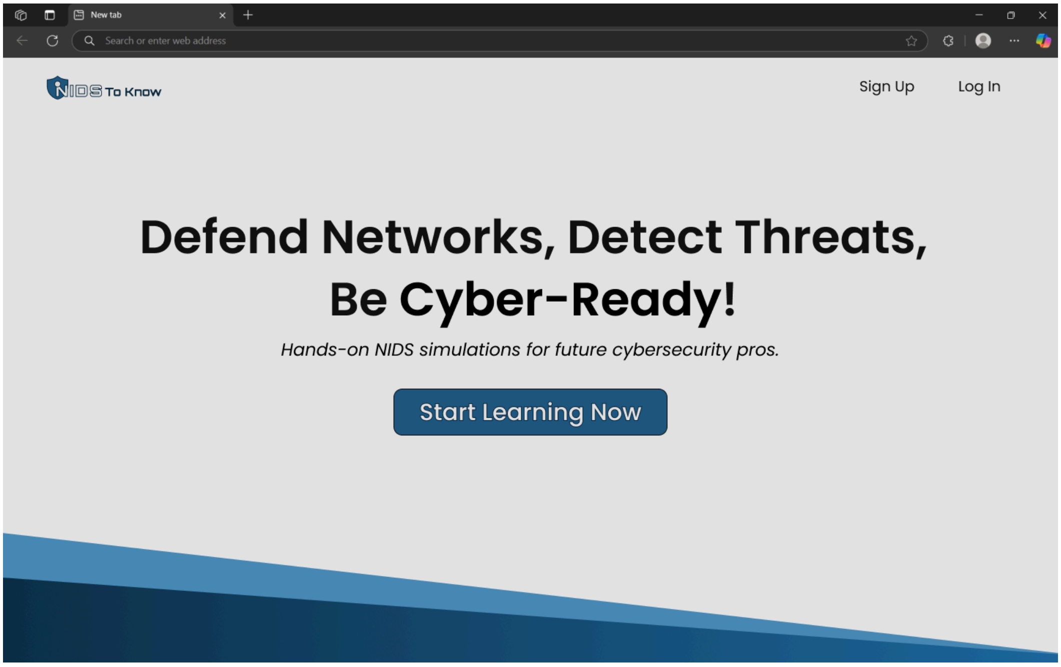
The proponents will deploy the system in an educational setting, granting access to selected students through a dedicated platform. Participants will be guided through structured activities designed to measure system effectiveness and ease of use from a learner's perspective. Data collected during this phase will help evaluate system responsiveness, clarity of content, and overall user experience.

Review

To ensure quality assurance, the proponents will utilize a set of rubrics containing performance indicators, scoring scales, and evaluation criteria. These tools will assess areas such as system clarity, functionality, and educational value. Feedback forms will also be provided to gather suggestions and recommendations from users, allowing the proponents to make changes and refine the platform for future deployment.

STORYBOARD

Landing Page



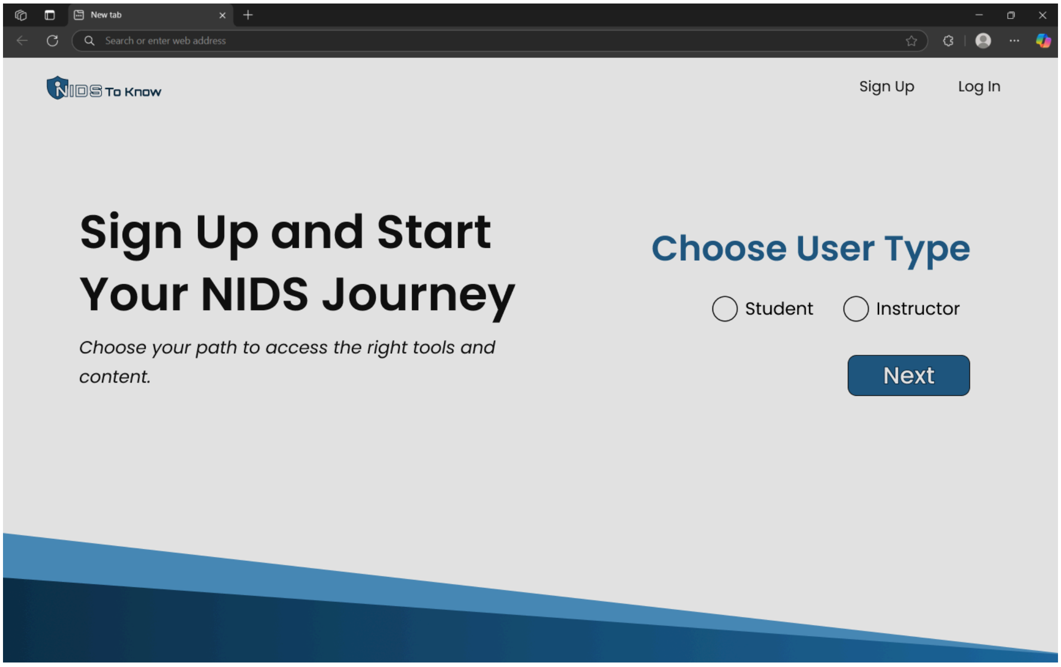
Defend Networks, Detect Threats, Be Cyber-Ready!

Hands-on NIDS simulations for future cybersecurity pros.

Start Learning Now

The landing page introduces a hands-on NIDS simulation platform, encouraging users to become cyber-ready. It features a clean design, a clear call to action, and easy access to Sign Up and Log In for smooth navigation.

