Project Title: OWSP Vulnerabilities

Part 1 Executive Summary

Overview :- The OWASP (Open Web Application Security Project) Top 10 Vulnerabilities list is a widely recognized standard for identifying the most critical security risks to web applications. This list is regularly updated by the OWASP community to reflect emerging threats and evolving attack vectors.

Understanding and addressing these vulnerabilities are essential for organizations to enhance the security posture of their web applications. By prioritizing remediation efforts based on the OWASP Top 10 list, organizations can mitigate risks, protect sensitive data, and maintain trust with users and stakeholders. Regular updates and proactive security measures are key to staying resilient against evolving cyber threats in today's dynamic threat landscape.

By identifying vulnerabilities within systems, applications, or networks, organizations can assess the potential risks they pose. This allows for informed decision-making regarding resource allocation for mitigation efforts. Prioritizing vulnerabilities based on their likelihood of exploitation and potential impact helps in allocating resources effectively to mitigate the most critical risks first.

Vulnerabilities can lead to breaches, data loss, operational disruptions, and even legal consequences. Understanding these risks enables organizations to implement measures to reduce the likelihood and impact of such incidents. This ensures continuity of operations and minimizes financial losses that may result from downtime, reputational damage, or regulatory fines.

Many industries are subject to regulations and standards that require organizations to protect sensitive information and maintain adequate cybersecurity measures. Understanding vulnerabilities helps organizations comply with these requirements, avoiding penalties and legal liabilities associated with data breaches or non-compliance.

Security breaches resulting from vulnerabilities can damage an organization's reputation and erode customer trust. Understanding vulnerabilities allows organizations to proactively protect sensitive data and demonstrate their commitment to security, thereby preserving customer confidence and loyalty.

Addressing vulnerabilities early in the development lifecycle or promptly after discovery is typically more cost-effective than dealing with the consequences of a security breach. Understanding vulnerabilities helps organizations prioritize investments in cybersecurity measures that mitigate risks and reduce potential financial impacts.

In summary, understanding vulnerabilities and their business impact enables organizations to implement proactive measures to protect their assets, maintain regulatory compliance, safeguard reputation and trust, and ensure continuity of operations. It's a critical aspect of effective risk management and cybersecurity strategy in today's interconnected and data-driven business environment.

List of teammates–

S.no	Name	Collage	Contact
1	Preeti Kathiria	Nirma University	preeti.kathiria@nirmauni.ac.in
2	Parita Oza	Nirma University	parita.prajapati@nirmauni.ac.in
3	Usha Patel	Nirma University	Ushapatel@nirmauni.ac.in
4	Zalak Jani	L. J University	zalak.jani@ljku.edu.in

List of Vulnerability Table:

S.no	Vulnerability Name	CWE - No
1	A01:2021-Broken Access Control	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
2	A02:2021-Cryptographic Failures	CWE-259: Use of Hard-coded Password
3	A03:2021-Injection	CWE-79: Cross-site Scripting
4	A04:2021-Insecure Design	CWE-256: Unprotected Storage of Credentials
5	A05:2021-Security Misconfiguration	CWE-16 Configuration
6	A06:2021-Vulnerable and Outdated Components	CWE-1104: Use of Unmaintained Third-Party Components
7	A07:2021-Identification and Authentication Failures	CWE-297: Improper Validation of Certificate with Host Mismatch
8	A08:2021-Software and Data Integrity Failures	CWE-829: Inclusion of Functionality from Untrusted Control Sphere
9	A09:2021-Security Logging and Monitoring Failures	CWE-117 Improper Output Neutralization for Logs
10	A10:2021-Server-Side Request Forgery	CWE-918:Server Side Request Forgery

REPORT:-

1. Vulnerability Name:- A01:2021-Broken Access Control

CWE : - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

OWASP/SANS Category:- OWASP 2021

Description:- The product contains a hard-coded password, which it uses for its own inbound authentication or for outbound communication to external components.

Business Impact::- The use of hard-coded passwords can lead to significant business impacts, including heightened risk of security breaches and unauthorized access, as well as regulatory non-compliance and associated fines. Additionally, it can cause operational inefficiencies and damage the company's reputation.

