STAGE -1

Title:

System that uses AI for real-time data classification, leak detection, and prevention to enhance data security.

Overview:

Introduction: In today's digital age, data security is paramount. Our project is a groundbreaking system that utilizes Artificial Intelligence (AI) for real-time data classification, leak detection, and prevention. This innovative approach fortifies data security by combining advanced AI algorithms with cutting-edge data protection measures.

Key Objectives:

1. Real-Time Data Classification: Our system employs AI to automatically classify data based on its sensitivity, ensuring proper labeling and handling. Machine learning models identify patterns, keywords, and metadata associated with different data types.
2. Leak Detection: The system continuously monitors data flows, detecting unauthorized access, unusual data transfers, and suspicious user behavior. It promptly identifies potential data breaches by comparing patterns to known threat profiles.
3. Leak Prevention: Beyond detection, our system proactively prevents data leaks by adjusting access permissions, applying encryption, and blocking unauthorized data transfers in real-time.

Key Features:

- AI-Driven Decision-Making: The system adapts and responds to emerging threats and changing data dynamics with AI algorithms.
- Scalability: Designed to handle large data volumes, it can grow with your organization's needs.
- User-Friendly Dashboard: An intuitive dashboard provides real-time insights, alerts, and statistics for informed decision-making.
- Customization: Tailored to your organization's data security requirements, ensuring compliance with regulatory standards.

Benefits:

- Enhanced Data Protection: Automating data classification and real-time security measures significantly strengthens data security.
- Cost-Efficiency: Reduced human intervention in security processes leads to cost savings.
- Compliance: Helps meet regulatory requirements by ensuring data is handled in accordance with guidelines.
- Peace of Mind: Focus on core operations, knowing your data is under constant, intelligent protection.

Conclusion: In an era of escalating data breaches, our project provides an intelligent, automated, and proactive solution for real-time data classification, leak detection, and prevention. By harnessing AI, we secure your data assets, ensuring confidentiality and integrity in a data-driven world.

List of Team Mates:

S.no	Name	College	Contact
1.	Yash Lulla	VIT	9967175220
2.	Nikhil Sri Harsha Battineni	VIT	9391294788
3.	Koganti Rohitha	VIT	8309874328
4.	Veligotla Yashasvi Koushik	VIT	9494358348

List of vulnerabilities –

S.no	**Vulnerability name**	**CWE-No**
1.	Protocol Detection	CWE-326
2.	Denial of service	CWE-400
3.	Remote code execution	CWE-94
4.	Request smuggling	CWE-444
5.	Privilege Escalation	CWE-269
6.	Multiple Vulnerabilities	CWE-20

REPORT:

Vulnerability Name: Privilege Escalation.
CWE: - CWE-269
OWASP Category: - A5
DESCRIPTION:
Privilege escalation is a security vulnerability or attack technique that involves gaining higher levels of access or permissions than originally intended or assigned within a computer system, network, or application. It is a significant concern in the field of cybersecurity, as it can allow unauthorized users to gain greater control over a system, potentially leading to data breaches, system compromise, and other security risks.
BUSSINESS IMPACT:
Privilege escalation vulnerabilities can have significant business impact, as they pose a serious threat to the security and integrity of a company's systems and data. Here are some of the potential business impacts of privilege escalation vulnerabilities:

Unauthorized Access: Privilege escalation vulnerabilities can allow attackers to gain elevated privileges on a system or network, giving them access to sensitive data, applications, and resources that they shouldn't have. This can lead to data breaches and the theft of confidential information.

Data Breaches: If an attacker exploits a privilege escalation vulnerability, they may be able to access and exfiltrate sensitive customer data, proprietary business information, or financial records. Data breaches can result in significant financial and reputational damage to a company.

Financial Loss: Privilege escalation attacks can result in financial losses due to theft, fraud, or the costs associated with remediation, such as system repairs, legal fees, and regulatory fines.

Vulnerability Name: 133845 - Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities.
CWE: - CWE -20
OWASP Category: - A5
DESCRIPTION:
The version of Tomcat installed on the remote host is 7.0.x prior to 7.0.100, 8.x prior to 8.5.51, or 9.0.x prior to 9.0.31. It is, therefore, affected by multiple vulnerabilities.

-An HTTP request smuggling vulnerability exists in Tomcat due to mishandling Transfer-Encoding headers behind a reverse proxy. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2019-17569)

-An HTTP request smuggling vulnerability exists in Tomcat due to bad end-of-line (EOL) parsing that allowed some invalid HTTP headers to be parsed as valid. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2020-1935)

-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).
BUSSINESS IMPACT:
The business impact of multiple vulnerabilities can be significant and wide-ranging. Vulnerabilities in a business's systems, processes, or infrastructure can expose the organization to various risks and potential negative consequences, including:

Data Breaches: Multiple vulnerabilities can lead to data breaches, which can result in the exposure of sensitive customer information, intellectual property, or confidential business data. This can damage the company's reputation, result in legal consequences, and lead to financial losses.

