Enhancing Security Operations: SIEM Qradar & SOC Dashboard Management

Prepared by,
Santhosh Kumar C,
Assistant Professor,
Department of Information Technology,
Sona College of Technology, Salem,
Tamil Nadu, India.
E-Mail: santhoshkumar.it@sonatech.ac.in

Stage 1

Title of the project:

Enhancing Security Operations: SIEM Qradar & SOC Dashboard Management

Overview:

Enhancing Security Operations: SIEM Qradar & SOC Dashboard Management "SIEM Implementation: The project team will deploy and configure the IBM Qradar SIEM solution, integrating it with the organization's existing network infrastructure, security devices, and data sources. This will enable centralized log collection, real-time event correlation, threat detection, and incident response capabilities. Dashboard Customization: The SOC dashboard will be designed and tailored to provide a comprehensive and intuitive view of the organization's security posture. The project team will collaborate with SOC analysts to identify key performance indicators (KPIs), relevant metrics, and visualizations that will empower analysts to effectively monitor, detect, and respond to security incidents. Threat Intelligence Integration: The SIEM system will be integrated with external threat intelligence feeds and vulnerability databases to enrich the analysis and detection capabilities. This integration will provide real-time information on emerging threats, known attack vectors, and potential vulnerabilities, empowering the SOC team to proactively respond to emerging risks.

List of teammates:

S.No.	Name of the Faculty	Designation & Collage	Contact
1.	Santhosh Kumar C	Assistant Professor Sona College of Technology	9994912969 santhoshkumar.it @sonatech.ac.in

List of Vulnerability Table

S.No.	Vulnerability Name	CWE - No
A01	Broken Access Control	CWE 285- Improper Authorization
A02	Cryptographic Failures	CWE-916: Use of Password Hash With Insufficient Computational Effort
A03	Injection	CWE-564: SQL Injection: Hibernate
A04	Insecure Design	CWE-653: Improper Isolation or Compartmentalization
A05	Security Misconfiguration	CWE-614:Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
A06	Vulnerable and Outdated Components	CWE-1395: Dependency on Vulnerable Third-Party Component
A07	Identification and Authentication Failures	CWE-521: Weak Password Requirements
A08	Software and Data Integrity Failures	CWE-565C: Reliance on Cookies without Validation and Integrity Checking
A09	Security Logging and Monitoring Failures	CWE-532: Insertion of Sensitive Information into Log File
A10	Server Side Request Forgery	CWE-918:Server Side Request Forgery

REPORT

VULNERABILITY NAME: Broken Access Control

CWE: CWE 285- Improper Authorization

OWASP CATEGORY: A01 2021 Broken Access Control

DESCRIPTION:

The product does not perform or incorrectly perform an authorization check when an actor attempts to access a resource or perform an action.

BUSINESS IMPACT:

Assuming a user with a given identity, authorization is the process of determining whether that user can access a given resource, based on the user's privileges and any permissions or other access-control specifications that apply to the resource. When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information exposures, denial of service, and arbitrary code execution.

VULNERABILITY NAME: Cryptographic Failures

CWE: CWE-916: Use of Password Hash with Insufficient Computational Effort

OWASP CATEGORY: A02 2021 Cryptographic Failure

DESCRIPTION:

The product generates a hash for a password, but it uses a scheme that does not provide a sufficient level of computational effort that would make password cracking attacks infeasible or expensive.

BUSINESS IMPACT:

In this design, authentication involves accepting an incoming password, computing its hash, and comparing it to the stored hash. After an attacker has acquired stored password hashes, they are always able to brute force hashes offline. As a defender, it is only possible to slow down offline attacks by selecting hash algorithms that are as resource-intensive as possible.

VULNERABILITY NAME: Injection

CWE: CWE 564: SQL Injection: Hibernate

OWASP CATEGORY: A03 2021 Injection

DESCRIPTION:

Using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.

BUSINESS IMPACT:

Hackers use SQL injection attacks to access sensitive business or personally identifiable information (PII), which ultimately increases sensitive data exposure. Using SQL injection, attackers can retrieve and alter data, which risks exposing sensitive company data stored on the SQL server. Compromise Users' Privacy: Depending on the data stored on the SQL server, an attack can expose private user data, such as credit card numbers.

VULNERABILITY NAME: Insecure Design

CWE: CWE 653: Improper Isolation or Compartmentalization

OWASP CATEGORY: A04 2021 Insecure Design

DESCRIPTION:

The product violates well-established principles for secure design. This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation. Because code is centered around design, it can be resource-intensive to fix design problems.

BUSINESS IMPACT:

Insecure system configuration risks stem from flaws in the security settings, configuration and hardening of the different systems across the pipeline (e.g. SCM, CI, Artifact repository), often resulting in “low hanging fruits” for attackers looking to expand their foothold in the environment.

VULNERABILITY NAME: Security Misconfiguration

CWE: CWE 614-Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

OWASP CATEGORY : A05 2021 Security Misconfiguration

DESCRIPTION:

The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over an HTTP session.

BUSINESS IMPACT:

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

VULNERABILITY NAME: Vulnerable and Outdated Components

CWE: CWE 1395: Dependency on Vulnerable Third-Party Component

OWASP CATEGORY: A06 2021 Vulnerable and Outdated Components

DESCRIPTION:

The product has a dependency on a third-party component that contains one or many products which are large enough or complex enough and that part of their functionality uses libraries, modules, or other intellectual property developed by third parties who are not the product creator.

BUSINESS IMPACT:

An entire operating system might be from a third-party supplier in some hardware products. Whether open or closed source, these components may contain publicly known vulnerabilities that could be exploited by adversaries to compromise the product with more known vulnerabilities. Dependency-Check is a Software Composition Analysis (SCA) tool that attempts to detect publicly disclosed vulnerabilities contained within a project's dependencies. It does this by determining if there is a Common Platform Enumeration (CPE) identifier for a given dependency.

