**Next-Gen Threat Intelligence Hub: Unveiling Dynamic Security Insights in Real Time**

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **S.No** | **Topic** | **Page No** |
| 1. | Project details, Team details | 2 |
| 2. | Abstract | 3 - 4 |
| 3. | Introduction | 5 - 10 |
| 4. | Vulnerability Assessment Reports | 11 - 19 |
| 5. | All about Nessus | 20 - 27 |
| 6. | Understanding SoC, SIEM and Qradar. | 28 - 33 |
| 7. | Conclusion | 34 - 35 |
| 8. | Future Scope | 35 - 36 |

# Project details:

**Project title:** Next-Gen Threat Intelligence Hub: Unveiling Dynamic Security Insights In Real Time.

## Phases involved in the Project:

* Ideation Phase
* Project Design Phase
* Project Planning Phase
* Project Development Phase
* Performance and Final Submission Phase

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Name** | **College** | **Contact** |
| 1 | Mrs. Ganga Sakkarai | Prince Shri Venkateshwara Padmavathy Engineering College, Chennai-127. | 9094526005 |

**Team Details**

**Abstract**

In the realm of evolving web technologies, the intricate nature of online systems underscores the critical importance of pinpointing and addressing vulnerabilities within web servers. This undertaking introduces a pioneering solution that conducts an exhaustive assessment of web vulnerabilities, leveraging the formidable capabilities of the Nikto in kalli linux ,Qradar,nessus.It is celebrated for its expansive vulnerability database and thorough scanning functionalities, takes center stage in systematically scrutinizing designated websites. The scrutiny spans server configurations, outdated software, potential entry points, and various security vulnerabilities.The project's ingenuity lies in its methodical approach, strategically tailored to execute focused scans that uncover vulnerabilities residing in both well-known and obscure corners of the server architecture.The resultant comprehensive vulnerability report serves as a detailed roadmap, categorizing findings based on severity levels. This nuanced classification facilitates a profound understanding of the implications, empowering stakeholders to prioritize and implement effective mitigation strategies. Through this innovative approach, the project not only enhances security measures but also ensures a strategic and informed response to potential threats, ultimately fortifying the protection of sensitive data and upholding user privacy.

This research, in contrast to traditional scanning techniques, takes a methodical and thorough approach to scrutinising the target website, investigating both known vulnerabilities and hidden entry points. It dives deeply into server configurations, discovering vulnerabilities that could otherwise go unnoticed, hence improving web security by utilising Nikto's sophisticated scanning capabilities. This methodical approach directly helps to the overall security of online platforms in a time when businesses, individuals, and governments are at serious risk from cyber assaults.Increasing web security helps to protect sensitive user data and financial information while also building user trust and promoting more self-assured use of online platforms. Businesses and organisations in need of routine web vulnerability assessments can choose among levels based on scan frequency with the suggested revenue model's subscription packages.

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Parameter** | **Description** |
| 1. | Problem Statement (Problem to be solved) | **Finding and fixing vulnerabilities in web servers has become essential to protecting sensitive data and guaranteeing user privacy as online technologies become more complicated. This project's goal is to carry out an extensive web vulnerability evaluation.** |
| 2. | Idea / Solution description | The suggested project entails using the potent Nikto tool to carry out an exhaustive evaluation of web vulnerabilities. Nikto will be used to thoroughly scan a target website thanks to its large database of known vulnerabilities and all-encompassing scanning features. Server configurations, out-of-date software, possible entry points, and other security flaws will all be carefully examined during the scanning process. The methodical approach is the primary innovation: the tool will be set up to conduct focused scans, finding vulnerabilities in both well-known and obscure server components. This thorough investigation will serve as the foundation for an extensive vulnerability report that classifies results according to degrees of severity. |
| 3. | Novelty / Uniqueness | In contrast to traditional scanning techniques, this project uses a methodical and thorough analysis of the target website, investigating both known vulnerabilities and hidden access points. Through the utilisation of Nikto's vast database and sophisticated scanning features, it probes deeply into the server configurations to find vulnerabilities that could otherwise go unnoticed. Website managers may efficiently prioritise and address security vulnerabilities by using the full vulnerability report that is provided, which not only details potential security breaches but also offers a nuanced knowledge of their ramifications. |
| 4. | Social Impact / Customer Satisfaction | Through the methodical identification and remediation of website vulnerabilities, this project immediately improves the overall security of online platforms. Increasing web security means protecting private, financial, and sensitive user data in a time when cyber threats are a serious concern to individuals, companies, and even governments. Users are then encouraged to trust one another as a result of this. |

