Smart Internz

AI ENHANCED INTRUSION DETECTION SYSTEM

Data Watchdogs

TEAM 1.5 MEMBERS -:

Priyanshu Srivastav

Rohan Idiculla Abraham

Gutta Vamsi Krishna

Bharath T

ABSTARCT

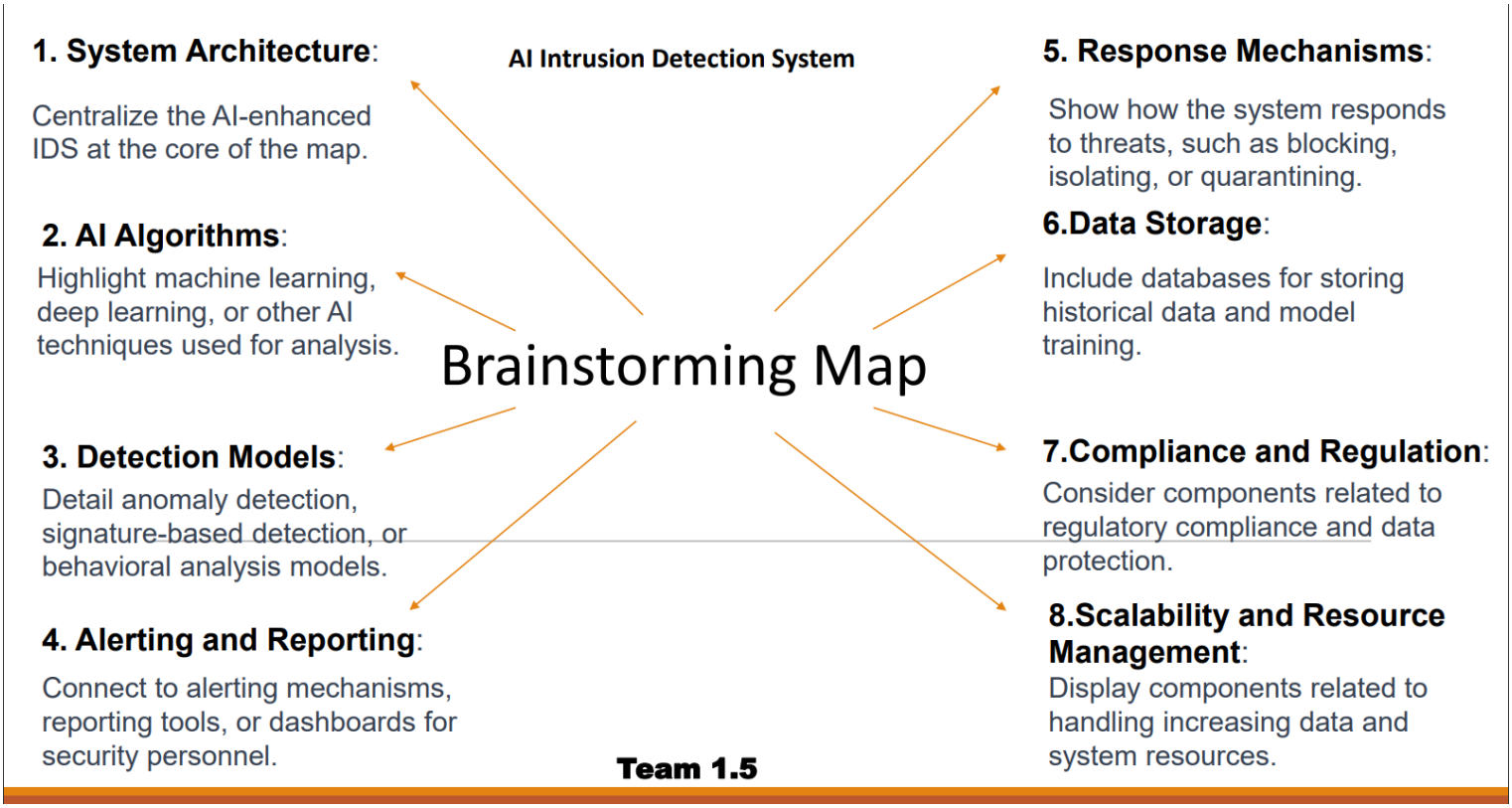
For years now, networks have been one of the main investments organisations of all sizes make to protect their networks, user, and data. In today's hyper-connected digital landscape, the need for robust cybersecurity measures is more critical than ever. The "AI-Based Intrusion Detection System" project presents an innovative solution poised to redefine the way we safeguard our networks and digital assets. Leveraging cutting-edge artificial intelligence and machine learning technologies, this system offers continuous monitoring and adaptive threat detection, significantly enhancing network security.

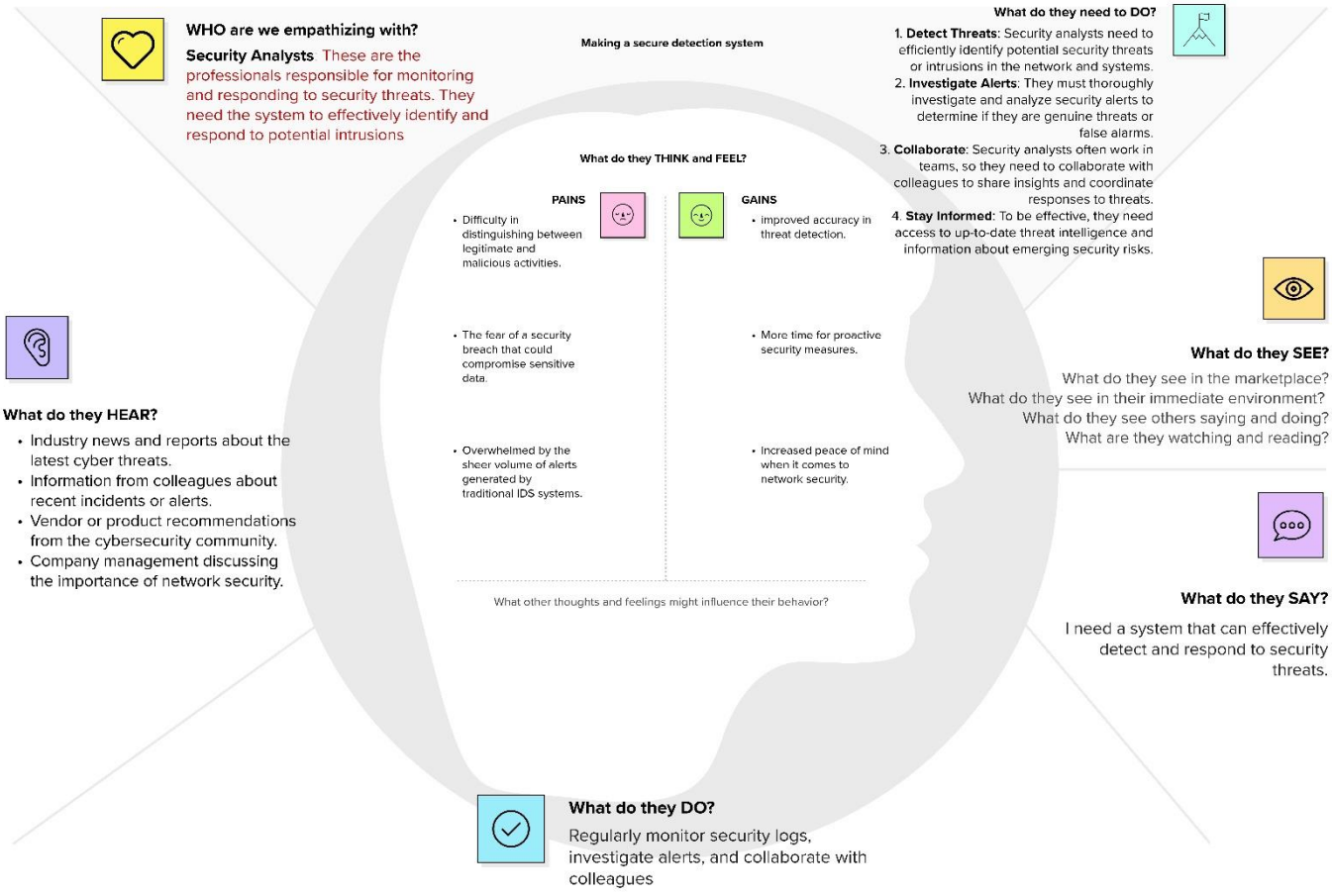
The answer to "what is intrusion" is typically an attacker gaining unauthorized access to a device, network, or system. Cyber criminals use increasingly sophisticated techniques and tactics to infiltrate organizations without being discovered. This includes common techniques like:

- Address Spoofing
- Fragmentation
- Pattern Evasion
- Coordinated attack

Encrypting data, using firewalls to prevent unauthorized traffic entering the network, employing antimalware solutions and a variety of other tools are upheld as a standard for more or less every organization, and are used to detect cyber-attacks and ultimately stop them.

Simply put, IDS is a software-based system used to detect and respond to malicious behaviour from outsiders or unauthorized attempts from within a network. It can detect malicious activities like virus and malware attacks as well as threats like phishing, brute force, DDoS and more. The IDS sends alerts to IT and security teams when it detects any security risks and threats. Our AI-based Intrusion Detection System is engineered to excel in various aspects of cybersecurity, making it a formidable defense against an evolving spectrum of threats. It operates in real-time, tirelessly analyzing network traffic and user behaviour patterns to swiftly identify potential security breaches, reducing the window of vulnerability in the face of cyberattacks. By leveraging the power of IDS + AI together, autonomous systems are able to protect a network better than ever before, allowing IT administrators to rest with the assurance that their cyber infrastructure is safe from threats and malicious activity. The combination also provides greater visibility across the network by collecting data from multiple sources and providing comprehensive situational awareness. This enables you to quickly detect potential threats and take action in real-time before they escalate into major issues.


AI Intrusion Detection System
1. System Architecture:
Centralize the AI-enhanced IDS at the core of the map.
2. AI Algorithms:
Highlight machine learning, deep learning, or other AI techniques used for analysis.
3. Detection Models:
Detail anomaly detection, signature-based detection, or behavioral analysis models.
4. Alerting and Reporting:
Connect to alerting mechanisms, reporting tools, or dashboards for security personnel.
Brainstorming Map
5. Response Mechanisms:
Show how the system responds to threats, such as blocking, isolating, or quarantining.
6.Data Storage:
Include databases for storing historical data and model training.
7.Compliance and Regulation:
Consider components related to regulatory compliance and data protection.
8.Scalability and Resource Management:
Display components related to handling increasing data and system resources.
Team 1.5


WHO are we empathizing with?
Security Analysts. These are the professionals responsible for monitoring and responding to security threats. They need the system to effectively identify and respond to potential intrusions
Making a secure detection system
What do they need to DO?
1. Detect Threats: Security analysts need to efficiently identify potential security threats or intrusions in the network and systems.
2. Investigate Alerts: They must thoroughly investigate and analyze security alerts to determine if they are genuine threats or false alarms.
3. Collaborate: Security analysts often work in teams, so they need to collaborate with colleagues to share insights and coordinate responses to threats.
4. Stay Informed: To be effective, they need access to up-to-date threat intelligence and information about emerging security risks.
What do they THINK and FEEL?
PAINS
• Difficulty in distinguishing between legitimate and malicious activities.
• The fear of a security breach that could compromise sensitive data.
• Overwhelmed by the sheer volume of alerts generated by traditional IDS systems.
GAINS
• improved accuracy in threat detection.
• More time for proactive security measures.
• Increased peace of mind when it comes to network security.
What other thoughts and feelings might influence their behavior?
What do they HEAR?
• Industry news and reports about the latest cyber threats.
• Information from colleagues about recent incidents or alerts.
• Vendor or product recommendations from the cybersecurity community.
• Company management discussing the importance of network security.
What do they SEE?
What do they see in the marketplace?
What do they see in their immediate environment?
What do they see others saying and doing?
What are they watching and reading?
What do they SAY?
I need a system that can effectively detect and respond to security threats.
What do they DO?
Regularly monitor security logs, investigate alerts, and collaborate with colleagues

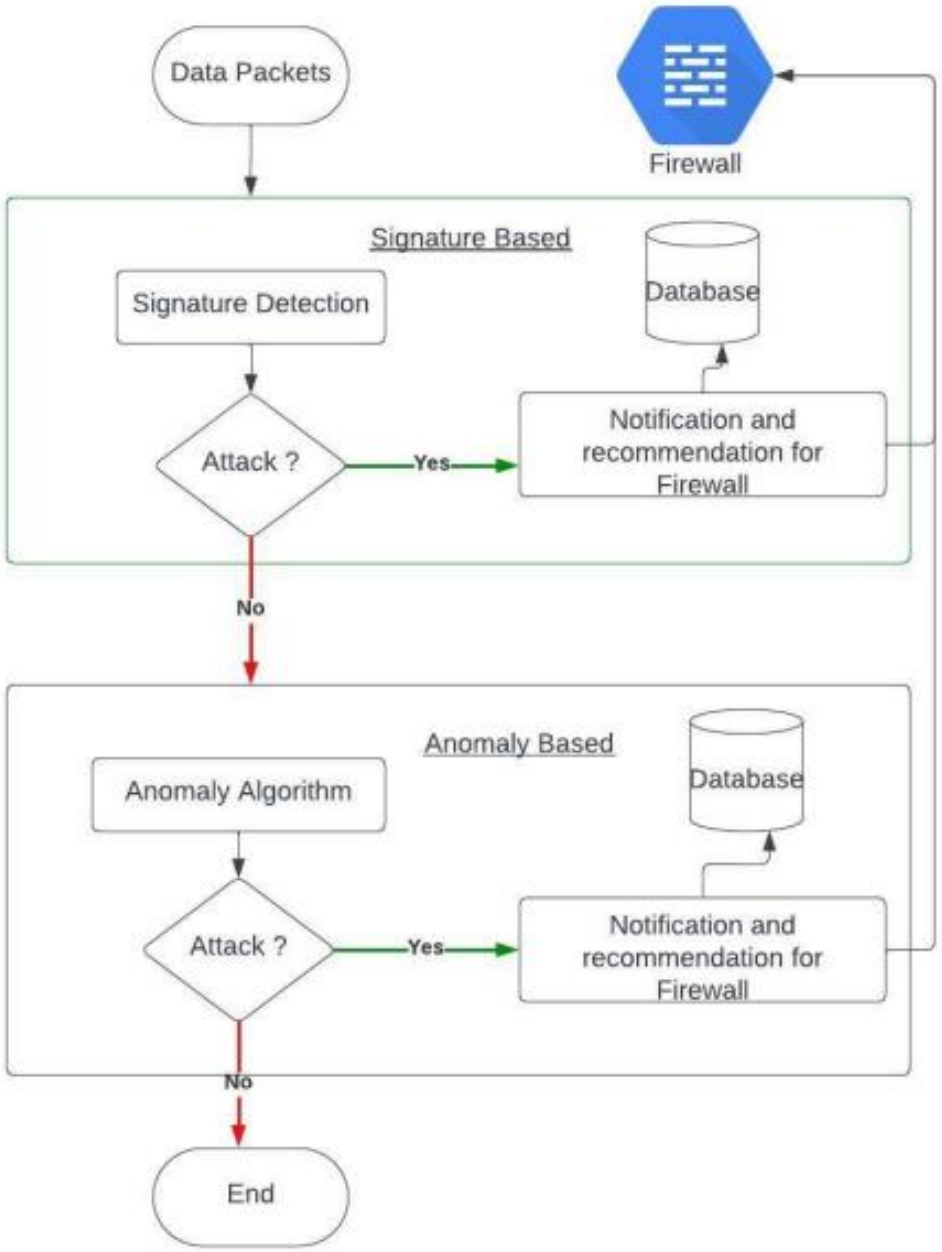
IDS consists of 2 layers of detection:

- Signature Based

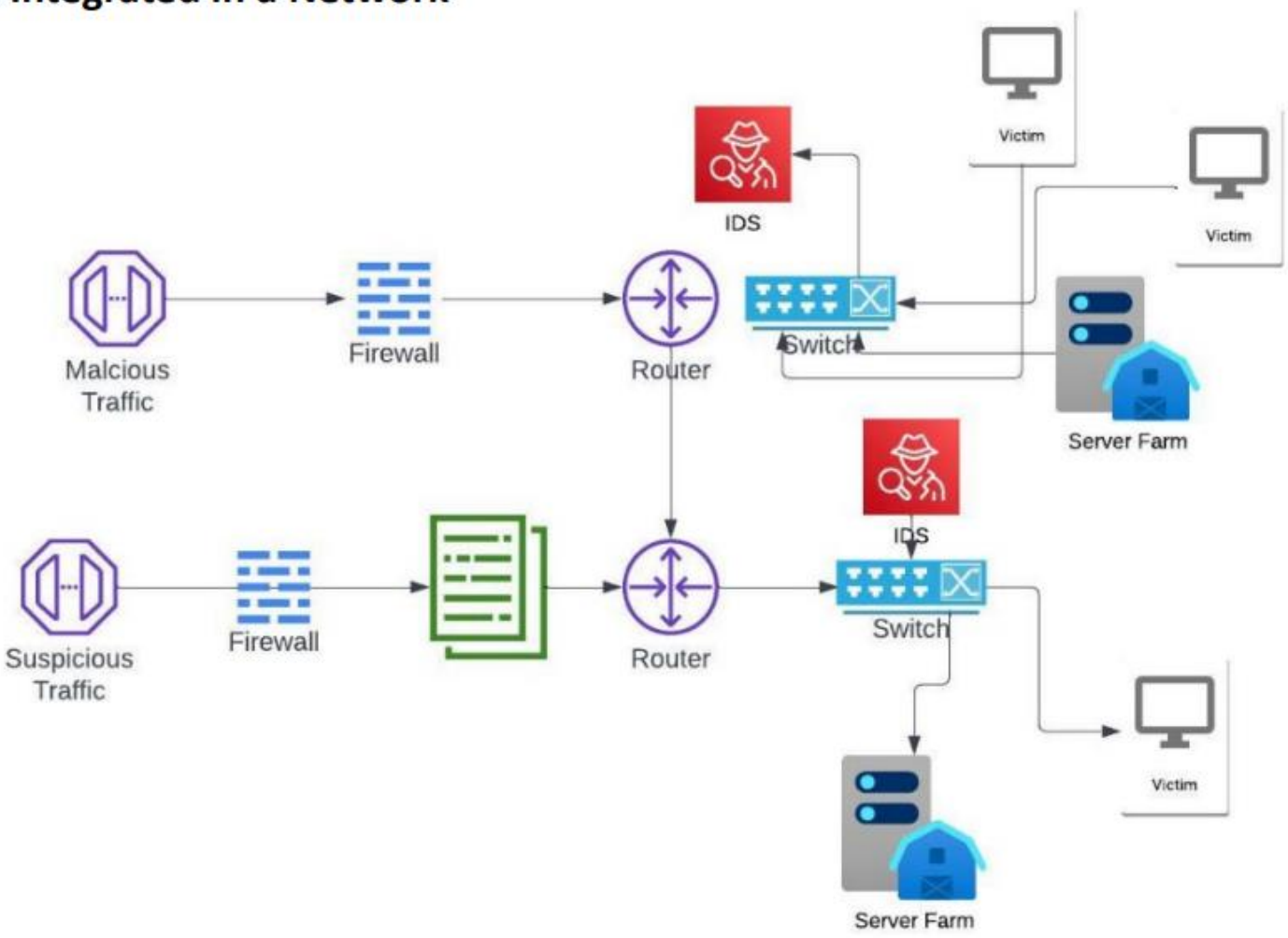
- Anomaly Based

• A copy of Data packets are inspected with predefined rules and policies. If an attack is detected, it is notified and recommendation is sent to firewall. If there are no atacks detected, the packets are moved to anomaly detection site.