VULNERABILITY NAME: Identification and Authentication Failures

CWE: CWE 521-Weak Password Requirements

OWASP CATEGORY: A07 2021 Identification and Authentication Failures

DESCRIPTION:

The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.

BUSINESS IMPACT:

Authentication mechanisms often rely on a memorized secret (also known as a password) to provide an assertion of identity for a user of a system. It is therefore important that this password be of sufficient complexity and impractical for an adversary to guess. The specific requirements around how complex a password needs to be depends on the type of system being protected. Selecting the correct password requirements and enforcing them through implementation are critical to the overall success of the authentication mechanism.

VULNERABILITY NAME: Software and Data Integrity Failures

CWE: CWE-565C Reliance on Cookies without Validation and Integrity Checking

OWASP CATEGORY: A08 2021 Software and Data Integrity Failures

DESCRIPTION:

The product relies on the existence or values of cookies when performing security-critical operations, but it does not properly ensure that the setting is valid for the associated user. Attackers can easily modify cookies, within the browser or by implementing the client-side code outside of the browser. Reliance on cookies without detailed validation and integrity checking can allow attackers to bypass authentication, conduct injection attacks such as SQL injection and cross-site scripting, or otherwise modify inputs in unexpected ways.

BUSINESS IMPACT:

This problem can be primary to many types of weaknesses in web applications. A developer may perform proper validation against URL parameters while assuming that attackers cannot modify cookies. As a result, the program might skip basic input validation to enable cross-site scripting, SQL injection, price tampering, and other attacks.

VULNERABILITY NAME: Security Logging and Monitoring Failures

CWE: CWE-918 insertion of Sensitive Information into Log File

OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures

DESCRIPTION:

While logging all information may be helpful during development stages, it is important that logging levels be set appropriately before a product ships so that sensitive user data and system information are not accidentally exposed to potential attackers.

BUSINESS IMPACT:

Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.

VULNERABILITY NAME: Server-Side Request Forgery

CWE: CWE-918 Server-Side Request Forgery

OWASP CATEGORY: A10 2021 - 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:

A successful SSRF attack can often result in unauthorized actions or access to data within the organization, either in the vulnerable application itself or on other back-end systems that the application can communicate with.

Stage 2

NESSUS Vulnerability Report

Overview

Performing a vulnerability assessment for a college website is crucial to identify and address potential security weaknesses that could be exploited by attackers. Security is an ongoing process, and continuous monitoring and improvement are essential to maintain a robust defense against potential threats. Additionally, if you lack the expertise to conduct a thorough assessment, it is wise to seek assistance from qualified cybersecurity professionals. Verify that the website is secure and displays correctly on various devices and browsers. Document all identified vulnerabilities, along with their severity and potential impact. Prioritize fixes based on criticality and help the college's IT team or web developers with the remediation process. Document all identified vulnerabilities, along with their severity and potential impact. Prioritize fixes based on criticality and help the college's IT team or web developers with the remediation process.

Nessus is a popular vulnerability assessment tool that is widely used by cybersecurity professionals and organizations to identify and address security weaknesses in their networks, systems, and applications. Here are some of the key uses of Nessus:

- **Vulnerability Scanning:** Nessus is primarily used for automated vulnerability scanning. It scans networks, servers, endpoints, and applications to detect known vulnerabilities and misconfigurations. This helps organizations identify potential entry points for attackers and prioritize their security efforts.
- **Patch Management:** The scan results generated by Nessus provide information about missing patches and updates for various software and operating systems. This assists in maintaining an up-to-date and secure IT environment by ensuring that critical security patches are applied promptly.

- **Compliance Auditing:** Nessus can assess whether an organization's systems and configurations comply with industry standards and regulatory requirements, such as PCI DSS, HIPAA, NIST, CIS, and more. It helps organizations identify gaps and achieve compliance with security best practices.
- **Web Application Scanning:** Nessus can scan web applications to identify vulnerabilities like SQL injection, cross-site scripting (XSS), and other issues that may expose web applications to potential attacks.
- **Network Inventory and Asset Management:** Nessus can provide valuable information about the devices and systems connected to the network, assisting in maintaining an up-to-date inventory and understanding the network's attack surface.
- **Security Awareness and Training:** By generating detailed vulnerability reports, Nessus helps security teams and IT personnel gain insights into the security posture of their systems. This information can be used to improve security awareness and training programs.
- **Risk Assessment:** Nessus assigns severity levels to identified vulnerabilities, helping organizations prioritize their efforts by focusing on high-risk vulnerabilities first.
- **Penetration Testing Support:** Nessus can complement manual penetration testing efforts by providing an initial overview of potential vulnerabilities before more extensive manual testing is conducted.
- **Cloud Infrastructure Security:** Many organizations are now using cloud infrastructure. Nessus can assess cloud environments and identify misconfigurations or vulnerabilities that might affect the security of cloud-based resources.
- **Continuous Monitoring:** Nessus can be used to implement continuous monitoring strategies, enabling organizations to regularly assess their security posture and detect changes that may introduce new vulnerabilities.
- **Threat Intelligence Integration:** Nessus can be integrated with threat intelligence feeds to cross-reference scan results with known exploits and threats, providing a more comprehensive view of potential risks.

Nessus is an excellent tool for identifying known vulnerabilities and misconfigurations, it should be part of a comprehensive security strategy that includes regular manual assessments, threat hunting, and ongoing security awareness efforts to address emerging and zero-day threats.

