Title of the project:- Web Application Testing in Cyber Security

Overview :-

Protecting sensitive data and important systems from online threats is known as cybersecurity. Cybersecurity measures, also referred to as information technology (IT) security, are intended to counter attacks to networked systems and applications, whether those threats come from within or outside of an organization.

Globally, a data breach cost an average of USD 3.86 million in 2020, whereas it cost an average of USD 8.64 million in the United States. The costs of finding and addressing the breach, the price of downtime and lost revenue, and the long-term reputational harm to a company and its brand are among these charges. Customers' personally identifiable information (PII), such as names, addresses, national identification numbers (such as Social Security numbers in the US and fiscal codes in Italy), and credit card numbers are the targets of cybercriminals who subsequently sell these details on unregulated online black markets. Customer distrust is frequently lost as a result of compromised PII, which can also result in regulatory penalties and even legal action.

These expenses may be increased by the complexity of security systems brought on by dissimilar technologies and a lack of internal expertise. However, businesses that have a thorough cybersecurity plan that is automated utilizing advanced analytics, artificial intelligence (AI), and machine learning can combat cyberthreats more successfully and lessen the impact of breaches when they do happen.

Layers of defense are included in a solid cybersecurity plan to combat cybercrime, such as attempts to access, modify, or delete data; demand money from users or the organization; or obstruct regular business activities. Countermeasures ought to focus on:

Critical infrastructure security

Procedures for safeguarding the networks, computers, and other assets that society depends on for economic viability, public safety, and/or national security. To assist enterprises in this area, the National Institute of Standards and Technology (NIST) has developed a cybersecurity framework, and the U.S. Department of Homeland Security (DHS) offers additional advice.

Application security

Processes that aid in protecting cloud-based and on-premises apps. Applications should be designed with security in mind from the beginning, taking into account user authentication, data handling, and other factors.

End-user education

Increasing security awareness within the company to improve endpoint security. Users can be taught, for instance, to discard dubious email attachments and steer clear of unidentified USB devices.

Disaster recovery

Tools and processes for addressing unanticipated occurrences, such as power outages, cybersecurity incidents, or natural disasters, with the least possible impact on crucial activities.

Storage security

Delivers incredibly strong data resiliency with many security measures. This comprises immutable and segregated data copies as well as encryption. These continue to be in the same pool so that they can be easily restored to aid in recovery, reducing the effects of a cyberattack.

List of employees participated

S. No.	Name	Designation	Mobile No.
1	Dr.RAJASEKARAN.P	ASSISTANT PROFESSOR	9994223667

List of Vulnerability Table

S.no	Vulnerability Name	CWE - No
1.	A01: Broken Access control	CWE-284: Improper Access Control
2.	A02: Cryptographic Failures	CWE-259: Use of Hard-coded Password
3.	A03: Injection	CWE-20: Improper Input Validation
4.	A04: Insecure Design	CWE-209: Generation of Error Message Containing Sensitive Information
5.	A05: Security Misconfiguration	CWE-11: ASP.NET Misconfiguration: Creating Debug Binary
6.	A06: Vulnerable and outdated components	CWE-1104: Use of Unmaintained Third-Party Components
7.	A07: Identification and Authentication Failures	CWE-297: Improper Validation of Certificate with Host Mismatch
8.	A08: Software and data integrity failures	CWE-209: Generation of Error Message Containing Sensitive Information
9.	A09: Security logging and monitoring failures	CWE-259: Use of Hard-coded Password
10.	A10: Server Side Request Forgery	CWE-918: Server-Side Request Forgery (SSRF)

REPORT: -

1.Vulnerability Name: - Broken Access control

CWE: -284

OWASP Category: - A01:2021 Broken Access control

Description: - it does not allow unauthorized users.

Business Impact: - Broken access control can have severe and far-reaching impacts on a business. Security breaches and unauthorized access to sensitive information can result in data loss, financial penalties, and legal liabilities. Intellectual property theft, regulatory non-compliance, and reputation damage are additional risks. Operational disruptions, financial losses, and increased recovery costs can ensue, affecting productivity and innovation. Furthermore, compromised access control can lead to delays in development, decreased efficiency, and potential legal consequences. To mitigate these risks, businesses must prioritize robust access control measures, regular security assessments, employee training, and a proactive approach to staying informed about security threats and best practices. Effective access control is integral to holistic business risk management.

