STUDY OF CYBER SECURITY THAT BRINGS SECURITY THREATS TO LIGHT BEFORE THEY HARM BUSINESS OPERATIONS

Overview :-

A web application is application software that is accessed using a web browser. Web applications are delivered on the World Wide Web to users with an active network connection. Web application security is the idea of building websites to function as expected, even when they are under attack. The concept involves a collection of security controls engineered into a Web application to protect its assets from potentially malicious agents. Web applications, like all software, inevitably contain defects. Some of these defects constitute actual vulnerabilities that can be exploited, introducing risks to organizations.

Web application security defends against such defects. It involves leveraging secure development practices and implementing security measures throughout the software development life cycle (SDLC), ensuring that design-level flaws and implementation-level bugs are addressed. Testing the security of a Web application often involves sending different types of input to provoke errors and make the system behave in unexpected ways. These so called “negative tests” examine whether the system is doing something it isn’t designed to do.

Web applications need to freely allow traffic through a variety of ports and usually require authentication; this means they also require a complex web application vulnerability scanner. Since websites must allow traffic to come and in and out of the network, hackers often attack the most commonly used ports. This includes:

- Port 80 (HTTP): For unsecured website traffic
- Port 443 (HTTPS): For secured website traffic
- Port 21 (FTP): The file transfer protocol for transferring files to and from your servers
- Ports 25 (SMTP), for simple mail transfer protocol, and port 110 (POP3), the default unencrypted port: Email protocols often used by organizations to send and receive email.

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

Tools discussed to reach the milestones

- Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources.

- PortSwigger offers tools for web application security, testing, & scanning. Choose from a range of security tools, & identify the very latest.

- Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

- Security information and event management, SIEM for short, is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

- QRadar is a network security management platform that provides situational awareness and compliance support. QRadar uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

List of teammates–

S.no	Name	Collage	contact
1	Dr.R.Menaka AP/IT	Velalar College of Engineering and Technology, Erode, Tamilnadu.	9842042627
2	Dr.M.Kavitha ASP/IT		9500719815
3			

List of Vulnerability Table –

Name of The Vulnerability	References-CWE
Broken Access Control	CWE-35 Path Traversal: '.../...//'
Cryptographic Failures	CWE-319 Cleartext Transmission of Sensitive Information
Injection	CWE-20 Improper Input Validation
A04 Insecure Design	CWE-235 Improper Handling of Extra Parameters
A05 Security Misconfiguration	CWE-16 Configuration
A06 Vulnerable and Outdated Components	CWE-1104 Use of Unmaintained Third Party Components
A07 Identification and Authentication Failures	CWE-287 Improper Authentication
A08 Software and Data Integrity Failures	CWE-345 Insufficient Verification of Data Authenticity
A09 Security Logging and Monitoring Failures	CWE-778 Insufficient Logging
A10 Server Side Request Forgery (SSRF)	CWE-918 Server-Side Request Forgery (SSRF)

REPORT:-

1 Vulnerability Name: Path Traversal: '.../...//'

CWE : CWE-35

OWASP Category: A01:2021 – Broken Access Control

Description: if pathname to access directory or files not properly neutralize '.../...//' (doubled triple dot slash) then path sequences can resolve to a location that is outside of that directory or otherwise construct a pathname resolved to a location that are not within a restricted directory,

Business Impact: The path traversal flaw occurs when the user parameters aren't sanitised and/or there is a lack of access control to the resources. It's then possible for an attacker to modify the parameters of the request to ask to return other resources. The impact of this flaw is generally critical. A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder.

Why Does The Path Traversal Vulnerability Occur?

1. **Insecure input validation:** if user input is not properly validated, it may be possible for an attacker to inject malicious input that could be used to exploit a path traversal vulnerability.

2. **Poorly configured web servers:** if a web server is not properly configured, it may be possible for an attacker to access restricted directories.

3. **Insecure file permissions:** if files or directories have lax permissions, it may be possible for an attacker to gain access to them.