Target Website: https://www.sonatech.ac.in/

Target IP Address: 162.215.219.65

List of Vulnerabilities:

S.No.	Vulnerability Name	Severity	Plugins
1.	HSTS Missing from HTTPS Server (RFC 6797)	Medium	142960
2.	SSL Certificate Cannot Be Trusted	Medium	51192
3.	TLS Version 1.0 Protocol Detection	Medium	104743
4.	TLS Version 1.1 Protocol Deprecated	Medium	157288
5.	IMAP Service STARTTLS Plaintext Command Injection	Medium	52609
6.	SSH Server CBC Mode Ciphers Enabled	Low	70658
7.	SSH Weak Key Exchange Algorithms Enabled	Low	153953
8.	Nessus SYN scanner	None	11219
9.	Service Detection	None	22964
10.	SSL Certificate Information	None	10863

REPORT

Vulnerability Name: HSTS Missing from HTTPS Server (RFC 6797)

Severity: Medium

Plugin: 142960

Port: 443, 2078, 2080, 2083, 2087, 2096

Description: The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, and SSL-stripping man-in-the-middle attacks and weakens cookie-hijacking protections.

Solution: Configure the remote web server to use HSTS.

Vulnerability Name: SSL Certificate Cannot Be Trusted

Severity: Medium

Plugin: 51192

Port: 110, 143, 465, 993, 995

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, as stated below:

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the middle attacks against the remote host.

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

Vulnerability Name: TLS Version 1.0 Protocol Detection

Severity: Medium

Plugin: 104743

Port: 110, 143, 465, 993, 995

Description: The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution: Enable support for TLS 1.2 and 1.3 and disable support for TLS 1.0.

Vulnerability Name: TLS Version 1.1 Protocol Deprecated

Severity: Medium

Plugin: 157288

Port: 110, 143, 465, 993, 995

Description: The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Solution: Enable support for TLS 1.2 and/or 1.3 and disable support for TLS 1.1.

Vulnerability Name: IMAP Service STARTTLS Plaintext Command Injection

Severity: Medium

Plugin: 52609

Port: 143

Description: The remote IMAP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase. Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

Solution: Contact the vendor to see if an update is available.

Vulnerability Name: SSH Server CBC Mode Ciphers Enabled

Severity: Low

Plugin: 70658

Port: 22

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption and enable CTR or GCM cipher mode encryption.

Vulnerability Name: SSH Weak Key Exchange Algorithms Enabled

Severity: Low

Plugin: 153953

Port: 22

Description:

The remote SSH server is configured to allow key exchange algorithms which are considered weak. This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

Solution: Contact the vendor or consult product documentation to disable the weak algorithms.

Vulnerability Name: Nessus SYN scanner

Severity: None

Plugin: 11219

Port: 21,22,25, 53, 80, 110, 111, 143, 443, 465, 587, 993, 995, 2077, 2078, 2079, 2080, 2082, 2083, 2086, 2087, 2095, 2096, 3306

Description: This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and leave unclosed connections on the remote target if the network is loaded.

Solution: Protect your target with an IP filter.

Vulnerability Name: Service Detection

Severity: None

Plugin: 22964

Port: 21,22,25, 53, 80, 110, 111, 143, 443, 465, 587, 993, 995, 2077, 2078, 2079, 2080, 2082, 2083, 2086, 2087, 2095, 2096, 3306

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: N/A

Vulnerability Name: SSL Certificate Information

Severity: None

Plugin: 10863

Port: 110, 111, 143, 443, 465, 993, 995, 2078, 2080, 2083, 2087, 2096

Description: This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution: N/A

Stage 3

Report

Title of the project:

Enhancing Security Operations: SIEM Qradar & SOC Dashboard Management

SOC

SOC plays a crucial role in continuously monitoring an organization's network, systems, and applications. It can detect and respond to potential security incidents, including malware infections, data breaches, and unauthorized access attempts. When a security incident occurs, time is of the essence. SOC teams are trained to respond swiftly and effectively to contain and mitigate the damage caused by security breaches. SOC doesn't merely react to incidents; it proactively identifies vulnerabilities and weaknesses in the organization's infrastructure. This proactive approach enables companies to strengthen their security posture and implement measures to prevent future attacks. SOC provides 24/7 monitoring, ensuring that security analysts are constantly vigilant and ready to respond to emerging threats, regardless of the time of day. SOC is a critical component of a robust cybersecurity strategy. It empowers organizations to detect, respond to, and prevent cyber threats, safeguarding sensitive data, maintaining business continuity, and preserving the organization's reputation in an increasingly interconnected and threat-prone digital landscape. SOC acts as the central hub for incident coordination and communication. It facilitates collaboration among various teams, such as IT, legal, communications, and executive management, ensuring a cohesive and efficient response to security incidents.

SOC - cycle

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

- **Threat Detection and Monitoring:**
  Continuous monitoring of the organization's network, systems, and applications to identify potential security threats and anomalies. Leveraging various security tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, SIEM (Security Information and Event Management) solutions, and threat intelligence feeds.
- **Alert Triage and Analysis:**
  Analyzing and prioritizing security alerts generated by the monitoring tools based on their severity and potential impact. Determining if an alert indicates a genuine security incident or a false positive.
- **Incident Investigation and Response:**
  If an alert is confirmed as a legitimate security incident, the SOC team conducts a thorough investigation to understand the nature and extent of the attack. Gathering evidence, analyzing log data, and performing digital forensics to determine the source and impact of the incident. Initiating the incident response process, which may involve isolating affected systems, containing the threat, and preventing further damage.
- **Incident Containment and Eradication:**
  Taking immediate actions to contain the incident and prevent it from spreading further within the organization's network. Removing the malicious elements and eradicating the threat to restore the affected systems to a secure state.
- **Recovery and Remediation:**
  After the threat is eradicated, the SOC team focuses on restoring affected systems and services to normal operation. Implementing remediation

measures to address the root cause of the incident and prevent similar attacks in the future.

