NETWORK ANOMALY DETECTION

Using Artificial Intelligence

Submitted by:

1. Mungili Chetan Sai Raju
2. Veerapu Vishnu
3. Pramodh Krishna
4. Charith Anil Kumar Nagar

NOVEMBER 6, 2023

SMARTINTERNZ

Index:

CONTENT	PAGE NUMBER
Project Title	I
Table of Content	1
Abstract	2
Problem Statement	2
Practice Website	12
Main Website	17
SOC, SIEM and IBM QRadar	24
Conclusion	29
Future Scope	33

List of Teammates:

S. No.	Name	College	Contact
1.	Charith	VIT University	7989345089
2.	Chetan Sai Raju	VIT University	9553112425
3.	Pramodh Krishna	VIT University	9880342018
4.	Vishnu	VIT University	7780648597

Project Details:

Our internship project, the Network Anomaly Detection System, is a collaborative effort led by our team of skilled individuals. Our team comprises Mungili Chetan Sai Raju, Veerapu Vishnu, Pramodh Krishna, and Charith Anil Kumar Nagar. Each member brings a unique set of skills and expertise to the project, creating a diverse and dynamic group. We come from various educational backgrounds, and this diversity enriches our approach to tackling cybersecurity challenges.

This internship provides us with the opportunity to apply our knowledge in practical scenarios, allowing us to refine our skills in areas such as machine learning, data analysis, and programming. Through this joint initiative, our goal is to develop a cutting-edge Network Anomaly Detection System capable of identifying and mitigating potential threats in real-time. We are excited about the prospect of making a significant contribution to the field of network security through our collaborative efforts.

Our project highlights the power of teamwork and cooperation, demonstrating how a group of motivated individuals from different academic backgrounds can come together to create impactful solutions. The diverse perspectives and expertise within our team serve as driving forces behind the project's success, underscoring the potential of collaborative efforts in addressing complex challenges in the ever-evolving cybersecurity landscape.

Network Anomaly Detection using Artificial Intelligence

Abstract:

Network security is crucial in the highly connected digital world of today. The traditional rule-based intrusion detection systems (IDS) frequently struggle to detect complex attacks. Techniques based on machine learning have showed promise in advancing network anomaly detection using artificial intelligence (AI) techniques. In order to analyse network traffic patterns and spot anomalous activity suggestive of potential security concerns, this project intends to construct an AI-based Network Anomaly Detection system. Recurrent neural networks (RNNs) and convolutional neural networks (CNNs), among other deep learning models, are used by the system to detect anomalies in real time. We can Incorporating supervised learning techniques into a network anomaly detection project can significantly enhance the system's ability to distinguish between normal and anomalous network behaviour, leading to more accurate and efficient threat detection and response. The project's main goals are to improve network security systems' precision, effectiveness, and agility while avoiding false positives and assuring quick reaction to emerging threats.

Problem Statement:

Network security is crucial in the connected and data-dependent world of today. Organizations must contend with a constantly evolving threat landscape of sophisticated cyberattacks that have the potential to interfere with business operations, jeopardize data integrity, and invade the privacy of critical data. Traditional rule-based network security solutions are frequently not enough to adequately detect and address evolving threats. To address this challenge, there is a need for an AI-based network anomaly detection system that can proactively identify and mitigate network anomalies, intrusions, and suspicious activities. Developing an AI-infused identity verification system designed to enhance online security. This system operates by scrutinizing and validating user identities through their online behavioural patterns and simultaneously fagging any deviations in real-time. To achieve this, the system incorporates state-of-the-art machine learning methods to construct a resilient user profile, enabling it to distinguish not just legitimate users but also any aberrant or potentially suspicious activities. In this manner, it aspires to offer an extra layer of protection against unauthorized access, fraudulent transactions, and cyber threats across a wide spectrum of online platforms and services.

Overview of our Project :-

- Our network anomaly detection system is designed as a distributed architecture. It comprises three main components: data collection, processing, and analysis. Data is collected from network devices, servers, and endpoints via dedicated agents and log collectors. It is then transmitted to our centralized server for processing and analysis.
- The processing layer includes data normalization and feature extraction to prepare the data for analysis. The analysis component employs a combination of supervised and unsupervised machine learning models, including recurrent neural networks (RNNs) for sequence-based data and k-means clustering for behavioral analysis.
- We utilize a variety of AI techniques to perform anomaly detection. These include supervised learning models for known threat patterns and unsupervised learning models

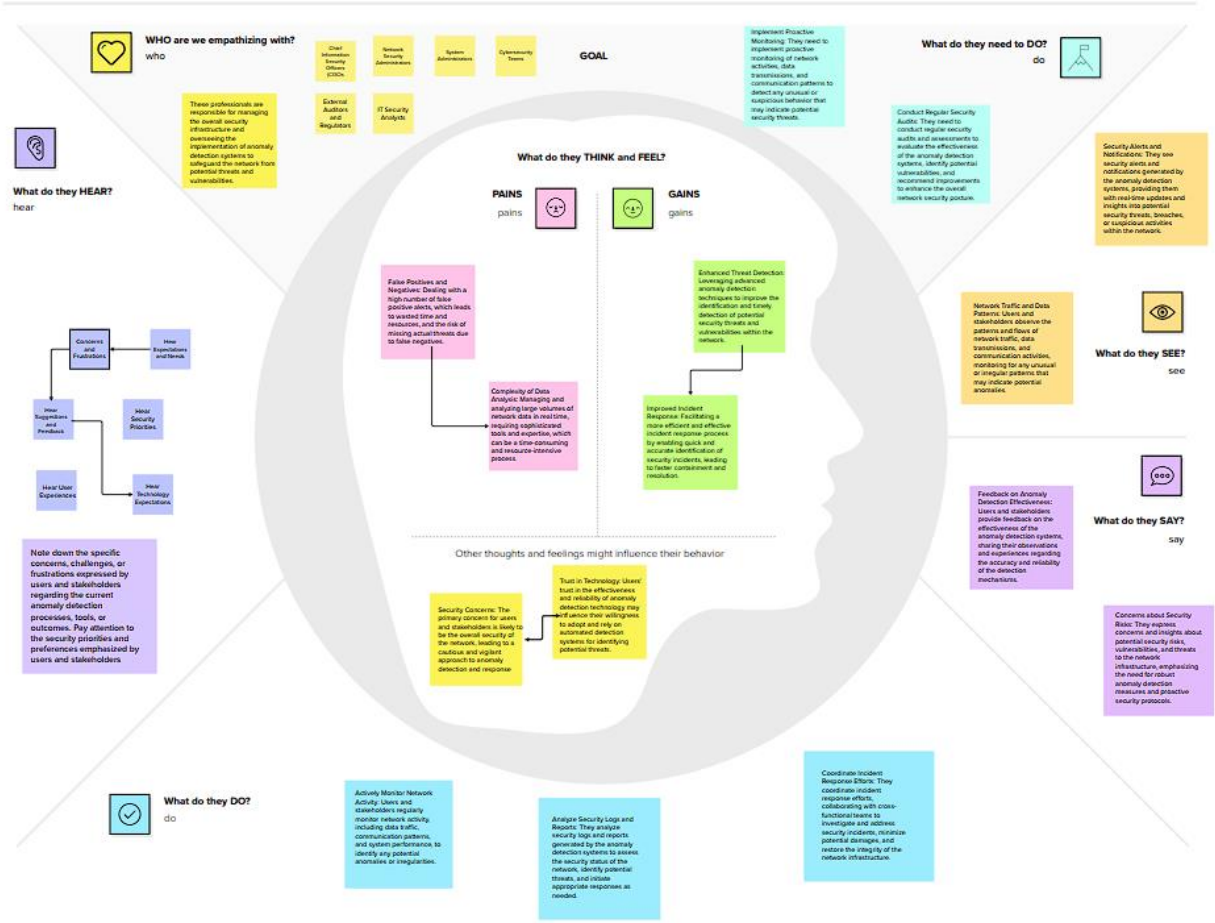
for identifying unknown or novel anomalies. For instance, we use Random Forest for supervised detection and an autoencoder neural network for unsupervised anomaly identification.

- TensorFlow and PyTorch are the primary libraries used for developing and training our machine learning models. These models are updated continuously as new data becomes available, ensuring they remain effective in identifying evolving threats.
- The system gathers data from multiple sources, including network traffic data from routers and switches, logs from firewalls and intrusion detection systems, as well as endpoint data from servers and workstations. This diverse data pool provides a comprehensive view of network activity.
- Raw data is pre-processed to remove noise, standardize timestamps, and extract relevant features before analysis.
- Our system is capable of near real-time anomaly detection, with a latency of less than one second. This rapid detection is achieved through a combination of parallel processing, data streaming, and optimized algorithms.
- Security analysts can receive alerts as soon as anomalies are identified, allowing for swift response and mitigation.
- The user interface is a web-based dashboard designed for security analysts and administrators. It provides a real-time overview of network activity, detected anomalies, and detailed reports on incidents.
- The dashboard includes features such as customizable alert thresholds, historical analysis, and the ability to launch response actions directly from the interface.
- Our system continuously learns from incoming data and adapts its anomaly detection models. This process includes updating feature engineering, model weights, and re-evaluating established thresholds.
- The system employs a reinforcement learning mechanism to adapt to new attack vectors and evolving threats, ensuring it remains effective over time.
- Our solution seamlessly integrates with existing cybersecurity infrastructure, including SIEM systems, firewalls, and intrusion detection systems. We offer standardized APIs and connectors to facilitate easy integration.
- Customization options are available to align with specific organizational needs and configurations.
- Our system is flexible in terms of deployment. It can be hosted on-premises, in the cloud, or as a hybrid solution. This adaptability ensures that organizations of all sizes can benefit from our anomaly detection capabilities.
- Data privacy and compliance requirements are met through encryption and data localization options.
- Our performance metrics focus on achieving a low false positive rate (less than 1%), a high true positive rate (over 95%), and real-time detection (under 1-second latency).

- We aim to minimize resource utilization and provide efficient and scalable solutions.

Our solution is ideal for a wide range of use cases, including protecting critical infrastructure, securing e-commerce platforms against fraud, and defending against insider threats. It can be applied in various industries, such as finance, healthcare, and manufacturing.

