Project Report

Candidate : S.Kathimathi

Institution : VIT Chennai

STAGE 1 OVERVIEW REPORT

Title: Cyber security Defender

1. Overview

Web application security testing is a broad process that includes a multitude of processes that enable security testing of a Web application. It is a systematic process that starts from identifying and scoping the entire application, followed by planning multiple tests. Typically, Web application security testing is performed after the Web application is developed. The Web application undergoes a rigorous testing process that includes a series of fabricated malicious attacks to see how well the Web application performs/responds. The overall security testing process is generally followed by a format report that includes the identified vulnerabilities, possible threats and recommendations for overcoming the security shortfalls.

Some of the processes within the testing process include:

- Brute force attack testing
- Password quality rules
- Session cookies
- User authorization processes
- SQL injection

Web application security also helps us to:

- Identify flaws and vulnerabilities in your application:
- Comply with laws:
- Analyze your current security:
- Detect security breaches and anomalous behavior:
- Formulate an effective security plan:

2. List of Vulnerability Table

S.no	Vulnerability Name	CWE - No
1	Broken Access Control	CWE -284 - Improper Access Control
2	Cryptographic Failures	CWE-327 - Use of a Broken or Risky Cryptographic Algorithm
3	Injection	CWE-89 - Improper Neutralization of Special Elements used in an SQL Command
4	Insecure Design	CWE-657 - Violation of Secure Design Principles
5	Security Misconfiguration	CWE-16 - Configuration
6	Vulnerable and Out-dated Components	CWE-1104 – Use of unmaintained Third party components
7	Identification and Authentication Failures	CWE- 287 – Improper Authentication
8	Software and Data Integrity Failures	CWE-494 - Download of Code without Integrity Check
9	Security Logging and Monitoring Failures	CWE-532 - Insertion of Sensitive Information into Log File
10	Server-Side Request Forgery	CWE-918 - Request Forgery attack (SSRF)

3. Vulnerability Report

1. **Vulnerability Name: Broken Access control**

   CWE: CWE-284 Improper Access Control

   OWASP Category: A01:2021

   Description: The restriction of access is less it provide easily access without many restrictions

   Business Impact: In business its access can be very devastated for the user as it can easily give access to hacker which can change or delete accounts.

2. **Vulnerability Name: Cryptographic Failures**

   CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm

   OWASP Category: A02:2021

   Description: Using such an algorithm means that an attacker may be able to easily decrypt the encrypted data.

   Business Impact: Attempting to create non-standard and non-tested algorithms, using weak algorithms, or applying algorithms incorrectly will pose a high weakness to data that is meant to be secure.

3. **Vulnerability Name: Injection**

   CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command

   OWASP Category: A03:2021

   Description: Using such an algorithm means that an attacker may be able to easily decrypt the encrypted data.

   Business Impact: The unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

4. **Vulnerability Name: Insecure Design**

   CWE: CWE-657: Violation of Secure Design Principles

   Description: It is related to critical design and architectural flaws in web applications that hackers can exploit.

Business Impact: Failing to do so can lead to flaws that threaten your organizational security, compromising sensitive data, granting privileges to individuals who can abuse them, and more.

5. **Vulnerability Name: Security Misconfiguration**

CWE: CWE-16 Configuration

Description: A security misconfiguration occurs when system or application configuration settings are missing or are erroneously implemented, allowing unauthorized access.

Business Impact: Security misconfigurations allow attackers to gain unauthorized access to networks, systems and data, which in turn can cause significant monetary and reputational damage to your organization.

6. **Vulnerability Name: Vulnerable and Out-dated Components**

CWE: CWE-1104

OWASP Category: A06:2021

Description: Use of Unmaintained Third Party Components

Business Impact: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

7. **Vulnerability Name: Identification and Authentication Failures**

CWE: CWE-287 Improper Authentication

OWASP Category: A06:2021

Description: When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.

Business Impact: Improper authentication can lead to various security threats, such as: Data breaches: Improper authentication can allow unauthorized users to gain access to sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.

8. **Vulnerability Name: Software and Data Integrity Failures**

   CWE: CWE-494

   OWASP Category: A06:2021

   Description: Download of Code without Integrity Check

   Business Impact: The product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code.

9. **Vulnerability Name: Security Logging and Monitoring Failures**

   CWE: CWE-532

   OWASP Category: A06:2021

   Description: Insertion of Sensitive Information into Log File

   Business Impact: Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information. Sensitive data exposure can be financially costly to your business and damage your reputation and brand. The type of data at risk of exposure includes financial reports, bank account numbers, credit card numbers, usernames, passwords, customers' personal details, and healthcare information.

10. **Vulnerability Name: Server-Side Request Forgery (SSRF)**

    CWE: CWE-918

    OWASP Category: A06:2021

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. A Server-Side Request Forgery attack (SSRF) is a security vulnerability in which a hacker tricks a server into accessing unintended resources on his behalf. An SSRF attack can lead to sensitive information being leaked or the attacker gaining control of other systems.