Financial Losses: Exploitation of vulnerabilities can result in financial losses through various means, such as theft of funds, fraud, or regulatory fines and penalties. Businesses may also incur expenses to remediate vulnerabilities and recover from security incidents.

Operational Disruption: Vulnerabilities can be exploited to disrupt business operations. For example, a cyberattack could render critical systems unavailable, leading to downtime, lost productivity, and the inability to meet customer demands.

Vulnerability Name: Request smuggling
CWE: - CWE-444
OWASP Category: - A1
DESCRIPTION:
Request smuggling is a security vulnerability that can occur in web applications when an attacker manipulates the way HTTP requests are handled by a front-end server or a proxy server. This technique can lead to a range of potential attacks, including data theft, privilege escalation, and more.
Business Impact:
Request smuggling is a security vulnerability that can have significant business impacts on organizations. It occurs when an attacker manipulates the way front-end and back-end servers process HTTP requests, leading to various security risks and potential financial consequences. Here are some of the business impacts of request smuggling:

Data Breach: Request smuggling can be exploited to access sensitive data or execute unauthorized actions on a web application. This could lead to data breaches, exposing customer information, financial data, or other sensitive business information, resulting in financial penalties and reputational damage.

Reputation Damage: A successful request smuggling attack can damage an organization's reputation. Customers may lose trust in a company that cannot secure its web applications, which can lead to a loss of business and brand damage.

Legal and Compliance Issues: Request smuggling vulnerabilities may result in legal actions and regulatory fines if an organization is found to be non-compliant with data protection and privacy regulations. Companies may also be liable for failing to protect customer data.

Vulnerability Name: Remote code execution
CWE: - CWE-94
OWASP: - A1
DESCRIPTION:
Remote code escalation, often referred to as remote code execution (RCE), is a cybersecurity term that describes a scenario where an attacker gains unauthorized access to a computer system or application and is able to execute arbitrary code on the remote target system. This type of security vulnerability is a significant concern because it can lead to various malicious actions, including taking control of the target system, stealing data, and compromising its integrity.
Business Impact:
Legal and Regulatory Consequences: Data breaches and security incidents resulting from remote code escalation can lead to legal and regulatory challenges. Companies may face lawsuits from affected customers, partners, or employees, and may also be subject to fines and penalties for failing to protect data as required by data protection laws.

Reputational Damage: Customers and partners may lose trust in a company that experiences remote code escalation incidents, and the company's reputation can suffer. Rebuilding trust and regaining a positive image can be a lengthy and costly process.

Downtime and Productivity Loss: When a security breach occurs, businesses may need to shut down affected systems to investigate, remediate, and recover from the incident. This downtime can lead to lost revenue and decreased productivity.

Vulnerability Name: Denial of service.
CWE: - CWE-400
OWASP Category: - A4
DESCRIPTION:
A Denial of Service (DoS) is a type of cyberattack in which an attacker or group of attackers seeks to disrupt the normal functioning of a computer system, network, website, or online service by overwhelming it with an excessive amount of traffic, requests, or malicious activities. The primary objective of a Denial-of-Service attack is to make the targeted resource or service unavailable to its intended users, essentially denying them access.
Business Impact:
Loss of Revenue: If a business relies on its online services or e-commerce platforms, a DoS attack can disrupt its operations, causing a loss of revenue. Downtime means customers cannot make purchases, access services, or conduct transactions.

Reputation Damage: DoS attacks can tarnish a company's reputation, leading to a loss of customer trust. Frequent service interruptions can make customers question the reliability and security of the business.

Vulnerability Name: 157288 - TLS Version 1.1 Protocol Deprecated
CWE: - CWE-326
OWASP Category: - A5
DESCRIPTION:
The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.
Business Impact:
Compatibility Issues: Deprecated protocols may not be compatible with newer technologies or systems. Businesses may face challenges when trying to integrate legacy systems with newer ones, leading to reduced efficiency and compatibility issues.

Security Risks: Deprecated protocols may have known security vulnerabilities that are no longer patched or updated. This can pose a significant security risk to businesses, as hackers and malicious actors may target vulnerabilities in outdated protocols to breach systems and compromise data.

