CYBER SECURITY



|  |  |
| --- | --- |
| DATE | 10 MARCH 2025 |
| TEAM ID |  |
| PROJECT NAME | UNDERSTANDING CYBER THREATS : EXPLORING THE NESSUS &BEYOND SCANNING TOOLS. |
| MAXIMUM MARKS | 8 MARKS |

Smart Internz : Understanding Cyber Threats :

Exploring the Nessus & Beyond Scanning Tools.

|  |  |  |  |
| --- | --- | --- | --- |
| S.NO | NAME OF THE STUDENT | COLLEGE | CONTACT |
| 1. | G.Sakshi | Dr.lankapalli bullayya college | 9553337804 |
| 2. | G.Hema Harshini | Dr.lankapalli bullayya college | 8074733327 |
| 3. | M.Lakshmitha Reddy | Dr.lankapalli bullayya college | 9949517249 |
| 4. | M.Kiran | Dr.lankapalli bullayya college | 9989327075 |

INTRODUCTION :-

Introduction to Cybersecurity :

Definition and Importance: Cybersecurity refers to the practices, technologies, and processes designed to protect systems, networks, and data from cyber threats, including hacking, malware, and data breaches.

Challenges in Cybersecurity: Address the growing complexity of threats, from simple attacks like phishing to advanced persistent threats (APTs).



Introduction to Cyber Threats :

Cyber threats are malicious activities that target computer networks, systems, and data with the intent of stealing, damaging, or disrupting operations. These threats come in various forms, including malware, phishing, ransomware, denial-of-service (DoS) attacks, and zero-day vulnerabilities. With the growing reliance on digital systems, cybersecurity has become a critical concern for organizations worldwide.

One of the most effective ways to counter cyber threats is through vulnerability scanning, which helps identify security weaknesses before attackers exploit them. Vulnerability scanners like Nessus, OpenVAS, Qualys, and Nexpose play a crucial role in assessing and mitigating security risks.



ABSTRACT OF THIS PROJECT :-

In the modern digital landscape, cyber threats have become increasingly sophisticated, targeting vulnerabilities in networks, systems, and applications. To mitigate these risks, vulnerability scanning tools play a vital role in detecting security weaknesses before they can be exploited by attackers. Nessus, developed by Tenable, is one of the most widely used vulnerability assessment tools, offering extensive scanning capabilities, real-time threat intelligence, and detailed reporting. However, other tools like OpenVAS, Qualys, and Nexpose provide additional features, scalability, and integration options tailored to different organizational needs. This study explores the role of Nessus and alternative scanning tools, comparing their effectiveness in enhancing cybersecurity. By leveraging these tools, organizations can strengthen their security posture, ensure compliance with industry standards, and proactively defend against evolving cyber threats.

Key points about cyber threats :

**Diverse attack vectors :**

Cyber threats can manifest in various forms, including phishing emails, denial-of-service attacks, data breaches, and advanced persistent threats (APTs) carried out by highly skilled attackers.

**Motivations :**

Cybercriminals may be motivated by financial gain, political disruption, personal vendetta, or espionage, leading to varied attack objectives.

**Impact on organizations :**

Cyber threats can significantly impact business operations by disrupting critical systems, causing data loss, damaging reputation, and leading to legal repercussions.

**Importance of cybersecurity :**

To combat cyber threats, organizations must implement strong cybersecurity practices, including network monitoring, data encryption, user access controls, employee awareness training, and incident response plans.

MAIN OBJECTIVE :-

Of Understanding Cyber Threats :

The primary objective of understanding cyber threats is to analyze and mitigate the risks associated with malicious activities targeting digital systems, networks, and data. This study aims to:

1. Identify Different Types of Cyber Threats –

Understand various cyber threats such as malware, phishing, ransomware, denial-of-service (DoS) attacks, and zero-day vulnerabilities.

1. Assess the Impact of Cyber Threats –

Evaluate how cyber threats affect individuals, businesses, and national security, leading to data breaches, financial loss, and reputational damage.