2— Vulnerability Name: Cryptographic Failures

CWE: CWE-259

OWASP Category: A02: Cryptographic Failures

Description: employs for either internal authentication or external component outbound communication

Business Impact: Cryptographic failures can have profound and far-reaching consequences for businesses, encompassing security breaches, financial losses, reputation damage, and regulatory non-compliance. These failures can lead to data breaches and privacy violations, potentially resulting in unauthorized access to sensitive information and regulatory fines. Financial implications arise from the costs of breach investigation, remediation, and legal actions. A tarnished reputation can erode customer trust, impacting loyalty and brand perception. Moreover, intellectual property theft, operational disruptions, delayed product releases, and legal consequences further underscore the seriousness of cryptographic weaknesses. To mitigate these risks, businesses must prioritize robust encryption practices, routine security evaluations, and ongoing staff training, fostering a culture of strong information security management.

3— Vulnerability Name: Injection

CWE: **CWE-20**

OWASP Category: A03:2021 Injection

Description: it does not verify or erroneously verifies that the input possesses the qualities necessary to securely and correctly handle the data.

Business Impact: Injection attacks pose significant risks to businesses, encompassing data breaches, financial losses, reputation harm, and regulatory non-compliance. These attacks can lead to unauthorized access, data theft, and operational disruptions, causing financial repercussions from breach-related expenses

and revenue loss. Additionally, a successful attack can tarnish a company's reputation, erode customer trust, and result in regulatory fines. Intellectual property theft, user impact, delayed development, and long-term security repercussions further underline the gravity of injection vulnerabilities. To counter these risks, businesses should prioritize secure coding practices, conduct routine security assessments, and foster a culture of proactive cybersecurity awareness, ultimately fortifying defenses against injection attacks and their far-reaching consequences.

4— Vulnerability Name: Insecure Design

CWE: CWE-**209**

OWASP Category: A04:2021 Insecure Design

Description: sends out an error message that contains private data about its surroundings, users, or related information.

Business Impact: Insecure design decisions within a business's technological solutions can have profound and wide-ranging consequences. Such choices can expose systems to exploitation, leading to data breaches, unauthorized access, and privacy violations. Financial losses may result from breach-related expenses and diminished revenue, while reputational damage can erode customer trust and brand value. Operational disruptions, regulatory non-compliance, and delayed time-to-market further compound the impact. Insecure design also raises maintenance costs, limits innovation, and brings legal and compliance challenges. To mitigate these risks, organizations must prioritize security throughout the design process, engaging experts, adhering to best practices, and fostering a culture that places security at the core of technological development.

5— Vulnerability Name: Security Misconfiguration

CWE: CWE-**11**

OWASP Category: A05:2021 Security Misconfiguration

Description: assist attackers in planning an attack by teaching them more about the system.

Business Impact: Security misconfigurations can have profound and multifaceted effects on businesses. These errors, stemming from improper setup and maintenance of security settings, can result in unauthorized access, data breaches, and financial losses due to breach-related expenses and reduced revenue. The aftermath of a misconfiguration can tarnish a company's reputation, eroding customer trust and triggering regulatory fines for non-compliance. Operational disruptions, intellectual property theft, and compromised user privacy further amplify the impact. Prompt detection and response can be hindered, prolonging the exposure to potential threats. In addition, addressing misconfigurations can prove resource-intensive. To counter these risks, businesses should prioritize proactive security measures, including regular assessments, adhering to best practices, robust training, and cultivating a security-conscious organizational culture. This comprehensive approach can help prevent security misconfigurations and their detrimental consequences.

6— Vulnerability Name: Vulnerable and outdated components

CWE: CWE-**1104**

OWASP Category: A06:2021 Vulnerable and outdated components

Description: dependable representative of the original developer does not actively support.

Business Impact: Relying on vulnerable and outdated software components within a business's systems can lead to profound repercussions. These components, with known security flaws or lacking developer support, increase the risk of data breaches, unauthorized access, and financial losses due to breach-related expenses and reputational damage. Operational disruptions, regulatory non-compliance, and delayed incident response further compound the impact. The potential harm extends to customer trust erosion, supply chain risks, and technical debt accumulation. To mitigate these risks, businesses must prioritize vigilant software supply chain management, promptly addressing vulnerabilities, staying informed about security advisories, and adopting a proactive approach to software development and maintenance. This comprehensive strategy can help safeguard against the adverse effects of vulnerable and outdated components.

7— Vulnerability Name: Identification and Authentication Failures

CWE: CWE-**297**

OWASP Category: A07:2021 Identification and Authentication Failures

Description: it does not adequately verify that the certificate is genuinely connected to that host.