Business Impact: In some situations, the SSRF vulnerability might allow an attacker to perform arbitrary command execution. An SSRF exploit that causes connections to external third-party systems might result in malicious onward attacks that appear to originate from the organization hosting the vulnerable application.

.

STAGE 2 : NESSUS VULNERABILITY REPORT

1. Overview

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

Features of Nessus

- Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.
- Nessus is very extensible, providing a scripting language for you to write tests specific to your system once you become more familiar with the tool. It also provides a plug-in interface, and many free plug-ins are available from the Nessus plug-in site.   These plugs are often specific to detecting a common virus or vulnerability.
- Up to date information about new vulnerabilities and attacks. The Nessus team updates the list of what vulnerabilities to check for on a daily basis in order to minimize the window between an exploit appearing in the wild, and you being able to detect it with Nessus.
- Open-source. Nessus is open source, meaning it costs nothing, and free to see and modify the source as needed.
- Patching Assistance: When Nessus detects a vulnerability, it is also most often able to suggest the best way that can mitigate the vulnerability.

Working of Nessus

Most high-level network traffic, such as email, web pages, etc reach a server via a high-level protocol that is transmitted reliably by a TCP stream. To keep different streams from interfering with each other, a computer divides its physical connection to the network into thousands of logical paths, called ports. So if you want to talk to a web server on a given machine, you would connect to port #80 (the standard HTTP port), but if you wanted to connect to an SMTP server on that same machine you would instead connect to port #25. Each computer has thousands of ports, all of which may or may not have services (ie: a server for a specific high-level protocol) listening on them. Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack. Nessus is called a "remote scanner" because it does not need to be installed on a computer for it to test that computer. Instead, it can be installed on only one computer and tested in as many computers needed.

Target website : www.vvcoe.org
Target IP address : 166.62.28.89 (ipv4)

List of vulnerability

S. no	**Vulnerability name**	**Severity**	**Plugins**	**Port**
1	CSP: Wildcard Directive	Medium	10055	443
2	Absence of Anti-CSRF Tokens	Medium	10202	993
3	Content Security Policy (CSP) Header Not Set	Medium	10038	995
4	Missing Anti-clickjacking Header	Medium	10020	2077
5	Vulnerable JS Library	Medium	10003	2078
6	Cookie Without Secure Flag	Low	10011	2082
7	Cookie No HttpOnly Flag	Low	10010	2083
8	X-Content-Type-Options Header Missing	Low	10021	2095
9	Strict-Transport-Security Header Not Set	Low	10035	3306
10	Server Leaks Version Information via "Server" HTTP Response Header Field	Low	10036	3307

Detailed Report About Each Vulnerability Listed In The Table

1. Vulnerability Name:- CSP: Wildcard Directive

Description:- Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:- Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

Business Impact::- Gain Privileges or Assume Identity It is dangerous to use cookies to set a user's privileges. The cookie can be manipulated to escalate an attacker's privileges to an administrative level.

2. Vulnerability Name:- Absence of Anti-CSRF Tokens

Description:- No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

Solution:- Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Business Impact::- The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.

3. Vulnerability Name:- Content Security Policy (CSP) Header Not Set

Description:- Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:- Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Business Impact::- The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. Please note that CWE definitions are provided as a quick reference only.

4. Vulnerability Name:- Missing Anti-clickjacking Header

Description:- The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

Solution:- Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Business Impact::- An attacker can trick a user into performing actions that are masked and hidden from the user's view. The impact varies widely, depending on the functionality of the underlying application

5. Vulnerability Name:- Vulnerable JS Library

Description:- The identified library jquery-ui, version 1.10.2 is vulnerable.

Solution:- Please upgrade to the latest version of jquery-ui.

Business Impact::- An attacker could insert malicious functionality into the program by causing the program to download code that the attacker has placed into the untrusted control sphere, such as a malicious web site.

6. Vulnerability Name:- Cookie Without Secure Flag

Description:- A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:- Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Business Impact::- A product does not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in plaintext over an HTTP session with the product.

7. Vulnerability Name:- Cookie No HttpOnly Flag

Description:- A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

Solution:- Ensure that the HttpOnly flag is set for all cookies.

Business Impact::- If the HttpOnly flag is not set, then sensitive information stored in the cookie may be exposed to unintended parties.

8. Vulnerability Name:- X-Content-Type-Options Header Missing

Description:- The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIMEsniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Solution:- Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Business Impact::- The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.

9. Vulnerability Name:- Strict-Transport-Security Header Not Set

Description:- HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Solution:- Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Business Impact::- The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

10. Vulnerability Name:- Server Leaks Version Information via "Server" HTTP Response Header Field

Description:- The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:- Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Business Impact::- Loss of confidentiality in the business

STAGE 3 : ENHANCING SECURITY USING SOC AND SIEM INTEGRATION

1) SOC

A security operations center (SOC) – sometimes called an information security operations center, or ISOC – is an in-house or outsourced team of IT security professionals that monitors an organization's entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible.

An SOC also selects, operates, and maintains the organization's cybersecurity technologies, and continually analyzes threat data to find ways to improve the organization's security posture.

