Project Name: Exploring Cybersecurity Threats and Solutions in the Digital Age

Prepared By: 1.Priti Shivaji Chavan-Patil

2.Pratibha Mahadev Chavan

3.Rajani Jayraj Salunkhe

4.Anuja Bhikaji Chavan

Stage 1:

List of Vulneability Table

S.No	Vulnerability Name	CWE No.
1	SQL Injection	CWE-89
2	Cross-Site Scripting(XSS)	CWE-79
3	Broken Authentication	CWE-287
4	Insucure Direct Object Reference(IDOR)	CWE-639
5	Security Misconfiguration	CWE-16
6	Sensitive Data Explosure	CWE-200
7	Broken Access Control	CWE-284
8	XML External Entity(XXE)Attack	CWE-611
9	Cross-Site Request Forgery(CSRF)	CWE-352
10	Use of Hardcoded Credentials	CWE-798
11	Unrestricted File Upload	CWE-434
12	Directory Traversal	CWE-22
13	Server-Side Request Forgery(SSRF)	CWE-918
14	Deserialization of Untrusted Data	CWE-502

15	Insufficient Logging &Monitoring	CWE-778

Report:

Vulnerability Name: SQL Injection

CWE: CWE-89

OWASP/SANS Category:

OWASP Top 10: A03:2021 – Injection

SANS 25: Improper Neutralization of Special Elements Used in an SQL Command

Description:

SQL Injection (SQLi) is a web security vulnerability that allows attackers to interfere with the queries that an application makes to its database. By injecting malicious SQL statements, attackers can manipulate the database to retrieve, modify, or delete data. This occurs when user input is not properly sanitized before being executed as part of an SQL query.

Business Impact:

Data Breach: Attackers can extract sensitive user data, including credentials and financial information.

Data Manipulation: They can alter or delete database records, leading to data integrity issues.

Unauthorized Access: Attackers may gain admin privileges and take full control of the system.

Financial & Reputational Loss: Compliance violations (GDPR, HIPAA) and loss of customer trust.

Stage 2:

Nessus is a powerful vulnerability assessment tool developed by Tenable. It is widely used by cybersecurity professionals to detect and mitigate security vulnerabilities in networks, applications, and systems. Nessus is known for its accuracy, efficiency, and comprehensive scanning capabilities, making it a valuable tool for penetration testing, security audits, and compliance checks.

How Nessus Works

Nessus works by scanning systems for known security flaws, misconfigurations, and missing patches. It uses an extensive database of vulnerabilities and regularly updates its plugins to detect the latest security threats. The scanning process includes:

1. Target Selection – The user specifies the IP addresses or domains to scan.

2. Vulnerability Detection – Nessus analyzes the system and identifies weaknesses.

3. Severity Assessment – It categorizes vulnerabilities as Low, Medium, High, or Critical.

4. Reporting & Recommendations – Generates detailed reports with remediation suggestions.

Nessus is essential for cybersecurity because it proactively scans systems to detect potential security threats. It is particularly useful in penetration testing, compliance auditing, and risk assessment. The tool continuously updates its vulnerability database, ensuring that organizations are protected against the latest security threats.

Key Takeaways:

1. Automated Vulnerability Scanning – Nessus scans networks, servers, and applications to identify misconfigurations, outdated software, and security vulnerabilities.

2. Risk-Based Prioritization – It assigns severity levels (Low, Medium, High, Critical) to vulnerabilities, helping security teams focus on the most critical issues first.

3. Compliance and Security Auditing – Nessus helps organizations comply with PCI-DSS, HIPAA, ISO 27001, and other security regulations by checking for policy violations.

4. Detailed Reporting and Remediation Guidance – It provides detailed reports on vulnerabilities, their impact, and recommended fixes.

5. Customizable and Scalable – Security teams can configure Nessus scans based on specific organizational needs, making it adaptable for businesses of all sizes.

Why Nessus is Important

It helps in identifying vulnerabilities before attackers exploit them.

Ensures network and system security by regularly scanning for misconfigurations.

Assists in regulatory compliance by automating security checks.

Saves time and resources by automating vulnerability management.

In summary, Nessus is a powerful and reliable tool that plays a crucial role in cybersecurity by identifying, assessing, and mitigating security risks efficiently. Let me know if you need further details or examples!

Target Website: https://www.tenable.com/products/nessus

Target IP Address:Does not fix IP address

List Of Vulnerability

S.No	Vulnerability Name	Severity	Plugin ID
1	SQL Injection	High	10002
2	Cross-Site Scripting(XSS)	Medium	12001
3	Insucure Direct Object Reference(IDOR)	High	15010
4	Open Ports	Low	10335
5	Outdated Software	Critical	16245

Report:

Vulnerability Name: SQL Injection

Severity: High

Plugin: 10002

Port: 443 (HTTPS)

Description:

SQL Injection occurs when user input is not properly sanitized before being used in a database query. Attackers can manipulate SQL queries to gain unauthorized access to data, modify records, or execute administrative operations.