Business Impact: CWE-297, the "Improper Validation of Certificate with Host Mismatch," poses significant business risks if left unaddressed. This vulnerability occurs when a system fails to appropriately validate SSL/TLS certificates during secure communication processes, such as HTTPS connections. If the common name (CN) or subject alternative name (SAN) in the certificate does not match the host to which the connection is established, attackers can exploit the flaw for man-in-the-middle (MITM) attacks, potentially gaining unauthorized access to sensitive data like login credentials or financial information. Consequently, data breaches may occur, leading to compromised customer trust, legal and compliance issues, and service disruptions. Businesses could face financial losses and reputational damage due to the theft of intellectual property or proprietary algorithms. To mitigate these risks, organizations should ensure proper certificate validation, keep SSL/TLS libraries updated, and use reputable SSL certificates from trusted CAs while implementing additional security measures like certificate pinning and monitoring to protect their systems and customers effectively.

8— Vulnerability Name: Software and data integrity failures

CWE: CWE-**209**

OWASP Category: A08:2021 Software and data integrity failures

Description: Sends out an error message that contains private data about its surroundings, users, or related information.

Business Impact: The business impact of CWE-209 can be severe. It can lead to loss of confidential data, loss of reputation, and financial loss1. It can also lead to legal issues and regulatory fines3. Therefore, it is important to ensure that applications and systems do not reveal sensitive information in error messages. Developers should ensure that error messages do not contain sensitive information and that they are properly handled

9— Vulnerability Name: Security logging and monitoring failures

CWE: CWE-**259**

OWASP Category: A09:2021 Security logging and monitoring failures

Description: hard-coded password that it employs for either internal authentication or external component outbound communication.

Business Impact: CWE-259 can lead to unauthorized access to sensitive data and systems2. It can also lead to loss of reputation and trust in the organization2. Is there anything else I can help you with?

10— Vulnerability Name: Server-Side Request Forgery

CWE: CWE-**918**

OWASP Category: A10:2021 Server-Side Request Forgery

Description: it does not appropriately check that the request is being transmitted to the intended recipient.

Business Impact: The business impact of an SSRF vulnerability can be severe. Attackers can use SSRF vulnerabilities to bypass security controls and access sensitive data or systems2. They can also use SSRF vulnerabilities to launch attacks against other systems on the network3. It is important for organizations to identify and remediate SSRF vulnerabilities in their web applications to prevent these types of attacks from occurring.

Stage 2

Overview: -

It's critical to do a vulnerability assessment for a college website to find and fix any potential security flaws that an attacker might exploit. Continuous monitoring is an ongoing practice in security and development are necessary to keep a strong resistance against possible dangers. Furthermore, if you lack the knowledge to do a complete evaluation, it is advisable to look for qualified cybersecurity specialists. Check to see if the webpage shows and is secure. Correctly across a range of platforms and browsers. all identified documents vulnerabilities, their degree, and the probable consequences. Prioritize the repairs according to importance, and aid the college's IT staff or site developers with the cleanup procedure. Keep a record of all vulnerabilities found, including their significance and potential effects.

Put fixes in order of importance and assist the college's IT staff or web developers in the remediation process.

Nessus is a well-known vulnerability assessment tool that businesses and cybersecurity experts use to find and fix security flaws in their networks, systems, and applications.

Nessus is mostly used for automatically scanning for vulnerabilities. To find known vulnerabilities and misconfigurations, it examines networks, servers, endpoints, and applications.

This aids businesses in prioritizing their security efforts and identifying potential avenues of entry for attackers.

Nessus scan findings reveal information about uninstalled updates and patches for a variety of programs and operating systems. This ensures that urgent security fixes are applied swiftly, helping to maintain an up-to-date and safe IT environment.

Nessus can be used to evaluate if a company's systems and configurations adhere to legal and industry standards including PCI DSS, HIPAA, NIST, CIS, and more. It assists businesses in locating weaknesses and achieving compliance with security best practices.

Web applications can be scanned by Nessus to find flaws like SQL injection, cross-site scripting (XSS), and other problems that could leave them vulnerable to assaults.

Nessus can offer useful details about the systems and devices connected to the network, helping to keep an accurate inventory and comprehend the attack surface of the network.

Nessus assists security teams and IT employees in understanding the security posture of their systems by producing thorough vulnerability reports.

This knowledge can be applied to enhance security awareness and training initiatives.

Nessus categorizes detected vulnerabilities into severity levels, assisting companies in prioritizing their efforts by concentrating on high-risk vulnerabilities first.

Nessus can support manual penetration testing efforts by giving a preliminary overview of potential vulnerabilities prior to more thorough manual testing being carried out.

These days, a lot of businesses use cloud infrastructure. Nessus can evaluate cloud environments and spot setup errors or security holes that could compromise the security of cloud-based resources.

Utilizing continuous monitoring techniques with Nessus enables businesses to review their security posture on a regular basis and spot changes that could lead to new vulnerabilities.