• This section is trained using AI, and if it finds any anomaly, it is notified and a recommendation is sent to the Firewall. Else the testing ends.

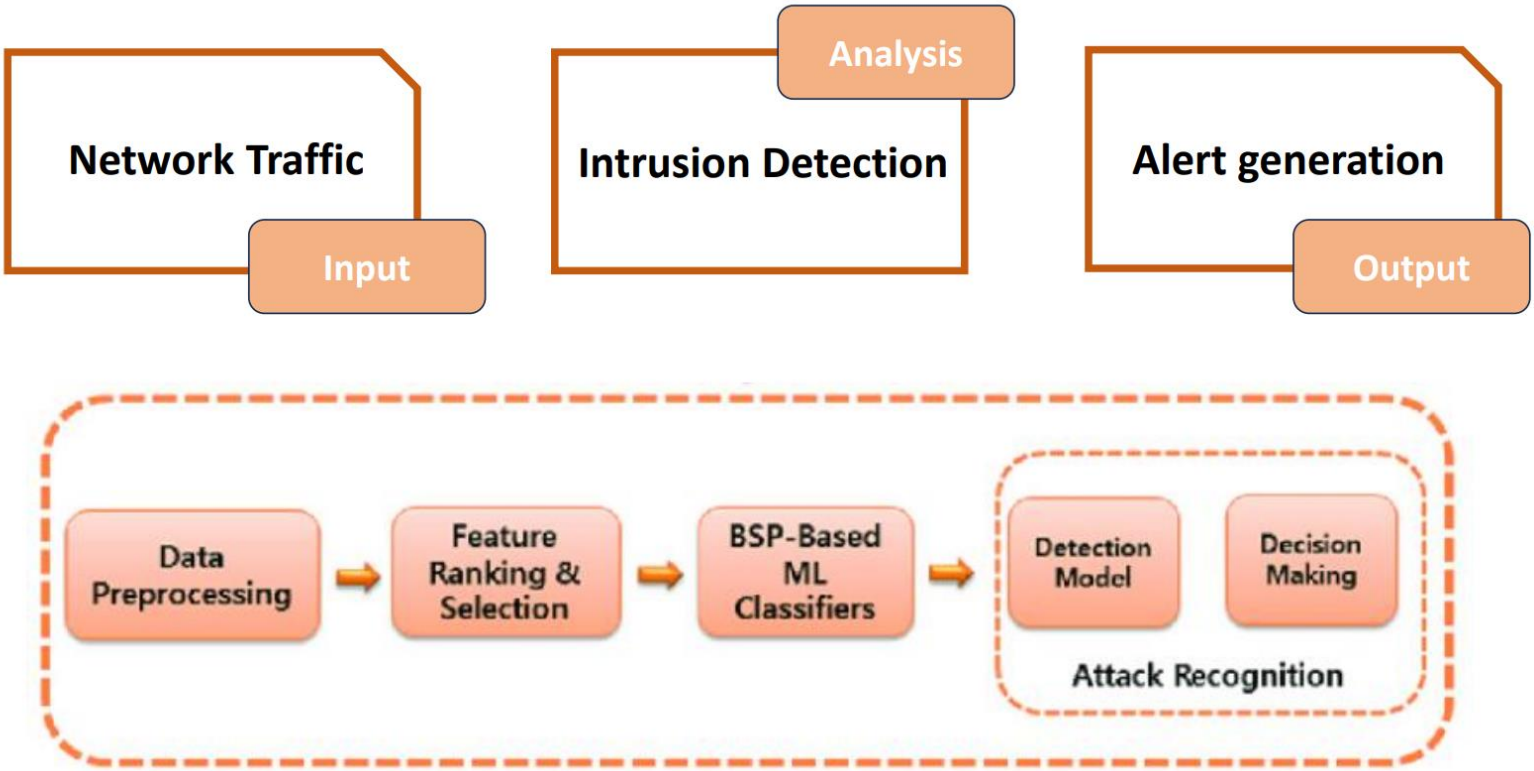


IDS Integrated in a Network



Proposed Solution Template:

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	To address the challenges of detecting unknown threats, reducing false positives, enabling real-time detection, improving adaptability, ensuring scalability, integrating with existing systems, and complying with ethical and regulatory requirements in the ever- evolving landscape of cybersecurity.
2.	Idea / Solution description	The AI-enhanced Intrusion Detection System is a cutting-edge cybersecurity solution that uses advanced AI and machine learning to detect known and unknown threats, reduce false positives, provide real- time monitoring, adapt to evolving threats, ensure scalability, integrate with existing systems, and comply with ethical and regulatory requirements. It offers organizations a powerful and adaptable defense against modern cybersecurity challenges.
3.	Novelty / Uniqueness	• Advanced AI Models: Utilizing cutting-edge AI and ML for comprehensive threat detection. • Anomaly Detection: Identifying unknown threats by recognizing abnormal behavior. • Real-time Response: Swiftly reacting to security incidents, reducing potential damage. • Continuous Learning: Adapting and improving over time for enhanced accuracy. • Reduced False Positives: Minimizing the burden on security teams through AI-driven precision. • Scalability: Built to handle growing data volumes and network traffic. • Integration and Compliance: Seamlessly integrating with existing systems while adhering to ethical and regulatory standards.
4.	Social Impact / Customer Satisfaction	This AI-enhanced IDS not only enhances cybersecurity but also promotes peace of mind by protecting sensitive data and systems. It reduces the risk of breaches, leading to higher customer satisfaction and trust in organizations that deploy it.
5.	Business Model (Revenue Model)	The revenue model for the AI-enhanced IDS is based on a subscription-based service, where organizations pay a recurring fee for ongoing access to the system's threat detection, monitoring, and response capabilities. This model ensures a steady stream of income and allows for continuous updates and support.
6.	Scalability of the Solution	The system is designed for easy scalability, capable of handling increasing data volumes and network traffic as organizations grow, ensuring long-term effectiveness and adaptability.


Network Traffic
Input
Analysis
Intrusion Detection
Alert generation
Output
Data Preprocessing
Feature Ranking & Selection
BSP-Based ML Classifiers
Detection Model
Decision Making
Attack Recognition

S.No	Component	Description	Technology
1.	User Interface	How user interacts with application e.g. configure ids, view alerts, generate reports.	HTML, CSS, JavaScript, React Js etc.
2.	Response mechanism	Depending On the severity of the intrusion, application logic component can trigger various responses, such as blocking network traffic, or sending alerts to administrators.	Python, Cloud services.
3.	Alert mechanism	When a potential intrusion is detected, this component generates alerts or notifications. This alerts may vary in severity based on the perceived threat level.	Email, HTTP API service.
4.	Cloud Database	These databases provide an flexible and scalable approach to data storage and management.	IBM DB2, IBM Cloud ant etc.
5.	File Storage	It refers to storage and management of files and data, in a structure consisting of folders and files.	Python, Java, MySQL, etc.
6.	Vulnerability databases.	IDS can query databases like CVE, database to check for known vulnerabilities associated with detected assets.	Python, SQL, Restful API, etc.
7.	Firewall API's	IDS can integrate with network firewalls to automatically block or isolate malicious IP's. This might involve firewall API's like windows firewall, cloud firewall services.	SSH, Restful API, etc.
8.	Machine Learning Algorithms.	This algorithms like neural networks or decision trees help in identifying abnormal patterns that might indicate an intrusion.	Python, R, Java, etc.
9.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud Local Server Configuration: Cloud Server Configuration :	Local, Cloud Foundry, Kubernetes, Recognition etc.

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	An open-source framework is a software development environment that is made available for public with its source code accessible and modifiable.	Kubernetes, Elastic stack, etc.
2.	Security Implementations	They can encompass a wide range of measures to protect systems, data, and information from unauthorized access, threats.	NIDS, HIDS, Clod-based IDS, IAM Controls, OWASP, etc.
3.	Scalable Architecture	An architecture that doesn't require changes to upkeep effective performance when there is an increase in workload.	Elastic cloud services, machine learning, etc.
4.	Availability	It refers to readiness and reliability of the system to be consistently accessible.	Load balancers, CDN's, etc.
5.	Performance	It refers to speed of a system in executing tasks and delivering results.	CDN's, Scalability, Caching, etc

Nessus Overview:-

Description:

Nessus is widely used vulnerability scanning tool and security software developed by tenable, Inc. It is primarily used to identify and access vulnerabilities in computer systems, networks, and applications.

Applications of Nessus:

- Vulnerability Scanning:

  Nessus is primarily known for its vulnerability scanning capabilities. It can target systems for known security issues, misconfigurations, and weaknesses. This helps organizations identify potential entry points for attackers and prioritize their remediation efforts.

- Plugin-Based Architecture:

  Nessus uses plugin-in-based architecture, where plugins are small programs or scripts that check for specific vulnerabilities or issues. This architecture allows nessus to support a wide range of vulnerabilities and technologies.

- Comprehensive Coverage:

  Nessus is capable of scanning a broad spectrum of system and devices, including servers, workstations, networking equipment, and web applications. It covers various operating systems and software packages.

- Scanning Types: It supports different types of scans, such as credentialed scans, and uncredentialed scans, and compliance scans.

- Risk Management:

  Nessus provides a risk management by assigning severity levels to identified vulnerabilities, allowing organizations to focus on the most critical issues first.

- Customization:

  Users can customize scans to meet their specific needs. This includes scheduling scans, defining scan policies, and tailoring the scan scope.

- Reporting:

Nessus generates detailed reports that provide a clear overview of the vulnerabilities discovered during the scan. These reports can be useful for compliance purposes and to communicate security status to stakeholders.

- Integration:

  It can be integrated with other security tools and systems, such as SIEM (Security Information and Event Management) solutions, to enhance an organization's overall security posture.

Target ip address: -

115.240.194.13

52.66.12.101

127.0.0.1

172.67.222.140

List of vulnerability :-

S.No	Vulnerability name	Severity	Plug-in Information
1	PHP Multiple Vulnerabilities.	Critical.	Published :2022/11/03 Modified : 2023/10/05
2	PHP Unsupported Version Detection.	Critical.	Published :2012/05/04 Modified : 2022/12/07
3	SSL Certificate Cannot be trusted.	Medium.	Published :2010/12/15 Modified : 2020/04/27
4	TLS Version 1.0 Protocol Detection.	Medium.	Published :2017/11/22 Modified : 2023/04/19
5	TLS Version 1.0 Protocol Deprecated.	Medium.	Published :2022/04/04 Modified : 2023/04/19
6	Apache HTTP Server Version.	-----	Published :2010/07/30 Modified : 2023/08/17
7	Backported Security Path Detection.	-----	Published :2009/06/25Modified : 2015/07/07
8	Common Platform Enumeration.	-----	Published :2010/04/21 Modified : 2023/10/16
9	Device Type.	-----	Published :2011/05/23 Modified : 2022/09/09
10	HSTS Missing From HTTPS Server.	-----	Published :2017/11/22 Modified : 2023/04/19

11	HTTP Server Type and Version.	-----	Published :2000/01/04 Modified : 2020/10/30
12	HTTP Information.	-----	Published :2007/01/30 Modified : 2019/11/22
13	Nessus SYN Scanner.	-----	Published :2009/02/04 Modified : 2023/09/25
14	HSTS Missing From HTTPS Server.(RFC 6797)	-----	Published :2020/11/17 Modified : 2023/06/08
15	Web Server allows Password Auto-Completion.	Medium	Published :2009/10/07 Modified : 2023/07/17
16	Web Server Transmits clear text credentials.	Low.	Published :2007/09/28 Modified : 2016/11/29
17	CGI Generic Tests Load Estimation.	Low.	Published :2009/10/26 Modified : 2022/04/11
18	CGI Generic Tests Timeout.	-----	Published :2009/06/19 Modified : 2021/01/19
19	External URL′s.	-----	Published :2010/10/04 Modified : 2011/08/19
20	HTTP Cookie secure property transport mismatch.	-----	Published :2013/09/10 Modified : 2021/12/20
21	HTTP Methods allowed.	-----	Published :2009/12/10 Modified : 2022/04/11
22	Missing content security policy frame ancestors HTTP Response Header.	-----	Published :2010/10/26 Modified : 2021/01/19

23	Nessus Scan information.	-----	Published :2005/08/26Modified : 2023/07/31
24	Web application cookies not marked http only.	-----	Published :2015/08/24 Modified : 2015/08/24
25	Web application cookies not marked secure.	-----	Published :2015/08/24 Modified : 2015/08/24
26	SMB Signing not required.	-----	Published :2012/01/19 Modified : 2022/10/05
27	OS name and installed package Enumeration.	Medium.	Published :2004/07/06 Modified : 2022/09/26
28	DCE Services Enumeration.	-----	Published :2001/08/26 Modified : 2021/10/04
29	Host FDQN Resolution.	-----	Published :2004/02/11 Modified : 2017/04/14
30	NTLMSSP Authentication request Remote Network name disclosure.	-----	Published :2009/11/06 Modified : 2019/11/22

REPORT:-

1.) **Vulnerability name: -**PHP Multiple Vulnerabilities.

- **Severity: -**Critical.
- **Plug-in: -** Published :2022/11/03, Modified: 2023/10/05
- **Port: -**80(TCP).
- **Description: -**PHP vulnerabilities encompass a range of security issues, including SQL injection, cross-site scripting (XSS), and remote code execution, which can lead to data breaches, service disruptions, and financial losses in web applications.

- **Solution: -**Upgrade to PHP version 7.4.33 or later.
- **Business Impact:-**Multiple PHP vulnerabilities can lead to financial losses, data breaches, reputational damage, and legal consequences, undermining a business's operations and customer trust.

2.) **Vulnerability name:-** PHP Unsupported Version Detection.

- **Severity:-** Critical.
- **Plug-in:-**Published :2012/05/04 ,Modified : 2022/12/07
- **Port:-** 80(TCP).
- **Description:-**PHP Unsupported Version Detection is a process of identifying outdated and unsupported PHP versions in web applications, which poses security risks and may require an upgrade to maintain system integrity and protect against vulnerabilities.

- **Solution:-** The remote host contains the unsupported version of a web application scripting language.
- **Business Impact:-**Detecting unsupported PHP versions is essential for business security as it helps prevent potential vulnerabilities and data breaches. Failure to address unsupported versions can result in security risks, regulatory compliance issues, and reputational damage

3.)

- **Vulnerability name:-** SSL Certificate Cannot be trusted.

- **Severity:-** Medium.
- **Plug-in:-**Published :2010/12/15 ,Modified : 2020/04/27
- **Port:-** 443(TCP).
- **Description:-** SSL certificate cannot be trusted" indicates that a website's certificate isn't recognized or validated by trusted authorities, potentially exposing users to security risks.

- **Solution:-** Purchase or generate a proper SSL certificate for this service.
- **Business Impact:-**When an SSL certificate is not trusted, it erodes user trust, leads to data breaches, and can result in lost revenue and reputational damage, as customers may avoid the site

due to security concerns. Addressing this issue promptly is crucial for maintaining business integrity and security.