**OWASP Top 10 Vulnerabilities**

**Practice Website: psvpec.in**

|  |  |  |
| --- | --- | --- |
| **Vulnerability Name** | | |
| **1.Broken Access Control** | CWE: | 284,285 |
| OWASP Category: | A01:2021 |
| Description: | Broken access control occur when there is no restriction or no authorization check and there is an incorrect restriction access or incorrect authorization check to a resource from an unauthorized actor. |
| Business Impact: | Any unknown person gaining access, privileges of an organisation, reading sensitive information and arbitrary code execution |
| **2.Cryptographic Failures** | CWE: | 326,327 |
| OWASP Category: | A02:2021 |
| Description: | 326-using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.  327-A broken or risky cryptographic algorithm or protocol leads to cryptographic failures. |
| Business Impact: | Insecure cryptography can be misused to reveal sensitive information, modify data in unexpected ways, spoof identities of other users or devices. |
| **3 - Injection** | CWE: | 78,89,94 |
| OWASP Category: | A03:2021 |
| Description: | 94-Improper Control of Generation of Code ('Code Injection')  78-OS Command Injection  89-SQL Injection  An injection happens when an attacker sends invalid data to the web application with the intention of making it do something that the application is not programmed to do. |
| Business Impact: | It causes data loss, data corruption, security breaches, and possibly the loss of control of the target host and the release of sensitive information linked to the host. |
| **4 - Insecure Design** | CWE: | 657 |
| OWASP Category: | A04:2021 |
| Description: | 657- violates well-established principles for secure design. |
| Business Impact: | It leads to functionality failures, data breaches, broken policies, and tarnished reputations of an organisation |
| **5- Security Misconfigurations** | CWE: | 547,526 |
| OWASP Category: | A05:2021 |
| Description: | 547-uses hard-coded constants instead of symbolic names for security-critical values, which increases the likelihood of mistakes during code maintenance or security policy change.  526- uses an environment variable to store unencrypted sensitive information. |
| Business Impact: | It cause significant monetary and reputational damage to an organization. |
| **6 - Vulnerable and Outdated Components** | CWE: | 1104 |
| OWASP Category: | A06:2021 |
| Description: | 1104-relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer. |
| Business Impact: | Outdated components risk can leave you open to a variety of hacks, including ransomware, malware, data breaches, and more, |
| **7 - Identification and Authentication Failures** | CWE: | 521,640 |
| OWASP Category: | A07:2021 |
| Description: | 521- does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.  640- contains a mechanism for users to recover or change their passwords without knowing the original password, but the mechanism is weak. |
| Business Impact: | It leaves the application susceptible to attacks and leaves user accounts/data at risk. |
| **8 - Software and Data Integrity Failures** | CWE: | 345,353 |
| OWASP Category: | A08:2021 |
| Description: | 345- does not sufficiently verify the origin or authenticity of data, in a way that causes it to accept invalid data.  353 - uses a transmission protocol that does not include a mechanism for verifying the integrity of the data during transmission, such as a checksum. |
| Business Impact: | It can result in financial losses, reputational damage, legal liabilities, loss of customer trust about an organisation |
| **9 - Security Logging & Monitoring Failures** | CWE: | 117,223 |
| OWASP Category: | A09:2021 |
| Description: | 117- does not neutralize or incorrectly neutralizes output that is written to logs.  223- does not record or display information that would be important for identifying the source or nature of an attack, or determining if an action is safe. |
| Business Impact: | Allows attackers to attack the company systems further, maintain persistence, pivot to more systems, and tamper, extract or destroy data. |
| **10 - Server-Side Request Forgery** | CWE: | 918 |
| OWASP Category: | A10:2021 |
| Description: | The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. |
| Business Impact: | It cause serious damage to an organization. |

**SANS Top 20 Security Vulnerabilities In Software Applications**

SANS stands for Sysadmin, Audit, Network, and Security.

|  |  |  |
| --- | --- | --- |
| **S.No** | **Vulnerability Name** | **CWE Number** |
| **1** | **Memory Buffer Error** | **119** |
| **2** | **Cross-site Scripting** | **79** |
| **3** | **Unvalidated Input Error** | **20** |
| **4** | **Sensitive Information Exposure Error** | **200** |
| **5** | **Out-of-bounds Read Error** | **125** |
| **6** | **SQL Injection** | **89** |
| **7** | **Free Memory Error** | **416** |
| **8** | **Integer Overflow Error** | **190** |
| **9** | **Cross-Site Request Forgery** | **352** |
| **10** | **Directory Traversal** | **22** |
| **11** | **OS Command Injection** | **78** |
| **12** | **Out-of-bounds Write Error** | **787** |
| **13** | **Improper Authentication Error** | **287** |
| **14** | **Dereferencing NULL Pointer** | **476** |
| **15** | **Incorrect Permission Assignment** | **732** |
| **16** | **Unrestricted File Upload** | **434** |
| **17** | **Information Exposure through XML Entities** | **611** |
| **18** | **Code Injection** | **94** |
| **19** | **Hard-coded Access Key** | **798** |
| **20** | **Uncontrolled Resource Consumption** | **400** |

