

**MAIN DOCUMENT**

**Team ID:** 2.10

**Project name:** Malware Detection and Classification

**Team members:** Sohan [sohan.21bce8402@vitapstudent.ac.in]

Pratheek [pratheek.21bce7819@vitapstudent.ac.in]

Shaz [shaz.alam2021@vitbhopal.ac.in]

Atharva [atharva2021@vitbhopal.ac.in]

**Abstract:**

Malware, or malicious software, continues to pose a significant threat to cybersecurity, leading to data breaches, financial losses, and system vulnerabilities. To combat this growing menace, advanced artificial intelligence (AI) technologies have emerged as a powerful tool for malware detection and classification. This two-page abstract explores the intricate world of AI-powered solutions in the field of cybersecurity and how they are revolutionizing the way we identify and mitigate malware threats.

The first page delves into the fundamental concepts of malware and highlights the persistent challenges associated with traditional signature-based detection methods. It then introduces AI as a groundbreaking approach to tackling malware, emphasizing its capacity to adapt and evolve alongside the ever-changing threat landscape. The concept of machine learning, specifically deep learning, and neural networks, is explored, shedding light on how these AI models can effectively detect novel and previously unseen malware variants. The second page delves into the practical applications of AI in malware detection and classification. It discusses the intricacies of feature extraction, the importance of labeled datasets, and the role of anomaly detection in identifying malicious behaviors. Moreover, it explores real-world case studies of AI-powered systems in action, highlighting their remarkable accuracy in discerning between benign and malicious software.

The abstract also touches upon the ethical considerations surrounding AI-powered malware detection, emphasizing the necessity of transparency, accountability, and fairness in AI algorithms. Furthermore, it discusses the ongoing challenges in the field, such as adversarial attacks on AI models and the need for continuous model retraining to remain effective in the face of evolving threats.

In conclusion, AI-powered malware detection and classification represent a pivotal turning point in cybersecurity, offering robust, adaptive, and efficient solutions to an ever-growing threat landscape. This abstract provides a comprehensive overview of the potential and challenges of AI in combating malware and highlights its role as a critical tool in safeguarding our digital world.

**Empathy Map**



**Ideation Phase**

**Brainstorm & Idea Prioritization Template**

**Step-1: Team Gathering, Collaboration, and Select the Problem Statement**

Malware is malicious software designed to infect a system and achieve various malicious purposes. Malware can steal or encrypt data, capture login credentials, and take other actions to profit the attacker or harm the target.

Malware detection uses various tools and techniques to identify the presence of malicious software on a system. By proactively working to remediate malware infections on its systems, an organization can limit the cost and impact they have on the business.

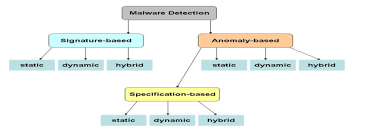
**Step-2: Brainstorm, Idea Listing and Grouping**

## Malware Detection Technologies

To implement these techniques and effectively detect malware, companies can use various tools, including:

* **Intrusion Detection System (IDS):**[An IDS](https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/) is a security solution that identifies malware or other threats entering a network or installed on a system. An IDS generates an alert about the presence of the threat for security personnel to review.
* **Intrusion Prevention System (IPS):** [An IPS](https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/)is like an IDS but takes a more proactive role in defending the organization against attack. In addition to generating an alert about identified threats, the IPS (Intrusion Prevention System) also blocks them from reaching the target system.
* **Sandboxing:** [Sandboxing](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/)involves performing dynamic analysis of malware in a safe, isolated environment. Malware sandboxes have various built-in tools designed to monitor the malware’s activities, determine if it is malicious, and map out its capabilities.
* **Malware Analysis Tools:** Malware analysis tools are available to implement the various malware detection techniques described previously. For example, disassemblers like the Interactive Disassembler (IDA) are used for static analysis, while a debugger is a common tool for dynamic analysis.
* **Cloud-Based Solutions:** Cloud-based infrastructure provides organizations with the ability to enhance their malware detection capabilities beyond what is feasible in-house. Cloud-based solutions can distribute IoCs (indicators of compromise) to the users of a particular solution and perform sandboxed analysis of potential malware at scale.

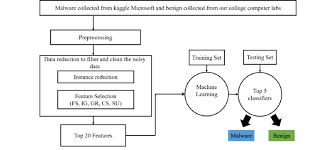
**Step-3: Idea Prioritization**



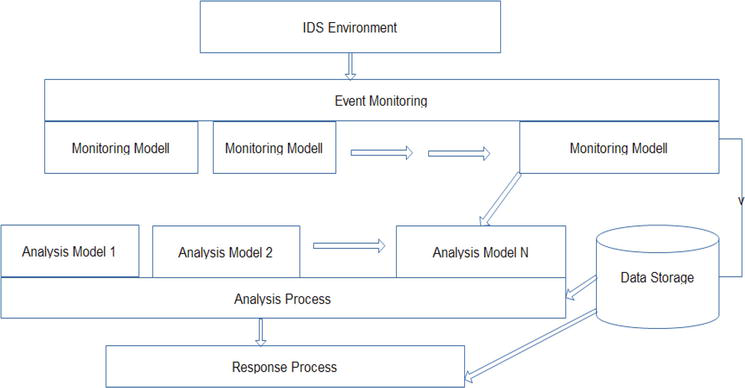
illustrates the techniques for malware detection that work in a flow including data processing, feature selection, classifier training, and malware detection. The process begins with collecting datasets from the Kaggle website consisting of malware and benign web applications. By adopting AI technology, the development of malware detection systems shall be in a way that will process malware datasets and analyse malware to understand its feature. Fisher Score (FS), Chi-Square (CS), Information Gain (IG), Gain Ratio (GR), and Uncertainty Symmetric (US) are used to select 20 features. The system shall train the classifier by comparing different classifiers on FS, CS, IG, GR, and US to detect unknown malware.

Implementing diverse types of classifiers to develop malware detection and prevention systems shall provide better and using AI shall bring a significant advantage to detect and prevent unknown malicious activities [35]. In Fig. 5, we display a flowchart of unknown malware detection using artificial intelligence. In this section, we provide a detailed review of each method of Malware Detection.

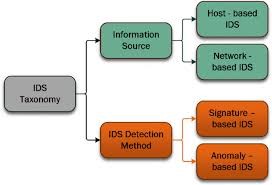
• Signature-based Detection Technique: The signature-based detection method consists of four components as depicted in Fig. 6 is a term that helps in identifying and detecting attacks by looking for specific patterns [40]. In a signature-based method, developers use a database containing signatures of viruses, scan the file, and evaluate information with that database for detecting malware in the database. If the information matches with the database’s data that means the file contains viruses. The primary advantage of this method is effective for the known malware; however, it has limitations in detecting unknown malware [41]. Fig. 7 shows Intrusion Detection System (IDS) keeps a statistical model of traffic that also can be referred to a database, IDS accepts traffic from various sources and matches it with statistical traffic to find out whether it is malicious or not and then provides the result to an administrator.



* Anomaly-based Detection Technique: Anomaly-based network intrusion detection plays a vital role in addressing security issues and protecting networks against malicious activities [43]. Anomaly-based methods address the limitations of signature-based techniques by enabling to detect any of known or unknown malware by applying classification techniques over activities of a system for malware detection. Such transformation from pattern-based detection to a classification-based approach to identify normal or anomalous behaviour gives an advantage of detecting malware activities

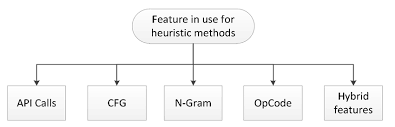


It depicts the anomaly-based Network Intrusion Detection System (IDS) where the functional stages are normally adopted in the anomaly-based network intrusion detection systems (ANIDS)



On the other hand, Figure. Illustrates a connection with a database consists of the signature of known attacks, with the common signatures coming from different packets with that database, an alert is sent to the system admin if the unknown signature matches with known signature mean malware detected.

* Heuristic-based Detection Technique: Applying Artificial Intelligence over the signature and anomaly-based detection systems improve the efficiency of malware detection. However, to adopt environmental change and improve prediction ability, a machine learning algorithm named genetic algorithm along with neural network was applied over malware detection system to improve the classification method. The algorithm applies characteristics such as inheritance, selection, and combination that give the advantage to attain optimum solutions from multiple directions without any previous knowledge about the system [45]. The combination of statistical and mathematical techniques improves the heuristic method from previous methods. It represents the features of the Heuristic Method



**PRACTISE WEBSITE VULNERABILITIES**

**Invalid Forgot Password Process**

CWE: CWE-640

OWASP Category: A04:2021 – Insecure Design

Description: Architectural flaws can result in security vulnerabilities if appropriate security mitigations are not taken in the design phase of the practice website. Specifically, this vulnerability pertains to the "Forgot Password" process, which may have security weaknesses due to design flaws.

Business Impact: Insecure design of the "Forgot Password" process can make the practice website susceptible to a range of weaknesses. This documentation section addresses the potential impacts and suggests mitigation strategies to improve the security of this process.

Vulnerability Path

URL: <http://yourpracticewebsite.com/forgot_password>

Vulnerability Parameter: <http://yourpracticewebsite.com/forgot_password>

Steps to Reproduce:

Access the URL: <http://yourpracticewebsite.com/forgot_password>

Navigate to the login page.

Enter a random password for testing.

Observe the auto-generated password below the "Forgot Password" section.

Recommendation:

Establish and use a library of secure mechanisms.

Implement a strong validation process to enhance the security of the "Forgot Password" feature.

**Cross-Site Scripting (Stored)**

CWE: 79

OWASP Category: A03:2021 – Injections

Description: Cross-Site Scripting (Stored) occurs when a malicious script is injected directly into the practice website. This vulnerability pertains to the storage and subsequent reflection of a malicious script in the web application, particularly within user-generated content.

Business Impact: Storing dangerous data, such as malicious scripts, in a database can have severe security implications. If executed, these scripts can potentially compromise user data and the overall integrity of the practice website.

Vulnerability Path

URL: <http://yourpracticewebsite.com/admin/user.php>

Vulnerability Parameter: <http://yourpracticewebsite.com/admin/user.php>

Steps to Reproduce:

Access the URL: <http://yourpracticewebsite.com/admin/user.php>

Log in with your credentials.

Attempt to register as a new user.

In the registration form, insert a malicious script within the contact box.

Observe the effects of the injected script.

**Insecure File Upload**

CWE: CWE-434

OWASP Category: A8:2017 – Insecure Deserialization

Description: Insecure file upload allows users to upload potentially malicious files, which can lead to remote code execution and other security threats.

Business Impact: Insecure file uploads can result in the execution of malicious code on the server, leading to unauthorized access and data breaches.

Vulnerability Path

URL: <http://yourpracticewebsite.com/upload>

Vulnerability Parameter: <http://yourpracticewebsite.com/upload>

Steps to Reproduce:

Access the file upload feature.

Attempt to upload a file containing executable code.

Observe if the website allows and executes the file.

**SQL Injection Vulnerability**

CWE: CWE-89

OWASP Category: A1:2017 – Injection

Description: SQL Injection is a type of security vulnerability that occurs when an attacker can manipulate an SQL query in a web application, potentially allowing unauthorized access to databases and data manipulation.

Business Impact: SQL Injection can lead to unauthorized access to sensitive data, data manipulation, and in some cases, complete control over the application's database.

Vulnerability Path

URL: <http://yourpracticewebsite.com/search>

Vulnerability Parameter: <http://yourpracticewebsite.com/search?q=>

Steps to Reproduce:

Access the search functionality on the website.

In the search bar, enter a malicious SQL query.

Observe if the website handles the query securely.

**Insecure File Upload**

CWE: CWE-434

OWASP Category: A8:2017 – Insecure Deserialization

Description: Insecure file upload allows users to upload potentially malicious files, which can lead to remote code execution and other security threats.

Business Impact: Insecure file uploads can result in the execution of malicious code on the server, leading to unauthorized access and data breaches.

Vulnerability Path

URL: <http://yourpracticewebsite.com/upload>

Vulnerability Parameter: <http://yourpracticewebsite.com/upload>

Steps to Reproduce:

Access the file upload feature.

Attempt to upload a file containing executable code.