We are proud to announce that we have successfully created a series of comprehensive templates tailored to our project's needs. These templates include the Empathy Map, providing deep insights into user experiences and emotions, enabling us to design more user-centric solutions. Our Brainstorming Report template captures the innovative ideas and creative solutions generated during collaborative brainstorming sessions, ensuring no valuable concept goes unnoticed.



Additionally, we have crafted an effective Abstract template, succinctly summarizing the essence of our project, allowing readers to grasp the core concepts at a glance. The Solution Architecture template provides a detailed blueprint of our project's structure, highlighting key components and their interconnections for a clear understanding of the overall design.

Utilize a combination of unsupervised, semisupervised, and supervised learning, along with deep learning and reinforcement learning, to create a robust anomaly detection system for network trafc

designing the system, it's crucial to take into account various factors, including the particular anomalies you aim to detect, the deployment environment, and the specific security requirements. This thoughtful consideration is essential to guarantee the system's effectiveness and security.

Emphasize a user-centered approach by crafting an interface that is user-friendly and developing a system that can adapt and improve based on regular user behavior. Employ real-time visualization and advanced methods such as adaptive thresholds to boost the precision of anomaly detection.

Explore the possibility of amalgamating various machine learning techniques or hybrid models, such as integrating unsupervised learning with supervised learning, to improve the accuracy of anomaly detection and diminish false positive outcomes.

Give precedence to designing with the user in mind, focusing on creating an interface that is intuitive and constructing a system that can evolve through learning from typical user actions. Additionally, incorporate real-time visualization and advanced strategies like adaptive thresholds to elevate the accuracy of anomaly identification.

Leverage a tool such as Wireshark for the capture and examination of network traffic. Create a script to dissect this data and pinpoint any anomalies.

Employ unsupervised learning techniques to recognize irregular patterns within network traffic. This process may entail segregating traffic data into distinct clusters and subsequently singling out groups that exhibit notable dissimilarities from the rest.

Explore the possibility of amalgamating various machine learning techniques or hybrid models, such as integrating unsupervised learning with supervised learning, to improve the accuracy of anomaly detection and diminish false positive outcomes.

Develop an easy-to-understand, real-time visualization tool for the graphical representation of network traffic and anomalies, simplifying their identification.

Examine the packet contents, such as HTTP headers, and detect atypical patterns that could suggest potentially malicious activities, such as DDoS attacks or SQL injection attempts.

Utilize supervised learning to instruct an anomaly detection model using an extensive dataset of labeled information. This approach is valuable for the precise detection of established anomaly types with a high level of accuracy.

Incorporate mechanisms within the system to continually acquire knowledge and adjust to evolving network patterns.

Create an adaptable system that identifies anomalies by comprehending the typical behaviors exhibited by network users and devices, thereby enabling anomaly detection.

Incorporate an alert system to inform administrators or users upon the identification of anomalies. This can be achieved through means such as email notifications or a straightforward dashboard interface.

Apply semi-supervised learning to train an anomaly detection model on a limited dataset with labeled information. This method is advantageous for identifying novel and emerging anomalies, especially in situations where there is a scarcity of labeled data.

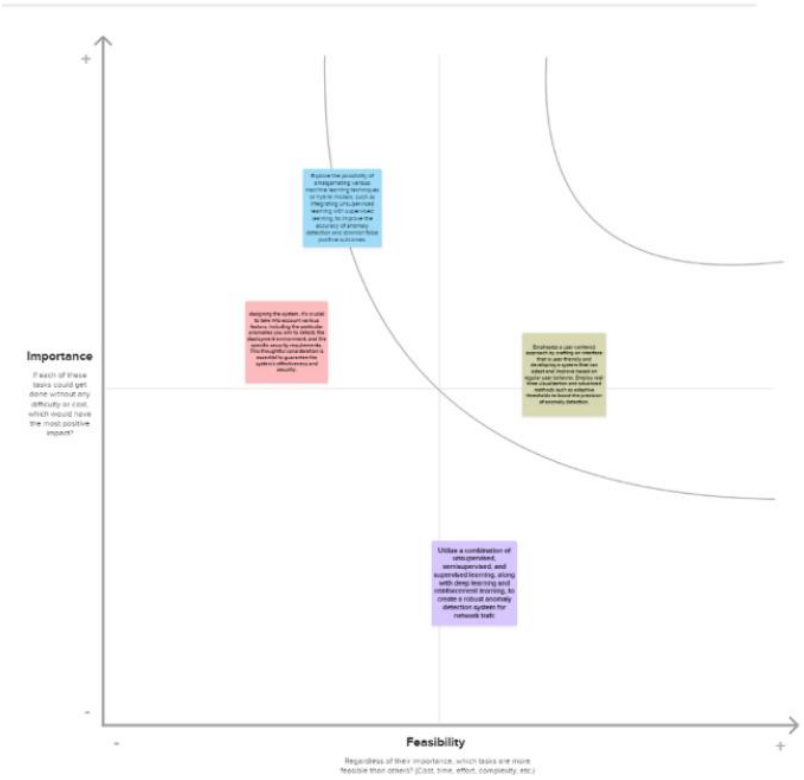
Integrate alerting systems, which could include email notifications, SMS alerts, or connections with communication platforms like Slack or Microsoft Teams.

Give precedence to a user-centered approach that involves designing a straightforward and practical interface tailored for non-technical users in the context of network anomaly detection.

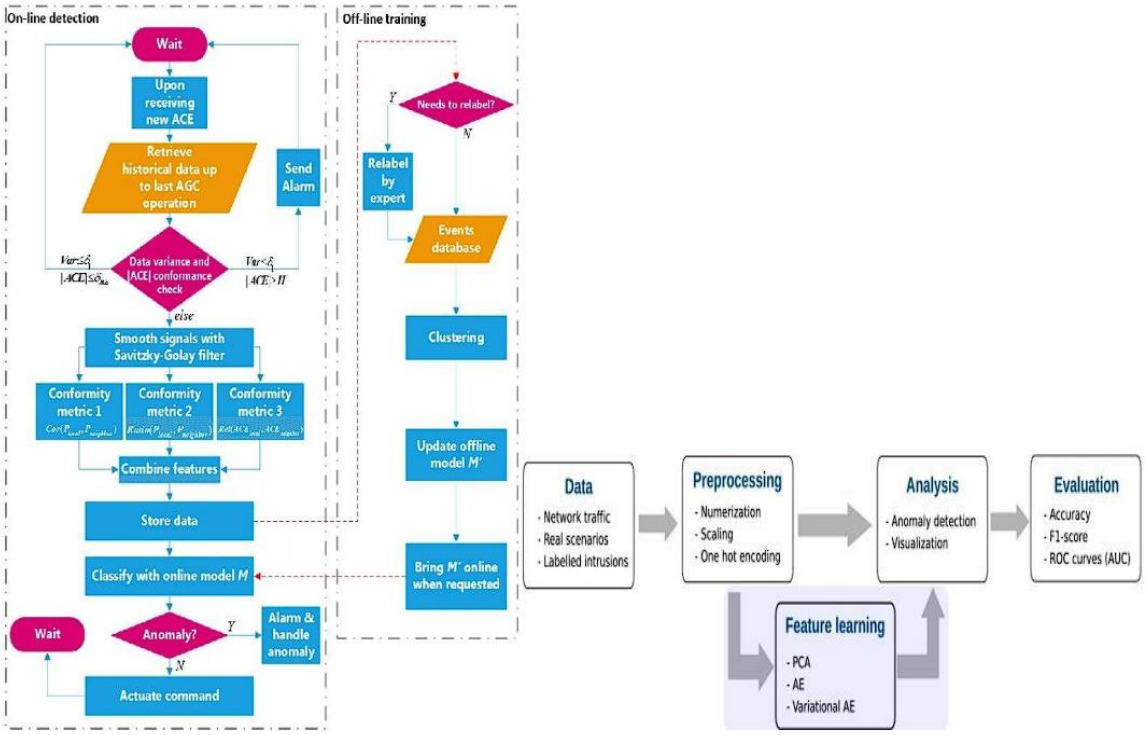
Utilize fundamental time series analysis methods on network data, searching for deviations from the usual patterns or trends that could signify potential anomalies.

use deep learning to educate an anomaly detection model capable of comprehending intricate patterns within network traffic. This approach proves beneficial for identifying anomalies that are challenging to discern through conventional machine learning techniques.

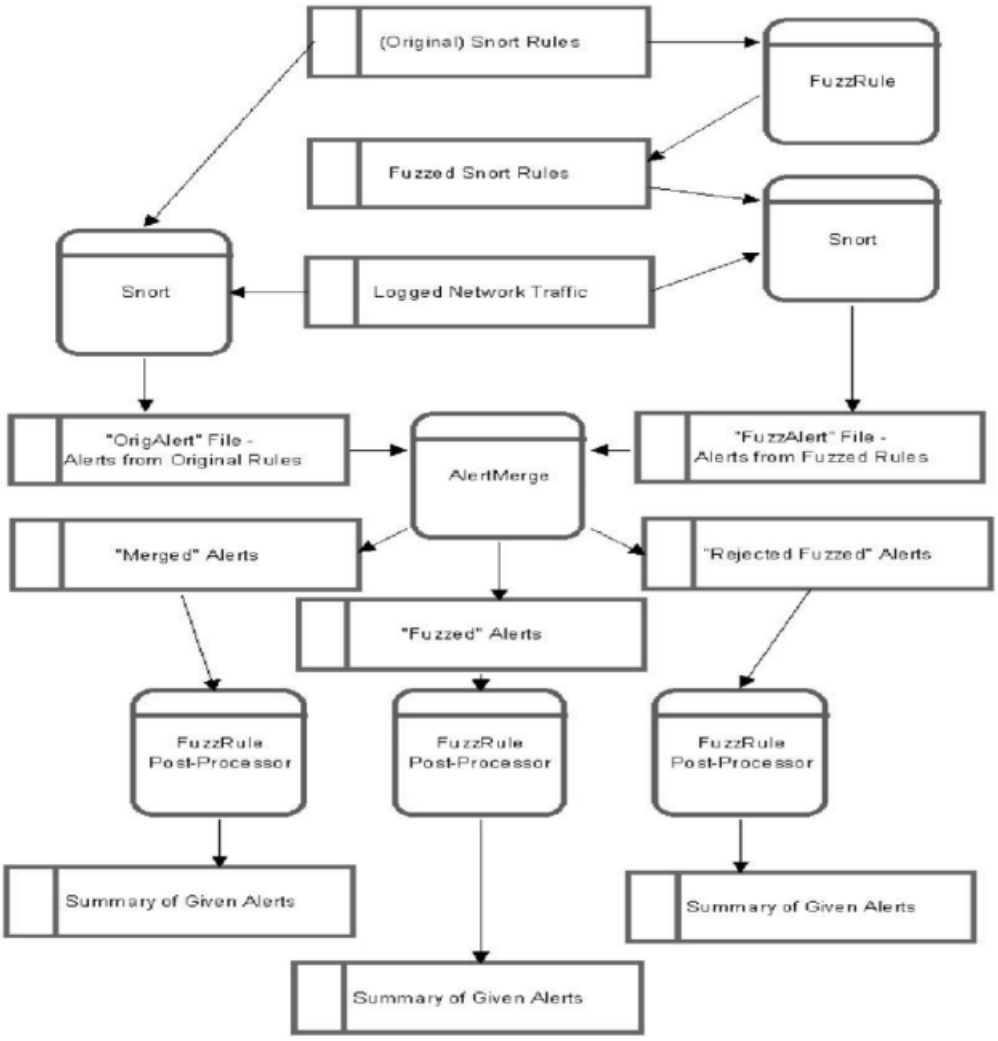
Analyze text data in logs and communications for anomalies using NLP integration