1. Explore Cybersecurity Measures –

Examine tools and techniques such as firewalls, encryption, intrusion detection systems, and vulnerability scanning to defend against threats.

1. Analyze Cyber Threat Intelligence –

Study how organizations collect and use threat intelligence to predict, prevent, and respond to cyber attacks effectively.

1. Enhance Cybersecurity Awareness –

Educate individuals and organizations about best practices for online security, risk management, and compliance with cybersecurity regulations.



Of Exploring Nessus :

The primary objective of exploring Nessus is to understand its role as a vulnerability scanning tool in identifying and mitigating security risks in IT infrastructures.

This study aims to:

1. Understand Nessus and Its Function -

Examine how Nessus operates as a vulnerability scanner and its importance in cybersecurity.

1. Analyze Key Features –

Explore Nessus’s features such as vulnerability detection, configuration auditing, compliance checks, and malware scanning.

1. Assess Its Effective –

Evaluate Nessus’s accuracy in identifying security weaknesses and prioritizing risks based on severity.

1. Compare Nessus with Other Tools –

Contrast Nessus with alternative scanners like OpenVAS, Qualys, and Nexpose to determine its advantages and limitations.

1. Enhance Cybersecurity Strategies –

Provide insights into how organizations can integrate Nessus into their security frameworks for proactive threat detection and compliance.



Of Beyond Scanning Tools :

The primary objective of exploring beyond scanning tools is to analyze alternative vulnerability assessment and security testing solutions beyond Nessus.

This study aims to:

1. Identify Advanced Scanning Tools –

Explore tools like OpenVAS, Qualys, Nexpose, Acunetix, and Burp Suite that offer specialized vulnerability detection.

1. Compare Features & Capabilities –

Analyze how these tools differ in terms of vulnerability detection, automation, cloud security, compliance checks, and integration with security frameworks.

1. Assess Effectiveness & Accuracy –

Evaluate the reliability of these tools in detecting vulnerabilities, prioritizing risks, and minimizing false positives.

1. Understand Use Cases –

Examine the practical applications of these tools for enterprises, government agencies, and security professionals.

1. Improve Cybersecurity Posture –

Provide insights on how organizations can leverage multiple security tools for a comprehensive security strategy to enhance threat detection and response.



THE VARIOUS THOUGHTS BEHIND THIS PROJECT :-

STEP 1 : Various Ideas

G.Sakshi

1. With the increasing number of cyber attacks, organizations must adopt proactive security measures to safeguard sensitive data.Understanding cyber threats helps organizations predict, prevent, and respond to security incidents effectively.

2. Tools like Nessus, OpenVAS, Qualys, and Nexpose play a crucial role in identifying weaknesses in networks, systems, and applications.These tools help in automating security assessments and ensuring compliance with security standards.

3. Nessus is one of the most widely used tools for detecting system misconfigurations, outdated software, and security vulnerabilities.It provides detailed reports and risk prioritization, helping cybersecurity teams focus on critical threats.

4. The tools help generate reports that demonstrate security readiness to auditors and regulatory bodies.

G.Hema Harshini

1.While Nessus is powerful, other tools like OpenVAS (open-source), Qualys (cloud-based), and Nexpose (risk-based prioritization) offer unique advantages.A multi-tool approach enhances security by covering different types of vulnerabilities and improving overall risk management.

2.Understanding cyber threats allows organizations to integrate threat intelligence with vulnerability scanning tools for real-time security monitoring.Combining penetration testing with vulnerability scanning strengthens defense mechanisms against cybercriminals.

3.Many industries follow cybersecurity regulations like GDPR, HIPAA, and ISO 27001, which require regular vulnerability assessments.Using scanning tools ensures compliance and minimizes legal risks associated with data breaches.

4. Future of Vulnerability Scanning :-

The integration of AI and machine learning in scanning tools will improve threat detection and response times.Cloud security and IoT vulnerability scanning are emerging trends that will shape the future of cybersecurity.

M.Lakshmitha Reddy

1.Nessus and similar tools help identify vulnerabilities before attackers exploit them.Regular vulnerability scanning is a preventive measure rather than a reactive one, ensuring security gaps are closed before they become serious risks.