Observe if the website allows and executes the file.

**Broken Session Management**

CWE: CWE-613

OWASP Category: A2:2017 – Broken Authentication

Description: Broken session management vulnerabilities can allow attackers to hijack sessions, impersonate users, and gain unauthorized access to sensitive data.

Business Impact: Broken session management can lead to unauthorized access, data breaches, and identity theft.

Vulnerability Path

URL: <http://yourpracticewebsite.com/profile>

Vulnerability Parameter: <http://yourpracticewebsite.com/profile>

Steps to Reproduce:

Log in to your user account.

Access the user profile.

Log out.

Attempt to access the profile again without logging in.

**Cross-Site Request Forgery (CSRF)**

CWE: CWE-352

OWASP Category: A8:2017 – Cross-Site Request Forgery (CSRF)

Description: CSRF is an attack that tricks the user into executing unwanted actions on a different website where they are authenticated.

Business Impact: CSRF attacks can lead to unauthorized actions being taken on behalf of the user, potentially compromising their account or data.

Vulnerability Path

URL: <http://yourpracticewebsite.com/change_password>

Vulnerability Parameter: <http://yourpracticewebsite.com/change_password>

Steps to Reproduce:

Log in to your user account.

Visit a malicious website that contains a CSRF attack.

Observe if unauthorized actions are taken on the practice website.

**XML External Entity (XXE) Injection**

CWE: CWE-611

OWASP Category: A4:2017 – XML External Entity (XXE) Processing

Description: XXE vulnerabilities occur when an application processes XML input from untrusted sources, potentially leading to disclosure of internal files, denial of service, and remote code execution.

Business Impact: XXE vulnerabilities can expose sensitive information, disrupt services, and lead to data breaches.

Vulnerability Path

URL: <http://yourpracticewebsite.com/parse-xml>

Vulnerability Parameter: <http://yourpracticewebsite.com/parse-xml?xml=>

Steps to Reproduce:

Access the XML parsing feature on the website.

Submit an XML file with a malicious external entity definition.

Observe if the website processes the XML insecurely.

**Security Misconfiguration**

CWE: CWE-732

OWASP Category: A6:2017 – Security Misconfiguration

Description: Security misconfigurations occur when an application is not securely configured, leading to vulnerabilities such as unauthorized access, data exposure, and other security risks.

Business Impact: Security misconfigurations can result in data breaches, unauthorized access, and financial costs.

Vulnerability Path

URL: <http://yourpracticewebsite.com/admin>

Vulnerability Parameter: <http://yourpracticewebsite.com/admin>

Steps to Reproduce:

Access the admin section of the website.

Observe if there are security misconfigurations that allow unauthorized access.

**Missing Function-Level Access Control**

CWE: CWE-284

OWASP Category: A5:2017 – Broken Access Control

Description: Missing function-level access control vulnerabilities occur when an application does not properly check whether a user has access to certain functions or actions.

Business Impact: This can lead to unauthorized access and the execution of restricted functions.

Vulnerability Path

URL: <http://yourpracticewebsite.com/change-email>

Vulnerability Parameter: <http://yourpracticewebsite.com/change-email>

Steps to Reproduce:

Log in as a regular user.

Access a privileged function, such as changing another user's email.

Observe if the website enforces proper access control.

**Cross-Origin Resource Sharing (CORS) Misconfiguration**

CWE: CWE-346

OWASP Category: A7:2017 – Cross-Site Scripting (XSS)

Description: CORS misconfigurations can allow unauthorized websites to make requests to your site on behalf of a user, potentially exposing sensitive data.

Business Impact: CORS misconfigurations can lead to data exposure, unauthorized access, and privacy violations.

Vulnerability Path

URL: <http://yourpracticewebsite.com/api>

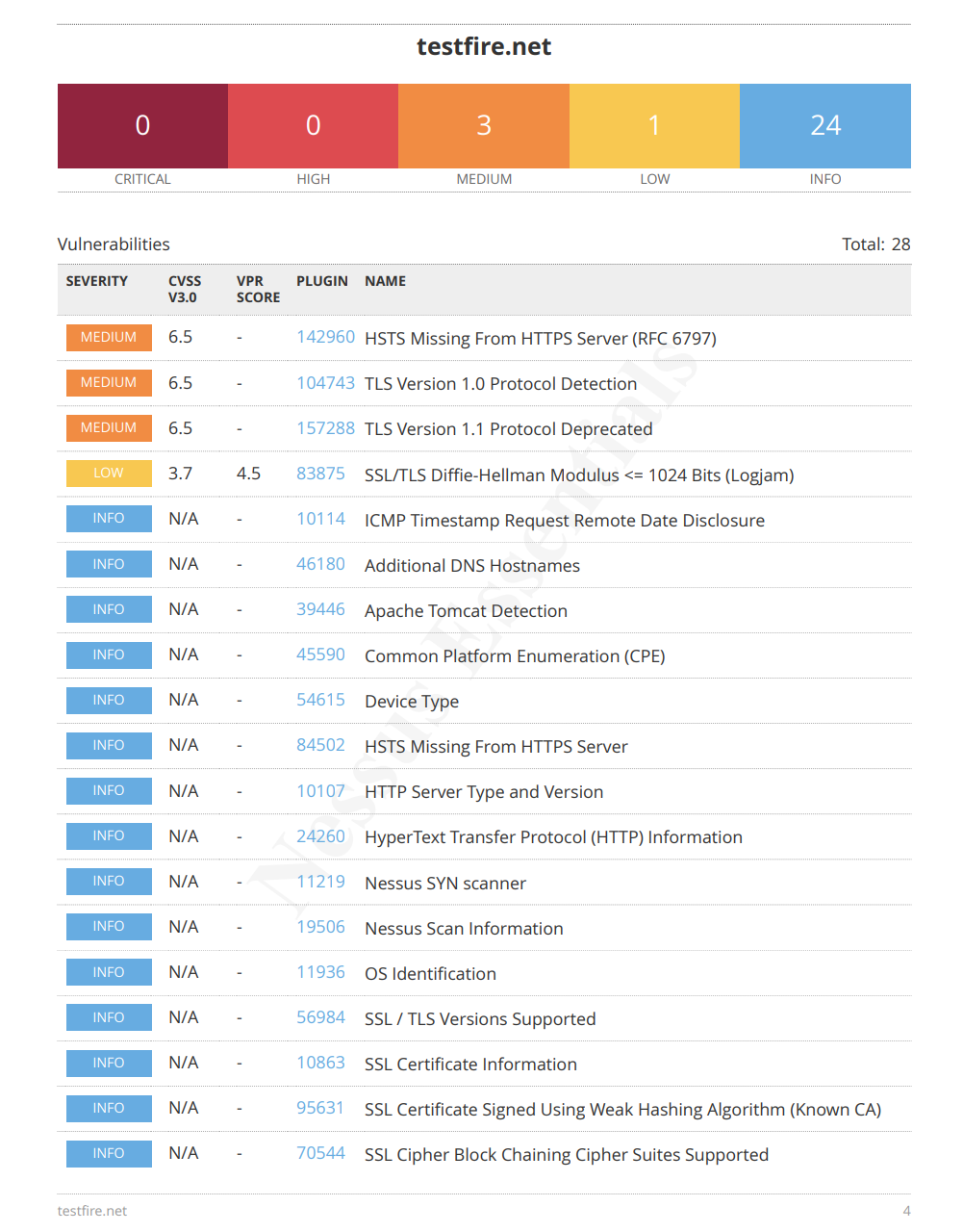
Vulnerability Parameter: <http://yourpracticewebsite.com/api>

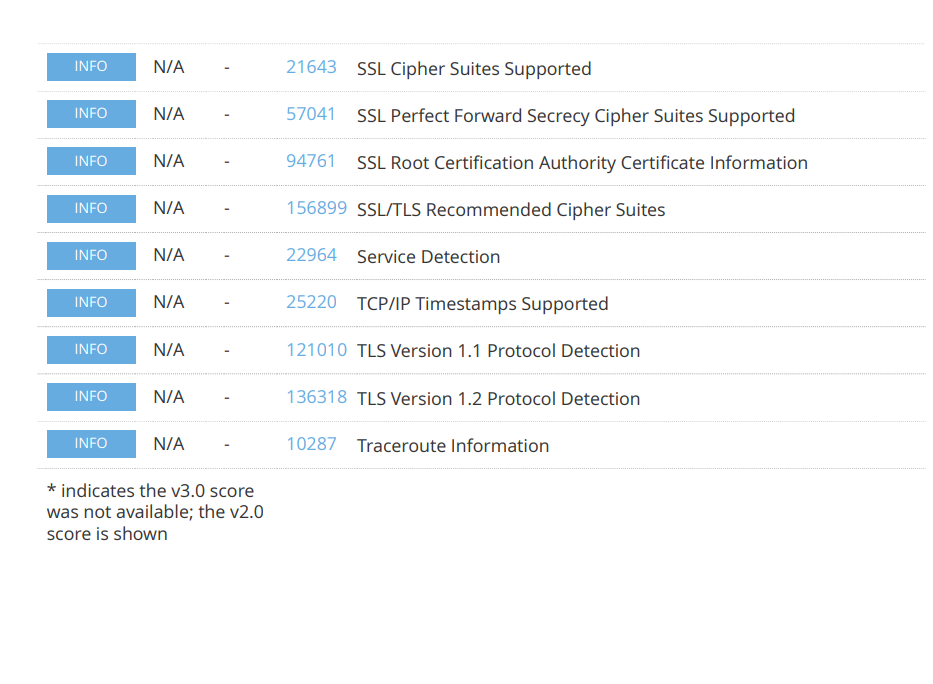
Steps to Reproduce:

Access the website's API.

Observe if there are misconfigured CORS settings that allow cross-origin requests.







**MAIN WEBSITE**

**Vulnerability Name**: Unquoted Search Path or Element

**CWE:** CWE-428

**OWASP Category**: A1: Injection

**Description:** The product uses a search path that contains an unquoted element, in which the element contains whitespace or other separators. This can cause the product to access resources in a parent path.

**Business impact:** CWE-428, the "Unquoted Search Path or Element" vulnerability, can result in serious business impacts:

Security Risks: It opens the door to security breaches and unauthorized access.

Operational Disruption: Exploitation can lead to downtime and loss of productivity.

Legal and Compliance Issues: Non-compliance may result in legal penalties and regulatory fines.

Reputation Damage: Trust and reputation can be severely damaged.

Financial Costs: Remediation and recovery can be costly.

**Vulnerability Name:** Out-of-bounds Write

**CWE:** CWE-787

**OWASP Category:** A7: Security Misconfiguration

**Description:** The product writes data past the end, or before the beginning, of the intended buffer. Typically, this can result in corruption of data, a crash, or code execution. The product may modify an index or perform pointer arithmetic that references a memory location outside of the buffer's boundaries. A subsequent write operation then produces undefined or unexpected results.

**Business impact:** CWE-787, "Out-of-bounds Write," can have significant business impacts, including:

1. Security Breaches: Exploiting this vulnerability can lead to unauthorized data manipulation, system crashes, or even remote code execution, potentially compromising sensitive information.

2. Loss of Customer Trust: Security incidents resulting from CWE-787 can erode trust and damage a company's reputation, leading to customer loss.

3. Operational Disruption: Addressing and recovering from security breaches can cause downtime and productivity loss, impacting business operations.

4. Legal and Compliance Issues: Non-compliance with data protection regulations may result in legal penalties and regulatory fines.

5. Financial Costs: Remediation and recovery can be costly, including expenses for forensics, legal, and reputation management.

6. Competitive Disadvantage: Businesses with a history of security vulnerabilities may lose customers to more secure competitors.

**Vulnerability Name:** Improper Authentication

**CWE:** CWE-287

**OWASP Category:** A2: Broken Authentication

**Description:** When an actor claims to have a given identity, the payments were indeed made, however.

**Business impact:**

CWE-287, "Improper Authentication," can have several significant business impacts when not properly addressed:

Unauthorized Access: Improper authentication can lead to unauthorized individuals gaining access to sensitive systems or data, potentially resulting in data breaches, theft, or unauthorized actions.

Data Breaches: If attackers exploit authentication weaknesses, they can gain access to sensitive customer or business data, leading to costly data breaches, legal consequences, and damage to a company's reputation.