The chief benefit of operating or outsourcing an SOC is that it unifies and coordinates an organization's security tools, practices, and response to security incidents. This usually results in improved preventative measures and security policies, faster threat detection, and faster, more effective and more cost-effective response to security threats. An SOC can also improve customer confidence, and simplify and strengthen an organization's compliance with industry, national and global privacy regulations.

2) SOC – cycle

The SOC (Security Operations Center) cycle, also known as the SOC lifecycle or SOC workflow, is a continuous process that outlines the key steps involved in managing an organization's cybersecurity. It encompasses activities from threat detection to incident response and recovery. The SOC cycle typically consists of the following stages:

i) Threat Detection and Monitoring: Continuous monitoring of the organization's network, systems, and applications to identify potential security threats and anomalies. Leveraging various security tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, SIEM (Security Information and Event Management) solutions, and threat intelligence feeds.

ii) Alert Triage and Analysis: Analyzing and prioritizing security alerts generated by the monitoring tools based on their severity and potential impact. Determining if an alert indicates a genuine security incident or a false positive.

iii) Incident Investigation and Response: If an alert is confirmed as a legitimate security incident, the SOC team conducts a thorough investigation to understand the nature and extent of the attack. Gathering evidence, analyzing log data, and performing digital forensics to determine the source and impact of the incident. Initiating the incident response process, which may involve isolating affected systems, containing the threat, and preventing further damage.

iv) Incident Containment and Eradication: Taking immediate actions to contain the incident and prevent it from spreading further within the organization's network. Removing the malicious elements and eradicating the threat to restore the affected systems to a secure state.

v) Recovery and Remediation: After the threat is eradicated, the SOC team focuses on restoring affected systems and services to normal operation. Implementing remediation measures to address the root cause of the incident and prevent similar attacks in the future.

vi) Post-Incident Analysis and Lessons Learned: Conducting a thorough post-mortem analysis of the incident to understand how it happened, what was the impact, and what steps were taken to respond. Identifying areas of improvement in the organization's security posture and incident response procedures. Updating security policies and procedures based on the lessons learned from the incident.

vii) Threat Intelligence and Proactive Measures: Integrating threat intelligence into the SOC workflow to stay ahead of emerging threats and known attack patterns. Proactively hunting for signs of potential threats and vulnerabilities before they lead to full-fledged security incidents.

viii) Continuous Monitoring and Improvement: The SOC cycle is a continuous process, with ongoing monitoring, analysis, and improvement of security measures to adapt to the evolving threat landscape. By following this cycle, the SOC team can effectively detect, respond to, and recover from security incidents, minimizing the impact of cyber threats on the organization's assets and data.

3) SIEM

SIEM Security information and event mangement, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response. Benefits Regardless of how large or small an organization may be, taking proactive steps to monitor for and mitigate IT security risks is essential. SIEM solutions benefit enterprises in a variety of ways and have become a significant component in streamlining security workflows.

Real-time threat recognition

SIEM solutions enable centralized compliance auditing and reporting across an entire business infrastructure. Advanced automation streamlines the collection and analysis of system logs and security events to reduce internal resource utilization while meeting strict compliance reporting standards.

AI-driven automation

Today's next-gen SIEM solutions integrate with powerful security orchestration, automation and response (SOAR) systems, saving time and resources for IT teams as they manage business security. Using deep machine learning that automatically learns from network behavior, these solutions can handle complex threat identification and incident response protocols in significantly less time than physical teams.

Improved organizational efficiency

Because of the improved visibility of IT environments that it provides, SIEM can be an essential driver of improving interdepartmental efficiencies. A central dashboard provides a unified view of system data, alerts and notifications, enabling teams to communicate and collaborate efficiently when responding to threats and security incidents.

Detecting advanced and unknown threats

Considering how quickly the cybersecurity landscape changes, organizations need to be able to rely on solutions that can detect and respond to both known and unknown security threats. Using integrated threat intelligence feeds and AI technology, SIEM solutions can help security teams respond more effectively to a wide range of cyberattacks including: Insider threats - security vulnerabilities or attacks that originate from individuals with authorized access to company networks and digital assets. Phishing - messages that appear to be sent by a trusted sender, often used to steal user data, login credentials, financial information, or other sensitive business information. Ransomware - malware that locks a victim's data or device and threatens to keep it locked—or worse—unless the victim pays a ransom to the attacker. Distributed denial of service (DDoS) attacks - attacks that bombard networks and systems with unmanageable levels of traffic from a distributed network of hijacked devices (botnet), degrading performance of websites and servers until they are unusable. Data exfiltration – theft of data from a computer or other device, conducted manually, or automatically using malware.

Conducting forensic investigations

SIEM solutions are ideal for conducting computer forensic investigations once a security incident occurs. SIEM solutions allow organizations to efficiently collect and analyze log data from all of their digital assets in one place. This gives them the ability to recreate past incidents or analyze new ones to investigate suspicious activity and implement more effective security processes. Assessing and reporting on compliance Compliance auditing and reporting is both a necessary and challenging task for many organizations. SIEM solutions dramatically reduce the resource expenditures required to manage this process by providing real-time audits and on-demand reporting of regulatory compliance whenever needed. Monitoring Users and Applications With the rise in popularity of remote workforces, SaaS applications and BYOD (bring your own device) policies, organizations need the level of visibility necessary to mitigate network risks from outside the traditional network perimeter. SIEM solutions track all network activity across all users, devices, and applications, significantly improving transparency across the entire infrastructure and detecting threats regardless of where digital assets and services are being accessed.