2.Scanning tools reduce manual effort in identifying vulnerabilities across networks and systems.Nessus provides automated updates with the latest threat intelligence, making it easier to stay ahead of emerging security risks.

3.Relying on a single scanning tool may not be enough, as different tools specialize in varied security assessments.Combining Nessus with OpenVAS (open-source scanning), Qualys (cloud security), and Nexpose (risk-based prioritization) provides a more comprehensive security evaluation.

4.The cybersecurity industry is moving towards AI-driven, self-learning scanning tools that adapt to new threats faster.Integration with SOAR (Security Orchestration, Automation, and Response) platforms will allow scanning tools to automatically initiate security responses based on detected vulnerabilities.

5.Modern cybersecurity strategies combine vulnerability scanning with real-time threat intelligence to predict and counter cyber threats effectively.Tools that integrate AI and machine learning for risk analysis will enhance cybersecurity in the future.

M.Kiran

1.Traditional vulnerability scanning tools like Nessus were initially designed for on-premise systems, but with cloud adoption and IoT growth, security scanning must evolve.Cloud-based scanners (e.g., Qualys) and IoT-specific scanning tools are needed to address these new attack surfaces.

2.Ethical hackers and penetration testers use Nessus as part of a broader security assessment but also rely on manual testing techniques to uncover deeper security flaws.Nessus is great for baseline security checks, but penetration testing tools like Metasploit or Burp Suite go beyond automated scans to simulate real-world attacks.

3.Nessus has a free version (Nessus Essentials) with limited capabilities, but organizations may need the paid version (Nessus Professional) for advanced features. Open-source alternatives like OpenVAS are free but may require more manual configuration and maintenance.

STEP 2 :- Selecting Some Features And Grouping Them

Data collection and Integration :

* One of the significant benefits of network scanning tools is their ability to support network inventorymanagement. By regularly scanning networks, organizations can maintain up-to-date records of their devices, including information about IP addresses, hardware, and software versions. This automated inventory management simplifies network administration and helps security teams track changes in the infrastructure. Additionally, network scanning tools can generate detailed logs and reports, which are valuable for security audits, compliance checks, and forensic investigations. where the tool incorrectly identifies a harmless service as vulnerable or fails to detect critical vulnerabilities. Moreover, active network
* **Network Scanning Tools** are widely used to gather information about network devices, active IP addresses, and open ports. Tools like **Nmap** and **Angry IP Scanner** help security professionals identify devices connected to the network and determine which ports are open or closed. These tools play a significant role in network mapping and vulnerability detection. Network scanning provides insights into the network's structure, helping security teams identify unauthorized devices and weak entry points. However, network scanning tools can generate a large volume of data, making it essential to filter out irrelevant information.

AI-POWERED ANALYTICS :

* AI with cybersecurity scanning is Nessus, a widely usedvulnerabilit scanning solution. Nessus performs comprehensive scans to identify software vulnerabilities, misconfiguration.
* AI-powered analytics uses machine learning, data mining, and predictivemodeling to provide deeper insights into cyber threats, automate threat detection, and enhance decision-making processes.
* Dashboards transform static scan reports into dynamic, actionable insights. They enable security teams to monitor the effectiveness of security controls, track remediation progress, and identify emerging threats in real-time.
* This operationalization is crucial for proactive security management, allowing organizations to respond to vulnerabilities before they are exploited.
* Dashboards should track vulnerability trends effectiveness areas for improvement.
* Dashboards provide a visual representation of the data collected by Nessus scans, making it easier to understand complex vulnerability information.They offer a quick overview of the organization's security posture .
* Dashboards often display vulnerability severity levels, allowing security teams to prioritize remediation efforts.
* They can highlight critical vulnerabilities that pose the greatest risk.