2. Vulnerability Name:- A202:2021 Cryptographic Failures

CWE :- CWE 259: Use of Hard-coded Password

OWASP/SANS Category:- OWASP 2021

Description:- We need to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

Business Impact::- The business impact of A02:2021 – Cryptographic Failures (formerly known as Sensitive Data Exposure) in software systems can be severe and multifaceted. Cryptographic failures refer to weaknesses or flaws in the implementation or use of cryptographic algorithms, protocols, and key management practices. Here are the primary business impacts: Data Breaches, Unauthorised access, Regulatory Non-compliance, Fines and Penalties, Incident Response Costs, System Downtime, Loss of Customer Trust, Brand Damage, Compensation Costs, Market Value Impact:

3. Vulnerability Name:- A03:2021-Injection

CWE : - CWE 79: Cross-site Scripting

OWASP/SANS Category:- OWASP 2021

Description:- Cross-Site Scripting (XSS) is a security vulnerability that allows attackers to inject malicious scripts into web pages viewed by users, leading to data theft, session hijacking, and

other malicious activities. This can significantly compromise the security and integrity of websites and user data.

Business Impact::-Cross-Site Scripting (XSS) can lead to significant business impacts, including loss of customer trust and reputational damage due to compromised user data and security breaches. Additionally, it can result in legal liabilities and financial losses from potential regulatory non-compliance and remediation costs.

4. Vulnerability Name:- A04:2021-Insecure Design

CWE : - CWE-256: Unprotected Storage of Credentials

OWASP/SANS Category:- OWASP 2021

Description:- Insecure Design refers to security flaws resulting from inadequate security controls and poor design choices in the software development lifecycle, leading to vulnerabilities exploitable by attackers. This encompasses a lack of threat modeling, secure design patterns, and adherence to best practices.

Business Impact::- Isecure Design can lead to increased risk of security breaches and data loss, causing financial losses and operational disruptions. It also undermines customer trust and can result in substantial legal and regulatory penalties.

5. Vulnerability Name:- A05:2021-Security Misconfiguration

CWE : CWE -16 Configuration

OWASP/SANS Category:- OWASP 2021

Description:- This refer to improper or insecure settings in software or hardware systems, potentially leading to vulnerabilities that can be exploited by attackers. These misconfigurations can result in unauthorized access, data breaches, and other security incidents.

Business Impact::- Configuration issues can lead to significant business impacts, including security breaches, operational disruptions, and financial losses. They also pose compliance risks and can damage an organization's reputation, resulting in loss of customer trust.

6. Vulnerability Name:- A06:2021-Vulnerable and Outdated Components

CWE:- CWE-1104: Use of Unmaintained Third-Party Components

OWASP/SANS Category:- OWASP 2021

Description:- This highlights security risks stemming from incorporating unsupported or unmaintained third-party software, emphasizing the importance of ongoing maintenance and updates to mitigate vulnerabilities effectively.

Business Impact:- The business impact of CWE-1104, focusing on the use of unmaintained third-party components, can be significant. Such components often lack necessary updates and patches, leaving systems vulnerable to security breaches and exploitation by malicious actors. This can lead to data breaches, financial losses due to downtime or remediation costs, and legal repercussions if sensitive information is compromised. Moreover, the reputational damage from being associated with a security incident can erode customer trust and loyalty, impacting long-term business viability. To mitigate these risks, businesses must implement robust software management practices, including regular audits and updates of third-party components, to ensure ongoing security and operational resilience.

7. Vulnerability Name:- A07:2021-Identification and Authentication Failures

CWE:- CWE-297: Improper Validation of Certificate with Host Mismatch

OWASP/SANS Category:- OWASP 2021

Description:- This refers to a vulnerability where software fails to properly validate a digital certificate's hostname against the hostname of the server it is connecting to. This can allow attackers to conduct man-in-the-middle attacks, intercepting and potentially altering communications between clients and servers, compromising the confidentiality and integrity of data.

Business Impact::- The business impact of CWE-297, which involves improper validation of certificates with host mismatches, can be severe. Such vulnerabilities can lead to attackers intercepting sensitive data transmitted between clients and servers, compromising confidentiality. This breach of trust can result in damaged customer relationships, loss of business credibility, and legal consequences if sensitive information like financial or personal data is exposed. Additionally, remediation efforts to fix the vulnerability may incur significant costs in terms of technical resources and operational downtime. To mitigate these risks, organizations must prioritize robust certificate validation practices and regularly update their security measures to protect against potential exploits.

