Stage-1

Web Goat Report

Part 1: Executive Summary

1. Overview:

WebGoat is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open source components.

Description

Web application security is difficult to learn and practice. Not many people have full blown web applications like online book stores or online banks that can be used to scan for vulnerabilities. In addition, security professionals frequently need to test tools against a platform known to be vulnerable to ensure that they perform as advertised. All of this needs to happen in a safe and legal environment.

Even if your intentions are good, we believe you should never attempt to find vulnerabilities without permission. The primary goal of the WebGoat project is simple: create a de-facto interactive teaching environment for web application security. In the future, the project team hopes to extend WebGoat into becoming a security benchmarking platform and a Java-based Web Site Honeypot.

2. List of Vulnerable Parameter, Location discovered

S.No	Name of The Vulnerability	References-CWE
1	A01-Broken Access Control	CWE-285: Improper Authorization
2	A02-Cryptographic Failures	CWE-310: Cryptographic Issues
3	A03-Injection	CWE 89: SQL Injection
4	A04-Insecure Design	CWE-235 Improper Handling of Extra Parameters
5	A05-Security Misconfiguration	CWE-12: ASP.NET Misconfiguration: Missing Custom Error Page
6	A06-Vulnerable and Outdated Components	CWE-1104: Use of Unmaintained Third Party Components
7	A07-Identification and Authentication Failures	CWE-287: Improper Authentication
8	A08-Software and Data Integrity Failures	CWE-1214: Data Integrity Issues
9	A09-Security Logging and Monitoring Failures	CWE-1210: Audit / Logging Errors
10	A10-Server-Side Request Forgery	CWE-918 - Server-Side Request Forgery

1- 1.1 Vulnerability Name: Improper Authorization

CWE: CWE-285

OWASP Category: A01-Broken Access Control

Description: Verification is missing during authorization check

Business Impact:

Broken access control can have severe business impacts, both financially and reputationally. It allows unauthorized access to sensitive information, leading to data breaches, compliance violations, and potential legal liabilities. Intellectual property theft becomes easier, risking a company's competitiveness and market position. Service disruptions or downtime can occur, causing lost productivity and customer dissatisfaction. Furthermore, it damages an organization's reputation and customer trust, resulting in increased security costs and potential legal actions. Ultimately, broken access control can lead to a loss of competitive advantage and hinder business growth. To mitigate these risks, organizations must prioritize access control, conduct regular security audits, and invest in employee education and awareness.

1.2 Vulnerability Name: Cryptographic Issues

CWE: CWE-310

OWASP Category: A02-Cryptographic Failures

Description: Weaknesses in this category are related to the design and implementation of data confidentiality and integrity.

Business Impact:

Cryptographic failures can have significant business impacts, including financial losses, data breaches, reputational damage, and legal consequences. Such failures may lead to the theft of sensitive information, erode customer trust, and result in regulatory fines and penalties. Additionally, businesses may suffer from intellectual property theft, loss of competitive advantage, and disruptions in operations, leading to decreased market value and increased remediation costs. To mitigate these risks, organizations should prioritize strong cryptographic practices, conduct regular security audits, and implement a comprehensive incident response plan.

1.3 Vulnerability Name: SQL Injection

CWE: CWE-89

OWASP Category: A03-Injection

Description: The software constructs all or part of an **SQL command** using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component

Business Impact:

Injection attacks can have severe business impacts, including data breaches, financial losses, reputational damage, and legal consequences. These attacks can expose sensitive information, lead to fraudulent transactions, and erode customer trust, resulting in potential revenue loss and damage to market reputation. Organizations may face legal actions and downtime to address vulnerabilities, while intellectual property theft can harm competitiveness. To mitigate the impact, businesses must prioritize secure coding practices, conduct regular security assessments, and educate staff on secure coding and best practices to defend against these threats effectively. 1.4 Vulnerability Name: Improper Handling of Extra Parameters

CWE: CWE-235

OWASP Category: A04-Insecure Design

Description: The product does not handle or incorrectly handles when the number of parameters, fields, or arguments with the same name exceeds the expected amount.

Business Impact:

Insecure design in business applications and systems can lead to significant negative consequences for organizations. It can result in data breaches, financial losses, and reputational damage due to unauthorized access to sensitive information. The loss of customer trust and competitive advantage are also potential outcomes, along with legal and regulatory repercussions for non-compliance. Insecure design can disrupt business operations, increase security costs, and limit market adoption. To mitigate these risks, organizations must prioritize security from the outset, implementing secure design principles, conducting regular security assessments, and fostering a culture of security awareness throughout the development process.

1.5 Vulnerability Name: ASP.NET Misconfiguration: Missing Custom Error Page

CWE: CWE-12

OWASP Category: A05-Security Misconfiguration

Description: An ASP .NET application must enable custom error pages in order to prevent attackers from mining information from the framework's built-in responses.

Business Impact:

Security misconfigurations can have serious business impacts, including data breaches, financial losses, and reputational damage. These misconfigurations create vulnerabilities that allow unauthorized access to sensitive data, leading to potential legal liabilities and non-compliance with data protection regulations. Downtime and disruptions in business operations may occur as a result, and intellectual property theft can compromise the organization's competitive advantage. The increased attack surface due to misconfigurations provides cybercriminals with more opportunities to exploit weaknesses, potentially leading to a loss of customer trust and loyalty. To mitigate these risks, organizations should prioritize robust security configurations, regular assessments, and employee education on secure practices.

1.6 Vulnerability Name: Use of Unmaintained Third Party Components

CWE: CWE-1104

OWASP Category: A06-Vulnerable and Outdated Components

Description: 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.

Business Impact:

The business impact of using vulnerable and outdated components in software applications or systems can be significant. Such components expose organizations to increased security risks, data breaches, and financial losses due to potential exploitation by cyber attackers. Reputational damage can result from a data breach or security incident, leading to a loss of customer trust and loyalty. Non-compliance with data protection regulations may lead to legal consequences, while downtime and disruptions can occur during incident response and remediation. Moreover, limited software functionality, incompatibility, and integration issues can hinder business operations and customer satisfaction. To mitigate these risks, organizations should adopt robust software development and maintenance practices, including regular security assessments, patch management, and the use of software composition analysis tools to identify and address vulnerabilities promptly.