* 

RISK ASSESSMENT:

* Risk assessment is the cornerstone of effective cybersecurity. It involves systematically identifying potential threats and vulnerabilities that could compromise an organization's assets.
* The first step in risk assessment is to identify all critical assets, including hardware, software, data, and personnel.
* This involves creating an inventory of assets and classifying them based on their importance to the organization.
* Vulnerability scanners like Nessus play a vital role in this step. They identify technical weaknesses in systems and applications that could be exploited by attackers.
* Beyond technical vulnerabilities, it's also important to consider human vulnerabilities, such as lack of security awareness, and physical vulnerabilities, such as inadequate access controls.
* Threat intelligence feeds, security advisories, and industry reports can help organizations stay informed about emerging threats.

TREND ANALYSIS :

1. Evolution of Cyber Threats :-

a) Increasing Cyber Attacks :

Rise in Ransomware & Phishing Attacks – Attackers exploit vulnerabilities to deploy ransomware and steal sensitive information.Zero-Day Vulnerabilities – Hackers target previously unknown security flaws before patches are available.IoT & Cloud Security Risks – More connected devices mean larger attack surfaces for cybercriminals.

b) Shift Towards Advanced Persistent Threats (APT) :

Cybercriminals are using AI-driven attacks to bypass traditional security measures.State-sponsored hacking groups conduct long-term, stealthy intrusions into critical systems.

2. Trends in Vulnerability Scanning Tools :-

a) Rise of Automated & AI-Powered Scanners :

Nessus and similar tools are integrating AI and machine learning to detect vulnerabilities faster and reduce false positives.AI-driven scanning tools help predict potential attack vectors before they are exploited.

b) Cloud-Based Security Solutions :

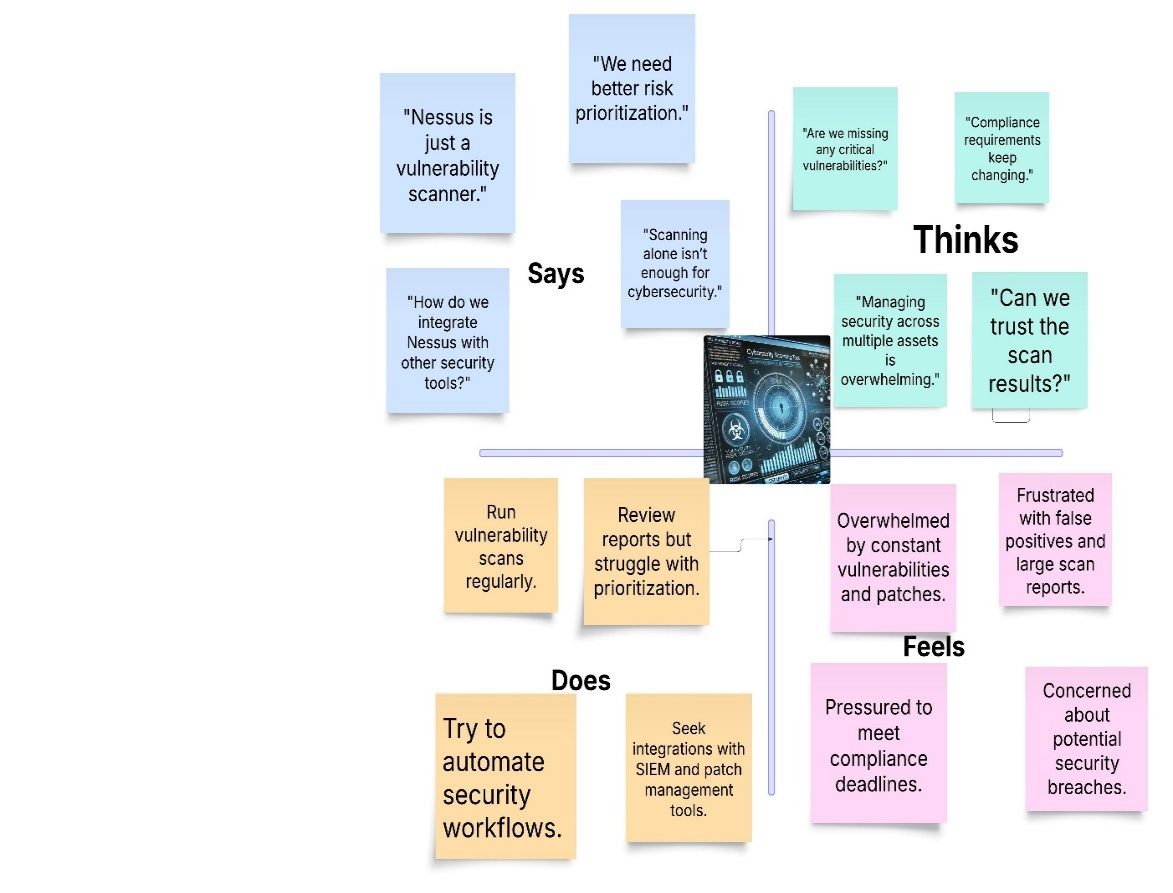
Traditional on-premise scanners are transitioning to cloud-based vulnerability scanning, as seen with Qualys and Tenable.io.Cloud-native security solutions allow real-time monitoring and remote security assessments.