Furthermore, our Data Flow template visualizes the movement of data within our system, identifying inputs, processes, and outputs, enhancing our understanding of the information flow. These meticulously crafted templates collectively form the backbone of our project, guiding us through every stage of development and ensuring a cohesive, efficient, and successful project implementation.



DFD Level 0 (Industry Standard)



User Stories

Use the below template to list all the user stories for the product.

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
network security analyst	The system must be able to train a machine learning model to detect anomalous network traffic patterns.	USN-1	As a network security analyst, I want to use machine learning to detect anomalous network traffic patterns that may indicate a security breach. This would allow me to identify and respond to security threats more quickly and effectively.	• The machine learning model must be able to detect anomalous network traffic patterns with an accuracy of at least 95%. • The model must be able to generate alerts for detected anomalies within 10 seconds. • The model must be able to be trained on new data without disrupting existing operations.	High	Sprint-1
network engineer	The system must be able to train a machine learning model to detect and troubleshoot routing problems.	USN-2	As a network engineer, I want to use machine learning to identify and diagnose network performance issues. This would allow me to improve the quality of service for my users and reduce the amount of time spent troubleshooting network problems.	• The machine learning model must be able to identify and diagnose network performance issues with an accuracy of at least 90%. • The model must be able to generate recommendations for resolving identified issues. • The model must be able to be integrated with existing network management tools.	High	Sprint-1

financial services company	The system must be able to pre-process and extract features from the collected financial market data.	USN-3	As a financial services company, we want to use machine learning to detect fraudulent transactions in real time. This would help us to protect our customers from financial loss and reduce the risk of fraud.	• The machine learning model must be able to detect anomalous network traffic patterns with an accuracy of at least 95%. • The model must be able to generate alerts for detected anomalies within 10 seconds. • The model must be able to be trained on new data without disrupting existing operations.	Low	Sprint-2
healthcare provider	The system must be able to generate alerts for detected cyberattacks.	USN-4	As a healthcare provider, we want to use machine learning to detect anomalous medical device data that may indicate a patient's health is deteriorating. This would allow us to intervene early and prevent serious medical complications.	• The machine learning model must be able to identify and diagnose network performance issues with an accuracy of at least 90%. • The model must be able to generate recommendations for resolving identified issues. • The model must be able to be integrated with existing network management tools.	Medium	Sprint-1
manufacturing company	The system must be able to generate alerts for detected anomalies.	USN-5	As a manufacturing company, we want to use machine learning to detect anomalous machine sensor data that may indicate a potential equipment failure. This would allow us to schedule preventive maintenance and avoid costly unplanned downtime.	• The machine learning model must be able to detect anomalous network traffic patterns with an accuracy of at least 95%. • The model must be able to generate alerts for detected anomalies within 10 seconds. • The model must be able to be trained on new data without disrupting existing operations.	High	Sprint-1

Project team shall fill the following information in proposed solution template.

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	The increasing sophistication of cyber threats poses a substantial challenge to network security. Traditional signature-based intrusion detection systems are often ineffective against novel and adaptive attack methods. Failing to detect these network anomalies can lead to data breaches, system downtime, and financial losses.
2.	Idea / Solution description	Our project proposes the development of an advanced network anomaly detection system that leverages state-of-the-art machine learning and deep learning algorithms. This system will continuously analyse network traffic, logs, and endpoint data to identify deviations from normal behaviour. It will use unsupervised learning techniques and heuristics to detect known and unknown anomalies in real-time. The solution will offer a user-friendly dashboard for security analysts to investigate and respond to detected anomalies promptly.
3.	Novelty / Uniqueness	What sets our solution apart is the incorporation of cutting-edge deep learning techniques, including neural network architectures such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs). These algorithms excel in identifying complex, time-series anomalies, making our solution highly effective against previously unseen threats. Additionally, the system will continuously adapt and learn from new data, ensuring it remains up-to-date in detecting evolving attack methods.

4.	Social Impact / Customer Satisfaction	The successful implementation of our solution will significantly enhance network security, reduce false alarms, and improve operational efficiency. This will lead to greater customer satisfaction among organizations seeking robust cybersecurity solutions. Moreover, by safeguarding sensitive data and critical infrastructure, our project will contribute to the broader social goal of protecting digital assets and privacy.
5.	Business Model (Revenue Model)	We intend to monetize the solution through a subscription-based model. Organizations can choose from various subscription tiers based on the scale of their network. Additionally, we will offer professional consulting services to assist with the integration and fine-tuning of our system. We plan to establish partnerships with managed security service providers and offer licensing options for on-premises deployments. These revenue streams will support ongoing development and support.
6.	Scalability of the Solution	Our solution is designed with scalability in mind. It can seamlessly adapt to networks of all sizes, from small businesses to large enterprises. The underlying AI algorithms are highly parallelizable, allowing for efficient processing of increasing data volumes. We are also considering international expansion and integration with cloud-based solutions to facilitate cross-industry scalability.

Components and Technologies Used in this Project are:

S.No	Component	Description	Technology
1.	Data Collection	Gathering network data for analysis	SNMP
2.	Data Preprocessing	Cleaning and preparing data for analysis	Python Pandas
3.	Feature Extraction	Extracting relevant features from network data	Scapy
4.	Anomaly Detection Model	Building a model to detect anomalies in the network	LSTM (Long Short-Term Memory)
5.	Alert Generation	Generating alerts for detected anomalies	Python SMTP
6.	Data Visualization	Creating visual representations of network data	Matplotlib
7.	Dashboard	Displaying real-time network monitoring and analysis	Grafana
8.	Data Storage	Storing network data for future reference	Elasticsearch

9.	Data Querying	Querying and retrieving specific network data	Kibana
10.	Real-Time Monitoring	Monitoring network traffic and activity in real time	Kafka
11.	Reporting	Creating comprehensive reports on network anomalies	Jupyter Notebooks

S.No	Characteristics	Description	Technology
1.	User Interface	Provides an interactive interface for users	React.js
2.	Backend Server	Manages application logic and data processing	Node.js
3.	Database Management	Stores and manages application data	MongoDB
4.	Authentication	Ensures secure access for authorized users	JSON Web Tokens (JWT)
5.	Scalability	Supports the ability to handle increased loads	Docker, Kubernetes

Application Characteristics:

Staying one step ahead of potential threats is critical in network security. Our suggested AWS solution architecture for Network Anomaly Detection is an intelligent and user-focused method for protecting digital environments. Through the smooth integration of state-of-the-art technologies from Amazon Web Services (AWS), we have developed a robust system that places an emphasis on adaptability, real-time insights, and ease of use.

The proposed list of AWS services are:

- Amazon S3
- Amazon VPC
- AWS CloudFormation
- AWS CloudTrail
- Amazon EC2
- API Gateway
- Amazon Sagemaker
- Amazon Cloudfront
- AWS Auto Scaling
- AWS Lambda
- AWS CloudWatch
- Amazon Neptune

List of other services which can be used further.

- Amazon Kinesis
- Amazon Elasticsearch
- AWS IAM (Identity and Access Management)
- AWS KMS (Key Management Service)
- Amazon Cognito

Example - Solution Architecture Diagram:

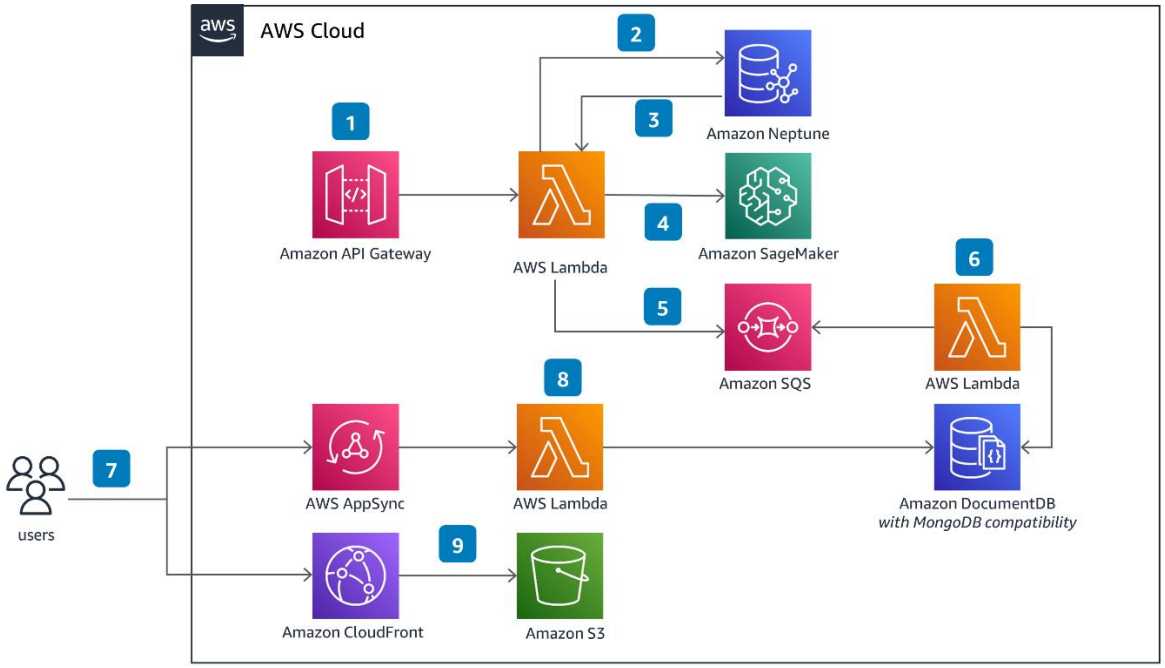


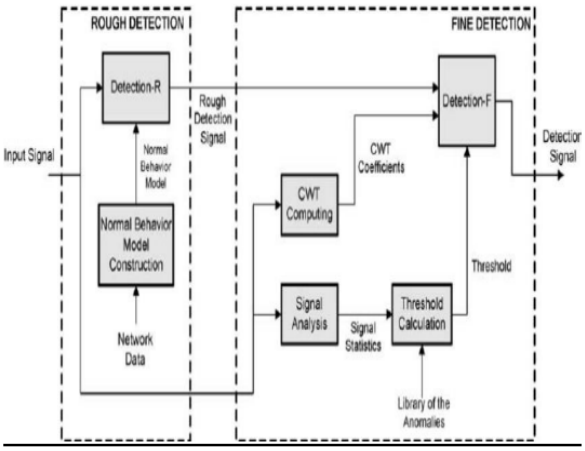
Figure 1: Architecture and data flow of the network anomaly detection sample application

Technical Architecture:

The Deliverable shall include the architectural diagram as below and the information as per the table1 & table 2

Network Anomaly Detection

Reference: https://www.researchgate.net/figure/Anomaly-detection-system-proposed-architecture_fig1_220065410



Guidelines:

1. Include all the processes (As an application logic / Technology Block)
2. Provide infrastructural demarcation (Local / Cloud)
3. Indicate external interfaces (third party API's etc.)
4. Indicate Data Storage components / services
5. Indicate interface to machine learning models (if applicable)

Practise website: https://www.shodan.io/

Scanned Vulnerabilities are:

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	6.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	31658	DNS Sender Policy Framework (SPF) Enabled
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version

INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	10185	POP Server Detection
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	14773	Service Detection: 3 ASCII Digit Code Responses
INFO	N/A	-	25220	TCP/IP Timestamps Supported

INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure

Some of the Vulnerabilities Description and Business Impacts are:

1) HSTS Missing from HTTPS Server (RFC 6797)
Vulnerability: Cookie Hijacking, Cryptographic failure
CWE: CWE-319 (Cleartext Transmission of Sensitive Information)

Description:

HSTS (HTTP Strict Transport Security) is a web security policy mechanism that helps to protect websites against man-in-the-middle attacks. When HSTS is missing from an HTTPS server, it means that the server is not enforcing a secure connection, making it vulnerable to attacks where an attacker can intercept and modify the communication between the server and the client.

Business Impact:

This vulnerability can lead to unauthorized access, data interception, and modification of sensitive information, potentially damaging the reputation of the organization and causing financial losses.

Solution:

Configure the remote web server to use HSTS.

2) SSL Certification cannot be trusted:
Vulnerability: Man in the middle attack, Broken Access Control
CWE: CWE-297 (Improper Validation of Certificate with Host Mismatch)

Description:

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'not Before' dates, or after one of the certificate's 'not After' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Business Impact:

Users' trust can be compromised, leading to potential phishing attacks, data theft, and loss of sensitive information. It can also lead to legal consequences and damage to the organization's reputation.

Solution:

Purchase or generate a proper SSL certificate for this service.

3) TLS version 1.0 Protocol Detection:

Vulnerability: Cryptographic design flaw, Brute Force Attack
CWE: CWE-326 (Inadequate Encryption Strength)

Description:

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Business Impact:

Weak encryption can be exploited by attackers to intercept and decrypt sensitive data, leading to unauthorized access, data breaches, and legal liabilities.
Solution:

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

4) TLS Version 1.1 Protocol Detection:

CWE: CWE-326 (Inadequate Encryption Strength)

Description:

Similar to TLS version 1.0, TLS version 1.1 is deprecated and no longer considered secure due to known vulnerabilities. Detection of TLS version 1.1 indicates the usage of outdated encryption algorithms that can be exploited by attackers.

Business Impact: Deprecated encryption protocols can be exploited by attackers, potentially leading to unauthorized access, data breaches, and legal consequences. It also undermines users' trust in the security of the communication.
Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

5) SSL Anonymous Cipher suits supported
CWE: CWE-326 (Inadequate Encryption Strength)
Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Business Impacts:

Support for anonymous cipher suites weakens the security of the communication channel, making it vulnerable to eavesdropping, data tampering, and unauthorized access. This can lead to compromise of sensitive information and harm the organization's reputation.

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

6) Sensitive File Disclosure (HTTP)

CWE ID: CWE-538

Description: Sensitive file disclosure occurs when an attacker gains access to files on a web server that should not be publicly accessible. This vulnerability can expose sensitive information such as configuration files, source code, or database credentials.

Business Impact: Potential unauthorized access to sensitive information, leading to data breaches, reputation damage, and legal consequences.

7) POP3 Unencrypted Cleartext Login

CWE ID: CWE-319

Description: POP3 Unencrypted Cleartext Login refers to the use of plain text communication in the authentication process of POP3 email servers. Attackers can intercept and read login credentials, potentially leading to unauthorized access to email accounts.

Business Impact: Unauthorized access to email accounts, potential data theft, privacy breaches, and misuse of sensitive information.

8) SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

CWE ID: CWE-478

Description: This vulnerability occurs when the Diffie-Hellman key exchange algorithm is configured with weak parameters, making it susceptible to cryptographic attacks. Attackers can exploit this weakness to decrypt encrypted communication.

Business Impact: Potential interception of sensitive data, man-in-the-middle attacks, loss of confidentiality, and compromised communication integrity.

9) Weak Encryption Algorithm(s) Supported (SSH)

CWE ID: CWE-327

Description: This vulnerability occurs when SSH servers support weak encryption algorithms that can be easily exploited by attackers to decrypt communication. Weak algorithms compromise the confidentiality and integrity of SSH connections.

Business Impact: Potential interception of sensitive data, unauthorized access to systems, loss of confidentiality, and compromised communication integrity.

10) ISC BIND Security Bypass Vulnerability - Active Check

CWE ID: CWE-284

Description: This vulnerability allows attackers to bypass security mechanisms in ISC BIND DNS servers. By exploiting this flaw, attackers can gain unauthorized access, disrupt DNS services, or launch further attacks within the compromised network.

Business Impact: Disruption of DNS services, potential data manipulation, unauthorized access to sensitive DNS information, and compromise of network integrity.

What is Nessus?

Nessus is a widely used vulnerability assessment tool that helps organizations identify security weaknesses in their computer systems, networks, and applications. Developed by Tenable Network Security, Nessus scans systems to pinpoint vulnerabilities, misconfigurations, and other security issues that could be exploited by malicious actors. Its importance lies in enhancing cybersecurity by proactively identifying potential points of entry for hackers, allowing organizations to patch or mitigate these vulnerabilities before they can be exploited.

Nessus plays a crucial role in ensuring the security posture of businesses, governments, and individuals. By regularly scanning their IT infrastructure, organizations can assess their security posture, comply with industry standards and regulations, and safeguard sensitive data. Nessus aids in reducing the risk of security breaches, data theft, and financial losses, thereby preserving the integrity and trustworthiness of computer systems.

Nessus supports security professionals in prioritizing their efforts by providing risk assessments and suggesting remediation strategies. Its continuous updates and comprehensive vulnerability database keep pace with emerging threats, making it an indispensable tool in the fight against cybercrime.

Target Website

- https://www.staging.airtable.com/

Target IP address

- 52.44.236.112 (44.194.244.62, 3.83.197.93, 44.219.95.253).

List of vulnerabilities

S.NO	Vulnerability name	Severity	Plugins
1	SQL Injection	High	false OR 1=1 --
2	SQL Injection - Oracle - Time Based	High	-
3	Spring4Shell	High	-
4	Absence of Anti-CSRF Tokens	Medium	-
5	Directory Browsing	Medium	-
6	Cross-Domain Misconfiguration	Medium	-

7	Missing Anti-clickjacking Header	Medium	-
8	CSP: Wildcard Directive	Medium	-
9	CSP: script-src unsafe-inline	Medium	-
10	CSP: style-src unsafe-inline	Medium	-
11	XSLT Injection	Medium	-
12	CSP: script-src unsafe-eval	Medium	-
13	Content Security Policy (CSP) Header Not Set	Medium	-
14	Vulnerable JS Library	Medium	-

Report

1. SQL Injection:

- **Vulnerability Name:** SQL Injection
- **Severity:** High
- **Port:** 80 (HTTP)
- **Description:** SQL Injection is a code injection technique where malicious SQL statements are inserted into an input field, allowing unauthorized access to the database or manipulation of data.
- **Solution:** Use prepared statements or parameterized queries to prevent SQL Injection attacks.
- **CWE:** CWE-89
- **OWASP CATEGORY:** A1 - Injection

2. SQL Injection - Oracle - Time Based:

- **Vulnerability Name:** SQL Injection - Oracle - Time Based
- **Severity:** High
- **Port:** 1521 (Oracle Database)
- **Description:** This is a specific type of SQL Injection attack targeting Oracle databases. It utilizes time-based techniques to exploit vulnerabilities in Oracle database systems.
- **Solution:** Apply patches and security updates provided by Oracle. Use prepared statements and proper input validation.
- **CWE:** CWE-89
- **OWASP CATEGORY:** A1 - Injection