|  |  |
| --- | --- |
| **Memory Buffer Error** | |
| CWE: | 119 |
| SAN Category: | S01 |
| Description: | This buffer overflow happens when an application process tries to store more data than it can hold in the memory. Since the buffers can only store some level of data and when that level is reached and exceeded, the data flows to another memory location which can corrupt the data already contained in that buffer. |
| Business Impact: | This buffer overflow can erase data, steal confidential information, and even the whole application could crash. |
| **2. Cross-site Scripting** | |
| CWE: | 79 |
| SAN Category: | S02 |
| Description: | Cross-site Scripting (XSS) is an injection attack that usually happens when an attacker injects malicious or harmful script into a web application which can be executed through the web browsers. Once the malicious script finds its way into the compromised system, it can be used to perform different malicious activities like transferring private information like cookies that have the session information from the victim’s computer to the attacker’s compute |
| Business Impact: | An attacker can deface a corporate website by altering its content, thereby damaging the company's image or spreading misinformation. |
| **3.|Unvalidated Input Error** | |
| CWE: | 20 |
| SAN Category: | S03 |
| Description: | When inputs are not properly validated, this will allow an attacker to send a malicious input that the main application will generously process and this will lead to changes in the control flow, arbitrary control of a resource, or arbitrary code execution. |
| Business Impact: | Attackers can manipulate input, resulting in data breaches and unauthorized access to sensitive information of an organisation. |
| **4.Sensitive Information Exposure Error** | |
| CWE: | 200 |
| SAN Category: | S04 |
| Description: | This happens when the application knowingly and unknowingly exposes information that is confidential and sensitive to an attacker who does not have the authorization to access these information.This id due to the errors like database connectivity error, run-time error, and network error on our applications or websites. |
| Business Impact: | Destroying your company's reputation |
| **5. Out-of-bounds Read Error** | |
| CWE: | 125 |
| SAN Category: | S05 |
| Description: | This usually occurs when the application reads data past the normal level, either to the end or before the beginning of the buffer. This gives unprivileged access to an attacker to read sensitive information from other memory locations, which can as well leads to a system or application crash. |
| Business Impact: | It crashes systems, make unexpected program behaviour , and potential security vulnerabilities. |
| **6. SQL Injection** | |
| CWE: | 89 |
| SAN Category: | S06 |
| Description: | The attacker injects a SQL code to the Webform input box in order to gain access to resources or change data that is not authorized to access. |
| Business Impact: | Cybercriminals could gain unwanted or administrative access to private information and resources of an organisation/Institution |
| **7. Free Memory Error** | |
| CWE: | 416 |
| SAN Category: | S07 |
| Description: | This issue is caused by the referencing of memory after it has been released, which can seriously lead to a program crash. |
| Business Impact: | It leads to resource exhaustion and system crashes. |
| **8.** **Integer Overflow Error** | |
| CWE: | 190 |
| SAN Category: | S08 |
| Description: | When a calculation is processed by an application and there is a logical assumption that the resulting value will be greater than the exact value, integer overflow happens. Here, an integer value increases to a value that cannot be stored in a location. |
| Business Impact: | It causes the program to use incorrect numbers and respond in unintended ways |
| **9. Cross-Site Request Forgery** | |
| CWE: | 352 |
| SAN Category: | S09 |
| Description: | It allows an attacker to abuse a user, a web browser and a server at the same time. |
| Business Impact: | It leads to data theft, unauthorized fund transfers, damaged client relationships |
| **10. Directory Traversal** | |
| CWE: | 22 |
| SAN Category: | S10 |
| Description: | Directory traversal is a web security vulnerability that allows an attacker to read arbitrary files on the server that is currently running an application |
| Business Impact: | sensitive information are being leaked or even the entire system being compromised |
| **11.OS Command Injection** | |
| CWE: | 78 |
| SAN Category: | S11 |
| Description: | It is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application |
| Business Impact: | corrupt a database, steal customer records, use an API to launch a specific process or event, or launch a distributed denial of service (DDoS) attack. |
| **12.Out-of-bounds Write Error** | |
| CWE: | 787 |
| SAN Category: | S12 |
| Description: | An out-of-bounds write happens when software (and sometimes hardware) alters memory it's not supposed to, such as by writing data to a memory buffer and overshooting the end of that buffer, causing it to unexpectedly change other variables and information and/or just crash. |
| Business Impact: | Causes memory corruption, exploitation by attackers, denial of service attacks, and data leakage. |
| **13. Improper Authentication Error** | |
| CWE: | 287 |
| SAN Category: | S13 |
| Description: | This is when an attacker claims to have a valid identity but the software failed to verify or proves that the claim is correct. |
| Business Impact: | Data theft, unauthorized access to sensitive information, and account takeover issues occur |
| **14. Dereferencing NULL Pointer** | |
| CWE: | 476 |
| SAN Category: | S14 |
| Description: | Dereferencing a null pointer is when the application dereferences a pointer that was supposed to return a valid result instead returns NULL and this leads to a crash. Dereferencing a null pointer can happen through many flaws like race conditions and some programming error. |
| Business Impact: | Result in the crash of the process |
| **15. Incorrect Permission Assignment** | |
| CWE: | 732 |
| SAN Category: | S15 |
| Description: | This vulnerability happens when an application assigns permissions to a very important and critical resource in such a manner that exposed the resource to be accessed by a malicious user. |
| Business Impact: | it could lead to the exposure of sensitive information, or the modification of that resource by unintended parties. |
| **16. Unrestricted File Upload** | |
| CWE: | 434 |
| SAN Category: | S16 |
| Description: | This vulnerability occurs when the application does not validate the file types before uploading files to the application. This vulnerability is language independent but usually occurs in applications written in ASP and PHP language. |
| Business Impact: | Someone takeover complete system control |
| **17.Information Exposure through XML Entities** | |
| CWE: | 611 |
| SAN Category: | S17 |
| Description: | When an XML document is uploaded into an application for processing and this document contains XML entities with uniform resource identifier that resolves to another document in another location different from the intended location. This anomaly can make the application to attach incorrect documents into its output. |
| Business Impact: | It compromise sensitive data from a target server. The vulnerable server can also be subject to Server-Side Request Forgery (SSRF) attacks. |
| **18. Code Injection** | |
| CWE: | 94 |
| SAN Category: | S18 |
| Description: | de injection is a type of attack that allows an attacker to inject malicious code into an application through a user input field, which is then executed on the fly |
| Business Impact: | Someone takeover complete control your host |
| **19. Hard-coded Access Key** | |
| CWE: | 798 |
| SAN Category: | S19 |
| Description: | It is referred to as embedded credentials, are plain text passwords or other secrets in source code. |
| Business Impact: | It expose sensitive information, such as passwords, keys, or other types of confidential information about your company to unauthorized parties. |
| **20.: Uncontrolled Resource Consumption** | |
| CWE: | 400 |
| SAN Category: | S20 |
| Description: | This vulnerability happens when the application does not control the allocation properly and maintenance of a limited resource, this allows an attacker to be able to influence the amount of resources consumed, which will eventually lead to the exhaustion of available resources |
| Business Impact: | It totally shutdown your entire organisation process |

