A
PROJECT REPORT
ON

“Intrusion Detection System”

In Partial Fulfillment of Diploma in Computer Engineering

(6th Semester)

In the subject of

Network And Information Security (22620)

Submitted By:

Rina Pawar

Nachiket Bhise

Sanket Nasare

Hemant Somkuwar

Sahil Pohane

Submitted To:

Maharashtra State Board of Technical Education, Mumbai. (M.S)

Under the guidance of

Mr.H.N.Ranotkar

Department in Computer Engineering

Government Polytechnic Arvi, Dist. – Wardha

(2023-2024)

Government Polytechnic, Arvi

Department in Computer Engineering

Certificate

This is to certify that below students of sixth Semester Diploma in Computer Engineering have satisfactorily completed the micro project entitled “Intrusion detection system” in NIS for the academic year 2023-2024 as prescribe in MSBTE curriculum**.**

Roll No	Name	Enrollment No.	Seat No.	Signature
50	Rina Pawar	2101320069	312633	
51	Nachiket Bhise	2101320099	312650	
52	Sanket Nasare	2101320100	312652	
54	Hemant Somkuwar	2101320107	312656	
60	Sahil Pohane	2201320472		

Mr. H. N. Ranotkar	Dr. M. A. Ali	Dr. M. A. Ali
Subject Teacher	Head Of Department	Principal

Place: - Arvi

Date: -

Declaration

We undersigned hereby declare that the micro project report entitled “Intrusion detection system”. Contents is the outcome of our own literature survey. We further declare that contents of this report are properly cited and well acknowledged. This present report is not submitted to any other examination of this or any other institute for the award of any diploma.

(Signature)

Government polytechnic, Arvi

Place: Arvi
Date:

Part A : Project Proposal

"Intrusion Detection System"

Brief Information:

An Intrusion Detection System (IDS) is a vital cybersecurity tool that monitors networks or systems for malicious activities or policy violations. By analyzing network traffic or system behavior, an IDS identifies patterns indicative of unauthorized access, attacks, or security breaches. It serves as an early warning system, promptly alerting security personnel to potential threats, allowing for swift response and mitigation actions. IDS can be network-based (NIDS), monitoring network traffic, or host-based (HIDS), analyzing activity on individual systems. It aids in regulatory compliance by fulfilling requirements for continuous monitoring and incident detection. IDS plays a crucial role in incident response and forensic investigations, providing detailed logs and alerts for security incidents.It enhances overall security posture by complementing existing security controls and mitigating security risks. With its ability to detect and respond to security threats proactively, an IDS helps organizations maintain business continuity and safeguard sensitive data from unauthorized access.

Aim Of the Micro-Project:

Intrusion Detection System

Intended Course Outcome

- Apply cryptographic algorithms and protocol to maintain computer security.
- Apply the encrypt and decrypt algorithm to protect our sensitive data.
- Apply user identification and authentication methods.
- Maintain secured network.

Literature Review

The Intrusion Detection Systems (IDS) underscores their significance in cybersecurity by providing early threat detection and response. Studies examine IDS techniques, including signature-based and anomaly-based detection, to adapt to evolving cyber threats. Research evaluates IDS effectiveness in identifying network intrusions, malware infections, and unauthorized access attempts, contributing insights for organizational security strategies. Studies emphasize the importance of integrating IDS with other security tools like IPS, EDR, and SIEM for comprehensive defense. Additionally, incorporating threat intelligence enhances detection accuracy and response. Evaluation of IDS effectiveness considers factors like detection accuracy and false positives, highlighting the need for ongoing refinement to keep pace with evolving threats.Collaborative efforts between academia, industry, and government are crucial for addressing cybersecurity challenges effectively. By leveraging IDS alongside complementary technologies and fostering continuous evaluation and improvement, organizations can bolster their defenses against a dynamic threat landscape. Signature-based detection relies on predefined patterns to spot known threats, while anomaly-based techniques identify deviations from normal behavior. Research shows that while signature-based methods excel at known threats, they struggle with novel attacks. Anomaly-based approaches, often using machine learning, show promise in detecting emerging threats and insider attacks.

