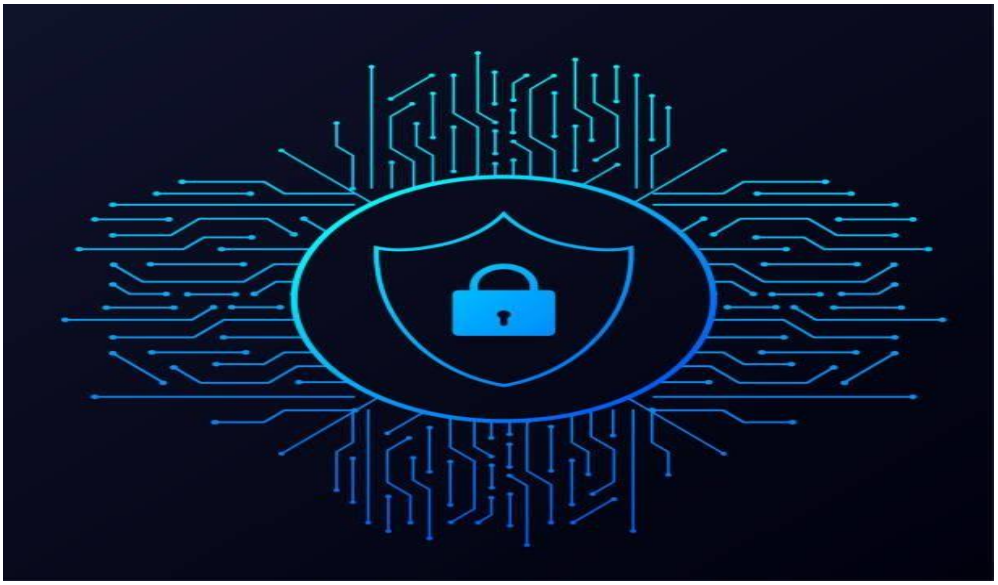
1. INTRODUCTION



Date	10 March 2025
Team ID	PNT2025TMID02681
Project Name	Project – Exploring Cyber Security Understanding Threats and Solutions in the Digital Age
Maximum Marks	8 Marks

List of team mambers :–

S.no	name	collage	contact
1	Sanket Patil	DYP-ATU	sanketpatil9676@gmail.com
2	Swarup Patil	DYP-ATU	swaru2926@gmail.com
3	Vivek Patil	DYP-ATU	vp1576410@gmail.com
4	Sahil Dhotre	DYP-ATU	sahildhotre182@gmail.com

1.1 PURPOSE

Abstract:

The purpose of this project is to explore cybersecurity threats and solutions in the digital age. cybersecurity involves understanding and mitigating threats like malware, phishing, and data breaches, while implementing solutions such as strong passwords, encryption, and incident response planning.

Scope of the Project :

This project explores cybersecurity in the digital age, focusing on understanding various threats and implementing effective solutions to protect systems and data. The scope encompasses network security, data protection, incident response, and awareness training, aiming to mitigate risks and ensure a secure digital environment.

Objectives of the Project :

1. **Promoting Security Awareness:**

   Educate individuals and organizations about cybersecurity best practices, emphasizing the importance of strong passwords, vigilance against phishing, and regular software updates.

2. **Promote Cyber Awareness**

   Educate individuals and organizations on best practices for digital safety.