- 4.)

- **Vulnerability name:-** TLS Version 1.0 Protocol Detection.

- **Severity:-** Medium.
- **Plug-in:-**Published :2017/11/22 ,Modified : 2023/04/19
- **Port:-** 443(TCP).
- **Description:-** TLS Version 1.0 Protocol Detection is the process of identifying and determining the usage of the TLS 1.0 encryption protocol in a network, which is considered outdated and potentially insecure.

- **Solution:-** Enable support for TLS 1.2 and 1.3, and disable support for 1.0
- **Business Impact: -**The detection of TLS 1.0 usage in a business environment can signal security vulnerabilities, increase the risk of data breaches, and lead to regulatory non-compliance, potentially resulting in financial losses, reputational damage, and legal consequences.

5.)

- **Vulnerability name:-** TLS Version 1.0 Protocol Deprecated.

- **Severity:-** Medium.
- **Plug-in:-**Published :2022/04/04 ,Modified : 2023/04/19
- **Port:-** 443(TCP).
- **Description:-** "TLS Version 1.0 Protocol Deprecated" means that TLS 1.0, an outdated and insecure encryption protocol, is no longer recommended for use due to known security vulnerabilities.

- **Solution:-** Enable support for TLS 1.2 and 1.3, and disable support for 1.1
- **Business Impact:-**The deprecation of TLS 1.0 mandates its replacement to maintain security standards; non-compliance can lead to data breaches, legal issues, and reputational damage, impacting customer trust and business continuity.

6.)

- **Vulnerability name:-** Apache HTTP Server Version.

- **Severity:-** -----
- **Plug-in:-**Published :2010/07/30 ,Modified : 2023/08/19
- **Port:-** 80(TCP).
- **Description:-**
  The Apache HTTP Server Version is a software component that provides web server capabilities, allowing it to serve web pages to clients over the internet.

- **Solution: - n/a**
- **Business Impact: -**Publicly revealing the Apache HTTP Server version can expose potential vulnerabilities, making the server a target for cyberattacks, which may lead to service disruptions, data breaches, and reputational damage, impacting business operations and customer trust. To

mitigate these risks, businesses often hide or obscure server version information and maintain vigilant security practices.

7.)

- **Vulnerability name:-** Backported Security Path Detection.

Severity:- -----

- **Plug-in:-**Published :2009/06/25 ,Modified : 2015/07/07
- **Port:-** 22(SSH).

- **Description:-** "Backported Security Patch Detection" is the process of identifying and verifying the application of security patches that have been applied to older software versions to address vulnerabilities and improve security.

- **Solution:- n/a**

Business Impact:-
Efficient backported security patch detection helps mitigate security risks, reduces the potential for data breaches and service disruptions, and demonstrates a commitment to robust cybersecurity, safeguarding business reputation and customer trust.

8.)

- **Vulnerability name:-** Common Platform Enumeration.

- **Severity:-** -----

- **Plug-in:-**Published :2010/04/21 ,Modified : 2023/10/16.
- **Port:- 0(TCP).**
- **Description:-** Common Platform Enumeration (CPE) is a standardized naming scheme to identify and describe software applications and operating systems based on their attributes and version information.

- **Solution:- n/a**
- **Business Impact:-**
  Common Platform Enumeration (CPE) aids businesses in managing and securing software assets by providing standardized identification, reducing the risk of vulnerabilities, and facilitating compliance, ultimately enhancing cybersecurity posture and minimizing operational risks.

9.)

- **Vulnerability name:-** Device Type.

- **Severity:-** -----
- **Plug-in:-**Published :2011/05/23 Modified : 2022/09/08

- **Port:-** 0(TCP).
- **Description:-** Device type refers to the category or classification of a hardware device based on its purpose, design, and functionality, such as a smartphone, laptop, or printer.

- **Solution:- n/a**
- **Business Impact:-**
  Understanding the device type is critical for businesses to tailor their services, optimize user experience, and ensure compatibility, which can lead to increased customer satisfaction and operational efficiency while minimizing support and compatibility issues.

10.)

- **Vulnerability name:-** HSTS Missing From HTTPS Server.

- **Severity:-** -----
- **Plug-in:-**Published :2017/11/22 ,Modified : 2023/04/19
- **Port:-** 443(TCP).
- **Description:-** "HSTS Missing from HTTPS Server" indicates that the server is not implementing HTTP Strict Transport Security, a security policy mechanism, which may expose the site to security risks and downgrade attacks.
- **Solution:-** Configure the remote web server to use HSTS.
- **Business Impact:-**
  The absence of HSTS leaves the website vulnerable to man-in-the-middle attacks and security breaches, potentially eroding customer trust and harming the business's reputation. Implementing HSTS is crucial to enhance security and protect sensitive user data, fostering trust and compliance with security standards
- 11.)

- **Vulnerability name:-** HTTP Server Type and Version.

- **Severity:-** -----
- **Plug-in:-**Published :2017/11/22 ,Modified : 2023/04/19
- **Port:-** 80(TCP).
- **Description:-** HTTP Server Type and Version refers to the software and version information of the web server handling HTTP requests, which can be used to identify potential vulnerabilities or misconfigurations.
- **Solution:- n/a**
- **Business Impact:-**Revealing HTTP server type and version can expose security weaknesses, making the server a target for cyberattacks and potentially leading to service disruptions, data breaches, and reputational damage, which can negatively impact business operations and customer trust. To mitigate these risks, businesses often hide or obscure server information and maintain vigilant security practices.

12.)

- **Vulnerability name:-** HTTP Information.

- **Severity:-** -----
- **Plug-in:-**Published :2007/01/30 , Modified : 2019/11/22
- **Port:-** 80(TCP).

- **Description:-** HTTP Information encompasses data exchanged between a client and server during a Hypertext Transfer Protocol (HTTP) request and response, including headers, status codes, and content.
- **Solution:-** n/a.
- **Business Impact:-** The proper management of HTTP information is essential for ensuring efficient and secure web communication, enhancing user experience, and protecting sensitive data, all of which impact business operations and customer trust.

13.)

- **Vulnerability name:-** Nessus SYN Scanner.

- **Severity:-** -----
- **Plug-in:-**Published :2009/02/04, Modified : 2023/09/25
- **Port:-** 22(TCP).
- **Description:-** The Nessus SYN scanner is a network vulnerability scanner that uses SYN packets to identify open ports and potential security vulnerabilities on target systems.
- **Solution:-** Protect your target with an IP filter.
- **Business Impact:-**The Nessus SYN scanner is a crucial tool for businesses to proactively identify and address network vulnerabilities, enhancing overall cybersecurity posture and reducing the risk of data breaches and service disruptions.

14.)

- **Vulnerability name:-** HSTS Missing From HTTPS Server.(RFC 6797)

- **Severity:-**Medium.
- **Plug-in:-**Published :2020/11/17 , Modified : 2023/06/08
- **Port:-** 443(TCP).
- **Description:-** "HSTS Missing From HTTPS Server (RFC 6797)" indicates the absence of HTTP Strict Transport Security, a security policy mechanism, which may expose the site to security risks and downgrade attacks, as defined by RFC 6797.
- **Solution:-** Configure the remote web server to HSTS.
- **Business Impact:-**The absence of HSTS as per RFC 6797 increases the risk of security breaches and lowers trust in a website, potentially leading to financial losses and reputational damage.

15.)

- **Vulnerability name:-** Web Server allows Password Auto-Completion.

- **Severity:-** Low.
- **Plug-in:-**Published :2009/10/07 Modified : 2023/07/17
- **Port:-** 80(TCP).
- **Description:-** A web server that allows password auto-completion permits browsers to store and autofill login credentials, potentially risking security if used on shared or public computers.
- **Solution:-** Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
- **Business Impact:-**Allowing password auto-completion can compromise user security, lead to unauthorized access, and damage a business's reputation if sensitive data is exposed due to improper credential handling.

16.)

- **Vulnerability name:-** Web Server Transmits cleartext credentials.

- **Severity:-** Low.
- **Plug-in:-**Published :2007/09/28 ,Modified : 2016/11/29
- **Port:-** 80(TCP).
- **Description:-** A web server transmitting cleartext credentials sends login information without encryption, making it susceptible to interception and exposing user data to security risks.
- **Solution:-** Make sure that every sensitive form transmits content over HTTPS.
- **Business Impact:-**
  The business impact of transmitting cleartext credentials includes the risk of data breaches, potential legal consequences, and damage to customer trust, which can lead to reputational harm and financial losses.

17.)

- **Vulnerability name:-** CGI Generic Tests Load Estimation.

- **Severity:-** -----
- **Plug-in:-**Published :2009/10/26, Modified : 2022/04/11
- **Port:-** 80(TCP).
- **Description:-** CGI Generic Tests Load Estimation is a method to assess a web server's capacity to handle Common Gateway Interface (CGI) scripts, helping to determine performance and resource requirements under different loads.
- **Solution:-** n/a
- **Business Impact:-**CGI Generic Tests Load Estimation aids businesses in optimizing web server performance, ensuring reliability under high loads, and preventing service disruptions, ultimately enhancing user experience and reducing operational risks.

18.)

- **Vulnerability name:-** CGI Generic Tests Timeout.

- **Severity:-** -----
- **Plug-in:-**Published :2009/06/19, Modified : 2021/01/19
- **Port:- 80(TCP).**
- **Description:-** CGI Generic Tests Timeout is a measure of the maximum time a web server should allow for the execution of Common Gateway Interface (CGI) scripts, preventing excessive delays in serving web requests.
- **Solution:-** Consider increasing the maximum run time preferences from the web application settings in order to prevent the CGI scanning for timming out.
- **Business Impact:-** Properly configuring CGI Generic Tests Timeout is critical to ensure timely server responses, prevent performance bottlenecks, and maintain user satisfaction, thus avoiding potential business disruptions.

19.)

- Vulnerability name:- External URL’s.

- **Severity:-** -----
- **Plug-in:-**Published :2010/10/04 ,Modified : 2011/08/19
- **Port:-** 80(TCP)
- **Description:-** External URLs are hyperlinks that point to web pages or resources outside the current website's domain or server.
- **Solution:-** n/a.
- **Business Impact:-**
  The inclusion of external URLs in web content can impact business operations and reputation, as it may introduce security risks and potential loss of control over linked content.

20.)

-Vulnerability name:- HTTP Cookie secure property transport mismatch.

- **Severity:-** -----
- **Plug-in:-**Published :2013/09/10 ,Modified : 2021/12/20
- **Port:-** 443(TCP).
- **Description:-** An "HTTP Cookie secure property transport mismatch" occurs when a cookie marked as secure is transmitted over an insecure (non-HTTPS) connection, potentially exposing sensitive information to security risks.
- **Solution:-** n/a
- **Business Impact:-**The business impact of an HTTP Cookie secure property transport mismatch includes the risk of data exposure, reduced trust, and potential security breaches, which can lead to financial losses and reputational damage.

21.)

- Vulnerability name:- HTTP Methods allowed.

- **Severity:-** -----
- **Plug-in:-**Published :2009/12/10 ,Modified : 2022/04/11
- **Port:-** 80(TCP).
- **Description:-**It refers to the types of HTTP request methods (e.g., GET, POST, PUT, DELETE) that a web server permits for communication with the server's resources.
- **Solution:-** n/a
- **Business Impact:-**Properly defining and limiting allowed HTTP methods is crucial to mitigate security risks, prevent unauthorized access, and safeguard sensitive data, protecting business operations and customer trust.

22.)

- Vulnerability name:- Missing content security policy frame ancestors HTTP Response Header.

- **Severity:-** -----
- **Plug-in:-**Published :2010/10/26 ,Modified : 2021/01/19
- **Port:-** 80(TCP).

- **Description:-** It indicates that a security header specifying who can embed the web page in a frame or if frame is not set, potentially exposing the site to click jacking attacks.
- **Solution:-** Set a non-permissive Consent-Security-policy frame-ancestors header for all requested resources.
- **Business Impact:-**
  The absence of the Content Security Policy frame-ancestors header can expose a business to click jacking attacks, data theft, and reputation damage, impacting customer trust and security.
-

23.)

- **Vulnerability name:-** Nessus Scan information.

- **Severity:-** -----
- **Plug-in:-**Published :2005/08/26 ,Modified : 2023/07/31
- **Port:-** 0(TCP).
- **Description:-** A Nessus scan provides detailed information about network vulnerabilities, misconfigurations, and security issues, helping organizations assess and improve their cybersecurity posture by identifying potential threats and weaknesses in their infrastructure and applications.
- **Solution:-** n/a
- **Business Impact:-** Nessus scan information has a significant business impact by enabling organizations to proactively address vulnerabilities, reduce the risk of data breaches, maintain compliance, and enhance overall cybersecurity, ultimately safeguarding reputation and customer trust while preventing financial losses.

24.)

- **Vulnerability name:-** Web application cookies not marked http only.

- **Severity:-** -----
- **Plug-in:-**Published :2015/08/24, Modified : 2015/08/24
- **Port:-** 80(TCP).
- **Description:-** Web application cookies not marked as "Http Only" lack a security attribute that prevents client-side JavaScript from accessing them, potentially making them vulnerable to cross-site scripting (XSS) attacks or other malicious client-side scripts.
- **Solution:-** Each Cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.
- **Business Impact:-**
  The absence of the "Http Only" attribute in web application cookies can result in security risks, allowing attackers to steal user session data, potentially leading to unauthorized access, data breaches, and reputational damage, which can negatively impact business operations and customer trust.

25.)

- **Vulnerability name:-** Web application cookies not marked secure.

- **Severity:- -----**
- **Plug-in:-**Published :2015/08/24 Modified : 2015/08/24
- **Port:-** 80(TCP).

- **Description:-** When web application cookies are not marked as "secure," they can be transmitted over unencrypted HTTP connections, potentially exposing sensitive data to interception and security risks.
- **Solution:-** Each cookie should be carefully reviewed to determine if it contains sensitive data for a security decision.
- **Business Impact:-** If failing to mark cookies as secure in a web application can compromise the security of user data and authentication. It's a best practice to use secure cookies, along with proper HTTPS configuration, to protect sensitive information and maintain the privacy.

26.)

- **Vulnerability name:-** SMB Signing not required.

- **Severity:-** Medium.
- **Plug-in:-**Published :2012/01/19 Modified : 2022/10/05
- **Port:-** 445(TCP).
- **Description:-** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
- **Solution:-** Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
- **Business Impact:-**The absence of SMB signing can result in significant security vulnerabilities, potentially leading to data breaches, unauthorized access, and compliance issues, which can damage an organization's reputation and incur operational and financial costs.

27.)

- **Vulnerability name:-** OS name and installed package Enumeration.

- **Severity:- -----**
- **Plug-in:-**Published :2004/07/06,Modified : 2022/09/26
- **Port:-** 0(TCP).
- **Description:-**
  OS name and installed package enumeration is the process of identifying the operating system and listing the software packages on a computer or server, crucial for system management and security assessment.

- **Solution:-** n/a
- **Business Impact:-**Accurate OS and package enumeration is essential for effective system management and security monitoring, helping organizations maintain up-to-date software, mitigate vulnerabilities, and ensure regulatory compliance, while failures in this process can lead to security gaps and potential exploitation by attackers.

28.)

- **Vulnerability name:-** DCE Services Enumeration.

- **Severity:-** -----
- **Plug-in:-**Published :2001/08/26 ,Modified : 2021/10/04
- **Port:-** 135(TCP).

- **Description:-**
  DCE (Distributed Computing Environment) services enumeration is the process of identifying and listing the available remote services and their attributes in a DCE-based network.

- **Solution:-** n/a.
- **Business Impact:-**DCE services enumeration can have a significant business impact as it helps in identifying potential vulnerabilities, misconfigurations, or unauthorized services in a network, which, if exploited, could lead to security breaches, data loss, or service disruptions, ultimately affecting the organization's reputation and financial stability.

29.)

- **Vulnerability name:-** Host FDQN Resolution.

- **Severity:-** -----
- **Plug-in:-**Published :2004/02/11, Modified : 2017/04/14
- **Port:-** 0(TCP).
- **Description:-**It is the process of converting a human-readable domain name into its corresponding IP address, allowing computers to locate and communicate with remote hosts on the internet or a network.

- **Solution:-** n/a.
- **Business Impact:-**
  Efficient and accurate FQDN resolution is crucial for businesses as it ensures seamless access to web services, applications, and data, enhancing user experience and productivity. However, issues with FQDN resolution can lead to downtime, connectivity problems, and disrupted operations, potentially resulting in lost revenue and damage to the company's reputation.

30.)

- **Vulnerability name:-** NTLMSSP Authentication request Remote Network name disclosure.

- **Severity:-** -----

- **Plug-in: -**Published :2009/11/06, Modified : 2019/11/22
- **Port: -** 445(TCP).

- **Description: -**The NTLMSSP authentication request vulnerability can lead to the disclosure of a remote network name when an attacker exploits weaknesses in the NTLMSSP authentication protocol, potentially revealing sensitive information about a target network.

- **Solution: -**n/a.
- **Business Impact:-**The business impact of NTLMSSP authentication request remote network name disclosure is significant, as it can expose sensitive network information to malicious actors, enabling them to launch targeted attacks, compromise systems, and potentially lead to data breaches, financial losses, and reputational damage for the affected organization.