Sign-up and Login Page



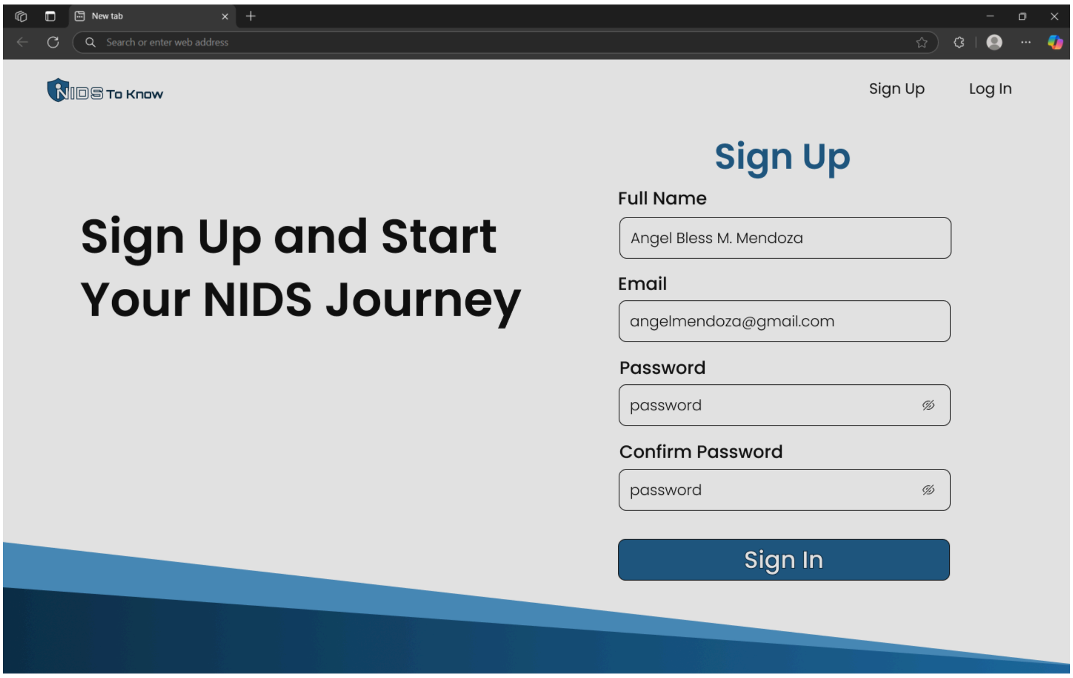
Sign Up and Start Your NIDS Journey

Choose your path to access the right tools and content.

Choose User Type

○ Student ○ Instructor

Next



Sign Up and Start Your NIDS Journey

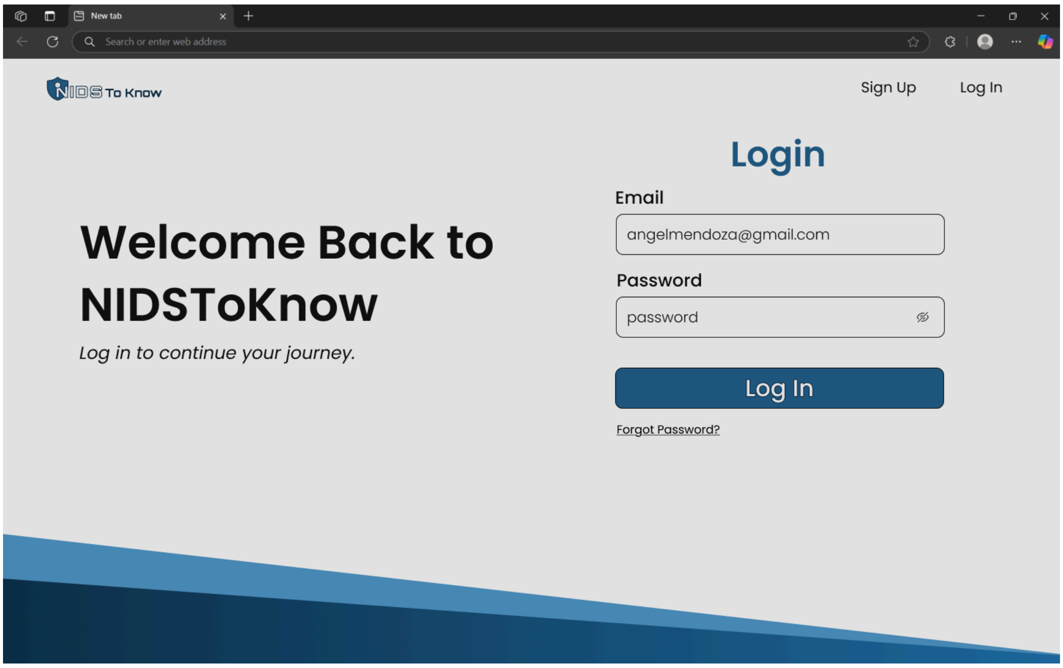
Sign Up

Full Name: Angel Bless M. Mendoza

Email: angelmendoza@gmail.com

Password: password

Confirm Password: password



Welcome Back to NIDSToKnow

Log in to continue your journey.