Action Plan

Sr. No	Details of Activity	Planned start date	Planned finish date	Team Members
1	To discuss and get the topic ofmicro project.			All
2	Start planning on topic of microproject.			All
3	Collect information about ourtopic.			All
4	Distribute works within groupmembers.			All
5	To start with creating with maincopy of micro project.			All
6	Collect different informationabout micro project.			All
7	Initiate different views aboutmicro project.			All
8	Editing process must be donebefore hard copy.			All
9	Check softcopy properly beforepreparing of hardcopy.			All
10	To start creating copy properly.			All
11	Checking the information frommonitor.			All
12	Check the soft copy.			All
13	To present soft copy via Gmail.			All
14	Represented the hard copy of main micro project.			All

❖ Name of Responsible Team Members

Name	Enrollment No.	Signature
Rina Pawar	2101320069	
Nachiket Bhise	2101320099	
Sanket Nasare	2101320100	
Hemant Somkuwar	2101320107	
Sahil Pohane	2201320472	

Part B : Project Report

"Intrusion Detection System"

Rationale

The The implementation of an Intrusion Detection System (IDS) is essential for organizations aiming to bolster their cybersecurity defenses and safeguard against various cyber threats. By continuously monitoring network traffic and system activity, an IDS serves as an early warning mechanism, promptly detecting and alerting on suspicious behavior indicative of potential security breaches.

It aids in compliance adherence by fulfilling regulatory requirements, facilitates incident response through detailed logging and forensic analysis, and enhances overall security posture by complementing existing security controls. With its ability to provide comprehensive coverage across network and host environments, an IDS plays a pivotal role in mitigating security risks, ensuring business continuity, and safeguarding sensitive data from unauthorized access and attacks.
.

Course Outcomes Addressed:

- Identify the advantages of using SFTP over other file transfer protocols
- Install and configure an SFTP server for secure file transfers within a network
- Demonstrate how to securely transfer files using SFTP
- Implement access control, monitoring, and auditing mechanisms for an SFTP server
- Troubleshoot common issues related to SFTP file transfers

Literature Review

Intrusion Detection Systems (IDS) constitutes a rich tapestry of research, emphasizing their pivotal role in modern cybersecurity. Scholars have extensively explored IDS as critical components in defending against a plethora of cyber threats, ranging from network intrusions and malware infections to unauthorized access attempts. Various detection techniques, such as signature-based, anomaly-based, and hybrid approaches, have been scrutinized for their efficacy in identifying and mitigating security breaches. Studies delve into the evolution of IDS methodologies, tracing advancements from rudimentary signature matching to sophisticated machine learning algorithms and artificial intelligence-driven anomaly detection systems.

Furthermore, research endeavors aim to assess the effectiveness of IDS in diverse contexts, including enterprise networks, critical infrastructure, cloud environments, and Internet of Things (IoT) ecosystems. Comparative analyses of different IDS implementations, such as network-based (NIDS), host-based (HIDS), and network behavior analysis (NBA) systems, shed light on their strengths, limitations, and operational challenges. Additionally, investigations into IDS deployment strategies, including placement, configuration, and tuning parameters, offer valuable insights into optimizing detection accuracy while minimizing false positives.

Actual Methodology Followed

- Discuss about our topic.
- Understand the intrusion detection concepts.
- Collect information about intrusion detection system.
- Deep study about secure file transfer protocol with network.
- Prepare had copy of project and submit edit.

Actual Resource used

Sr. no.	Name of resource	Specification	Qty
1	World	Windows 11 Compatible	1
2	Internet Explorer	64-Bit	1

Application of this Micro-Project:

- Network Security Enhancement: By deploying the IDS within organizational networks, companies can bolster their defenses against external threats, such as unauthorized access attempts, malware infections, and network intrusions. The IDS serves as a vigilant guardian, continuously monitoring network traffic and promptly alerting security personnel to potential security breaches.
- Threat Intelligence Integration: IDS integration with threat intelligence feeds enriches threat detection capabilities, enabling organizations to identify emerging threats, zero-day vulnerabilities, and advanced persistent threats (APTs). By correlating IDS alerts with threat intelligence data, organizations can proactively defend against sophisticated cyber attacks and anticipate evolving threat landscapes.
- Security Operations Optimization: IDS deployment streamlines security operations by automating threat detection, alert triaging, and incident prioritization processes. Security analysts can focus their efforts on high-priority alerts and critical security incidents, leveraging IDS insights to orchestrate effective incident response workflows and minimize response times..
- Risk Mitigation and Business Continuity: By mitigating security risks and proactively identifying and addressing security threats, IDS contributes to maintaining business continuity and safeguarding organizational assets, reputation, and customer trust. Organizations can mitigate financial losses associated with security breaches and preserve stakeholder confidence by investing in robust IDS solutions..