List of teammates–

S.no	Name	College	Contact
1	Priyanshu Srivastav	VIT Chennai	9717249434
2	Rohan Idiculla Abraham	VIT Chennai	8148817054
3	Gutta Vamsi Krishna	VIT AP	81438 07048
5	Bharath T	VIT Chennai	98941 82091

List of Vulnerability Table

S.no	Vulnerability Name	CWE - No
1	ICMP Timestamp Request Remote Date Disclosure	**200**
2	OS Identification	**78**
3	Device Type	**200**
4	Web Application Potentially Vulnerable to Clickjacking	**693**
5	Web Server Transmits Cleartext Credentials	**522,523,718**
6	Web Application Cookies Not Marked Secure	**522, 718, 724, 928, 930**
7	CGI Generic Injectable Parameter	**86**
8	SQL Injection Vulnerability	**89**
9	Displaying internal server error from tomcat	**502**
10	Cross site Scripting XSS	**79**
11	Insecure Direct Object Reference	**639**
12	Security Misconfiguration	**16**
13	HTTP Server type and Version	**444**
14	Traceroute Infromation	**293**
15	Additional DNS Hostnames	**350**
16	HTTP/2 Cleartext Detection(main start)	**319**
17	OS Identification	**78**

18	Inconsistent Hostname and IP Address	**350**
19	SSL Certificate 'commonName' Mismatch	**297**
20	SSL Certificate Signed Using Weak Hashing Algorithm	**328**
21	Apache Tomcat Detection - Remote Code Execution	**94**
22	Apache Tomcat Detection - Request Smuggling Vulnerability	**444**
23	Apache Tomcat Detection - Privilege Escalation Vulnerability	**269**
24	Web Server No 404 Error Code Check	**404**
25	Insecure cookie setting: missing HttpOnly flag	**1004**
26	Missing security header: X-Content-Type-Options	**16**
27	Unsafe security header: Content-Security-Policy	**693**
28	Missing security header: Referrer-Policy	**200**
29	SQL Injection Vulnerability	**89**
30	CGI Generic XSS	**74,20,79**

Report:

ICMP Timestamp Request Remote Date Disclosure

CWE: - 200

OWASP Category:- Broken Access Control

Description: The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 /2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Business Impacts: Revealing system information can provide attackers with valuable insights into your network architecture and infrastructure. This information can be exploited to plan and execute more targeted attacks.

OS Identification

CWE: - 78

OWASP Category:- Software and Data Integrity Failures

Description: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Business Impacts: An OS identification vulnerability might reveal the specific operating system version and its associated vulnerabilities. Attackers can use this information to target known vulnerabilities in the OS, potentially gaining unauthorized access to the system. This could lead to data breaches, data loss, and damage to the organization's reputation.

Device Type

CWE: - 200

OWASP Category: - Information Exposure

Description: Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Business Impacts: When vulnerabilities are exploited and lead to incidents like data breaches or service disruptions, an organization's reputation can suffer. Customers may lose trust, leading to a loss of business and difficulty acquiring new customers.

Web Application Potentially Vulnerable to Clickjacking

CWE: - 693

OWASP Category: - Security Misconfiguration

Description: The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

Business Impacts: Attackers can use this technique to perform unauthorized actions on behalf of the user, such as making purchases, changing settings, or posting content, which can lead to financial losses or reputation damage.

Web Server Transmits Cleartext Credentials

CWE: - 522,523,718

OWASP Category: - Sensitive Data Exposure

Description: The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

Business Impacts: Cleartext credentials are transmitted without encryption, making them vulnerable to interception by malicious actors. This can lead to data breaches, where sensitive user information, such as usernames and passwords, is exposed.

Web Application Cookies Not Marked Secure

CWE: - 522,718,724,928

OWASP Category: - Insufficient Transport Layer Protection

Description: The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Business Impacts: Users expect their data to be treated with care and security. If a web application does not mark cookies as "Secure," users may lose trust in the application. This can result in decreased user engagement and potentially lead to users abandoning the application for more secure alternatives.

CGI Generic Injectable Parameter

CWE: - 86

OWASP Category: - Injection

Description: The parameter is found to be at risk of cross-site scripting attacks

Business Impacts: Injection attacks can lead to financial losses in various ways, including fraud, theft, and regulatory fines.

SQL Injection Vulnerability (for login bypass)

CWE: - 89

OWASP Category:- Injection

Vulnerability Level: High

Description: The test website https://testfire.net/ is vulnerable to SQL injection attacks, and allows even basic SQL injection attacks, enabling attackers to obtain successful unauthorized access as admin or any user of the website.

Business impacts: SQL injection vulnerability leading to unauthorized access can result in severe data breaches, compromising customer trust and potentially leading to legal repercussions and financial losses.

Displaying internal server error from tomcat

CWE: - 502

OWASP Category:- Injection

Vulnerability Level: High

Description: The website displays all the internal server error along with the entire error trace stack, also displays the Apache tomcat version. The allows attackers to debug or understand the code logics and also find vulnerabilities associated with that specific tomcat server version.

Business impacts: This vulnerability can expose sensitive system information, enabling attackers to identify weaknesses and potentially exploit them, leading to security breaches, data loss, and reputational damage with significant business and financial consequences.

Cross site Scripting XSS

CWE: - 79

OWASP Category:- Injection

Vulnerability Level: Moderate

Description: Improper query field validation or input filed validation. The website doesn't sanitize the input or query fields. Attackers will be able to send crafted inputs to users and can steal sensitive data like cookies and gain access.

Business Impact: Cross-Site Scripting (XSS) can have various business impacts, including compromised user data, damaged reputation, legal liabilities, and financial losses due to potential theft or manipulation of sensitive information, leading to decreased customer trust and operational disruptions.

Insecure Direct Object Reference

CWE: 639.
OWASP Category: - Broken Access Control

Description: Insecure Direct Object Reference is an access control problem that allows an attacker to view data by manipulating an identifier.

Business impact: Insecure Direct Object References (IDOR) occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files.

Security Misconfiguration

CWE : 16

OWASP Category: - Security Misconfiguration

Description : Security misconfigurations are security controls that are inaccurately configured or left insecure, putting your systems and data at risk. Basically, any poorly documented configuration changes, default settings, or a technical issue across any component in your endpoints could lead to a misconfiguration.

Business impact : It a misconfigured database server can cause data to be accessible through a basic web search. If this data includes administrator credentials, an attacker may be able to access further data beyond the database, or launch another attack on the company's servers

HTTP Server type and Version

CWE: 444

OWASP Category: - Security Misconfiguration

Description: This plugin attempts to determine the type and the version of the remote web server.

Business Impacts: Knowing the server type and version allows an attacker to focus on the vulnerabilities of that specific version, whereas someone without this knowledge would have to try different vulnerabilities by brute- force. In addition, some servers disclose the operating system version within HTTP response headers. For example, Apache often discloses UNIX or Windows whilst Microsoft-IIS only runs on Windows, and each version of IIS only runs on a single version of Windows.

Traceroute Information

CWE: 293

OWASP Category: - Security Misconfiguration

Description: A traceroute provides a map of how data on the internet travels from its source to its destination

Business Impacts: One way that a traceroute can be used to determine if a website is hacked is by looking for any unexpected or unfamiliar IP addresses or domains in the traceroute results. If a hacker has gained access to a website, they may have inserted their own code or servers into the website's infrastructure, which would likely show up in a traceroute as an unexpected IP address or domain. Additionally, if a website is experiencing a DDoS attack, the traceroute may show a large number of requests originating from a single IP address or domain, which could indicate that the website is under attack.

Additional DNS Hostnames

CWE: 350

OWASP Category: - security

Description: Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for hosts discovered on a web server. Different web servers may be hosted on name-based virtual hosts.

Business Impacts: An attacker with the ability to conduct a successful cache poisoning attack can cause a nameserver's clients to contact the incorrect, and possibly malicious, hosts for particular services. Consequently, web traffic, email, and other important network data can be redirected to systems under the attacker's control.

HTTP/2 Cleartext Detection

CWE: 319

OWASP Category: - web application

Description: The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

Solution: Limit incoming traffic to this port if desired.

Business Impact: Depending on the industry and location of a business, there may be legal requirements to encrypt certain types of data. Cleartext detection is essential for complying with these regulations, which can have significant legal and financial implications.

OS Identification

CWE: 78

OWASP Category: - Software and Data Integrity Failures

Description: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Business Impacts: An OS identification vulnerability might reveal the specific operating system version and its associated vulnerabilities. Attackers can use this information to target known vulnerabilities in the OS, potentially gaining unauthorized access to the system. This could lead to data breaches, data loss, and damage to the organization's reputation.

Inconsistent Hostname and IP Address

CWE: 350

OWASP Category: - Security Misconfiguration

Description: This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and leave unclosed connections on the remote target, if the network is loaded.

Solution:

Protect your target with an IP filter.

Business Impact:

Inconsistent hostname and IP address configurations can lead to network disruptions and connectivity issues. Inconsistent configurations can be exploited by malicious actors to launch attacks on your network. This can result in incorrect routing, failed DNS resolution, and other configuration-related issues that affect the functionality and reliability of your network.

SSL Certificate 'commonName' Mismatch

CWE: 350

OWASP Category: - Transport Layer Protection

Description: The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution:

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Business Impact:

This mismatch can be exploited by attackers to launch man-in-the-middle (MITM) attacks, intercept sensitive data, or impersonate the legitimate website. This poses a significant security risk to both the business and its customers.

SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

CWE: 328

OWASP Category: - Cryptographic Failures

Description: The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm. These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service. Known certificate

authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

Business Impact:

Weak hashing algorithms, such as MD5 or SHA-1, are susceptible to cryptographic attacks. Attackers can exploit these vulnerabilities to forge certificates, intercept encrypted data, or impersonate a legitimate website. Search engines like Google consider website security when ranking search results. Sites with SSL certificates signed using weak algorithms may experience a decline in search engine rankings, leading to reduced online visibility and potentially decreased organic traffic. Various industry standards and regulations (e.g., PCI DSS) require websites to use strong encryption and secure hashing algorithms. Using weak hashing algorithms can lead to non-compliance, potentially resulting in fines and legal consequences.

Apache Tomcat Detection - Remote Code Execution

CWE:94

OWASP Category: - Injection

Description
Nessus was able to detect a remote Apache Tomcat web server. The installed Tomcat version is 9.0.20. The version of Tomcat installed on the remote host is prior to 9.0.35. It is, therefore, affected by a remote code execution vulnerability as referenced in the fixed_in_apache_tomcat_9.0.35_security-9 advisory. An arbitrary file read vulnerability exists in Tomcat's Apache JServ Protocol (AJP) due to an implementation defect. A remote, unauthenticated attacker could exploit this to access files which, under normal conditions, would be restricted. If the Tomcat instance supports file uploads, the vulnerability could also be leveraged to achieve remote code execution. (CVE-2020-1938)

Business Impact:

This Apache Tomcat vulnerability presents a critical business impact, including the risk of data breaches with financial, legal, and reputational repercussions, potential service disruptions causing revenue loss and customer dissatisfaction, the specter of non-compliance with data protection regulations leading to substantial fines and legal liabilities, erosion of customer trust, and reputational damage with the potential loss of competitive advantage, as well as operational and financial impacts through remediation efforts, legal costs, and resource allocation for mitigation.

Apache Tomcat Detection - Request Smuggling Vulnerability

CWE: 444

OWASP Category: - Injection

Description
The version of Tomcat installed on the remote host is 9.0.0-M1 or later but prior to 9.0.68. It is, therefore, affected by a request smuggling vulnerability as referenced in the fixed_in_apache_tomcat_9.0.68_security-9

advisory. If Tomcat was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (not the default), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

Business Impact:

In the presence of a reverse proxy that also fails to reject requests with invalid headers, this vulnerability allows for malicious actors to potentially manipulate and compromise the server's behavior, leading to potential data breaches, service disruptions, and reputational damage. The consequences include data integrity risks, loss of service availability, potential regulatory non-compliance, and the erosion of customer trust, all of which can result in financial loss and legal liabilities. Addressing this vulnerability promptly is crucial to mitigate these risks and ensure the security and resilience of your web server infrastructure.

Apache Tomcat Detection - Privilege Escalation Vulnerability

CWE:269

OWASP Category: - Injection

Description
The version of Tomcat installed on the remote host is prior to 9.0.30. It is, therefore, affected by a privilege escalation vulnerability as referenced in the 'Fixed in Apache Tomcat 9.0.30' advisory.

- When using FORM authentication there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563)

Business Impact:

The privilege escalation vulnerability found in the pre-9.0.30 Apache Tomcat version introduces a significant security risk, as it opens the door to potential session fixation attacks, jeopardizing data integrity and confidentiality. While considered challenging to exploit, it presents a credible threat that could result in unauthorized access, operational disruptions, reputational damage, regulatory non-compliance, and resource allocation for mitigation, including legal liabilities, making it imperative to promptly update to a secure version (9.0.30 or later) to mitigate these potential business impacts.

Web Server No 404 Error Code Check

CWE: 404

OWASP Category: - Security Misconfiguration

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning instead a site map, search page or authentication page.

Business Impact:

Not returning a 404 error for missing pages might provide misleading information to users. They may think that content is available when it's not, leading to frustration.

Insecure cookie setting: missing HttpOnly flag

CSE: 1004

OWASP Category: -

Description: A cookie has been set without the `HttpOnly` flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted to another site. In case of a session cookie, this could lead to session hijacking.

Business Impact: Without the HttpOnly flag, malicious scripts running on a user's browser can access the cookie data, potentially exposing sensitive information, session tokens, or user credentials.

Missing security header: X-Content-Type-Options

CSE: 16

OWASP Category: - Broken Authentication

Description: The HTTP header `X-Content-Type-Options` is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Business Impact: Addressing security breaches, handling data breaches, and regaining trust can be costly, both in terms of financial resources and time.

Unsafe security header: Content-Security-Policy

CSE: 693

OWASP Category: - Security Misconfiguration

Description: The HTTP header `X-Content-Type-Options` is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Business Impact: Many industries and regions have regulations and compliance requirements related to data protection and web security. Failing to implement a proper CSP can lead to non-compliance, potentially resulting in fines and legal consequences.

Missing security header: Referrer-Policy

CSE: 200

OWASP Category: - Security Misconfiguration

Description: The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application. For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Business Impact: Attackers can use referrer information to gather intelligence about your website's structure and potential vulnerabilities. This information can be used to launch targeted attacks.

SQL Injection Vulnerability

CWE: - 89

OWASP Category: - Injection

Description: The website is vulnerable to SQL injection attacks, and allows even basic SQL injection attacks, enabling attackers to obtain successful unauthorized access as admin or any user of the website.

Business impacts: SQL injection vulnerability leading to unauthorized access can result in severe data breaches, compromising customer trust and potentially leading to legal repercussions and financial losses.

CGI Generic XSS

CWE: - 20,79,74

OWASP Category: - Injection

Description: The remote web server hosts CGI scripts that fail to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS are likely to be 'non-persistent' or 'reflected'.

Business Impacts: Attackers can hijack user sessions, allowing them to impersonate users and perform unauthorized actions on the web application, potentially leading to financial fraud or unauthorized access.

Practice Website Vulnerabilities

Vulnerability Name: ICMP Timestamp Request Remote Date Disclosure

CWE: 200

Description: The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 /2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Business Impacts: Revealing system information can provide attackers with valuable insights into your network architecture and infrastructure. This information can be exploited to plan and execute more targeted attacks.

Vulnerability Pub Date: January 1, 1995

Vulnerability Path: http://testfire.net/

Vulnerability Name: OS Identification

Description: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Business Impacts: An OS identification vulnerability might reveal the specific operating system version and its associated vulnerabilities. Attackers can use this information to target known vulnerabilities in the OS, potentially gaining unauthorized access to the system. This could lead to data breaches, data loss, and damage to the organization's reputation.

Vulnerability Path: http://testfire.net/

Vulnerability Name: Device Type

Description: Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Business Impacts: When vulnerabilities are exploited and lead to incidents like data breaches or service disruptions, an organization's reputation can suffer. Customers may lose trust, leading to a loss of business and difficulty acquiring new customers.