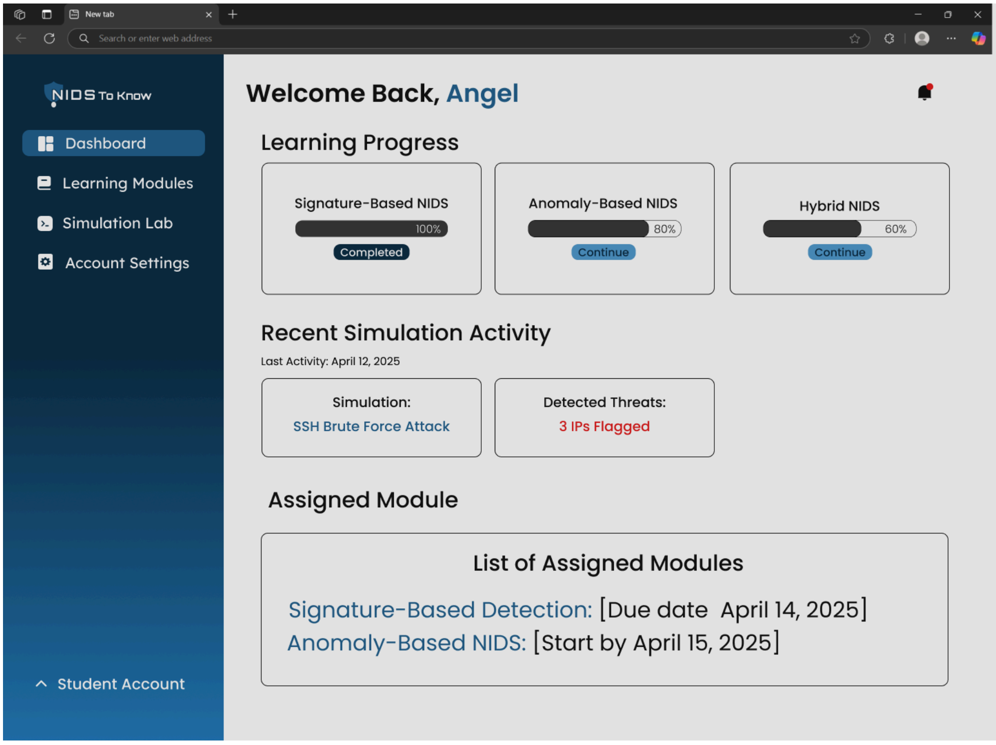
Login

Email: angelmendoza@gmail.com

Password: password

The Sign-up and Login pages allow users to begin their learning journey by selecting a user type—Student or Instructor—and creating an account with their details.

Student Dashboard Page



Welcome Back, Angel

Learning Progress

Signature-Based NIDS 100% Completed

Anomaly-Based NIDS 80% Continue

Hybrid NIDS 60% Continue

Recent Simulation Activity

Last Activity: April 12, 2025

Simulation: SSH Brute Force Attack

Detected Threats: 3 IPs Flagged

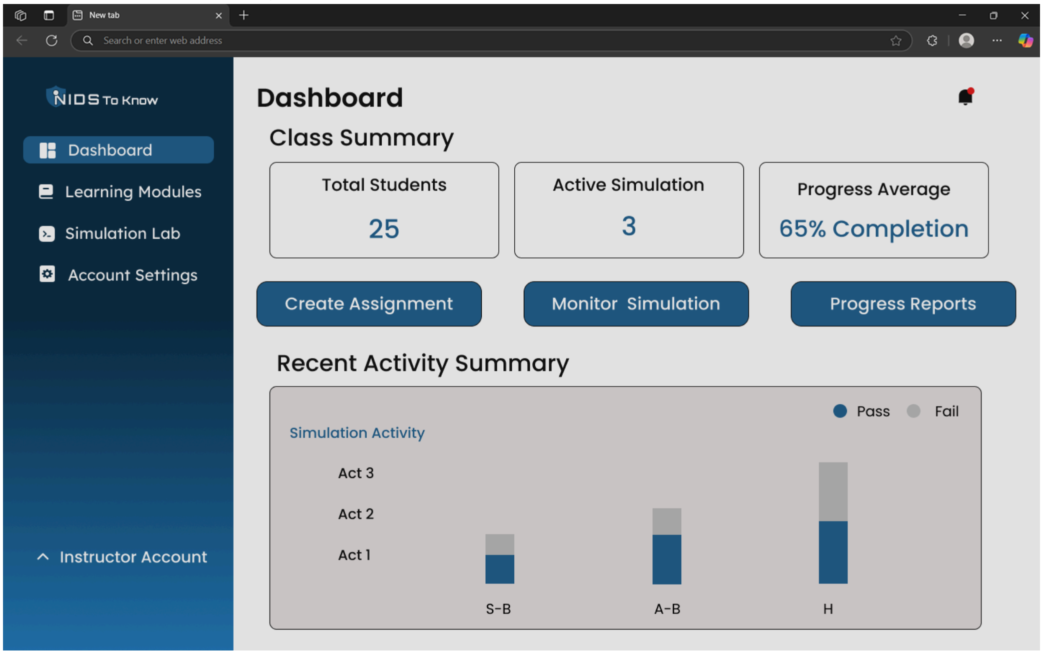
Assigned Module

List of Assigned Modules

Signature-Based Detection: [Due date April 14, 2025]
Anomaly-Based NIDS: [Start by April 15, 2025]

The **Student Dashboard Page** allows students to view their progress on each module and recent simulation activity. It also has a sidebar navigation for easy access to the other page.