1.7 Vulnerability Name: Improper Authentication

CWE: CWE-287

OWASP Category: A07-Identification and Authentication Failures

Description: The product does not prove or insufficiently proves that the claim is correct.

Business Impact:

Identification and authentication failures can have serious business impacts, allowing unauthorized access to sensitive data and systems. This may lead to data breaches, financial losses, and reputational damage due to compromised customer privacy and potential fraud. Non-compliance with data protection regulations can result in legal consequences and regulatory fines. The disruption of business operations, loss of customer trust, and intellectual property theft are also potential outcomes. To mitigate these risks, organizations must implement robust identification and authentication measures, such as multi-factor authentication and strong password policies, and conduct regular security assessments. Additionally, ongoing staff training on secure authentication practices and a strong security culture are essential to protect sensitive data and maintain customer confidence.

1.8 Vulnerability Name: Data Integrity Issues

CWE: CWE-1214

OWASP Category: A08-Software and Data Integrity Failures

Description: To ensure the integrity of data, such as messages, resource files, deployment files, and configuration files

Business Impact:

Software and data integrity failures can have significant business impacts, compromising the reliability of systems and critical data. Such failures can result in data corruption, inaccurate information, and financial losses due to errors in transactions and decision-making. Reputational damage is a potential consequence as customers may lose trust in the organization's ability to secure their data properly. Non-compliance with data integrity regulations can lead to legal actions and regulatory fines, while operational disruptions may occur, affecting productivity and recovery costs. Intellectual property theft and loss of customer trust are additional risks associated with integrity failures. To mitigate these impacts, organizations should implement robust data validation mechanisms, disaster recovery plans, and employee training on data integrity best practices to maintain a secure and trustworthy environment

1.9 Vulnerability Name: Audit / Logging Errors

CWE: CWE-1210

OWASP Category: A09-Security Logging and Monitoring Failures

Description: It deal with logging user activities in order to identify undesired access and modifications to the system

Business Impact:

Security logging and monitoring failures can have serious business impacts, compromising incident detection and response capabilities. Delayed incident detection and increased dwell time allow attackers to operate undetected, potentially leading to data breaches and financial losses. Reputational damage can result from compromised customer data and non-compliance with regulations. The inability to conduct thorough forensic investigations and limited incident response capabilities further exacerbate the risks. To mitigate these impacts, organizations must implement robust logging and monitoring practices, including real-time alerts and regular security assessments. Investing in modern SIEM solutions and providing training for security personnel and staff on incident response procedures are essential for maintaining a strong security posture.

1.10 Vulnerability Name: Server-Side Request Forgery

CWE: CWE-918

OWASP Category: A10- Server-Side Request Forgery

Description: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

Business Impact:

Server-Side Request Forgery (SSRF) can have significant business impacts, posing serious risks to organizations. Attackers can exploit SSRF to access sensitive internal resources, leading to data breaches, financial losses, and service disruptions. Such attacks can also result in legal liabilities, reputational damage, and loss of customer trust. To mitigate the risks, organizations must adopt secure coding practices, implement input validation, and employ network-level security controls. Regular security assessments and staff training on SSRF risks are essential to strengthen the defense against this vulnerability.

Stage 2

Overview :-

Nessus is a widely used vulnerability scanner developed by Tenable, Inc. It is designed to help identify and assess vulnerabilities and misconfigurations in computer systems, networks, and applications.

Vulnerability scanning is a critical cybersecurity practice used to identify security weaknesses, flaws, and vulnerabilities within computer systems, networks, applications, and other IT infrastructure components. These weaknesses, if left unaddressed, could potentially be exploited by attackers to compromise the system's confidentiality, integrity, or availability. Nessus scans target systems for known vulnerabilities in their software, operating systems, and configurations. It can assess a wide range of devices, including servers, workstations, routers, switches, and virtual machines.

Plugin architecture, also known as a plugin system or plugin framework, is a software design pattern that allows developers to extend the functionality of an application without modifying its core codebase. The plugin architecture enables the dynamic loading and execution of external code modules, known as plugins or extensions, which can add new features, capabilities, or customizations to the base application. Nessus employs a plugin-based system to perform scans. Each plugin is a set of rules and scripts that can detect specific vulnerabilities or potential security issues. Tenable regularly updates these plugins to keep pace with emerging threats and vulnerabilities.

Policy Compliance Auditing: Besides vulnerability scanning, Nessus can also check systems against specific compliance policies (e.g., PCI DSS, HIPAA) to ensure they meet relevant security standards. Credential-Based Scanning: Nessus can perform both non-credentialed scans (where it gathers information without authenticating) and credentialed scans (where it uses provided credentials to access the target system). Credentialed scans often provide more accurate and detailed results. Reporting and Remediation: After completing a scan, Nessus generates comprehensive reports outlining identified vulnerabilities and possible remediation steps. These reports help security teams prioritize and address potential threats effectively. Nessus Professional and HomeFeed: Nessus is available in different editions. Nessus Professional is a paid version that offers more features, while Nessus HomeFeed is a free edition with limited functionality.

Target website: https://roeverengg.edu.in/

Target ip address: 35.213.140.165

List of vulnerability –

S.No	Vulnerability Name	Severity	plugins
1	SSL Certificate Cannot Be Trusted	Medium	51192
2	SMTP Service Cleartext Login Permitted	Low	54582
3	Service Detection	Low	22964
4	FTP Service AUTH TLS Command Support	Low	42149
5	SSL Certificate 'commonName' Mismatch	Low	45410
6	SSL Certificate Signed Using Weak Hashing Algorithm	Low	95631
7	SMTP Authentication Methods	Low	54580
8	Reverse NAT/Intercepting Proxy Detection	Medium	31422
9	SSL Root Certification Authority Certificate Information	Low	94761
10	SSL/TLS Recommended Cipher Suites	Low	156899

REPORT

1. Vulnerability Name: SSL Certificate Cannot Be Trusted

Severity: Medium

Plugin: #51192

Port: 443, 110, 143 & 993

Description: The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken

Solution: Purchase or generate a proper SSL certificate for this service.