Loss of Trust: Security incidents involving improper authentication erode trust in a business or service. Customers, partners, and stakeholders may lose confidence in the organization's ability to protect their information.

Legal and Regulatory Consequences: Non-compliance with data protection and privacy regulations can result in fines, legal actions, and other regulatory penalties, further impacting the company's financial health.

Operational Disruption: Remediation efforts, including resetting user accounts or implementing stronger authentication mechanisms, can cause operational disruptions and productivity loss.

**Vulnerability Name:** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

**CWE:** CWE-78

**OWASP Category:** A1: Injection

**Description:** The product constructs all or part of an OS command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.

**Business impact:** CWE-78, which relates to "OS Command Injection," can have several significant business impacts when not properly mitigated:

Unauthorized Access: Command injection vulnerabilities can allow attackers to execute arbitrary commands on a system, potentially leading to unauthorized access and data breaches.

Data Loss or Manipulation: Attackers exploiting this vulnerability may manipulate data, delete critical information, or even compromise the integrity of the system, resulting in data loss and operational disruptions.

Loss of Trust: Security incidents involving OS command injection erode trust in a business or service. Customers, partners, and stakeholders may lose confidence in the organization's ability to protect their information.

Legal and Regulatory Consequences: Non-compliance with data protection and privacy regulations can result in fines, legal actions, and other regulatory penalties, further impacting the company's financial health.

Operational Disruption: Remediation efforts and recovery from a successful attack can cause operational disruptions, resulting in productivity loss.

**Vulnerability Name:** Observable Discrepancy

**CWE:** CWE-203

**OWASP Category:** Observable Differences Based on Input

**Description:** The product behaves differently or sends different responses under different circumstances in a way that is observable to an unauthorized actor, which exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not.

Discrepancies can take many forms, and variations may be detectable in timing, control flow, communications such as replies or requests, or general behavior. These discrepancies can reveal information about the product's operation or internal state to an unauthorized actor. In some cases, discrepancies can be used by attackers to form a side channel.

**Business impact:** CWE-203, "Observable Differences Based on Input," is a type of information leakage vulnerability. While this CWE (Common Weakness Enumeration) may not be as well-known as some other common vulnerabilities, it can still have business impacts:

Data Exposure: Observable differences based on input can inadvertently reveal sensitive information, such as internal data structures, error messages, or system behavior. This exposure can provide valuable information to attackers.

Security Risk: The information leakage can be used by malicious actors to plan and execute targeted attacks. It may help attackers understand the inner workings of a system, identify weaknesses, and devise a more effective attack strategy.

Loss of Competitive Advantage: If proprietary information or unique data structures are exposed, it can undermine a company's competitive advantage, potentially leading to imitations by competitors.

Regulatory Non-Compliance: Depending on the type of data exposed, CWE-203 may result in non-compliance with data protection regulations and privacy laws. Non-compliance can lead to legal penalties and damage an organization's reputation.

**Vulnerability Name:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**CWE:** CWE-22

**OWASP Category:** A4: XML External Entities (XXE)

**Description:** The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

**Business impact:** CWE-22, "Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)," can have several significant business impacts when not properly mitigated:

Data Exposure: Path traversal vulnerabilities can allow attackers to access and retrieve sensitive files or data from the server. This exposure can lead to data breaches and unauthorized access to confidential information.

Loss of Confidentiality: If sensitive data, such as customer records, intellectual property, or financial information, is exposed, it can result in a loss of confidentiality and legal consequences.

Regulatory Non-Compliance: Depending on the type of data exposed, CWE-22 may lead to non-compliance with data protection regulations and privacy laws, resulting in legal penalties and damage to the company's reputation.

Operational Disruption: Remediation efforts, including securing the application and investigating the breach, can disrupt business operations and lead to productivity loss.

Reputation Damage: Data breaches and improper handling of sensitive information can damage an organization's reputation, causing customers and partners to lose trust in the company's ability to protect their data.

Financial Costs: Remediation, legal, and public relations costs associated with path traversal vulnerabilities can be substantial, affecting the company's bottom line.

**Vulnerability Name:** Inappropriate Encoding for Output Context

**CWE:** CWE-838

**OWASP Category:** Security Misconfiguration

**Description:** The product uses or specifies an encoding when generating output to a downstream component, but the specified encoding is different from the encoding that is expected by the downstream component.

**Business impact:** CWE-838, "Inappropriate Access of Resource Through Identifying Information," typically occurs when an application improperly handles sensitive data, leading to business risks and impacts:

Data Exposure: Inappropriate access can result in unauthorized parties gaining access to sensitive data, including customer records, financial information, or intellectual property.

Loss of Confidentiality: The exposure of sensitive data may lead to a loss of confidentiality, resulting in legal consequences and damage to the company's reputation.

Regulatory Non-Compliance: If unauthorized access violates data protection or privacy regulations, it can result in legal penalties, regulatory fines, and additional damage to the organization's reputation.

Operational Disruption: Efforts to secure the application and investigate the breach can disrupt business operations, causing productivity loss.

Reputation Damage: Data breaches and improper handling of sensitive information can damage the organization's reputation, eroding trust in its ability to protect data.

**Vulnerability Name:** Incorrect Authorization

**CWE:** CWE-863

**OWASP Category:** Access Control

**Description:** The product uses or specifies an encoding when generating output to a downstream component, but the specified encoding is different from the encoding that is expected by the downstream component.

**Business impact:**

CWE-863, "Incorrect Authorization," can lead to unauthorized access, data breaches, legal consequences, operational disruptions, reputation damage, financial costs, and a competitive disadvantage. Improper authorization can result in data exposure, privacy violations, regulatory non-compliance, and eroded trust, impacting the company's integrity and success.

**Vulnerability Name:** Exposure of Sensitive Information to an Unauthorized Actor

**CWE:** CWE-200

**OWASP Category:** Sensitive Data Exposure

**Description: The product exposes sensitive information to an actor not explicitly authorized to have access to it.**

**Business impact:**

CWE-200, "Exposure of Sensitive Information to an Unauthorized Actor," can have severe business impacts when not properly mitigated:

Data Breaches: The exposure of sensitive information can lead to data breaches, resulting in unauthorized access to confidential data, including customer records and financial information.

Loss of Trust: Security incidents involving sensitive data exposure erode trust in a business or service. Customers, partners, and stakeholders may lose confidence in the organization's ability to protect their information.

**Vulnerability Name:** Incorrect Permission Assignment for Critical Resource

**CWE:** CWE-732

**OWASP Category:** Security Misconfiguration

**Description:** The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

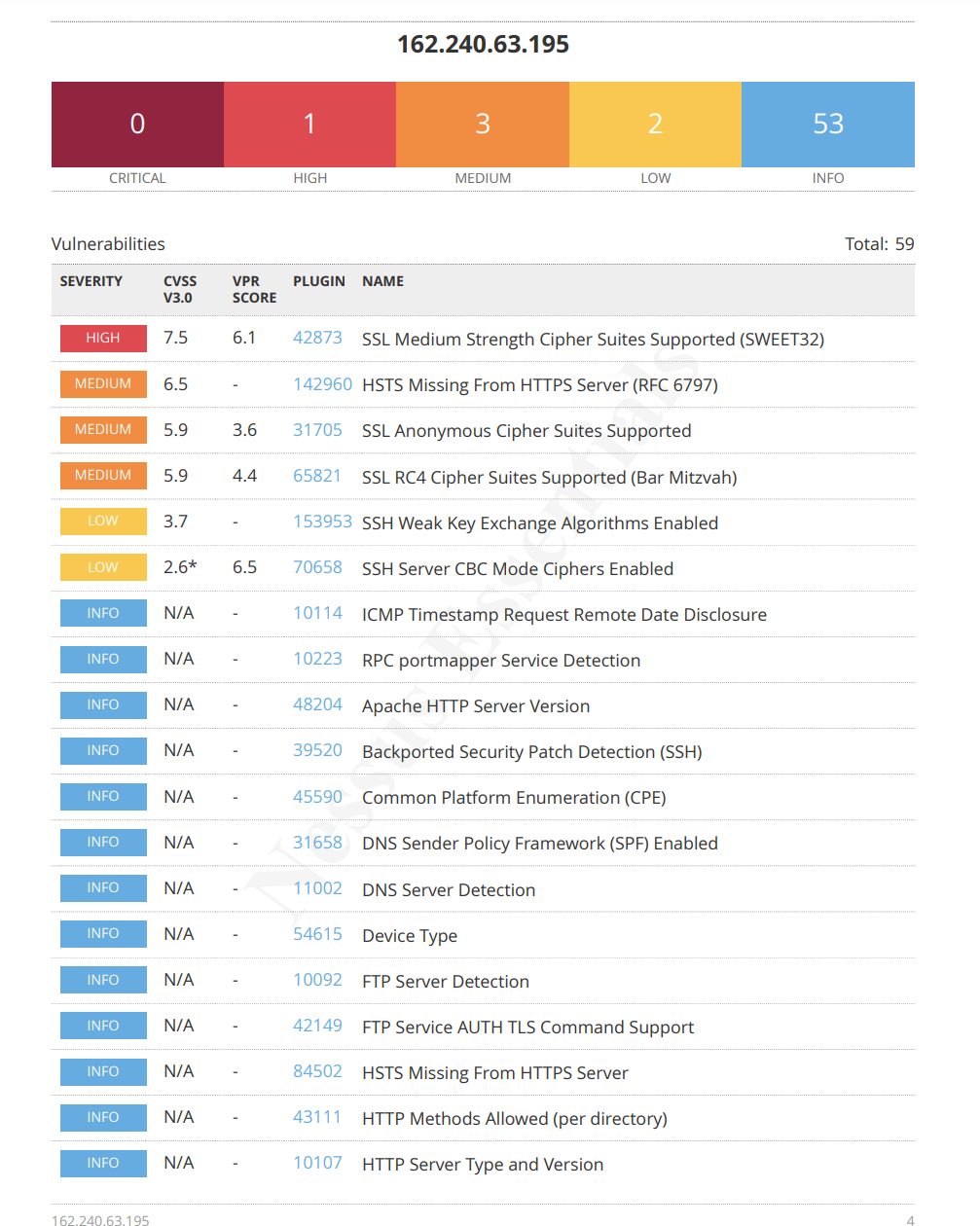
When a resource is given a permission setting that provides access to a wider range of actors than required, it could lead to the exposure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution, or sensitive user data. For example, consider a misconfigured storage account for the cloud that can be read or written by a public or anonymous user.

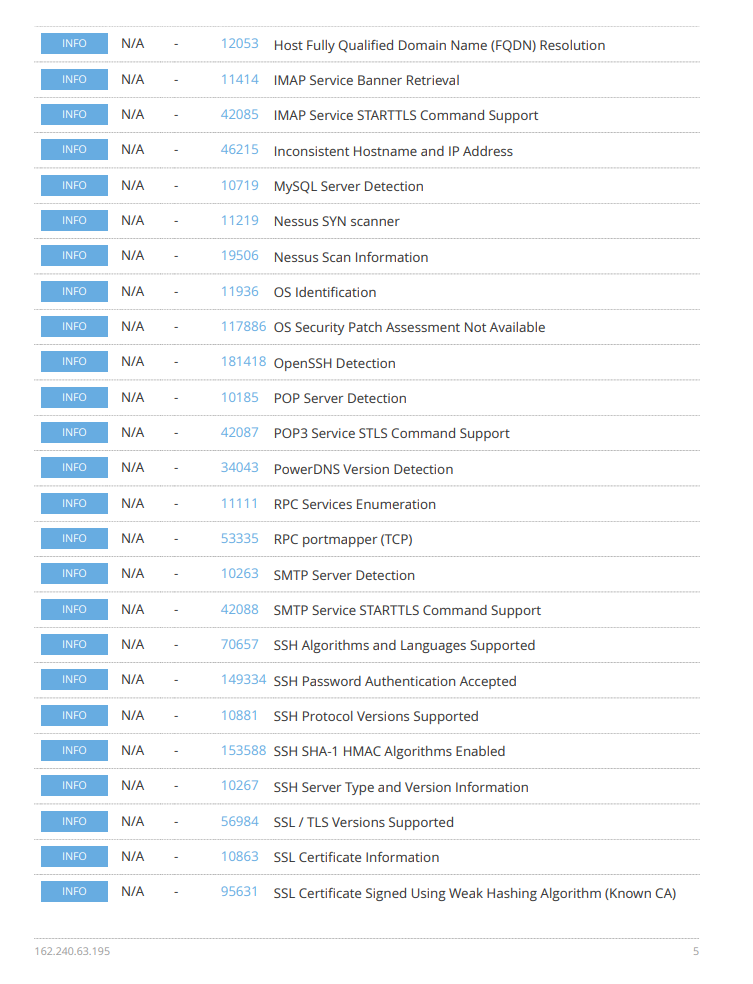
**Business impact:**

CWE-732, "Insecure Permission Assignment for Critical Resource," can have significant business impacts, including unauthorized access to critical resources, data breaches, operational disruption, legal consequences, financial costs, reputation damage, and competitive disadvantages. Failing to secure access to critical resources can lead to data exposure, regulatory fines, trust erosion, and loss of business opportunities, negatively affecting the organization's integrity and success.