Instructor Dashboard Page



Dashboard

Class Summary

Total Students 25

Active Simulation 3

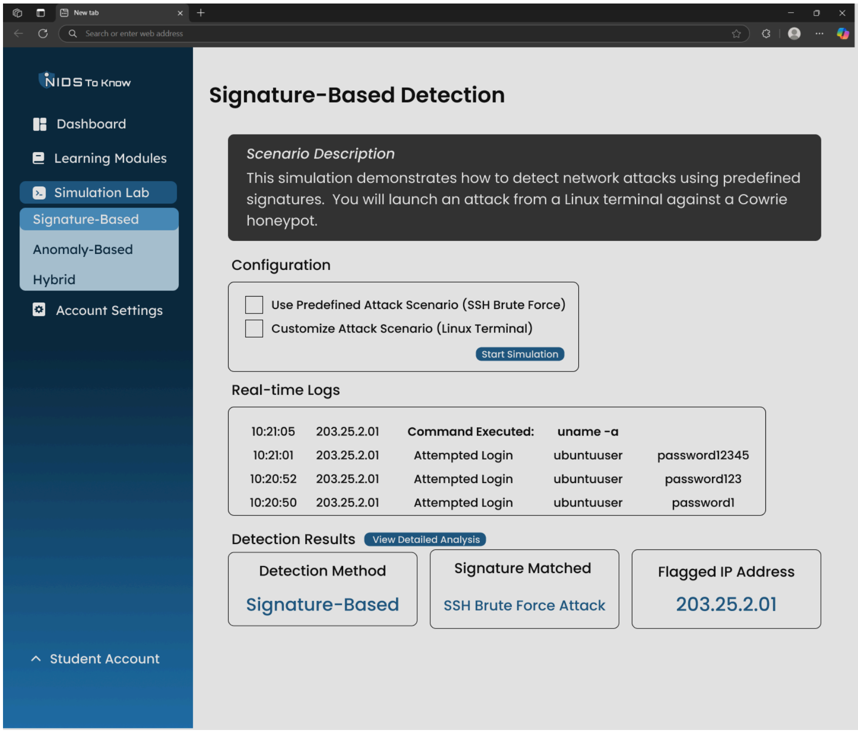
Progress Average 65% Completion

Recent Activity Summary

The **Instructor Dashboard Page** shows the class summary that indicates how total students, simulations, and progress. It also shows the recent activity summary of the student using the system.

Simulation Lab Page

Signature-Based Detection



Signature-Based Detection

Scenario Description
This simulation demonstrates how to detect network attacks using predefined signatures. You will launch an attack from a Linux terminal against a Cowrie honeypot.

Configuration

□ Use Predefined Attack Scenario (SSH Brute Force)
□ Customize Attack Scenario (Linux Terminal)
Start Simulation

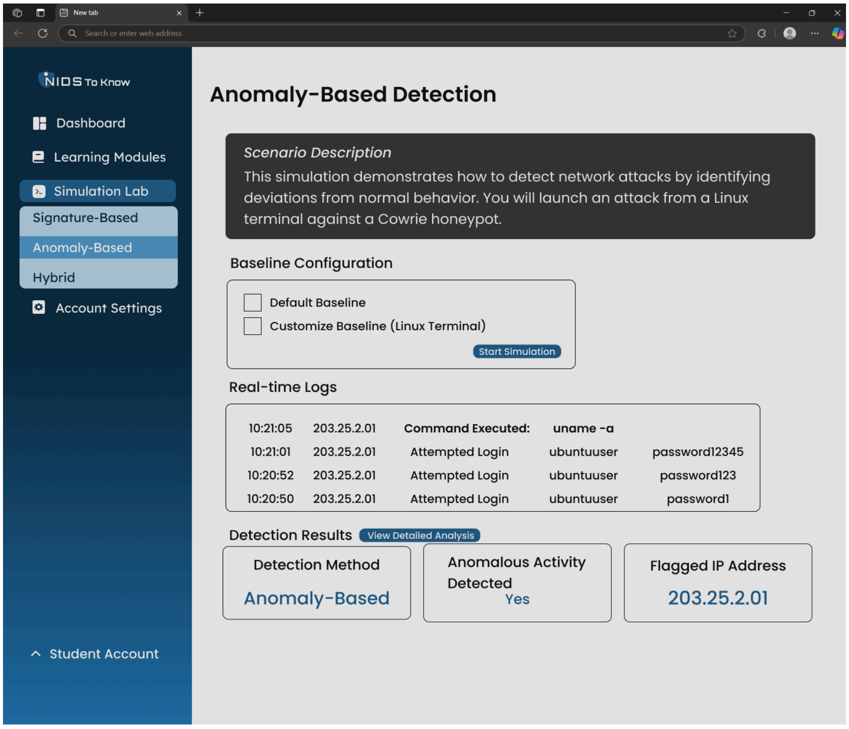
Real-time Logs

```
10:21:05   203.25.2.01   Command Executed:   uname -a
 10:21:01   203.25.2.01    Attempted Login    ubuntuuser    password12345
10:20:52   203.25.2.01    Attempted Login    ubuntuuser     password123
10:20:50   203.25.2.01    Attempted Login    ubuntuuser      password1
```

Detection Results View Detailed Analysis

Detection Method	Signature Matched	Flagged IP Address
Signature-Based	SSH Brute Force Attack	203.25.2.01

Anomaly-Based Detection



Anomaly-Based Detection

Scenario Description
This simulation demonstrates how to detect network attacks by identifying deviations from normal behavior. You will launch an attack from a Linux terminal against a Cowrie honeypot.