- **Post-Incident Analysis and Lessons Learned:**
  Conducting a thorough post-mortem analysis of the incident to understand how it happened, what was the impact, and what steps were taken to respond. Identifying areas of improvement in the organization's security posture and incident response procedures. Updating security policies and procedures based on the lessons learned from the incident.
- **Threat Intelligence and Proactive Measures:**
  Integrating threat intelligence into the SOC workflow to stay ahead of emerging threats and known attack patterns. Proactively hunting for signs of potential threats and vulnerabilities before they lead to full-fledged security incidents.
- **Continuous Monitoring and Improvement:**
  The SOC cycle is a continuous process, with ongoing monitoring, analysis, and improvement of security measures to adapt to the evolving threat landscape. By following this cycle, the SOC team can effectively detect, respond to, and recover from security incidents, minimizing the impact of cyber threats on the organization's assets and data.

SIEM

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

- **Real-time threat recognition**
  SIEM solutions enable centralized compliance auditing and reporting across an entire business infrastructure. Advanced automation streamlines the collection and analysis of system logs and security events to reduce internal resource utilization while meeting strict compliance reporting standards.
- **AI-driven automation**
  Today's next-gen SIEM solutions integrate with powerful security orchestration, automation and response (SOAR) systems, saving time and resources for IT teams as they manage business security. Using deep machine learning that automatically learns from network behavior, these solutions can handle complex threat identification and incident response protocols in significantly less time than physical teams.
- **Improved organizational efficiency**
  Because of the improved visibility of IT environments that it provides, SIEM can be an essential driver of improving interdepartmental efficiencies. A central dashboard provides a unified view of system data, alerts and notifications, enabling teams to communicate and collaborate efficiently when responding to threats and security incidents.
- **Detecting advanced and unknown threats**
  Considering how quickly the cybersecurity landscape changes, organizations need to be able to rely on solutions that can detect and respond to both known and unknown security threats. Using integrated threat intelligence feeds and AI technology, SIEM solutions can help security teams respond more effectively to a wide range of cyberattacks including:
    - Insider threats - security vulnerabilities or attacks that originate from individuals with authorized access to company networks and digital assets.
    - Phishing - messages that appear to be sent by a trusted sender, often used to steal user data, login credentials, financial information, or other sensitive business information.

- Ransomware - malware that locks a victim's data or device and threatens to keep it locked—or worse—unless the victim pays a ransom tothe attacker.
- Distributed denial of service (DDoS) attacks - attacks that bombard networks and systems with unmanageable levels of traffic from a distributed network of hijacked devices (botnet), degrading performance of websites and servers until they are unusable.
- Data exfiltration – theft of data from a computer or other device, conducted manually, or automatically using malware.

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

SIEM Cycle

The SIEM cycle is a continuous process that involves collecting, analyzing, and responding to security events. It can be divided into the following phases:

1. Data collection: This phase involves collecting security logs and other data from various sources, such as network devices, servers, applications, and cloud platforms.
2. Data normalization: This phase involves converting the collected data into a common format that can be easily analyzed.
3. Data correlation: This phase involves analyzing the normalized data to identify patterns and relationships that may indicate a security threat.
4. Incident detection: This phase involves identifying and prioritizing security incidents.
5. Incident response: This phase involves taking steps to mitigate the impact of a security incident, such as isolating the affected systems and investigating the incident.
6. Reporting and analysis: This phase involves generating reports and analyzing data to improve the SIEM's effectiveness.

The SIEM cycle is an iterative process, meaning that it is constantly being refined and improved. As new threats emerge, the SIEM must be updated to detect and respond to them.

Here are some of the benefits of using a SIEM:

- Increased visibility into security events: A SIEM can provide organizations with a centralized view of all security events, which can help them to identify and respond to threats more quickly.
- Improved threat detection: A SIEM can use machine learning and other advanced analytics techniques to identify patterns and relationships in security data that may indicate a threat.

- Reduced false positives: A SIEM can help to reduce the number of false positives, which can free up security teams to focus on more important threats.
- Improved incident response: A SIEM can help organizations to respond to security incidents more quickly and effectively by providing them with the information they need to investigate and mitigate the impact of the incident.

If you are looking for a way to improve your organization's security posture, a SIEM can be a valuable tool. However, it is important to choose a SIEM that is right for your needs and to implement it properly.

Here are some additional things to keep in mind when implementing a SIEM:

- Make sure that the SIEM can collect data from all the sources you need to monitor.
- Configure the SIEM's rules and alerts to be relevant to your organization's specific threats.
- Train your security team on how to use the SIEM effectively.
- Monitor the SIEM's performance and adjust as needed.

By following these tips, you can ensure that your SIEM is an asset to your organization's security program.

MISP

MISP stands for Malware Information Sharing Platform. It is an open-source, free software platform for collecting, storing, sharing, and analyzing cyber threat information. MISP is used by a wide range of organizations, including government agencies, security companies, and private businesses.

MISP has a number of features that make it a valuable tool for threat intelligence sharing:

- It can store various threat information, including Indicators of Compromise (IOCs), threat actor profiles, and vulnerability information.
- It allows users to share threat information with other MISP users or specific organizations or communities.
- It has a powerful search engine that allows users to find the information they need quickly.
- It includes a number of tools for analyzing threat information, such as correlation, visualization, and reporting.

MISP is a valuable tool for organizations that want to improve their threat intelligence capabilities. It can help organizations to:

- Identify and respond to threats more quickly.
- Mitigate the impact of threats.
- Share threat information with other organizations to improve the overall security posture of the community.

If you are looking for a way to improve your organization's threat intelligence capabilities, MISP is a good option to consider.

Here are some of the benefits of using MISP:

- Open source and free: MISP is an open-source software, which means that it is free to use and modify. This makes it a cost-effective option for many organizations.
- Flexible: MISP is a very flexible platform that can be adapted to the specific needs of different organizations. This makes it a good choice for organizations of all sizes and with different security needs.
- Scalable: MISP is designed to be scalable, so it can be used by organizations of all sizes.