Five Predictions For The Future Of SIEM

1. Usage-based pricing models will become the norm. With these models, teams only pay for precisely the data throughput and processing incurred each month. This trend follows suit with cloud infrastructure platforms such as AWS and GCP and gives predictability to service usage. Pressure for security teams to reduce the amount of data they use will become a thing of the past.
2. The decoupling of SIEM platforms — which has already started with SOAR coming from SIEM and other extract, transform and load (ETL) tools — will continue, and I suspect that the next phase would be building analysis tools on top of a universal SIEM

data platform. This way, the companies building tools can focus on specific verticals and produce the most robust, high-quality and scalable software possible.

3. As decoupling continues to occur, security companies will create strong partnerships to provide an elegant integration and improve the time-to-value. These partnerships should help push the security industry forward, help with mutual company growth by referring customers to each other and ensure security teams have the best possible user experience.
4. The cost and complexity of a SIEM will continue to be reduced (per the availability of cloud services), enabling smaller and newer security teams to get up to speed even quicker. With legacy SIEMs, it could take teams more than six months to get started, which means data onboarding, analysis and alerting integrations are non-trivial. Next-gen SIEMs can improve quality and simplicity, enabling security teams to move quickly and focus on the work that matters. This trend will continue to reduce startup time, which is critical for a business's bottom line and a security team's efficiency.
5. More startups will continue to be funded to address the multifaceted challenges of upholding strong security. Venture funding is at an all-time high, and security breaches continue to be an issue for organizations of all sizes — including the large, sophisticated Fortune 1000 companies. Healthy competition means that not a single company will own a majority of the market share. This competition gives security teams optionality and the freedom to move to other platforms as they see fit. Then, the battle will become about ease of use, capabilities and flexibility.

4) SIEM Cycle

The lifecycle of a Security Information and Event Management (SIEM) system involves several interconnected stages that ensure the effective implementation, operation, and maintenance of the SIEM solution. The SIEM life cycle typically includes the following phases:

a) Planning and Assessment: Define the objectives and scope of the SIEM implementation, considering the organization's security requirements and compliance goals. Conduct a thorough assessment of the existing security infrastructure, data sources, and log management practices to identify gaps and necessary improvements. Develop a detailed plan for deploying the SIEM solution, including resource allocation, timeline, and responsibilities

b) Design and Architecture: Design the SIEM architecture based on the organization's requirements and data sources, considering factors like scalability, redundancy, and performance. Determine the best deployment model (on-premises, cloud-based, hybrid) that aligns with the organization's needs and resources. Plan the integration of data sources into the SIEM, ensuring that relevant security events are collected and centralized for analysis.

c) Data Collection and Integration: Implement data collectors and agents to gather logs and events from various sources, such as firewalls, network devices, servers, applications, and endpoints. Normalize and enrich the collected data to facilitate efficient analysis and correlation. Configure connectors and parsers to integrate data feeds from security devices and other sources into the SIEM platform.

d) Event Correlation and Analysis: Develop and fine-tune correlation rules and use cases to identify patterns of malicious activity and security threats. Conduct real-time event correlation and analysis to generate actionable alerts for potential security incidents. Utilize threat intelligence feeds to enhance the SIEM's ability to detect emerging threats and known attack vectors.

e) Incident Detection and Response: Respond to generated alerts by investigating potential security incidents. Perform detailed analysis to determine the scope and impact of identified security events. Initiate incident response activities, including containment, eradication, and recovery. Forensics and Investigation: Conduct in-depth forensics analysis to understand the root cause of incidents and the methods used by attackers. Preserve and document evidence for potential legal or regulatory purposes. Reporting and Compliance: Generate and present security reports and dashboards for various stakeholders, including IT management, executives, auditors, and regulatory authorities. Ensure compliance with relevant industry standards and regulations by monitoring and reporting on security events and incidents. Continuous Monitoring and Maintenance: Continuously monitor the SIEM infrastructure and adjust the configuration as needed to maintain optimal performance. Regularly update correlation rules, threat intelligence feeds, and other components to keep the SIEM effective against evolving threats. Conduct periodic reviews and assessments of the SIEM's performance and effectiveness to identify areas for improvement.

f) Training and Knowledge Transfer: Train SOC personnel and IT staff on the effective use of the SIEM solution. Foster knowledge sharing and best practices from incident investigations and analysis within the organization. The SIEM lifecycle is a continuous and iterative process, with each phase building upon the insights and experiences gained from previous stages. This approach ensures that the SIEM solution remains relevant, efficient, and effective in helping organizations detect and respond to security threats. As a syslog server incessantly pings with every security notification, security teams can feel as though they are drowning in a sea of security warnings. Without a SIEM, it’s difficult to know which events are truly critical and which can be ignored. However, when a SIEM has been implemented, security teams get a much clearer picture of their environment’s security. There could truly be no threats, or multiple incidents may be occurring that simply have not yet affected performance.