Baseline Configuration

□ Default Baseline
□ Customize Baseline (Linux Terminal)
Start Simulation

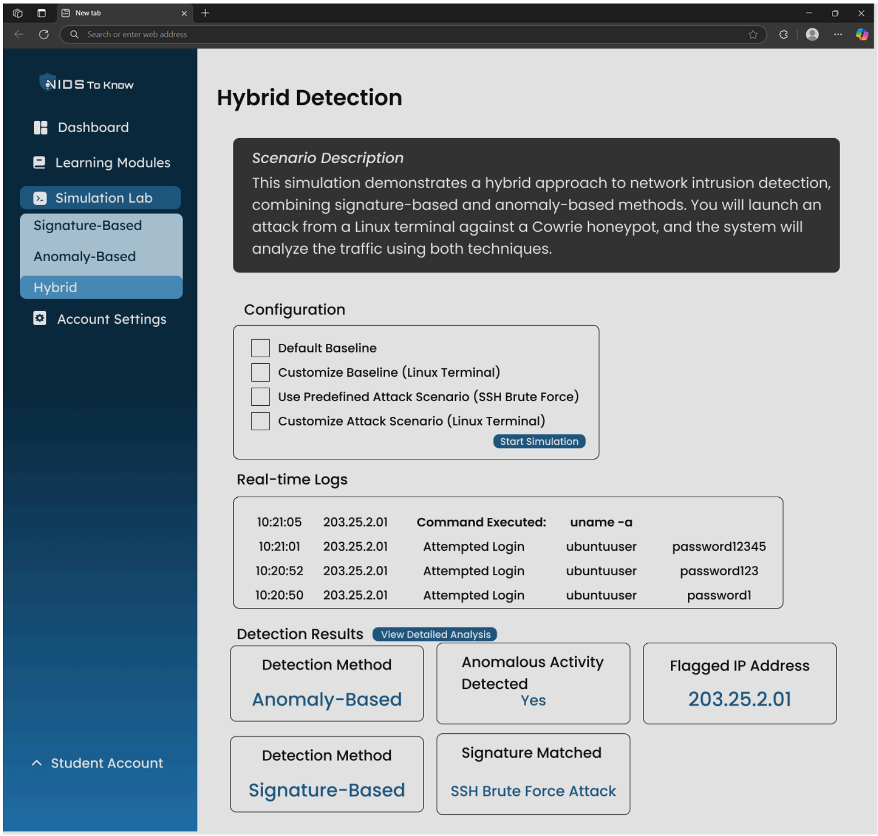
Real-time Logs

```
10:21:05   203.25.2.01   Command Executed:   uname -a
 10:21:01   203.25.2.01    Attempted Login    ubuntuuser    password12345
10:20:52   203.25.2.01    Attempted Login    ubuntuuser     password123
10:20:50   203.25.2.01    Attempted Login    ubuntuuser      password1
```

Detection Results View Detailed Analysis

Detection Method	Anomalous Activity Detected	Flagged IP Address
Anomaly-Based	Yes	203.25.2.01

Hybrid Detection



Hybrid Detection

Scenario Description

This simulation demonstrates a hybrid approach to network intrusion detection, combining signature-based and anomaly-based methods. You will launch an attack from a Linux terminal against a Cowrie honeypot, and the system will analyze the traffic using both techniques.

Configuration

- □ Default Baseline
- □ Customize Baseline (Linux Terminal)
- □ Use Predefined Attack Scenario (SSH Brute Force)
- □ Customize Attack Scenario (Linux Terminal)

Start Simulation

Real-time Logs

```
10:21:05   203.25.2.01   Command Executed:   uname -a
10:21:01   203.25.2.01   Attempted Login     ubuntuuser    password12345
10:20:52   203.25.2.01   Attempted Login     ubuntuuser    password123
10:20:50   203.25.2.01   Attempted Login     ubuntuuser    password1
```

Detection Results View Detailed Analysis

Detection Method: Anomaly-Based

Anomalous Activity Detected: Yes

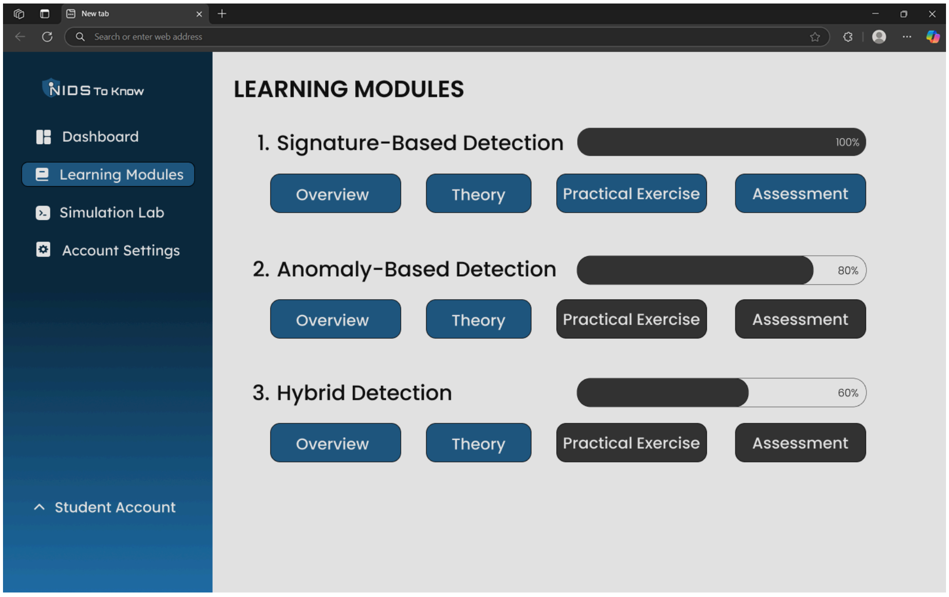
Flagged IP Address: 203.25.2.01

Detection Method: Signature-Based

Signature Matched: SSH Brute Force Attack

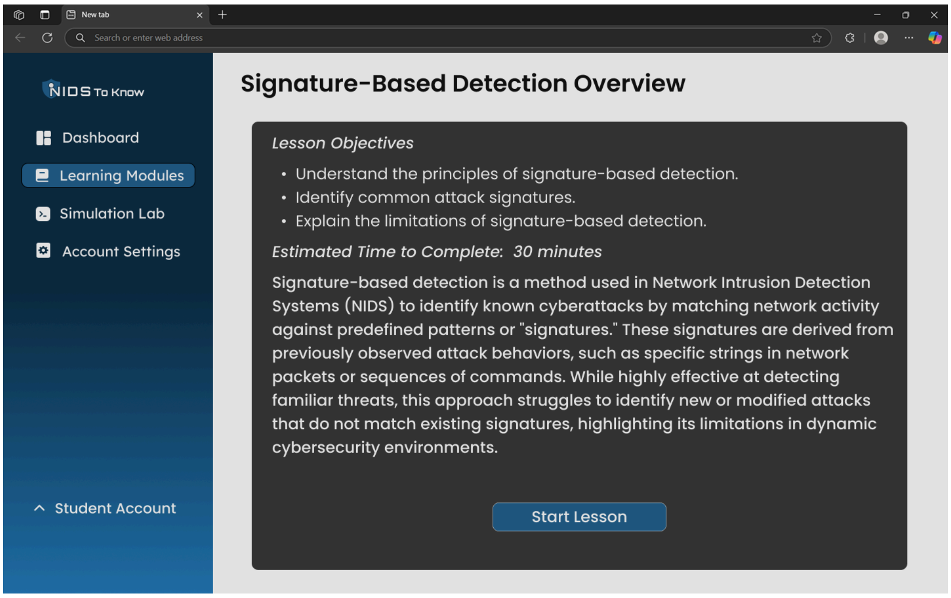
The **Simulation Lab Page** is where the students will be able to try how the 3 methods of NIDS work. Each 3 has its own page for its simulation. Users can check the box if you want the logs to come from a pre-configure or on your own using linux terminal. After that it will show the Real-time Logs and the Detected Results from the configured attack.