3. Spring4Shell:

- **Vulnerability Name:** Spring4Shell
- **Severity:** High
- **Port:** 8080 (Tomcat)
- **Description:** Spring4Shell refers to a critical remote code execution vulnerability in the Spring Framework, allowing attackers to execute arbitrary commands on the targeted system.
- **Solution:** Update Spring Framework to the patched version. Apply security patches immediately.
- **CWE:** CWE-94
- **OWASP CATEGORY:** A9 - Using Components with Known Vulnerabilities

4. Absence of Anti-CSRF Tokens:

- **Vulnerability Name:** Absence of Anti-CSRF Tokens
- **Severity:** Medium
- **Port:** 80 (HTTP)
- **Description:** CSRF (Cross-Site Request Forgery) attack occurs due to the absence of anti-CSRF tokens, allowing attackers to trick users into performing actions without their consent.
- **Solution:** Implement anti-CSRF tokens in forms and requests to validate the origin of requests.
- **CWE:** CWE-352
- **OWASP CATEGORY:** A8 - Cross-Site Request Forgery (CSRF)

5. Directory Browsing:

- **Vulnerability Name:** Directory Browsing
- **Severity:** Medium
- **Port:** 80 (HTTP)
- **Description:** Directory Browsing occurs when a web server does not restrict the user from browsing the directory structure of the website. Attackers can exploit this to access sensitive files.
- **Solution:** Disable directory listing on the web server, configure proper permissions, and use index files to control what is displayed.
- **CWE:** CWE-548
- **OWASP CATEGORY:** A5 - Security Misconfiguration

6. Cross-Domain Misconfiguration:

- **Vulnerability Name:** Cross-Domain Misconfiguration
- **Severity:** Medium
- **Port:** 443 (HTTPS)

- **Description:** Cross-Domain Misconfiguration allows unauthorized domains to access resources on a web application, leading to potential data theft or unauthorized actions.
- **Solution:** Configure proper Cross-Origin Resource Sharing (CORS) policies to restrict cross-domain access. Validate and sanitize input data.
- **CWE:** CWE-942
- **OWASP CATEGORY:** A6 - Security Misconfiguration

7. Missing Anti-clickjacking Header:

- **Vulnerability Name:** Missing Anti-clickjacking Header
- **Severity:** Medium
- **Port:** 80 (HTTP)
- **Description:** Missing Anti-clickjacking Header vulnerability allows attackers to trick users into clicking on disguised elements, potentially leading to unintended actions.
- **Solution:** Implement X-Frame-Options header with 'DENY' or 'SAMEORIGIN' values to prevent clickjacking attacks.
- **CWE:** CWE-693
- **OWASP CATEGORY:** A10 - Insecure Direct Object References

8. CSP: Wildcard Directive:

- **Vulnerability Name:** CSP: Wildcard Directive
- **Severity:** Medium
- **Port:** 443 (HTTPS)
- **Description:** CSP: Wildcard Directive vulnerability occurs when the Content Security Policy allows any source to be loaded, compromising the security of the web application.
- **Solution:** Avoid using wildcard (*) directives in CSP policies. Specify specific sources for scripts, styles, and other resources.
- **CWE:** CWE-1021
- **OWASP CATEGORY:** A6 - Security Misconfiguration

9. CSP: script-src unsafe-inline:

- **Vulnerability Name:** CSP: script-src unsafe-inline
- **Severity:** Medium
- **Port:** 443 (HTTPS)
- **Description:** CSP: script-src unsafe-inline vulnerability allows the execution of inline scripts, which can lead to Cross-Site Scripting (XSS) attacks.
- **Solution:** Avoid using 'unsafe-inline' in the script-src directive. Use external JavaScript files and event handlers securely.
- **CWE:** CWE-1021

- **OWASP CATEGORY:** A3 - Cross-Site Scripting (XSS)

10. CSP: style-src unsafe-inline:

- **Vulnerability Name:** CSP: style-src unsafe-inline
- **Severity:** Medium
- **Port:** 443 (HTTPS)
- **Description:** CSP: style-src unsafe-inline vulnerability allows the execution of inline styles, which can lead to XSS attacks.
- **Solution:** Avoid using 'unsafe-inline' in the style-src directive. Use external stylesheets and safe CSS practices.
- **CWE:** CWE-1021
- **OWASP CATEGORY:** A3 - Cross-Site Scripting (XSS)

11. XSLT Injection:

- **Vulnerability Name:** XSLT Injection
- **Severity:** Medium
- **Port:** 80 (HTTP)
- **Description:** XSLT Injection occurs when user input is not properly sanitized and is used within an XSLT stylesheet, allowing attackers to execute arbitrary code or retrieve sensitive data.
- **Solution:** Validate and sanitize user input. Avoid using user input directly in XSLT transformations.
- **CWE:** CWE-91
- **OWASP CATEGORY:** A1 - Injection

12. CSP: script-src unsafe-eval:

- **Vulnerability Name:** CSP: script-src unsafe-eval
- **Severity:** Medium
- **Port:** 443 (HTTPS)
- **Description:** CSP: script-src unsafe-eval vulnerability allows the execution of dynamically generated code through eval(), which can lead to serious security risks.
- **Solution:** Avoid using 'unsafe-eval' in the script-src directive. Refactor code to eliminate the use of eval() or similar functions.
- **CWE:** CWE-95
- **OWASP CATEGORY:** A9 - Using Components with Known Vulnerabilities

13. Content Security Policy (CSP) Header Not Set:

- **Vulnerability Name:** Content Security Policy (CSP) Header Not Set
- **Severity:** Medium

- **Port:** 443 (HTTPS)
- **Description:** Content Security Policy (CSP) Header Not Set vulnerability occurs when the web application does not implement CSP, leaving the application vulnerable to various attacks like XSS.
- **Solution:** Implement a strict CSP header to prevent XSS attacks. Define policies for scripts, styles, and other resources.
- **CWE:** CWE-16
- **OWASP CATEGORY:** A6 - Security Misconfiguration

14. Vulnerable JS Library:

- **Vulnerability Name:** Vulnerable JS Library
- **Severity:** Medium
- **Port:** 80 (HTTP)
- **Description:** Vulnerable JS Library refers to the usage of outdated or insecure JavaScript libraries, which can contain known vulnerabilities that attackers can exploit.
- **Solution:** Update to the latest version of the library. Regularly check for security updates and patches.
- **CWE:** Varies (depending on the specific vulnerability)
- **OWASP CATEGORY:** A9 - Using Components with Known Vulnerabilities

15. Cloud Metadata Potentially Exposed:

- **Description**: This vulnerability indicates that cloud metadata, which often contains sensitive information about the cloud instance and its configuration, may be exposed to unauthorized users.
- **OWASP Category**: Not directly categorized by OWASP, but it falls under A6 - Security Misconfiguration or A5 - Broken Access Control depending on the context.
- **CWE Category**: CWE-200 - Information Exposure
- **Business Impact**: Unauthorized access to cloud metadata can lead to sensitive data exposure, potential security misconfigurations, and exploitation of cloud resources.
- **Solution**: To mitigate this vulnerability, ensure that access controls are properly configured to restrict access to cloud metadata. Review and update cloud security policies and configurations to prevent unauthorized access. Regularly audit and monitor cloud infrastructure for security vulnerabilities. Implement strong authentication mechanisms and encryption for sensitive metadata. Additionally, follow cloud service provider's best practices and security guidelines to secure cloud resources effectively.

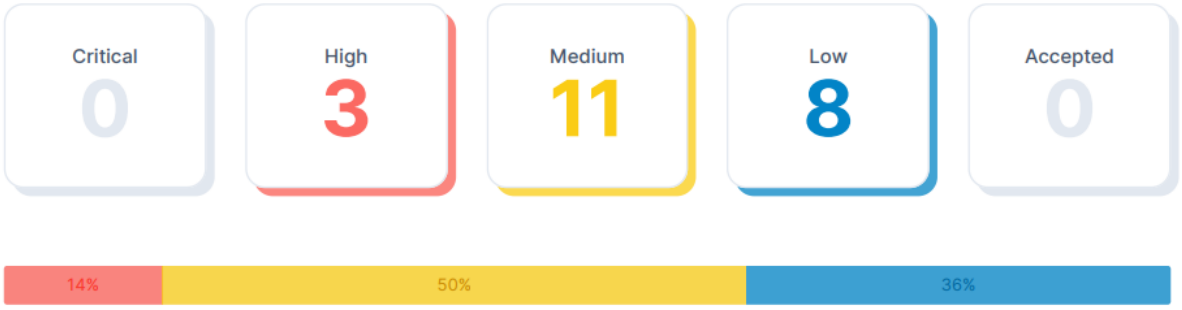
The complete report of the scan can be accessed using the following link:

https://drive.google.com/file/d/1kiZqPBJLw8_ELe1tPOetQQ181ZOvg3C0/view?usp=sharing

Scanned Vulnerabilities are:

3.1 Total Risks

Total number of risks found by severity.



Summary list of all detected risks.

Title	Threat Level	Open	Accepted
SQL Injection	High	1	0
SQL Injection - Oracle - Time Based	High	1	0
Spring4Shell	High	1	0
Absence of Anti-CSRF Tokens	Medium	1	0
Directory Browsing	Medium	1	0
Cross-Domain Misconfiguration	Medium	1	0
Missing Anti-clickjacking Header	Medium	1	0
CSP: Wildcard Directive	Medium	1	0
CSP: script-src unsafe-inline	Medium	1	0
CSP: style-src unsafe-inline	Medium	1	0
XSLT Injection	Medium	1	0
CSP: script-src unsafe-eval	Medium	1	0
Content Security Policy (CSP) Header Not Set	Medium	1	0
Vulnerable JS Library	Medium	1	0
Cookie No HttpOnly Flag	Low	1	0
Cross-Domain JavaScript Source File Inclusion	Low	1	0
X-Content-Type-Options Header Missing	Low	1	0
Cookie Without Secure Flag	Low	1	0
Cookie with SameSite Attribute None	Low	1	0
CSP: Notices	Low	1	0
Strict-Transport-Security Header Not Set	Low	1	0
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1	0

SOC, SIEM and IBM QRadar

SOC

A security operations center (SOC) – sometimes called an information security operations center, or ISOC is an in-house or outsourced team of IT security professionals that monitors an organization's entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and as effectively as possible.