5) MISP

MISP, Malware Information Sharing Platform and Threat Sharing, core functionalities are: An efficient IOC and indicators database, allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.

Features of MISP, the open source threat sharing platform A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. Discover how MISP is used today in multiple organisations. Not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organisations or people. An efficient IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence. Automatic correlation finding relationships between attributes and indicators from malware, attacks campaigns or analysis. Correlation engine includes correlation between attributes and more advanced correlations like Fuzzy hashing correlation (e.g. ssdeep) or CIDR block matching. Correlation can be also enabled or event disabled per attribute. A flexible data model where complex objects can be expressed and linked together to express threat intelligence, incidents or connected elements. Built-in sharing functionality to ease data sharing using different models of distributions. MISP can synchronize automatically events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a flexible sharing group capacity and an attribute level distribution mechanism. An intuitive user-interface for end-users to create, update and collaborate on events and attributes/indicators. A graphical interface to navigate seamlessly between events and their correlations. An event graph functionality to create and view relationships between objects and attributes. Advanced filtering functionalities and warning list to help the analysts to contribute events and attributes. storing data in a structured format (allowing automated use of the database for various purposes) with an extensive support of cyber security indicators along fraud indicators as in the financial sector. export: generating IDS (Suricata, Snort and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools import: bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV or MISP format. Flexible free text import tool to ease the integration of unstructured reports into MISP. A gentle system to collaborate on events and attributes allowing MISP users to propose changes or updates to attributes/indicators. Data-sharing: automatically exchange and synchronization with other parties and trust-groups using MISP. Feed import: flexible tool to import and integrate MISP feed and any threatintel or OSINT feed from third parties. Many default feeds are included in standard MISP installation. Delegating of sharing: allows a simple pseudo-anonymous mechanism to delegate publication of event/indicators to another organization. Flexible API to integrate MISP with your own solutions. MISP is bundled with PyMISP which is a flexible Python Library to fetch, add or update events attributes, handle malware samples or search for attributes. Adjustable taxonomy to classify and tag events following your own classification schemes or existing taxonomies. The taxonomy can be local to your MISP but also shareable among MISP instances. MISP comes with a default set of well-known taxonomies and classification schemes to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organizations. Intelligence vocabularies called MISP galaxy and bundled with existing threat actors, malware, RAT, ransomware or MITRE ATT&CK which can be easily linked with events in MISP. Expansion modules in Python to expand MISP with your own services or activate already available misp-modules. sighting support to get observations from organizations concerning shared indicators and attributes. Sighting can be contributed via MISP user-interface, API as

MISP document or STIX sighting documents. Starting with MISP 2.4.66, Sighting has been extended to support false-negative sighting or expiration sighting. STIX support: export data in the STIX format (XML and JSON) including export/import in STIX 2.0 format. integrated encryption and signing of the notifications via PGP and/or S/MIME depending on the user preferences. Real-time publish-subscribe channel within MISP to automatically get all changes (e.g. new events, indicators, sightings or tagging) in ZMQ (e.g. misp-dashboard) or Kafka. Sharing with humans Data you store is immediately available to your colleagues and partners. Store the event id in your ticketing system or be informed by the signed and encrypted email notifications. Sharing with machines By generating Snort/Suricata/Bro/Zeek IDS rules, STIX, OpenIOC, text or csv exports MISP allows you to automatically import data in your detection systems resulting in better and faster detection of intrusions. Importing data can also be done in various ways: free-text import, OpenIOC, batch import, sandbox result import or using the preconfigured or custom templates. If you run MISP internally, data can also be uploaded and downloaded automagically from and to externally hosted MISP instances. Thanks to this automation and the effort of others you are now in possession of valuable indicators of compromise with no additional work. Collaborative sharing of analysis and correlation How often has your team analyzed to realize at the end that a colleague had already worked on another, similar, threat? Or that an external report has already been made? When new data is added MISP will immediately show relations with other observables and indicators. This results in more efficient analysis, but also allows you to have a better picture of the TTPs, related campaigns and attribution.