Learning Module Page



LEARNING MODULES

1. Signature-Based Detection 100%
2. Anomaly-Based Detection 80%
3. Hybrid Detection 60%



Signature-Based Detection Overview

Lesson Objectives

- Understand the principles of signature-based detection.
- Identify common attack signatures.
- Explain the limitations of signature-based detection.

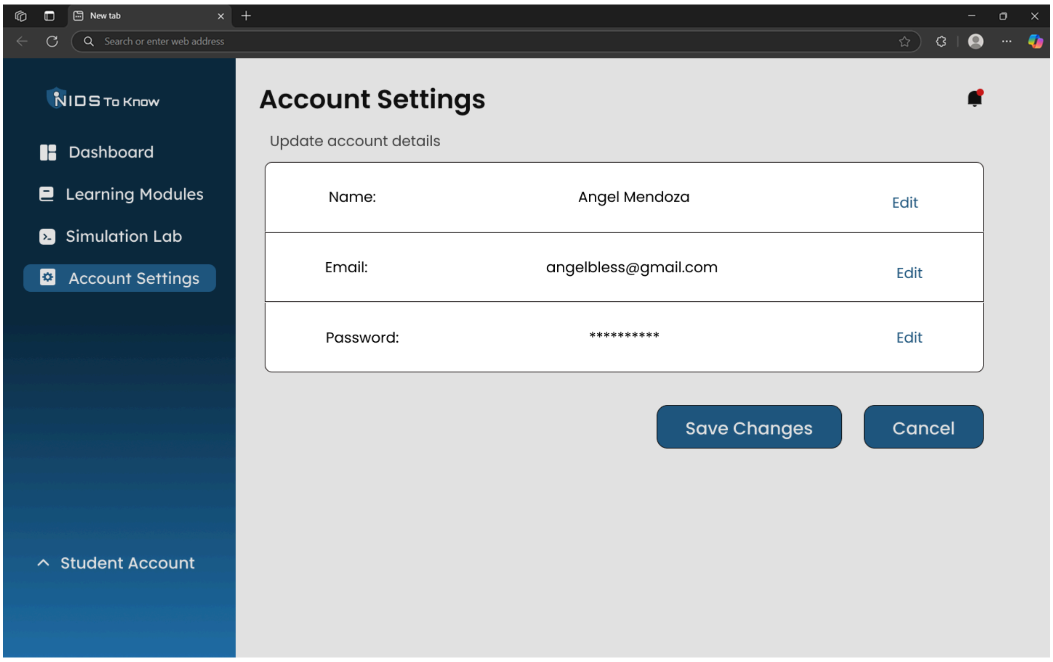
Estimated Time to Complete: 30 minutes

Signature-based detection is a method used in Network Intrusion Detection Systems (NIDS) to identify known cyberattacks by matching network activity against predefined patterns or "signatures." These signatures are derived from previously observed attack behaviors, such as specific strings in network packets or sequences of commands. While highly effective at detecting familiar threats, this approach struggles to identify new or modified attacks that do not match existing signatures, highlighting its limitations in dynamic cybersecurity environments.

The **Learning Module Page** consists of the lessons from each 3 methods (Signature, Anomaly, and Hybrid). Each lesson will be divided into Theoretical, Practical, and Assessment.

Account Settings Page

In the **Account Settings Page,** users can change their personal information and security settings.



Account Settings

Update account details

Name:	Angel Mendoza
Email:	angelbless@gmail.com
Password:	**********

References:

Abdulhammed, R., Musafer, H., Alessa, A., Faezipour, M., & Abuzneid, A. (2019). Features dimensionality reduction approaches for machine learning based network intrusion detection. Electronics, 8(3), 322. https://doi.org/10.3390/electronics8030322

Alawida, M., Shawar, B., Abiodun, O., Mehmood, A., Omolara, A., & Hwaitat, A. (2024). Unveiling the dark side of chatgpt: exploring cyberattacks and enhancing user awareness. Information, 15(1), 27. https://doi.org/10.3390/info15010027

Al‐Balushi, S. and Martin‐Hansen, L. (2019). The development of students' justifications for their positions regarding two theoretical models: electron cloud or sodium chloride crystal—after engaging in different learning activities. Journal of Research in Science Teaching, 56(8), 1011-1036. https://doi.org/10.1002/tea.21535

Azizan, A., Mostafa, S., Mustapha, A., Foozy, C., Wahab, M., Mohammed, M., … & Khalaf, B. (2021). A machine learning approach for improving the performance of network intrusion detection systems. Annals of Emerging Technologies in Computing, 5(5), 201-208. https://doi.org/10.33166/aetic.2021.05.025

Az-zahra, F., Lukman, H., & Balkist, P. (2023). Development of pbl-based mathematics teaching modules to improve the mathematical critical thinking skills of elementary school students. Jurnal Inovasi Matematika, 5(2), 131-150. https://doi.org/10.35438/inomatika.v5i2.392