STAGE -2

OVERVIEW : Title: Overview of Nessus Scan

Introduction:

Nessus is a powerful and widely used vulnerability scanning tool designed to help organizations identify and mitigate security weaknesses in their IT infrastructure. Developed by Tenable, Nessus has become an essential component of cybersecurity practices, aiding in the ongoing battle to safeguard systems, networks, and data from potential threats. This one-page overview delves into the key features, benefits, and best practices associated with Nessus scans.

Key Features of Nessus:

1. **Comprehensive Scanning:**

Nessus offers comprehensive vulnerability scanning, ensuring that it can detect a wide range of vulnerabilities, including software flaws, misconfigurations, and potential threats across networks, systems, and applications.

2. Extensive Vulnerability Database:

The tool maintains an extensive database of known vulnerabilities, which it uses to compare scan results with up-to-date information. This enables Nessus to accurately identify security issues and prioritize them based on their severity.

3. Plugin Architecture:

Nessus relies on a flexible plugin architecture, allowing users to customize their scans by selecting specific plugins, adjusting settings, and creating custom scripts tailored to their unique needs.

4. Compliance and Policy Auditing:

Nessus supports compliance checks for various industry standards and regulatory requirements. Users can assess their systems' compliance with standards like PCI DSS, HIPAA, and CIS benchmarks.

5. Scheduled Scans:

Nessus enables organizations to schedule scans at regular intervals, ensuring that they continuously monitor their network's security posture and detect newly emerging vulnerabilities.

Benefits of Nessus Scans:

1. Risk Reduction:

Nessus scans help organizations identify and mitigate vulnerabilities, reducing the risk of security breaches, data leaks, and cyberattacks.

2. Time and Cost Savings:

By automating the scanning process, Nessus saves time and reduces the cost associated with manual vulnerability assessment.

3. Prioritization:

Nessus provides a risk-based approach to prioritizing vulnerabilities, helping organizations focus their resources on addressing the most critical security issues first.

4. Reporting and Documentation:

The tool generates detailed reports that allow security professionals and decision-makers to understand the state of their network's security and track improvements over time.

Best Practices for Nessus Scans:

1. Regular Scanning:

Perform scans on a regular basis to stay updated on the security posture of your network, as vulnerabilities can change over time.

2. Proper Configuration:

Ensure that Nessus is properly configured and uses the latest plugins and vulnerability databases to deliver accurate results.

3. Risk-Based Approach:

Prioritize vulnerabilities based on their criticality to your organization and address high-risk issues first.

4. Integration:

Integrate Nessus with your organization's security information and event management (SIEM) systems to streamline threat response and management.

5. Continuous Monitoring:

Use Nessus in conjunction with other security tools to establish continuous monitoring and improve the overall security of your IT infrastructure.

In conclusion, Nessus is an invaluable tool for organizations seeking to proactively identify and mitigate vulnerabilities in their IT infrastructure. Its robust feature set, up-to-date vulnerability database, and customizable scanning capabilities make it a go-to choice for cybersecurity professionals in their quest to protect critical assets from potential threats and ensure a resilient security posture. By following best practices and making Nessus an integral part of their security strategy, organizations can fortify their defenses and reduce the risk of security incidents.

Target website : vtop2.vitap.ac.in

Target IP address : 220.158.183.5

List of vulnerability –

s.no	Vulnerability name	Severity	plugins
1.	**Protocol Detection**	**TLS (Transport Layer Security) version 1.0 is an outdated and insecure protocol that is known to have multiple security vulnerabilities, including susceptibility to various cryptographic attacks. As a result, it is generally considered to be weak and obsolete.**	TLSV1 is enabled and the server supports at least one cipher. **Tcp/443/www**

2.	Denial of service	A moderate-severity DoS attack can result in more prolonged or significant disruptions, possibly affecting a limited number of users. This could include more sophisticated attack techniques.	Tcp/443/www Installed version : 9.0.0.M26 Fixed version : 9.0.8
3.	Multiple vunerabilities	The severity can vary based on the systems or software affected. Vulnerabilities in critical infrastructure or widely used software can be more severe than those in less critical systems.	**Tcp/443/www** Fixed version : 9.0.31
4.	Remote code execution	Consider the potential impact of the RCE. If an attacker can execute arbitrary code, they can potentially steal sensitive data, manipulate or delete files, disrupt services, or take over the entire system. The more significant the potential damage, the more severe the vulnerability.	Tcp/443/www Installed version : 9.0.0.M26 Fixed version : 9.0.35
5.	Request smuggling	The impact of request smuggling largely depends on how an attacker can exploit it. If an attacker can use request smuggling to perform actions that compromise the security of the application or its users, the severity is high. The severity can also vary depending on which components are affected. For instance,	Tcp/443/www Installed version : 9.0.0.M26 Fixed version : 9.0.68

		if a web application firewall is vulnerable to request smuggling, it can lead to the bypassing of security measures, making the vulnerability more critical.	
6.	Privilege Escalation	The method an attacker uses to perform privilege escalation also plays a significant role. If an attacker can exploit a widely known and easily accessible vulnerability to escalate privileges, it is more severe than a highly complex and rare method.	Tcp/443/www Installed version : 9.0.0.M26 Fixed version : 9.0.30