Solution:

Use prepared statements and parameterized queries to prevent injection.

Implement input validation and whitelisting.

Regularly update and patch databases and web applications.

Stage 3:

SOC:

A Security Operations Center (SOC) is a centralized unit that monitors, detects, responds to, and mitigates cybersecurity threats in real time. It consists of security analysts, engineers, and incident responders who use various tools and techniques to protect an organization's digital assets. A SOC continuously monitors network traffic, logs, and security events to prevent data breaches and cyberattacks. It plays a crucial role in ensuring an organization's cybersecurity posture remains strong**.**

SOC-Cycle:

The SOC cycle refers to the systematic approach SOC teams follow to detect, analyze, and respond to security incidents. The cycle includes:

1. Monitoring & Detection – Continuous surveillance of network activities.

2. Threat Identification – Detecting potential security threats and anomalies.

3. Incident Response – Investigating and mitigating threats**.**

4. Recovery & Remediation – Restoring systems and applying security patches.

5. Continuous Improvement – Learning from past incidents to strengthen defenses.

SIEM :

SIEM is a security solution that collects, analyzes, and correlates security data from multiple sources to detect potential cyber threats. SIEM helps security teams by aggregating logs, identifying anomalies, and triggering alerts for suspicious activities. It improves threat visibility and assists in compliance with regulatory standards like GDPR, HIPAA, and PCI-DSS. Popular SIEM tools include Splunk, IBM QRadar, and ArcSight.

SIEM Cycle

The SIEM cycle involves key processes that make security monitoring effective:

1. Data Collection – Gathering logs from various sources like firewalls, IDS/IPS, and servers.

2. Normalization & Correlation – Converting raw data into structured formats and linking related events.

3. Threat Detection – Using rule-based analysis, machine learning, and behavior analytics.

4. Alerting & Reporting – Generating real-time alerts for suspicious activities.

5. Incident Response & Mitigation – Investigating alerts and taking appropriate actions to neutralize threats.

MISP :

MISP is an open-source platform designed to improve threat intelligence sharing among organizations. It enables security teams to share, store, and analyze indicators of compromise (IOCs) related to malware, phishing, and other cyber threats. MISP enhances collaboration among security professionals and helps organizations proactively defend against evolving cyber threats.

Your College Network Information:

The college network is a structured system that connects students, faculty, and administrative staff. It consists of routers, switches, servers, firewalls, and endpoint devices. A secure college network should have firewall protection, access control policies, network segmentation, and regular vulnerability assessments to prevent cyber threats like phishing, malware, and unauthorized access.

How You Think You Can Deploy SOC in Your College:

To deploy a SOC in a college, the following steps can be taken:

Establish a dedicated security team to monitor network activities.

Implement SIEM solutions for log analysis and threat detection.

Use firewalls and intrusion detection systems (IDS) to protect against external attacks.

Educate students and faculty about cybersecurity best practices.

Conduct regular penetration testing and vulnerability assessments to identify weak points.

Threat Intelligence:

Threat intelligence refers to the process of gathering, analyzing, and applying information about potential and existing cyber threats. It helps organizations proactively identify and mitigate security risks. Threat intelligence sources include MISP, MITRE ATT&CK, and government security agencies (e.g., CISA, CERT-IN). Effective threat intelligence enhances an organization's ability to defend against sophisticated attacks like zero-day vulnerabilities and advanced persistent threats (APTs).

Incident Response

Incident response (IR) is a structured approach to detecting, investigating, and mitigating cybersecurity incidents. The incident response lifecycle includes:

1. Preparation – Developing an incident response plan.

2. Detection & Analysis – Identifying security breaches and assessing their impact.

3. Containment & Eradication – Isolating affected systems and removing threats.

4. Recovery – Restoring affected systems and validating security fixes.

5. Lessons Learned – Reviewing the incident to improve future security measures.

QRadar & Understanding the Tool:

IBM QRadar is a popular SIEM tool that helps security teams detect, analyze, and respond to cyber threats. It collects and correlates security logs, applies advanced analytics, and provides real-time alerts. QRadar improves an organization's threat visibility, incident response efficiency, and compliance with security regulations. It integrates with threat intelligence feeds to enhance security monitoring and proactive threat mitigation.

Conclusion:

Understanding SOC, SIEM, threat intelligence, and incident response is essential for building a robust cybersecurity framework. Implementing a SOC in a college or organization enhances security by monitoring threats, responding to incidents, and ensuring compliance with security policies. By using tools like Nessus, MISP, and QRadar, organizations can strengthen their defenses against cyber threa