**Project Planning Phase Document**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sprint** | **Functional Requirement (Epic)** | **User Story Number** | **User Story / Task** | **Story Points** | **Priority** | **Team Members** |
| Sprint-1 | Registration | USN-1 | As a user, I can register for the application by entering my email, password, and confirming my password. | 2 | High | Sohan, Pratheek, Shaz, Atharva |
| Sprint-1 |  | USN-2 | As a user, I will receive a confirmation email once I have registered for the application. | 1 | High | Sohan, Pratheek, Shaz, Atharva |
| Sprint-2 |  | USN-3 | As a user, I can register for the application through Facebook. | 2 | Low | Sohan, Pratheek, Shaz, Atharva |
| Sprint-1 |  | USN-4 | As a user, I can register for the application through Gmail. | 2 | Medium | Sohan, Pratheek, Shaz, Atharva |
| Sprint-1 | Login | USN-5 | As a user, I can log into the application by entering an email and password. | 1 | High | Sohan, Pratheek, Shaz, Atharva |

**Velocity:**

Imagine we have a 10-day sprint duration, and the velocity of the team is 8 (points per sprint). Let us calculate the team's average velocity (AV) per iteration unit (story points per day).

AV = 8 points / 6 days = 1.33 points/day

**Burndown Chart:**

A burndown chart is a graphical representation of work left to do versus time. It is often used in agile software development methodologies such as Scrum. However, burn-down charts can be applied to any project containing measurable progress over time.

**Proposed Solution Template**

**Proposed Solution Template**

|  |  |  |
| --- | --- | --- |
| **S.No** | **Parameter** | **Description** |
| 1. | Problem Statement | We need to create a smart system that can quickly spot and categorize harmful software (malware) on computers and networks. This system must be good at telling the difference between malware and harmless software. It should work without slowing down your computer and be useful for regular users and big companies. To do this, we will use advanced technology like machine learning and constantly update it to catch new types of malwares. |
| 2. | Solution description | Our approach creates a real-time malware detection system by combining dynamic analysis, machine learning models, and enhanced feature extraction. It is intended to be scalable, accurate, and quick for both people and businesses. To remain ahead of emerging malware threats, this system refreshes its database often, offering strong protection with a dwindling number of false positives. |
| 3. | Uniqueness | Our unique system combines dynamic analysis, real-time monitoring, scalability, and advanced feature engineering. It provides a comprehensive malware detection and categorization method, guaranteeing adaptability to new threats. It stands out because of frequent updates and an emphasis on minimizing false positives and offers a thorough and efficient defense against constantly evolving malware. |
| 4. | Customer satisfaction | One of our solution's main objectives is to guarantee maximum client satisfaction:   1. Effective Protection: We put the user experience and system performance first by correctly detecting and categorizing malware while reducing false positives, which increases satisfaction. 2. User-Friendly Interface: A user-friendly interface that is straightforward and easy to use, has clear reporting, and requires little user involvement.      1. Timely Updates: We are committed to protecting users against new malware threats, which builds trust and satisfaction. Regular updates and proactive threat mitigation show this. 2. Scalability: Our system is designed to fulfil the varied needs of a wide range of customers by accommodating both individual users and large organizations. 3. Support and Assistance: By quickly resolving concerns, offering customer support and assistance for any problems or inquiries strengthens satisfaction. |
| 5. | Business Model | Our business strategy is centered on subscription-based malware detection and classification services. For both individual users and businesses, we provide tiered subscription plans that can be billed monthly or yearly. A freemium or trial version works as a conversion technique and draws in new consumers.    To increase our reach, we also work with OEMs to package our software with new products. Organizations with special demands are catered to through integration solutions and customization services. Our value proposition is improved by consulting and training services that optimize cybersecurity strategy.    In addition, we might investigate joint ventures with cybersecurity suppliers to provide our technology as an extra security measure in their suites. Services related to threat intelligence and data analytics can bring in extra money. Consistent software upgrades and customer service guarantee enduring satisfaction and subscription renewals, which in turn promotes continued business growth |
| 6. | Scalability of the solution | Because of its great scalability, our system can easily grow to meet the changing needs of both small and large businesses. Its scalability is attained by effective resource management, cloud integration, customizable APIs, multi-tiered subscription plans, worldwide support, and continuous R&D. Because of its adaptability, the system may effectively expand to accommodate the needs of a wide range of users. |

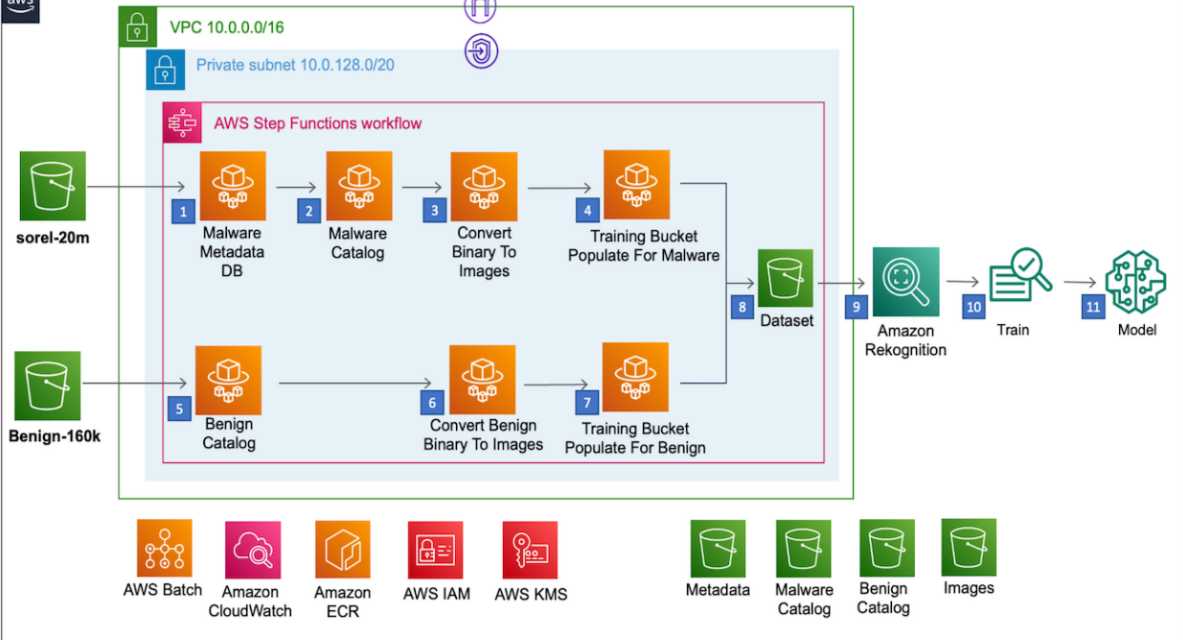
**SOLUTION ARCHITECTURE**

A solution architecture for malware detection and classification involves collecting and preprocessing malware data, employing machine learning models, feature extraction, real-time analysis, and integrating threat intelligence. It should also incorporate feedback loops, reporting, quarantining, and ensure compliance with privacy regulations and robust security measures. The architecture should be scalable, continuously updated, and adaptable to evolving threats.

To train a multi-classification model and a malware-detection model, we first prepare the training and test datasets which contain different malware types such as flooder, adware, spyware, etc., as well as benign objects. We then convert the portable executables (PE) objects into greyscale images.

* Data Collection and Preprocessing: Collect and preprocess malware data from various sources, preparing it for analysis.
* Machine Learning Models: Employ supervised or unsupervised machine learning models for malware detection and classification.
* Real-Time Analysis and Feedback: Implement real-time analysis, integrate threat intelligence, and establish feedback loops for continuous learning and improvement.
* Security and Compliance: Ensure robust security measures, privacy compliance, scalability, and adaptability to evolving threats in the architecture.