So, The attacker might be able:

- to read files, potentially:
  - Configuration files where there are usually secrets (credentials, keys…) which then allow to exploit new vulnerabilities,
  - Sensitive operating system files,
- to read the source code,
- to analyse the organisation of the server,
- sometimes to write on the server, which can lead to:
  - a modification of the application's behaviour,
  - even, to take control of the server.

How to protect yourself from path traversal?

To avoid these flaws, several measures should be implemented:

- Do not use user input directly to call a file.
- User data shouldn't be interpreted. It should be encoded, escaped and cleaned.
- It should be validated against a list of allowed expressions. If this isn't possible, then the validation must confirm that there are only allowed contents (e.g. only alphanumeric characters).

2. Vulnerability Name: Cleartext Transmission of Sensitive Information

CWE : CWE-319

OWASP Category:A02:2021-Cryptographic Failures

Description:

Cleartext is the one where the data is unencrypted and is not intended for the encryption process.

Business Impact:The first thing is to determine the protection needs of data in transit and at rest. Encrypts credit card numbers in a database using automatic database encryption and allowing data to automatically decrypted when retrieved, allowing a SQL injection flaw to retrieve credit card numbers in clear text. Between transmits to rest, sensitive or security-critical data in cleartext in a communication channel surely be sniffed by unauthorized actors.

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., GDPR and PCI DSS.

3 Vulnerability Name: Improper Input Validation

CWE : CWE-20

OWASP Category: A03:2021 – Injection

Description: **Input validation** is a frequently-used technique for checking potentially dangerous **inputs** in order to ensure that the **inputs** are safe for processing . Improper input validation or unchecked user input is a type of vulnerability in computer software that may be used for security exploits. This vulnerability is caused when "[t]he product does not validate or incorrectly validates input that can affect the control flow or data flow of a program."

Business Impact: For web applications, input validation usually means verifying user inputs provided in web forms, query parameters, uploads, and so on. Missing or improper input validation is a major factor in many web security vulnerabilities, including cross-site scripting (XSS) and SQL injection. Eg. Cookies are another common source of user input. Like form data, cookies can be used to input data into your application. However, cookies are often used to store session information, and if they are not properly validated, they can be used to hijack user sessions.

4 Vulnerability Name: Improper Handling of Extra Parameters

CWE : CWE-235

OWASP Category: A04:2021 – 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: Several versions of Apache Tomcat 5, 6, and 7 inefficiently handled parameters. Attackers could use this inefficency to overload the system with an extreme amount of parameters to cause a denial of service attack.

5 Vulnerability Name: Configuration

CWE : CWE-16

OWASP Category: A05:2021 – Security Misconfiguration

Description: Weaknesses in this category are typically introduced during the configuration of the software.

Business Impact: The application server's configuration allows detailed error messages, e.g., stack traces, to be returned to users. This potentially exposes sensitive information or underlying flaws such as component versions that are known to be vulnerable.

6 Vulnerability Name: Use of Unmaintained Third Party Components

CWE : CWE-1104

OWASP Category: A06:2021 Vulnerable and Outdated Components

Description: Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete.

Business Impact: This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities.

7 Vulnerability Name: Improper Authentication

CWE : CWE-287

OWASP Category: A07:2021 Identification and Authentication Failures

Description: Examples of improper authentication vulnerabilities include: No authentication: When there is no authentication for a critical function, then attackers get unrestricted access easily

Business Impact: . Weak passwords: When users choose weak passwords, it makes it easier for attackers to guess or crack them. Authentication vulnerabilities are issues that affect authentication processes and make websites and applications susceptible to security attacks in which an attacker can masquerade as a legitimate user

8 Vulnerability Name: Insufficient Verification of Data Authenticity

CWE : CWE-345

OWASP Category: A08:2021 Software and Data Integrity Failures

Description his class of weaknesses is a result of trust issues between data exchange parties. If the application fails to verify data origin or its authenticity, an attacker might be able to perform spoofing attacks against vulnerable application or their clients.