**3. Comparative Analysis of Nessus vs. Other Tools**

| **Feature** | **Nessus** | **OpenVAS** | **Qualys** | **Nexpose** |
| --- | --- | --- | --- | --- |
| **Scanning Type** | Network & system | Network | Cloud & hybrid | Risk-based scanning |
| **Deployment** | On-prem & cloud | Open-source | Cloud-based | On-prem & cloud |
| **Threat Intelligence** | Real-time updates | Community-based | AI-powered | Adaptive scanning |
| **Compliance Support** | Strong | Moderate | Enterprise-grade | High |
| **Best For** | Enterprises, IT Teams | Small Security Teams | Large Organizations | Security Professionals |

**4. Future Trends in Cybersecurity & Scanning Tools**

✔ **AI-Driven Vulnerability Detection** – Machine learning will improve threat prediction and risk prioritization.  
✔ **Cloud & Hybrid Security Scanning** – More organizations will adopt cloud-based scanners for remote security assessments.  
✔ **Automated Incident Response** – Integration with **SOAR systems** will allow automated remediation of detected threats.  
✔ **Zero Trust Security Models** – Vulnerability scanning will be part of Zero Trust frameworks for **continuous verification** of network assets.  
✔ **Increased Focus on Web & API Security** – Web applications and APIs will require **specialized scanning tools** like Acunetix and Burp Suite.

Step-3: Empathy Map

PROJECT PLANNING :

Product backlog,sprint schedule,and Estimation

Use the below template to create product backlog and sprint schedule

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sprint | Functional  Requirement  (Epic) | User  Story  Number | User Story/Task | Story  Points | Priority | Team Members |
| Sprint 1 | Data  Collection | USN-1 | Collect data from various  Cybersecurity websites like (Krebs on security , info security magine , etc.). | 5 | High | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |
| Sprint 1 |  | USN-2 | Use Real Time APIs to gather data. | 3 | Medium | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |
| Sprint 2 |  | USN-3 | Get various news about the different kinds of cybersecurity vulnerabilities like (XSS , RCE , etc.). | 2 | Low | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |
| Sprint 2 | Processing | USN-4 | Use of data processing platforms like (Apache Storm , SIEM , etc.). | 5 | High | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |
| Sprint 2 |  | USN-5 | Use of cybersecurity libraries like (Scapy , cryptography , etc.) to work on the given data. | 4 | High | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sprint 3 | User Interface | USN-6 | Use of various coding languages like (Ruby , Assembly language) and React.js helps to create a simple yet effective dashboard for the user. | 5 | High | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |
| Sprint 3 |  | USN-7 | Having a separate login implemented for users to see dashboard particular to their content. | 3 | Medium | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |
| Sprint 3 | Data Visualization | USN-8 | Use tools like Datadog , Loggly , Qradar , etc. to show various data in a more readable format to the user for easy to understand. | 5 | High | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |
| Sprint 4 |  | USN-9 | Have a feature to ask user for their suggestions reagarding the given task. | 2 | Low | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |
| Sprint 4 | Scalability | USN-10 | Use Docker , Kubernetes to scale the whole project. | 5 | High | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |
| Sprint 4 |  | USN-11 | Have a better database system to store the real time and other various data. | 5 | High | Sakshi ,  Harshini ,  Lakshmitha Reddy ,  Kiran |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SPRINT | TOTAL STORY POINTS | DURATION | SPRINT START DATE | SPRINT END DATE (PLANNED) | STORY POINTS COMPLETED (AS ON PLANNED END DATE) | SPRINT RELEASE DATE(ACTUAL) |
| SPRINT-1 | 12 | 6 DAYS | 21 JAN 2025 | 26 JAN 2025 | 12 | 26 JAN 2025 |
| SPRINT-2 | 12 | 6 DAYS | 28 JAN 2025 | 2 FEB 2025 | 08 | 3 FEB 2025 |
| SPRINT-3 | 12 | 6 DAYS | 6 FEB 2025 | 11 FEB 2025 | 12 | 11 FEB 2025 |
| SPRINT-4 | 12 | 6 DAYS | 14 FEB 2025 | 19 FEB 2025 | 10 | 20 FEB 2025 |