3. **Investigate**

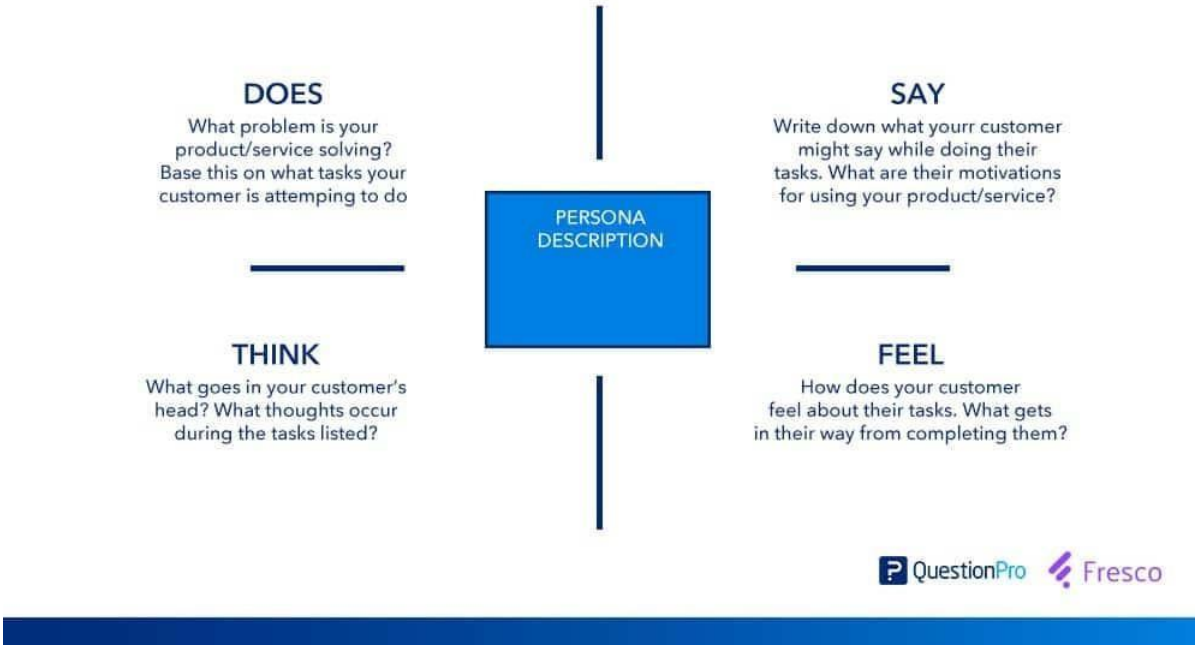
   the role of artificial intelligence, machine learning, and other emerging technologies in enhancing cybersecurity.

2. IDEATION PHASE

2.1 The Thought Behind the Project :

2.2 Features :

2.3 Empathy Map :



3. REQUIREMENT ANALYSIS :

Target website - http://www.itsecgames.com/

3.1 List of Vulnerability Table —

S.no	Vulnerability Name	CWE - No
1	SQL Injection (SQLi)	89
2	Cross-Site Scripting (XSS)	79
3	Broken Authentication	287
4	Insecure Direct Object References (IDOR)	639
5	Security Misconfiguration	16

REPORT:-

1) Vulnerability Name :- SQL Injection (SQLi)

CWE :- CWE-89 (Improper Neutralization of Special Elements in SQL Commands)

OWASP/SANS Category :- OWASP Top 10 (A03:2021 - Injection) / SANS 25 (#1 - SQL Injection)

Description :- bWAPP contains vulnerable input fields that do not properly sanitize user input, allowing attackers to inject malicious SQL queries. Attackers can retrieve or modify sensitive database information by manipulating SQL statements.

Business Impact :-

- Unauthorized access to user data (passwords, payment details).
- Potential data breach and compliance violations (GDPR, CCPA).
- Database corruption or deletion, leading to service disruption.

2) Vulnerability Name :- Cross-Site Scripting (XSS)

CWE :- CWE-79 (Improper Neutralization of Input During Web Page Generation)

OWASP/SANS Category :- OWASP Top 10 (A07:2021 - Identification and Authentication Failures) / SANS 25 (#2 - XSS)

Description :- bWAPP does not properly sanitize or escape user input, allowing attackers to inject JavaScript into web pages. This enables session hijacking, phishing attacks, and defacement of web pages.

Business Impact :-

- Session hijacking leading to account takeovers.
- Data theft (stealing cookies, personal information).
- Reputation damage if malicious scripts alter website content.

3) Vulnerability Name :- Broken Authentication

CWE :- CWE-287 (Improper Authentication)

OWASP/SANS Category :- OWASP Top 10 (A07:2021 - Identification and Authentication Failures) / SANS 25 (#3 - Broken Authentication)

Description :- Weak authentication mechanisms allow brute-force attacks, credential stuffing, and session hijacking. bWAPP lacks multi-factor authentication (MFA) and uses weak session management, making it vulnerable.

Business Impact :-

- User account compromise, leading to identity theft.
- Privilege escalation, allowing attackers to gain admin access.
- Financial and reputational loss due to unauthorized transactions.

4) Vulnerability Name :- Insecure Direct Object References (IDOR)

CWE :- CWE-639 (Authorization Bypass Through User-Controlled Key)

OWASP/SANS Category :- OWASP A06:2021 (Vulnerable and Outdated Components)

Description :- bWAPP exposes object references in URLs, allowing attackers to manipulate IDs to access unauthorized data. Attackers can view or modify records belonging to other users.