An SOC also selects, operates, and maintains the organization's cybersecurity technologies, and continually analyzes threat data to find ways to improve the organization's security posture. The chief benefit of operating or outsourcing an SOC is that it unifies and coordinates an organization's security tools, practices, and response to security incidents. This usually results in improved preventative measures and security policies, faster threat detection, and faster, more effective and more cost-effective response to security threats. An SOC can also improve customer confidence, and simplify and strengthen an organization's compliance with industry, national and global privacy regulations.

SOC cycle

The SOC (Security Operations Center) cycle is a structured approach to managing cybersecurity within an organization. It encompasses various stages to ensure effective threat detection, response, and mitigation.

Firstly, the cycle begins with "Detection and Monitoring." This involves constant surveillance of an organization's digital environment, including networks, systems, and applications. Advanced tools and technologies are employed to identify anomalous activities, potential vulnerabilities, or signs of a security breach. This proactive monitoring helps in early threat identification, reducing the likelihood of a successful cyber-attack.

Once a potential threat is detected, the SOC moves into the "Analysis and Investigation" phase. Here, skilled cybersecurity professionals thoroughly examine the identified indicators of compromise (IoCs) or suspicious behavior. They assess the severity, scope, and potential impact of the threat. This stage involves deep dives into logs, network traffic, and system behavior to gain a comprehensive understanding of the incident. It is crucial for determining the appropriate response measures and understanding the threat's nature.

SIEM

Security information and event management, SIEM for short, is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.SIEM, pronounced "sim," combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.

In short, SIEM gives organizations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements. In the past decade, SIEM technology has evolved to make threat detection and incident response smarter and faster with artificial intelligence.

SIEM Cycle

The SIEM (Security Information and Event Management) cycle is a critical process in cybersecurity that involves collecting, correlating, and analyzing security data from various sources within an organization's IT infrastructure.

Firstly, the cycle commences with "Data Collection and Aggregation." This phase involves gathering

security-related data from diverse sources like firewalls, intrusion detection systems, servers, and applications. This data is then centralized in a SIEM platform, which acts as a centralized nerve center for security events. The platform normalizes and structures this data, making it easier to analyze and identify potential security incidents.

Next comes "Event Correlation and Analysis." In this phase, the SIEM system uses predefined rules and algorithms to correlate and analyze the collected data. It looks for patterns, anomalies, and potential threats that might be indicative of a security incident. Security analysts play a crucial role in this stage, fine-tuning the rules and investigating any alerts generated by the system. They also contextualize the information, assessing the potential impact and determining the appropriate response. This phase is pivotal in identifying and prioritizing security incidents for further investigation and action.

MISP

MISP (Malware Information Sharing Platform)is an open-source threat intelligence platform that enables organizations to share and collaborate on information about malware, vulnerabilities, and other cybersecurity threats. It is a community-driven project that is used by organizations of all sizes, including government agencies, businesses, and non-profit organizations.

MISP provides a number of features that make it a valuable tool for cybersecurity teams, including:

- Structured data model: MISP uses a structured data model to represent threat intelligence information. This makes it easy to share and correlate information across different organizations and systems.
- Flexible sharing policies: MISP provides flexible sharing policies that allow organizations to controlwho has access to their data and how it can be used.
- Powerful search and filtering capabilities: MISP's powerful search and filtering capabilities make it easy to find the information you need quickly and easily.
- Integration with other security tools: MISP can be integrated with other security tools, such as SIEMs and intrusion detection systems, to automate the sharing and consumption of threat intelligence information.

MISP can be used for a variety of cybersecurity purposes, including:

- Incident response: MISP can be used to share information about ongoing incidents with other organizations, which can help to accelerate the response and recovery process.
- Threat hunting: MISP can be used to search for and correlate threat intelligence information to identify new and emerging threats.
- Security awareness: MISP can be used to share threat intelligence information with employees to help them raise awareness of the latest threats and how to protect themselves.

Overall, MISP is a valuable tool for cybersecurity teams of all sizes. It can help organizations to improve their security posture by enabling them to share and collaborate on threat intelligence information more effectively.

MISP architecture: MISP is a web-based application that is typically hosted on a server within an organization's network. Users can access MISP through a web browser using their organization's credentials.

MISP data model: MISP uses a structured data model to represent threat intelligence information. This data model is based on the Common Vocabulary for Information Exchange (CVE) and the OpenIOC format.

- MISP features: MISP provides a number of features that make it a valuable tool for cybersecurity teams, including:

- Collaboration: MISP allows organizations to share threat intelligence information with each other in a secure and controlled manner.
- Analysis: MISP provides tools for analyzing threat intelligence information, such as correlation and enrichment.
- Automation: MISP can be integrated with other security tools, such as SIEMs and intrusion detection systems, to automate the sharing and consumption of threat intelligence information.

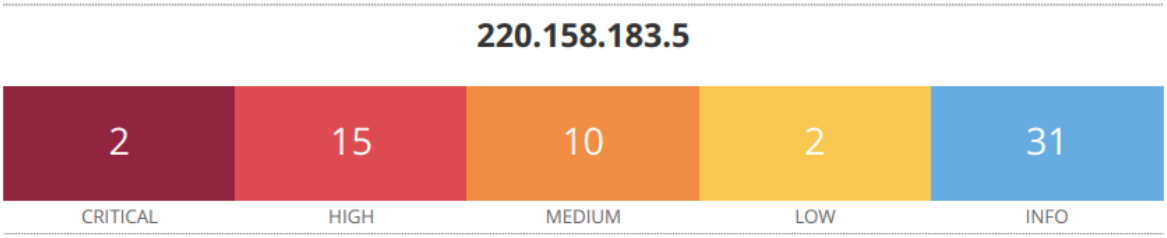
MISP community: MISP is an open-source project with a large and active community. The community provides support to MISP users through a variety of channels, including mailing lists, IRC chat, and forums. MISP deployments: MISP is used by a wide range of organizations, including government agencies, businesses, and non-profit organizations. Some notable examples include:

- The United States Department of Homeland Security
- The United Kingdom National Cyber Security Centre
- The Australian Cyber Security Centre
- The NATO Cooperative Cyber Defence Centre of Excellence
- The Financial Services Information Sharing and Analysis Center (FS-ISAC)

College Network Information:

Most of the colleges and universities use CAN (Campus Area Network) is a computer network that connects multiple buildings within a college or university campus. CANs typically provide Internet access to students, faculty, and staff, as well as allow for the sharing of files and resources across the campus.

CANs are typically larger and more complex than local area networks (LANs), which are typically limited to a single building or office. However, CANs are smaller than metropolitan area networks (MANs) and wide area networks (WANs), which connect networks across large geographic areas. CANs are typically owned and operated by the college or university itself. This allows the institution to have complete control over the network and its security. Our website was scanned by Nessus and below are the results of the scan:



Components of a college network

A college network typically consists of the following components:

- Core network: The core network is the backbone of the CAN and connects the different buildings
- and networks on campus. It typically consists of high-speed switches and routers.
- Distribution network: The distribution network connects the core network to the access networks in
- each building. It typically consists of switches and routers that are less powerful than the core
- network devices.
- Access network: The access network provides connectivity to end users in each building. It typically
- consists of switches and wireless access points.
- Internet access: College networks typically provide Internet access to students, faculty, and staff.
- This is done through a connection to an Internet service provider (ISP).

Security of college networks

College networks are a prime target for cyberattacks. This is because they contain a wealth of sensitive data, such as student records, research data, and financial information.

Colleges and universities take a number of steps to secure their networks, including:

- Firewalls: Firewalls are used to block unauthorized access to the network.
- Intrusion detection systems (IDS): IDS are used to detect and respond to malicious activity on the
- network.
- Encryption: Encryption is used to protect sensitive data from unauthorized access.
- User education: Users are educated about cybersecurity best practices, such as how to create strong passwords and avoid phishing scams.

Benefits of college networks:

College networks provide a number of benefits to students, faculty, and staff, including:

- Internet access: College networks provide students, faculty, and staff with access to the Internet, which is essential for academic research and collaboration.
- Resource sharing: College networks allow students, faculty, and staff to share files and resources across the campus. This can save time and money.
- Communication: College networks facilitate communication between students, faculty, and staff. This can be done through email, instant messaging, and other online tools.
- Security: College networks are typically secure and provide protection from cyberattacks. This helps to protect the sensitive data that is stored on the network.

Overall, college networks play an important role in the academic and administrative life of colleges and universities. They provide students, faculty, and staff with the tools and resources they need to succeed.

How do you think you deploy soc in your college?

To deploy a SOC in a college, the following steps are recommended:

1. Establish a SOC team. The SOC team should be composed of experienced cybersecurity professionals who have the skills and knowledge to monitor and protect the college network.
2. Select and implement the appropriate security tools. The SOC team will need to select and implement a variety of security tools, such as firewalls, intrusion detection systems, and SIEMs.
3. Develop a SOC playbook. The SOC playbook should outline the steps that the SOC team will take to respond to different types of security incidents.
4. Train the SOC team. The SOC team should be trained on the security tools that they will be using and on the SOC playbook.
5. Communicate with stakeholders. The SOC team should communicate with key stakeholders on campus, such as the IT department, the administration, and the student body, about the SOC and its mission.

Here is a more detailed look at each step:

1. Establish a SOC team

The SOC team should be composed of experienced cybersecurity professionals who have the skills and knowledge to monitor and protect the college network. The team should be responsible for the following tasks:

• Monitoring the college network for suspicious activity

• Investigating security incidents

• Responding to security incidents

• Proactively improving the college's security posture

2. Select and implement the appropriate security tools

The SOC team will need to select and implement a variety of security tools to monitor and protect the college network. Some of the essential tools include:

• Firewalls: Firewalls block unauthorized access to the college network.

• Intrusion detection systems (IDS): IDS detect malicious activity on the network.

• Security information and event management (SIEM): SIEMs aggregate and correlate security events from across the network.

In addition to these essential tools, the SOC team may also want to consider implementing other security tools, such as threat intelligence feeds, vulnerability scanners, and security orchestration, automation, and response (SOAR) tools.