Business Impact: it can have significant business impacts, affecting both the organization's reputation and its ability to conduct secure online transactions. Such issues lead to a loss of trust and reputation, reduced customer engagement and conversion rates, increased abandonment rates, heightened data breach risks, compliance concerns, potential SEO impact, increased customer support overhead, and hindered partnerships and business relationships. To mitigate these consequences, organizations should regularly monitor and maintain their SSL certificates, ensuring they are up-to-date and issued by trusted Certificate Authorities (CAs) to provide a secure online experience and maintain customer trust.

2. Vulnerability Name: SMTP Service Cleartext Login Permitted

Severity: Low

Plugin: 54582

Port: 25, 587

Description: The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

Solution: Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Business Impact: SMTP Service Cleartext Login Permitted can have both positive and negative impacts on a business. On the positive side, it allows compatibility with older email clients and simplifies configuration for organizations with limited IT expertise. However, the major concern lies in the security risk posed by transmitting login credentials in plain text, making them vulnerable to interception and unauthorized access. This could lead to data breaches, reputational damage, and non-compliance with data protection regulations. Additionally, enabling cleartext login increases the risk of phishing attacks as attackers can easily capture login credentials from intercepted communications. To prioritize security, modern organizations typically enforce encrypted authentication methods like SSL/TLS or STARTTLS to safeguard sensitive information and maintain compliance with industry regulations, ensuring a more secure and trustworthy email system.

3. Vulnerability Name: Service Detection

Severity: Low

Plugin: 22964

Port: 21,25,587,80,110,143,443

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

Solution: An FTP server is running on this port.

Business Impact: Service detection, or service discovery, has significant business impacts, both positive and negative. On the positive side, it offers enhanced network visibility, enabling efficient resource allocation and proactive monitoring, leading to improved operational efficiency and faster troubleshooting. It also facilitates scalability and adaptability, crucial for meeting changing business demands. Moreover, service detection aids in identifying security vulnerabilities, ensuring compliance, and safeguarding sensitive data. On the downside, it may add complexity, requiring extra resources and expertise for management, and raise privacy concerns if not handled securely. Nevertheless, the overall benefits of service detection empower businesses to make informed decisions, optimize performance, and strengthen their IT infrastructure to align with their organizational goals.

4. Vulnerability Name: FTP Service AUTH TLS Command Support

Severity: Low

Plugin: 42149

Port: 21

Description: The remote FTP service supports the use of the 'AUTH TLS' command to switch from a clear text to an encrypted communications channel.

Solution: The remote FTP service responded to the 'AUTH TLS' command with a '234' response code, suggesting that it supports that command.

Business Impact: Enabling FTP Service AUTH TLS command support has notable business impacts. It enhances data security by encrypting sensitive information during transfers, ensuring compliance with regulations and bolstering customer trust. While potential compatibility issues with older systems exist, the benefits include reduced data breach risks and improved data protection, outweighing any minimal performance overhead associated with encryption.

5. Vulnerability Name: SSL Certificate 'commonName' Mismatch

Severity: Low

Plugin: 45410

Port: 443, 993, 21, 465

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

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

Business Impact: An SSL certificate 'commonName' mismatch can have significant business impacts. It leads to a loss of customer trust, decreased online sales, and a damaged reputation, as visitors perceive the website as untrustworthy or compromised. E-commerce sites suffer from reduced conversions and potential legal and compliance issues. Moreover, the mismatch negatively affects SEO ranking, increases customer support costs, and may result in lower website traffic. To mitigate these effects, businesses must ensure SSL certificates are correctly configured and regularly monitored, maintaining a secure and trusted online presence.

6. Vulnerability Name: SSL Certificate Signed Using Weak Hashing Algorithm

Severity: Low

Plugin: 95631

Port: 443, 993, 110

Description: The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm

Solution: Contact the Certificate Authority to have the certificate reissued.

Business Impact: The business impact of an SSL certificate signed using a weak hashing algorithm can be severe, as it undermines security, leads to a loss of customer trust, and raises non-compliance concerns with industry standards. Weak hashing algorithms increase the vulnerability to cyberattacks, potentially resulting in data breaches and negative impacts on reputation and search rankings. To mitigate these risks, businesses must adopt SSL certificates with strong encryption algorithms, ensuring data protection, maintaining customer trust, and safeguarding their online reputation. Regular updates and adherence to security standards are crucial in preserving a secure and trusted online presence.

7. Vulnerability Name: SMTP Authentication Methods

Severity: Low

Plugin: 54580

Port: 25, 587

Description: The remote SMTP server advertises that it supports authentication.

Solution: Review the list of methods and whether they're available over an encrypted channel.

Business Impact: SMTP authentication methods have significant business impacts, including enhanced email security by preventing unauthorized access, reducing the risk of email spoofing and phishing attacks, and protecting sensitive business information. Implementing strong authentication methods like SPF, DKIM, and DMARC helps maintain brand reputation and trust by preventing email spoofing and fraudulent activities. It also positively affects email deliverability and inbox placement, leading to higher open and click-through rates for marketing and communication campaigns. Compliance with industry regulations and data protection requirements is facilitated, reducing the risk of legal and financial penalties. Moreover, businesses can save costs by preventing email abuse and resource misuse. Additionally, enhanced analytics and reporting provided by DMARC aid in identifying potential security threats and fine-tuning email delivery settings for improved performance. Overall, implementing SMTP authentication methods ensures secure and efficient email communication, benefiting businesses and their stakeholders.

8. Vulnerability Name: Reverse NAT/Intercepting Proxy Detection

Severity: Low

Plugin: 31422

Port: N/A

Description: Reverse NAT is a technology which lets multiple computers offer public services on different ports via the same IP address.

Solution: Make sure that this setup is authorized by your security policy.

Business Impact:

Reverse NAT and Intercepting Proxy Detection have significant business impacts. Reverse NAT enables improved accessibility by redirecting incoming internet traffic to specific internal servers without exposing the entire network. This technology enhances security by isolating critical internal systems and facilitates scalability by allowing multiple servers to share the same public IP address. On the other hand, Intercepting Proxy Detection is vital for data privacy and security as it helps identify and manage intercepting proxies that may compromise sensitive information. Accurate user analytics and fair usage enforcement are additional benefits of detecting and handling intercepting proxies. Understanding and effectively managing both technologies contribute to enhanced network security, user experience, and overall business operations.

