Project Title: **AI enhanced Intrusion Detection System**

Overview:-

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

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

• Address Spoofing

• Fragmentation

• Pattern Evasion

• Coordinated attack

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

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

**List of teammates–**

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

**List of Vulnerability Table**

|  |  |  |
| --- | --- | --- |
| S.no | Vulnerability Name | CWE - No |
| **1** | ICMP Timestamp Request Remote Date Disclosure | **200** |
| **2** | OS Identification | **78** |
| **3** | Device Type | **200** |
| **4** | Web Application Potentially Vulnerable to Clickjacking | **693** |
| **5** | Web Server Transmits Cleartext Credentials | **522,523,718** |
| **6** | Web Application Cookies Not Marked Secure | [**522**](http://cwe.mitre.org/data/definitions/522)**,**[**718**](http://cwe.mitre.org/data/definitions/718)**,**[**724**](http://cwe.mitre.org/data/definitions/724)**,**[**928**](http://cwe.mitre.org/data/definitions/928)**,**[**930**](http://cwe.mitre.org/data/definitions/930) |
| **7** | CGI Generic Injectable Parameter | **86** |
| **8** | SQL Injection Vulnerability | **89** |
| **9** | Displaying internal server error from tomcat | **502** |
| **10** | Cross site Scripting XSS | **79** |
| **11** | Insecure Direct Object Reference | **639** |
| **12** | Security Misconfiguration | **16** |
| **13** | HTTP Server type and Version | **444** |
| **14** | Traceroute Infromation | **293** |
| **15** | Additional DNS Hostnames | **350** |
| **16** | HTTP/2 Cleartext Detection(main start) | **319** |
| **17** | OS Identification | **78** |
| **18** | Inconsistent Hostname and IP Address | **350** |
| **19** | SSL Certificate 'commonName' Mismatch | **297** |
| **20** | SSL Certificate Signed Using Weak Hashing Algorithm | **328** |
| **21** | Apache Tomcat Detection - Remote Code Execution | **94** |
| **22** | Apache Tomcat Detection - Request Smuggling Vulnerability | **444** |
| **23** | Apache Tomcat Detection - Privilege Escalation Vulnerability | **269** |
| **24** | Web Server No 404 Error Code Check | **404** |
| **25** | Insecure cookie setting: missing HttpOnly flag | **1004** |
| **26** | Missing security header: X-Content-Type-Options | **16** |
| **27** | Unsafe security header: Content-Security-Policy | **693** |
| **28** | Missing security header: Referrer-Policy | **200** |
| **29** | SQL Injection Vulnerability | **89** |
| **30** | CGI Generic XSS | **74,20,79** |