# Nessus

## Overview:

Nessus is a powerful and widely used vulnerability scanning tool that plays a crucial role in helping organizations identify and address security weaknesses in their networks, systems, and applications. Developed by Tenable Network Security, Nessus has become an indispensable tool for security professionals and IT administrators worldwide.Nessus, known for its comprehensive and user-friendly approach to vulnerability scanning, serves as a valuable asset in the proactive management of security risks. It employs an extensive database of known vulnerabilities, continuously updated to stay current with emerging threats, making it an indispensable tool for maintaining the integrity of an organization's digital assets.

One of the notable features of Nessus is its capability to conduct both authenticated and unauthenticated scans. Authenticated scans require login credentials to perform a more in-depth assessment of the target system, while unauthenticated scans provide a basic assessment without needing access privileges. This flexibility allows organizations to choose the level of scrutiny they require, depending on their security policies and the nature of the assets being scanned.Nessus scans provide a multitude of benefits. First and foremost, they enable organizations to identify and prioritize vulnerabilities, helping them allocate resources efficiently. The tool categorizes vulnerabilities based on severity, providing clear guidance on which issues need immediate attention. This aids in making informed decisions about security patching, system hardening, and risk mitigation.Furthermore,

Nessus offers detailed reports that are essential for communicating vulnerability findings to stakeholders. These reports are customizable, allowing organizations to tailor them to their specific needs.Security professionals can generate executive summaries for management, detailed technical reports for IT teams, and compliance reports to satisfy regulatory requirements

Nessus scans also assist in compliance auditing. Organizations across various industries are often subject to specific regulatory requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) or the Health Insurance Portability and Accountability Act (HIPAA). Nessus can check for compliance with these standards, making it easier for organizations to adhere to their industry-specific regulations.The flexibility of Nessus extends to its scanning options. It supports network scans, web application scans, cloud infrastructure scans, and more. This versatility makes it a valuable tool for organizations with complex and heterogeneous environments, as it can comprehensively assess their entire technology stack.Another crucial aspect of Nessus is its ability to detect zero-day vulnerabilities. While Nessus primarily relies on a database of known vulnerabilities, it can also identify potential weaknesses by analyzing system configurations and behavior. This proactive approach to identifying threats is vital in an era where attackers constantly evolve and develop new attack vectors.