9. Vulnerability Name: SSL Root Certification Authority Certificate Information

Severity: Low

Plugin: 94761

Port: 993, 443,465

Description: The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

Solution: Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Business Impact: The business impact of SSL Root Certification Authority (CA) certificate information is substantial. SSL certificates, issued by trusted Root CAs, ensure the security and encryption of sensitive data, building user trust and confidence. Websites with valid SSL certificates from reputable CAs are more likely to rank higher in search engines, contributing to better SEO and increased organic traffic. Complying with industry standards and regulations is essential to avoid penalties and maintain a positive reputation. SSL certificates also reduce cart abandonment in e-commerce and protect businesses from legal liabilities in case of data breaches.

10. Vulnerability Name: SSL/TLS Recommended Cipher Suites

Severity: Low

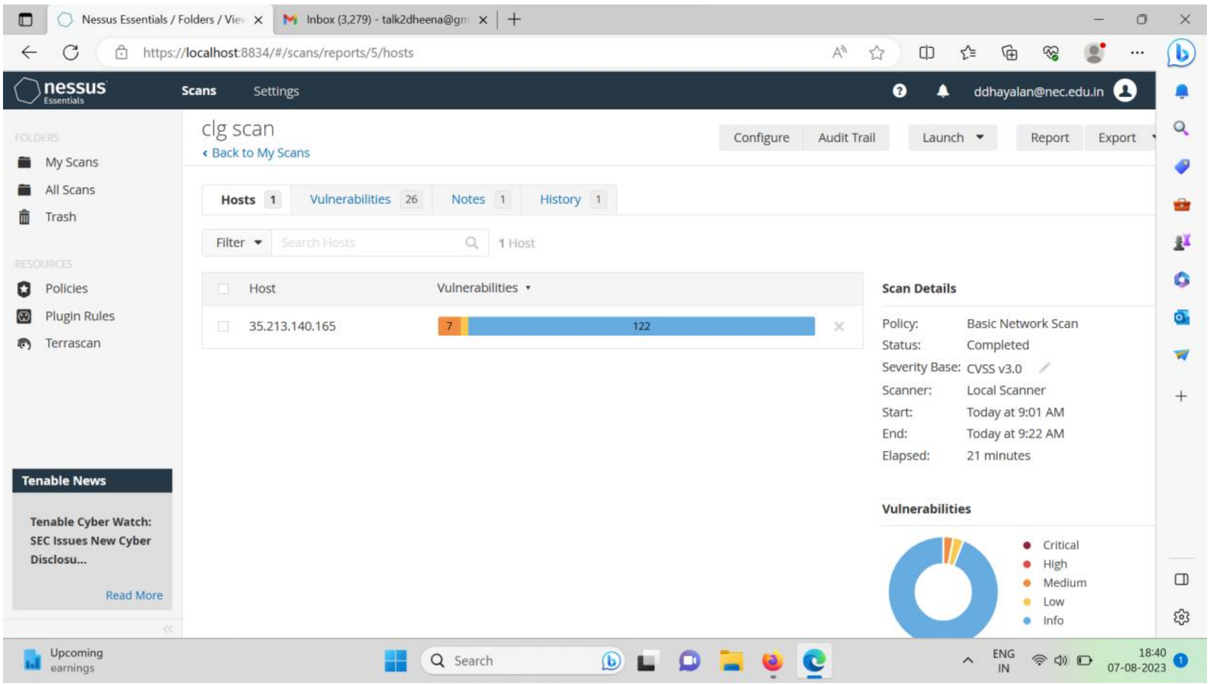
Plugin: 156899

Port: 21, 993, 995,465

Description: The remote host has open SSL/TLS ports which advertise discouraged cipher suites.

Solution: Only enable support for recommened cipher suites.

Business Impact: SSL/TLS recommended cipher suites is substantial. By utilizing strong cryptographic algorithms during the SSL/TLS handshake, businesses can enhance data security, protecting sensitive information from cyberattacks and unauthorized access. Compliance with regulatory requirements becomes more attainable, reducing the risk of penalties and legal liabilities. Users gain trust and confidence in the security of their data, fostering positive brand reputation and customer loyalty. Additionally, improved performance and compatibility ensure seamless communication between clients and servers, enhancing the user experience and potentially boosting search engine rankings. Proactive implementation of recommended cipher suites helps mitigate vulnerabilities and stay ahead of evolving cyber threats, reinforcing the commitment to data protection and maintaining a secure online environment.



Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:01 AM
End: Today at 9:22 AM
Elapsed: 21 minutes

Stage 3

Report

Title: Threat Intelligence in Cyber Space

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) is a centralized facility within an organization responsible for monitoring, detecting, and responding to cybersecurity threats and incidents.The primary objective of a SOC is to ensure the security, confidentiality, and integrity of an organization's information systems, data, and assets. SOC teams use various security tools and technologies, such as SIEM solutions, intrusion detection systems, firewalls, and endpoint security tools, to monitor and analyze network traffic and log data in real-time. SOC analysts investigate security alerts, identify potential threats, and initiate incident response actions to contain and mitigate cybersecurity incidents.Threat intelligence plays a crucial role in SOC operations, providing valuable insights into the latest cyber threats and attack trends.

SOC Cycle:

The Security Operations Center (SOC) cycle is a continuous process that involves monitoring, detecting, and responding to cybersecurity threats. Here are short notes on each stage of the SOC cycle:

1. **Monitoring:** Continuous monitoring of networks, systems, and applications using security tools to identify potential threats and abnormal activities.
2. **Detection:** Analyzing alerts generated by monitoring systems to identify genuine security incidents from false positives.
3. **Threat Intelligence:** Leveraging threat intelligence sources to understand the latest cyber threats and attack techniques.
4. **Incident Response:** Initiating incident response actions to contain, eradicate, and recover from security incidents.
5. **Remediation:** Collaborating with IT teams to address vulnerabilities and apply patches to prevent future incidents.
6. **Continuous Improvement:** Learning from incidents to improve SOC capabilities, tools, and procedures.
7. **Threat Hunting:** Proactively searching for hidden threats that may have bypassed initial security measures.
8. **Reporting:** Communicating incident trends and security posture to key stakeholders.
9. **Training and Awareness:** Providing ongoing training for SOC personnel and promoting cybersecurity awareness across the organization.