Vulnerability Path: http://testfire.net/

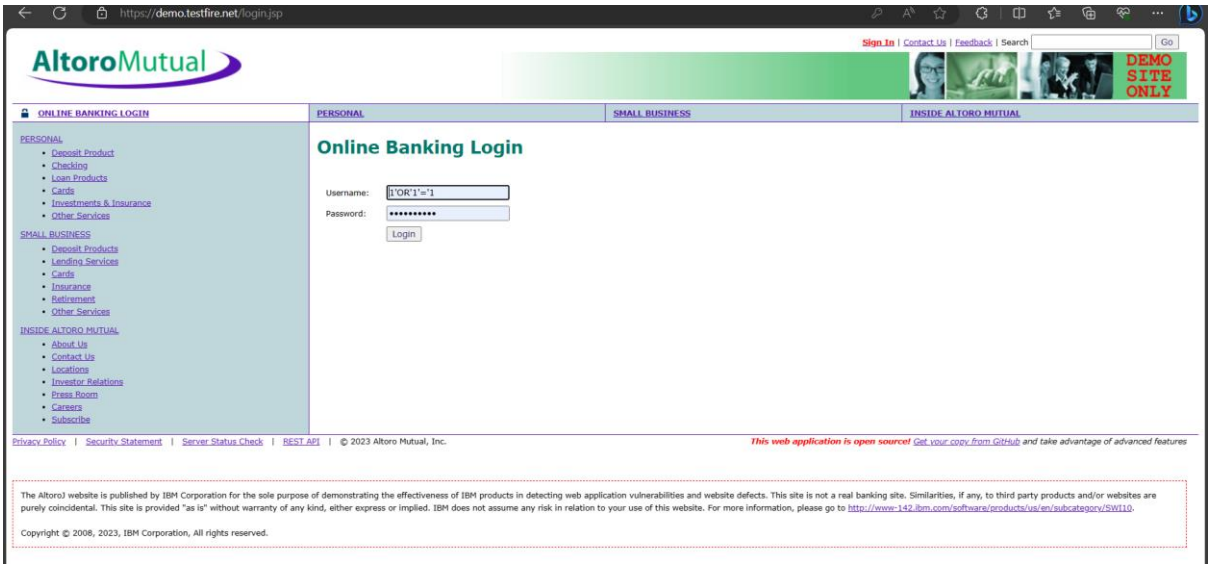
Vulnerability Name: SQL Injection Vulnerability (for login bypass)

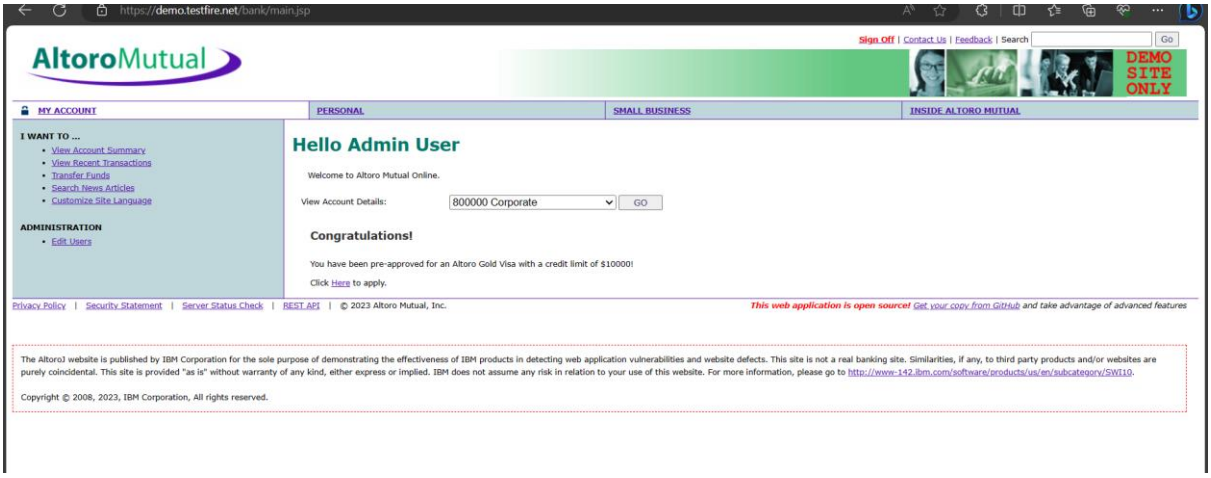
Vulnerability Level: High

Description: The test website https://testfire.net/ is vulnerable to SQL injection attacks, and allows even basic SQL injection attacks, enabling attackers to obtain successful unauthorized access as admin or any user of the website.

Business impacts: SQL injection vulnerability leading to unauthorized access can result in severe data breaches, compromising customer trust and potentially leading to legal repercussions and financial losses.

Vulnerability path: https://demo.testfire.net/login.jsp





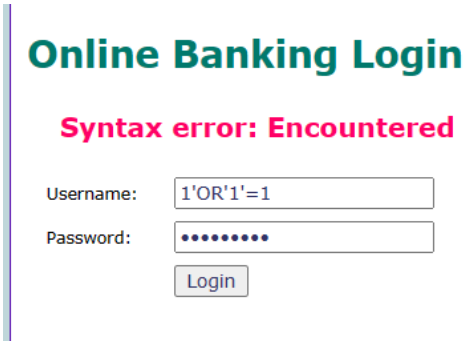
Vulnerability Name: Displaying internal server error from tomcat

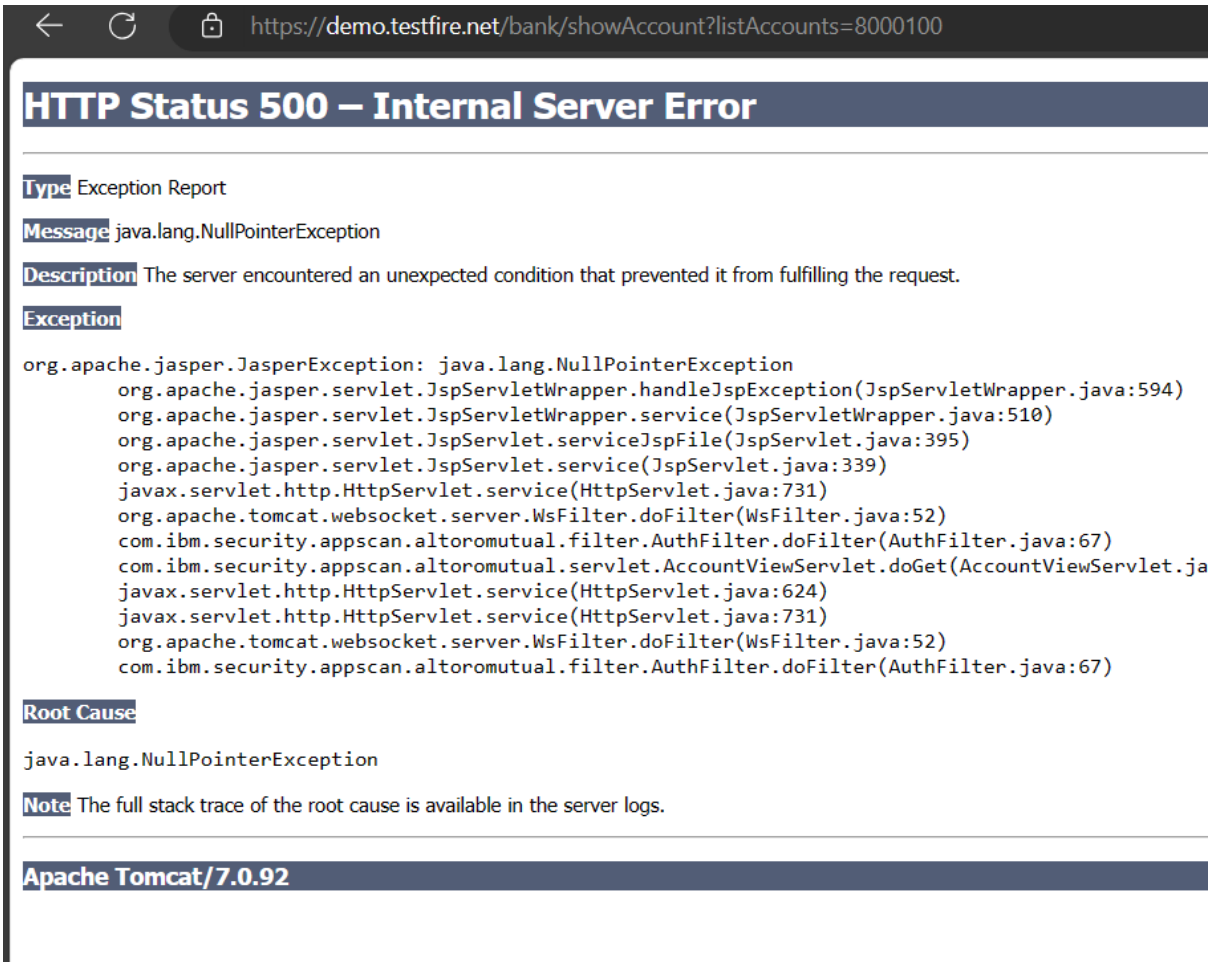
Vulnerability Level: High

Description: The website displays all the internal server error along with the entire error trace stack, also displays the Apache tomcat version. The allows attackers to debug or understand the code logics and also find vulnerabilities associated with that specific tomcat server version.

Business impacts: This vulnerability can expose sensitive system information, enabling attackers to identify weaknesses and potentially exploit them, leading to security breaches, data loss, and reputational damage with significant business and financial consequences.

Vulnerability path: https://demo.testfire.net/login.jsp





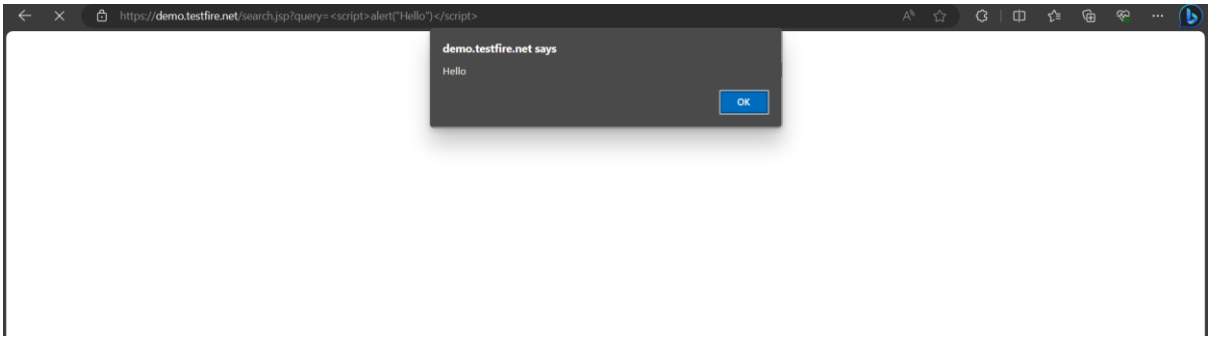
Vulnerability Name: Cross site Scripting XSS

Vulnerability Level: Moderate

Description: Improper query field validation or input filed validation. The website doesn't sanitize the input or query fields. Attackers will be able to send crafted inputs to users and can steal sensitive data like cookies and gain access.

Business Impact: Cross-Site Scripting (XSS) can have various business impacts, including compromised user data, damaged reputation, legal liabilities, and financial losses due to potential theft or manipulation of sensitive information, leading to decreased customer trust and operational disruptions.

Vulnerability path: https://demo.testfire.net/search.jsp?query



Vulnerability name : Insecure Direct Object Reference.

CWE : 639.

Description : Insecure Direct Object Reference is an access control problem that allows an attacker to view data by manipulating an identifier.

Business impact : Insecure Direct Object References (IDOR) occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files.

Vulnerability path : https://demo.testfire.net/

Vulnerability name : Security Misconfiguration

CWE : OWASP A05 Category.

Description : Security misconfigurations are security controls that are inaccurately configured or left insecure, putting your systems and data at risk. Basically, any poorly documented configuration changes, default settings, or a technical issue across any component in your endpoints could lead to a misconfiguration.

Business impact : It a misconfigured database server can cause data to be accessible through a basic web search. If this data includes administrator credentials, an attacker may be able to access further data beyond the database, or launch another attack on the company's servers.

Vulnerability path : https://demo.testfire.net/

Vulnerability Name:HTTP Server type and Version

CWE: 444

Description: This plugin attempts to determine the type and the version of the remote web server.

Business Impacts: Knowing the server type and version allows an attacker to focus on the vulnerabilities of that specific version, whereas someone without this knowledge would have to try different vulnerabilities by brute- force. In addition, some servers disclose the operating system version within HTTP response headers. For example, Apache often discloses UNIX or Windows whilst Microsoft-IIS only runs on Windows, and each version of IIS only runs on a single version of Windows.

Vulnerability Pub Date: 1/4/2000

Vulnerability Path: http://testfire.net/

Vulnerability Name: Traceroute Infromation

Description: A traceroute provides a map of how data on the internet travels from its source to its destination

Business Impacts: One way that a traceroute can be used to determine if a website is hacked is by looking for any unexpected or unfamiliar IP addresses or domains in the traceroute results. If a hacker has gained access to a website, they may have inserted their own code or servers into the website's infrastructure, which would likely show up in a traceroute as an unexpected IP address or domain. Additionally, if a website is experiencing a DDoS attack, the traceroute may show a large number of requests originating from a single IP address or domain, which could indicate that the website is under attack.

Vulnerability Path: http://testfire.net/

Vulnerability Name: Additional DNS Hostnames

Description: Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for hosts discovered on a web server. Different web servers may be hosted on name-based virtual hosts.

Business Impacts: An attacker with the ability to conduct a successful cache poisoning attack can cause a nameserver's clients to contact the incorrect, and possibly malicious, hosts for particular services.

Consequently, web traffic, email, and other important network data can be redirected to systems under the attacker's control.

Vulnerability Path: http://testfire.net/

Main Website Vulnerabilities

Team 1.5

Website: https://vtopcc.vit.ac.in/vtop/login

Host Fully Qualified Domain Name (FQDN) Resolution

Description: It was possible to resolve the name of the remote host.

Business Impact: Properly managing FQDN resolution is critical for cybersecurity. Attackers can manipulate DNS records to redirect users to malicious websites or intercept sensitive data. A strong FQDN resolution system can help protect against DNS-related attacks.

Vulnerability Path: 115.240.194.17

HTTP/2 Cleartext Detection

Description: The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

Solution: Limit incoming traffic to this port if desired.

Business Impact: Depending on the industry and location of a business, there may be legal requirements to encrypt certain types of data. Cleartext detection is essential for complying with these regulations, which can have significant legal and financial implications.

Vulnerability Path: 115.240.194.17

OS Identification

Description: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Business Impacts: An OS identification vulnerability might reveal the specific operating system version and its associated vulnerabilities. Attackers can use this information to target known vulnerabilities in the OS, potentially gaining unauthorized access to the system. This could lead to data breaches, data loss, and damage to the organization's reputation.

Vulnerability Path: 115.240.194.17

46215 - Inconsistent Hostname and IP Address

Description: This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and leave unclosed connections on the remote target, if the network is loaded.

Solution:

Protect your target with an IP filter.

Business Impact:

Inconsistent hostname and IP address configurations can lead to network disruptions and connectivity issues. Inconsistent configurations can be exploited by malicious actors to launch attacks on your network. This can result in incorrect routing, failed DNS resolution, and other configuration-related issues that affect the functionality and reliability of your network.

Vulnerability Path:

122.187.117.185

45410 - SSL Certificate 'commonName' Mismatch

Description: The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution:

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Business Impact:

This mismatch can be exploited by attackers to launch man-in-the-middle (MITM) attacks, intercept sensitive data, or impersonate the legitimate website. This poses a significant security risk to both the business and its customers.

Vulnerability Path:

122.187.117.185

SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Description: The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm. These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service. Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

Business Impact:

Weak hashing algorithms, such as MD5 or SHA-1, are susceptible to cryptographic attacks. Attackers can exploit these vulnerabilities to forge certificates, intercept encrypted data, or impersonate a legitimate website. Search engines like Google consider website security when ranking search results. Sites with SSL certificates signed using weak algorithms may experience a decline in search engine rankings, leading to reduced online visibility and potentially decreased organic traffic. Various industry standards and regulations (e.g., PCI DSS) require websites to use strong encryption and secure hashing algorithms. Using weak hashing algorithms can lead to non-compliance, potentially resulting in fines and legal consequences.

Vulnerability Path:

122.187.117.185

Apache Tomcat Detection - Remote Code Execution

Description
Nessus was able to detect a remote Apache Tomcat web server. The installed Tomcat version is 9.0.20. The version of Tomcat installed on the remote host is prior to 9.0.35. It is, therefore, affected by a remote code execution vulnerability as referenced in the fixed_in_apache_tomcat_9.0.35_security-9 advisory. An arbitrary file read vulnerability exists in Tomcat's Apache JServ Protocol (AJP) due to an implementation defect. A remote, unauthenticated attacker could exploit this to access files which, under normal conditions, would be restricted. If the Tomcat instance supports file uploads, the vulnerability could also be leveraged to achieve remote code execution. (CVE-2020-1938)

Business Impact:

This Apache Tomcat vulnerability presents a critical business impact, including the risk of data breaches with financial, legal, and reputational repercussions, potential service disruptions causing revenue loss and customer dissatisfaction, the specter of non-compliance with data protection regulations leading to

substantial fines and legal liabilities, erosion of customer trust, and reputational damage with the potential loss of competitive advantage, as well as operational and financial impacts through remediation efforts, legal costs, and resource allocation for mitigation.

Vulnerability Path: 122.187.117.185

Apache Tomcat Detection - Request Smuggling Vulnerability

Description

The version of Tomcat installed on the remote host is 9.0.0-M1 or later but prior to 9.0.68. It is, therefore, affected by a request smuggling vulnerability as referenced in the fixed_in_apache_tomcat_9.0.68_security-9 advisory. If Tomcat was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (not the default), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

Business Impact:

In the presence of a reverse proxy that also fails to reject requests with invalid headers, this vulnerability allows for malicious actors to potentially manipulate and compromise the server's behavior, leading to potential data breaches, service disruptions, and reputational damage. The consequences include data integrity risks, loss of service availability, potential regulatory non-compliance, and the erosion of customer trust, all of which can result in financial loss and legal liabilities. Addressing this vulnerability promptly is crucial to mitigate these risks and ensure the security and resilience of your web server infrastructure.

Vulnerability Path: 122.187.117.185

Apache Tomcat Detection - Privilege Escalation Vulnerability

Description

The version of Tomcat installed on the remote host is prior to 9.0.30. It is, therefore, affected by a privilege escalation vulnerability as referenced in the 'Fixed in Apache Tomcat 9.0.30' advisory.