- Secure: MISP is a secure platform that uses a variety of security features to protect the data stored in it.
- Active community: MISP has a large and active community of users and developers who are constantly working to improve the platform. This means that MISP is constantly evolving and getting better.

Your college network information

- Sona College of Technology, Salem, Tamilnadu
- https://www.sonatech.ac.in/
- A total of 15 laboratories and approximately 1200 systems are available.

How you think you deploy SOC in your college

Deploying a SOC in Sona College of Technology can be a daunting task, but it is essential to protect the institution's students, faculty, and staff from cyberattacks. Here are the steps involved in deploying a SOC in a college:

1. Develop a security operations center strategy. This document should define the goals of the SOC, the roles and responsibilities of the team members, and the processes and procedures that will be used to monitor, detect, analyze, and investigate cyber threats.
2. Design your SOC solution. This includes selecting the tools and technologies that will be used to collect, store, and analyze security data.
3. Create processes, procedures, and training. This ensures that the SOC team members are properly trained on how to use the tools and technologies, as well as the processes and procedures that have been put in place.
4. Prepare your environment. This includes ensuring that the SOC has the necessary infrastructure, such as network bandwidth, storage, and computing power.
5. Implement your solution. This involves installing the tools and technologies, configuring them, and testing them to ensure that they are working properly.

6. Deploy end-to-end use cases. This involves testing the SOC's ability to detect, analyze, and investigate cyber threats using real-world data.
7. Maintain and evolve your solution. This includes keeping the tools and technologies up-to-date, as well as updating the processes and procedures as needed.

Here are some additional considerations for deploying a SOC in a college:

- Cost: Deploying and maintaining a SOC can be significant. Colleges should carefully consider their budget and resources before making a decision to deploy a SOC.
- Staffing: The SOC team should be composed of qualified IT security professionals with experience in monitoring, detecting, analyzing, and investigating cyber threats. Colleges may need to hire outside consultants or contract with a managed security service provider (MSSP) to help them deploy and maintain a SOC.
- Compliance: Colleges are subject to a variety of compliance regulations, such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). The SOC should be designed to meet the requirements of these regulations.
- Education: The college community should be educated about cybersecurity risks and how to protect themselves. The SOC can play a role in this education by providing training and resources to students, faculty, and staff.

Deploying a SOC in a college is a complex and challenging task, but it is essential to protect the institution's assets from cyberattacks.

Threat intelligence

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

There are two main types of threat intelligence:

- Strategic threat intelligence: This type of intelligence provides a broad overview of the threat landscape and is intended to help organizations understand the risks they face and make informed decisions about their security posture.
- Tactical threat intelligence: This type of intelligence provides more specific information about specific threats, such as the tactics, techniques, and procedures (TTPs) used by threat actors.

Threat intelligence can be collected from a variety of sources, including:

- Open-source intelligence (OSINT): This includes publicly available information, such as news articles, social media posts, and hacking forums.
- Closed source intelligence (CSINT): This includes proprietary information, such as threat actor reports and vulnerability assessments.
- Human intelligence (HUMINT): This includes information gathered from human sources, such as informants and undercover agents.

Threat intelligence can be used to improve an organization's security in a number of ways, including:

- Identifying and prioritizing threats: Threat intelligence can help organizations identify the most serious threats they face and prioritize their security efforts accordingly.

- Developing mitigation strategies: Threat intelligence can be used to develop mitigation strategies to prevent or mitigate the impact of cyberattacks.
- Improving incident response: Threat intelligence can help organizations improve their incident response procedures by providing them with information about the threat actors and their TTPs.
- Building awareness: Threat intelligence can be used to build awareness of cyber threats among employees and help them to identify and report suspicious activity.

Threat intelligence is a valuable tool for organizations of all sizes. By collecting, processing, and analyzing threat intelligence, organizations can improve their understanding of the threat landscape and make more informed decisions about their security posture.

Incident response

Incident response is the process of identifying, containing, and recovering from a cybersecurity incident. It is a critical part of any organization's security posture.

The incident response process typically includes the following phases:

1. Preparation: This phase involves developing and implementing an incident response plan, training staff on the plan, and testing the plan.
2. Detection: This phase involves identifying that an incident has occurred. This can be done through monitoring systems, analyzing logs, or receiving reports from users.
3. Containment: This phase involves stopping the spread of the incident and preventing further damage. This may involve isolating the affected systems, removing malicious code, or blocking malicious traffic.
4. Eradication: This phase involves removing the malware or other malicious code from the affected systems.
5. Recovery: This phase involves restoring the affected systems to their original state. This may involve restoring data from backups, rebuilding systems, or reconfiguring systems.

6. Lessons learned: This phase involves reviewing the incident and identifying areas where improvements can be made to the incident response plan.

The incident response process should be tailored to the specific needs of the organization. However, there are some key principles that should be followed in all cases. These principles include:

- Proactivity: Organizations should be proactive in their approach to incident response. This means having a plan in place and being prepared to respond to incidents quickly and effectively.
- Communication: Communication is essential during an incident response. Organizations should communicate with affected employees, customers, and partners throughout the incident response process.
- Documentation: Organizations should document all aspects of the incident response process. This documentation will be valuable for future incidents and for regulatory compliance purposes.
- Collaboration: Organizations should collaborate with other organizations during an incident response. This may include sharing information, coordinating resources, or providing mutual assistance.

By following these principles, organizations can improve their ability to respond to and recover from cybersecurity incidents.

Qradar & understanding about tool

IBM QRadar is a security information and event management (SIEM) platform that provides real-time visibility into your IT infrastructure, which you can use for threat detection and prioritization. It collects, correlates, and analyzes security data from a variety of sources, including network traffic, logs, and endpoint data. QRadar uses machine learning and artificial intelligence to identify threats and anomalies, and it can also be used to automate incident response.