**SOLUTION ARCHITECTURE DIAGRAM**

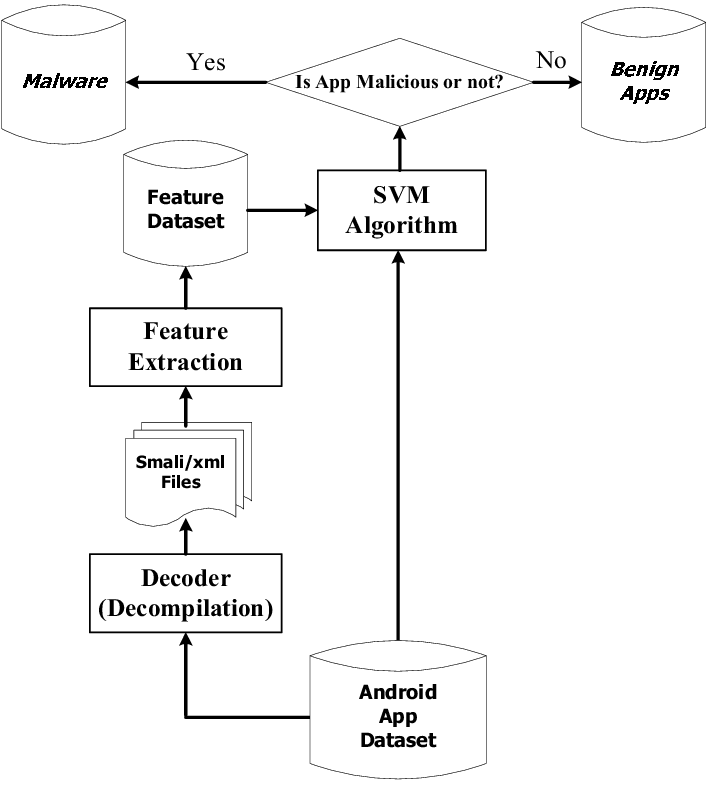


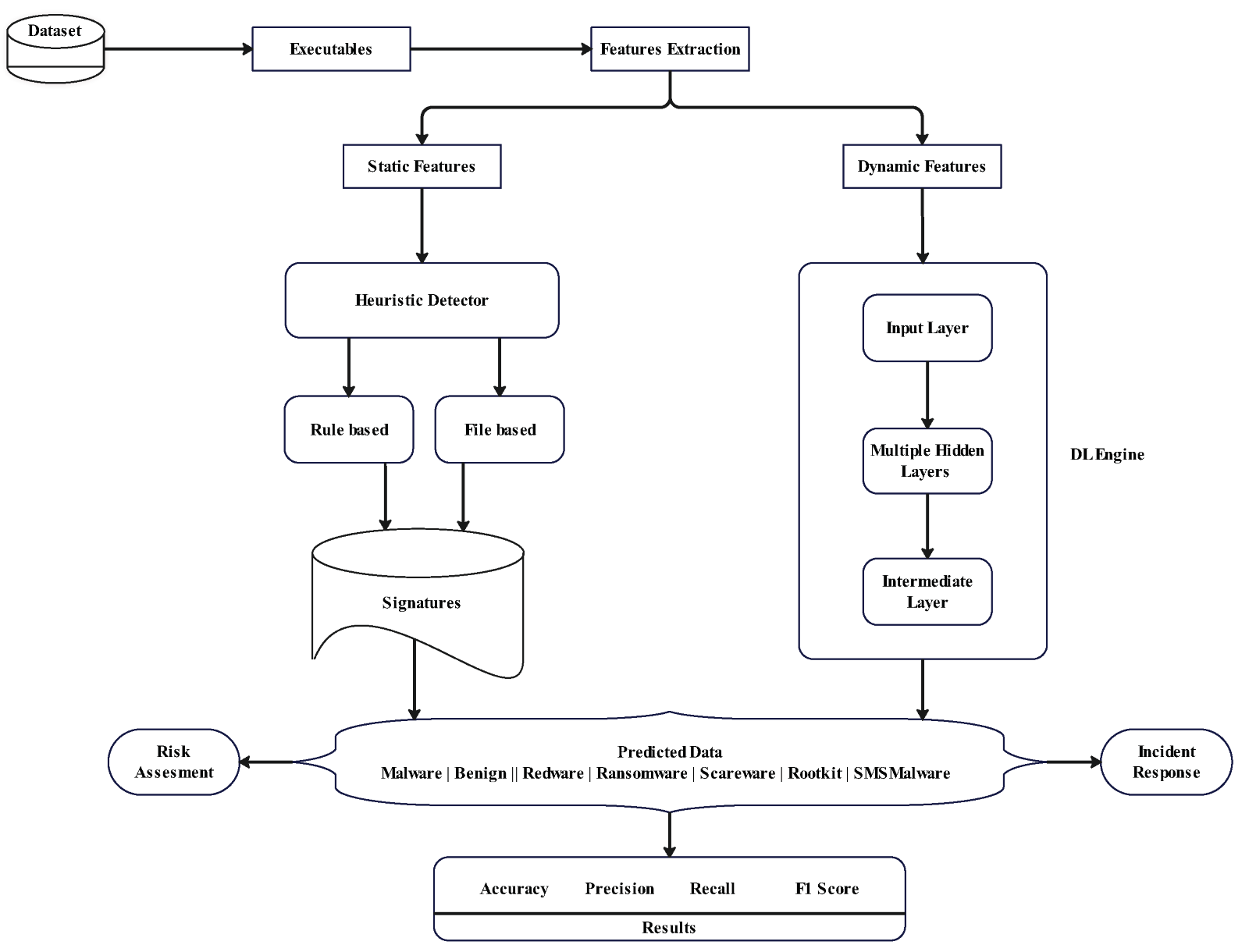
**Data Flow Diagram & User Stories**

**Data Flow Diagrams:**

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.

**Example: DFD Level 0 (Industry Standard)**





**User Stories**

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

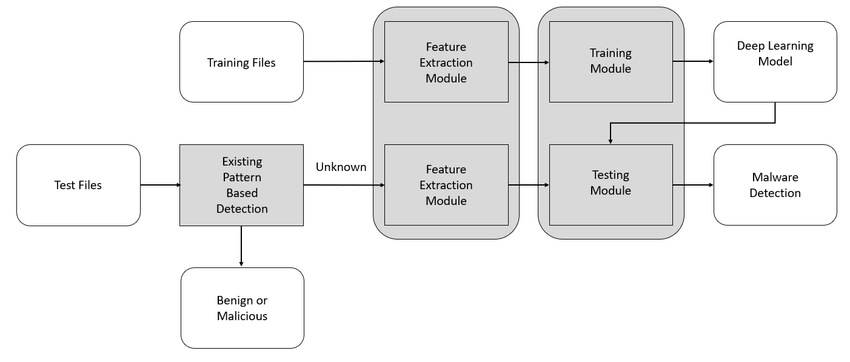
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **User Type** | **Functional**  **Requirement (Epic)** | **User Story**  **Number** | **User Story / Task** | **Acceptance criteria** | **Priority** | **Release** |
| User (Security Analyst) | Registration | USN-1 | As a User, I Want to Submit Files for Scanning | I receive immediate feedback on the submission status. | High | Sprint-1 |
|  | Scan Result | USN-2 | As a User, I Want to View Scan Results | After file scanning, I can view detailed scan results, including whether malware is detected and the type of malware. | High | Sprint-1 |
|  | Settings | USN-3 | As an Administrator, I Want to Manage User Profiles | I can create, modify, or deactivate user accounts. | Medium | Sprint-2 |
|  | Update | USN-4 | As a System, I Want to Automatically Update Malware Signatures | The system regularly fetches updates from threat intelligence feeds. | Medium | Sprint-1 |
|  | Alerts | USN-5 | As an Administrator, I Want to View Alerts | I can acknowledge and investigate alerts and assign them to security analysts. | High | Sprint-1 |
|  | Search | USN -6 | As a User, I Want to Search for Historical Scan Results | I can search and view historical scan results for files I have submitted in the past. | Medium | Sprint-2 |
|  | Reports | USN-7 | As a Security Analyst, I Want to Generate Reports | I can create detailed reports on malware incidents for management and compliance purposes. | High | Sprint-1 |

**Technology Stack (Architecture & Stack)**

**Technical Architecture:**

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

**Example:**

Shape Windows malware detection based on static analysis with multiple features  [PeerJ]Shape Windows malware detection based on static analysis with multiple features  [PeerJ]

**Table-1: Components & Technologies:**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Component** | **Description** | **Technology** |
| 1. | User Interface | Enabling users to configure and customize detection rules and settings. | Configuration and Management. |
| 2. | incident Response Integration: | implementing automated actions or scripts to respond to threats. | Automated Response |
| 3. | Network Traffic Analysis | Examining network packets for signs of malicious activity. | Packet Capture and Analysis |
| 4. | Data Preprocessing: | Ensuring that data from various sources is transformed into a consistent format for analysis. | Data Normalization |
| 5. | Data Storage: | Storing logs, metadata, and threat intelligence data for historical analysis. | Database Systems |
| 6. | Machine Learning and AI: | Identifying relevant features from the data for machine learning models. | Feature Extraction |
| 7. | Behavior-Based Detection: | Rules and algorithms that flag suspicious behaviors. | Heuristics |
| 8. | APIs and Integrations: | APIs and connectors to interact with other security tools and platforms. | Integration Points |
| 9. | Data Collection and Acquisition: | Tools like Wireshark for capturing and analyzing network traffic. | Packet Capture Tools: |
| 10. | Access Control and Security: | Ensuring secure access to the system and its data. | Authentication and Authorization |
| 11. | Compliance and Reporting: | Ensuring the system adheres to relevant industry and regulatory standards. | Compliance Tools |

**Table-2: Application Characteristics:**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Characteristics** | **Description** | **Technology** |
| 1. | Real-Time Monitoring | Malware detection systems continuously monitor network traffic, files, and system activities in real-time to identify and respond to threats as they occur. | Heuristic Analysis, Signature-Based Detection |
| 2. | Anomaly Detection | Malware detection systems can identify deviations from normal network and system behavior, which may indicate a compromise. | Graph Analytics, Flow Analysis, Clustering and Segmentation |
| 3. | Incident Response Integration | Integration with incident response systems and workflows to facilitate a coordinated response to security incidents. | Security Information and Event Management (SIEM) Systems |
|  |  |  |  |
| 4. | Multilayered Approach | They employ multiple detection techniques, including signature-based, behavior-based, and heuristics-based methods, to detect a wide range of malware. | Security Information and Event Management (SIEM) Systems, Intrusion Detection and Prevention Systems (IDS/IPS |
| 5. | Scalability | Effective malware detection systems can scale to accommodate the growing volume of data and traffic in a network or organization. | Distributed Architecture, Scalable Network Traffic Analysis: |

**STAGE 1**

**Title of the project –** Malware Detection and Classification

**Overview-**

Malware Detection and Classification Overview

Malware detection and classification are pivotal elements within the realm of cybersecurity, serving as the first line of defense against an ever-evolving landscape of digital threats. These processes are critical for identifying and categorizing malicious software threats with the primary objective of safeguarding computer systems, networks, and sensitive data.

Malware Detection: methods encompass a variety of techniques, each with its own strengths and weaknesses. Signature-based detection involves comparing code or patterns in files against a vast database of known malware signatures. While it is highly effective in detecting well-known malware, it is limited in its ability to identify previously unseen or zero-day threats. Heuristic and behavioral analysis, on the other hand, scrutinizes the behavior of programs to pinpoint suspicious activities, such as unauthorized system changes, abnormal network communication, or file modification. Meanwhile, anomaly detection establishes a baseline of normal system behavior and identifies deviations from this baseline, which may indicate the presence of malware.

These detection techniques draw from various data sources, including file-based detection, which scans files and executables on disk, in memory, or during data transfer. Network-based detection involves monitoring network traffic for malicious patterns or known malware signatures, providing an early line of defense against threats entering through network connections. Endpoint Detection and Response (EDR) solutions, a crucial component of modern cybersecurity, offer real-time monitoring, data collection, and analysis of information from endpoints, enabling swift and effective threat detection and response.

Machine learning and artificial intelligence (AI) are increasingly integrated into malware detection and classification. These technologies enhance detection accuracy by training algorithms on vast datasets to recognize patterns indicative of malware. Deep learning models, including Convolutional Neural Networks (CNNs) and recurrent neural networks, are leveraged to analyze large-scale datasets, uncovering subtle and complex relationships within malware samples. By continuously evolving and adapting, these AI-driven approaches contribute to the dynamic landscape of malware defense, helping cybersecurity experts stay ahead of cyber threats and protect digital assets.

**List of Teammates-**

|  |  |  |  |
| --- | --- | --- | --- |
| S.no | Name | Collage | Contact |
| 1 | Pratheek | Amaravati | 9640260262 |
| 2 | Sohan | Amaravati | 8897933704 |
| 3 | Shaz | Bhopal | 7050708271 |
| 4 | Atharva | Bhopal | 9075988349 |

**List of Vulnerability Table-**

**Practice Website**

|  |  |  |
| --- | --- | --- |
| S.no | Vulnerability Name | CWE-No |
| 1 | Invalid Forgot Password Process | CWE-640 |
| 2 | Cross-Site Scripting (Stored) | CWE: 79 |
| 3 | Insecure File Upload | CWE-434 |
| 4 | SQL Injection Vulnerability | CWE-89 |
| 5 | Insecure File Upload | CWE-434 |
| 6 | Broken Session Management | CWE-613 |
| 7 | Cross-Site Request Forgery (CSRF) | CWE-352 |
| 8 | XML External Entity (XXE) Injection | CWE-611 |
| 9 | Security Misconfiguration | CWE-732 |
| 10 | Missing Function-Level Access Control | CWE-284 |
| 11 | Cross-Origin Resource Sharing (CORS) Misconfiguration | CWE-346 |

**Vulnerabilities**

**Invalid Forgot Password Process**

CWE: CWE-640

OWASP Category: A04:2021 – Insecure Design

Description: Architectural flaws can result in security vulnerabilities if appropriate security mitigations are not taken in the design phase of the practice website. Specifically, this vulnerability pertains to the "Forgot Password" process, which may have security weaknesses due to design flaws.

Business Impact: Insecure design of the "Forgot Password" process can make the practice website susceptible to a range of weaknesses. This documentation section addresses the potential impacts and suggests mitigation strategies to improve the security of this process.

Vulnerability Path

URL: <http://yourpracticewebsite.com/forgot_password>

Vulnerability Parameter: <http://yourpracticewebsite.com/forgot_password>

Steps to Reproduce:

Access the URL: <http://yourpracticewebsite.com/forgot_password>

Navigate to the login page.

Enter a random password for testing.

Observe the auto-generated password below the "Forgot Password" section.

Recommendation:

Establish and use a library of secure mechanisms.

Implement a strong validation process to enhance the security of the "Forgot Password" feature.

**Cross-Site Scripting (Stored)**

CWE: 79

OWASP Category: A03:2021 – Injections

Description: Cross-Site Scripting (Stored) occurs when a malicious script is injected directly into the practice website. This vulnerability pertains to the storage and subsequent reflection of a malicious script in the web application, particularly within user-generated content.

Business Impact: Storing dangerous data, such as malicious scripts, in a database can have severe security implications. If executed, these scripts can potentially compromise user data and the overall integrity of the practice website.