Velocity **:-**

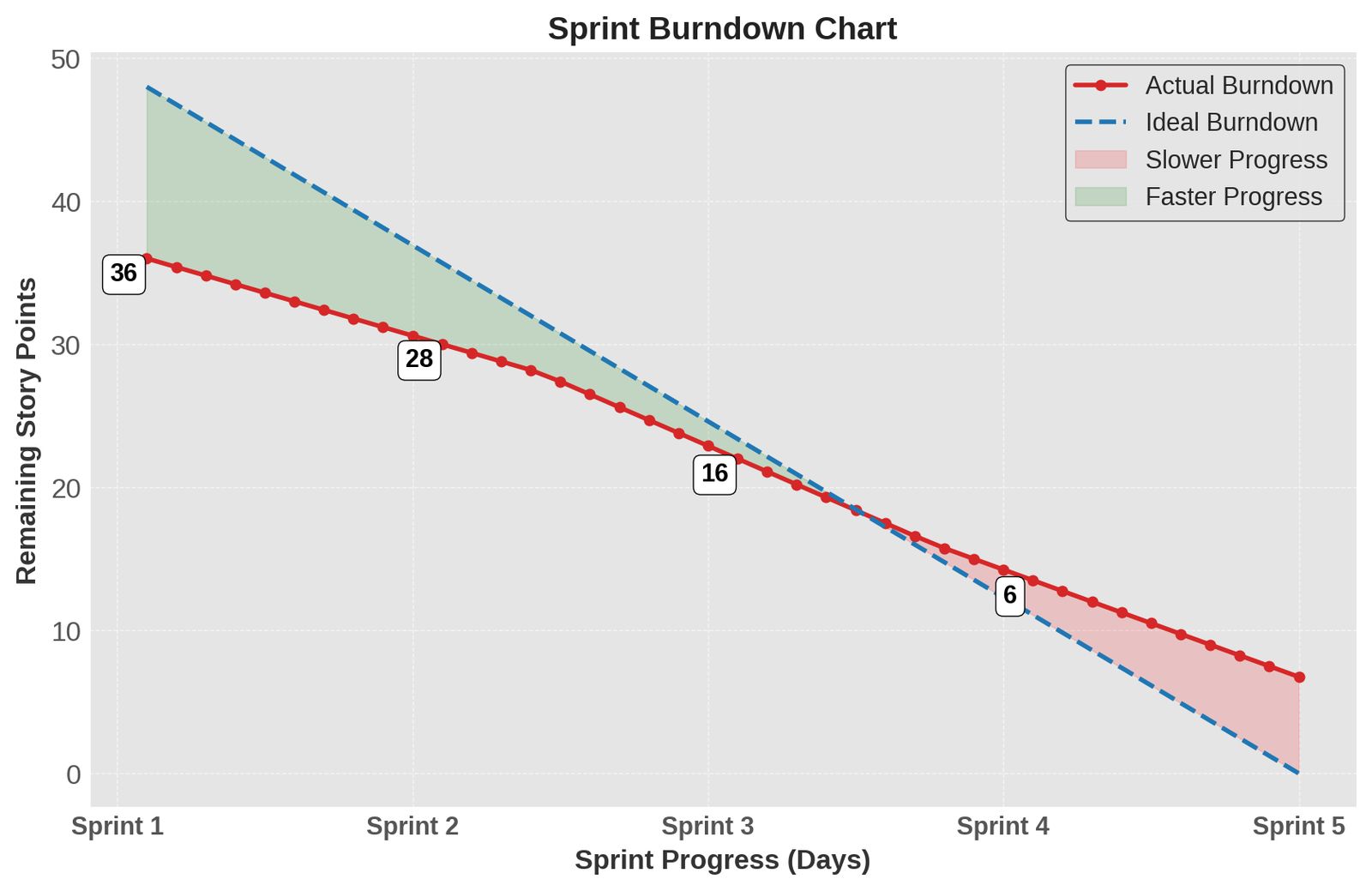
Imagine we have a 10-day sprint duration and the velocity