To compare scan results with known exploits and threats, Nessus may be connected with threat intelligence feeds, giving users a more complete picture of the risks, they may face

Target website www.srmist.edu.in
Target ip address: - 13.235.158.125

List of vulnerability

s.no	Vulnerability name	Severity	plugins
1.	HTTP Server Type and Version	This plugin attempts to determine the type and the version of the remote web server.	10107
2.	Nessus SYN scanner	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.	11219
3.	Service Detection	Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.	22964
4.	Web Server No 404 Error Code Check	The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.	10386
5.	Apache HTTP Server Version	The remote host is running the Apache HTTP Server, an open-source web server. It was possible to read the version number from the banner.	48204

6.	Host Fully Qualified Domain Name (FQDN) Resolution	Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.	12053
7.	OS Identification	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	11936
8.	TCP/IP Timestamps Supported	The remote host implements TCP timestamps, as defined by RFC1323.	25220
9.	Traceroute Information	Makes a traceroute to the remote host.	10287
10.	Asset Attribute: Fully Qualified Domain Name (FQDN)	Report Fully Qualified Domain Name (FQDN) for the remote host.	166602

REPORT: -

1.Vulnerability Name: - HTTP Server Type and Version

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

Plugin: - 10107

Port: - 80 / tcp / www

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

solution: -

Business Impact:- The choice of HTTP server type and version for a website can have significant business impacts. Several options are available, including widely used ones like Apache HTTP Server (httpd), Nginx, Microsoft Internet Information Services (IIS), LiteSpeed Web Server, Cherokee, Caddy, and Lighttpd. Apache is known for its flexibility and strong community support, Nginx for high performance and scalability, IIS for integration with Microsoft technologies, LiteSpeed for speed optimization, Cherokee for user-friendly configuration, Caddy for easy HTTPS setup, and Lighttpd for efficiency in resource-constrained environments. The selected server can influence performance, scalability, security, compatibility, ease of configuration, and cost, making it important to align the choice with specific business needs and goals.

2.Vulnerability Name:- Nessus SYN scanner

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

Plugin:- 11219

Port :- 80 / tcp / www

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

solution:- Protect your target with an IP filter.

Business Impact::- The Nessus SYN scanner, a component of the Nessus vulnerability assessment tool, holds significant business impact. By identifying vulnerabilities, open ports, and potential risks in computer systems and networks, it empowers businesses to enhance their security posture and mitigate potential cyber threats. This proactive approach aids in regulatory compliance, resource optimization, and timely remediation, ultimately safeguarding business continuity and reputation. The scanner's role in early detection and remediation of vulnerabilities leads to cost savings, demonstrating a commitment to data protection and customer trust.

3.Vulnerability Name:- Service Detection

severity : - Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Plugin:- 22964

Port :- 80 / tcp / www

Description:- Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

solution:-

Business Impact::- Service detection plays a vital role in business by providing accurate identification and categorization of services running on network devices and servers. This capability offers a range of benefits, including enhanced network visibility, improved security through the identification of unauthorized services, effective vulnerability management, compliance with industry regulations, streamlined incident response, optimized resource allocation, ensured business continuity, comprehensive asset management, reduced risks through informed decision-making, and the ability to generate detailed audits and reports. These advantages collectively contribute to a more secure, resilient, and well-managed IT environment, aligning with business goals and mitigating potential threats.

4.Vulnerability Name:- Web Server No 404 Error Code Check

severity : - The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.
Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Plugin:- 10386

Port :- 80 / tcp / www

Description:- The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.
Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

solution:-

Business Impact::- Enabling a "No 404 Error Code Check" feature on a web server can significantly impact a business by enhancing user experience, improving search engine optimization (SEO), reducing bounce

rates, and fostering customer satisfaction. This feature, achieved through customized error pages or redirects, minimizes user frustration, maintains link equity for better SEO, and promotes brand credibility. By offering relevant content suggestions and engagement opportunities, businesses can retain visitors, gather valuable data insights, ensure accessibility compliance, and provide helpful support resources. Overall, this approach contributes to a positive online impression, customer retention, and effective alignment with business objectives.

5.Vulnerability Name:- Apache HTTP Server Version

severity : - The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Plugin:- 48204

Port :- 443 / tcp / www

Description:- The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

solution:-

Business Impact::- The version of the Apache HTTP Server being used can have substantial business impacts across multiple domains. Upgrading to a newer version can lead to enhanced performance, faster page loads, and access to new features. More importantly, it often includes critical security patches, safeguarding against cyber threats and data breaches. Compatibility with modern technologies, ongoing support, and adherence to regulations become easier to maintain with up-to-date versions. Furthermore, a current Apache version contributes to improved search engine rankings, developer productivity, resource utilization, and user trust. By aligning with the latest advancements, businesses can ensure resilience, security, and optimal performance in the dynamic digital landscape, fostering growth and customer confidence.