QRadar is a comprehensive security solution that can be used to protect your organization from a wide range of threats, including:

- Data breaches: QRadar can help you to detect and respond to data breaches by identifying unauthorized access to sensitive data.
- Malware attacks: QRadar can help you to detect and respond to malware attacks by identifying malicious traffic and files.
- DDoS attacks: QRadar can help you to detect and respond to DDoS attacks by identifying and mitigating malicious traffic.
- Zero-day attacks: QRadar can help you to detect and respond to zero-day attacks by using machine learning to identify anomalies in your traffic.
- Insider threats: QRadar can help you to detect and respond to insider threats by identifying suspicious user behavior.

QRadar is a powerful tool that can help you to protect your organization from a wide range of threats. It is a complex system, but it is easy to use and manage. QRadar is a good choice for organizations of all sizes.

Here are some of the key features of IBM QRadar:

- Real-time threat detection: QRadar collects and analyzes security data in real time, so you can quickly identify and respond to threats.
- Machine learning and artificial intelligence: QRadar uses machine learning and artificial intelligence to identify threats and anomalies that would otherwise be missed.
- Threat intelligence: QRadar integrates with threat intelligence feeds to provide you with the latest information about threats.
- Incident response automation: QRadar can automate incident response tasks, so you can focus on more important things.
- Compliance reporting: QRadar can generate reports that help you to demonstrate compliance with regulations.

If you are looking for a comprehensive SIEM platform that can help you to protect your organization from a wide range of threats, IBM QRadar is a good choice.

Conclusion

Stage 1 : What you understand from Web application testing ?

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

The specific outcomes of web application testing include:

- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Security Compliance and Risk Mitigation
- Optimization Recommendations
- Enhanced Quality Assurance
- Increased Customer Confidence
- Compliance with Regulatory Requirements

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

Stage 2 : What you understand from the Nessus report?

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

Stage 3 : What you understand from SOC / SEIM / Qradar Dashboard?

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 andinsights. 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

To meet the challenges of the future, testing professionals will need to:

- Stay up-to-date on the latest technologies and trends in web application testing.
- Be able to use a variety of testing methods and tools.
- Have a strong understanding of security and reliability testing.
- Be able to work independently and as part of a team.
- Be able to communicate effectively with stakeholders.

Stage 2 : Future scope of testing process you understood.

To stay relevant in the future of software testing, professionals will need to:

- Develop strong skills in automation testing: Automation testing is a essential skill for testing professionals in the future. They should be able to use automation tools to perform repetitive tasks quickly and efficiently.
- Stay up-to-date on emerging technologies: Emerging technologies are constantly changing the landscape of software testing. Testing professionals should stay up-to-date on the latest technologies and trends to ensure that they are using the most effective methods.
- Develop a strong understanding of quality, security, and performance: Testing professionals should have a deep understanding of the principles of quality, security, and performance testing. They should be able to develop and execute testing strategies that address these critical concerns.
- Be able to work independently and as part of a team: Testing professionals should be able to work independently and as part of a team. They should be able to communicate effectively with stakeholders and other members of the testing team.

Stage 3 : Future scope of SOC / SEIM

To meet the challenges of the future, SOC/SIEM solutions will need to:

- Be able to collect and analyze large amounts of security data in real time.
- Be able to identify and respond to threats automatically.
- Be integrated with emerging technologies, such as AI and ML.
- Be able to meet the compliance requirements of various regulations.

Topics explored:

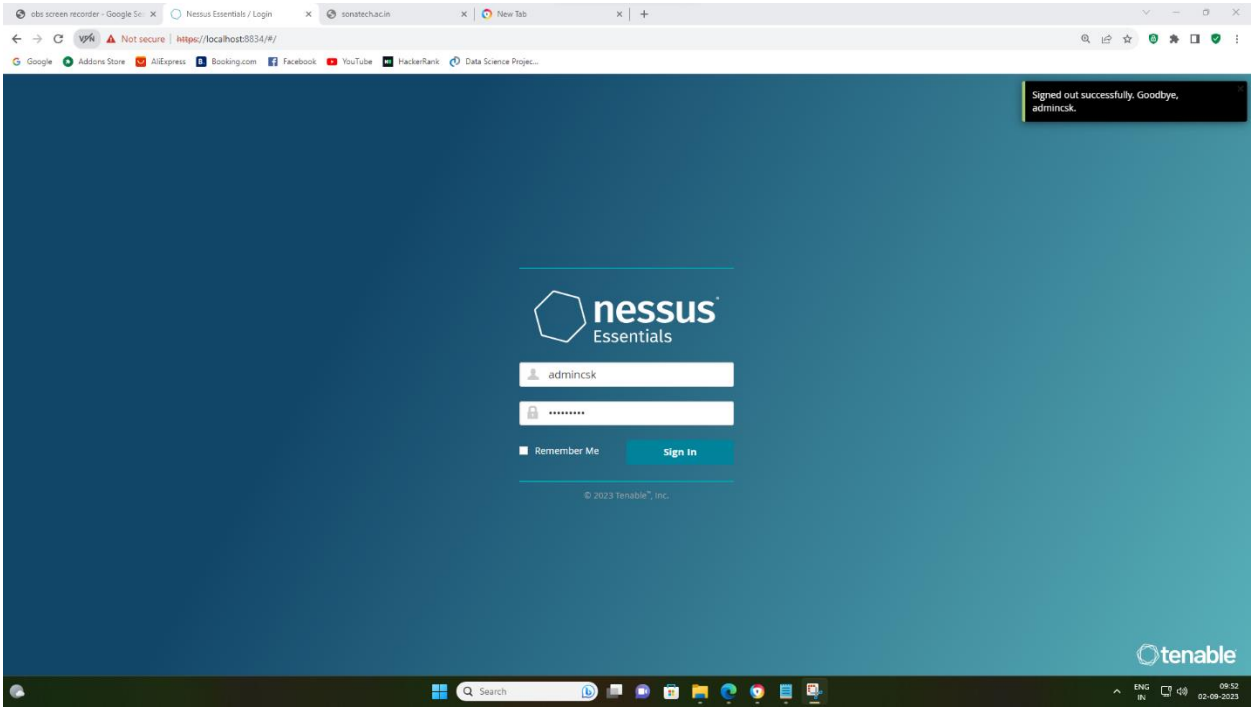
Introduction to cybersecurity, Growth of cybersecurity, Data sanity, Cloud service and cloud security, Data breach, Firewall, Antivirus, Digital ecosystem, Data protection, Types of cyber attacks, Essential terminology, Introduction to networking, Web APIs, web hooks, Web shell concepts, Vulnerability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