Back, S., LaPrade, J., & Soor, S. (2018). Spatial and temporal patterns of cyberattacks: effective cybercrime prevention strategies around the globe. J-Institute, 3(1), 7-13.

https://doi.org/10.22471/protective.2018.3.1.07

Banik, S. and Peña, L. (2015). Deploying agents in the network to detect intrusions.. https://doi.org/10.1109/icis.2015.7166574

Begley, K., Monaghan, M., & Qi, Y. (2013). Repeated testing to improve skills in a pharmacy practice laboratory course. American Journal of Pharmaceutical Education, 77(6), 130. https://doi.org/10.5688/ajpe776130

Bernhardsson, L., Gellerstedt, M., & Winman, T. (2017). Work-integrated-learning: so, what? a framework for describing the level of integration between work and learning.. https://doi.org/10.21125/iceri.2017.0165

Carrillo-Mondejar, J., Carrillo-Mondejar, J., Roldán-Gómez, J., Gómez, S., & Villafranca, G. (2024). Stories from a customized honeypot for the IoT. https://doi.org/10.53106/160792642024012501010

Croft, D. (2018). Embedding constructive alignment of reading lists in course design. Journal of Librarianship and Information Science, 52(1), 67-74. https://doi.org/10.1177/0961000618804004

Cruz, L. and Rivera, K. (2022). Development and validation of project-based module for selected topics in biology. International Journal of Educational Research & Social Sciences.

De Ramos, N. M., & Esponilla, F. D. II. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. International Journal of Evaluation and Research in Education (IJERE), 11(3), 1198–1209. https://doi.org/10.11591/ijere.v11i3.22863

Department of Information and Communications Technology. (2022). National Cybersecurity Plan 2022. Republic of the Philippines. https://dict.gov.ph/national-cybersecurity-plan-2022

Duan, T., Tian, Y., Zhang, H., Liu, Y., Li, Q., Jiang, J., … & Shi, Z. (2020). Intelligent processing of intrusion detection data. Ieee Access, 8, 78330-78342. https://doi.org/10.1109/access.2020.2989498

Eniodunmo, O. and Al-Aqtash, R. (2023). A predictive model to predict a cyberattack using self normalizing neural networks. International Journal of Statistics and Probability, 12(6), 60. https://doi.org/10.5539/ijsp.v12n6p60

Farooq, M., Abbas, S., Rahman, A., Sultan, K., Khan, M., & Mosavi, A. (2023). A fused machine learning approach for intrusion detection system. Computers Materials & Continua, 74(2), 2607-2623. https://doi.org/10.32604/cmc.2023.032617

Ferm, L. (2021). Vocational students' ways of handling the academic/vocational divide. International Journal for Research in Vocational Education and Training, 8(1). https://doi.org/10.13152/ijrvet.8.1.1

Gudimetla, S. and Kotha, N. (2024). Enhancing threat detection and response strategies. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets55883

Helmer, H. (2021). Humorous or occasioned instructions: learning the "shoulder check" in theoretical and practical driving lessons. International Journal of Applied Linguistics, 31(1), 109-131. https://doi.org/10.1111/ijal.12325

Ho, S., Al-Jufout, S., Dajani, K., & Mozumdar, M. (2021). A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network. Ieee Open Journal of the Computer Society, 2, 14-25. https://doi.org/10.1109/ojcs.2021.3050917

Holmgren, D., Nilsson, M., & Wekell, P. (2019). Combining learning for educators and participants in a paediatric cpd programme. BMC Medical Education, 19(1). https://doi.org/10.1186/s12909-019-1461-x

Ibraheem, I. (2022). Enhancing intrusion detection systems using ensemble machine learning techniques. Data & Metadata, 1, 33. https://doi.org/10.56294/dm202271

Jain, J. and Waoo, A. (2023). An artificial neural network technique for prediction of cyber-attack using intrusion detection system. Journal of Artificial Intelligence Machine Learning and Neural Network, (32), 33-42. https://doi.org/10.55529/jaimlnn.32.33.42

Jain, Y. K., & Singh, S. (2011). Honeypot-based secure network system. International Journal on Computer Science and Engineering (IJCSE), 3(2), 615.

Koehler, R., Sharma, U., & Nord, P. (2024). Addressing the cybersecurity skills gap with higher education. IBM. https://www.ibm.com/new/announcements/addressing-cybersecurity-skills-gap-higher-education

Korda, D. and Dapaah, E. (2023). The role of cyberattacks on modern warfare: a review. International Journal of Research and Innovation in Applied Science, VIII(VII), 286-292. https://doi.org/10.51584/ijrias.2023.8733

Laghrissi, F., Douzi, S., Douzi, K., & Hssina, B. (2021). Intrusion detection systems using long short-term memory (lstm). Journal of Big Data, 8(1). https://doi.org/10.1186/s40537-021-00448-4

Lavrova, D. (2025). Cybersecurity threatscape in Southeast Asia. PositiveTechnology. https://global.ptsecurity.com/analytics/cybersecurity-threatscape-in-southeast-asia

Ledezma, C., Font, V., & Sala, G. (2022). Analysing the mathematical activity in a modelling process from the cognitive and onto-semiotic perspectives. Mathematics Education Research Journal, 35(4), 715-741. https://doi.org/10.1007/s13394-022-00411-3

Lee, C. and Sen, A. (2018). Students voice in their learning: incorporating students' expectations in learning design of e-learning of pharmacotherapy. International Journal of Learning and Teaching, 203-208. https://doi.org/10.18178/ijlt.4.3.203-208

Mäkelä, M., Sarvelainen, H., & Lyytikäinen, T. (2018). Learning heat dynamics using modelling and simulation.. https://doi.org/10.3384/ecp17142403

Maraj, A., Sutherland, C., & Butler, W. (2021). The challenges to cybersecurity education in developing countries: A case study of Kosovo. AAB College, Faculty of Computer Sciences; Capitol Technology University.

