Project Title: Network Anomaly Detection Using AI

Overview:

- Creating an AI-powered network anomaly detection system entails applying machine learning or AI algorithms to detect deviations or abnormalities in network activity.

- Collect network data such as traffic patterns, packet information, logs, and other network activity data. This data is used to train and test the anomaly detection system.

- The acquired data should be cleaned and preprocessed. This may entail reducing noise, standardizing data formats, dealing with missing values, and translating data into a format suited for machine learning algorithms.

- Determine the key features that will be used for anomaly detection. This might entail extracting useful information from raw data or picking the most important features to define network activity.

- Select the best AI model or algorithm for anomaly detection. Unsupervised learning (e.g., clustering, autoencoders), supervised learning (e.g., classification), and even deep learning approaches (e.g., neural networks) might be included.

- Use labeled or unlabeled data to train the chosen model (based on supervised or unsupervised learning). To guarantee that the model learns to discriminate between anomalies and typical network behavior, the training dataset should include an acceptable representation of both.

- Evaluate the AI model's performance using validation data or techniques such as cross-validation. This stage determines the model's accuracy, precision, recall, and F1 score in identifying anomalies.

- Implement tools to adapt to changing network behaviors and update the AI model on a regular basis. Continuous improvement is required to keep the anomaly detection system accurate and effective.

- Anomaly detection should be combined with suitable security measures and reaction mechanisms. When an anomaly is found, the system should initiate appropriate steps, such as alerting, blocking suspicious traffic, or commencing incident response processes.

- Completely document the project, including methodology, models utilized, results, and any findings or insights received. Regular reports highlighting the system's performance and any notable results should be generated.

List of teammates:

S.no	Name	Collage	Contact
1	Karthik G	VIT Vellore	9342706587
2	Vasan	VIT	93472 28869
3	Rohit	VIT	91766 17809
4	Prince Levin	VIT	79937 60310

List of Vulnerability Table:

S.no	VulnerabilityName	CWE - No
1	SQL Injection	CWE-89
2	Cross-Site Scripting (XSS)	CWE-79
3	Remote Code Execution	CWE-94
4	Insecure Direct Object References (IDOR)	CWE-639
5	Man-in-the-Middle (MitM) Attack	CWE-300

Report:

1. Vulnerability Name: SQL Injection

CWE (Common Weakness Enumeration): CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

OWASP Category: OWASP Top 10 - A1: Injection

Description:

SQL Injection is a type of security vulnerability that occurs when an attacker can insert malicious SQL code into a query via an application's input data, potentially allowing unauthorized access to the database. If unmitigated, this vulnerability can lead to the exposure, alteration, or deletion of sensitive data.

Business Impact:

The potential impact of a successful SQL injection attack can be severe. It can lead to unauthorized access to sensitive information, including customer data, financial records, and other confidential information. This could result in data breaches, financial loss, damage to reputation, legal repercussions, and disruption of services or operations.

2. Vulnerability Name:
Cross-Site Scripting (XSS)

CWE (Common Weakness Enumeration): CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

OWASP Category: OWASP Top 10 - A7: Cross-Site Scripting (XSS)

Description:

Cross-Site Scripting (XSS) is a type of security vulnerability that enables attackers to inject malicious scripts into web pages viewed by

other users. This vulnerability occurs when an application fails to properly sanitize user-supplied input, allowing the injection of scripts (usually in the form of HTML or JavaScript) into web pages.

Business Impact:

If exploited, XSS vulnerabilities can lead to a range of consequences, including the theft of session cookies, website defacement, unauthorized access to sensitive data, and the potential for executing arbitrary code within users' browsers. The impact can include compromised user accounts, reputation damage, and exposure of confidential information, leading to legal and compliance issues for the affected organization.

3. Vulnerability Name: Remote Code Execution (RCE)

CWE (Common Weakness Enumeration): CWE-94: Improper Control of Generation of Code ('Code Injection')

OWASP Category: Not listed in OWASP Top 10 but considered highly critical.

Description:

Remote Code Execution (RCE) is a severe vulnerability that allows attackers to execute arbitrary code on a target system from a remote location. This vulnerability often occurs due to improper input validation or lack of proper security measures in an application or system. Successful exploitation could grant an attacker unauthorized access, enabling the execution of commands and potentially taking over the affected system.

Business Impact:

RCE vulnerabilities pose a significant threat, allowing attackers to gain complete control over a system or application. The impact can range from unauthorized access to sensitive data, disruption of services, installation of malware, theft of intellectual property, and potential system compromise. The consequences could lead to severe financial loss, reputational damage, legal liabilities, and significant operational

disruption. Immediate mitigation is crucial to prevent exploitation and limit potential damage.

4. Vulnerability Name:
Insecure Direct Object References (IDOR)

CWE (Common Weakness Enumeration): CWE-639: Authorization Bypass Through User-Controlled Key

OWASP Category: OWASP Top 10 - A4: Insecure Direct Object References

Description:

Insecure Direct Object References (IDOR) occur when an application exposes internal implementation objects, such as files or database keys, in a way that allows attackers to manipulate references to gain unauthorized access to sensitive data. This vulnerability typically arises from a lack of proper authorization checks, allowing attackers to access resources they are not authorized to access.

Business Impact:

IDOR vulnerabilities can lead to unauthorized access to sensitive data, such as personally identifiable information, financial records, or proprietary data. Exploitation of IDOR could result in data breaches, privacy violations, loss of confidential information, regulatory non-compliance, and reputational damage for the organization. Mitigation involves proper access controls and comprehensive authorization checks to prevent unauthorized access to sensitive resources.

5. Vulnerability Name:
Man-in-the-Middle (MitM) Attack

CWE (Common Weakness Enumeration): CWE-300: Channel Accessible by Non-Endpoint

OWASP Category: Not listed in OWASP Top 10 but considered a

critical network security threat.

Description:

A Man-in-the-Middle (MitM) attack occurs when an attacker intercepts communication between two parties without their knowledge. The attacker can eavesdrop on, alter, or even impersonate the legitimate parties, leading to potential data theft, session hijacking, or other unauthorized actions.

Business Impact:

MitM attacks can lead to severe consequences, including the compromise of sensitive information (such as login credentials, financial data, or confidential communications), unauthorized access to secure networks, and manipulation of data in transit. This can result in breaches of privacy, financial loss, damaged reputation, and legal issues. Implementing encryption, using secure communication protocols, and regularly monitoring for unusual network activities are essential to mitigate the risks associated with MitM attacks.

Thank You!