Business Impact: This weakness occurs when the application transmits or stores authentication credentials and uses an insecure method that is susceptible to unauthorized interception and/or retrieval. When the Access Control List (ACL) connected to the NGC folder is corrupted, the error message “Your credentials could not be verified” may also appear. In this case, you can try to reset the ACL in safe mode to fix the matter.

9 Vulnerability Name: Insufficient Logging

CWE : CWE-778

OWASP Category: A09:2021 Security Logging and Monitoring Failures

Description: Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident . Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.

Business Impact: . One strategy for determining if you have sufficient monitoring is to examine the logs following penetration testing. The testers’ actions should be recorded sufficiently to understand what damages they may have inflicted.

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

CWE : CWE-918

OWASP Category: A10:2021:Server Side Request Forgery (SSRF)

Description: Server-side request forgery is a type of computer security exploit where an attacker abuses the functionality of a server causing it to access or manipulate information in the realm of that server that would otherwise not be directly accessible to the attacker.

Business Impact: let an attacker send crafted requests from the back-end server of a vulnerable application. Criminals usually use SSRF attacks to target internal systems that are behind firewalls and are not accessible from the external network. An attacker may also leverage SSRF to access services available through the loopback interface (127.0.0.1) of the exploited server.

Stage 2

Overview :-

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it. Nessus tool used by an administrator in charge of any computer (or group of computers) connected to the internet, Nessus is a great tool help keep their domains free of the easy vulnerabilities that hackers and viruses commonly look to exploit.

Key points include:

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

Nessus is used during penetration testing and vulnerability assessments, including malicious assaults. It is a program that scans computers for security holes that hackers could exploit. When running on a computer, Nessus examines each port to see whether or not hackers may exploit any vulnerabilities to launch damaging attacks. Nessus will test each service once it has determined what is operating on each port to ensure no vulnerabilities.

Target website ━www.w3schools.com

Target ip address:- 192.229.173.207

Vulnerabilities Total: 24

List of vulnerability ━

s.no	Vulnerability name	Severity	plugins
1	Common Platform Enumeration (CPE)	INFO	45590
2	Device Type	INFO	54615

3	**HSTS Missing From HTTPS Server**	**INFO**	**84502**
4	**HTTP Methods Allowed (per directory)**	**INFO**	**43111**
5	**HTTP Server Type and Version**	**INFO**	**10107**
6	**HyperText Transfer Protocol (HTTP) Information**	**INFO**	**24260**
7	**Nessus SYN scanner**	**INFO**	**11219**
8	**Nessus Scan Information**	**INFO**	**19506**
9	**- OS Identification**	**INFO**	**11936**
10	**SSL / TLS Versions Supported**	**INFO**	**56984**
11	**SSL Certificate Information**	**INFO**	**10863**
12	**SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)**	**INFO**	**95631**
13	**SSL Cipher Block Chaining Cipher Suites Supported**	**INFO**	**70544**
14	**SSL Cipher Suites Supported**	**INFO**	**21643**
15	**SSL Perfect Forward Secrecy Cipher Suites Supported**	**INFO**	**57041**
16	**SSL Root Certification Authority Certificate Information**	**INFO**	**94761**
17	**SSL/TLS Recommended Cipher Suites**	**INFO**	**156899**
18	**Service Detection**	**INFO**	**22964**
19	**TCP/IP Timestamps Supported 192.229.173.207 4**	**INFO**	**25220**
20	**TLS ALPN Supported Protocol Enumeration**	**INFO**	**84821**
21	**TLS NPN Supported Protocol Enumeration**	**INFO**	**87242**
22	**TLS Next Protocols Supported**	**INFO**	**62564**
23	**TLS Version 1.2 Protocol Detection**	**INFO**	**136318**
24	**Traceroute Information**	**INFO**	**10287**

REPORT:-

Vulnerability Name:- Common Platform Enumeration

severity : - Info

Plugin:- 45590

Port :- HTTPS 443

Description:- A standard method of describing and identifying classes of applications, operating systems, and hardware devices