8. Vulnerability Name:- A08:2021-Software and Data Integrity Failures

CWE : - CWE-829: Inclusion of Functionality from Untrusted Control Sphere

OWASP/SANS Category:- OWASP 2021

Description:- It refers to a vulnerability where software incorporates code or functionality from external, untrusted sources without adequate validation or safeguards. This can lead to security risks such as unauthorized access, data breaches, or compromise of the host system due to malicious or insecure code being executed within the application's environment.

Business Impact::- This involves the inclusion of functionality from an untrusted control sphere, can be significant. By incorporating code or functionality from unreliable or malicious sources, organizations risk exposing their systems to various threats such as data breaches, unauthorized access, and malware distribution. This can result in financial losses due to theft of intellectual property or sensitive information, operational disruptions leading to downtime and productivity losses, and reputational damage due to compromised customer trust and brand reputation. Additionally, remediation efforts to address these vulnerabilities may require extensive resources and time, impacting overall business agility and competitiveness. To mitigate these risks, businesses must implement strict controls for verifying and validating the integrity and security of third-party code before integration into their systems.

9. Vulnerability Name:- A09:2021-Security Logging and Monitoring Failures

CWE :- CWE-117 Improper Output Neutralization for Logs

OWASP/SANS Category:- OWASP 2021

Description:- It refers to a vulnerability where software fails to properly sanitize or neutralize input before logging it. This can allow attackers to inject malicious code or sensitive information into log files, potentially leading to unauthorized access, data leakage, or other security compromises.

Business Impact::- which involves improper output neutralization for logs, can be detrimental to business operations. If software fails to sanitize or neutralize input before logging, attackers can inject malicious content into log files. This could lead to unauthorized access to sensitive information, exposure of critical system details, and potential exploitation of vulnerabilities within the organization's infrastructure. The repercussions include compromised data integrity, regulatory non-compliance, damage to reputation, and financial losses due to remediation efforts, legal penalties, or loss of customer trust. To mitigate these risks, businesses must enforce rigorous input validation and output sanitization practices across their software applications to ensure the security and confidentiality of logged information.

10. Vulnerability Name:- A10:2021-Server-Side Request Forgery

CWE : - CWE-918:Server Side Request Forgery

OWASP/SANS Category:- OWASP 2021

Description:- Here an attacker can manipulate a web application into making unauthorized requests on behalf of the server itself. This can lead to information disclosure, unauthorized access to internal systems, and potential compromise of sensitive data or services that the server can access.

Business Impact::- Attackers exploiting SSRF can force a server to make unauthorized requests to internal systems or other external resources, potentially accessing sensitive data or services. This could lead to data breaches, financial losses due to theft of intellectual property or sensitive information, and operational disruptions from compromised services. Additionally, SSRF can damage customer trust and brand reputation, especially if confidential customer data is exposed. Remediation efforts may involve substantial costs for investigating the breach, implementing security fixes, and recovering from any legal or regulatory consequences. To mitigate these risks, organizations must implement strong access controls, validate and sanitize input effectively, and monitor and audit server activities to detect and prevent SSRF vulnerabilities.

In this is stage 1 we understand web application testing. We take help from OWASP top 10 to understand them

Stage 2

Overview :-

- Content About Nessus :
  Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources. Nessus is a widely recognized and utilized vulnerability assessment tool developed by Tenable, Inc. It is designed to help organizations identify and manage vulnerabilities within their IT environments, thereby enhancing their overall security posture. Key Features are Vulnerability Scanning, Configuration and Compliance Audits, Detection of Malware and Backdoors, Ease of use, Detailed Reporting and Analysis, Integration and Automation, and type of scan is Network Scan, Credentialed Scan, Agent-Base Scans, Web Application Scans, and Deployment Options of Nessus are Nessus Professional, Nessus Manager and Nessus Essentials. and benefits of Nessus are proactive security, regulatory compliance, risk management, cost-effective.
  Nessus is a powerful and versatile tool for vulnerability assessment and management, widely used by organizations to enhance their cybersecurity defenses. Its comprehensive scanning capabilities, user-friendly interface,and detailed reporting make it an essential component of any robust security strategy.