3. Develop a SOC playbook

The SOC playbook should outline the steps that the SOC team will take to respond to different types of security incidents. The playbook should include the following information:

• Incident response procedures

• Communication protocols

• Escalation procedures

The SOC playbook should be reviewed and updated on a regular basis to reflect changes in the college's security environment.

4. Train the SOC team

The SOC team should be trained on the security tools that they will be using and on the SOC playbook. The training should cover the following topics:

• Security fundamentals

• Security tools and technologies

• SOC procedures

• Incident response

• Communicate with stakeholders

The SOC team should communicate with key stakeholders on campus, such as the IT department, the administration, and the student body, about the SOC and its mission. The SOC team should provide regular updates on the college's security posture and should communicate any security incidents that occur. By following these steps, a college can deploy a SOC that will help to protect its network and its students, faculty, and staff from cyberattacks.

Threat intelligence

Threat intelligence is detailed, actionable threat information for preventing and fighting cyberthreats targeting an organization. It is data containing detailed knowledge about the cybersecurity threats targeting an organization. Threat intelligence helps security teams be more proactive, enabling them to

take effective, data-driven actions to prevent cyber-attacks before they occur. It can also help an organization better detect and respond to attacks in progress .

Threat intelligence involves gathering, analysing, and using information about current and potential cybersecurity threats. It helps organizations understand the types of threats they might face, the tactics, techniques, and procedures used by threat actors, and the vulnerabilities they might exploit.Threat intelligence is crucial for proactive cybersecurity. It helps organizations assess their risks, make informed decisions, and improve their security posture.

Incident response

Incident response refers to an organization's processes and technologies for detecting and responding to cyberthreats, security breaches or cyberattacks. The goal of incident response is to prevent cyberattacks before they happen, and to minimize the cost and business disruption resulting from any cyberattacks that occur. Ideally, an organization defines incident response processes and technologies in a formal incident response plan (IRP) that specifies exactly how different types of cyberattacks should be identified, contained, and resolved .

The key steps in incident response include preparation, identification, containment, eradication, recovery, and lessons learned. It's a cyclical process designed to minimize damage and reduce recovery time and costs. Effective incident response can help organizations limit the impact of a breach and prevent it from happening again.

Qradar & understanding about tool

QRadar is a network security management platform that provides situational awareness and compliance support. QRadar uses a combination of flow-based network knowledge, security event correlation, and asset based vulnerability assessment. It collects log data from an enterprise, its network devices, host assets and os (Operation System), applications, vulnerabilities, and user activities and behaviours. QRadar administrators can browse and download apps from the IBM Security App Exchange to address specific security requirements .

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Failure Audit: The Windows Filtering Platform blocked a packet	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:49 PM	Access Denied	192.168.0.100	443	192.168.0.100	59447	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:48 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59452	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:48 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59452	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	51723	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	51723	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	51914	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59451	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59451	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59450	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59450	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59449	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59449	N/A	
Failure Audit: A privileged service was called	WindowsAuthServer @ LAPT...	424	Sep 18, 2023, 7:47:37 PM	Misc Authorization	192.168.0.100	0	192.168.0.100	0	MANASA	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:46 PM	Access Permitted	192.168.0.100	0	192.168.0.100	53560	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:46 PM	Access Permitted	192.168.0.100	0	192.168.0.100	53560	N/A	
Success Audit: The Windows Filtering Platform has allowed a co...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:45 PM	Access Permitted	192.168.0.100	130	192.168.0.100	100	N/A	
Success Audit: The Windows Filtering Platform has allowed a co...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:43 PM	Access Permitted	192.168.0.100	0	224.0.0.22	0	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:42 PM	Access Permitted	192.168.0.100	0	192.168.0.100	52629	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:42 PM	Access Permitted	192.168.0.100	0	192.168.0.100	52629	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:41 PM	Access Permitted	0.0.0.0	0	192.168.0.100	59446	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:41 PM	Access Permitted	192.168.0.100	0	192.168.0.100	65252	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:41 PM	Access Permitted	192.168.0.100	0	192.168.0.100	65252	N/A	

Stage 1 : What you understand from Web application testing?

Web application testing is a thorough evaluation of a web-based software application, focusing on functionality, security, and performance.

The assessment of functionality covers various aspects, from basic navigation to complex tasks like database interactions, ensuring a bug-free user experience. Compatibility with different browsers and devices is also checked for seamless user interaction.

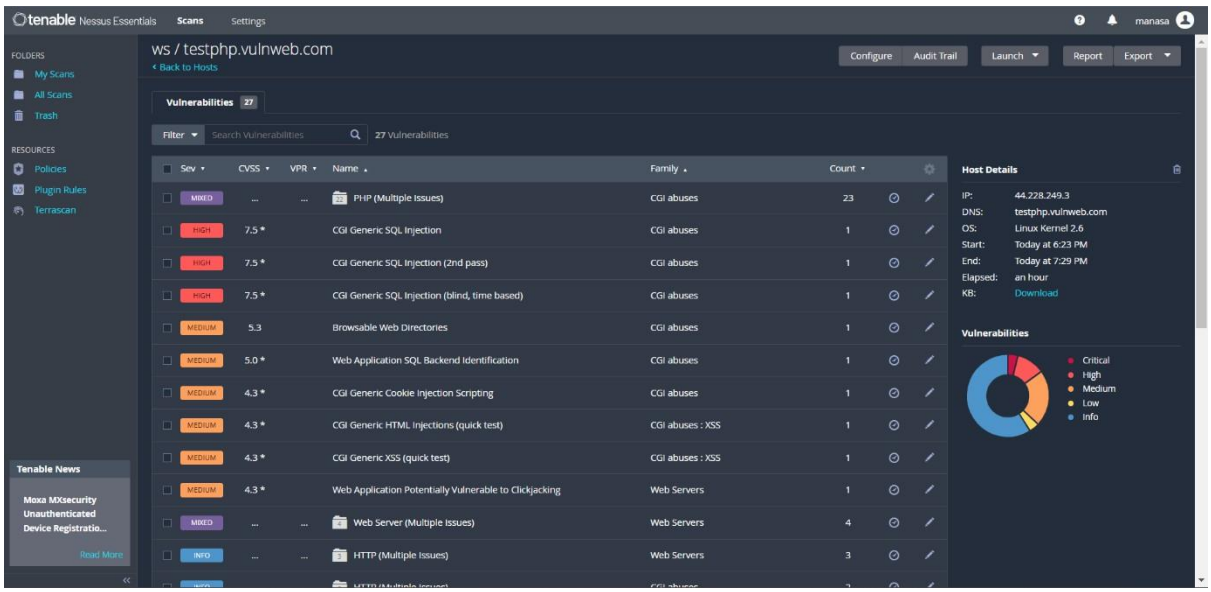
Security is a key concern, with testers actively seeking vulnerabilities like SQL injection and cross-site scripting. By simulating potential attacks, weaknesses are identified, and recommendations for fortification are provided. This ensures the protection of sensitive data and resilience against cyber

threats. Overall, web application testing is crucial for a secure, reliable, and user-friendly online experience.

Stage 2 : What you understand from the Nessus report?

A Nessus report refers to a report generated by Nessus, which is a popular vulnerability scanning tool used for identifying and assessing security vulnerabilities in computer systems and networks. Nessus is often employed by cybersecurity professionals, network administrators, and penetration testers to conduct security assessments and ensure the security of their systems.

A Nessus report typically includes information like vulnerability findings, risk management, historical data, recommendations etc. The report lists all identified vulnerabilities, including their severity level, a brief description, and the affected systems or devices as a part of vulnerability findings. Nessus assigns a risk score or severity level to each vulnerability, helping users prioritize their remediation efforts as a part of risk assessment. Common severity levels include Critical, High, Medium, and Low.



In recommendations, for each vulnerability, Nessus provides recommendations and remediation steps to help system administrators or security professionals mitigate or resolve the identified issues. The report often includes detailed technical information about each vulnerability, such as its CVE (Common Vulnerabilities and Exposures) identifier, affected software versions, and any additional relevant details.

Nessus can also check systems against specific security compliance standards (e.g., CIS benchmarks, NIST guidelines), and the report may include compliance-related findings and recommendations. Some Nessus reports include an executive summary section designed for non-technical stakeholders, providing an overview of the security posture and key findings in a more easily digestible format. Nessus can be used to track changes in a network's vulnerability over time, and some reports may include historical data to show how vulnerabilities have evolved.

Stage-3: What do you understand from SOC/ SIEM/ QRadar Dashboard?

SOC:

A Security Operations Center (SOC) is a centralized team of cybersecurity professionals responsible for monitoring, detecting, investigating, and responding to cybersecurity threats. SOCs typically operate 24/7/365 to ensure that organizations are protected from a wide range of cyberattacks, including malware infections, data breaches, and denial-of-service attacks.

SOC functions:

SOCs perform a variety of functions, including:

• Security monitoring: SOCs use a variety of security tools and technologies to monitor organization networks and systems for suspicious activity. This activity may include unusual network traffic, unauthorized access attempts, and malicious code infections.

• Threat detection: SOCs use security monitoring data and threat intelligence feeds to detect cybersecurity threats. This may involve identifying known malware signatures, identifying new and emerging threats, and correlating events from different sources to identify patterns of malicious activity.

• Incident investigation: SOCs investigate cybersecurity incidents to determine the root cause, assessthe impact, and recommend remediation steps. This may involve gathering evidence, analyzing logs, and interviewing stakeholders.

• Incident response: SOCs respond to cybersecurity incidents to contain the threat, mitigate the damage, and recover from the incident. This may involve deploying security countermeasures, restoring affected systems, and communicating with stakeholders.

SOC benefits

SOCs provide a number of benefits to organizations, including:

• Improved security posture: SOCs help organizations to improve their security posture by proactively monitoring for threats and responding to incidents quickly and effectively.

• Reduced risk of data breaches: SOCs can help organizations to reduce the risk of data breaches by detecting and responding to threats before they can compromise sensitive data.

• Compliance with regulations: Many regulations require organizations to have a SOC in place. SOCs can help organizations to comply with these regulations and avoid penalties.