❖ Introduction

In an era characterized by pervasive digital connectivity and evolving cyber threats, the imperative to safeguard organizational networks and data assets has never been more pressing. Intrusion Detection Systems (IDS) emerge as indispensable tools in the cybersecurity arsenal, tasked with the crucial mission of detecting and mitigating malicious activities and unauthorized access attempts. At its core, an IDS serves as a vigilant sentry, tirelessly monitoring network traffic and system activity to identify patterns indicative of potential security breaches. By leveraging sophisticated detection algorithms and threat intelligence feeds, IDS solutions empower organizations to fortify their defenses, proactively identify security threats, and respond swiftly to emerging cyber risks..

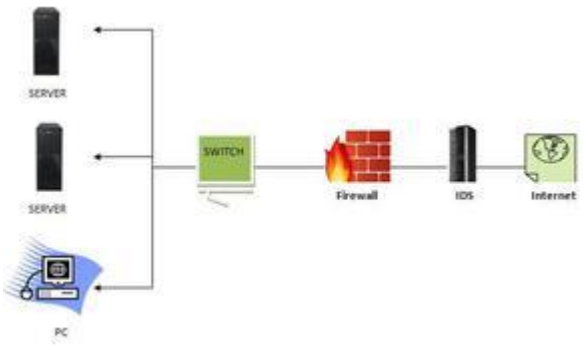
The landscape of cybersecurity is dynamic and multifaceted, encompassing an array of threat actors, attack vectors, and vulnerabilities. Against this backdrop, IDS solutions play a pivotal role in bolstering the resilience of organizational networks and infrastructure. From network-based (NIDS) deployments that scrutinize incoming and outgoing traffic to host-based (HIDS) solutions that monitor individual systems for signs of compromise, IDS implementations offer comprehensive coverage across diverse attack surfaces. Moreover, advancements in anomaly-based detection techniques, machine learning algorithms, and behavioral analytics augment the capabilities of IDS, enabling more accurate and proactive threat detection.

Beyond the realm of threat detection, IDS solutions also play a vital role in incident response and forensic investigations. By providing real-time alerts, detailed logs, and forensic evidence, IDS solutions facilitate rapid incident triaging, root cause analysis, and mitigation actions. Furthermore, the integration of IDS with other cybersecurity technologies, such as firewalls, intrusion prevention systems (IPS), and security information and event management (SIEM) platforms, enhances overall threat detection capabilities and enables seamless information sharing across security operations centers (SOCs) and incident response teams.

In addition to its operational benefits, IDS solutions also play a pivotal role in regulatory compliance and governance. Compliance mandates such as PCI DSS, HIPAA, GDPR, and NIST SP 800-61 underscore the importance of continuous monitoring and incident detection capabilities provided by IDS solutions. By aligning with industry standards and regulatory requirements, organizations can demonstrate due diligence in safeguarding sensitive data, protecting customer privacy, and mitigating legal and regulatory risks.

❖ What is an Intrusion Detection System?

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using an SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections.



❖ Working of Intrusion Detection System (IDS)

● An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.

● It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.

● The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.

● If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.