- What you understood about Nessus
  Nessus is a widely used vulnerability scanner developed by Tenable, Inc. It is designed to identify vulnerabilities in computer systems, networks, and applications. Here are key aspects of Nessus in cybersecurity

  Vulnerability Scanning:
  Nessus scans systems for known vulnerabilities, misconfigurations, and compliance issues. It can detect missing patches, weak passwords, and other security weaknesses.

  Comprehensive Coverage:
  Nessus covers a broad range of systems, including operating systems, databases, web servers, and network devices. It supports various types of scans, such as credentialed, non-credentialed, and agent-based scans.

Regular Updates:

Nessus regularly updates its vulnerability database to include the latest security threats and vulnerabilities. This ensures that the scanner can identify the most recent and relevant security issues.

Reporting and Analysis:

Nessus generates detailed reports on the findings of its scans, including the severity of vulnerabilities, affected systems, and recommendations for remediation. This helps security teams prioritize and address the most critical issues.

Integration:

Nessus can integrate with other security tools and platforms, such as Security Information and Event Management (SIEM) systems, to enhance an organization's overall security posture.

User-Friendly Interface:

Nessus provides an intuitive interface for configuring and managing scans, making it accessible to both novice and experienced security professionals.

Nessus is a critical tool for organizations looking to identify and mitigate security risks in their IT environments proactively.

- Target website ▬http://testhtml5.vulnweb.com
- Target ip address:-44.228.249.3

List of vulnerability ▬

s.no	Vulnerability name	Severity	plugins
1	ICMP Timestamp Request Remote Date Disclosure	Low	10114
2	Port SYN scanner	Info	11219

3	Common Platform Enumeration (CPE)	Info	45590
4	Nessus SYN scanner	Info	11219
5	OS Identification	Info	11936
6	Service Detection (HELP Request)	Info	11153
7	TCP/IP Timestamps Supported	Info	25220
8	Ping the remote host	Info	10180
9	HyperText Transfer Protocol (HTTP) Information	Info	24260
10	Traceroute Information	Info	10287

REPORT:-

Vulnerability Name:- ICMP Timestamp Request Remote Date Disclosure

severity : - Low

Plugin:- 10114

Port :- 0 / icmp

Description:- The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

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

Business Impact::-Business Impact of the ICMP Timestamp Request Remote Data Disclosure Vulnerability,organization can better Prepare for potential risks and strengthen their overall security posture.

2. Vulnerability Name:-   Port SYN scanner

severity : - Info

Plugin:-   11219

Port :-   11219

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

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

Solution:-   Protect your target with an IP filter.

Business Impact::-

3. Vulnerability Name:- Common Platform Enumeration (CPE)

severity : - Info

Plugin:- 45590

Port :- N/A

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

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

Solution:- NIL

Business Impact::-By understanding the business impact of CPE vulnerabilities and implementing effective mitigation strategies,organizations can reduce their risk exposure and enhance their overall security posture.

4. Vulnerability Name:- Nessus SYN scanner

severity : - Info

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.

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

Solution:- Open TCP ports on target systems by sending SYN packets and analyzing the responses.

Business Impact::-By effectively managing the use of the Nessus SYN scanner, organizations can enhance their security posture while minimizing potential business impacts. This balance is crucial for maintaining operational efficiency and protecting against threats.

5. Vulnerability Name:- OS Identification

severity : - Info

Plugin:- 11936

Port :- 80 / tcp / www

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

Solution:- Protect your target with an IP filter.

Business Impact::-Organization can effectively mitigate OS identification vulnerabilities, reduce their risk exposure, and enhance their overall cybersecurity posture.Regular reviews and updates to security measures are essential to adapt to new threats and maintain robust protection against potential exploits.

6. Vulnerability Name:- Service Detection (HELP Request)

severity : - Info

Plugin:- 11153

Port :- 80 / tcp / www

Description:- It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution:-   Deploy IDS/IPS solutions to detect and prevent unauthorized access and suspicious activity on the network.

Business Impact::-To mitigate these risk, proactive security measures like regular vulnerability assessment patch management, and employee training are crucial.

7. Vulnerability Name:- TCP/IP Timestamps Supported

severity : - Info

Plugin:- 25220

Port :- NA

Description:- The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:-   use tools like Nessus , qualys, or OpenVAS to scan and identify devices on the network that expose OS identification details .

Business Impact::-OS identification vulnerabilities expose specific details about the operating systems running on network devices and servers,potentially aiding attackers in targeting known vulnerabilities.