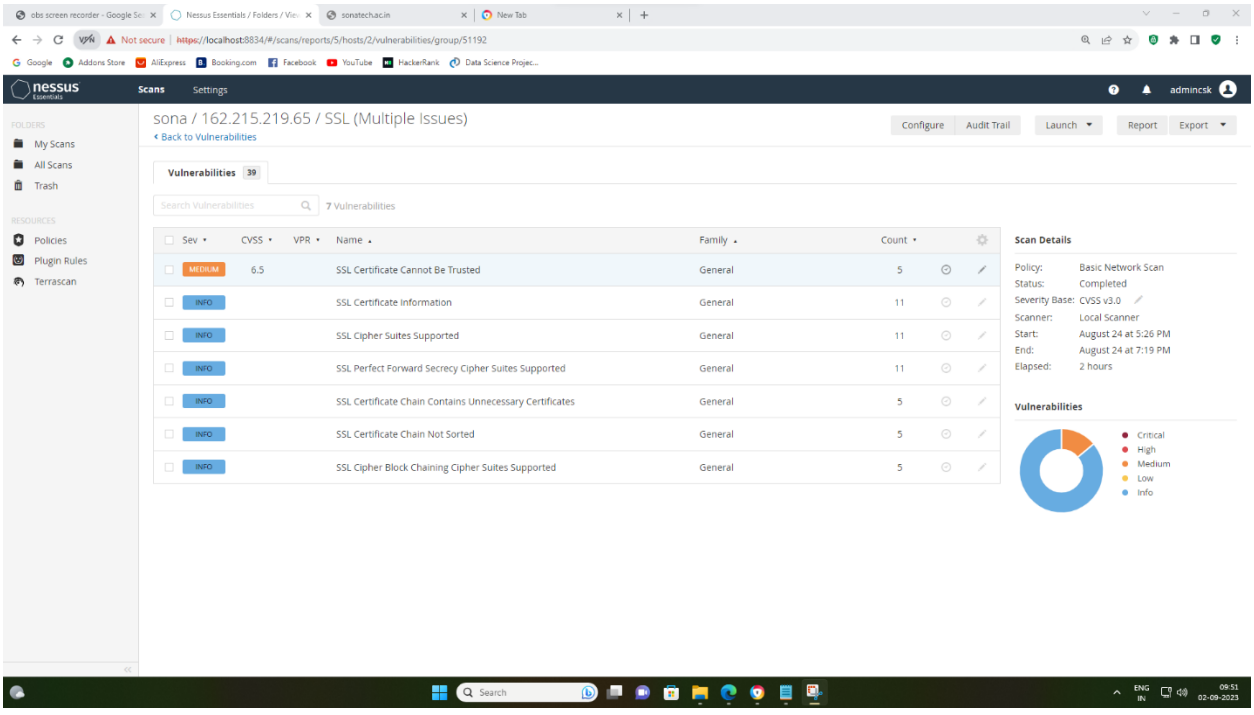
Tools explored:

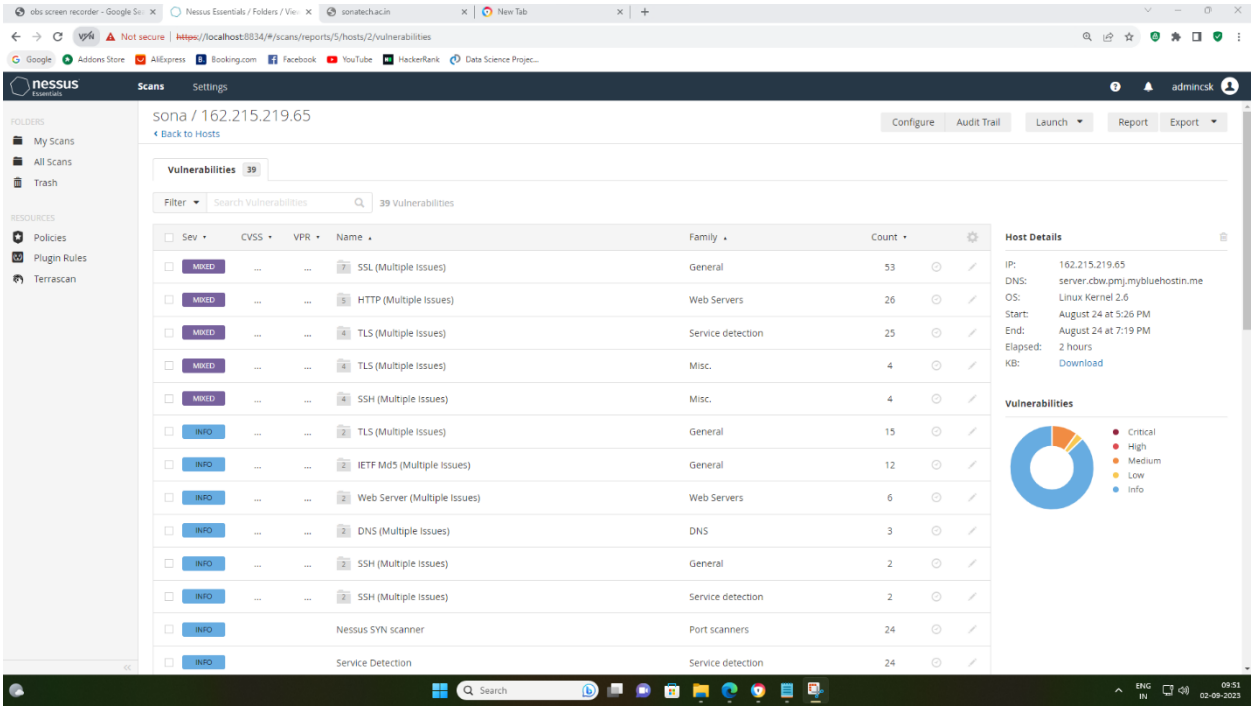
Nessus, chaptgpt, wepik.com (AI image editor), Gamma (AI based PPT), OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation, mobaxterm, tools-nmtui, Nmap, sqlmap,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