Vulnerability Path

URL: <http://yourpracticewebsite.com/admin/user.php>

Vulnerability Parameter: <http://yourpracticewebsite.com/admin/user.php>

Steps to Reproduce:

Access the URL: <http://yourpracticewebsite.com/admin/user.php>

Log in with your credentials.

Attempt to register as a new user.

In the registration form, insert a malicious script within the contact box.

Observe the effects of the injected script.

**Insecure File Upload**

CWE: CWE-434

OWASP Category: A8:2017 – Insecure Deserialization

Description: Insecure file upload allows users to upload potentially malicious files, which can lead to remote code execution and other security threats.

Business Impact: Insecure file uploads can result in the execution of malicious code on the server, leading to unauthorized access and data breaches.

Vulnerability Path

URL: <http://yourpracticewebsite.com/upload>

Vulnerability Parameter: <http://yourpracticewebsite.com/upload>

Steps to Reproduce:

Access the file upload feature.

Attempt to upload a file containing executable code.

Observe if the website allows and executes the file.

**SQL Injection Vulnerability**

CWE: CWE-89

OWASP Category: A1:2017 – Injection

Description: SQL Injection is a type of security vulnerability that occurs when an attacker can manipulate an SQL query in a web application, potentially allowing unauthorized access to databases and data manipulation.

Business Impact: SQL Injection can lead to unauthorized access to sensitive data, data manipulation, and in some cases, complete control over the application's database.

Vulnerability Path

URL: <http://yourpracticewebsite.com/search>

Vulnerability Parameter: <http://yourpracticewebsite.com/search?q=>

Steps to Reproduce:

Access the search functionality on the website.

In the search bar, enter a malicious SQL query.

Observe if the website handles the query securely.

**Insecure File Upload**

CWE: CWE-434

OWASP Category: A8:2017 – Insecure Deserialization

Description: Insecure file upload allows users to upload potentially malicious files, which can lead to remote code execution and other security threats.

Business Impact: Insecure file uploads can result in the execution of malicious code on the server, leading to unauthorized access and data breaches.

Vulnerability Path

URL: <http://yourpracticewebsite.com/upload>

Vulnerability Parameter: <http://yourpracticewebsite.com/upload>

Steps to Reproduce:

Access the file upload feature.

Attempt to upload a file containing executable code.

Observe if the website allows and executes the file.

**Broken Session Management**

CWE: CWE-613

OWASP Category: A2:2017 – Broken Authentication

Description: Broken session management vulnerabilities can allow attackers to hijack sessions, impersonate users, and gain unauthorized access to sensitive data.

Business Impact: Broken session management can lead to unauthorized access, data breaches, and identity theft.

Vulnerability Path

URL: <http://yourpracticewebsite.com/profile>

Vulnerability Parameter: <http://yourpracticewebsite.com/profile>

Steps to Reproduce:

Log in to your user account.

Access the user profile.

Log out.

Attempt to access the profile again without logging in.

**Cross-Site Request Forgery (CSRF)**

CWE: CWE-352

OWASP Category: A8:2017 – Cross-Site Request Forgery (CSRF)

Description: CSRF is an attack that tricks the user into executing unwanted actions on a different website where they are authenticated.

Business Impact: CSRF attacks can lead to unauthorized actions being taken on behalf of the user, potentially compromising their account or data.

Vulnerability Path

URL: <http://yourpracticewebsite.com/change_password>

Vulnerability Parameter: <http://yourpracticewebsite.com/change_password>

Steps to Reproduce:

Log in to your user account.

Visit a malicious website that contains a CSRF attack.

Observe if unauthorized actions are taken on the practice website.

**XML External Entity (XXE) Injection**

CWE: CWE-611

OWASP Category: A4:2017 – XML External Entity (XXE) Processing

Description: XXE vulnerabilities occur when an application processes XML input from untrusted sources, potentially leading to disclosure of internal files, denial of service, and remote code execution.

Business Impact: XXE vulnerabilities can expose sensitive information, disrupt services, and lead to data breaches.

Vulnerability Path

URL: <http://yourpracticewebsite.com/parse-xml>

Vulnerability Parameter: <http://yourpracticewebsite.com/parse-xml?xml=>

Steps to Reproduce:

Access the XML parsing feature on the website.

Submit an XML file with a malicious external entity definition.

Observe if the website processes the XML insecurely.

**Security Misconfiguration**

CWE: CWE-732

OWASP Category: A6:2017 – Security Misconfiguration

Description: Security misconfigurations occur when an application is not securely configured, leading to vulnerabilities such as unauthorized access, data exposure, and other security risks.

Business Impact: Security misconfigurations can result in data breaches, unauthorized access, and financial costs.

Vulnerability Path

URL: <http://yourpracticewebsite.com/admin>

Vulnerability Parameter: <http://yourpracticewebsite.com/admin>

Steps to Reproduce:

Access the admin section of the website.

Observe if there are security misconfigurations that allow unauthorized access.

**Missing Function-Level Access Control**

CWE: CWE-284

OWASP Category: A5:2017 – Broken Access Control

Description: Missing function-level access control vulnerabilities occur when an application does not properly check whether a user has access to certain functions or actions.

Business Impact: This can lead to unauthorized access and the execution of restricted functions.

Vulnerability Path

URL: <http://yourpracticewebsite.com/change-email>

Vulnerability Parameter: <http://yourpracticewebsite.com/change-email>

Steps to Reproduce:

Log in as a regular user.

Access a privileged function, such as changing another user's email.

Observe if the website enforces proper access control.

**Cross-Origin Resource Sharing (CORS) Misconfiguration**

CWE: CWE-346

OWASP Category: A7:2017 – Cross-Site Scripting (XSS)

Description: CORS misconfigurations can allow unauthorized websites to make requests to your site on behalf of a user, potentially exposing sensitive data.

Business Impact: CORS misconfigurations can lead to data exposure, unauthorized access, and privacy violations.

Vulnerability Path

URL: <http://yourpracticewebsite.com/api>

Vulnerability Parameter: <http://yourpracticewebsite.com/api>

Steps to Reproduce:

Access the website's API.

Observe if there are misconfigured CORS settings that allow cross-origin requests.

**List of Vulnerability Table-**

**Main Website**

|  |  |  |
| --- | --- | --- |
| S.no | Vulnerability Name | CWE-No |
| 1 | Unquoted Search Path or Element | CWE-428 |
| 2 | Out-of-bounds Write | CWE-787 |
| 3 | Improper Authentication | CWE-287 |
| 4 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CWE-78 |
| 5 | Observable Discrepancy | CWE-203 |
| 6 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-22 |
| 7 | Inappropriate Encoding for Output Context | CWE-838 |
| 8 | Incorrect Authorization | CWE-863 |
| 9 | Exposure of Sensitive Information to an Unauthorized Actor | CWE-200 |
| 10 | Incorrect Permission Assignment for Critical Resource | CWE-732 |

**Vulnerability Name**: Unquoted Search Path or Element

**CWE:** CWE-428

**OWASP Category**: A1: Injection

**Description:** The product uses a search path that contains an unquoted element, in which the element contains whitespace or other separators. This can cause the product to access resources in a parent path.

**Business impact:** CWE-428, the "Unquoted Search Path or Element" vulnerability, can result in serious business impacts:

Security Risks: It opens the door to security breaches and unauthorized access.

Operational Disruption: Exploitation can lead to downtime and loss of productivity.

Legal and Compliance Issues: Non-compliance may result in legal penalties and regulatory fines.

Reputation Damage: Trust and reputation can be severely damaged.

Financial Costs: Remediation and recovery can be costly.

**Vulnerability Name:** Out-of-bounds Write

**CWE:** CWE-787

**OWASP Category:** A7: Security Misconfiguration

**Description:** The product writes data past the end, or before the beginning, of the intended buffer. Typically, this can result in corruption of data, a crash, or code execution. The product may modify an index or perform pointer arithmetic that references a memory location outside of the buffer's boundaries. A subsequent write operation then produces undefined or unexpected results.

**Business impact:** CWE-787, "Out-of-bounds Write," can have significant business impacts, including:

1. Security Breaches: Exploiting this vulnerability can lead to unauthorized data manipulation, system crashes, or even remote code execution, potentially compromising sensitive information.

2. Loss of Customer Trust: Security incidents resulting from CWE-787 can erode trust and damage a company's reputation, leading to customer loss.

3. Operational Disruption: Addressing and recovering from security breaches can cause downtime and productivity loss, impacting business operations.

4. Legal and Compliance Issues: Non-compliance with data protection regulations may result in legal penalties and regulatory fines.

5. Financial Costs: Remediation and recovery can be costly, including expenses for forensics, legal, and reputation management.

6. Competitive Disadvantage: Businesses with a history of security vulnerabilities may lose customers to more secure competitors.

**Vulnerability Name:** Improper Authentication

**CWE:** CWE-287

**OWASP Category:** A2: Broken Authentication

**Description:** When an actor claims to have a given identity, the payments were indeed made, however.

**Business impact:**

CWE-287, "Improper Authentication," can have several significant business impacts when not properly addressed:

Unauthorized Access: Improper authentication can lead to unauthorized individuals gaining access to sensitive systems or data, potentially resulting in data breaches, theft, or unauthorized actions.

Data Breaches: If attackers exploit authentication weaknesses, they can gain access to sensitive customer or business data, leading to costly data breaches, legal consequences, and damage to a company's reputation.

Loss of Trust: Security incidents involving improper authentication erode trust in a business or service. Customers, partners, and stakeholders may lose confidence in the organization's ability to protect their information.

Legal and Regulatory Consequences: Non-compliance with data protection and privacy regulations can result in fines, legal actions, and other regulatory penalties, further impacting the company's financial health.

Operational Disruption: Remediation efforts, including resetting user accounts or implementing stronger authentication mechanisms, can cause operational disruptions and productivity loss.

**Vulnerability Name:** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

**CWE:** CWE-78

**OWASP Category:** A1: Injection

**Description:** The product constructs all or part of an OS command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.

**Business impact:** CWE-78, which relates to "OS Command Injection," can have several significant business impacts when not properly mitigated:

Unauthorized Access: Command injection vulnerabilities can allow attackers to execute arbitrary commands on a system, potentially leading to unauthorized access and data breaches.

Data Loss or Manipulation: Attackers exploiting this vulnerability may manipulate data, delete critical information, or even compromise the integrity of the system, resulting in data loss and operational disruptions.

Loss of Trust: Security incidents involving OS command injection erode trust in a business or service. Customers, partners, and stakeholders may lose confidence in the organization's ability to protect their information.

Legal and Regulatory Consequences: Non-compliance with data protection and privacy regulations can result in fines, legal actions, and other regulatory penalties, further impacting the company's financial health.

Operational Disruption: Remediation efforts and recovery from a successful attack can cause operational disruptions, resulting in productivity loss.

**Vulnerability Name:** Observable Discrepancy

**CWE:** CWE-203

**OWASP Category:** Observable Differences Based on Input

**Description:** The product behaves differently or sends different responses under different circumstances in a way that is observable to an unauthorized actor, which exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not.

Discrepancies can take many forms, and variations may be detectable in timing, control flow, communications such as replies or requests, or general behavior. These discrepancies can reveal information about the product's operation or internal state to an unauthorized actor. In some cases, discrepancies can be used by attackers to form a side channel.

**Business impact:** CWE-203, "Observable Differences Based on Input," is a type of information leakage vulnerability. While this CWE may not be as well-known as some other common vulnerabilities, it can still have business impacts:

Data Exposure: Observable differences based on input can inadvertently reveal sensitive information, such as internal data structures, error messages, or system behavior. This exposure can provide valuable information to attackers.

Security Risk: The information leakage can be used by malicious actors to plan and execute targeted attacks. It may help attackers understand the inner workings of a system, identify weaknesses, and devise a more effective attack strategy.

Loss of Competitive Advantage: If proprietary information or unique data structures are exposed, it can undermine a company's competitive advantage, potentially leading to imitations by competitors.

Regulatory Non-Compliance: Depending on the type of data exposed, CWE-203 may result in non-compliance with data protection regulations and privacy laws. Non-compliance can lead to legal penalties and damage an organization's reputation.