Solution:-: A standard machine-readable format for encoding names of IT products and platforms

Business Impact::- workflow will be automated

Vulnerability Name:- Common Platform Enumeration

severity : - Info

Plugin:- 87242

Port :- HTTPS 443

Description:- A standard method of describing and identifying classes of applications, operating systems, and hardware devices

Solution:-: A standard machine-readable format for encoding names of IT products and platforms

Business Impact::- workflow will be automated

Vulnerability Name:- TLS NPN Supported Protocol Enumeration

severity : - Info

Plugin:- 87242

Port :- 443

Description:- The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

Solution:- renegotiations on the same connection MUST NOT include the next_protocol_negotiation extension..

Business Impact::- ALPN and NPN are both TLS extensions that allow the server and the client to exchange a list of supported protocols during the TLS handshake.

Vulnerability Name:- TLS Next Protocols Supported

severity : - Info

Plugin:- 62564

Port :- 443

Description:- This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Solution:- The remote service advertises one or more protocols as being supported over TLS.

Business Impact::- However, it also permits an unprecedented amount of attacker control over the contents of the connection.

Vulnerability Name:- TLS Version 1.2 Protocol Detection

severity : - Info

Plugin:- 136318

Port :- 443

Description:- The remote service accepts connections encrypted using TLS 1.2.

Solution:- Safety communiciation

Business Impact::- The TLS implementations use secure algorithms where possible while not preventing connections from or to legacy clients or servers.

Vulnerability Name:- Traceroute Information

severity : - Info

Plugin:- 10287

Port :- 33434

Description:- The TRACERT diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination.

Solution:- it was possible to obtain traceroute information.

Business Impact::- can use TRACERT to find out where a packet stopped on the network.

Stage 3 Report

Title :- ALERT TO PREVENT DATA BREACHES BY TWO EYES SOC AND SIEM PLATFORM

Security operations center, SOC is a team of experts that proactively monitor an organization's ability to operate securely. Increasingly, today's SOC is less a single room full of people that led the SOC team to be more remotely distributed and more concern to essential security function in an organization. They are responsible for a variety of activities, including proactive monitoring, incident response and recovery, remediation activities, compliance, and coordination and context.

- **Proactive Monitoring:**

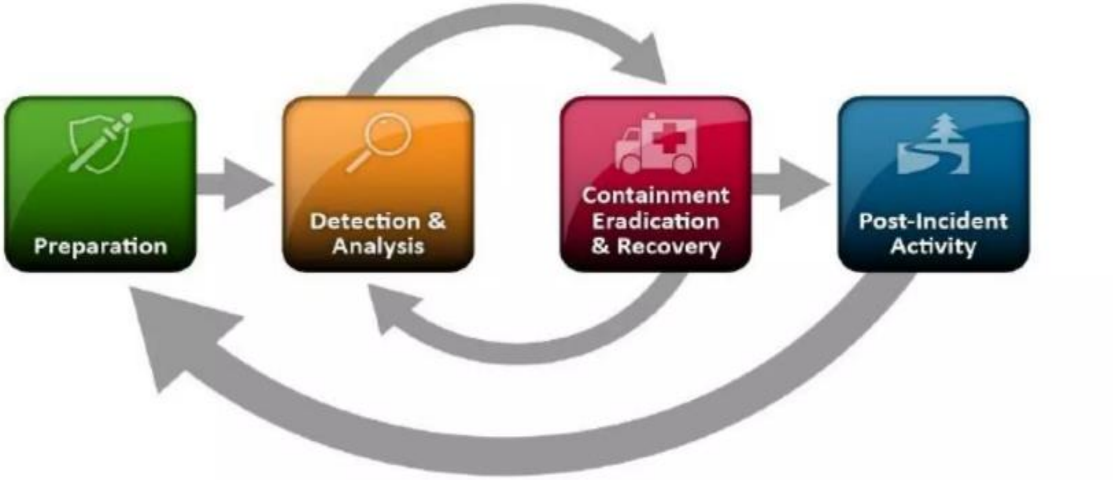
  * log file analysis.-> Logs can come from end points (e.g., a notebook computer, a mobile phone or an IoT device) or from network resources, such as routers, firewalls, intrusion detection system (IDS) applications and email appliances.