Nessus also supports integration with other security tools and systems, such as Security Information and Event Management (SIEM) solutions. This allows organizations to streamline their security processes, automating the sharing of vulnerability data and alerting mechanisms, thus improving overall security posture.

In conclusion, Nessus is an invaluable asset in the realm of cybersecurity. Its robust scanning capabilities, comprehensive vulnerability database, flexible scanning options, and detailed reporting make it a top choice for organizations striving to secure their digital assets. By identifying and prioritizing vulnerabilities, supporting compliance efforts, and offering a proactive approach to security, Nessus helps organizations stay ahead of the ever-evolving threat landscape. It is a tool that not only identifies weaknesses but also empowers organizations to take swift and informed actions to mitigate security risks, ultimately safeguarding their critical data and systems.

**Target website ➖www.psvpec.in**

**Target ip address:-** **72.167.87.185**

**List of vulnerability**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Vulnerability name** | **Severity** | **plugins** |
| **1** | ***SSH Weak Algorithms Supported*** | Medium | 90317 |
| **2** | ***SSH Server CBC Mode Ciphers Enabled*** | Low | 70658 |
| **3** | SSH Weak Key Exchange Algorithms Enabled | low | 153953 |
| **4** | SSH Weak MAC Algorithms Enabled | low | 71049 |
| **5** | Apache Server ETag Header Information Disclosure | Medium | 88098 |

|  |
| --- |
| REPORT1.Vulnerability Name:- SSH Weak Algorithms Supported **Severity : -** Medium  **Plugin:-90317** Published :April 4, 2016 Modified: December 14, 2016  **Port :-** 22 / tcp / ssh  **Description:-** **Nessus has detected that the remote SSH server is configured to use the Arc four stream cipher or no cipher at all. RFC 4253 advises against using Arc four due to an issue with weak keys**  **solution:-** Contact the vendor or consult product documentation to remove the weak ciphers.  **Business Impact**::- Data breach, Data corruption, Reputation damage |
| 2. Vulnerability Name:- SSH Server CBC Mode Ciphers Enabled **Severity:low**  **Plugin:70658** Published:October 28, 2013 Modified:October 27, 2023  **Port:** 22 / tcp / ssh  **Description:** The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.  **Solution:** Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.  **Business Impact:** An attacker could steal sensitive information, alter the server’s configuration, or launch further attacks on the network. |
| 3. Vulnerability Name:- SSH Weak Key Exchange Algorithms Enabled **Severity:** Low  **Plugin:** 153953 Published:October 13, 2021 Modified:October 13, 2021  **Port:** 22 / tcp / ssh  **Description:** The remote SSH server is configured to allow key exchange algorithms which are considered weak. This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes: diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1 gss-gex-sha1-\* gss-group1-sha1-\* gss-group14-sha1-\* rsa1024-sha1  **Solution:** Contact the vendor or consult product documentation to disable the weak algorithms.  **Business Impact**:T his can lead to data breaches, unauthorized access, loss of productivity, reputational damage, and legal liabilities1 |
| 4. Vulnerability Name:- SSH Weak MAC Algorithms Enabled **Severity:low**  **Plugin:** 71049  **Port:** 22 / tcp / ssh Published:November 22, 2013 Modified:December 14, 2016  **Description:** The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.  **Solution:** Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.  **Business Impact:** **Data breaches and loss of confidential information,**  **Reputation damage and loss of customer trust,**  **Legal liabilities and regulatory fines,**  **Operational disruptions and downtime** |
| 5. Vulnerability Name:- Apache Server ETag Header Information Disclosure **Severity:medium**  **Plugin:** 88098 Published:January 22, 2016 Modified:April 27, 2020  **Port:** 80 / tcp / www  **Description:** The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.  **Solution:** Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.  **Business Impact** : **Bypass authorization mechanisms, access restricted resources, or launch further attacks on the web server or the network** |