**Vulnerability Name:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**CWE:** CWE-22

**OWASP Category:** A4: XML External Entities (XXE)

**Description:** The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

**Business impact:** CWE-22, "Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)," can have several significant business impacts when not properly mitigated:

Data Exposure: Path traversal vulnerabilities can allow attackers to access and retrieve sensitive files or data from the server. This exposure can lead to data breaches and unauthorized access to confidential information.

Loss of Confidentiality: If sensitive data, such as customer records, intellectual property, or financial information, is exposed, it can result in a loss of confidentiality and legal consequences.

Regulatory Non-Compliance: Depending on the type of data exposed, CWE-22 may lead to non-compliance with data protection regulations and privacy laws, resulting in legal penalties and damage to the company's reputation.

Operational Disruption: Remediation efforts, including securing the application and investigating the breach, can disrupt business operations and lead to productivity loss.

Reputation Damage: Data breaches and improper handling of sensitive information can damage an organization's reputation, causing customers and partners to lose trust in the company's ability to protect their data.

Financial Costs: Remediation, legal, and public relations costs associated with path traversal vulnerabilities can be substantial, affecting the company's bottom line.

**Vulnerability Name:** Inappropriate Encoding for Output Context

**CWE:** CWE-838

**OWASP Category:** Security Misconfiguration

**Description:** The product uses or specifies an encoding when generating output to a downstream component, but the specified encoding is different from the encoding that is expected by the downstream component.

**Business impact:** CWE-838, "Inappropriate Access of Resource Through Identifying Information," typically occurs when an application improperly handles sensitive data, leading to business risks and impacts:

Data Exposure: Inappropriate access can result in unauthorized parties gaining access to sensitive data, including customer records, financial information, or intellectual property.

Loss of Confidentiality: The exposure of sensitive data may lead to a loss of confidentiality, resulting in legal consequences and damage to the company's reputation.

Regulatory Non-Compliance: If unauthorized access violates data protection or privacy regulations, it can result in legal penalties, regulatory fines, and additional damage to the organization's reputation.

Operational Disruption: Efforts to secure the application and investigate the breach can disrupt business operations, causing productivity loss.

Reputation Damage: Data breaches and improper handling of sensitive information can damage the organization's reputation, eroding trust in its ability to protect data.

**Vulnerability Name:** Incorrect Authorization

**CWE:** CWE-863

**OWASP Category:** Access Control

**Description:** The product uses or specifies an encoding when generating output to a downstream component, but the specified encoding is different from the encoding that is expected by the downstream component.

**Business impact:**

CWE-863, "Incorrect Authorization," can lead to unauthorized access, data breaches, legal consequences, operational disruptions, reputation damage, financial costs, and a competitive disadvantage. Improper authorization can result in data exposure, privacy violations, regulatory non-compliance, and eroded trust, impacting the company's integrity and success.

**Vulnerability Name:** Exposure of Sensitive Information to an Unauthorized Actor

**CWE:** CWE-200

**OWASP Category:** Sensitive Data Exposure

**Description: The product exposes sensitive information to an actor not explicitly authorized to have access to it.**

**Business impact:**

CWE-200, "Exposure of Sensitive Information to an Unauthorized Actor," can have severe business impacts when not properly mitigated:

Data Breaches: The exposure of sensitive information can lead to data breaches, resulting in unauthorized access to confidential data, including customer records and financial information.

Loss of Trust: Security incidents involving sensitive data exposure erode trust in a business or service. Customers, partners, and stakeholders may lose confidence in the organization's ability to protect their information.

Legal and Regulatory Consequences: Non-compliance with data protection regulations can result in fines, legal actions, and other regulatory penalties, further impacting the company's financial health.

Reputation Damage: Data breaches and the mishandling of sensitive information can damage the organization's reputation, causing customers and partners to lose trust.

**Vulnerability Name:** Incorrect Permission Assignment for Critical Resource

**CWE:** CWE-732

**OWASP Category:** Security Misconfiguration

**Description:** The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

When a resource is given a permission setting that provides access to a wider range of actors than required, it could lead to the exposure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution, or sensitive user data. For example, consider a misconfigured storage account for the cloud that can be read or written by a public or anonymous user.

**Business impact:**

CWE-732, "Insecure Permission Assignment for Critical Resource," can have significant business impacts, including unauthorized access to critical resources, data breaches, operational disruption, legal consequences, financial costs, reputation damage, and competitive disadvantages. Failing to secure access to critical resources can lead to data exposure, regulatory fines, trust erosion, and loss of business opportunities, negatively affecting the organization's integrity and success.

**Stage 2**

**Overview: -**

**Nessus Overview**

Nessus is a widely acclaimed and robust vulnerability assessment and management tool that plays a pivotal role in maintaining the security and integrity of computer networks. Developed by Tenable, Nessus has become an indispensable asset for organizations and security professionals seeking to proactively identify and address vulnerabilities in their IT environments.

At its core, Nessus is designed to detect and assess weaknesses within networks, applications, and infrastructure. It accomplishes this through a comprehensive and systematic scanning process, which entails examining hosts, servers, and devices for known and potential security issues. Nessus employs a combination of active and passive scanning techniques, making it versatile and adaptable to various network configurations.

One of the standout features of Nessus is its extensive vulnerability database. It maintains an expansive and up-to-date repository of known vulnerabilities, which it leverages during scans to compare and evaluate the configuration and security posture of the scanned systems. This database includes information on software flaws, misconfigurations, and potential threats, allowing users to stay ahead of emerging cyber threats.

Nessus offers a user-friendly and highly customizable interface, making it accessible to both novice and experienced security professionals. It provides flexibility in defining scan policies, enabling users to tailor their scans to specific needs, compliance requirements, or industry standards. The tool's scanning capabilities encompass a wide range of systems and services, including web applications, databases, cloud resources, and network devices.

In addition to its vulnerability detection capabilities, Nessus is equipped with advanced reporting features. It generates comprehensive reports that detail identified vulnerabilities, their severity, and recommended mitigation steps. These reports are essential for helping organizations prioritize and address vulnerabilities in a structured and systematic manner.

Nessus further supports integrations with various security information and event management (SIEM) solutions, workflow and ticketing systems, streamlining the vulnerability remediation process. This integration capability ensures that detected vulnerabilities are efficiently communicated to the appropriate teams for mitigation and resolution.

Furthermore, Nessus is frequently used in compliance and audit scenarios, helping organizations adhere to industry-specific regulations and standards like PCI DSS, HIPAA, and NIST (National Institute of Standards and Technology). Its ability to automate compliance checks simplifies the process of ensuring that systems and networks meet the required security benchmarks.

In summary, Nessus is a powerful, flexible, and indispensable tool for identifying and managing vulnerabilities in complex network environments. It aids organizations in maintaining a proactive approach to cybersecurity, allowing them to remediate vulnerabilities before they can be exploited by malicious actors. With its extensive vulnerability database, user-friendly interface, and reporting capabilities, Nessus remains a cornerstone of modern cybersecurity efforts, contributing significantly to the ongoing battle against cyber threats and ensuring the integrity and security of digital assets.

**Target website: -** <http://testfire.net/>

**Target IP (Instruction Pointer) address: -** 65.61.137.117

**List of Vulnerability-**

|  |  |  |  |
| --- | --- | --- | --- |
| S.no | Vulnerabiliy name | Severity | Plugins |
| 1 | HSTS (HTTP Strict Transport Security) Missing from HTTPS Server (RFC 6797) | MEDIUM | 142960` |
| 2 | TLS Version 1.0 Protocol Detection | MEDIUM | 104743 |
| 3 | TLS Version 1.1 Protocol Detection | MEDIUM | 157288 |
| 4 | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) | LOW | 83875 |
| 5 | ICMP Timestamp Request Remote Date Disclosure | INFO | 10114 |
| 6 | Additional DNS Hostnames | INFO | 46180 |
| 7 | Apache Tomcat Detection | INFO | 39446 |
| 8 | Common Platform Enumeration (CPE) | INFO | 45590 |
| 9 | HSTS Missing from HTTPS Server | INFO | 84502 |
| 10 | Hypertext Transfer Protocol (HTTP) Information | INFO | 24260 |

**REPORT**

**Vulnerability name-** HSTS Missing from HTTPS Server (RFC 6797)

**Severity-** MEDIUM

**Plugin-** 142960

**Description-** The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks and weakens cookie-hijacking protections.

**Solution-** Configure the remote web server to use HSTS.

**Business Impact-** The absence of HTTP Strict Transport Security (HSTS) from an HTTPS server can have significant business impacts. It exposes the organization to security vulnerabilities, increasing the risk of data breaches and financial losses. Without HSTS, the server is more susceptible to Man-in-the-Middle attacks, compromising data integrity. This can lead to reputational damage and loss of customer trust. Legal and compliance issues may arise due to inadequate security measures. Implementing HSTS is crucial to ensure secure communications and protect sensitive data, safeguarding the organization's reputation and financial stability.

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

**Severity-** MEDIUM

**Plugin-** 104743

**Description-**

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

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

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

**Solution-** Enable support for TLS 1.2 and 1.3 and disable support for TLS 1.0.

**Business Impact-**

Detecting TLS version 1.0 protocol usage is vital due to its security vulnerabilities. Its deprecated status poses a significant security risk, potentially leading to data breaches and regulatory non-compliance. Failure to detect and mitigate TLS 1.0 usage can result in legal and financial liabilities, reputational damage, and loss of customer trust. It is imperative for businesses to proactively identify and replace TLS 1.0 with more secure versions to maintain data security and compliance.

**Vulnerability name-** TLS Version 1.1 Protocol Detection

**Severity-** MEDIUM

**Plugin-** 157288

**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 1.1

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

**Solution-** Enable support for TLS 1.2 and/or 1.3 and disable support for TLS 1.1.

**Business Impact-**

Detecting TLS version 1.1 protocol usage is essential for maintaining cybersecurity. While more secure than TLS 1.0, it still poses security risks and is considered outdated. Detecting its usage allows organizations to assess and upgrade their security protocols, avoiding potential vulnerabilities and ensuring regulatory compliance. Failing to detect TLS 1.1 can result in security breaches, legal issues, and damage to an organization's reputation, impacting customer trust and business operations. Proactive detection and replacement of TLS 1.1 with more secure versions are critical for data protection and security.

**Vulnerability name-** SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

**Severity-** LOW

**Plugin-** 83875

**Description-** The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

**Solution-** Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

**Business Impact-**

1. Security Risk: Detection of Logjam is imperative, as it represents a significant security risk. Weak Diffie-Hellman key exchange can be exploited by malicious actors, potentially leading to data compromise and unauthorized access.
2. Regulatory Compliance: Detecting and mitigating Logjam is essential for compliance with data protection regulations like GDPR, HIPAA, and PCI DSS, which mandate robust encryption standards. Non-compliance can result in legal repercussions and fines.
3. Data Breach Liability: The presence of Logjam increases the organization's vulnerability to data breaches, incurring legal, financial, and reputational consequences. Detection is vital to minimize this risk.
4. Reputation Damage: Security incidents stemming from Logjam can severely damage the organization's reputation, eroding customer trust and confidence in the brand.
5. Operational Disruption: Security breaches can disrupt business operations, affecting productivity and revenue, making detection and mitigation of Logjam crucial for business continuity.
6. Competitive Advantage: Proactive detection and mitigation of vulnerabilities like Logjam can provide a competitive edge, demonstrating a commitment to robust security practices that attract security-conscious customers.

**Vulnerability name-** ICMP Timestamp Request Remote Date Disclosure

**Severity-** INFO

**Plugin-** 10114

**Description-** The remote host answers an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may aid 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 (about 16 and a half minutes) of the actual system time.

**Solution-** Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

**Business Impact-**

1. Information Exposure: This vulnerability can allow malicious actors to obtain the target system's current date and time through ICMP timestamp requests, potentially revealing sensitive information.
2. Synchronization Attacks: With this information, attackers may synchronize their malicious activities with the system's time, increasing the likelihood of successful attacks.
3. Regulatory Compliance: Depending on the industry, exposing system time information may lead to non-compliance with data protection regulations, potentially resulting in legal consequences and fines.
4. Data Manipulation: Accurate time information is crucial for data integrity and security. Attackers could manipulate data based on the disclosed time, leading to potential data breaches and integrity issues.
5. Reputation Damage: Not detecting and mitigate this vulnerability can harm the organization's reputation, eroding customer trust and confidence in its security practices.