- When using FORM authentication there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563)

Business Impact:

The privilege escalation vulnerability found in the pre-9.0.30 Apache Tomcat version introduces a significant security risk, as it opens the door to potential session fixation attacks, jeopardizing data integrity and confidentiality. While considered challenging to exploit, it presents a credible threat that could result in unauthorized access, operational disruptions, reputational damage, regulatory non-compliance, and resource allocation for mitigation, including legal liabilities, making it imperative to promptly update to a secure version (9.0.30 or later) to mitigate these potential business impacts.

Vulnerability Path: 122.187.117.185

Web Server No 404 Error Code Check

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning instead a site map, search page or authentication page.

Business Impact:

Not returning a 404 error for missing pages might provide misleading information to users. They may think that content is available when it's not, leading to frustration.

Vulnerability Path: 122.187.117.185

Nessus Overview:-

- **Description:**
- Nessus is widely used vulnerability scanning tool and security software developed by tenable, Inc. It is primarily used to identify and access vulnerabilities in computer systems, networks, and applications.

- **Applications of Nessus:**

- 1. Vulnerability Scanning:

  Nessus is primarily known for its vulnerability scanning capabilities. It can target systems for known security issues, misconfigurations, and weaknesses. This helps organizations identify potential entry points for attackers and prioritize their remediation efforts.

- 2. Plugin-Based Architecture:

  Nessus uses plugin-in-based architecture, where plugins are small programs or scripts that check for specific vulnerabilities or issues. This architecture allows nessus to support a wide range of vulnerabilities and technologies.

- 3. Comprehensive Coverage:

  Nessus is capable of scanning a broad spectrum of system and devices, including servers, workstations, networking equipment, and web applications. It covers various operating systems and software packages.

- 4. Scanning Types: It supports different types of scans, such as credentialed scans, and uncredentialed scans, and compliance scans.

- 5. Risk Management:

Nessus provides a risk management by assigning severity levels to identified vulnerabilities, allowing organizations to focus on the most critical issues first.

- 6.Customization:

  Users can customize scans to meet their specific needs. This includes scheduling scans, defining scan policies, and tailoring the scan scope.

- 7.Reporting:

  Nessus generates detailed reports that provide a clear overview of the vulnerabilities discovered during the scan. These reports can be useful for compliance purposes and to communicate security status to stakeholders.

- 8. Integration:

  It can be integrated with other security tools and systems, such as SIEM (SecurityInformationandEventManagement)solutions,toenhanceanorganization's overall security posture.

- Target ip address:-

- 115.240.194.13

- 52.66.12.101

- 127.0.0.1

- 172.67.222.140

- List of vulnerability :-

S.No	Vulnerability name	Severity	Plug-in Information
1	PHP Multiple Vulnerabilities.	Critical.	Published :2022/11/03 Modified : 2023/10/05
2	PHP Unsupported Version Detection.	Critical.	Published :2012/05/04 Modified : 2022/12/07
3	SSL Certificate Cannot be trusted.	Medium.	Published :2010/12/15 Modified : 2020/04/27
4	TLS Version 1.0 Protocol Detection.	Medium.	Published :2017/11/22 Modified : 2023/04/19
5	TLS Version 1.0 Protocol Deprecated.	Medium.	Published :2022/04/04 Modified : 2023/04/19
6	Apache HTTP Server Version.	-----	Published :2010/07/30 Modified : 2023/08/17
7	Backported Security Path Detection.	-----	Published :2009/06/25Modified : 2015/07/07
8	Common Platform Enumeration.	-----	Published :2010/04/21 Modified : 2023/10/16
9	Device Type.	-----	Published :2011/05/23 Modified : 2022/09/09

10	HSTS Missing From HTTPS Server.	-----	Published :2017/11/22 Modified : 2023/04/19
11	HTTP Server Type and Version.	-----	Published :2000/01/04 Modified : 2020/10/30
12	HTTP Information.	-----	Published :2007/01/30 Modified : 2019/11/22
13	Nessus SYN Scanner.	-----	Published :2009/02/04 Modified : 2023/09/25
14	HSTS Missing From HTTPS Server.(RFC 6797)	-----	Published :2020/11/17 Modified : 2023/06/08
15	Web Server allows Password Auto-Completion.	Medium	Published :2009/10/07 Modified : 2023/07/17
16	Web Server Transmits clear text credentials.	Low.	Published :2007/09/28 Modified : 2016/11/29
17	CGI Generic Tests Load Estimation.	Low.	Published :2009/10/26 Modified : 2022/04/11
18	CGI Generic Tests Timeout.	-----	Published :2009/06/19 Modified : 2021/01/19
19	External URL′s.	-----	Published :2010/10/04 Modified : 2011/08/19
20	HTTP Cookie secure property transport mismatch.	-----	Published :2013/09/10 Modified : 2021/12/20
21	HTTP Methods allowed.	-----	Published :2009/12/10 Modified : 2022/04/11

22	Missing content security policy frame ancestors HTTP Response Header.	-----	Published :2010/10/26 Modified : 2021/01/19
23	Nessus Scan information.	-----	Published :2005/08/26Modified : 2023/07/31
24	Web application cookies not marked http only.	-----	Published :2015/08/24 Modified : 2015/08/24
25	Web application cookies not marked secure.	-----	Published :2015/08/24 Modified : 2015/08/24
26	SMB Signing not required.	-----	Published :2012/01/19 Modified : 2022/10/05
27	OS name and installed package Enumeration.	Medium.	Published :2004/07/06 Modified : 2022/09/26
28	DCE Services Enumeration.	-----	Published :2001/08/26 Modified : 2021/10/04
29	Host FDQN Resolution.	-----	Published :2004/02/11 Modified : 2017/04/14
30	NTLMSSP Authentication request Remote Network name disclosure.	-----	Published :2009/11/06 Modified : 2019/11/22

REPORT:-

1.)

- **Vulnerability name:-**PHP Multiple Vulnerabilities.
- **Severity:-**Critical.
- **Plug-in:-** Published :2022/11/03 ,Modified : 2023/10/05
- **Port:-**80(TCP).
- **Description:-**PHP vulnerabilities encompass a range of security issues, including SQL injection, cross-site scripting (XSS), and remote code execution, which can lead to data breaches, service disruptions, and financial losses in web applications.
- **Solution:-**Upgrade to PHP version 7.4.33 or later.
- **Business Impact:-**Multiple PHP vulnerabilities can lead to financial losses, data breaches, reputational damage, and legal consequences, undermining a business's operations and customer trust.

2.)

- **Vulnerability name:-** PHP Unsupported Version Detection.
- **Severity:-** Critical.
- **Plug-in:-**Published :2012/05/04 ,Modified : 2022/12/07
- **Port:-** 80(TCP).
- **Description:-**PHP Unsupported Version Detection is a process of identifying outdated and unsupported PHP versions in web applications, which poses security risks and may require an upgrade to maintain system integrity and protect against vulnerabilities.
- **Solution:-** The remote host contains the unsupported version of a web application scripting language.
- **Business Impact:-**Detecting unsupported PHP versions is essential for business security as it helps prevent potential vulnerabilities and data breaches. Failure to address unsupported versions can result in security risks, regulatory compliance issues, and reputational damage.

3.)

- **Vulnerability name:-** SSL Certificate Cannot be trusted.

- **Severity:-** Medium.
- **Plug-in:-**Published :2010/12/15 ,Modified : 2020/04/27
- **Port:-** 443(TCP).
- **Description:-** SSL certificate cannot be trusted" indicates that a website's certificate isn't recognized or validated by trusted authorities, potentially exposing users to security risks.

- **Solution:-** Purchase or generate a proper SSL certificate for this service.
- **Business Impact:-**When an SSL certificate is not trusted, it erodes user trust, leads to data breaches, and can result in lost revenue and reputational damage, as customers may avoid the site due to security concerns. Addressing this issue promptly is crucial for maintaining business integrity and security.

4.)

- **Vulnerability name:-** TLS Version 1.0 Protocol Detection.

- **Severity:-** Medium.
- **Plug-in:-**Published :2017/11/22 ,Modified : 2023/04/19
- **Port:-** 443(TCP).
- **Description:-** TLS Version 1.0 Protocol Detection is the process of identifying and determining the usage of the TLS 1.0 encryption protocol in a network, which is considered outdated and potentially insecure.

- **Solution:-** Enable support for TLS 1.2 and 1.3, and disable support for 1.0
- **Business Impact:-**The detection of TLS 1.0 usage in a business environment can signal security vulnerabilities, increase the risk of data breaches, and lead to regulatory non-compliance, potentially resulting in financial losses, reputational damage, and legal consequences.

5.)

- **Vulnerability name:-** TLS Version 1.0 Protocol Deprecated.

- **Severity:-** Medium.

- **Plug-in:-**Published :2022/04/04 ,Modified : 2023/04/19

- **Port:-** 443(TCP).

- **Description:-** "TLS Version 1.0 Protocol Deprecated" means that TLS 1.0, an outdated and insecure encryption protocol, is no longer recommended for use due to known security vulnerabilities.

- **Solution:-** Enable support for TLS 1.2 and 1.3, and disable support for 1.1

- **Business Impact:-**The deprecation of TLS 1.0 mandates its replacement to maintain security standards; non-compliance can lead to data breaches, legal issues, and reputational damage, impacting customer trust and business continuity.

6.)

- **Vulnerability name:-** Apache HTTP Server Version.

- **Severity:-** -----
- **Plug-in:-**Published :2010/07/30 ,Modified : 2023/08/17
- **Port:-** 80(TCP).
- **Description:-**

  The Apache HTTP Server Version is a software component that provides web

  server capabilities, allowing it to serve web pages to clients over the

  internet.

- **Solution:- n/a**
- **Business Impact:-**Publicly revealing the Apache HTTP Server version can expose potential vulnerabilities, making the server a target for cyberattacks, which may lead to service disruptions, data breaches, and reputational damage, impacting business operations and customer trust. To mitigate these risks, businesses often hide or obscure server version information and maintain vigilant security practices.

7.)

- Vulnerability name:- Backported Security Path Detection.

Severity:- -----

- **Plug-in:-**Published :2009/06/25 ,Modified : 2015/07/07
- **Port:-** 22(SSH).
- **Description:-** "Backported Security Patch Detection" is the process of identifying and verifying the application of security patches that have been applied to older software versions to address vulnerabilities and improve security.

- **Solution:- n/a**

Business Impact:-

Efficient backported security patch detection helps mitigate security risks, reduces the potential for data breaches and service disruptions, and demonstrates a commitment to robust cybersecurity, safeguarding business reputation and customer trust.

8.)

- Vulnerability name:- Common Platform Enumeration.

- **Severity:-** -----

- **Plug-in:-**Published :2010/04/21 ,Modified : 2023/10/16.
- **Port:- 0(TCP).**
- **Description:-** Common Platform Enumeration (CPE) is a standardized naming scheme to identify and describe software applications and operating systems based on their attributes and version information.

- **Solution:- n/a**
- **Business Impact:-**
  Common Platform Enumeration (CPE) aids businesses in managing and securing software assets by providing standardized identification, reducing the risk of vulnerabilities, and facilitating compliance, ultimately enhancing cybersecurity posture and minimizing operational risks.

9.)

- **Vulnerability name:-** Device Type.

- **Severity:-** -----
- **Plug-in:-**Published :2011/05/23 Modified : 2022/09/09
- **Port:-** 0(TCP).
- **Description:-** Device type refers to the category or classification of a hardware device based on its purpose, design, and functionality, such as a smartphone, laptop, or printer.

- **Solution:- n/a**
- **Business Impact:-**
  Understanding the device type is critical for businesses to tailor their services, optimize user experience, and ensure compatibility, which can lead to increased customer satisfaction and operational efficiency while minimizing support and compatibility issues.

10.)

- **Vulnerability name:-** HSTS Missing From HTTPS Server.

- **Severity:-** -----
- **Plug-in:-**Published :2017/11/22 ,Modified : 2023/04/19
- **Port:-** 443(TCP).
- **Description:-** "HSTS Missing from HTTPS Server" indicates that the server is not implementing HTTP Strict Transport Security, a security policy mechanism, which may expose the site to security risks and downgrade attacks.

- **Solution:-** Configure the remote web server to use HSTS.
- **Business Impact:-**
  The absence of HSTS leaves the website vulnerable to man-in-the-middle attacks and security breaches, potentially eroding customer trust and harming the business's reputation. Implementing HSTS is crucial to enhance security and protect sensitive user data, fostering trust and compliance with security standards.

11.)

- **Vulnerability name:-** HTTP Server Type and Version.

- **Severity:-** -----
- **Plug-in:-**Published :2017/11/22 ,Modified : 2023/04/1
- **Port:-** 80(TCP).
- **Description:-** HTTP Server Type and Version refers to the software and version information of the web server handling HTTP requests, which can be used to identify potential vulnerabilities or misconfigurations.

- **Solution:- n/a**
- **Business Impact:-**Revealing HTTP server type and version can expose security weaknesses, making the server a target for cyberattacks and potentially leading to service disruptions, data breaches, and reputational damage, which can negatively impact business operations and customer trust. To mitigate these risks, businesses often hide or obscure server information and maintain vigilant security practices.

12.)

- **Vulnerability name:-** HTTP Information.

- **Severity:-** -----
- **Plug-in:-**Published :2007/01/30 , Modified : 2019/11/22
- **Port:-** 80(TCP).
- **Description:-** HTTP Information encompasses data exchanged between a client and server during a Hypertext Transfer Protocol (HTTP) request and response, including headers, status codes, and content.

- **Solution:-** n/a.
- **Business Impact:-** The proper management of HTTP information is essential for ensuring efficient and secure web communication, enhancing user experience, and protecting sensitive data, all of which impact business operations and customer trust.

13.)

- **Vulnerability name:-** Nessus SYN Scanner.

- **Severity:-** -----
- **Plug-in:-**Published :2009/02/04, Modified : 2023/09/25
- **Port:-** 22(TCP).
- **Description:-** The Nessus SYN scanner is a network vulnerability scanner that uses SYN packets to identify open ports and potential security vulnerabilities on target systems.

- **Solution:-** Protect your target with an IP filter.
- **Business Impact:-**The Nessus SYN scanner is a crucial tool for businesses to proactively identify and address network vulnerabilities, enhancing overall cybersecurity posture and reducing the risk of data breaches and service disruptions.

14.)

- **Vulnerability name:-** HSTS Missing From HTTPS Server.(RFC 6797)

- **Severity:-**Medium.
- **Plug-in:-**Published :2020/11/17 , Modified : 2023/06/08
- **Port:-** 443(TCP).
- **Description:-** "HSTS Missing From HTTPS Server (RFC 6797)" indicates the absence of HTTP Strict Transport Security, a security policy mechanism, which may expose the site to security risks and downgrade attacks, as defined by RFC 6797.

- **Solution:-** Configure the remote web server to HSTS.
- **Business Impact:-**The absence of HSTS as per RFC 6797 increases the risk of security breaches and lowers trust in a website, potentially leading to financial losses and reputational damage.

15.)

- **Vulnerability name:-** Web Server allows Password Auto-Completion.

- **Severity:-** Low.
- **Plug-in:-**Published :2009/10/07 Modified : 2023/07/17
- **Port:-** 80(TCP).
- **Description:-** A web server that allows password auto-completion permits browsers to store and autofill login credentials, potentially risking security if used on shared or public computers.

- **Solution:-** Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
- **Business Impact:-**Allowing password auto-completion can compromise user security, lead to unauthorized access, and damage a business's reputation if sensitive data is exposed due to improper credential handling.

16.)

- **Vulnerability name:-** Web Server Transmits cleartext credentials.

- **Severity:-** Low.
- **Plug-in:-**Published :2007/09/28 ,Modified : 2016/11/29
- **Port:-** 80(TCP).
- **Description:-** A web server transmitting cleartext credentials sends login information without encryption, making it susceptible to interception and exposing user data to security risks.

- **Solution:-** Make sure that every sensitive form transmits content over HTTPS.
- **Business Impact:-**
  The business impact of transmitting cleartext credentials includes the risk of data breaches, potential legal consequences, and damage to customer trust, which can lead to reputational harm and financial losses.

17.)

- **Vulnerability name:-** CGI Generic Tests Load Estimation.

- **Severity:-** -----
- **Plug-in:-**Published :2009/10/26, Modified : 2022/04/11
- **Port:-** 80(TCP).
- **Description:-** CGI Generic Tests Load Estimation is a method to assess a web server's capacity to handle Common Gateway Interface (CGI) scripts, helping to determine performance and resource requirements under different loads.

- **Solution:-** n/a
- **Business Impact:-**CGI Generic Tests Load Estimation aids businesses in optimizing web server performance, ensuring reliability under high loads, and preventing service disruptions, ultimately enhancing user experience and reducing operational risks.

18.)

- **Vulnerability name:-** CGI Generic Tests Timeout.

- **Severity:-** -----
- **Plug-in:-**Published :2009/06/19, Modified : 2021/01/1
- **Port:- 80(TCP).**
- **Description:-** CGI Generic Tests Timeout is a measure of the maximum time a web server should allow for the execution of Common Gateway Interface (CGI) scripts, preventing excessive delays in serving web requests.