The SOC cycle is iterative, ensuring continuous improvement and proactive defense against cyber threats.

SIEM:

Security Information and Event Management (SIEM) is a cybersecurity approach that centralizes the collection, analysis, and correlation of security event data from diverse sources within an organization's IT infrastructure. It provides real-time monitoring and threat detection capabilities, alerting security teams to potential anomalies and suspicious activities. SIEM's event correlation allows for the identification of complex attack patterns, enhancing incident response and enabling efficient investigation of security incidents. Additionally, SIEM supports compliance reporting, log management, and integration with other security solutions, contributing to an organization's proactive defense against cyber threats and overall cybersecurity effectiveness.

SIEM cycle:

The SIEM cycle is a continuous process that involves several stages to effectively manage and respond to security events and incidents using Security Information and Event Management (SIEM) technology. The SIEM cycle includes the following stages:

1. **Data Collection:** The cycle begins with the collection of data from various sources, such as logs from network devices, servers, applications, and security tools. This data is aggregated into a centralized repository for analysis.
2. **Data Normalization:** Once the data is collected, it undergoes normalization, where it is converted into a standardized format for consistent analysis and correlation.
3. **Event Correlation:** The normalized data is analyzed and correlated to identify patterns, trends, and potential security incidents. This process allows SIEM to detect complex attack patterns that might be missed when examining individual events.
4. **Alerting and Monitoring:** SIEM continuously monitors the correlated data in real-time. When predefined rules, signatures, or anomalies are detected, the system generates alerts, notifying security analysts of potential threats.
5. **Alert Investigation:** Security analysts investigate the alerts to determine if they represent genuine security incidents or false positives. This stage involves analyzing the context and severity of the alerts.
6. **Threat Detection and Response:** After confirming a security incident, the SIEM triggers incident response actions. This may involve containing the incident, eradicating threats, and recovering affected systems and data.
7. **Forensic Analysis:** Post-incident, SIEM allows for retrospective analysis to understand the root cause of the incident, identify attack vectors, and develop strategies to prevent similar incidents in the future.
8. **Reporting and Compliance:** SIEM generates reports and dashboards that provide insights into the organization's security posture, incident trends, and compliance status. These reports are often used for regulatory compliance purposes.
9. **Continuous Improvement:** Lessons learned from incidents and ongoing monitoring allow the organization to fine-tune SIEM rules, improve incident response procedures, and enhance the overall effectiveness of the SIEM system.

The SIEM cycle is iterative, meaning it is a recurring process that continuously adapts to changing threats and the organization's evolving IT environment. It plays a crucial role in enhancing an organization's cybersecurity capabilities by providing centralized visibility, proactive threat detection, and efficient incident response.

MISP:

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source threat intelligence platform designed to facilitate the sharing of structured and actionable cyber threat information among cybersecurity professionals, organizations, and communities. MISP enables the collection, storage, and distribution of threat data in a standardized and machine-readable format, allowing for better collaboration and more effective defense against cyber threats.

Key features of MISP include:

1. **Event Management:** MISP organizes threat information into "events," which contain details about a specific cyber threat, such as indicators of compromise (IOCs), threat actor information, and associated malware or attack patterns.
2. **Data Correlation:** MISP allows analysts to correlate and group related threat data from different sources, helping to identify and understand broader attack campaigns and cyber threat trends.
3. **Sharing and Collaboration:** MISP promotes information sharing and collaboration by providing organizations and communities with a secure platform to exchange threat intelligence. Sharing can be done with specific trusted partners or with the broader MISP community.
4. **Taxonomies and Galaxy Clusters:** MISP supports the use of standardized taxonomies and galaxy clusters, enabling consistent and structured threat data classification for easier analysis and understanding.
5. **STIX and TAXII Support:** MISP supports the use of STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information) standards, facilitating interoperability with other threat intelligence platforms and tools.
6. **Integration with Threat Feeds:** MISP can be integrated with various external threat intelligence feeds and sources to enrich its threat data and provide a more comprehensive view of the threat landscape.
7. **API and Automation:** MISP offers a powerful API that allows for automation and integration with other security tools, enabling seamless data exchange and automated threat analysis.
8. **Data Visualization:** MISP provides visual representations of threat data through graphs, matrices, and timelines, aiding analysts in identifying relationships and patterns among cyber threats.
9. **Community Support:** MISP has an active community of users, developers, and cybersecurity professionals who contribute to its development, share knowledge, and collaborate on threat intelligence initiatives.

MISP is widely used by various organizations, including government agencies, threat intelligence teams, and cybersecurity service providers, to enhance their ability to detect, analyze, and respond to cyber threats more effectively. Its open-source nature and commitment to information sharing make it a valuable tool in the fight against cybercrime and the protection

Your college network information:

The entire campus is connected with fiber backbone, and internal blocks are connected with local area networks with 310 Mbps (1:1) high-speed internet connectivity to all computer systems available in the college. The college has various high-speed advanced servers such as IBM X3650M3, HP make of Domain servers, ERP Server, Linux Server, Web Servers and Moodle LMS Server. All faculty members provided with College Mail id (@nec.edu.in) through G-suite. HP DL380 Gen10 File server, HP DL380 Gen9 server with 48 TB storage capacity is available to ensure the reliable storage of data for staff and students. Sophos XG550 firewall is used to provide secured internet access along with a monitoring system. The other IT services and application portals supported by the ICTS centre are Student Attendance (Student Attendance Monitory System), Exam Process Automation (Automation of Examination Process) and Faculty profile updation. A biometric-based staff attendance system also has been implemented. All the departments are provided with a smart interactive board for the teaching and learning process. Internet Details The details of the internet facility on our campus are 155 Mbps Airtel (1:1) leased line internet connectivity 155 Mbps Reliance (1:1) leased line internet connectivity Microsoft Edu Cloud Campus Agreement, the entire campus is WiFi enabled by 189 numbers dual-band Ruckus access points with Ruckus wireless controller (Zone Director 3000) and 310 Mbps internet connectivity to allow the students and staff to access the internet wherever they are. WiFi coverage is not only in classrooms but also extends to all the areas, including Library and hostels. The websites browsed by students are regularly monitored.