6.Vulnerability Name:- Host Fully Qualified Domain Name (FQDN) Resolution

severity : - Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Plugin:- 12053

Port :- NA

Description:- Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

solution:-

Business Impact::- Host Fully Qualified Domain Name (FQDN) resolution holds a significant business impact. It ensures easy access to network resources, enhancing user experience and building trust. A well-

resolved FQDN strengthens branding efforts, positively affecting brand recognition and professionalism. Additionally, it influences SEO rankings, email communication, data security through SSL/TLS certificates, remote access for collaboration, efficient server management, and the functionality of third-party integrations. Proper FQDN resolution contributes to seamless operations, customer satisfaction, and a strong online presence, aligning with business objectives and fostering growth.

7.Vulnerability Name:- OS Identification

severity : - 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

Plugin:- 11936

Port :- NA

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

solution:-

Business Impact::- The identification of vulnerabilities in an operating system (OS) can have profound business impacts. Such vulnerabilities, which represent weaknesses in software that malicious actors can exploit, may lead to security breaches, unauthorized access to sensitive data, and potential data loss. Additionally, attacks exploiting OS vulnerabilities can result in system downtime, disrupting operations and causing financial losses. The aftermath of such incidents can encompass substantial costs, including those related to investigations, patch implementation, system audits, and potential legal repercussions. Moreover, businesses risk reputational damage, eroded customer trust, and potential regulatory fines. To mitigate these impacts, proactive cybersecurity measures such as vulnerability assessments, timely patch management, employee training, and robust security controls are crucial to safeguarding systems and maintaining business resilience.

8.Vulnerability Name:- TCP/IP Timestamps Supported

severity : - The remote host implements TCP timestamps, as defined by RFC1323

Plugin:- 25220

Port :- NA

Description:- The remote host implements TCP timestamps, as defined by RFC1323

solution:-

Business Impact::- The adoption of TCP/IP timestamps in networking can have multifaceted effects on businesses. On the positive side, these timestamps facilitate enhanced network performance optimization,

real-time application responsiveness, and more effective troubleshooting through accurate round-trip time measurements. They also contribute to robust network monitoring and security analysis, aiding in identifying anomalies and potential cyber threats. Moreover, TCP/IP timestamps support precise time synchronization for time-sensitive operations, such as financial transactions. However, their usage can introduce concerns, including potential security and privacy risks due to information exposure, a slight increase in network overhead, compatibility issues across diverse systems, and the possibility of generating false positives in security systems. Therefore, businesses need to carefully balance the benefits and potential drawbacks, implementing TCP/IP timestamps thoughtfully within the context of their specific network environment and operational requirements.

9.Vulnerability Name:- Traceroute Information

severity : - Makes a traceroute to the remote host

Plugin:- 10287

Port :- 0 / udp

Description:- Makes a traceroute to the remote host

solution:-

Business Impact::- Traceroute information can significantly impact businesses by enabling efficient network troubleshooting, enhanced Quality of Service (QoS), better vendor management, and informed network planning. It assists IT teams in swiftly identifying and resolving network issues, optimizing resource allocation for critical applications, and ensuring vendor compliance with service level agreements. Additionally, traceroute aids in anticipating challenges during network expansion. However, businesses must be cautious about potential security risks and data privacy concerns, as traceroute exposes network architecture. Balancing the benefits with these considerations is essential for leveraging traceroute effectively and minimizing any performance overhead or misinterpretation of results.

10.Vulnerability Name:- Asset Attribute: Fully Qualified Domain Name (FQDN)

severity : - Report Fully Qualified Domain Name (FQDN) for the remote host.

Plugin:- 166602

Port :- NA

Description:- Report Fully Qualified Domain Name (FQDN) for the remote host.

solution:-

Business Impact::- The adoption of Fully Qualified Domain Names (FQDNs) as asset attributes can significantly impact businesses in various ways. FQDNs streamline network management and monitoring,

enhancing operational efficiency and remote troubleshooting. They promote standardized naming conventions, improving communication and collaboration across teams. Furthermore, FQDNs enable effective load balancing and service redundancy, ensuring high availability. However, businesses must remain vigilant about potential security risks, such as information exposure and DNS vulnerabilities. Complexity in management and potential vendor dependencies should also be considered. Striking a balance between the benefits and potential drawbacks of FQDN usage is crucial for maximizing their value while minimizing associated risks.