- **Solution:-** Consider increasing the maximum run time preferences from the web application settings in order to prevent the CGI scanning for timming out.
- **Business Impact:-** Properly configuring CGI Generic Tests Timeout is critical to ensure timely server responses, prevent performance bottlenecks, and maintain user satisfaction, thus avoiding potential business disruptions.

19.)

- Vulnerability name:- External URL’s.

- **Severity:-** -----
- **Plug-in:-**Published :2010/10/04 ,Modified : 2011/08/19
- **Port:-** 80(TCP).
- **Description:-** External URLs are hyperlinks that point to web pages or resources outside the current website's domain or server.

- **Solution:-** n/a.
- **Business Impact:-**
  The inclusion of external URLs in web content can impact business operations and reputation, as it may introduce security risks and potential loss of control over linked content.

20.)

-Vulnerability name:- HTTP Cookie secure property transport mismatch.

- **Severity:-** -----
- **Plug-in:-**Published :2013/09/10 ,Modified : 2021/12/20
- **Port:-** 443(TCP).
- **Description:-** An "HTTP Cookie secure property transport mismatch" occurs when a cookie marked as secure is transmitted over an insecure (non-HTTPS) connection, potentially exposing sensitive information to security risks.

- **Solution:-** n/a
- **Business Impact:-**The business impact of an HTTP Cookie secure property transport mismatch includes the risk of data exposure, reduced trust, and potential security breaches, which can lead to financial losses and reputational damage.

21.)

- Vulnerability name:- HTTP Methods allowed.

- **Severity:-** -----
- **Plug-in:-**Published :2009/12/10 ,Modified : 2022/04/1
- **Port:-** 80(TCP).
- **Description:-**It refers to the types of HTTP request methods (e.g., GET, POST, PUT, DELETE) that a web server permits for communication with the server's resources.

- **Solution:-** n/a
- **Business Impact:-**Properly defining and limiting allowed HTTP methods is crucial to mitigate security risks, prevent unauthorized access, and safeguard sensitive data, protecting business operations and customer trust.

22.)

- Vulnerability name:- Missing content security policy frame ancestors HTTP Response Header.

- **Severity:-** -----
- **Plug-in:-**Published :2010/10/26 ,Modified : 2021/01/19
- **Port:-** 80(TCP).
- **Description:-** It indicates that a security header specifying who can embed the web page in a frame or if frame is not set, potentially exposing the site to click jacking attacks.

- **Solution:-** Set a non-permissive Consent-Security-policy frame-ancestors header for all requested resources.
- **Business Impact:-**
  The absence of the Content Security Policy frame-ancestors header can expose a business to click jacking attacks, data theft, and reputation damage, impacting customer trust and security.

23.)

- **Vulnerability name:-** Nessus Scan information.

- **Severity:-** -----
- **Plug-in:-**Published :2005/08/26 ,Modified : 2023/07/31
- **Port:-** 0(TCP).
- **Description:-** A Nessus scan provides detailed information about network vulnerabilities, misconfigurations, and security issues, helping organizations assess and improve their cybersecurity posture by identifying potential threats and weaknesses in their infrastructure and applications.

- **Solution:-** n/a
- **Business Impact:-** Nessus scan information has a significant business impact by enabling organizations to proactively address vulnerabilities, reduce the risk of data breaches, maintain compliance, and enhance overall cybersecurity, ultimately safeguarding reputation and customer trust while preventing financial losses.

24.)

- **Vulnerability name:-** Web application cookies not marked http only.

- **Severity:-** -----
- **Plug-in:-**Published :2015/08/24, Modified : 2015/08/24
- **Port:-** 80(TCP).
- **Description:-** Web application cookies not marked as "Http Only" lack a security attribute that prevents client-side JavaScript from accessing them, potentially making them vulnerable to cross-site scripting (XSS) attacks or other malicious client-side scripts.

- **Solution:-** Each Cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.
- **Business Impact:-**
  The absence of the "Http Only" attribute in web application cookies can result in security risks, allowing attackers to steal user session data, potentially leading to unauthorized access, data breaches, and reputational damage, which can negatively impact business operations and customer trust.

25.)

- **Vulnerability name:-** Web application cookies not marked secure.

- **Severity:- -----**
- **Plug-in:-**Published :2015/08/24 Modified : 2015/08/24
- **Port:-** 80(TCP).
- **Description:-** When web application cookies are not marked as "secure," they can be transmitted over unencrypted HTTP connections, potentially exposing sensitive data to interception and security risks.

- **Solution:-** Each cookie should be carefully reviewed to determine if it contains sensitive data for a security decision.
- **Business Impact:-** Iffailing to mark cookies as secure in a web application can compromise the security of user data and authentication. It's a best practice to use secure cookies, along with proper HTTPS configuration, to protect sensitive information and maintain the privacy and integrity of user sessions.

26.)

- **Vulnerability name:-** SMB Signing not required.

- **Severity:-** Medium.
- **Plug-in:-**Published :2012/01/19 Modified : 2022/10/05
- **Port:-** 445(TCP).
- **Description:-** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

- **Solution:-** Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
- **Business Impact:-**The absence of SMB signing can result in significant security vulnerabilities, potentially leading to data breaches, unauthorized access, and compliance issues, which can damage an organization's reputation and incur operational and financial costs.

27.)

- **Vulnerability name:-** OS name and installed package Enumeration.

- **Severity:- -----**
- **Plug-in:-**Published :2004/07/06,Modified : 2022/09/26
- **Port:-** 0(TCP).
- **Description:-**
  OS name and installed package enumeration is the process of identifying the operating system and listing the software packages on a computer or server, crucial for system management and security assessment.

- **Solution:-** n/a
- **Business Impact:-**Accurate OS and package enumeration is essential for effective system management and security monitoring, helping organizations maintain up-to-date software, mitigate vulnerabilities, and ensure regulatory compliance, while failures in this process can lead to security gaps and potential exploitation by attackers.

28.)

- **Vulnerability name:-** DCE Services Enumeration.

- **Severity:-** -----
- **Plug-in:-**Published :2001/08/26 ,Modified : 2021/10/04
- **Port:-** 135(TCP).
- **Description:-**
  DCE (Distributed Computing Environment) services enumeration is the process of identifying and listing the available remote services and their attributes in a DCE-based network.

- **Solution:-** n/a.
- **Business Impact:-**DCE services enumeration can have a significant business impact as it helps in identifying potential vulnerabilities, misconfigurations, or unauthorized services in a network, which, if exploited, could lead to security breaches, data loss, or service disruptions, ultimately affecting the organization's reputation and financial stability.

29.)

- **Vulnerability name:-** Host FDQN Resolution.

- **Severity:-** -----
- **Plug-in:-**Published :2004/02/11, Modified : 2017/04/14
- **Port:-** 0(TCP).
- **Description:-**It is the process of converting a human-readable domain name into its corresponding IP address, allowing computers to locate and communicate with remote hosts on the internet or a network.

- **Solution:-** n/a.
- **Business Impact:-**
  Efficient and accurate FQDN resolution is crucial for businesses as it ensures seamless access to web services, applications, and data, enhancing user experience and productivity. However, issues with FQDN resolution can lead to downtime, connectivity problems, and disrupted operations, potentially resulting in lost revenue and damage to the company's reputation.

30.)

- **Vulnerability name:-** NTLMSSP Authentication request Remote Network name disclosure.

- **Severity:-** -----
- **Plug-in:-**Published :2009/11/06, Modified : 2019/11/22
- **Port:-** 445(TCP).

- **Description:-**The NTLMSSP authentication request vulnerability can lead to the disclosure of a remote network name when an attacker exploits weaknesses in the NTLMSSP authentication protocol, potentially revealing sensitive information about a target network.

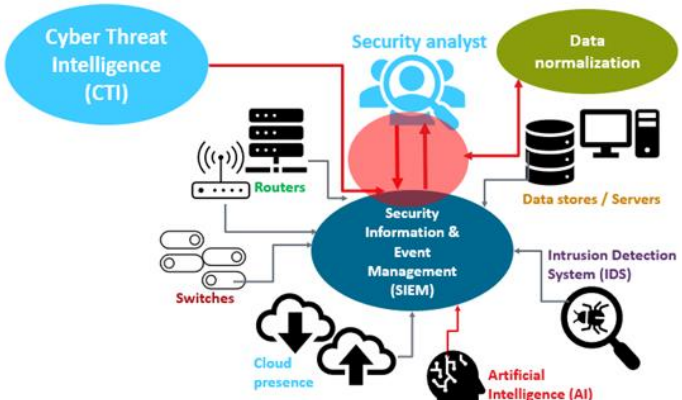
- **Solution:-**n/a.
- **Business Impact:-**The business impact of NTLMSSP authentication request remote network name disclosure is significant, as it can expose sensitive network information to malicious actors, enabling them to launch targeted attacks, compromise systems, and potentially lead to data breaches, financial losses, and reputational damage for the affected organization.

SOC

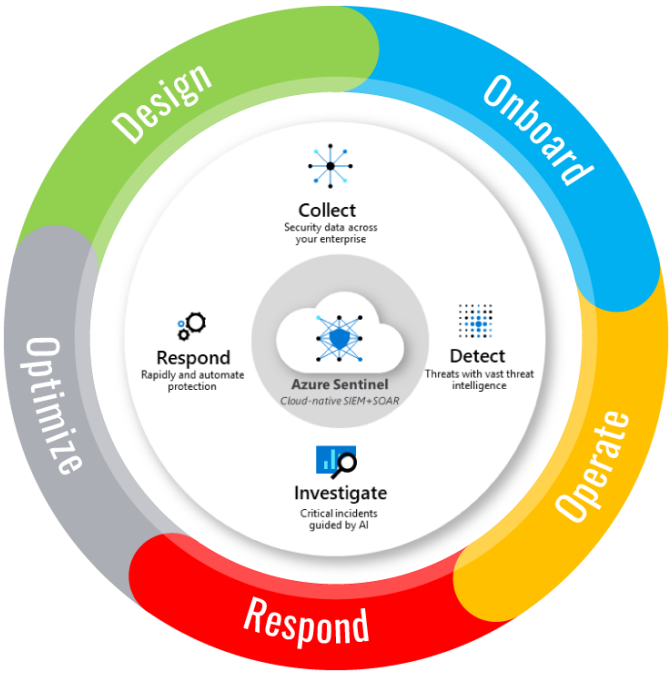
SOC stands for Security Operations Center. It is a centralized facility or team responsible for monitoring an organization's security, detecting and responding to cybersecurity incidents, and protecting against threats to the organization's information systems and data.

Primary functions of SOC include:

- Monitoring: The SOC continuously monitors network traffic, system logs, and security events to identify abnormal or suspicious activities. This monitoring can be done in real-time or through retrospective analysis.
- Incident Detection: SOC analysts use various tools and technologies to detect security incidents, including unauthorized access, malware infections, data breaches, and other cyber threats. They look for patterns and anomalies in the data that could indicate an attack.
- Incident Response: When a security incident is detected, the SOC team responds by investigating the incident, containing the threat, and mitigating the impact. This may involve isolating affected systems, removing malware, and patching vulnerabilities.
- Threat Intelligence: SOC teams often rely on threat intelligence feeds and databases to stay informed about the latest cyber threats and vulnerabilities. This information helps them proactively defend against known threats.
- Security event analysis: SOC analysts analyze security events to determine their severity and impact on the organization. They prioritize incidents based on their potential harm and take appropriate action accordingly.
- Security alerts: When a security incident is confirmed, the SOC team generates security alerts and notifies the relevant stakeholders, including IT personnel, management, and, in some cases, external authorities and incident response teams.
- Forensics and Investigation: In the event of a security breach, the SOC conducts detailed forensic analysis to understand how the breach occurred, what data may have been compromised, and how to prevent future incidents.
- Vulnerability management: The SOC may be responsible for managing vulnerability assessments and helping to remediate security weaknesses in the organization's infrastructure and applications.
- Threat hunting: Proactive threat hunting is the practice of actively searching for signs of potential threats or vulnerabilities in an organization's environment, even before they trigger security alerts.
- Security Training and awareness: The SOC often plays a role in educating employees about security best practices and helping to raise awareness of potential threats through security awareness programs.



SOC Cycle



SIEM

Security information and event management, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response.

How does SIEM work?

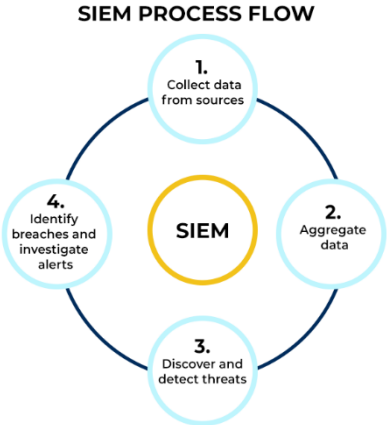
- **Log Management**
  SIEM ingests event data from a wide range of sources across an organization's entire IT infrastructure, including on-premises and cloud environments. Event log data from users, endpoints, applications, data sources, cloud workloads, and networks—as well

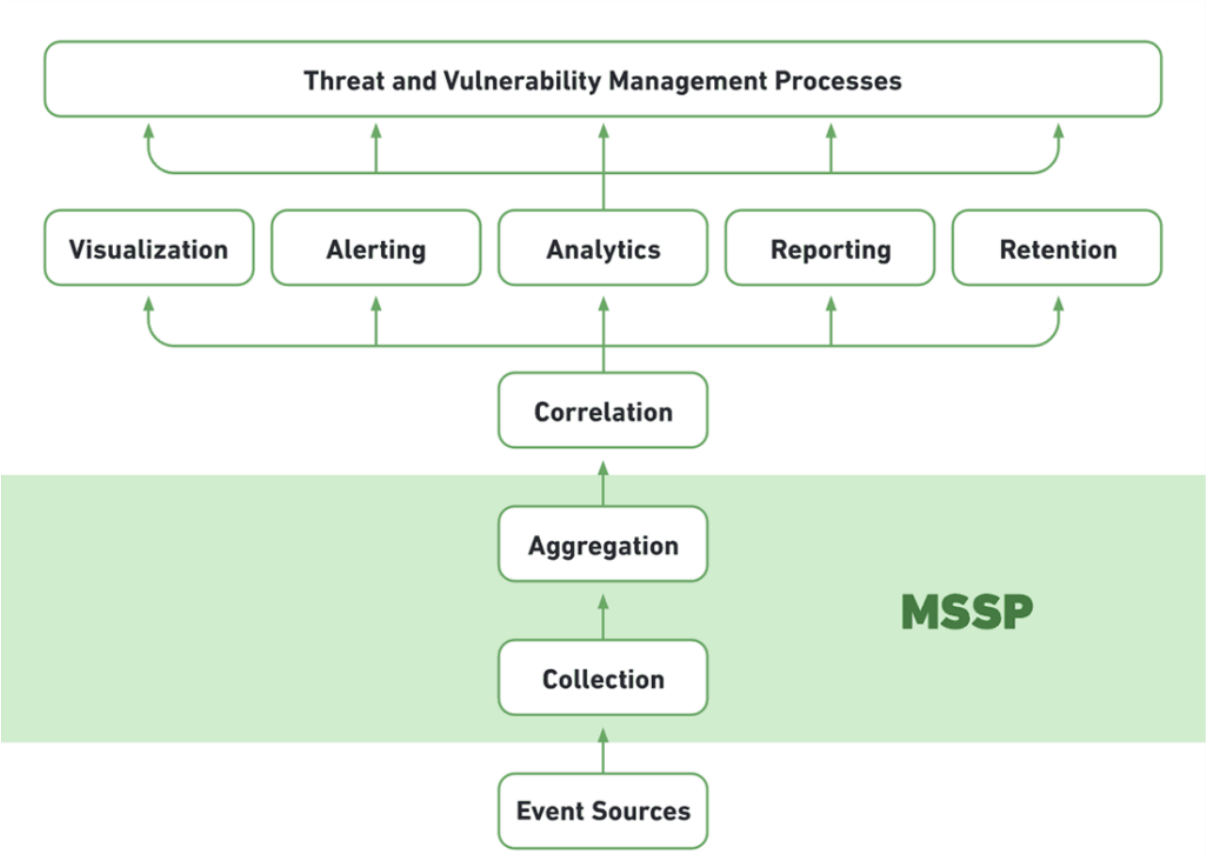
data from security hardware and software such as firewalls or antivirus software—is collected, correlated and analyzed in real-time.

- **Event Correlation and Analytics**
  Utilizing advanced analytics to identify and understand intricate data patterns, event correlation provides insights to quickly locate and mitigate potential threats to business security. SIEM solutions significantly improve mean time to detect (MTTD) and mean time to respond (MTTR) for IT security teams by offloading the manual workflows associated with the in-depth analysis of security events.
- **Incident Monitoring and Security Alerts**
  SIEM consolidates its analysis into a single, central dashboard where security teams monitor activity, triage alerts, identify threats and initiate response or remediation. Most SIEM dashboards also include real-time data visualizations that help security analysts spot spikes or trends in suspicious activity. Using customizable, predefined correlation rules, administrators can be alerted immediately and take appropriate actions to mitigate threats before they materialize into more significant security issues.
- **Compliance Management and Reporting**
  SIEM solutions are a popular choice for organizations subject to different forms of regulatory compliance. Due to the automated data collection and analysis that it provides, SIEM is a valuable tool for gathering and verifying compliance data across the entire business infrastructure.