8. Vulnerability Name:- Ping the remote host

severity : - Info

Plugin:- 10180

Port :- 80 / tcp / www

Description:- Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution:-   ICMP ping requested.

Business Impact::-By taking these precautions, organizations can reduce the likelihood and impact of vulnerabilities associated with ICMP ping requested.

9. Vulnerability Name:- HyperText Transfer Protocol (HTTP) Information

severity : - Info

Plugin:- 24260

Port :- 80 / tcp / www

Description:- This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

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

Solution:- NIL

Business Impact::-HTTP information vulnerabilities can have significant business impacts depending on the nature and severity of the vulnerabilities.

10. Vulnerability Name:- Traceroute Information

severity : - Info

Plugin:- 10287

Port :- 0/ UDP

Description:- Makes a traceroute to the remote host.

For example:

For your information, here is the traceroute from 10.1.151.39 to 104.21.58.78 :

10.1.151.39

10.1.62.3

202.131.110.1

27.109.3.165

27.109.16.17

202.131.98.145

202.131.99.206

103.27.170.48

172.71.196.2

104.21.58.78

104.21.58.78

Hop Count: 14

Solution:- Configure firewalls to limit or block ICMP

Business Impact::- By implementing these strategies, organizations can minimize the risk associated with traceroute information vulnerabilities and enhance their overall network security posture.

Stage 3

Report

Title :- Ex :- Ability of SOC / SEIM
(this Title should be related to SOC / SEIM)

————--

Below are side headings we need to write at least a paragraph for each what we understood from each topic :-

- Soc

A Security Operations Center (SOC) serves as the nerve center for cybersecurity defense within an organization, employing advanced technologies and skilled personnel to detect, analyze, and respond to potential threats in real-time. Utilizing a combination of SIEM (Security Information and Event Management), threat intelligence feeds, and advanced analytics, the SOC continuously monitors network traffic, system logs, and endpoint activities to identify anomalous behavior indicative of potential security incidents. Once identified, security analysts investigate these alerts to determine their validity and severity, leveraging incident response playbooks and collaboration tools to swiftly mitigate threats and minimize impact. The SOC also plays a pivotal role in threat hunting, proactively searching for hidden threats that may evade automated detection systems. By maintaining robust defenses and staying ahead of emerging threats, the SOC safeguards critical assets, ensuring the resilience and security posture of the organization against a dynamic and evolving threat landscape.

- SOC - cycle

The Security Operations Center (SOC) operates within a continuous cycle of monitoring, detection, analysis, and response to safeguard an organization's digital assets against cyber threats. Initially, the SOC monitors various data sources, including network traffic, system logs, and endpoint activities, using advanced tools such as SIEM (Security Information and Event Management) to gather real-time information. Through proactive threat hunting and the integration of threat intelligence feeds, potential security incidents

are detected early. Once an alert is triggered, security analysts conduct thorough analysis to assess the nature and scope of the incident, utilizing playbooks and standardized procedures for effective response. Immediate action is taken to contain and mitigate the threat, followed by post-incident activities such as forensic analysis and incident documentation to prevent future occurrences. Continuous improvement is achieved through incident review sessions, where lessons learned are incorporated to enhance detection capabilities and response efficiency, ensuring the SOC remains adaptive and resilient in combating emerging cyber threats.

- Siem

SIEM, or Security Information and Event Management, is a critical component of modern cybersecurity infrastructure, designed to centralize the collection, normalization, correlation, and analysis of security-related data across an organization's IT environment. By aggregating data from various sources such as network devices, servers, endpoints, and applications, SIEM platforms provide security teams with a comprehensive view of potential threats and security incidents in real-time. Through sophisticated correlation rules and algorithms, SIEM systems identify patterns of suspicious behavior that may indicate cyber attacks, enabling security analysts to promptly investigate and respond to threats. Additionally, SIEM solutions facilitate compliance reporting by generating audit trails and reports based on regulatory requirements, helping organizations demonstrate adherence to security policies and standards. Continuous tuning and refinement of SIEM configurations ensure optimal performance and relevance of threat detection capabilities, making it an indispensable tool for enhancing overall cybersecurity posture and incident response effectiveness.