**Target website ➖kgr.ac.in**

**Target ip address ➖**184.168.115.31

**List of vulnerability**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Vulnerability name** | **Severity** | **plugins** |
| **1** | ***SSL Anonymous Cipher Suites Supported*** | Medium | 31705 |
| **2** | ***SSL Medium Strength Cipher Suites Supported*** | High | 42873 |
| **3** | **SSL RC4 Cipher Suites Supported** | Medium | 65821 |
| **4** | **Apache Server ETag Header Information Disclosure** | Medium | : 88098 |
| **5** | **SMTP Service Cleartext Login Permitted** | Low | 54582 |
| **6** | **SSH Weak Algorithms Supported** | Medium | : 90317 |
| **7** | **SSH Server CBC Mode Ciphers Enabled** | Low | 70658 |

|  |
| --- |
| 1. Vulnerability Name:- SSL Anonymous Cipher Suites Supported **Severity: Medium**  **Plugin:** 31705  **Published**:March 28, 2008 **Modified**:October 27, 2023  **Port:21/tcp**  **Description:** The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.  **Solution:** Reconfigure the affected application if possible to avoid use of weak ciphers.  **Business Impact :** Results in data breaches,fraud,identity theft,or legal liabilities |
| 2. Vulnerability Name:- SSL Medium Strength Cipher Suites Supported **Severity:**high  **Plugin:** 42873  **Published:**November 23, 2009 **Modified:**February 3, 2021  **Port:** **21 / tcp**  **Description:** The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.  **Solution:** Reconfigure the affected application if possible to avoid use of medium strength ciphers.  **Business Impact:** Damage the reputation and trust of the business, as well as incur legal and regulatory consequences if the data breach affects customers or partners |

|  |
| --- |
| **3. Vulnerability Name:-** **SSL RC4 Cipher Suites Supported**  **Severity:Medium**  **Plugin:** 65821  **Published:**April 5, 2013 **Modified:**February 3, 2021  **Port: 21 / tcp**  **Description:** The remote host supports the use of RC4 in one or more cipher suites.The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.  **Solution:**  Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.  **Business Impact**   1. Regulatory Compliance 2. Browser and Server Compatibility issue |
| **4. Vulnerability Name:-** Apache Server ETag Header Information Disclosure  **Severity: Medium**  **Plugin:** 88098  **Published:** January 22, 2016 **Modified:** April 27, 2020  **Port: 21 / tcp**  **Description:**  The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.  **Solution:**Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.  **Business Impact :**  The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files. |
| **5. Vulnerability Name:-** SMTP Service Cleartext Login Permitted  **Severity:Low**  **Plugin:** 54582  **Published:**May 19, 2011 **Modified:**January 19, 2021  **Port: 587 / tcp / smtp**  **Description:**  The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.  **Solution:** Configure the service to support less secure authentication mechanisms only over an encrypted channel.  **Business Impact :**  An **attacker** may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used. |
| 6. Vulnerability Name:- SSH Weak Algorithms Supported **Severity: Medium**  **Plugin:** 90317  **Published:** April 4, 2016 **Modified:** December 14, 2016  **Port: 22 / tcp / ssh**  **Description:**  Nessus has detected that the remote SSH server is configured to use the Arc four stream cipher or no cipher at all. RFC 4253 advises against using Arc four due to an issue with weak keys.  **Solution:**  Contact the vendor or consult product documentation to remove the weak ciphers.  **Business Impact**  1.Data breach 2.Data corruption 3.Reputation damage |
| 7. Vulnerability Name:- SSH Server CBC Mode Ciphers Enabled **Severity:Low**  **Plugin:** 70658  **Published**:October 28, 2013 **Modified:**October 27, 2023  **Port:** 22 / tcp / ssh  **Description:**  The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.  **Solution:**  Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.  **Business Impact**  This can potentially lead to the attacker gaining access to confidential information, as well as gaining control over the server itself |

# Understanding SOC / SEIM and Qradar

**SOC: (Security Operations Center):** A SOC is a centralized team or facility responsible for monitoring, detecting, responding to, and mitigating security incidents within an organization.

**SOC-Cycle:** This cycle typically includes the following stages

## 1.Monitoring and Detection:

In the initial stage, the SOC uses the SIEM system to continuously monitor and collect data from various sources, such as logs, network traﬃc, and security events.

## 2.Analysis and Alerting:

The collected data is analyzed by the SIEM system to identify anomalies, patterns, and potential security threats. When the SIEM detects a security incident or suspicious activity, it generates alerts and sends them to the SOC.

**3. Investigation and Response:**

SOC analysts receive these alerts and conduct investigations to determine the nature and severity of the security incident. They may gather additional context and evidence to understand the incident fully. Once the incident is understood, the SOC initiates a response plan to mitigate the threat and minimize potential damage.

**4. Resolution and Remediation:**

After the incident is contained, the SOC works on resolving the issue and remediating and vulnerabilities that may have been exploited. This may involve patching systems, updating security policies, or making conﬁguration changes to prevent a similar incident from happening in the future

**5. Documentation and Reporting:**

The SOC documents the details of the incident, including its timeline, impact, and the actions taken for future reference and compliance purposes.