Of the team is 20 (points per sprint). Let’s calculate the teams average velocity (AV) per iteration unit (story points per day)

Average Velocity (AV)=Total Story Points / number of Sprints

=42/4 =10.5(approx.)

**The Sprint Burndown Chart : -**

****

1. X-Axis: Represents sprint progress in days.

2. Y-Axis: Represents remaining story points (work left to complete).

3. Red Line (Actual Burndown): Shows the real progress of the team in completing work.

4. Blue Dashed Line (Ideal Burndown): Represents the ideal rate of progress

if the team completed work at a steady pace.

5. Green Shaded Area (Faster Progress): Indicates where the actual burndown is ahead of the ideal burndown.

6. Red Shaded Area (Slower Progress): Indicates where the actual burndown is behind the ideal burndown.

7. Labeled Story Points: Highlights remaining work at certain points (e.g., 36, 28, 16, and 6 story points).

PROPOSED SOLUTION TEMPLATE :

STAGE -1

Understanding Various Vulnerabilities :

|  |  |  |
| --- | --- | --- |
| S.NO | VULNERABILITY | CWE-NO. |
| 1. | SQL Injection (SQLi) | CWE-89 |
| 2. | Cross-Site Scripting (XSS) | CWE-79 |
| 3. | Cross-Site Request Forgery (CSRF) | CWE-352 |
| 4. | Security Misconfiguration | CWE-16 |
| 5. | Server-Side Request Forgery (SSRF) | CWE-918 |

Top 5 Vulnerabilitiy Exploitation

Vunlerability Name :- SQL Injection (SQLi)

SQL Injection (SQLi)

CWE No. :- CWE-89

OWASP/SANS Category :- Top 5

Description :

SQL Injection (SQLi) is a critical security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. By injecting malicious SQL statements into input fields, an attacker can manipulate, retrieve, or even delete data stored in the database. SQLi occurs due to improper input validation and insufficient sanitization of user inputs before they are used in SQL queries.

**Business Impact :**

* + Data leakage (sensitive customer/financial data exposure)
  + Unauthorized access to databases
  + Loss of data integrity and application compromise

**Steps to Identify:**

* + Use single quotes ('), double quotes ("), or comment markers (--, /\* \*/) in input fields to check for SQL errors.
  + Use automated tools like SQLMap, Burp Suite, or OWASP ZAP.
  + Check for error messages exposing database details.

Vulnerability Name :- Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS)

CWE No. :- CWE-79

Description :

Cross-Site Scripting (XSS) is a security vulnerability that allows an attacker to inject **malicious scripts (typically JavaScript)** into a web application. These scripts execute in the victim's browser, enabling the attacker to steal sensitive information, hijack user sessions, or manipulate website content.

XSS occurs when user input is not **properly validated or escaped** before being displayed in the web page. Since web browsers trust scripts from legitimate websites, the injected script executes as if it came from the original site.