- Siem Cycle

The SIEM cycle begins with data collection from diverse sources across an organization's IT infrastructure, including network devices, servers, endpoints, and applications. This data is aggregated and normalized to ensure consistency and compatibility for analysis. Next, the normalized data undergoes correlation, where events and logs are compared against predefined rules and baselines to identify patterns indicative of potential security incidents or anomalies. Once suspicious activities are detected, alerts are generated and prioritized based on severity and relevance. Security analysts investigate these alerts to determine the nature and scope of the incidents, leveraging additional contextual information and threat intelligence feeds to validate and prioritize responses. Following incident resolution, SIEM systems facilitate post-incident analysis and reporting, providing insights into the incident timeline, impact assessment, and recommendations for improving security defenses. Continuous monitoring and refinement of the SIEM configuration and correlation rules ensure ongoing effectiveness in detecting and

responding to evolving cyber threats, thereby enhancing the organization's overall cybersecurity posture.

- MISP

MISP, or Malware Information Sharing Platform and Threat Sharing, is an open-source intelligence platform designed to facilitate the sharing of structured threat information among cybersecurity professionals and organizations. At its core, MISP serves as a centralized repository where security teams can collaboratively document, store, and share details about security threats, including indicators of compromise (IOCs), malware samples, and attack patterns. It supports the integration of threat intelligence feeds and automated data sharing, enabling real-time updates and synchronization across interconnected MISP instances. Security analysts utilize MISP to enrich their own threat intelligence capabilities, leveraging shared data to enhance detection and response efforts against cyber threats. The platform's flexibility allows customization of data models and taxonomies to accommodate specific organizational needs and industry standards, fostering a community-driven approach to cybersecurity collaboration and information exchange.

- Your college network information

- How you think you deploy soc in your college

- Threat intelligence

Threat intelligence is a systematic process involving the collection, analysis, and dissemination of data regarding cyber threats. This process aims to identify, understand, and mitigate potential or existing threats to an organization's cybersecurity. Key scientific components include:

1. Data Collection: Aggregating raw data from diverse sources such as network logs, open-source intelligence (OSINT), and threat feeds.
2. Analysis: Applying advanced analytical methods, including statistical analysis and machine learning, to identify patterns, tactics, techniques, and procedures (TTPs) used by threat actors.
3. Dissemination: Communicating the analyzed intelligence to stakeholders for informed decision-making and enhanced cybersecurity measures.
4. Response: Implementing security actions based on the intelligence to prevent, detect, and respond to threats.

This structured approach improves an organization's ability to anticipate, understand, and counteract cyber threats effectively.

- Incident response

Incident response in cybersecurity is a systematic process designed to manage and mitigate the effects of cyber attacks. It begins with preparation, where an incident response plan and team are developed, detection tools are deployed, and regular training is conducted. Next, the identification phase involves detecting and confirming incidents using monitoring tools and analysis. Once an incident is identified, the containment phase isolates affected systems to prevent the threat from spreading. The eradication phase focuses on removing the root cause of the incident, such as malware or vulnerabilities. Following eradication, the recovery phase restores systems to normal operation and verifies their security. Finally, the lessons learned phase involves analyzing the incident response to improve future practices and prevent recurrence. This structured approach enhances an organization's ability to effectively manage and mitigate cybersecurity incidents.

- Qradar & understanding about tool

IBM QRadar is an advanced Security Information and Event Management (SIEM) system designed to facilitate the detection, analysis, and mitigation of cybersecurity threats within an organizational context. It consolidates and correlates log data from diverse sources, such as network infrastructure, server environments, application layers, and cloud platforms, thereby providing an integrative and holistic view of the security posture. QRadar employs sophisticated real-time data analytics and machine learning algorithms to identify anomalous patterns and correlations, generating prioritized alerts known as offenses based on their potential impact. The system's customizable dashboards and reporting tools enable precise visualization and in-depth analysis of security metrics. Integration with external threat intelligence feeds, coupled with user behavior analytics, augments its capability to detect both known and emerging threats. Furthermore, QRadar's incident response functionalities support automated and manual intervention strategies. Its architecture is inherently scalable, supporting deployment in both on-premises and cloud-based infrastructures, thus accommodating the evolving security

demands of organizations. Key operational concepts include the configuration and management of log sources, rule-based detection mechanisms, offense management, utilization of reference data sets, and analysis of network traffic flows. In essence, QRadar serves as a comprehensive, flexible, and scalable solution for advanced cybersecurity threat management.