Stage 3
Report
The Role of SIEM Solutions in SOCs

- **Soc**

  A Security Operations Center (SOC) is a centralized team or facility within an organization responsible for continuous monitoring, detection, analysis, and response to cybersecurity incidents. Operating around the clock, a SOC's primary functions include monitoring network activities and security alerts, investigating and analyzing incidents, executing incident response actions, gathering threat intelligence, managing vulnerabilities, and collaborating with internal departments and external partners. By combining technology, skilled professionals, and efficient processes, a SOC plays a vital role in safeguarding the organization's systems and data against evolving cyber threats, ensuring early detection, and enabling effective mitigation strategies.

- **SOC – cycle**

  The SOC (Security Operations Center) cycle is a continuous process that safeguards organizations against cybersecurity threats. It encompasses multiple stages, beginning with monitoring and detection, where the SOC team watches for unusual activities and potential threats. Upon identification, incidents are analyzed to understand their scope and impact. Subsequently, the SOC initiates incident response measures, containing and mitigating the threat. Clear communication and reporting ensure stakeholders are informed, and post-incident, the team focuses on recovery and remediation. Lessons learned contribute to refining procedures, while continuous monitoring and adaptation keep the organization agile and prepared for evolving threats. This comprehensive cycle allows the SOC to proactively manage cybersecurity, from threat identification to ongoing risk mitigation.

- **Siem**

  SIEM, or Security Information and Event Management, is a holistic security approach that merges security information management (SIM) and security event management (SEM). It involves real-time analysis of security alerts from various sources within an organization's infrastructure, such as network devices, servers, and applications. SIEM collects and correlates data to identify potential security incidents, offering event correlation, alert generation, incident response support, and compliance reporting. By detecting patterns and anomalies, SIEM assists in early threat detection, provides context for incident investigation, aids in compliance adherence, and enhances an organization's overall security posture. With its comprehensive capabilities, SIEM is instrumental in maintaining vigilant cybersecurity monitoring and effective incident management.

- **Siem Cycle**

  The SIEM (Security Information and Event Management) cycle is a continuous process that enhances cybersecurity within organizations. It starts with data collection from diverse sources, followed by event correlation to identify patterns and anomalies. Real-time alerts are generated based on predefined rules, guiding incident investigation and response. The SIEM system aids in incident containment, subsequent forensic analysis, and reporting for compliance. This iterative process drives continuous improvement by refining detection rules and response procedures. Integration of threat intelligence keeps the organization updated on emerging threats. Ultimately, the SIEM cycle ensures vigilant monitoring, swift incident response, and ongoing enhancement of cybersecurity defenses, contributing to a more resilient and secure environment.

- **MISP**

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source threat intelligence platform designed for streamlined threat information management. It empowers organizations to collect, normalize, and enrich threat data from diverse sources, facilitating effective threat analysis and response. MISP supports collaboration through the sharing of structured threat indicators and artifacts, enabling the identification of complex attack patterns and enhancing collective cybersecurity defense. The platform's compatibility with standards like STIX2, integration capabilities, and community-driven development further solidify its role in enabling proactive threat intelligence sharing, aiding early detection, and bolstering overall cybersecurity strategies.

- **Your college network information**
- Name : SRM University, Kattankulathur
- Ip address : 13.235.158.125
- **Threat intelligence**

  Threat intelligence refers to the knowledge and insights gained from analyzing and understanding potential cybersecurity threats and risks. It encompasses a wide range of information, including data about malicious actors, their tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), vulnerabilities, and emerging attack trends. Threat intelligence aims to provide organizations with actionable insights to enhance their cybersecurity defenses and decision-making processes. It plays a crucial role in proactive threat detection, incident response, and risk mitigation strategies. By collecting, analyzing, and sharing threat intelligence, organizations can better understand the threat landscape, identify vulnerabilities, and implement effective measures to protect their systems, data, and digital assets.
- **Incident response**

  Incident response involves a structured approach by organizations to manage and mitigate the impact of cybersecurity incidents or breaches. The main objective is to minimize damage, swiftly contain the incident, investigate its origin, and restore normal operations promptly. This process encompasses several key phases. It starts with preparation, which entails creating a detailed incident response plan, defining roles, and establishing communication protocols. Swift identification of incidents is vital, followed by containing the threat to prevent further harm. Eradication involves removing the root cause, while recovery focuses on restoring systems. Lessons learned are documented for future prevention, and effective communication is maintained throughout. Legal compliance and regulatory adherence are crucial, making incident response an ongoing and adaptive process.
- **Qradar & understanding about tool**

With over 700 supported connectors and partner extensions, QRadar SIEM is designed on an open platform and has a large partner ecosystem. Utilizing these features will allow your business to effortlessly integrate current security products, thereby increasing ROI. Since QRadar SIEM doesn't need to be fine-tuned, it can start detecting right away. There is no longer any need for complex customization of onboarding log sources, which frequently takes a long period (upwards of 6+ months).