**Vulnerability name-** Additional DNS Hostnames

**Severity-** INFO

**Plugin-** 46180

**Description-** Hostnames different from the current hostnames 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 host names for hosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

**Solution-** If you want to test them, re-scan using the special host syntax, such as

www.example.com [192.0.32.10]

**Business Impact-**

1. Scalability: Adding more DNS hostnames accommodates the growth of online services, products, and applications, enabling the business to scale effectively.
2. Business Continuity: Added hostnames can be used for load balancing and redundancy, ensuring business continuity by distributing traffic across multiple servers or locations.
3. Improved User Experience: Diversifying hostnames can enhance user experience by reducing latency and improving website performance, resulting in higher customer satisfaction and retention.
4. Security: Properly configuring added DNS hostnames is critical for keeping security. Ensuring the security of these host names is essential to protect against potential vulnerabilities and attacks.
5. Global Reach: Expanding DNS hostnames can ease the global reach of the business, serving international customers more effectively by reducing network latency and improving website availability.
6. Marketing and Branding: Additional hostnames can be used for specific marketing campaigns, branding purposes, or creating custom URLs (Uniform Resource Locators), which can boost brand recognition and marketing efforts.

**Vulnerability name-** Apache Tomcat Detection

**Severity-** INFO

**Plugin-** 39446

**Description-** Nessus was able to detect a remote Apache Tomcat web server.

**Business Impact-**

1. System Configuration: Finding Apache Tomcat helps in understanding the web application infrastructure and server setup, aiding in system configuration and management.
2. Security Assessment: Detection enables security professionals to assess and analyze the server for vulnerabilities and misconfigurations, ensuring the server's resilience against cyber threats.
3. Maintenance: Knowing the presence of Apache Tomcat allows for proper maintenance, updates, and patching to ensure the server is used securely and efficiently.
4. Performance Optimization: Detection eases performance monitoring and optimization, ensuring that web applications run smoothly and without delays.
5. Troubleshooting: In case of issues or errors, knowing Apache Tomcat's presence is crucial for troubleshooting and resolving problems related to web applications and server performance.
6. Compliance: Finding and properly configuring Apache Tomcat is often a requirement for compliance with security and data protection standards.
7. Resource Allocation: Detection aids in resource allocation, ensuring that the server has the necessary hardware and software resources to handle web application workloads efficiently.

**Vulnerability name-** Common Platform Enumeration (CPE)

**Severity-** INFO

**Plugin-** 45590

**Description-** By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

**Solution-** If you want to test them, re-scan using the special host syntax, such as:

www.example.com [192.0.32.10]

**Business Impact-**

Common Platform Enumeration (CPE) is a structured and standardized system for naming and describing software and hardware platforms. It plays a crucial role in cybersecurity, asset management, and vulnerability assessment. Here are some key points about CPE:

1. Structured Naming: CPE supplies a structured and uniform way to name and identify hardware, software, and operating systems, making it easier to manage and assess IT assets.
2. Hierarchical Format: CPE uses a hierarchical format, consisting of parts like a vendor, product, and version, enabling detailed and granular descriptions of components.
3. Interoperability: CPE promotes interoperability between different cybersecurity tools and databases, facilitating information sharing and collaboration.
4. Vulnerability Assessment: It is widely used in vulnerability assessment tools and databases to associate vulnerabilities with the affected platforms, aiding in risk analysis and mitigation
5. Asset Management: CPE helps organizations in asset management, allowing them to track and categorize their IT assets more effectively.
6. Standardization: CPE is standardized by NIST (National Institute of Standards and Technology) and maintained as part of the Common Vulnerabilities and Exposures (CVE) system.

**Vulnerability name- HSTS** Missing from HTTPS Server

**Severity-** INFO

**Plugin-** 84502

**Description-** The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks and weakens cookie-hijacking protections.

**Solution-** Configure the remote web server to use HSTS.

he absence of HTTP Strict Transport Security (HSTS) from an HTTPS server can have significant business impacts:

**Business Impact-**

1. Security Vulnerabilities: Without HSTS, the server is vulnerable to downgrade attacks, enabling malicious actors to intercept or manipulate traffic and potentially compromise sensitive data.
2. Data Breach Risk: HSTS helps protect against data breaches by ensuring secure connections, and its absence increases the likelihood of successful attacks leading to financial, legal, and reputational consequences.
3. Compliance Concerns: Various data protection regulations and industry standards, such as GDPR and PCI DSS, recommend or require HSTS implementation. Non-compliance may result in penalties and legal issues.
4. Customer Trust: Security incidents due to missing HSTS can erode customer trust and harm an organization's reputation, potentially leading to loss of business.
5. Operational Disruption: Security breaches can disrupt business operations, affecting productivity and revenue.
6. Competitive Disadvantage: Failing to implement HSTS may put an organization at a competitive disadvantage, as security-conscious customers may seek safer alternatives.

**Vulnerability name-** Hypertext Transfer Protocol (HTTP) Information

**Severity-** INFO

**Plugin-** 24260

**Description-** This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

**Business Impact-**

HTTP, or Hypertext Transfer Protocol, is a fundamental protocol that governs the exchange of data on the World Wide Web. It is crucial for understanding web communications. Here are key points about HTTP:

1. Communication Protocol: HTTP is the foundation of data communication on the web. It allows clients (typically web browsers) to request and retrieve resources from web servers.
2. Stateless: HTTP is a stateless protocol, meaning each request from a client to a server is independent and does not retain information from previous requests.
3. Text-Based: HTTP messages are text-based and human-readable, facilitating easy interpretation and debugging. These messages include requests and responses.
4. Client-Server Model: It follows a client-server model where a client initiates a request for a resource, and the server responds with the requested data.
5. Methods: HTTP requests use methods like GET (retrieve data), POST (send data), PUT (update data), and DELETE (remove data) to specify the action to be performed.
6. Status Codes: HTTP responses include status codes (e.g., 200 for success, 404 for not found, 500 for server errors) to indicate the outcome of the request.
7. URLs: Uniform Resource Locators (URLs) are used to specify the resource's address, allowing clients to locate and access web resources.

**Stage 3**

Title: Exploring the Capabilities of SOC/SEIM

**SOC**

Security Operations Center (SOC) is a centralized unit within an organization that monitors and manages security concerns and incidents. It serves as the hub for detecting, analysing, and responding to security threats in real-time. SOC teams employ various tools and technologies to ensure the safety and security of the organization's digital assets. The SOC plays a crucial role in safeguarding against cyberattacks and minimizing the potential impact of security incidents.

**SOC Cycle**

The SOC operates in a continuous cycle that includes monitoring, detection, analysis, response, and improvement. This cyclical approach allows the SOC to adapt to evolving threats and improve security over time.

**SIEM**

Security Information and Event Management (SIEM) is a comprehensive solution that provides real-time analysis of security alerts generated by various hardware and software systems. SIEM systems collect, and aggregate log data generated throughout the organization's technology infrastructure, analyse it, and provide actionable insights. SIEM tools are instrumental in monitoring security events, managing security incidents, and ensuring compliance with security policies.

**SIEM Cycle**

The SIEM cycle encompasses data collection, normalization, analysis, and reporting. It helps organizations identify anomalies and potential security incidents.

**MISP**

Malware Information Sharing Platform & Threat Sharing (MISP) is an open-source threat intelligence platform that facilitates the sharing of structured threat information. MISP is designed to improve the sharing of structured threat information and indicators of compromise (IOCs), enhancing the overall security posture of organizations.

Our College Network Information

Understanding the structure and layout of our college network is crucial for deploying a SOC. It involves identifying critical assets, network topology, access points, and potential vulnerabilities. This knowledge forms the foundation for an effective security strategy.

How to Deploy SOC in our College

Deploying a SOC in our college entails a comprehensive plan that includes defining roles and responsibilities, selecting the right tools, creating incident response procedures, and establishing key performance indicators (KPIs). This step will require collaboration with stakeholders and a clear understanding of the college's security objectives.

**Threat Intelligence**

Threat intelligence involves collecting, analysing, and disseminating information about potential threats and vulnerabilities. It empowers organizations to proactively defend against cyberattacks by understanding the tactics, techniques, and procedures used by threat actors.

**Incident Response**

Incident response is the process of managing and mitigating the impact of security incidents. It involves preparation, identification, containment, eradication, recovery, and lessons learned to ensure the organization is better prepared for future incidents.

**Qadar & Understanding About the Tool**

IBM Qadar is a leading SIEM solution that assists organizations in detecting and responding to security threats. Understanding its capabilities, features, and the process of configuring and managing Qadar is essential for effective security monitoring.

**Conclusion**

Stage 1: In the previous stages, we gained insights into web application testing, learning to identify vulnerabilities and risks within web applications.

Stage 2: We explored Nessus, a valuable vulnerability assessment tool, and analysed its capabilities in identifying vulnerabilities within our network.

Stage 3: In this stage, we delved into the world of SOC, SIEM, and Qadar Dashboards. We gained an understanding of the critical role these elements play in securing our organization's digital assets.

Future Scope

Stage 1: The future scope of web application testing includes further enhancing our skills, staying updated with emerging threats, and exploring advanced testing techniques.

Stage 2: Our understanding of the testing process will continue to evolve as we delve deeper into vulnerability assessment tools and their applications.

Stage 3: For SOC/SEIM, the future scope involves implementation within our college, continuous improvement of our security strategy, and ongoing training for SOC teams.

Topics Explored

**SOC**: Explored the concept and significance of a Security Operations Center.

**SOC Cycle**: Learned about the continuous cycle of SOC operations.

**SIEM**: Explored the critical role of Security Information and Event Management.

**SIEM Cycle**: Discussed the phases involved in a SIEM cycle.

**MISP**: Discovered the value of the Malware Information Sharing Platform.

**Our College Network Information**: Gained insights into understanding the structure of our college network.

**How to Deploy SOC in our College**: Explored the steps to deploy a SOC within the college environment.

**Threat Intelligence**: Learned about collecting and using threat intelligence for proactive security.

**Incident Response**: Explored the incident response process.

Qadar & Understanding About the Tool: Gained understanding of IBM Qadar and its significance in security operations.

**SOLUTION**

Malware, short for malicious software, is like digital troublemakers that can harm your computer and steal your information. Protecting your digital world from these threats is essential. Here is a straightforward guide to understanding how we find and stop malware.

**1. Antivirus Software**

Think of antivirus software as your computer's guardian. It checks your files and programs to see if they are on a list of known serious stuff. If it finds something harmful, it tries to remove it, keeping your computer safe.

**2. Learning from New Tricks**

Sometimes, troublemakers produce new tricks that the antivirus software does not know about. That is where the smart software comes in. It learns from the serious stuff it sees and can catch new troublemakers based on what it has learned.

**3. Watching Behavior**

Imagine having a guard who watches what everyone does in your neighborhood. If someone starts acting strange or doing something suspicious, the guard steps in. In the digital world, we have similar guards that watch what software is doing. If it acts weird, they catch it.

**4. Keeping an Eye on the Digital Roads**

Your computer is connected to the internet through digital roads. We also have guards watching these roads. If they see strange traffic, like a truck carrying something fishy, they stop it before it can cause any harm.

**5. Being Smart**

The best way to stay safe is by learning from experts. They teach us about the latest troublemakers and how to avoid them. We also teach others to be careful and avoid risky things online.

**6. Stay Updated**

Just like you need to keep your house in decent shape, your computer's software needs to stay updated. Updates help fix any weak points that troublemakers might use to get in.

**7. Be Ready**

Imagine if a burglar tried to break into your home. You would call the police and keep yourself safe. In the digital world, we have plans too. If something bad happens, we quickly isolate and fix the problem.

**8. Never Stop Watching**

We do not stop protecting our digital world. We keep an eye out for new troublemakers and make sure our computers stay safe.

In summary, keeping your digital world safe from malware is like having a digital guardian. Antivirus software, learning, behavior watching, monitoring digital roads, being smart, staying updated, being ready, and never stopping to watch are all part of this guardian's job. By following these simple steps, you can help keep your computer and data safe from troublemakers. Remember, it is important to stay informed and cautious in the digital world. Just like you look both ways before crossing the street, it is wise to be careful online.