Conclusion :-

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

In conclusion, web application testing plays a crucial role in identifying and mitigating vulnerabilities that could compromise the security and integrity of online platforms. By systematically probing for weaknesses through techniques such as penetration testing, vulnerability scanning, and code review, organizations can proactively address potential threats before they can be exploited by malicious actors. Effective web application testing not only helps in securing sensitive data and protecting user privacy but also ensures compliance with regulatory requirements and industry standards. Continuous monitoring and updating of security measures based on testing results are essential to maintaining robust defenses against evolving cyber threats in today's interconnected digital landscape.

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

A Nessus report serves as a comprehensive documentation of vulnerabilities identified through scans conducted by Tenable Nessus vulnerability scanner. This report provides detailed insights into the security posture of scanned systems or networks, typically including an executive summary summarizing critical findings and overall risk levels. It enumerates vulnerabilities with precise technical details such as severity ratings based on the Common Vulnerability Scoring System (CVSS), affected systems, potential impacts on confidentiality, integrity, and availability (CIA triad), and recommended remediation actions. The report often includes graphical representations for visual analysis of vulnerability distribution and may incorporate compliance checks against industry standards or regulatory requirements, highlighting any deviations or non-compliance

issues. Ultimately, Nessus reports equip IT and security professionals with the information needed to prioritize and implement mitigation strategies effectively, enhancing the organization's cybersecurity defenses and regulatory adherence.

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

Integrating ML and DL into SOC workflows and QRadar dashboards can revolutionize how Nessus reports are utilized, transforming them from static documents into dynamic, actionable intelligence. Automated detection, predictive prioritization, anomaly detection, and adaptive security measures, all displayed in an intuitive and interactive dashboard, empower security teams to respond swiftly and effectively to threats, ultimately enhancing the organization's cybersecurity posture.

Future Scope :-

- Stage 1 :- future scope of web application testing

Looking ahead, the future of testing web applications will focus on using more automation, AI, and machine learning to work faster and more accurately. There will be more continuous testing and better integration with security (called DevSecOps) during the whole process of making software. Also, new tools and ways of testing will help understand more about what's happening in web applications, like how they use data and connect with other services. As web apps get more complex, testing will need to keep up with new challenges, like making sure they work with devices like smart gadgets, keeping data safe in the cloud, and following strict privacy rules. Overall, the future of testing web applications is about being ready for new cyber threats and helping digital tools work better and smarter.

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

In the realm of machine learning (ML) and deep learning (DL), the future application of Nessus reports promises significant advancements in vulnerability assessment and mitigation strategies. ML algorithms are poised to automate the detection and classification of vulnerabilities identified in Nessus scans, enhancing accuracy and speed.

Predictive ML models can prioritize vulnerabilities based on potential impact and exploitability, leveraging historical data and threat intelligence feeds for proactive risk management. DL techniques, such as anomaly detection with neural networks, offer the capability to identify emerging threats and anomalous behaviors from Nessus scan data, enabling preemptive security measures. Automated remediation recommendations driven by ML systems aim to streamline response actions based on past remediation successes. Integrating Nessus with ML-powered continuous monitoring enhances adaptive security measures, dynamically adjusting defenses against evolving threats. ML-enhanced security analytics and visualization provide deeper insights into vulnerability trends and attack correlations, while augmented threat intelligence enriches Nessus reports with context-specific insights for informed decision-making. Together, these advancements empower organizations to bolster cybersecurity defenses, mitigate risks more effectively, and maintain resilience in the face of evolving cyber threats.

- Stage 3 :- future scope of SOC / SEIM

The future scope of SOC and SIEM systems is poised to be shaped by significant advancements in automation, AI, cloud security, and integration capabilities. These developments will enable more efficient, proactive, and adaptive security operations, enhancing the ability to detect, respond to, and mitigate evolving cyber threats. By leveraging these technologies, SOCs and SIEMs will become more effective in safeguarding organizations against increasingly sophisticated and persistent cyber attacks.

Topics explored :-

 During this training following topics are explored.
CEH, Stages of hacking, Types of cyber attacks, Hacker's categories, Various LINUX commands, Kali LINUX, SQL map,

Tools explored :-

DNS lookup, NESSUS, Shodan, OSINT framework, Metasploitable

——--------THE END ——----------------------