The QRadar SIEM builds a strong integration ecosystem by integrating threat intelligence feeds, vulnerability management tools, and endpoint security platforms. This provides analysts with a highly customized security experience that enables them to identify and eliminate threats more quickly.

Community Edition is a low memory, low EPS, and perpetual license version of QRadar that is completely free. This version supports apps, however it is based on a lower footprint for non-enterprise use and is limited to 50 events per second and 5,000 network flows per minute.

Users, students, security experts, and app developers have unlimited access to the most recent features of QRadar 7.3.3 thanks to the QRadar Community Edition.

QRadar Community Edition Overview

The free IBM QRadar Community Edition is a non-guaranteed version of the software that is designed for personal use.

Many of the same features as QRadar are available in IBM QRadar Community Edition, which has a license for 50 events per second and 5,000 flows per minute.

Free download and testing are available for QRadar Community Edition. If you are a SOC analyst who wants to determine whether an integrated security analytics platform is a good fit for your company, download the community edition.

•You need a setting where you can test apps without disrupting your live QRadar system because you are a developer building QRadar apps.

•You need to test and validate new use cases for QRadar without having an impact on your production.

Procedure

Download the OVA file for the QRadar Community Edition from IBM Developer.

(Qradar/CE) is available at (developer.ibm.com).

2. Using the OVA file, construct a virtual machine that satisfies the following conditions:

• 8GB RAM is the minimum.

If you're utilizing X-Force testing or Ariel queries, you'll need 10 GB or more. You require additional RAM.

for certain apps. All apps share the 10% of RAM that is made accessible to them.

• 250 GB or less of disk space

• At least 2 CPU cores

Note: If you are utilizing X-force testing, you require a minimum of 6 CPU cores for best performance.

If you use Ariel queries with X-force data, you require a minimum of 8 CPU cores.

• At least one network adapter with internet connectivity is required.

The hostname must be a fully qualified domain name and cannot exceed 63 characters in length.

3. Log in as the root user and enter a password.

4. Start the set up process by typing the following command: ./setup

5. Press Enter to accept the CentOS end user license agreement (EULA).

6. Accept the QRadar Community Edition EULA. a) Press Space to advance through the EULA screen. b) Press q to be prompted to accept the EULA. c) Press Enter to accept the EULA.

7. Press Y to continue set up.

8. Enter a password for the admin account. Set a strong password that meets the following criteria:

9. Restart the appliance by typing the following command: reboot 10. Log in to QRadar Community Edition user interface as the admin user and accept the EULA. Access QRadar Community Edition in a web browser at https:///console. If you are using a locally hosted virtual machine with a local IP address, access QRadar Community Edition in a web browser on your host system at https://:8444/console.

Conclusion :-

- **Stage 1 :- Web application testing .**

Web application testing encompasses a comprehensive evaluation of a web application's functionality, security, performance, usability, and compatibility. Testers scrutinize features, links, and navigation to ensure seamless functionality across diverse browsers and devices. They uncover vulnerabilities like SQL injection and cross-site scripting through rigorous security testing. Performance testing assesses responsiveness and scalability, while usability testing enhances user experience and interface design. Compatibility testing guarantees consistent performance across various platforms, and accessibility testing ensures inclusivity for users with disabilities. Regression testing guards against new bugs with code changes, while penetration testing probes security vulnerabilities. All these tests collectively contribute to a robust web application that meets quality standards, user expectations, and security benchmarks.

- **Stage 2 :- Nessus report .**

  A Nessus report is a comprehensive document generated by the Nessus vulnerability scanner, a widely utilized tool for identifying and assessing vulnerabilities in computer systems, networks, and applications. It furnishes detailed insights into security vulnerabilities, misconfigurations, and potential threats discovered during vulnerability assessments or penetration testing. The report includes a summary of the scan, categorized vulnerability details, actionable recommendations for remediation, technical specifics of each vulnerability, risk ratings, compliance assessments, and graphical representations of vulnerability distribution. Nessus reports serve as crucial references to comprehend security status, prioritize mitigation, and demonstrate regulatory compliance, playing a vital role in enhancing overall cybersecurity.
- **Stage 3 :- SOC Dashboard**
- A Security Operations Center (SOC) dashboard is a centralized visual tool that offers real-time insights into an organization's cybersecurity status. It presents key security metrics, alerts, and activities, enabling SOC analysts to monitor, detect, and respond to potential threats efficiently. The dashboard displays alerts, incidents, threat intelligence, network traffic patterns, endpoint security information, user behavior, compliance status, and incident response progress. It provides a comprehensive overview of the organization's security posture and facilitates informed decision-making for timely threat mitigation and continuous improvement of cybersecurity measures.
- **SEIM**