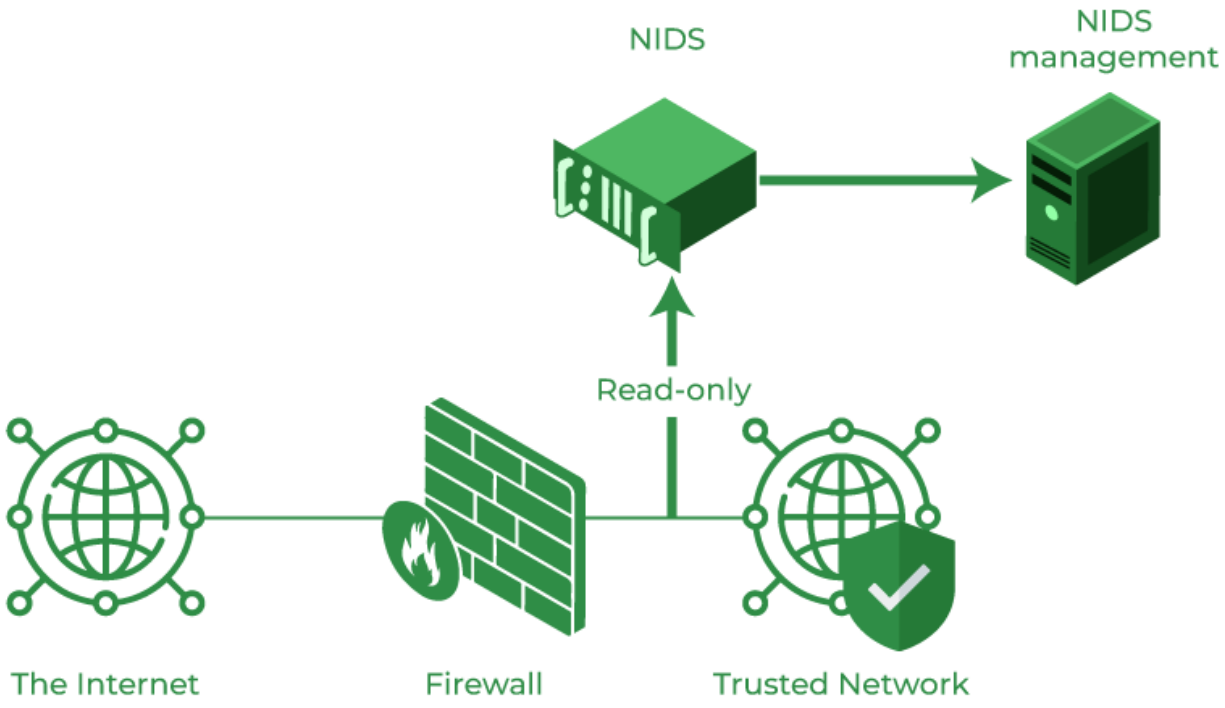
● The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

❖ Classification of Intrusion Detection System (IDS)

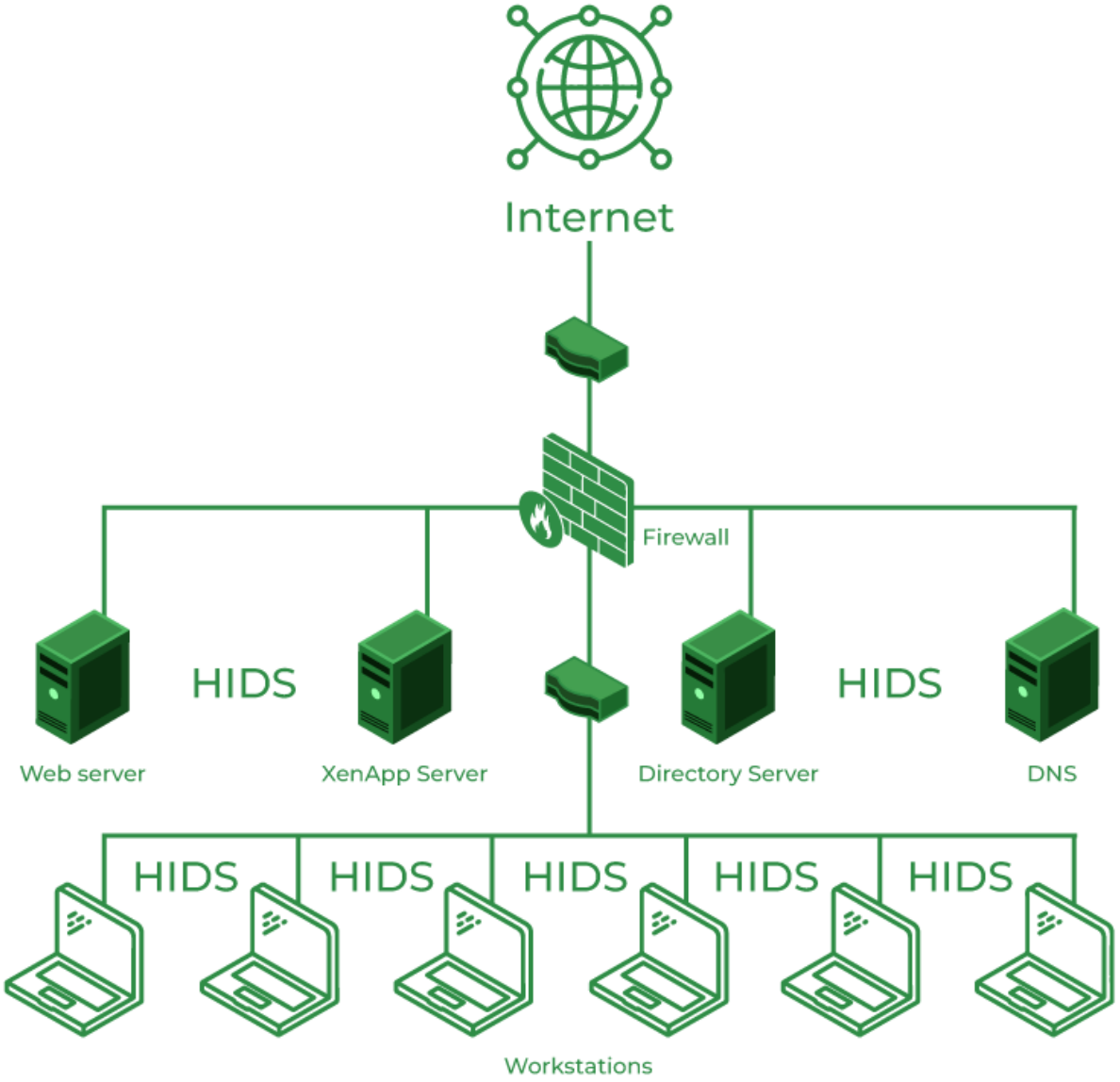
● Intrusion Detection System are classified into 5 types:

- **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

- NIDS plays a critical role in detecting and mitigating network-based attacks, such as denial-of-service (DoS) attacks, port scans, malware propagation, and unauthorized access attempts. By providing real-time visibility into network traffic and identifying potential security threats, NIDS helps organizations strengthen their cybersecurity defenses, protect sensitive data, and maintain the integrity and availability of their network infrastructure.



- **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.

- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

- **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

❖ Intrusion Detection System Evasion Techniques

•**Fragmentation:** Dividing the packet into smaller packet called fragment and the process is known as fragmentation. This makes it impossible to identify an intrusion because there can't be a malware signature

.

•**Packet Encoding:** Encoding packets using methods like Base64 or hexadecimal can hide malicious content from signature-based IDS.

•**Traffic Obfuscation**: By making message more complicated to interpret, obfuscation can be utilised to hide an attack and avoid detection.

•**Encryption:** Several security features, such as data integrity, confidentiality, and data privacy, are provided by encryption. Unfortunately, security features are used by malware developers to hide attacks and avoid detection.

❖ Benefits of IDS

- **Detects malicious activity:** IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- **Improves network performance:** IDS can identify any performance issues on the network, which can be addressed to improve network performance.
- **Compliance requirements:** IDS can help in meeting compliance requirements by monitoring network activity and generating reports.
- **Provides insights:** IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

❖Detection Method of IDS

Signature-based Method: Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.

Anomaly-based Method: Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. The machine learning-based method has a better-generalized property in comparison to signature-based

Code:

```
class IntrusionDetectionSystem:
    def __init__(self):
        self.failed_attempts = {}

    def log_attempt(self, username, password):
        # For simplicity, we're assuming the password is correct if the username is correct
        if username in self.failed_attempts:
            self.failed_attempts[username] += 1
        else:
            self.failed_attempts[username] = 1

        threshold = 3  # Default threshold for failed login attempts
        if self.failed_attempts[username] >= threshold:
            print(f"Alert: Possible intrusion detected for user {username}!")

    def reset_attempts(self, username):
        if username in self.failed_attempts:
            del self.failed_attempts[username]

if __name__ == "__main__":
    # Create an instance of the IntrusionDetectionSystem
    ids = IntrusionDetectionSystem()

    correct_username = "admin"  # Example correct username
    correct_password = "password"  # Example correct password

    while True:
        print("\nEnter 'q' to quit.")
        username = input("Enter username: ")

        # Check if user wants to quit
        if username.lower() == 'q':
            break

        password = input("Enter password: ")

        # Check if the username is correct
        if username == correct_username and password == correct_password:
            print("Welcome, administrator!")

        # Log the login attempt
        ids.log_attempt(username, password)

    print("\nExiting...")

:
```