Masaguni, A., Lamangantjo, C., Katili, N., Pikoli, M., Buhungo, T., & Payu, C. (2023). Development of science learning modules based on project based leraning on additives and addictive substances (a research in class viii smp negeri 7 telaga biru). Jurnal Penelitian Pendidikan Ipa, 9(12), 10758-10767. https://doi.org/10.29303/jppipa.v9i12.5731

Mispriatin, M., Ginting, J., & Arifwidodo, B. (2022). Analisis kinerja honeypot dionaea dan cowrie dalam mendeteksi serangan. Prosiding Seminar Nasional Teknoka, 6, 170-178. https://doi.org/10.22236/teknoka.v6i1.448

MixMode Threat Research. (2024). Global cybercrime report 2024: Which countries face the highest risk? MixMode. https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk/

Morić, Z., Mršić, L., Kunić, Z., & Đambić, G. (2024). Honeypots in cybersecurity: their analysis, evaluation and importance.. https://doi.org/10.20944/preprints202408.0946.v1

Naik, N., Shang, C., Jenkins, P., & Shen, Q. (2020). Building a cognizant honeypot for detecting active fingerprinting attacks using dynamic fuzzy rule interpolation. Expert Systems, 38(5). https://doi.org/10.1111/exsy.12557

National Cyber Security Index. (2023). Archived data from 2016-2023. https://ncsi.ega.ee/country/ph_2022/

Neves, B., Altermann, C., Gonçalves, R., Lara, M., & Mello‐Carpes, P. (2017). Home-based vs. laboratory-based practical activities in the learning of human physiology: the perception of students. Ajp Advances in Physiology Education, 41(1), 89-93. https://doi.org/10.1152/advan.00018.2016

Qi, G., Chen, Z., Zhao, H., & Chensheng, W. (2019). Construction and application of machine learning model in network intrusion detection.. https://doi.org/10.2991/pntim-19.2019.83

Republic of the Philippines. (2012). Republic Act No. 10175: An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes. The Lawphil Project. https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html

S, D., & Chakkaravarthy, S. (2023). Containerized cloud-based honeypot deception for tracking attackers. Scientific Reports, 13(1). https://doi.org/10.1038/s41598-023-28613-0

Sayed, M. and Taha, M. (2023). Oblivious network intrusion detection systems.. https://doi.org/10.21203/rs.3.rs-3232596/v1

Setianto, F., Tsani, E., Sadiq, F., Domalis, G., Tsakalidis, D., & Kostakos, P. (2021). GPT-2C: A GPT-2 parser for Cowrie honeypot logs. https://doi.org/10.48550/arxiv.2109.06595

Sivanantham, S., Mohanraj, V., Suresh, Y., & Senthilkumar, J. (2023). Association rule mining frequent-pattern-based intrusion detection in network. Computer Systems Science and Engineering, 44(2), 1617-1631. https://doi.org/10.32604/csse.2023.025893

Song, Z., Hong, Y., & Palaoag, T. (2022). An intelligent cyber security detection and response platform. International Journal for Research in Advanced Computer Science and Engineering, 8(12), 1-10. https://doi.org/10.53555/cse.v8i12.2167

Suratnu, R. (2023). The adoption of the addie model in designing an instructional module: the case of malay language remove students. International Journal of Indonesian Education and Teaching, 7(2), 262-270. https://doi.org/10.24071/ijiet.v7i2.3521

Susanti, R., Muhammad, A., & Prabowo, W. (2022). Implementasi intrusion prevention system (ips) ossec dan honeypot cowrie. Jurnal Sisfokom (Sistem Informasi Dan Komputer), 11(1), 73-78. https://doi.org/10.32736/sisfokom.v11i1.1246

Thanh, N. (2020). Promoting learner autonomy through self-assessment and reflection. Vnu Journal of Foreign Studies, 35(6). https://doi.org/10.25073/2525-2445/vnufs.4483

Tinnaluri, V. and Shaik, N. (2024). A comprehensive approach: developing a honeypot system to thwart cyber attackers. eatp. https://doi.org/10.53555/kuey.v30i5.4517

Tsoy, A., Ten, S., & Rakhimova, A. (2023). Project-based learning technology in classes for technical and it-orientating groups: experience and results of implementation. E3s Web of Conferences, 460, 05016. https://doi.org/10.1051/e3sconf/202346005016

Vanin, P., Newe, T., Dhirani, L., O'Connell, E., O'Shea, D., Lee, B., … & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. Applied Sciences, 12(22), 11752. https://doi.org/10.3390/app122211752

Vauderwange, O., Javahiraly, N., & Curticapean, D. (2019). Increased knowledge transfer through the integration of research projects into university teaching., 140. https://doi.org/10.1117/12.2523865

Vikram. (2024). 12 best countries to study cyber security. Kanan.co. https://www.kanan.co/blog/best-countries-to-study-cyber-security/

Wang, H., Morić, J., & Ng, D. (2022). Automating attack detection with machine learning techniques for honeypots. Computers & Security, 106, 102365. https://doi.org/10.1016/j.cose.2021.102365

Xiao, H., Wei, H., Liao, Q., Ye, Q., Cao, C., & Zhong, Y. (2023). Exploring the gamification of cybersecurity education in higher education institutions: An analytical study. SHS Web of Conferences, 166, 01036. https://doi.org/10.1051/shsconf/202316601036

Yeboah-Ofori, A., Mouratidis, H., Ismai, U., Islam, S., & Papastergiou, S. (2021). Cyber supply chain threat analysis and prediction using machine learning and ontology., 518-530. https://doi.org/10.1007/978-3-030-79150-6_41