**Business Impact:**

* Stealing user cookies and session tokens
* Defacement of the website
* Phishing and spreading malware

**Steps to Identify:**

* Input <script>alert('XSS')</script> into form fields and check if an alert pops up.
* Use automated scanners like OWASP ZAP and Burp Suite.
* Look for missing input sanitization and improper output encoding.

Vulnerability Name :- Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF)

CWE No. :- CWE-352

Description :

Cross-Site Request Forgery (CSRF) is a web security vulnerability that **tricks an authenticated user into performing unintended actions** on a web application. The attack exploits the fact that web browsers automatically include user credentials (cookies, session tokens, etc.) in requests to a website.

**Business Impact:**

* + Unauthorized actions performed on behalf of a logged-in user
  + Funds transfer, email change, or account takeover
  + Data manipulation and exposure

**Steps to Identify:**

* + Check if critical actions (password reset, transactions) can be performed without authentication tokens.
  + Test by embedding malicious requests in HTML <img> or <iframe> tags.
  + Use OWASP CSRF Tester or Burp Suite.

Vunlerability Name :- Security Misconfiguration

Security Misconfiguration

CWE No. :- CWE-16

Description :

**Security Misconfiguration** occurs when an application, server, database, or cloud environment is not **properly configured**, leaving security gaps that attackers can exploit. This can happen due to **default settings, unnecessary features, lack of hardening, or exposed sensitive information**.

Misconfigurations can lead to **unauthorized access, data leaks, privilege escalation, and system compromise**. It is one of the most common and **easily exploitable** vulnerabilities.

**Business Impact of Security Misconfiguration**

Security misconfigurations can lead to **critical security breaches** with severe consequences:

* **Data Breaches** – Exposed cloud storage or open directories leak **sensitive user information**.
* **System Compromise** – Default credentials allow attackers to **take over databases or servers**.
* **Privilege Escalation** – Misconfigured access controls let attackers gain **higher privileges**.
* **Compliance Violations** – Misconfigurations can result in **GDPR, HIPAA, or PCI DSS** violations.
* **Financial & Reputational Damage** – Public data leaks lead to **customer trust issues** and **legal consequences**.
* Use **OWASP ZAP, Nessus, and Burp Suite** to find vulnerabilities.

**Steps to Identify Security Misconfigurations**

1. **Check for Default Credentials & Unused Accounts**
   * Audit **admin panels, databases, and services** for **default usernames & passwords**
2. **Scan for Exposed Services & Open Ports**
   * Use **Nmap** or **Shodan** to detect open ports and exposed services.
3. **Test for Open Directories & Cloud Storage**
   * Check if **AWS S3, Google Cloud Buckets, or Azure Blobs** are publicly accessible.
4. **Inspect Configuration Files & Permissions**
   * Review .env, config.php, and .htaccess for **exposed credentials**.
5. **Check for Unpatched Software & Weak Security Headers**
   * Use **Nikto** or **Burp Suite** to detect outdated software and missing security headers.

Top of Form

Bottom of Form

Vunlerability Name :- Server-Side Request Forgery (SSRF)

Server-Side Request Forgery (SSRF)

CWE No. :- CWE-918

Description :

**Server-Side Request Forgery (SSRF)** is a web security vulnerability that allows an attacker to manipulate a server into making unintended requests to internal or external resources. Unlike **Cross-Site Request Forgery (CSRF),** which tricks a user’s browser into making a request, SSRF exploits a vulnerable server **to send unauthorized requests** on behalf of the attacker.

This vulnerability is especially dangerous when the targeted server can access **internal networks, cloud metadata services, or sensitive endpoints** that are otherwise inaccessible to an attacker.

**Business Impact:**

* + Internal network scanning and data exfiltration
  + Access to cloud metadata (AWS/GCP credentials leak)
  + Remote code execution in extreme cases

**Steps to Identify:**

* + Test by submitting internal IP addresses (127.0.0.1, 169.254.169.254).
  + Check for open URL fetching via user input.
  + Use Burp Suite, SSRFMap, or manual payload injection.