How you think you deploy soc in your college

Deploying a Security Operations Center (SOC) in an organization involves careful planning, resource allocation, and a structured approach. Here are the key steps to deploy a SOC:

Assessment and Requirements Gathering:

- Conduct a thorough assessment of the organization's current cybersecurity posture, including existing security measures, tools, and processes.
- Identify the specific security challenges, risks, and compliance requirements that a SOC will address.
- Define the goals and objectives of the SOC deployment to align with the organization's overall security strategy.

Budget and Resource Allocation:

- Determine the budget and resource requirements for establishing and maintaining the SOC.
- Allocate personnel, hardware, software, and other necessary resources to support the SOC operations.

Build a Skilled Team:

- Recruit or assign skilled security professionals to form the SOC team.
- The team should include security analysts, incident responders, threat hunters, and SOC management personnel.

Infrastructure and Technology Setup:

- Establish the physical or virtual infrastructure for the SOC, including servers, network equipment, and storage.
- Deploy the required security technologies, such as SIEM, intrusion detection and Prevention systems (IDS/IPS), firewalls, endpoint protection, and threat intelligence feeds.

Implement Monitoring and Alerting:

- Configure the SIEM to generate real-time alerts based on predefined correlation rules and security use cases.
- Fine-tune alerting thresholds to minimize false positives and focus on critical alerts.

Threat Intelligence:

Threat intelligence refers to the knowledge and insights gained from analyzing and understanding potential cyber threats, including the methods, motivations, and capabilities of threat actors. It involves collecting, processing, and analyzing vast amounts of data from various sources to identify and assess potential risks to an organization's cybersecurity.

Key aspects of threat intelligence include:

1. **Data Collection:** Threat intelligence involves gathering data from diverse sources, such as security logs, threat feeds, dark web forums, incident reports, and open-source intelligence.
2. **Analysis and Contextualization:** The collected data is analyzed and contextualized to identify patterns, trends, and relationships that provide a deeper understanding of potential threats.
3. **Types of Threat Intelligence:** Threat intelligence can be categorized into strategic, tactical, and operational intelligence. Strategic intelligence helps in understanding the overall threat landscape, while tactical and operational intelligence focus on specific threats and their mitigations.
4. **Indicators of Compromise (IOCs):** Threat intelligence often involves identifying IOCs, which are artifacts or patterns of behavior associated with malicious activities, such as IP addresses, domain names, malware hashes, or suspicious file paths.
5. **Threat Actor Attribution:** In some cases, threat intelligence attempts to attribute cyber threats to specific threat actors or groups, helping organizations understand their motivations and potential targets.
6. **Sharing and Collaboration:** Threat intelligence is most effective when shared and collaborated on within the cybersecurity community, as it enhances collective defenses and enables faster response to emerging threats.
7. **Proactive Defense:** Threat intelligence allows organizations to proactively defend against potential threats by identifying vulnerabilities and implementing preventive measures.
8. **Incident Response and Forensics:** Threat intelligence supports incident response and digital forensics efforts by providing insights into the nature and scope of cyberattacks.
9. **Risk Management and Decision Making:** Threat intelligence informs risk assessments and decision-making processes, helping organizations prioritize security investments and resource allocations.

Overall, threat intelligence is a vital component of a robust cybersecurity strategy. By leveraging threat intelligence effectively, organizations can better understand the threat landscape, detect and respond to cyber threats proactively, and enhance their overall resilience against evolving cyber risks.

Incident Response:

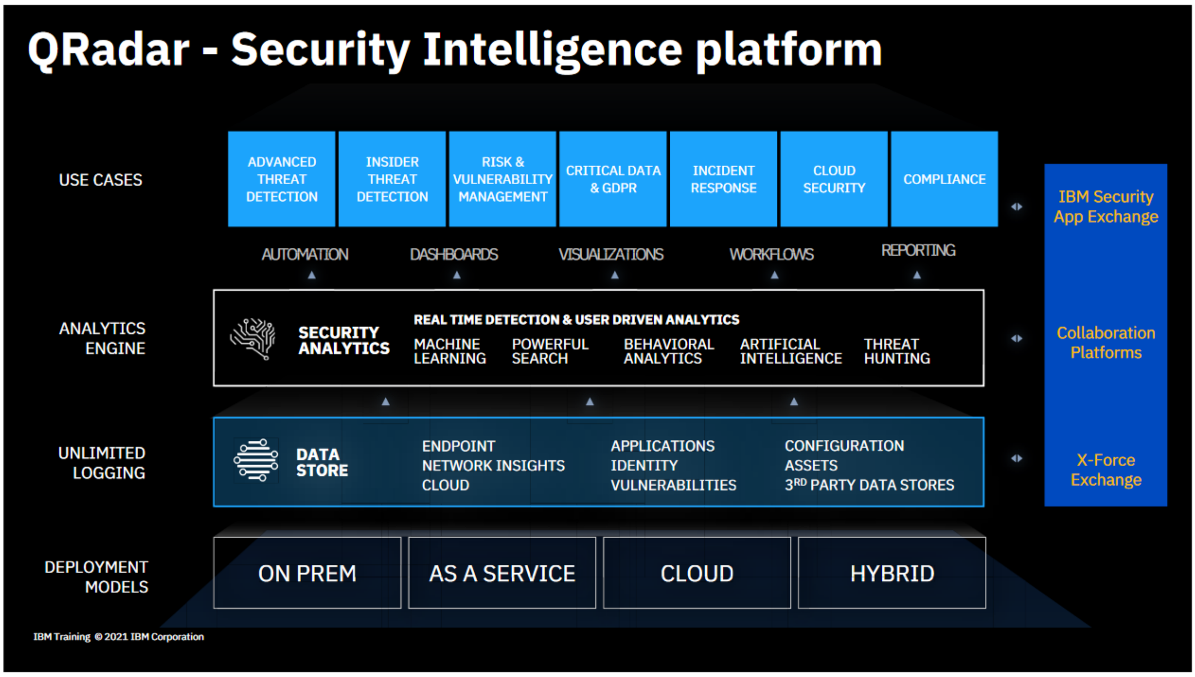
Incident Response (IR) is a structured approach taken by organizations to effectively manage and respond to cybersecurity incidents. It involves a series of actions and procedures aimed at identifying, containing, eradicating, and recovering from security incidents. The primary goal of incident response is to minimize the impact of a cybersecurity breach or attack and restore normal operations as quickly as possible. Here are the key aspects of incident response:

1. **Preparation:** Incident response begins with proactive planning and preparation. Organizations establish an Incident Response Plan (IRP) that outlines the roles and responsibilities of the incident response team, the communication procedures, and the steps to be taken in case of different types of incidents.
2. **Detection and Identification:** The first step in incident response is detecting and identifying potential security incidents. This is done through various means, such as real-time monitoring, security alerts from SIEM, intrusion detection systems (IDS), or reports from employees or users.
3. **Containment:** Once an incident is confirmed, the focus shifts to containing its spread and limiting its impact on the organization's network, systems, or data. This may involve isolating affected systems, disabling compromised accounts, or blocking malicious traffic.
4. **Eradication:** After containment, the next step is eradicating the root cause of the incident. This involves identifying and removing the source of the attack, closing vulnerabilities, and eliminating any traces of malicious activity.
5. **Recovery:** With the threat eradicated, the focus shifts to recovering affected systems and services to their normal functioning state. This may involve restoring data from backups, reinstalling software, and verifying the integrity of the restored systems.
6. **Lessons Learned and Improvement:** Post-incident, the incident response team conducts a thorough analysis of the incident. Lessons learned are used to improve the incident response plan, update security measures, and implement necessary changes to prevent similar incidents in the future.
7. **Communication:** Throughout the incident response process, effective communication is vital. The incident response team communicates with key stakeholders, such as management, employees, customers, and regulatory authorities, providing updates on the incident, response progress, and mitigation efforts.
8. **Forensic Analysis:** In cases of more sophisticated or severe incidents, a detailed forensic analysis may be conducted to understand the scope, impact, and tactics of the attackers. This information helps improve incident response strategies and contributes to threat intelligence.

Incident response is a dynamic and iterative process that requires collaboration among different teams, including IT, security, legal, and communications. A well-prepared and executed incident response capability is crucial for minimizing damage, reducing downtime, and maintaining the trust and confidence of stakeholders during and after a cybersecurity incident.

QRADAR:

IBM QRadar is a powerful Security Information and Event Management (SIEM) tool that provides real-time monitoring, threat detection, and incident response capabilities for organizations. It is designed to help security teams efficiently manage and analyze vast amounts of security event data to identify potential threats and respond to cybersecurity incidents effectively.



QRadar - Security Intelligence platform

USE CASES

ADVANCED THREAT DETECTION | INSIDER THREAT DETECTION | RISK & VULNERABILITY MANAGEMENT | CRITICAL DATA & GDPR | INCIDENT RESPONSE | CLOUD SECURITY | COMPLIANCE

AUTOMATION | DASHBOARDS | VISUALIZATIONS | WORKFLOWS | REPORTING

ANALYTICS ENGINE

SECURITY ANALYTICS

REAL TIME DETECTION & USER DRIVEN ANALYTICS

MACHINE LEARNING | POWERFUL SEARCH | BEHAVIORAL ANALYTICS | ARTIFICIAL INTELLIGENCE | THREAT HUNTING

UNLIMITED LOGGING

DATA STORE

ENDPOINT
NETWORK INSIGHTS
CLOUD

APPLICATIONS
IDENTITY
VULNERABILITIES

CONFIGURATION
ASSETS
3RD PARTY DATA STORES

DEPLOYMENT MODELS

ON PREM | AS A SERVICE | CLOUD | HYBRID

IBM Security App Exchange

Collaboration Platforms

X-Force Exchange

IBM Training © 2021 IBM Corporation

QRadar - Security Intelligence platform

Key features and functionalities of QRadar:

1. **Data Collection:** QRadar collects security event data from various sources, including network devices, servers, applications, firewalls, antivirus solutions, and more. It supports the integration of diverse log formats and protocols.
2. **Event Correlation:** QRadar uses advanced correlation techniques to analyze and correlate data from different sources. This helps identify patterns, relationships, and potential security incidents that might not be evident from individual events.
3. **Real-time Monitoring:** QRadar provides real-time monitoring of security events, generating alerts for suspicious activities, anomalies, and potential threats.
4. **Rules and Offenses:** Security analysts can create custom rules and use built-in rule sets to define conditions for triggering offenses (security incidents). Offenses help prioritize and categorize potential threats for further investigation.
5. **Threat Intelligence Integration:** QRadar can integrate with external threat intelligence feeds, enriching its analysis with up-to-date information about emerging threats and attack patterns.
6. **Incident Response:** QRadar supports incident response workflows, allowing security teams to track and manage incidents through the investigation and remediation process.
7. **Dashboards and Reports:** QRadar offers customizable dashboards and extensive reporting capabilities. These provide visual representations of security data and trends, facilitating decision-making and reporting to stakeholders.
8. **Anomaly Detection:** The tool leverages machine learning algorithms for anomaly detection, identifying deviations from normal behavior that may indicate potential security threats.
9. **Forensics and Investigation:** QRadar supports post-incident forensics and investigation by providing a comprehensive historical view of security events and activities.
10. **Integration with Other Security Solutions:** QRadar can integrate with other security tools and technologies, such as endpoint protection, vulnerability scanners, and threat intelligence platforms, to enhance the overall cybersecurity ecosystem.

11. **Automated Response:** QRadar can automate certain response actions, allowing security teams to respond to specific threats quickly and efficiently.
12. **Community Support:** As part of the broader cybersecurity community, QRadar benefits from an active user base and community support, contributing to its continuous improvement and threat intelligence sharing.

QRadar's capabilities make it a valuable tool for security operations centers (SOCs), incident response teams, and cybersecurity professionals, enabling them to stay vigilant, detect threats in real-time, and respond effectively to a wide range of cyber threats.