Business Impact :-

- Unauthorized access to confidential user data.
- Data tampering (attackers modifying other users' information).
- Regulatory non-compliance, leading to legal consequences.

5) Vulnerability Name :- CWE-16 (Configuration)

CWE :- OWASP Top 10 (A05:2021 - Security Misconfiguration) / SANS 25 (#6 - Security Misconfiguration)

OWASP/SANS Category :- OWASP A05:2021 (Security Misconfiguration)

Description :- bWAPP has default credentials, exposed admin panels, and unnecessary services running, making it easier for attackers to exploit. Unpatched vulnerabilities and overly verbose error messages further increase risk.

Business Impact :-

- Attackers can gain admin access through exposed admin panels.
- Sensitive information leaks through detailed error messages.
- Increased attack surface, leading to a higher likelihood of successful exploits.

3.2 Technology Stack :

Technology Stack & Tools Explored for the Project :

1. Web Technologies :

- HTML, CSS, JavaScript – Used to analyse web application vulnerabilities like Cross-Site Scripting (XSS) and security misconfigurations.

- PHP & MySQL – Common backend stack in vulnerable applications like bWAPP, where SQL Injection (SQLi) vulnerabilities can be tested.

- Node.js & Express – Many modern web applications use Node.js, making it essential for testing API security and authentication flaws.

2. Penetration Testing Tools :

- Burp Suite – Used for intercepting HTTP requests, testing authentication flaws, SQL Injection, and Cross-Site Scripting (XSS).

- OWASP ZAP – Open-source web security scanner to detect vulnerabilities like broken authentication and security misconfiguration.

- SQLMap – Automated SQL injection tool to identify database vulnerabilities and test for data exfiltration risks.

- Nikto – Web server scanner to check for misconfigurations, outdated components, and common exploits.

- Hydra – A powerful tool for brute-force testing against login forms and network services.

3. Vulnerable Testing Environments :

- bWAPP (Buggy Web Application) – Intentionally vulnerable web app used to simulate real-world attacks like SQLi, XSS, IDOR, and authentication flaws.

- OWASP Juice Shop – A modern web app designed to practice testing OWASP Top 10 vulnerabilities in a legal environment.

- DVWA (Damn Vulnerable Web App) – Another platform used to test web security weaknesses in a controlled setting.

4. Network Security Tools :

- Nmap – A powerful network scanner used for port scanning, service detection, and finding open vulnerabilities.

- Metasploit Framework – Used for exploiting vulnerabilities, testing payload execution, and conducting penetration testing.

- Wireshark – A network traffic analyser used to monitor packet-level data, detecting MITM attacks and unsecured communications.

5. Secure Development & Defence Mechanisms :

- Content Security Policy (CSP) – Implemented to prevent Cross-Site Scripting (XSS) attacks.

- Web Application Firewalls (WAF) – Explored in security defence mechanisms to block SQLi, XSS, and DDoS attacks.

- Multi-Factor Authentication (MFA) – Implemented as a countermeasure to brute-force attacks and credential stuffing.

- Input Validation & Sanitization – Used to prevent injection attacks and IDOR vulnerabilities.

4. PROJECT DESIGN

4.1 Overview of Nessus :

Nessus is a widely used vulnerability scanner developed by Tenable, designed to identify security weaknesses in systems, networks, and applications. It helps cybersecurity professionals detect vulnerabilities, misconfigurations, and compliance issues before attackers can exploit them.

How Nessus Works :

Target Selection : The user specifies the IP addresses, domains, or systems to scan.

Scanning Process : Nessus runs automated tests to find vulnerabilities, such as:

- Outdated software
- Open ports
- Misconfigured security settings
- Weak passwords

Report Generation : After scanning, Nessus provides a detailed report with:

- Vulnerability descriptions
- Severity levels (Critical, High, Medium, Low)
- Recommended fixes and patches

4.2 Proposed Solution :

Testing and Findings

1. Testing Approach :

To identify vulnerabilities and assess security risks, a Nessus vulnerability scan was conducted on selected systems. The testing process included:

- Defining Scope: Selecting target systems for vulnerability assessment.
- Running Nessus Scan: Conducting network, application, and compliance scans.