  *threat monitoring. SOC team members work with various resources, which can include other IT workers (e.g., help desk technicians), as well as artificial intelligence (AI) tools and log files.

- **Incident Response and Recovery:** A SOC coordinates an organization's ability to take the necessary steps to mitigate damage and communicate properly to keep the organization running after an incident and recover.Example, recovery can include activities such as handling acute malware or ransomware incidents.
- **Remediation Activities:** SOC team members provide data-driven analysis that helps an organization address vulnerabilities and adjust security monitoring and alerting tools. For example, using information obtained from log files and other sources, a SOC member can recommend a better network segmentation strategy or a better system patching regimen. Improving existing cybersecurity is a major responsibility of a SOC.
- **Compliance:** Organizations secure themselves through conformity to a security policy, as well as external security standards,the NIST Cybersecurity Framework (CSF) and the General Data Protection Regulation (GDPR). Organizations need a SOC to help ensure that they are compliant with important security standards and best practices.
- **Coordination and Context:** Above all, a SOC team member helps an organization coordinate disparate elements and services and provide visualized, useful information. Part of this coordination is the ability to provide a helpful, useful set of narratives for activities on the network. These narratives help shape a company's cybersecurity policy and posture for the future.

A SOC team member helps an organization identify the primary causes of cyberattacks. When a SOC analyst does this, they are said to engage in root-cause analysis. In short, a SOC analyst works to figure out exactly when, how and even why an attack was successful. To this end, a SOC analyst reviews evidence of attacks. Such evidence is called an indicator of attack. If an attack is successful, a SOC analyst will then study indicators of compromise to help the organization respond appropriately, as well as make changes so that similar attacks don’t happen in the future.

SOC Life Cycle



Pain Points Identification for SOC function establishment

 * **Platform** was required to correlate and analyze the logs generated by our systems to identify the event anomalies and also critical security alerts that impede our ability to effectively respond to the potential threats.

* Sufficient **playbook & automation** to do around-the-clock monitoring of our security infrastructure for timely detection and response to the potential threats.

SIEM Technology Implementation

Security information and event management, SIEM for short, is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

We start identifying the feasible solution to overcome our pain point by looking at the platform which has the capability to collect, aggregate, filter, store, correlate and visualize security-relevant data and form it into actionable information. The relevant technology which will be able to accommodate this requirement is Security Information and Event Management (SIEM).

SIEM Technology will help us to collect the logs, time-strapped records of events, using either agentless or agent-based mechanisms and once the logs are aggregated within the SIEM, the next step will be the normalization process by using various analytical techniques, including log correlation and machine learning algorithms.

 SIEM event lifecycle.