  A Security Information and Event Management (SIEM) dashboard is a centralized interface that offers real-time insights into an organization's security landscape. It aggregates and visualizes data from diverse sources, such as logs, alerts, and correlations, providing security analysts with a holistic view of potential threats and incidents. Through log data visualization, real-time alerts, behavioral analysis, and threat intelligence integration, the SIEM dashboard aids in swift threat detection, incident response, and compliance reporting. Customizable and equipped with historical data, it enables proactive decision-making, helping organizations stay ahead of security challenges and maintain a robust cybersecurity posture.
- **Qradar Dashboard**

  A QRadar dashboard serves as the visual interface within the IBM QRadar Security Information and Event Management (SIEM) platform, offering real-time insights into an organization's security landscape. By aggregating and presenting data, alerts, and offenses from diverse sources, the QRadar dashboard provides security analysts with a centralized hub for monitoring, detecting, and responding to potential threats and incidents. With features like real-time monitoring, threat

intelligence integration, network activity visualizations, and custom widgets, the dashboard empowers analysts to swiftly assess and investigate security events, aiding in proactive threat detection, incident response, and compliance monitoring. It facilitates informed decision-making and enhances an organization's ability to maintain a robust cybersecurity posture.

Future Scope :-

- **Stage 1 :- future scope of web application testing**

  The future scope of web application testing is poised for dynamic evolution driven by technological advancements and evolving security challenges. Testing methodologies are expected to align closely with development through practices like Shift Left testing and DevSecOps, facilitating early vulnerability detection. Microservices and API testing will gain prominence to ensure seamless interactions in complex application ecosystems. Progressive Web Apps (PWAs) will necessitate comprehensive testing for consistent cross-device functionality. Automation powered by AI and machine learning will drive efficiency, especially in security and vulnerability management. Containerization, serverless architecture, and IoT will introduce new dimensions to testing paradigms, while performance testing will simulate real-world usage. User experience testing will encompass accessibility, usability, and personalization, aligning with user expectations. Stricter data privacy regulations will emphasize compliance testing, and emerging technologies like blockchain and smart contracts will require specialized validation methods. In essence, the future of web application testing will be characterized by innovation, integration, and an unwavering focus on cybersecurity.

- **Stage 2 :- future scope of testing process**

  The future scope of the testing process is poised for significant transformation driven by advancing technology and evolving software development practices. Key trends include the shift towards early testing and continuous feedback through Shift Left and DevTestOps approaches, automation and AI-driven testing for enhanced efficiency, and a growing emphasis on performance engineering, security validation, and compliance testing. As IoT, wearables, AR/VR, and multi-platform applications become more prevalent, testing will extend to these domains, ensuring seamless functionality and user experience. Additionally, codeless and low-code testing tools will empower non-technical users, while metrics-driven quality assurance and context-driven testing will guide testing strategies. The future testing landscape will be characterized by integration, automation, and adaptability, ensuring software quality and security in a rapidly evolving technological landscape.

- **Stage 3 :- future scope of SOC**

  The future scope of Security Operations Centers (SOCs) is undergoing significant evolution, driven by technological advancements and the evolving cybersecurity landscape. SOCs are set to embrace automation and orchestration for streamlined operations, while artificial intelligence and machine learning will enhance threat detection and response. Proactive threat hunting, cloud security, and Zero Trust architecture will become integral to SOC strategies. Collaborative threat sharing, user behavior analytics, and compliance with regulations will shape SOC practices. Additionally, SOCs will adapt to the challenges posed by IoT, OT, and integrated security platforms, while continuous skills development and incident response services will ensure SOC teams remain at the forefront of effective cyber defense.

- **SEIM**

  The future scope of Security Information and Event Management (SIEM) systems is characterized by technological advancements and evolving security requirements. SIEM is expected to embrace

advanced analytics, artificial intelligence, and machine learning for real-time threat detection and response. It will focus on behavioral analysis, user-centric monitoring, and proactive threat hunting, while also adapting to cloud, hybrid, and IoT environments. Automation, orchestration, and integration with other security tools, such as SOAR platforms, will enhance incident response. SIEM's role in regulatory compliance, real-time monitoring, and machine-to-machine communication will remain pivotal. As a cornerstone of cybersecurity strategies, SIEM systems will continue to provide comprehensive visibility, analysis, and proactive defense against evolving cyber threats.

Topics explored :- CEH course, Certified Ethical Hacker, Vulnerability analysis, Social Engineering, Hacking Web applications, Security operations center.
Tools explored :-Burp suite, Nessus, Qradar, mobaxterm, metasploitable

—--------THE END —----------