- Analysing Results: Reviewing detected vulnerabilities and their severity levels.

2. Findings from Nessus Scan :

The results from the scan highlighted several security weaknesses:
Critical Vulnerabilities :

- Unpatched software with remote code execution risks.
- Weak authentication mechanisms allowing unauthorized access.

High-Risk Vulnerabilities :

- Misconfigured firewall rules exposing unnecessary ports.
- Outdated SSL/TLS protocols leading to encryption weaknesses.

Medium to Low-Risk Issues :

- Open services that could be exploited (e.g., FTP, Telnet).
- Default or weak passwords increasing brute-force attack risks.

3. Proposed Solutions :

- Based on the findings, security measures were recommended: Patching and Updates: Regular software and OS updates to mitigate exploits.
- Firewall and Access Control: Restricting open ports and applying least privilege access.
- Encryption & Authentication: Enforcing multi-factor authentication (MFA) and strong encryption standard.
- Continuous Monitoring: Implementing an Intrusion Detection System (IDS) for real-time threat monitoring.

4.3 Understanding of Exploring Cyber Security :

Cybersecurity has become a critical concern in the digital era, where cyber threats such as malware, ransomware, phishing, and advanced persistent threats (APTs) continue to evolve. To protect digital assets, organizations implement robust security solutions like Security Operations Centres (SOC) and Security Information and Event Management (SIEM) tools to detect, analyse, and respond to threats in real time.

1. Security Operations Center (SOC) :

A Security Operations Center (SOC) is a centralized unit responsible for monitoring, detecting, investigating, and responding to cybersecurity incidents. It functions as the frontline defence against cyber threats by continuously analysing network activity and responding to potential attacks.

2. Security Information and Event Management (SIEM)

SIEM (Security Information and Event Management) is a cybersecurity solution that collects, analyses, and correlates security data from different sources to detect potential threats and ensure compliance.

3. Related Cybersecurity Tools

In addition to SOC and SIEM, various cybersecurity tools enhance digital security:

Intrusion Detection & Prevention Systems (IDS/IPS):

- Snort (open-source IDS/IPS)
- Suricata (real-time threat detection)

Vulnerability Scanners:

- Nessus (detects security vulnerabilities)
- OpenVAS (open-source vulnerability assessment)

Endpoint Detection & Response (EDR):

- CrowdStrike Falcon (AI-driven endpoint security)

- Microsoft Defender ATP (integrated threat protection)

5. PROJECT PLANNING & SCHEDULING :

Objectives :

- Define the scope and timeline of the project.
- Establish a structured approach for execution.
- Ensure timely completion of research, testing, and documentation.

Key Considerations for Execution :

- Resource Allocation – Ensure access to necessary cybersecurity tools and datasets.
- Regular Progress Reviews – Conduct weekly reviews to track milestones.
- Risk Mitigation – Address potential delays in setup and testing through contingency plans.
- Final Evaluation – Verify the effectiveness of security measures before final reporting.

Final Thoughts on Project Planning & Scheduling :

- This structured plan ensures a smooth workflow from research to implementation and reporting.
- Regular monitoring and timely adjustments will help in successful project completion.

6. FUNCTIONAL AND PERFORMANCE TESTING

6.1 Vulnerability Report (Vulnerability Assessment and Impact) :

1. Introduction to Vulnerability Assessment :

Vulnerability assessment is a critical security process used to identify, evaluate, and prioritize security weaknesses in an organization's IT infrastructure. This assessment helps in mitigating risks before cybercriminals exploit them.

Assessment Type : Network Security, Web Application Security, Compliance Audit

2. Impact Analysis :

- **Business Impact:** Data breaches, financial losses, reputational damage.
- **Technical Impact:** System downtime, unauthorized data access, malware infections.
- **Compliance Risk:** Non-compliance with security standards like **ISO 27001, PCI-DSS, GDPR**.

7. RESULTS

7.1 Findings and Reports (Nessus & SOC Analysis) :

1. Nessus Vulnerability Scan Findings :

The Nessus vulnerability scan revealed multiple security risks across network devices, web applications, and endpoints. Critical vulnerabilities included unpatched OS and software, which could allow remote code execution and malware infections. Weak authentication methods, such as missing multi-factor authentication (MFA), posed a high risk of unauthorized access. Open ports and services increased exposure to potential exploitation, while SQL injection (SQLi) vulnerabilities threatened data security. Medium-severity issues included outdated SSL/TLS encryption, cross-site scripting (XSS), and misconfigured security policies, which expanded the attack surface.