REPORT :

Vulnerability Name : **Privilege Escalation.**

Severity : The severity of privilege escalation in the context of computer security can vary widely depending on several factors, including how it occurs, what privileges are escalated, and the potential impact on a system or network. Privilege escalation is a security vulnerability that allows an attacker to gain higher-level privileges than they should have.

In summary, the severity of privilege escalation depends on the context and various factors, and it can range from low to critical, with critical privilege escalations posing the most significant risk to system security and data integrity.

Pulgin :

tcp/443/www

PORT : tcp/443

DESCRIPTION : Privilege escalation is a security vulnerability or attack technique that involves gaining higher levels of access or permissions than originally intended or assigned within a computer system, network, or application. It is a significant concern in the field of cybersecurity, as it can allow unauthorized users to gain greater control over a system, potentially leading to data breaches, system compromise, and other security risks.

SOLUTION : Principle of Least Privilege (PoLP):

Limit user and application permissions to the minimum necessary for their tasks.
Use role-based access control (RBAC) to assign permissions.
Regularly review and update permissions based on job roles and responsibilities.

Strong Authentication and Authorization:

Implement strong authentication methods like multi-factor authentication (MFA).
Use strong password policies and password management practices.
Employ robust authorization mechanisms to control access to resources.
Regular Patching and Updates:

Keep the operating system, software, and applications up to date with security patches.
Vulnerabilities in outdated software can be exploited for privilege escalation.
Vulnerability Scanning and Penetration Testing:

Regularly scan your systems for vulnerabilities.
Conduct penetration testing to identify and address weaknesses.

Monitor and Audit:

Set up monitoring systems to detect unusual or unauthorized activities.
Implement auditing and logging to track access and changes to sensitive resources.

BUSSINESS IMPACT : Privilege escalation vulnerabilities can have significant

business impact, as they pose a serious threat to the security and integrity of a company's systems and data. Here are some of the potential business impacts of privilege escalation vulnerabilities:

Unauthorized Access: Privilege escalation vulnerabilities can allow attackers to gain elevated privileges on a system or network, giving them access to sensitive data, applications, and resources that they shouldn't have. This can lead to data breaches and the theft of confidential information.

Data Breaches: If an attacker exploits a privilege escalation vulnerability, they may be able to access and exfiltrate sensitive customer data, proprietary business information, or financial records. Data breaches can result in significant financial and reputational damage to a company.

Financial Loss: Privilege escalation attacks can result in financial losses due to theft, fraud, or the costs associated with remediation, such as system repairs, legal fees, and regulatory fines.

Vulnerability Name : 133845 - Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities.

Serverity : The severity of multiple vulnerabilities can vary widely depending on various factors, including the nature of the vulnerabilities, the systems they affect, and the potential impact they can have. Vulnerability severity is typically assessed using a common scale, such as the Common Vulnerability Scoring System (CVSS), which assigns a score to vulnerabilities to help determine their severity. The CVSS score takes into account factors like exploitability, impact, and access complexity.

Pulgin :

tcp/443/www

PORT : tcp/443

DESCRIPTION : The version of Tomcat installed on the remote host is 7.0.x prior to 7.0.100, 8.x prior to 8.5.51, or 9.0.x prior to 9.0.31. It is, therefore, affected by multiple vulnerabilities.

- An HTTP request smuggling vulnerability exists in Tomcat due to mishandling Transfer-Encoding headers behind a reverse proxy. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2019-17569)

- An HTTP request smuggling vulnerability exists in Tomcat due to bad end-of-line (EOL) parsing that allowed some invalid HTTP headers to be parsed as valid. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2020-1935)

- 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).

SOLUTION : Addressing multiple vulnerabilities typically involves a systematic approach to identifying, prioritizing, and mitigating security issues in software, systems, or networks. Here is a general process for addressing multiple vulnerabilities:

Vulnerability Assessment:

Identify all vulnerabilities present in your system or software. This can be done through vulnerability scanning tools, manual code review, or security assessments.
Prioritization:

Prioritize vulnerabilities based on their severity, potential impact, and exploitability. This is usually done by assigning a Common Vulnerability Scoring System (CVSS) score to each vulnerability.
Patch Management:

For software or systems with known vulnerabilities, apply patches and updates provided by the vendors. Make sure to keep all software components up-to-date.