6) Your college network information

- **10 Labs with nearly 500 systems**

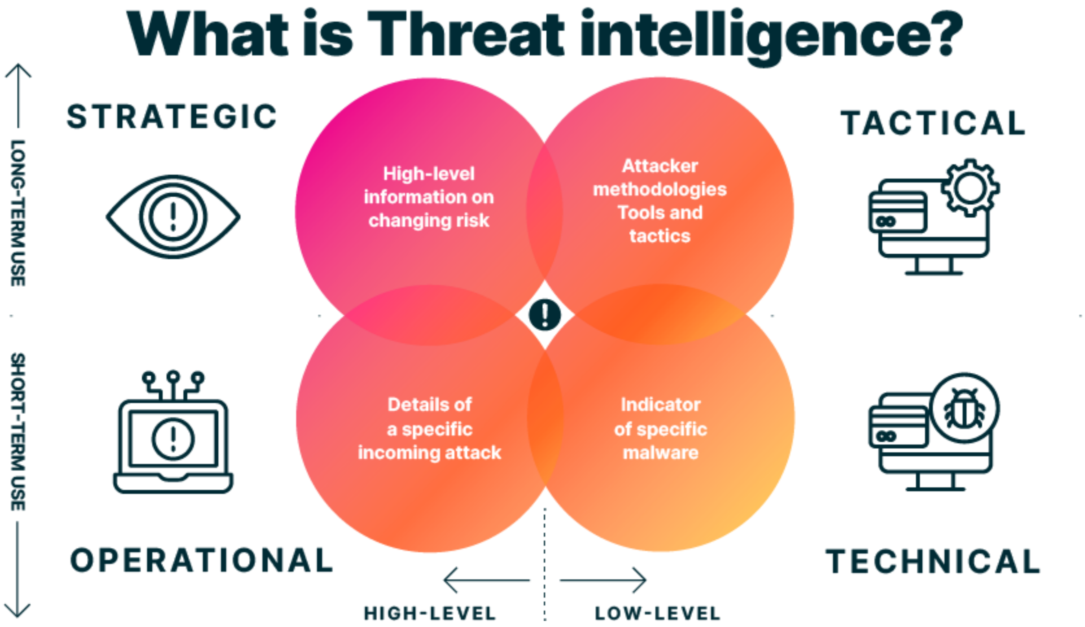
7) How you think you deploy soc in your college

1. Identify the purpose and scope of the lab. Determine what types of security threats and scenarios wanted to be tested and simulated.
2. Gather the necessary equipment and software. This might include a computer or server, virtualization software (such as VMware or VirtualBox), and various security tools and software (such as IDS/IPS, firewall, and SIEM).
3. Set up a virtualized environment. Use virtualization software to create multiple virtual machines that can be used to simulate different parts of the network and test different security scenarios.
4. Configure and test the security tools and software. Set up and configure the various security tools and software you have gathered, and test them to ensure they are working as expected.
5. Build out the lab environment. Create a network topology that mimics the type of network want to be protected, and populate it with virtual machines that represent different types of devices and servers.

6. Test and refine the lab. Use the lab to test different security scenarios and attack vectors, and use the results to refine and improve your security posture.
7. Keep the lab environment updated. Keep the software and tools updated and current, and regularly evaluate and update your lab's security posture.

8) Threat intelligence

Threat intelligence is **data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors**. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.


What is Threat intelligence?
STRATEGIC
TACTICAL
OPERATIONAL
TECHNICAL
LONG-TERM USE
SHORT-TERM USE
High-level information on changing risk
Attacker methodologies Tools and tactics
Details of a specific incoming attack
Indicator of specific malware
HIGH-LEVEL
LOW-LEVEL

Importance of Threat Intelligence

In the world of cybersecurity, advanced persistent threats (APTs) and defenders are constantly trying to outmaneuver each other. Data on a threat actor's next move is crucial to proactively tailoring your defenses and preempt future attacks.

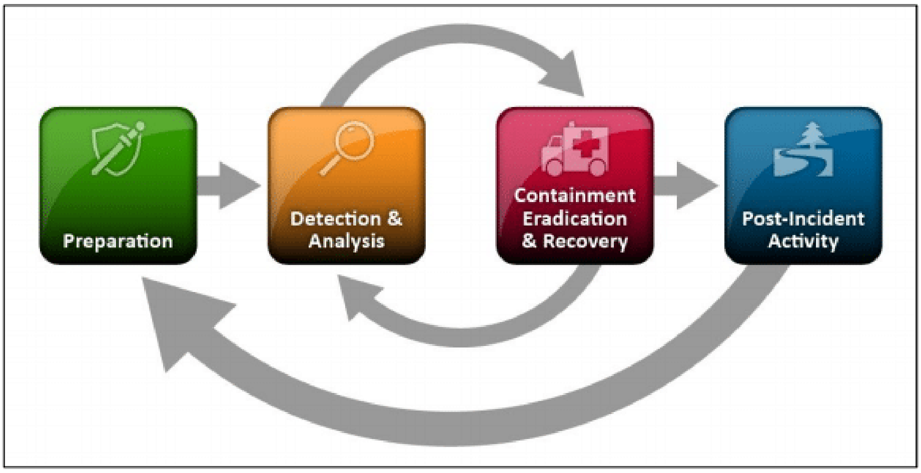
Organizations are increasingly recognizing the value of threat intelligence, with 72 percent planning to increase threat intelligence spending in upcoming quarters.

However, there is a difference between recognizing value and receiving value. **Most organizations today are focusing their efforts on only the most basic use cases**, such as integrating threat data feeds with existing network, IPS, firewalls, and SIEMs — without taking full advantage of the insights that intelligence can offer

9) Incident response

Incident response (sometimes called cyber security incident response) refers to an organization's processes and technologies for detecting and responding to cyber threats, security breaches or cyber-attacks. The goal of incident response is to prevent cyber-attacks before they happen, and to minimize the cost and business disruption resulting from any cyber-attacks that occur.