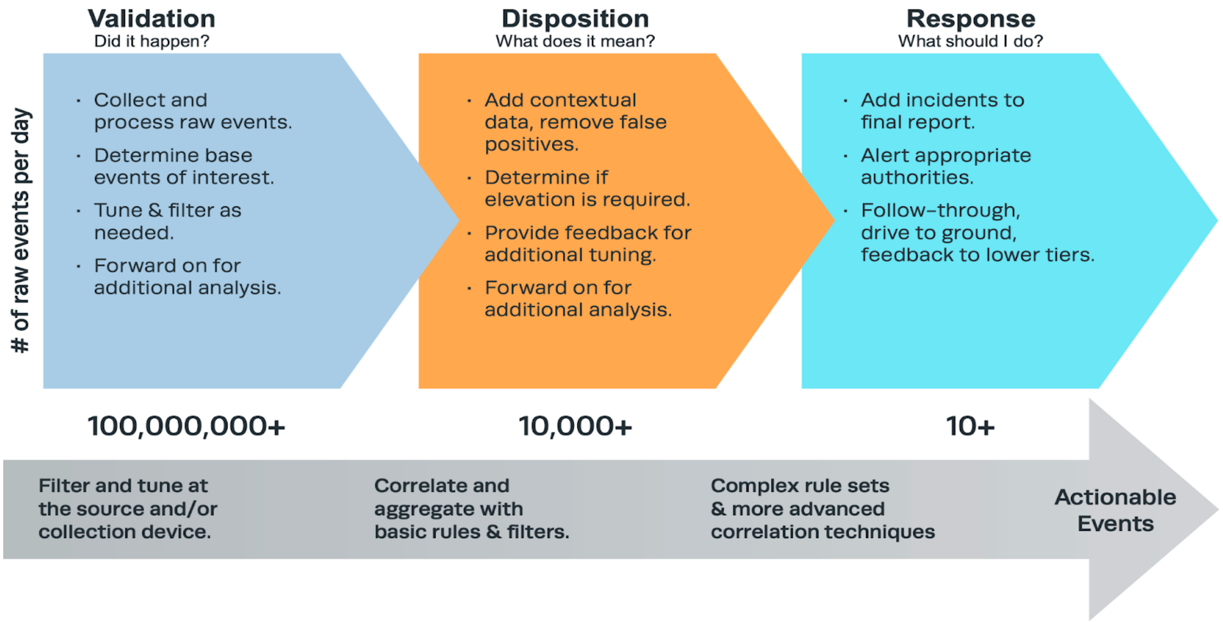

Validation
Did it happen?
· Collect and process raw events.
· Determine base events of interest.
· Tune & filter as needed.
· Forward on for additional analysis.
Disposition
What does it mean?
· Add contextual data, remove false positives.
· Determine if elevation is required.
· Provide feedback for additional tuning.
· Forward on for additional analysis.
Response
What should I do?
· Add incidents to final report.
· Alert appropriate authorities.
· Follow-through, drive to ground, feedback to lower tiers.
# of raw events per day
100,000,000+
10,000+
10+
Filter and tune at the source and/or collection device.
Correlate and aggregate with basic rules & filters.
Complex rule sets & more advanced correlation techniques
Actionable Events

Figure 2. SIEM Technology Lifecycle

It help us identify and prioritize the log sources that we are going to monitor for security events that will help us to collect and analyze the relevant data sources if there are any dependencies, technical limitations that need to be addressed during the SIEM technology development.

Malware Information Sharing Platform (MISP)

The MISP is an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. In addition, MISP also helps to make the rules for network intrusion detection systems (NIDS) and enables the sharing of malware information with third parties. In simpler words, MISP aims to create a platform of trust by locally storing threat information and enhancing malware detection to encourage information exchange among organizations.

Our College IT Infrastructure

IT Management

- To maintain, secure and ensure legal and appropriate use of IT infrastructure on the campus.
- To establish the responsibilities of all IT users for protecting integrity and confidentiality of the managed and controlled information assets.
- To monitor infrastructural assets like computers, servers, laptops, LCDs, and projectors and information assets like data, network devices and documents.

No. of Systems and their Configuration

Institution has a total of 1191 computers with the following configuration: i3 / i5 / i7 Processor , 4GB / 8GB RAM, 500 GB / 1 TB HardDisk, 3.41 GHz Processor clock speed and above CPU Speed.

Internet Connection

Internet connection is distributed across the college through Wi-Fi networks. The institute regularly upgrades the internet connection every year. The campus is enabled with 24x7 Wi-Fi, 500 Mbps bandwidth connectivity. Upgrade of network infrastructure from 100 Mbps to 1000 Mbps. 61 Wi-Fi access points have been installed in the campus to improve the Internet access. The coverage of Wi-Fi is extended to all areas including classrooms, library, conference halls, cafeteria and hostels. The Wi-Fi system has been functioning with 500 Mbps (1:1) leased line connectivity provided by Wireline Solution Private Limited.

Networking Peripherals

VCET uses fibre optical networking cable with a speed of 100 / 1000 MBPS media converters and layer 2 switches like CISCO SG 500 / 350 / 300.
Lower end configurations and obsolete systems are periodically replaced with high configuration systems.