  Ultimately, a SIEM solution offers a centralized view with additional insights, combining context information about your users, assets and more. It consolidates and analyzes the data for deviations against behavioral rules defined by your organization to identify potential threats. Data sources can include:

- Network devices: Routers, switches, bridges, wireless access points, modems, line drivers, hubs
- Servers: Web, proxy, mail, FTP
- Security devices: Intrusion prevention systems (IPS), firewalls, antivirus software, content filter devices, intrusion detection systems (IDS) and more
- Applications: Any software used on any of the above devices
- Cloud and SaaS solutions: Software and services not hosted on-premises





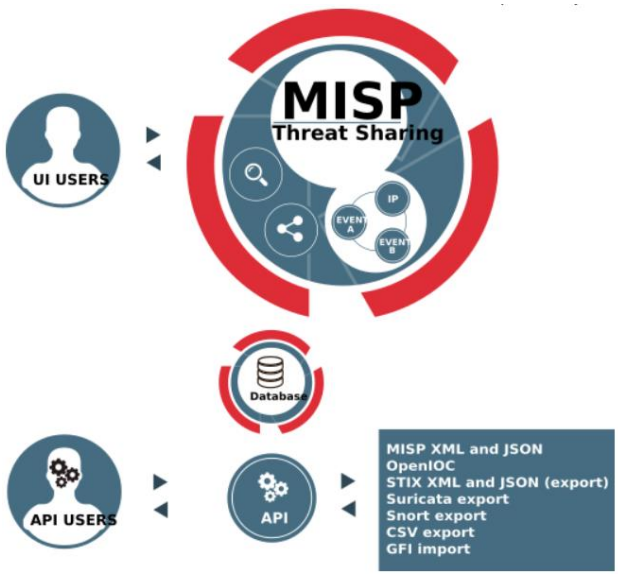
MISP

Malware Information Sharing Platform

MISP - Open Source Threat Intelligence and Sharing Platform allows organizations to share information such as threat intelligence, indicators, threat actor information or any kind of threat which can structured in MISP. MISP users benefit from the collaborative knowledge about existing malware or threats. The aim of this trusted platform is to help improving the counter-measures used against targeted attacks and set-up preventive actions and detection.

Features:

- An efficient IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers, and intelligence.
- A flexible data model where complex objects can be expressed and linked together to express threat intelligence, incidents or connected elements.
- Built-in sharing functionality to ease data sharing using different model of distributions. MISP can automatically synchronize events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a flexible sharing group capacity and an attribute level distribution mechanism.
- An intuitive user-interface for end-users to create, update and collaborate on events and attributes/indicators. A graphical interface to navigate seamlessly between events and their correlations. An event graph functionality to create and view relationships between objects and attributes.
- data-sharing: automatically exchange and synchronization with other parties and trust-groups using MISP.
- Flexible API to integrate MISP with your own solutions. MISP is bundled with PyMISP which is a flexible Python Library to fetch, add or update events attributes, handle malware samples or search for attributes.



MSSP

A managed security service provider (MSSP) is an information technology (IT) service provider that sells security services to businesses. The role of an MSSP is to help protect businesses from security threats, whether that means providing software and services that keep company data safe or building a network of security experts who can respond to attacks as they happen.

What is MSSP used for?

An MSSP should provide a complete outsourced security solution for an organization. The core of the MSSP business is providing security monitoring and incident response for an organization's enterprise networks and endpoints. However, as enterprise networks grow and evolve, support for other platforms, such as cloud-based infrastructure, has become a common component of MSSPs' security portfolio.

Benefits of an MSSP

An MSSP is intended to augment or replace an organization's internal security team. By partnering with an MSSP, a company can reap several benefits:

- **Filling Vacant Roles**: The cybersecurity skills gap means that filling vacant positions on an organization's internal security team can be difficult and expensive. Partnering with an MSSP enables an organization to fill gaps within its internal security team or to replace it entirely.
- **Access to Specialist Expertise**: Limited cybersecurity headcount isn't the only impact of the cybersecurity skills gap. Organizations also periodically require access to specialized cybersecurity expertise (such as malware analysts or forensics specialists) if an incident has occurred. An MSSP has the scale required to retain this expertise in-house and makes it available to customers as needed.
- **Round-the-Clock Protection**: Cyberattacks can occur at any time, not just during an organization's standard business hours. An MSSP should provide a 24/7 SOC, providing continual detection and response to potential cyberattacks.
- **Increased Security Maturity**: Many organizations, especially small and medium-sized businesses, do not have the level of cybersecurity maturity that they require. With an MSSP, SMBs can rapidly deploy a mature cybersecurity solution.
- **Solution Configuration and Management**: Cybersecurity solutions are most effective when they are configured and managed by an expert. When partnering with an MSSP, an organization gains the benefit of expert security management without paying to have the required talent in-house.
- **Lower Total Cost of Ownership**: Many cybersecurity solutions offer support for multi-tenancy and high scalability. This enables an MSSP to use the same solution to support multiple clients, spreading the cost of a robust cybersecurity infrastructure across their client base.
- **Compliance Support**: The regulatory landscape is growing more complex as new data protection regulations (such as the GDPR and the CCPA) join existing laws (like HIPAA and PCI DSS). An MSSP can help with collecting data and generating reports for demonstrating compliance during audits or after a potential incident.

Implementing SOC in Campus

Colleges and universities require a large and diverse network to provide easy access to students, faculty, and office staff. These types of open
SOC teams use a variety of technologies, software, and processes to spot system vulnerabilities and avoid attacks. Some of the most common tools used by a SOC team include firewalls, probes, security information and event management (SIEM) services, and data logs. Here, we can implement IBM QRadar as the SIEM.

Steps to Building a SOC:

- Organizational Buy-in
- Form an SOC leadership team.
- Define audit scope.
- Write policies and procedures.
- Implement technical configuration and controls.
- Conduct a readiness assessment.

Threat Intelligence:

Threat intelligence is a critical component of modern cybersecurity, providing organizations with the knowledge and insights needed to defend against cyber threats effectively. It encompasses the collection, analysis, and dissemination of information about potential and existing cyber threats, including malware, vulnerabilities, and the tactics, techniques, and procedures (TTPs) used by threat actors. Threat intelligence helps organizations stay one step ahead of cybercriminals, enhance their security posture, and proactively respond to security incidents.

There are various sources of threat intelligence, including open-source feeds, commercial services, and government agencies. These sources provide data about known threats, vulnerabilities, and indicators of compromise (IoCs). Security teams use this information to understand the threat landscape and make informed decisions about security measures and incident response.

Threat intelligence can be categorized into three main types:

1. **Strategic Threat Intelligence:** This provides a high-level view of long-term trends and risks, helping organizations make informed decisions about their overall security strategy and investments.
2. **Operational Threat Intelligence:** This type focuses on the immediate threats that an organization may face, such as known vulnerabilities or malware campaigns. It aids in day-to-day decision-making, like patch management or adjusting security policies.
3. **Tactical Threat Intelligence:** Tactical intelligence offers specific details about threats, including detailed IoCs, tactics, and threat actor profiles. This is invaluable for incident response and threat detection.

Threat intelligence is invaluable for enhancing an organization's security posture. By understanding the threat landscape, organizations can take proactive measures to protect their systems and data, including implementing security controls, patching vulnerabilities, and configuring security tools to detect and block known threats. It also plays a vital role in incident response, as it enables security teams to recognize and mitigate security incidents swiftly.

Incident Response:

Incident response is a structured approach to addressing and managing security incidents effectively. Security incidents can range from a wide array of events, including data breaches, malware infections, insider threats, and denial-of-service attacks. An incident response plan provides organizations with the procedures and tools necessary to identify, contain, eradicate, and recover from these incidents. A well-defined incident response process is essential to minimize the impact of a security breach and reduce recovery time and costs.

Key components of an incident response plan include:

1. **Preparation:** This stage involves creating and maintaining an incident response plan, assembling an incident response team, and ensuring that the necessary tools and resources are available.
2. **Identification:** During this phase, security incidents are detected and confirmed. This may involve monitoring alerts, analyzing logs, and conducting forensics to understand the nature and scope of the incident.
3. **Containment:** Once an incident is confirmed, immediate actions are taken to prevent it from spreading further and causing additional damage.
4. **Eradication:** Security teams work to eliminate the root cause of the incident, ensuring that the threat is completely removed from the affected systems.
5. **Recovery:** After the threat is eradicated, the organization can start the process of restoring normal operations. This may involve restoring data from backups, patching vulnerabilities, and strengthening security measures.
6. **Lessons Learned:** After an incident is resolved, it's crucial to conduct a post-incident analysis to identify weaknesses in the response process and make improvements for the future.

Incident response is not only about dealing with the aftermath of a security incident but also about being well-prepared in advance. Proactive measures, such as creating an incident response plan, training staff, and implementing security controls, are vital to effective incident response.

Qradar and Understanding About the Tool:

IBM QRadar is a powerful Security Information and Event Management (SIEM) solution designed to help organizations collect, analyze, and respond to security events and incidents

in real-time. It provides a comprehensive view of an organization's security landscape, combining data from various sources, such as logs, network traffic, and vulnerability data, to detect and respond to threats efficiently.

Key features and capabilities of IBM QRadar include:

1. **Log and Event Management:** QRadar collects and normalizes data from numerous sources, making it easier to analyze and correlate events across the network. It supports a wide range of log sources, including network devices, security appliances, and operating systems.
2. **Real-time Monitoring:** QRadar offers real-time monitoring and alerting, enabling security teams to quickly detect and respond to suspicious activities and security incidents.
3. **Behavior Analytics:** The tool uses advanced analytics to detect anomalous behavior patterns, allowing organizations to identify threats even when there are no known signatures.
4. **Incident Management:** QRadar provides workflows for incident investigation and management. It helps security teams coordinate and document their response efforts.
5. **Threat Intelligence Integration:** QRadar can ingest threat intelligence feeds and indicators of compromise (IoCs), helping organizations stay updated on the latest threats and vulnerabilities.
6. **User and Entity Behavior Analytics (UEBA):** QRadar includes UEBA functionality to monitor the behavior of users and entities within the organization, helping to detect insider threats and abnormal activities.
7. **Forensics and Data Retention:** The tool offers capabilities for forensic analysis and long-term data retention, allowing organizations to investigate historical data when needed.
8. **Compliance and Reporting:** QRadar helps organizations meet regulatory compliance requirements by providing pre-built reports and dashboards for various compliance standards.

Conclusion:

Stage 1: Web Application Testing:

Web application testing is a critical process in the field of software quality assurance. It involves systematically assessing web-based applications to ensure they function correctly and securely. The primary goal is to identify vulnerabilities, bugs, and usability issues that

may affect the user experience or expose the application to security threats. During this stage, the testing team conducts various types of assessments, including functional testing, security testing, performance testing, and usability testing. The results help developers and stakeholders make necessary improvements to the application. In conclusion, web application testing is essential for delivering a reliable and secure online experience for users.

Stage 2: The Nessus Report:

A Nessus report is a comprehensive document generated by the Nessus vulnerability scanning tool. This report provides an in-depth analysis of the security vulnerabilities present in a network, system, or web application. It includes information about identified vulnerabilities, their severity, and recommendations for mitigating these issues. The Nessus report is an invaluable resource for IT security professionals, enabling them to proactively address vulnerabilities and strengthen their organization's security posture.

Stage 3: SOC / SIEM / Qradar Dashboard:

A Security Operations Center (SOC) is a centralized unit responsible for monitoring and responding to security threats within an organization. A Security Information and Event Management (SIEM) system, like Qradar, is a crucial component of a SOC. It aggregates and analyzes security-related data from various sources to detect and respond to security incidents effectively. The Qradar dashboard is a user interface that displays real-time information about security events and incidents. It provides SOC analysts with a visual representation of the organization's security status, facilitating quick decision-making and incident response.

Future Scope:

Stage 1: Future Scope of Web Application Testing:

The future of web application testing is promising, given the rapid growth of online services. With the increasing complexity of web applications and the evolving threat landscape, the demand for more sophisticated testing methodologies will rise. Automation will play a pivotal role, with AI and machine learning contributing to more accurate testing and quicker identification of vulnerabilities. Additionally, with the adoption of DevOps and continuous integration/continuous deployment (CI/CD) practices, testing will become an integral part of the development process, ensuring quicker releases while maintaining security and quality.

Stage 2: Future Scope of Testing Processes:

The future of testing processes will be characterized by greater automation, integration, and collaboration. Test automation will continue to evolve, enabling faster and more comprehensive testing. The integration of testing into the CI/CD pipeline will become seamless, ensuring that quality is maintained throughout the development lifecycle. Additionally, there will be a growing emphasis on security testing, as the need for robust cybersecurity practices becomes more critical.

Stage 3: Future Scope of SOC / SIEM:

The future of Security Operations Centers and SIEM systems will involve more advanced threat detection and response capabilities. Machine learning and artificial intelligence will be used to predict and prevent security incidents. Integration with cloud-based and IoT devices will become more complex, requiring adaptable and scalable SIEM solutions. Moreover, the role of the SOC will expand to cover not only threat detection but also compliance monitoring and risk management, making it a crucial component of overall business operations.

Conclusion

In conclusion, the development of an AI-enhanced Intrusion Detection System (IDS) is a significant step forward in the realm of cybersecurity. This project has aimed to harness the power of artificial intelligence to improve the accuracy and efficiency of detecting and responding to various forms of cyber threats. Through the integration of machine learning algorithms and advanced data analysis techniques, the system has shown promise in effectively identifying abnormal network behaviour and potential security breaches.

The key findings and outcomes of this project include:

1. **Improved Accuracy**: The AI-enhanced IDS has demonstrated an ability to identify both known and previously unseen threats with a higher level of accuracy compared to traditional rule-based IDS systems.
2. **Real-time Threat Detection**: The system can provide real-time threat detection and alerting, enabling organizations to respond promptly to security incidents and minimize potential damage.
3. **Reduced False Positives**: By leveraging machine learning, the system has successfully reduced the rate of false positives, helping security teams focus their efforts on genuine threats and reduce unnecessary alerts.
4. **Scalability**: The AI-enhanced IDS can scale to handle large and complex network environments, making it suitable for a variety of organizations, from small businesses to large enterprises.
5. **Continuous Learning**: The system's ability to adapt and learn from evolving threats is a significant advantage, as it can continuously improve its threat detection capabilities.
6. **Enhanced Security Posture**: Implementation of this system contributes to an organization's overall security posture, protecting critical data and infrastructure from potential cyberattacks.

It is important to note that while AI-enhanced IDS systems offer great promise, they are not a one-size-fits-all solution. Proper deployment and ongoing monitoring are essential for their effectiveness. Additionally, as the threat landscape evolves, this system will require regular updates and adjustments to maintain its efficacy.

In summary, the development of an AI-enhanced Intrusion Detection System represents a pivotal advancement in cybersecurity, providing organizations with a more robust and adaptive defense against cyber threats. This project's success underscores the importance of integrating AI and machine learning into security solutions and paves the way for further innovations in the field of cybersecurity.

Future Scope

The future scope for an AI-enhanced Intrusion Detection System (IDS) is promising and aligns with the growing importance of cybersecurity in an increasingly digital world. As technology evolves and cyber threats become more sophisticated, the scope for AI-enhanced IDS systems is expected to expand in several ways:

- **Enhanced Threat Detection**: AI-enhanced IDS systems will continue to improve in identifying and mitigating both known and emerging threats. They will evolve to recognize complex attack patterns and adapt to new attack techniques.
- **Behavioral Analysis**: AI will play a more significant role in understanding and analyzing user and network behavior. This includes the ability to detect insider threats, anomalous activities, and deviations from normal network behavior.
- **Real-time Response**: Future AI-enhanced IDS systems will not only detect threats but also respond in real-time. Automated responses, such as isolating compromised devices or blocking malicious traffic, will become more sophisticated.
- **IoT and OT Security**: With the proliferation of Internet of Things (IoT) and Operational Technology (OT) devices, AI-enhanced IDS systems will expand to secure these areas, providing protection for critical infrastructure and industrial control systems.
- **Cloud Security**: As more organizations move their infrastructure to the cloud, AI-enhanced IDS systems will be tailored for cloud environments, offering protection against cloud-specific threats and vulnerabilities.
- **Machine Learning Advancements**: Future IDS systems will incorporate more advanced machine learning techniques, such as deep learning and reinforcement learning, to improve accuracy and adaptability.
- **Integration with SIEM**: Seamless integration with Security Information and Event Management (SIEM) systems will become essential for comprehensive threat intelligence and incident response.
- **AI-Driven Threat Intelligence**: AI-enhanced IDS systems will rely on AI-driven threat intelligence feeds, allowing them to proactively defend against emerging threats by learning from global cybersecurity trends.
- **Blockchain for Security**: The use of blockchain technology to enhance the security and transparency of logs and alerts in IDS systems may become more prevalent.
- **Threat Hunting**: AI-enhanced IDS systems will facilitate threat hunting activities, where security teams proactively search for hidden threats and vulnerabilities within the network.
- **Human-Machine Collaboration**: Human-machine collaboration will become more prominent, where human analysts work alongside AI-enhanced IDS systems to investigate and respond to security incidents effectively.
- **Customization and Adaptability**: Future systems will be highly customizable to meet the unique needs of different organizations and industries, and they will be capable of adapting to evolving threats.

The future of AI-enhanced IDS systems will be closely tied to ongoing advancements in AI and the evolving threat landscape. Continuous research and development in this field will be crucial to stay ahead of cyber adversaries and protect critical digital assets effectively.