BUSSINESS IMPACT : The business impact of multiple vulnerabilities can be significant and wide-ranging. Vulnerabilities in a business's systems, processes, or infrastructure can expose the organization to various risks and potential negative consequences, including:

Data Breaches: Multiple vulnerabilities can lead to data breaches, which can result in the exposure of sensitive customer information, intellectual property, or confidential business data. This can damage the company's reputation, result in legal consequences, and lead to financial losses.

Financial Losses: Exploitation of vulnerabilities can result in financial losses through various means, such as theft of funds, fraud, or regulatory fines and penalties. Businesses may also incur expenses to remediate vulnerabilities and recover from security incidents.

Operational Disruption: Vulnerabilities can be exploited to disrupt business operations. For example, a cyberattack could render critical systems unavailable, leading to downtime, lost productivity, and the inability to meet customer demands.

Vulnerability Name : Request smuggling

SERVERITY : The impact of request smuggling largely depends on how an attacker can exploit it. If an attacker can use request smuggling to perform actions that compromise the security of the application or its users, the severity is high.

The severity can also vary depending on which components are affected. For instance, if a web application firewall is vulnerable to request smuggling, it can lead to the bypassing of security measures, making the vulnerability more critical.

Pulgin :

tcp/443/www

PORT : tcp/443

DESCRIPTION :

Request smuggling is a security vulnerability that can occur in web applications when an attacker manipulates the way HTTP requests are handled by a front-end server or a proxy server. This technique can lead to a range of potential attacks, including data theft, privilege escalation, and more.

SOLUTION :

Patch and Update: Ensure that all your web servers, load balancers, and proxy servers are running the latest software versions with security patches. Many request smuggling vulnerabilities are found and fixed in updates.

Request Sanitization: Validate and sanitize incoming requests on the front-end servers. This can prevent attackers from injecting malicious data.

Request Parsing: Pay special attention to how your server parses requests, especially when dealing with request headers, content-length, and chunked encoding. Ensure that your server follows HTTP protocol specifications correctly.

Business Impact :

Request smuggling is a security vulnerability that can have significant business impacts on organizations. It occurs when an attacker manipulates the way front-end and back-end servers process HTTP requests, leading to various security risks and potential financial consequences. Here are some of the business impacts of request smuggling:

Data Breach: Request smuggling can be exploited to access sensitive data or execute unauthorized actions on a web application. This could lead to data breaches, exposing customer information, financial data, or other sensitive business information, resulting in financial penalties and reputational damage.

Reputation Damage: A successful request smuggling attack can damage an organization's reputation. Customers may lose trust in a company that cannot secure its web applications, which can lead to a loss of business and brand damage.

Legal and Compliance Issues: Request smuggling vulnerabilities may result in legal actions and regulatory fines if an organization is found to be non-compliant with data protection and privacy regulations. Companies may also be liable for failing to protect customer data.

Vulnerability Name : Remote code execution

Serverity : Consider the potential impact of the RCE. If an attacker can execute arbitrary code, they can potentially steal sensitive data, manipulate or delete files, disrupt services, or take over the entire system. The more significant the potential damage, the more severe the vulnerability.

Pulgin :

tcp/443/www

PORT : tcp/443

DESCRIPTION : Remote code escalation, often referred to as remote code execution (RCE), is a cybersecurity term that describes a scenario where an attacker gains unauthorized access to a computer system or application and is able to execute arbitrary code on the remote target system. This type of security vulnerability is a significant concern because it can lead to various malicious actions, including taking control of the target system, stealing data, and compromising its integrity.

SOLUTION :
Remote code escalation is a security vulnerability that allows an attacker to execute malicious code on a remote system with higher privileges than they should have. Mitigating and resolving such vulnerabilities is critical for maintaining the security of computer systems and networks. Here are some general steps you can take to address remote code escalation issues:

Identify Vulnerabilities:

Conduct a security assessment or penetration testing to identify potential vulnerabilities in your systems.

Stay informed about security updates and patches for your software and operating systems.
Patch and Update:

Apply all available security patches and updates for your operating system, software, and applications. This is the most effective way to fix known vulnerabilities.

Business Impact :
Legal and Regulatory Consequences: Data breaches and security incidents resulting from remote code escalation can lead to legal and regulatory challenges. Companies may face lawsuits from affected customers, partners, or employees, and may also be subject to fines and penalties for failing to protect data as required by data protection laws.

Reputational Damage: Customers and partners may lose trust in a company that experiences remote code escalation incidents, and the company's reputation can suffer. Rebuilding trust and regaining a positive image can be a lengthy and costly process.