SOC deployment

SOCs can be deployed in a variety of ways. Some organizations choose to build and operate their own SOCs, while others choose to outsource SOC services to a managed security service provider (MSSP).

SOC best practices:

There are a number of best practices that organizations can follow when deploying and operating a SOC, including:

• Establish a clear mission and scope: The SOC's mission and scope should be clearly defined and aligned with the organization's overall security strategy.

• Select the right security tools and technologies: The SOC should be equipped with the right security tools and technologies to monitor and protect the organization's network and systems.

• Train and hire qualified staff: The SOC team should be composed of qualified cybersecurity professionals who have the skills and knowledge to monitor, detect, investigate, and respond to cybersecurity threats.

• Develop and implement a SOC playbook: The SOC should develop and implement a playbook that outlines the steps that the team will take to respond to different types of security incidents.

• Test and improve the SOC: The SOC should be regularly tested and improved to ensure that it is effective in detecting and responding to cybersecurity threats.

SOCs play an important role in protecting organizations from cybersecurity threats. By following the best practices outlined above, organizations can deploy and operate effective SOCs that can help to reduce the risk of data breaches and improve their overall security posture.

SIEM:

SIEM stands for Security Information and Event Management. It is a security solution that collects, analyzes, and correlates security events from across an organization's IT infrastructure. SIEMs can be used to detect, investigate, and respond to security incidents, as well as to improve an organization's overall security posture.

SIEMs typically collect data from a variety of sources, including:

• Network devices (such as firewalls and routers)

• Security devices (such as intrusion detection systems and intrusion prevention systems)

• Servers

• Applications

• End user devices

Once the data is collected, SIEMs use a variety of techniques to analyze and correlate it. This can include:

• Pattern matching: SIEMs can look for patterns in security events that may indicate a malicious attack.

• Anomaly detection: SIEMs can identify anomalous activity that may be indicative of a security incident.

• Correlation: SIEMs can correlate security events from different sources to identify relationships that may not be obvious from looking at the events individually. Once SIEMs have identified potential security incidents, they can be used to investigate and respond to them. This can include:

• SIEMs can provide analysts with context for the security events that have been identified.

• SIEMs can help analysts to prioritize their investigations.

• SIEMs can automate some of the tasks involved in responding to security incidents, such as blocking malicious IP addresses and quarantining infected systems.

SIEMs can also be used to improve an organization's overall security posture. This can be done by:

• Identifying security gaps

• Measuring the effectiveness of security controls

• Proactively detecting and responding to emerging threats

SIEMs are an essential tool for any organization that wants to protect its IT infrastructure from cyberattacks.

By collecting, analyzing, and correlating security events from across the organization, SIEMs can help to detect, investigate, and respond to security incidents more effectively.

Here are some specific examples of how SIEMs can be used in a college environment:

• SIEMs can be used to detect unauthorized access to student records or financial data.

• SIEMs can be used to detect malware infections on college servers or student devices.

• SIEMs can be used to detect phishing attacks directed at college students or faculty.

• SIEMs can be used to monitor for suspicious activity on the college network, such as brute force attacks or denial-of-service attacks.

By using SIEMs to monitor and protect its network, a college can help to ensure the confidentiality, integrity, and availability of its data and systems.

Qradar Dashboard

QRadar dashboard is a visual representation of security data that is collected and analyzed by the QRadar SIEM platform. QRadar dashboards can be used to monitor the security posture of an organization's network and systems, to investigate security incidents, and to generate reports on security trends.

QRadar dashboards typically contain a variety of widgets, such as charts, graphs, and tables. Each widget displays a different type of security data, such as the number of security events that have occurred, the top sources of security events, and the most common types of security events.

QRadar dashboards are customizable, so organizations can create dashboards that are tailored to their specific needs. For example, an organization may create a dashboard to monitor the security of its web servers, or it may create a dashboard to monitor the security of its network endpoints.

QRadar dashboards can be used for a variety of purposes, including:

• Security monitoring: QRadar dashboards can be used to monitor the security posture of an organization's network and systems in real time. This allows organizations to quickly identify and respond to security incidents.

• Incident investigation: QRadar dashboards can be used to investigate security incidents by providing insights into the root cause of the incident and the impact of the incident.

• Security reporting: QRadar dashboards can be used to generate reports on security trends and incidents. This information can be used to improve the organization's security posture over time.

Here are some examples of specific QRadar dashboards that an organization might use:

•Overview dashboard: This dashboard provides a high-level overview of the organization's security posture. It typically includes widgets that display the number of security events that have occurred,the top sources of security events, and the most common types of security events.

• Endpoint security dashboard: This dashboard provides a detailed view of the security of the organization's network endpoints. It typically includes widgets that display the status of endpoint security software, the number of security events that have occurred on each endpoint, and the most common types of security events on each endpoint.

• Web security dashboard: This dashboard provides a detailed view of the security of the organization's web servers. It typically includes widgets that display the number of web attacks that have occurred, the top sources of web attacks, and the most common types of web attacks.

• Incident response dashboard: This dashboard provides a single view of all open security incidents. It typically includes widgets that display the status of each incident, the severity of each incident, andthe assigned investigator for each incident.

QRadar dashboards are a valuable tool for organizations of all sizes. They can help organizations to improve their security posture by providing insights into their security data and by helping them to quickly and effectively respond to security incidents.

Future Scope :

Stage 1 : Future scope of web application testing

The future scope of web application testing is poised for significant growth and evolution, driven by the continuous advancement of technology and the increasing reliance on web-based solutions across industries.

Firstly, with the proliferation of complex web applications and the adoption of emerging technologies like AI, IoT, and blockchain, the demand for specialized testing approaches is expected to rise. This will necessitate the development of more sophisticated testing tools and methodologies to ensure the robustness, security, and performance of these advanced applications.

Secondly, as cybersecurity threats continue to escalate, web application testing will play an even more critical role in safeguarding digital assets. With the expanding attack surface, including cloud-based services and interconnected systems, there will be a heightened need for comprehensive security testing. This will lead to the integration of advanced security testing techniques, such as threat modelling and vulnerability assessments, to fortify web applications against evolving cyber threats. Additionally, compliance with stringent data protection regulations will further drive the demand for rigorous testing practices. Overall, the future of web application testing is poised to be dynamic and pivotal in ensuring the reliability and security of the digital landscape.

Stage 2 : Future scope of testing process you understood

The future scope of testing process holds significant promise. This integration combines the strengths of traditional vulnerability scanning with the advanced capabilities of artificial intelligence. First and foremost, it offers an enhanced approach to threat detection. Nessus, with its vast plugin library, can systematically identify known vulnerabilities and weaknesses within a network. When complemented by AI-driven anomaly detection, it becomes capable of spotting unusual patterns or behaviors that might go unnoticed through conventional vulnerability scans. This comprehensive approach empowers organizations to proactively safeguard their networks by detecting both known issues and emerging threats.

Moreover, the integration of Nessus and AI brings about a crucial reduction in false positives. Traditional network security scanning often generates numerous false alarms, which can be resource-intensive to investigate and rectify. AI algorithms can be employed to discern genuine threats from benign anomalies, streamlining the security analysis process. This, in turn, allows security teams to concentrate their efforts on addressing actual risks and thus optimizes resource allocation while bolstering the network's overall security posture.

A critical facet of this integration is the shift from a reactive to a proactive security approach. By using Nessus to identify vulnerabilities and AI for anomaly detection, organizations can act proactively. They can pre-emptively pinpoint potential threats before they can be exploited, a fundamental requirement in today's dynamic threat landscape where zero-day vulnerabilities and sophisticated attacks are prevalent.

Lastly, this combination facilitates continuous improvement in network security. AI algorithms, learning from historical data, refine the anomaly detection process and enhance accuracy over time. The network becomes increasingly adept at identifying real threats and adapting to new attack vectors. This self improving capability ensures that organizations remain resilient against emerging threats, making it a forward-looking approach to network security that is adaptable and future-ready. In essence, the

integration of Nessus with AI-driven anomaly detection presents a powerful and comprehensive solution for addressing the ever-evolving challenges of network security in an era dominated by artificial intelligence.

Stage 3 : Future scope of SOC / SEIM

The future of Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems is incredibly promising, reflecting the evolving landscape of cybersecurity threats and technological advancements.

Firstly, SOCs are poised to become even more sophisticated and proactive in threat detection and response. As cyber threats become more advanced and persistent, SOCs will increasingly leverage artificial intelligence and machine learning algorithms to analyze vast amounts of data in real-time. This predictive approach will enable SOCs to identify and mitigate potential threats before they can cause significant damage. Additionally, SOCs will likely integrate with threat intelligence platforms and collaborate more closely with other security teams to stay ahead of emerging threats.

Secondly, SIEM systems are anticipated to become more intelligent and context-aware. They will evolve to not only detect security incidents but also provide richer insights into the nature and impact of these incidents. SIEM platforms will likely incorporate advanced analytics and behavioral analysis to differentiate between genuine threats and false alarms. Moreover, the integration of automation and orchestration capabilities will enhance the efficiency of incident response, allowing security teams to react swiftly to mitigate risks.

Overall, the future of SOCs and SIEM systems promises a more robust, agile, and intelligent approach to cybersecurity, crucial in safeguarding organizations against increasingly sophisticated threats.

Topics explored :

1. Web Application Testing
2. Nessus
3. SOC
4. SIEM
5. QRadar
6. Anomaly Detection
7. Deep Learning
8. Machine Learning
9. Intrusion Detection
10. Network Security
11. Predictive Analytics
12. Behavioral Analysis
13. Pattern Recognition
14. Data Mining
15. Threat Detection
16. Packet Analysis

17. Network Traffic Analysis
18. Feature Engineering
19. Alert Prioritization
20. DNS Traffic Analysis
21. User Behavior Profiling
22. Network Forensics
23. Signature-based Detection
24. Heuristic Analysis

Tools explored :

1. Burpsuite
2. SQL Map
3. Nessus
4. Kali Linux
5. Wireshark
6. Python
7. TensorFlow
8. Scikit-learn
9. Keras
10. Pandas
11. Numpy
12. Matplotlib
13. GitHub
14. Jupyter Notebook
15. Jira
16. Mural

----------THE END ----------