Annexure

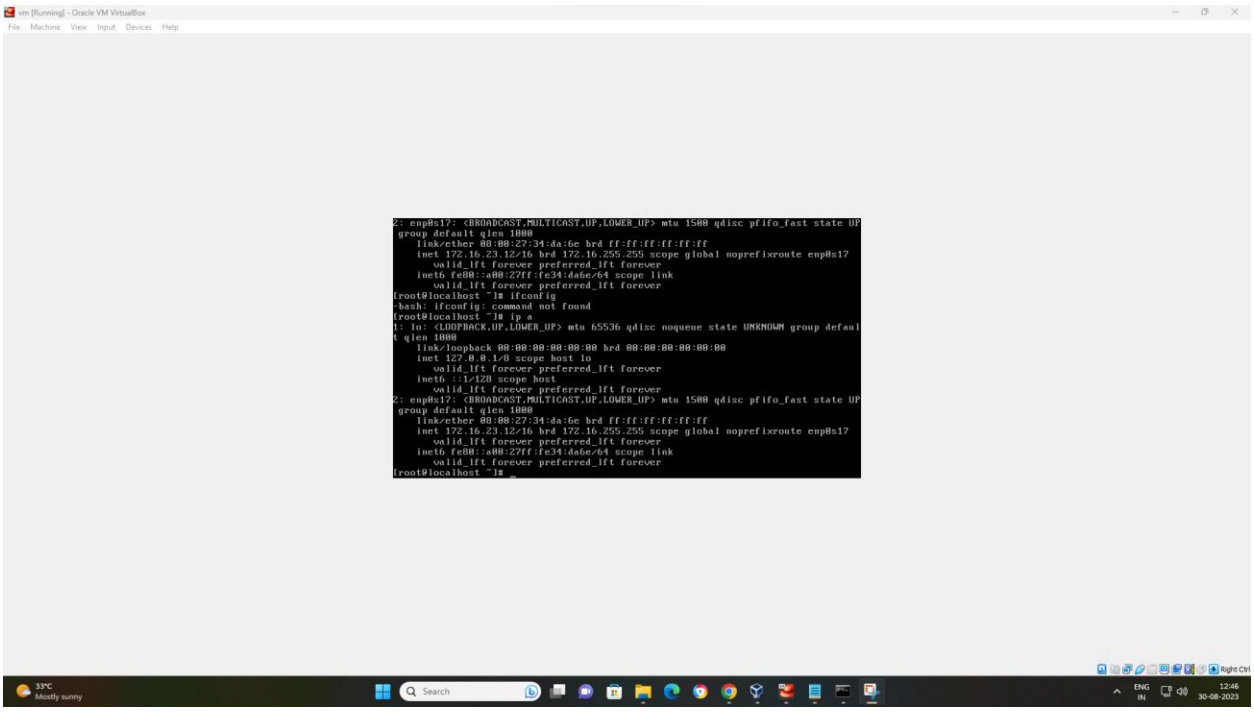
Nessus






nessus
Essentials
Scans
Settings
adminсsk
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
sona / 162.215.219.65
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 39
Filter
Search Vulnerabilities
39 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MIXED SSL (Multiple Issues) General 53
MIXED HTTP (Multiple Issues) Web Servers 26
MIXED TLS (Multiple Issues) Service detection 25
MIXED TLS (Multiple Issues) Misc. 4
MIXED SSH (Multiple Issues) Misc. 4
INFO TLS (Multiple Issues) General 15
INFO IETF Md5 (Multiple Issues) General 12
INFO Web Server (Multiple Issues) Web Servers 6
INFO DNS (Multiple Issues) DNS 3
INFO SSH (Multiple Issues) General 2
INFO SSH (Multiple Issues) Service detection 2
INFO Nessus SYN scanner Port scanners 24
INFO Service Detection Service detection 24
Host Details
IP: 162.215.219.65
DNS: server.cbw.pmj.mybluehostin.me
OS: Linux Kernel 2.6
Start: August 24 at 5:26 PM
End: August 24 at 7:19 PM
Elapsed: 2 hours
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info

IBM QRadar


2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:34:da:6e brd ff:ff:ff:ff:ff:ff
inet 172.16.23.12/16 brd 172.16.255.255 scope global noprefixroute enp0s17
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe34:da6e/64 scope link
valid_lft forever preferred_lft forever
[root@localhost ~]# ifconfig
-bash: ifconfig: command not found
[root@localhost ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:34:da:6e brd ff:ff:ff:ff:ff:ff
inet 172.16.23.12/16 brd 172.16.255.255 scope global noprefixroute enp0s17
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe34:da6e/64 scope link
valid_lft forever preferred_lft forever
[root@localhost ~]#