Downtime and Productivity Loss: When a security breach occurs, businesses may need to shut down affected systems to investigate, remediate, and recover from the incident. This downtime can lead to lost revenue and decreased productivity.

Vulnerability Name : Denial of service.

Serverity : A moderate-severity DoS attack can result in more prolonged or significant disruptions, possibly affecting a limited number of users. This could include more sophisticated attack techniques.

Pulgin :

tcp/443/www

PORT : tcp/443

DESCRIPTION : A Denial of Service (DoS) is a type of cyberattack in which an attacker or group of attackers seeks to disrupt the normal functioning of a computer system, network, website, or online service by overwhelming it with

an excessive amount of traffic, requests, or malicious activities. The primary objective of a Denial of Service attack is to make the targeted resource or service unavailable to its intended users, essentially denying them access.

SOLUTION :
Network Security:

Implement firewalls and intrusion detection/prevention systems to filter and monitor incoming traffic.
Use rate limiting to control the number of requests a server can handle from a single source.
Content Delivery Networks (CDNs):

Utilize CDNs to distribute traffic and absorb a large portion of the attack traffic, preventing it from reaching your server
.
Load Balancing:

Deploy load balancers to distribute traffic across multiple servers. This can help prevent overwhelming a single server.

Business Impact :
Loss of Revenue: If a business relies on its online services or e-commerce platforms, a DoS attack can disrupt its operations, causing a loss of revenue. Downtime means customers cannot make purchases, access services, or conduct transactions.

Reputation Damage: DoS attacks can tarnish a company's reputation, leading to a loss of customer trust. Frequent service interruptions can make customers question the reliability and security of the business.

Vulnerability Name : Protocol Detection

Serverity : TLS (Transport Layer Security) version 1.0 is an outdated and insecure protocol that is known to have multiple security vulnerabilities, including susceptibility to various cryptographic attacks. As a result, it is generally considered to be weak and obsolete.

Pulgin :

tcp/443/www

PORT : tcp/443

DESCRIPTION : Protocol detection is the process of identifying and categorizing network protocols and services used in data communication. It is a fundamental aspect of network security and management, as it allows administrators and security professionals to monitor, control, and secure network traffic effectively.

SOLUTION : Implement Network Security Controls:

Firewalls: Configure firewalls to filter and control incoming and outgoing traffic. Ensure that only necessary protocols are allowed, and block or restrict unnecessary or deprecated ones.
Intrusion Detection/Prevention Systems (IDS/IPS): Implement IDS/IPS to detect and block any malicious traffic that might exploit protocol detection vulnerabilities.
Content Inspection: Implement content inspection mechanisms to detect and block malformed or unexpected protocol requests.

Business Impact : Data Exfiltration:

Once inside the network, attackers may use these vulnerabilities to exfiltrate sensitive data. This can result in the exposure of customer data, trade secrets, or proprietary information, leading to legal and reputational damage.
Service Disruption:

Protocol detection vulnerabilities can be exploited to disrupt network services or applications, leading to downtime. This can directly impact business operations, resulting in lost revenue and productivity.

Malware Injection:

Attackers may use protocol detection vulnerabilities to inject malware into systems. This can lead to the spread of malware within the organization, causing further security issues and potential damage to business operations.

Vulnerability Name :

157288 - TLS Version 1.1 Protocol Deprecated

Serverity : Protocols that are moderately deprecated are those with a larger user base or are still in use but have known issues or vulnerabilities. Deprecating such protocols may cause inconvenience for some users, but it's generally manageable.

Pulgin :

tcp/443/www

PORT : tcp/443

DESCRIPTION : The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.

SOLUTION : Check for Documentation: First, consult the documentation or error message itself to see if it provides any information on which protocol is deprecated and what protocol you should use instead**.**

Update Software: Ensure that you are using the latest version of the software or library that's generating the error. Developers often release updates to address deprecated protocols.

Business Impact : Compatibility Issues: Deprecated protocols may not be compatible with newer technologies or systems. Businesses may face challenges when trying to integrate legacy systems with newer ones, leading to reduced efficiency and compatibility issues.

Security Risks: Deprecated protocols may have known security vulnerabilities that are no longer patched or updated. This can pose a significant security risk to businesses, as hackers and malicious actors may target vulnerabilities in outdated protocols to breach systems and compromise data.

Vulnerability Name : 161159 - Apache Tomcat 9.0.0.M1 < 9.0.21 vulnerability

Serverity : Ease of Exploitation: The level of skill, effort, and resources required to successfully exploit the vulnerability. Vulnerabilities that can be easily and quickly exploited are often considered more severe.