Output:

```
Enter 'q' to quit.
Enter username: user1
Enter password: pass1

Enter 'q' to quit.
Enter username: user1
Enter password: pass2

Enter 'q' to quit.
Enter username: user1
Enter password: pass3
Alert: Possible intrusion detected for user user1!

Enter 'q' to quit.
Enter username: user2
Enter password: pass1

Enter 'q' to quit.
Enter username: user2
Enter password: pass2

Enter 'q' to quit.
Enter username: user2
Enter password: pass3
Alert: Possible intrusion detected for user user2!

Enter 'q' to quit.
Enter username: q

Exiting...
```

Area of Future Improvement

To further enhance the Intrusion Detection System (IDS) micro-project, several areas of future improvement can be considered. Firstly, implementing advanced authentication mechanisms such as multi-factor authentication (MFA) or biometric authentication could fortify the login process, augmenting the system's resilience against unauthorized access attempts. Secondly, integrating dynamic threshold adjustment based on user behavior analytics would enable the IDS to adaptively respond to evolving attack patterns, ensuring accurate intrusion detection while minimizing false positives. Additionally, the introduction of a real-time notification system capable of promptly alerting administrators or security personnel upon detecting suspicious login activity could expedite incident response and mitigation efforts. Furthermore, enhancing logging and reporting functionalities to capture comprehensive details of login attempts, including timestamps and IP addresses, would facilitate thorough forensic analysis and compliance reporting. Lastly, integrating the IDS with external threat intelligence feeds could provide valuable insights into emerging threats, enabling proactive threat mitigation and strengthening the overall security posture of the system.

Application of this Micro-Project

The Intrusion Detection System (IDS) micro-project finds applications across various domains where cybersecurity is paramount. In corporate environments, IDS can safeguard sensitive data and critical infrastructure by detecting and mitigating unauthorized access attempts, malware infections, and network intrusions. In the financial sector, IDS plays a crucial role in protecting customer assets and preventing fraud by monitoring for suspicious activities and fraudulent transactions. Within government agencies, IDS aids in safeguarding national security interests by detecting and thwarting cyber attacks aimed at disrupting government operations or compromising sensitive information. Additionally, IDS can be utilized in healthcare settings to ensure the confidentiality and integrity of patient data, mitigating the risk of data breaches and unauthorized access to medical records. Overall, the IDS micro-project serves as a versatile tool in safeguarding digital assets, preserving data integrity, and maintaining the security posture of organizations across various industries.

Skill Developed/ learning out of this Micro-Project

Through the development and implementation of the Intrusion Detection System (IDS) micro-project, several skills and learning outcomes can be attained. Firstly, participants gain proficiency in Python programming, including concepts such as classes, methods, conditional statements, and loops. Additionally, they develop a deeper understanding of cybersecurity principles, including threat detection, incident response, and intrusion prevention. Moreover, participants enhance their problem-solving and critical thinking abilities by devising algorithms to detect and respond to suspicious login attempts effectively. Furthermore, the micro-project fosters collaboration and teamwork skills as participants may collaborate on designing, testing, and refining the IDS solution. Lastly, participants gain practical experience in software development methodologies, including requirements analysis, design, implementation, testing, and deployment, which are transferable to various other programming projects and real-world applications.

Conclusion:

In conclusion, the Intrusion Detection System (IDS) micro-project serves as a valuable learning opportunity for participants to develop essential skills in Python programming and cybersecurity. By implementing an IDS solution capable of detecting and responding to suspicious login attempts, participants gain hands-on experience in software development, problem-solving, and critical thinking. Moreover, the micro-project enables participants to deepen their understanding of cybersecurity principles, including threat detection, incident response, and intrusion prevention. Through collaboration and teamwork, participants refine their communication and collaboration skills while working towards a common goal. Overall, the IDS micro-project equips participants with practical experience and knowledge that are transferable to various programming projects and real-world cybersecurity challenges, empowering them to contribute effectively to the field of cybersecurity.

Reference

- **https://www.cybersecurityhub.com/introduction-to-cybersecurity**
- **https://www.ibm.com/topics/intrusion-detection-system#:~:text=An%20intrusion%20detection%20system%20(IDS)%20is%20a%20network%20security%20tool,activity%20or%20security%20policy%20violations.**
- **https://www.geeksforgeeks.org/intrusion-detection-system-ids/**