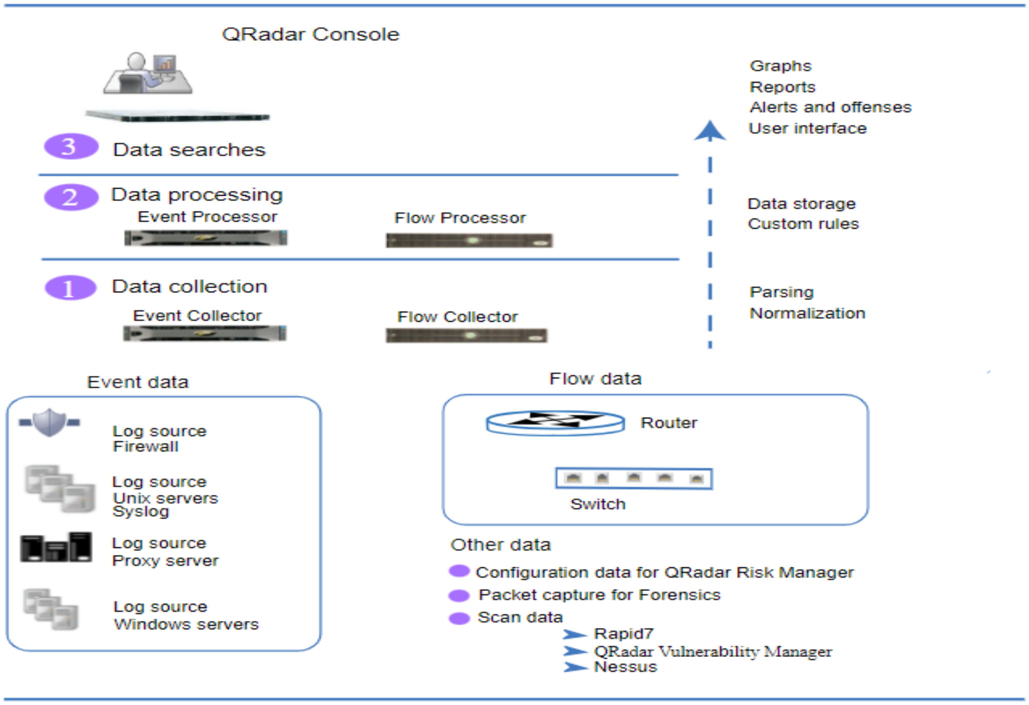
Ideally, an organization defines incident response processes and technologies in a formal incident response plan (IRP) that specifies exactly how different types of cyber-attacks should be identified, contained, and resolved. An effective incident response plan can help cyber security teams detect and contain cyber threats and restore affected systems faster, and reduce the lost revenue, regulatory fines and other costs associate with these threats. IBM's *Cost of a Data Breach 2022 Report* found that organizations with incident response teams and regularly tested incident response plans had an average data breach cost USD 2.66 million lower than that of organizations without incident response teams and IRPs. The below diagram shows the process of Incident response.



10) Qradar & understanding about tool

The operation of the QRadar security intelligence platform consists of three layers, and applies to any QRadar deployment structure, regardless of its size and complexity. The following diagram shows the layers that make up the QRadar architecture.

The QRadar architecture functions the same way regardless of the size or number of components in a deployment. The following three layers that are represented in the diagram represent the core functionality of any QRadar system.



1) Data collection Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data. The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format. The core functionality of QRadar SIEM is focused on event data collection, and flow collection. Event data represents events that occur at a point in time in the user's environment such as user logins, email, VPN connections, firewall denys, proxy connections, and any other events that you might want to log in your device logs. Flow data is network activity information or session information between two hosts on a network, which QRadar translates in to flow records. QRadar translates or normalizes raw data in to IP addresses, ports, byte and packet counts, and other information into flow records, which effectively represents a session between two hosts. In addition to collecting flow information with a Flow Collector, full packet capture is available with the QRadar Incident Forensics component.

2) Data processing After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage. Event data, and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you might need to add Event Processors, Flow Processors or any other processing appliance to handle the additional requirements. You might also need more storage capacity, which can be handled by adding Data Nodes. Other features such as QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM), or QRadar Incident Forensics collect different types of data and provide more functions. QRadar Risk Manager collects network infrastructure configuration, and provides a map of your network topology. You can use the data to manage risk by simulating various network scenarios through altering configurations and implementing rules in your network. Use QRadar Vulnerability Manager to scan your network and process the vulnerability data or manage the vulnerability data that is collected from other scanners such as Nessus, and Rapid7. The vulnerability data that is collected is used to identify various security risks in your network. Use QRadar Incident Forensics to perform in-depth forensic investigations, and replay full network sessions.

3) Data searches In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search, and manage the security admin tasks for their network from the user interface on the QRadar Console. In an All-in-One system, all data is collected, processed, and stored on the All-in-One appliance. In distributed environments, the QRadar Console does not perform event and flow processing, or storage. Instead, the QRadar Console is used primarily as the user interface where users can use it for searches, reports, alerts, and investigations.