Access and Privilege: Whether the vulnerability allows an attacker to gain access to sensitive data or systems and the level of privileges or control they can obtain once inside

Pulgin :

tcp/443/www

PORT : tcp/443

DESCRIPTION : The version of Tomcat installed on the remote host is prior to 9.0.21. It is, therefore,
affected by a vulnerability as referenced in the
fixed_in_apache_tomcat_9.0.21_security-9 advisory.
- If a web application sends a WebSocket message concurrently with the WebSocket
connection closing when running on Apache Tomcat 8.5.0 to 8.5.75 or Apache Tomcat 9.0.0.M1 to 9.0.20, it is possible that the application will continue to use the
socket atier it has been closed. The error handling triggered in this case could cause
the a pooled object to be placed in the pool twice. This could result in subsequent
connections using the same object concurrently which could result in data being
returned to the wrong use and/or other errors. (CVE-2022-25762)

SOLUTION : Applying patches or updates: Many vulnerabilities can be fixed by applying patches or updates provided by software vendors.
Configuration changes: Adjust system configurations to reduce the attack surface and enhance security**.**
Code fixes: If vulnerabilities are in custom software, developers may need to

fix the underlying code.
Network or firewall rules: Implement rules or policies that restrict access to vulnerable services or ports.

Business Impact : Intellectual Property Theft: Vulnerabilities can be exploited to steal intellectual property, which can harm a business's long-term innovation and competitiveness.

Supply Chain Risks: Vulnerabilities in an organization's supply chain can impact the availability and quality of products or services, which can affect customer satisfaction and revenue.

Increased Costs: Vulnerabilities often require investments in security measures, compliance efforts, and incident response. These additional costs can strain an organization's budget.

Stage 3 Report

Title:- Ability of SOC / SEIM

SOC:

Security Operations Centers (SOCs) :-

A Security Operations Center (SOC) is a team of highly skilled IT security experts who work tirelessly to monitor an organization's complete IT infrastructure around the clock. Their primary focus is to identify any cybersecurity events in real-time and respond to them with speed and efficiency. In addition, the SOC is responsible for selecting, operating, and maintaining an organization's cybersecurity technologies while continuously analyzing threat data to enhance the organization's overall security posture. The most significant advantage of SOC is the ability to unify and coordinate an organization's security tools, practices, and response to security incidents. This results in a swift, efficient, and cost-effective response to security threats..

SOC - CYCLE

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

To begin the cycle, the first stage is "Detection and Monitoring," which involves constant surveillance of an organization's digital environment. This includes networks, systems, and applications, all monitored using advanced tools and technologies to identify potential vulnerabilities, anomalous activities, or signs of a security breach. Proactive monitoring helps identify early threats, thereby reducing the likelihood of a successful cyber-attack.

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

SIEM

SIEM, short for Security Information and Event Management, is a comprehensive solution that empowers organizations to identify, analyze, and respond to security threats before they disrupt business operations. This cutting-

edge technology combines Security Information Management (SIM) and Security Event Management (SEM) to create a powerful security management system that collects event log data from various sources, identifies deviant activity in real-time, and takes appropriate action. Essentially, SIEM provides organizations with complete visibility into their network activity, allowing them to respond quickly to potential cyber threats and stay compliant. With the advancements in artificial intelligence, SIEM technology has become smarter and faster in detecting threats and responding to incidents in the past decade.

SIEM - CYCLE

The process of SIEM (Security Information and Event Management) is a crucial component in cybersecurity that involves the collection, correlation, and analysis of security data from various sources within an organization's IT infrastructure.

To begin, the process starts with "Data Collection and Aggregation," which involves gathering security-related data from multiple sources such as firewalls, intrusion detection systems, servers, and applications. This data is then centralized in a SIEM platform, which serves as a centralized nerve center for security events. The platform standardizes and organizes this data, making it easier to analyze and identify potential security incidents.

Following this is the "Event Correlation and Analysis" phase. During this stage, the SIEM system utilizes predefined rules and algorithms to correlate and analyze the collected data. The system searches for patterns, anomalies, and potential threats that may indicate a security incident. Security analysts are instrumental in this phase, refining the rules and investigating any alerts generated by the system. They also contextualize the information, evaluating the potential impact, and determining the appropriate response. This phase is critical in identifying and prioritizing security incidents for further investigation and action.

MISP:

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

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

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

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

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

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

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

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

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

Collaboration: MISP allows organizations to share threat intelligence information with each other in a secure and controlled manner.
Analysis: MISP provides tools for analyzing threat intelligence information, such as correlation and enrichment.

Automation: MISP can be integrated with other security tools, such as SIEMs and intrusion detection systems, to automate the sharing and consumption of threat intelligence information.

MISP community: MISP is an open-source project with a large and active community. The community provides support to MISP users through a variety of channels, including mailing lists, IRC chat, and forums.