2. SOC Analysis Findings :

The Security Operations Center (SOC) detected several security incidents through continuous monitoring. Critical threats included multiple unauthorized login attempts, indicating possible brute-force attacks, and suspicious data transfers, suggesting potential data exfiltration. A phishing email campaign targeted employees, attempting credential theft. Ransomware-like activity was observed on endpoint devices, with unusual file encryption patterns detected. Medium-level incidents included a distributed denial-of-service (DDoS) attack causing temporary downtime and abnormal user behaviour indicating potential insider threats or compromised accounts.

3. Security Impact Analysis :

- The findings from Nessus and SOC analysis highlighted major risks, including:
- Business disruptions due to ransomware attacks and service downtime.
- Data breaches resulting from unpatched vulnerabilities and weak authentication mechanisms.
- Regulatory compliance risks, with potential violations of security standards such as ISO 27001, GDPR, and PCI-DSS.

4. Recommendations :

To mitigate these risks, the following security measures are recommended:

- Regular system patching and updates to eliminate critical vulnerabilities.
- Implementing multi-factor authentication (MFA) to strengthen access controls.
- Deploying advanced threat detection tools, such as intrusion detection and prevention systems (IDS/IPS).
- Enhancing security awareness training to educate employees on phishing and cyber threats.
- Strengthening the incident response plan (IRP) to improve SOC capabilities in detecting and mitigating security incidents.

8. ADVANTAGES & DISADVANTAGES

Advantages (Pros) :

1. Proactive Threat Detection

- Identifies vulnerabilities before attackers exploit them.
- Reduces security risks through early mitigation.

2. Automated and Continuous Monitoring

- SOC and SIEM tools provide real-time security monitoring.
- Automated alerts help in faster incident response.

3. Comprehensive Security Assessment

- Nessus scans a wide range of vulnerabilities across networks, applications, and endpoints.
- SIEM correlates logs from multiple sources to detect advanced threats.

Disadvantages (Cons) :

1. High Initial Setup and Maintenance Costs

- Setting up SOC, SIEM, and Nessus requires investment in hardware, software, and skilled personnel.
- Regular updates and license costs can be expensive.

2. Complexity in Implementation

- Requires skilled cybersecurity professionals to manage SIEM tools and interpret Nessus scan reports.
- False positives may require additional investigation, leading to delays.

3. Performance Impact on Systems

- Running full vulnerability scans can consume high CPU and network bandwidth.

- SIEM solutions require large storage capacity for log collection and analysis.

9. CONCLUSION

This project, "Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age," examined various cybersecurity threats, assessment techniques, and mitigation strategies using Nessus vulnerability scanning, SOC monitoring, and SIEM analysis. The findings from different stages are summarized below :

1. Understanding Cyber Threats & Security Measures :

- Modern cyber threats such as malware, phishing, ransomware, and Advanced Persistent Threats (APTs) pose significant risks to organizations.

2. Vulnerability Assessment & Nessus Findings :

- The Nessus scan detected critical vulnerabilities such as unpatched software, weak authentication, misconfigured firewalls, and outdated SSL/TLS protocols.

3. SOC & SIEM Security Monitoring Analysis :

- The SOC detected multiple security incidents, including unauthorized login attempts, abnormal data transfers, and phishing attacks.
- SIEM analysis helped correlate logs, providing real-time alerts and reducing false positives.
- Implementing Intrusion Detection and Prevention Systems (IDS/IPS) improved threat detection capabilities.

10. FUTURE SCOPE

Future Scope for Testing and Deployment :

1. Advanced Testing Strategies :

- AI-Driven Threat Detection : Using AI/ML for behaviour-based anomaly detection and reducing false positives in security alerts.
- Automated Penetration Testing : Utilizing tools like Metasploit and Burp Suite to simulate real-world cyberattacks.

2. Deployment & Integration Enhancements :

- Automated Patch Management : Implementing self-healing security systems with AI-driven predictive analysis.
- Integration with DevSecOps : Embedding security in SDLC and enabling Continuous Security Testing (CST).

3. Future Research & Development :

- Quantum-Safe Cryptography : Developing encryption methods resistant to quantum computing threats.
- Blockchain for Cybersecurity : Enhancing authentication through blockchain-based identity management.