**Report:**

**ICMP Timestamp Request Remote Date Disclosure**

**CWE:** - 200

**OWASP Category:-** Broken Access Control

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

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

**OS Identification**

**CWE:** - 78

**OWASP Category:-** Software and Data Integrity Failures

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

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

**Device Type**

**CWE:** - 200

**OWASP Category: -** Information Exposure

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

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

**Web Application Potentially Vulnerable to Clickjacking**

**CWE:** - 693

**OWASP Category: -** Security Misconfiguration

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

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

**Web Server Transmits Cleartext Credentials**

**CWE:** - 522,523,718

**OWASP Category: -** Sensitive Data Exposure

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

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

**Web Application Cookies Not Marked Secure**

**CWE:** - 522,718,724,928

**OWASP Category: -** Insufficient Transport Layer Protection

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

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

**CGI Generic Injectable Parameter**

**CWE:** - 86

**OWASP Category: -** Injection

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

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

**SQL Injection Vulnerability (for login bypass)**

**CWE:** - 89

**OWASP Category:-** Injection

**Vulnerability Level:** High

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

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

**Displaying internal server error from tomcat**

**CWE:** - 502

**OWASP Category:-** Injection

**Vulnerability Level:** High

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

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

**Cross site Scripting XSS**

**CWE:** - 79

**OWASP Category:-** Injection

**Vulnerability Level:** Moderate

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

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

**Insecure Direct Object Reference**

**CWE:** 639.

**OWASP Category: -** Broken Access Control

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

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

**Security Misconfiguration**

**CWE :** 16

**OWASP Category: -** Security Misconfiguration

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

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

**HTTP Server type and Version**

**CWE**: 444

**OWASP Category: -** Security Misconfiguration

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

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

**Traceroute Information**

**CWE**: 293

**OWASP Category: -** Security Misconfiguration

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

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

**Additional DNS Hostnames**

**CWE**: 350

**OWASP Category: -** security

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

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

**HTTP/2 Cleartext Detection**

**CWE**: 319

**OWASP Category: -** web application

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

**Solution:** Limit incoming traffic to this port if desired.

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

**OS Identification**

**CWE**: 78

**OWASP Category: -** Software and Data Integrity Failures

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

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

**Inconsistent Hostname and IP Address**

**CWE**: 350

**OWASP Category: -** Security Misconfiguration

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

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

**Solution**:

Protect your target with an IP filter.

**Business Impact:**

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

**SSL Certificate 'commonName' Mismatch**

**CWE**: 350

**OWASP Category: -** Transport Layer Protection

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

**Solution**:

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

**Business Impact:**

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

**SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)**

**CWE**: 328

**OWASP Category: -** Cryptographic Failures

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

**Business Impact:**

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

#### Apache Tomcat Detection - Remote Code Execution

**CWE**:94

**OWASP Category: -** Injection

##### **Description**

Nessus was able to detect a remote Apache Tomcat web server. The installed Tomcat version is 9.0.20. The version of Tomcat installed on the remote host is prior to 9.0.35. It is, therefore, affected by a remote code execution vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.35\_security-9 advisory. An arbitrary file read vulnerability exists in Tomcat's Apache JServ Protocol (AJP) due to an implementation defect. A remote, unauthenticated attacker could exploit this to access files which, under normal conditions, would be restricted. If the Tomcat instance supports file uploads, the vulnerability could also be leveraged to achieve remote code execution. (CVE-2020-1938)

**Business Impact:**

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

#### Apache Tomcat Detection - Request Smuggling Vulnerability

**CWE:** 444

**OWASP Category: -** Injection

##### **Description**

The version of Tomcat installed on the remote host is 9.0.0-M1 or later but prior to 9.0.68. It is, therefore, affected by a request smuggling vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.68\_security-9 advisory. If Tomcat was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (not the default), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

**Business Impact:**

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

#### Apache Tomcat Detection - Privilege Escalation Vulnerability

**CWE**:269

**OWASP Category**: - Injection

##### **Description**

The version of Tomcat installed on the remote host is prior to 9.0.30. It is, therefore, affected by a privilege escalation vulnerability as referenced in the 'Fixed in Apache Tomcat 9.0.30' advisory.  
  
- When using FORM authentication there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563)

**Business Impact:**

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

**Web Server No 404 Error Code Check**

**CWE**: 404

**OWASP Category: -** Security Misconfiguration

**Description**

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

**Business Impact:**

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

**Insecure cookie setting: missing HttpOnly flag**

**CSE:** 1004

**OWASP Category: -**

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

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

**Missing security header: X-Content-Type-Options**

**CSE:** 16

**OWASP Category: -** Broken Authentication

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

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

**Unsafe security header: Content-Security-Policy**

**CSE:** 693

**OWASP Category: -** Security Misconfiguration

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

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

**Missing security header: Referrer-Policy**

**CSE:** 200

**OWASP Category: -** Security Misconfiguration

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

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

**SQL Injection Vulnerability**

**CWE:** - 89

**OWASP Category: -** Injection

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

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

**CGI Generic XSS**

**CWE:** - 20,79,74

**OWASP Category: -** Injection

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

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