How you think you deploy soc in your college

IT Usage Policy

- To ensure that institution’s proprietary information stored on electronic and computing devices remains its sole property. It should be ensured that proprietary information is protected in accordance with Data protection Standard.
- Every user on the premises has a responsibility to promptly report the theft, loss or unauthorized disclosure of institution’s proprietary information.
- Members of Velalar College of Engineering and Technology may access proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.
- Authorized individuals may monitor systems and network traffic at any time.

IT Security Policy

- Installation of Anti-malware software, Firewalls and access authentication systems.
- Effective security is a team effort involving the participation and support of every IT user.

Firewall/Security

VCET uses firewall service from MIKROTIK CLOUD CONTROL ROUTER and have lifetime validity.

Surveillance Facilities

There is a 24/7 CCTV surveillance security available in the institution. Through this security system, the faculty members and students have been secured from unwanted grievances.

All the faculty members, students, technical staff and other workers of our institution are responsible for exercising appropriate use of information and network resources in accordance with the policies and standards.

Threat intelligence— data containing detailed knowledge about the cybersecurity threats targeting an organization. Threat intelligence helps security teams be more proactive, enabling them to take effective, data-driven actions to prevent cyber attacks before they occur. It can also help an organization better detect and respond to attacks in progress.

Security analysts create threat intelligence by gathering raw threat information and security-related from multiple sources, then correlating and analyzing the data to uncover trends, patterns and relationships that provide in-depth understand of the actual or potential threats. The resulting intelligence is

- Organization-specific, focused not on generalities (e.g., lists of common malware strains) but on specific vulnerabilities in the organization's attack surface, the attacks they enable, and the assets they expose

- Detailed and contextual, covering not only the threats targeting the company but the threat actors who may carry out the attacks, the tactics, techniques and procedures (TTPs) those threat actors use, and the indicators of compromise (IoCs) that may signal a specific cyberattack

- Actionable, providing information security teams can use to address vulnerabilities, prioritize and remediate threats, and even evaluate existing or new cybersecurity tools.

Threat intelligence can furnish security teams with the information they need to detect attacks sooner, reducing detection costs and limiting the impact of successful breaches.

Incident Response

Incident response refers to an organization's processes and technologies for detecting and responding to cyberthreats, security breaches or cyberattacks. The goal of incident response is to prevent cyberattacks before they happen, and to minimize the cost and business disruption resulting from any cyberattacks that occur.

The Incident Response Process

Preparation. This first phase of incident response is also a continuous one, to make sure that the CSIRT always has best possible procedures and tools in place to respond to identify, contain and recover from an incident as quickly as possible and within minimal business disruption.

Detection and Analysis. During this phase, security team members monitor the network for suspicious activity and potential threats. They analyze data, notifications and alerts gathered from device logs and from various security tools (antivirus software, firewalls) installed on the network, filtering out the false positives and triage the actual alerts in order of severity.

Containment. The incident response team takes steps to stop the breach from doing further damage to the network. Containment activities can be split into two categories:

Short-term containment measures focus on preventing the current threat from spreading by isolating the affected systems, such as by taking infected devices offline.

Long-term containment measures focus on protecting unaffected systems by placing stronger security controls around them, such as segmenting sensitive databases from the rest of the network.

Eradication. Once the threat has been contained, the team moves on to full remediation and complete removal of the threat from the system. This involves actively eradicating the threat itself—e.g., destroying malware, booting an unauthorized or rogue user from the network—and reviewing both affected and unaffected systems to ensure no traces of the breach are left behind.

Recovery. When the incident response team is confident the threat has been entirely eradicated, they restore affected systems to normal operations. This may involve deploying patches, rebuilding systems from backups, and bringing remediated systems and devices back online.

Post-incident review. Throughout each phase of the incident response process, the CSIRT collects evidence of the breach and documents the steps it takes to contain and eradicate the threat. At this stage, the CSIRT reviews this information to better understand the incident. The

CSIRT seeks to determine the root cause of the attack, identify how it successfully breached the network, and resolve vulnerabilities so that future incidents of this type don't occur.