Conclusion:

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

Web application testing is a comprehensive process involving the evaluation of web-based applications to ensure their functionality, security, performance, and usability meet desired standards. It includes functional testing to verify features and user interactions, security testing to identify vulnerabilities, and performance testing to assess responsiveness under different conditions. Usability, compatibility, accessibility, regression, integration, data validation, error handling, caching, and compliance testing are also integral parts of the process. Web application testing is essential for delivering reliable, secure, and user-friendly applications that adhere to industry standards and user expectations.

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

From the Nessus report, I understand that Nessus is a widely used vulnerability scanning tool that helps identify security weaknesses in a network or system. The Nessus report provides a detailed analysis of the vulnerabilities discovered during the scanning process. It typically includes the following information:

1. **Scan Summary:** The report provides an overview of the scan, including the target system or network, date of the scan, and the duration of the scanning process.
2. **Vulnerability Details:** It lists the specific vulnerabilities that Nessus has identified during the scan. Each vulnerability is described with its severity level, a detailed explanation of the issue, and the potential impact on the target system.
3. **CVE Identifiers:** The report includes Common Vulnerabilities and Exposures (CVE) identifiers for each vulnerability, allowing security professionals to access additional information about the vulnerabilities from the CVE database.
4. **Recommendations:** For each identified vulnerability, the report often includes recommended actions or mitigation measures to address the issue and reduce the risk.
5. **Risk Scoring:** Nessus may provide a risk score for each vulnerability, indicating the level of risk associated with each security flaw. This score helps prioritize the remediation efforts based on the severity of the vulnerabilities.
6. **Affected Hosts:** The report specifies the hosts or systems where the vulnerabilities were found, allowing administrators to pinpoint the affected assets.
7. **False Positives:** Nessus may identify some findings as potential vulnerabilities that are not actually security risks. The report may include a section for false positives, explaining why certain items may not pose a threat.

8. **Compliance Checks:** If configured, Nessus can perform compliance checks against industry standards or regulatory requirements. The report may include compliance results, indicating the organization's adherence to specific security standards.
9. **Historical Data:** For regular scanning, the report may include historical data, allowing users to compare the results with previous scans and track the progress of vulnerability remediation efforts.
10. **Executive Summary:** For management and stakeholders, the report may include an executive summary that provides a high-level overview of the most critical vulnerabilities and the overall security posture of the organization.

Nessus reports are essential tools for security professionals and IT administrators to understand the security status of their systems, prioritize vulnerability remediation, and maintain a proactive approach to cybersecurity.

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

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.

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:

a. Centralized Log Management: SIEM aggregates log data from diverse sources, making it easier for analysts to access and analyze information from a single dashboard.

b. Early Threat Detection: SIEM tools can identify patterns and anomalies in the data, enabling early detection of security incidents and potential breaches.

c. Simplified Incident Investigation: SIEM allows analysts to correlate events from different sources, providing a comprehensive view of security incidents for faster and more accurate investigations.

d. Compliance and Reporting: SIEM can help organizations meet regulatory compliance requirements by generating security reports and audits.

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:

a. Real-Time Visibility: The QRadar dashboard provides real-time visibility into security events and incidents, enabling analysts to respond promptly to emerging threats.

b. Customizable Visualizations: Analysts can customize the dashboard to display relevant information, such as top threats, network traffic, or security incidents.

c. Threat Intelligence Integration: QRadar integrates with various threat intelligence feeds, enhancing its ability to detect and respond to advanced threats.

d. Incident Response Automation: The QRadar dashboard can be integrated with automation tools to streamline incident response processes. It's important to note that the effectiveness of these security measures relies on the expertise of the security team, the quality of data collected, and the organization's commitment to maintaining a strong security posture. Continuous monitoring, analysis, and improvement are crucial for maximizing the outcomes and benefits of SOC, SIEM, and QRadar implementations.

Future Scope :-

Stage 1 :- Future scope of web application testing

The future scope of web application testing is promising, with increased complexity due to advanced technologies like SPAs and PWAs, a focus on mobile and IoT testing, and the integration of AI and ML into testing tools. Security testing will remain a priority, with continuous advancements in performance testing for enhanced user experience. Integration with DevOps and continuous testing will streamline development processes, and shift-left testing will detect and fix issues early. API testing, blockchain testing, and compliance testing will become more crucial, while cloud-based testing and crowdsourced testing will be widely adopted. The future of web application testing will rely on innovation, automation, and a strong emphasis on cybersecurity to deliver secure and high-quality applications in the dynamic digital landscape.

Stage 2 :- Future scope of testing process you understood

The future scope of the testing process is promising, driven by advancements in technology, methodologies, and industry demands. AI and ML integration will lead to smarter and more automated testing, while shift-left testing will empower developers to take ownership of testing for faster bug detection. Continuous testing and DevOps will ensure quality throughout the software delivery pipeline. IoT, API, and microservices testing will address the challenges posed by emerging technologies, and performance testing will focus on scalability. Security testing will grow in importance to combat cyber threats, and cloud-based testing will gain popularity for its scalability and cost-effectiveness. Automation, virtualization, and containerization will streamline testing practices, and data management and analytics will play key roles in ensuring test efficiency. Overall, the future of testing will be marked by efficiency, innovation, and a focus on delivering high-quality software in a rapidly evolving digital landscape.

Stage 3 :- Future scope of SOC / SEIM

The future scope of Security Operations Center (SOC) and Security Information and Event Management (SIEM) is promising, driven by advanced threat detection with analytics and machine learning, adaptability to cloud and hybrid environments, integration with XDR for comprehensive threat response, and increased automation and orchestration to streamline incident handling. SOC and SIEM systems will actively participate in threat intelligence sharing networks, incorporate User and Entity Behaviour Analytics (UEBA) to identify anomalous behaviours, and extend monitoring to IoT and OT environments. Compliance support, proactive threat hunting, and managed services will be emphasized, along with human-machine collaboration for more effective cybersecurity operations. Additionally, SOC and SIEM will address future challenges related to quantum computing and post-quantum security to maintain robust protection against 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, Nessus, NMAP

Tools Explored: -

Nessus, cybermap, chaptgpt, OWASP top 10 vulnerabilities(2021), CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, IBM fix central, QRadar Installation, mobaxterm, tools-nmtui, Nmap, sqlmap, Identify fixes-wincollect agent, metasploitable, malware bytes.

----THE END----