QRadar components Use IBM QRadar components to scale a QRadar deployment, and to manage data collection and processing in distributed networks.

QRadar maximum EPS certification methodology IBM QRadar appliances are certified to support a certain maximum events per second (EPS) rate. Maximum EPS depends on the type of data that is processed, system configuration, and system load.

QRadar events and flows The core functions of IBM QRadar SIEM are managing network security by monitoring flows and events.

Conclusion

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

The outcome of web application testing is to ensure that the application is secure, reliable, and meets its intended functionality. The testing process aims to identify and address potential vulnerabilities, bugs, and usability issues that could impact the application's performance and user experience.

The specific outcomes of web application testing include:

- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Compatibility Testing Insights
- Accessibility Compliance
- Security Compliance and Risk Mitigation

- Optimization Recommendations
- Enhanced Quality Assurance
- Increased Customer Confidence
- Compliance with Regulatory Requirements

In summary, the outcome of web application testing is an enhanced, secure, and reliable web application that meets user expectations and delivers a smooth and seamless experience to its users. It provides developers and stakeholders with the confidence that the application is ready for deployment and can withstand potential security threats and performance challenges.

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

Nessus is a vulnerability scanning tool used to identify and report security issues in computer systems and networks. The outcome of a Nessus report will depend on the specific target scanned and the vulnerabilities found. Typically, a Nessus report will list the identified vulnerabilities along with their severity levels, detailed descriptions, and recommendations for remediation. The severity levels are usually categorized as critical, high, medium, and low, depending on the potential impact and exploitability of the vulnerability.

Stage 3 :- what you understand from SOC / SEIM / Qradar Dashboard.

a) SOC (Security Operations Center): The primary purpose of a SOC is to monitor and defend an organization's IT infrastructure against security threats and incidents. SOC analysts use various tools and technologies to detect, analyze, and respond to security events in real-time.

The expected outcomes of a well-functioning SOC include:

a. Improved Threat Detection: SOC analysts monitor network traffic, log data, and security alerts to identify potential threats and security incidents promptly.

b. Faster Incident Response: With a SOC in place, organizations can respond quickly to security incidents and mitigate the impact of breaches or attacks.

c. Enhanced Security Posture: A proactive SOC helps organizations implement robust security measures and continually improve their overall security posture.

d. Reduced Downtime and Losses: Detecting and mitigating security incidents swiftly can minimize downtime and financial losses resulting from cyber-attacks.

b) SIEM (Security Information and Event Management):

SIEM is a technology that helps collect, analyze, and correlate log data from various sources within an organization's IT environment. The main goal of SIEM is to provide a centralized platform for real-time monitoring, threat detection, and incident response. The expected outcomes of using a SIEM system are

- Centralized Log Management
- Early Threat Detection
- Simplified Incident Investigation
- Compliance and Report

c) QRadar Dashboard (IBM QRadar):

QRadar is a popular SIEM solution provided by IBM. The QRadar dashboard is a critical component of the QRadar system, offering a visual representation of security-related data and insights. The expected outcomes of using QRadar and its dashboard include:

- Real-Time Visibility
- Customizable Visualizations
- Threat Intelligence Integration
- Incident Response Automation

Future Scope

Stage 1 :- Future scope of web application testing

The future scope of web application testing will be shaped by technological advancements, changing user expectations, and the need to ensure security and reliability in an increasingly interconnected digital world. Testing professionals will need to adapt to these trends and continuously upgrade their skills to meet the evolving demands of web application testing.

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

The future scope of the testing process will see increased automation, integration with emerging technologies, and a focus on ensuring quality, security, and performance in the ever-evolving software landscape. Testing professionals will need to adapt to these changes and continuously upgrade their skills to stay relevant in the dynamic field of software testing.

Stage 3 :- future scope of SOC / SEIM

The future scope of SOC (Security Operations Center) and SIEM (Security Information and Event Management) is expected to expand and evolve in response to the changing cybersecurity landscape and technological advancements. The future scope of SOC and SIEM will involve increased automation, advanced threat detection, integration with emerging technologies, and a proactive approach to cybersecurity. Organizations will need to invest in the latest tools and technologies while continuously developing the expertise of their cybersecurity teams to stay ahead of evolving threats.

Topics explored

Introduction to cybersecurity, Growth of cybersecurity, Data sanity, Cloud service and cloud security, Data breach, Firewall, Antivirus, Digital ecosystem, Data protection, Types of cyber attacks, Essential terminology, Introduction to networking, Web APIs, web hooks, Web shell concepts, Vulnerability stack,OWASP top 10 applications, QRadar, SOC, SIEM.

Tools explored

Nessus, cybermap.kaspersky.com, thehackersone.com, chaptgpt, wepik.com (AI image editor), Gamma (AI based PPT), OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation, mobaxterm, tools-nmtui, Nmap, sqlmap, Identify fixes-wincollect agent, metasploitable, malware bytes, Linux cheatsheet, QRadar for SOC dashboard presentation, Kali linux