Qradar & understanding about tool

IBM QRadar is a single architecture for analyzing logs, flows, vulnerabilities, users, and asset data. It renders real-time correlation and behavioral anomaly detections to identify high-risk threats. It has high priority incident detections among multiple data points. It provides full visibility into your network, applications, and user activity.

It also has automated regulatory compliance with the collection, correlation, and reporting capabilities. IBM QRadar is a security information and event management tool that assembles data from the organization and the network devices. It is a SIEM product that was framed for enterprises so that they can connect to the operating systems, host assets, applications, vulnerabilities, user activities, and behaviors.

IBM QRadar is utilized to conduct an examination of the log data and the network flows in real-time so malignant exercises can be recognized and halted in the shortest span of time. Consequently, IBM QRadar makes sure that it either prevents or minimizes the harm to its host organization.

The IBM QRadar tools

There are many different tools under IBM QRadar that aid in the data processing. The important ones are:

IBM QRadar Vulnerability Manager: This tool is used to scan the process and network vulnerability data. This data is then utilized to recognize the security risks in the network.

IBM QRadar Risk Manager: : This tool is used to collect the network infrastructure configuration and issue a draft of the network topology. The data can be practiced to control risk by the simulation of network situations by executing rules and modifying the configurations in the network.

IBM QRadar Incident Forensics : This tool is used to conduct in-depth network forensics and replays full network sessions.

Conclusion :-

Stage 1 :- Common Weakness Enumeration (CWE) is a system to categorize software and hardware security flaws—implementation defects that can lead to vulnerabilities. It is a community project to understand security weaknesses or errors in code and vulnerabilities and create tools to help prevent them. CWE strives to stop vulnerabilities and bugs by educating developers on building better products that aren't susceptible to exploitation. Programmers can use CWE as a resource while writing code to prevent vulnerabilities during the development process.

Stage 2 :- Nessus identifies software flaws, missing patches, malware, denial-of-service vulnerabilities, default passwords and misconfiguration errors, among other potential flaws. The report contain following information for each record: Hostname — The record's hostname. IP Address — The IP address related to the record. Ports — The discovered open ports on the scanned IP, if applicable. A vulnerability assessment report details the security weaknesses discovered in a vulnerability assessment. It is your roadmap to a better state of security preparedness, laying out the unique risks you face due to the technology that underpins your organization.

Stage 3 :- An enterprise's security operations center (SOC), which houses IT security professionals who monitor the enterprise's security posture, are responsible for tackling cyberattacks and simultaneously addressing regulatory compliance requirements.Attackers are becoming more dangerous and regulatory mandates are continuously evolving, and basic tools just can't keep up. It's time to deploy a more sophisticated solution: security information and event management (SIEM). SIEM solutions have become an integral part of the network and data security ecosystem, and are critical in tackling advanced and targeted cyberattacks. Thus, the IBM QRadar makes sure that it either prevents or minimizes the harm to its host organization.

Future Scope :-

- Stage 1 :- CVE stands for Common Vulnerabilities and Exposures. CVE is a glossary that classifies vulnerabilities. The glossary analyzes vulnerabilities and then uses the Common Vulnerability Scoring System (CVSS) to evaluate the threat level of a vulnerability.
- Stage 2 :- Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. IBM QRadar is used to perform analysis of the log data and the network flows in real-time so that malicious activities can be identified and stopped as soon as possible. Thus gives safety for cyberspace.
- Stage 3 :- Detect, investigate, and resolve security incidents and threats using a single, scalable SIEM solution

Topics explored :- Web Application, Web services, CVE, CWE, Vulnerabilties, threat, hacking types, methodology, web testing tools, threat intelligent,planning preparation, incident response,recovery, tempmail etc

Tools explored :- Nessus, Qradar, metasploit ,mobaxterm, nsmap,s qltool, oracle vitual Box, kalilinux

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