## SIEM (Security Information and Event Management):

SIEM solutions are software platforms that collect and analyze data from various sources, including logs, events, and security-related data, to provide a holistic view of an organization's security posture.

## SIEM Cycle:

The SIEM cycle is a continuous process that allows organizations to maintain a proactive and adaptive approach to cybersecurity. It empowers

the SOC by providing valuable data and automated analysis, which helps in identifying and responding to security threats more eﬃciently.

The SIEM cycle begins with the collection of data from various sources within the organization, including logs, events, network traffic, and

**1. Data Collection:**

security-related data. Data is gathered from diverse systems, devices, and applications, both on-premises and in the cloud.

The collected data is normalized and parsed to ensure that it is in a consistent format that the SIEM system can analyze. This stage helps in standardizing data and making it more understandable for analysis.

**2. Normalization and Parsing:**

1. **Data Analysis and Correlation:**

The SIEM system analyzes the normalized data to identify patterns, anomalies, and potential security threats. Correlation rules are applied to correlate various events and identify potential security incidents.

1. **Alerting and Notification:**

When the SIEM system detects an event or a set of events that match predefined rules or indicate a potential security incident, it generates alerts. These alerts are sent to the SOC for further investigation.

## MISP:

MISP (Malware Information Sharing Platform & Threat Sharing) is an

open-source threat intelligence platform designed to improve the sharing of

structured threat information. MISP can significantly enhance the capabilities of a Security Operations Center (SOC) and a Security Information and Event Management (SIEM) system by providing valuable threat intelligence data and facilitating collaboration among security professionals. Incorporating MISP into the SOC and SIEM ecosystem enables organizations to harness the power of threat intelligence, improve their ability to detect and respond to cyber threats, and strengthen their overall cybersecurity posture

## Deploying soc in college/Institute:

Deploying a Security Operations Center (SOC) in a college or educational institution is a vital step in ensuring the security of sensitive data, intellectual property, and the privacy of students, faculty, and staff.

Identify Objectives: Clearly define the goals and objectives of the SOC. Determine what you want to protect, what threats you want to address, and what resources are available. Risk Assessment: Conduct a risk assessment to identify vulnerabilities and threats specific to the college environment. This assessment will help prioritize security measures.

**1. Assessment and Planning:**

Budget and Resources: Determine the budget and resources available for setting up and operating the SOC. This includes staffing, technology, and ongoing operational costs.

**2. Design and Infrastructure:**

Select Location: Choose a suitable physical location for the SOC. It should

be secure, accessible, and equipped with the necessary infrastructure. Hardware and Software: Acquire the hardware and software necessary for the SOC. This includes servers, network monitoring tools, SIEM systems, and incident response platforms. Connectivity: Ensure that the SOC has robust connectivity to monitor network traffic and security logs effectively.

Hire and Train Staff: Recruit and train SOC analysts and incident responders who will staff the center. They should be well-versed in cybersecurity, incident detection, and response. Continuous Training: Provide ongoing training to keep SOC staff updated on the latest threats and technologies.

**3. Staffing and Training:**

## Threat intelligence:

Subscribe to threat intelligence feeds, such as those from commercial providers, open-source platforms, government agencies, and information sharing and analysis centers (ISACs). These feeds provide real-time information about known threats and vulnerabilities.

**1.Threat Intelligence Feeds:**

Tailor threat intelligence to the college's specific needs and environment. Focus on collecting information relevant to the educational sector and the institution's infrastructure.

1. **Integrate with SIEM:**

Integrate threat intelligence feeds with the Security Information and Event Management (SIEM) system to automatically enrich security event data with relevant threat indicators. This helps the SIEM in identifying potential threats more accurately.

1. **Customized Threat Intelligence:**

## Qradar

**Overview:** QRadar is a security information and event management (SIEM) software. It is designed for enterprises and provides a complete overview of an organization’s security system to detect and report incidents head-on1. QRadar collects log data from an enterprise, its network devices, host assets and operating systems, applications, vulnerabilities, and user activities and behaviors. QRadar uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

**1.Data Collection and Normalization:**

QRadar is used to collect and normalize data from various sources, including logs, network traffic, and security events across the college's IT infrastructure. This data provides the foundation for monitoring and analysis.

QRadar's advanced correlation engine helps identify patterns, anomalies, and potential security threats in real time. It can correlate events to detect complex, multi-stage attacks that might go unnoticed by simpler tools.

**2.Real-time Event Correlation:**

When QRadar detects suspicious or potentially malicious activities based on predefined rules and threat intelligence, it generates alerts and notifications. These alerts are sent to the SOC team for investigation.

**3.Alerting and Notification:**

**4.Threat Intelligence Integration:** QRadar allows the integration of threat intelligence feeds, helping the SOC to keep up with the latest threat information. These feeds can provide context and relevance to detected security events.