MISP deployments: MISP is used by a wide range of organizations, including government agencies, businesses, and non-profit organizations. Some notable examples include:

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

College Network Information:

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

CANs are typically larger and more complex than local area networks (LANs), which are typically limited to a single building or office. However, CANs are smaller than metropolitan area networks (MANs) and wide area networks (WANs), which connect networks across large geographic areas.

CANs are typically owned and operated by the college or university itself. This allows the institution to have complete control over the network and its security.

How do you think you deploy soc in your college?

To deploy a SOC in a college, I would recommend the following steps:

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

- Threat intelligence :

Threat intelligence is detailed, actionable threat information for preventing and fighting cyber threats targeting an organization. It is data containing detailed knowledge about the cybersecurity threats targeting an organization. Threat intelligence helps security teams be more proactive, enabling them to take effective, data-driven actions to prevent cyber attacks before they occur. It can also help an organization better detect and respond to attacks in progress .

Threat intelligence involves gathering, analyzing, and using information about current and potential cybersecurity threats. It helps organizations understand the types of threats they might face, the tactics, techniques, and procedures used by threat actors, and the vulnerabilities they might exploit.

Threat intelligence is crucial for proactive cybersecurity. It helps organizations assess their risks, make informed decisions, and improve their security posture.

- Incident response :

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

The key steps in incident response include preparation, identification, containment, eradication, recovery, and lessons learned. It's a cyclical process designed to minimize damage and reduce recovery time and costs.

Effective incident response can help organizations limit the impact of a breach and prevent it from happening again.

- Qradar & understanding about tool :

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

QRadar collects and analyzes data from a wide range of sources, including network traffic, logs, and events, to identify security threats and anomalies.

Key features of QRadar include real-time event correlation, log management, user behavior analytics, and vulnerability assessment.

QRadar is often used by organizations to centralize their security information, detect and respond to security incidents, and improve compliance with security regulations.

Stage 1 :- what you understand from Web application testing .

Web application testing is a comprehensive evaluation of web-based software applications that focuses on functionality, security, and performance. Functionality testing examines various aspects, ranging from basic navigation to complex tasks such as database interactions, to ensure a seamless user experience free of bugs. In addition, compatibility with different browsers and devices is checked to ensure smooth user interaction.

Security is a major concern, and testers actively look for vulnerabilities such as SQL injection and cross-site scripting. By simulating potential attacks, weaknesses are identified, and recommendations are made for fortification. This ensures the protection of sensitive data and resilience against cyber threats. In summary, web application testing is essential for a secure, reliable, and user-friendly online experience.

- Stage 2 :- what you understand from the nessus report .

The Nessus tool generates a detailed report known as a Nessus report, which is widely used by cybersecurity professionals, network administrators, and penetration testers to identify and evaluate security vulnerabilities in computer systems and networks. This report typically includes crucial information such as

historical data, risk management, and recommendations. It also provides a comprehensive list of identified vulnerabilities, their severity level, a brief description, and the systems or devices affected. The severity levels assigned by Nessus, such as Critical, High, Medium, and Low, enable users to prioritize their remediation efforts in risk assessment.
- Stage 3 :- what you understand from SOC / SEIM / Qradar Dashboard .
The SOC, or Security Operations Center, serves as a centralized hub for an organization to monitor, detect, and respond to any security threats or incidents. SIEM, which stands for Security Information and Event Management, is a powerful technology that collects and analyzes security event data in order to detect and respond to any security incidents that may occur.
The QRadar Dashboard is a highly intuitive interface within IBM's QRadar SIEM that provides real-time information and analytics on an organization's security events and incidents, offering an effective means of monitoring and responding to any potential threats.

Future Scope :-
- Stage 1 :- future scope of web application testing
The future scope of web application testing is poised for significant growth and evolution, driven by the continuous advancement of technology and the increasing reliance on web-based solutions across industries.

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

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

- Stage 2 :- future scope of testing process you understood .

As the Nessus scanning technology continues to evolve, it is expected to offer even more advanced features to its users. One such area of improvement is the automation of various scanning processes, leading to a more streamlined and efficient experience. In addition to this, the scope of Nessus scanning is set to expand to include coverage for cloud and IoT devices, which are becoming increasingly popular among businesses and individuals. Furthermore, the integration of advanced threat intelligence is expected to enhance the scanning capabilities of Nessus, making it easier to identify and mitigate potential vulnerabilities. Finally, Nessus scanning is also expected to offer more advanced reporting features, allowing for more comprehensive and efficient vulnerability assessments.

- Stage 3 :- future scope of SOC / SEIM

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

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

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

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