## Conclusion:

The comprehensive vulnerability report that is produced is categorised according to the severity of the results and provides a comprehensive grasp of their consequences for efficient prioritisation and mitigation. In contrast to traditional scanning techniques, this project uses a methodical and thorough analysis of the target website, investigating both known vulnerabilities and hidden access points. This methodical approach directly helps to the overall security of online platforms in a time when businesses, individuals, and governments are at serious risk from cyber assaults. Businesses and organisations in need of recurring web vulnerability assessments can choose among tiers based on scan frequency, depth of analysis, and support levels with the suggested revenue model's subscription packages. Cloud-based infrastructure, parallel processing, automated scaling, distributed computing, optimised algorithms, and API connections all contribute to the scalability of the solution.

Our solution is made to meet this demand by using the powerful Nikto tool to carry out an in-depth analysis of web servers, methodically finding and fixing vulnerabilities. The scanning procedure carefully checks server configurations, finds security weaknesses, looks for out-of-date software, and investigates possible entry points. It investigates both well-known and hidden entry points by utilising Nikto's vast database and sophisticated scanning capabilities, giving a comprehensive picture of the website's security posture. In addition to just listing potential security flaws, the resulting vulnerability report provides website administrators with a detailed explanation of their ramifications, allowing them to prioritise and effectively fix the issues. The suggested subscription-based company model makes a reliable source of income and is scalable thanks to cutting-edge infrastructure and technology.

It employs an extensive database of known vulnerabilities, continuously updated to stay current with emerging threats, making it an indispensable tool for maintaining the integrity of an organization's digital assets. By identifying and prioritizing vulnerabilities, supporting compliance efforts, and offering a proactive approach to security, Nessus helps organizations stay ahead of the ever-evolving threat landscape. The future scope of web application testing in the project of deploying a SOC and SIEM in a college involves staying ahead of emerging technologies, security threats, and compliance requirements. The testing process will continually evolve to address new challenges, emphasizing proactive and adaptive security measures to protect the educational institution's web applications and data. The future scope of SOC and SIEM in a college or educational institution is characterized by continuous adaptation, automation, advanced threat detection, and a proactive approach to security.

# Future Scope:

The future scope of this report extends far beyond its current ﬁndings, encompassing a wide range of potential directions for further research and development in the ﬁeld of cybersecurity. To ensure the ongoing effectiveness of cybersecurity practices, several key areas warrant exploration.

First and foremost, there is a pressing need for the development and implementation of advanced vulnerability assessment techniques. As the threat landscape evolves, researchers and practitioners should delve into cutting-edge methods and tools that can provide a more nuanced and accurate understanding of vulnerabilities. Embracing emerging technologies, particularly artiﬁcial intelligence and machine learning, has the potential to revolutionize vulnerability identiﬁcation and mitigation, enabling organizations to adopt a proactive defense strategy against constantly evolving threats.

Furthermore, the scope of vulnerability assessments should expand to encompass a broader spectrum of digital assets. While web servers have traditionally been the primary focus, the rise of mobile applications, cloud services, and IoT devices demands thorough investigation. Addressing

vulnerabilities associated with these diverse technologies is essential to maintain a comprehensive security posture.

Staying up-to-date with regulatory requirements and compliance standards is another critical aspect of future scope. As regulations adapt to address emerging threats and protect sensitive data, vulnerability assessment methodologies should evolve in tandem to ensure that organizations can meet their legal obligations.

Integrating Security Information and Event Management (SIEM) solutions into vulnerability assessment processes represents a promising avenue for enhancing cybersecurity. Research should explore how SIEM can improve threat detection, incident response, and real-time monitoring, providing organizations with a more holistic and proactive security approach.

The human element of cybersecurity is often underestimated, and future efforts should include the development of educational programs and user awareness initiatives. By promoting a culture of cybersecurity and empowering employees and users with knowledge and best practices, the risk of human errors and negligence can be signiﬁcantly reduced.

Collaboration between different stakeholders across sectors and borders is crucial to combating cyber threats effectively. Encouraging the sharing of threat intelligence and best practices can strengthen the collective defense against such threats and improve incident response capabilities.

Finally, an emerging aspect of cybersecurity is the evaluation of its environmental and social impact. Researchers should explore the environmental consequences of security measures, such as the carbon footprint, as well as the societal implications of data breaches. This broader perspective can contribute to a more comprehensive understanding of the far-reaching effects of cybersecurity practices.

In conclusion, the future scope of this report envisions a dynamic and adaptable approach to cybersecurity that incorporates ongoing research, innovation, collaboration, and a commitment to staying ahead of emerging threats. This approach is crucial to ensuring the safety and integrity of digital assets in an ever-evolving digital landscape.