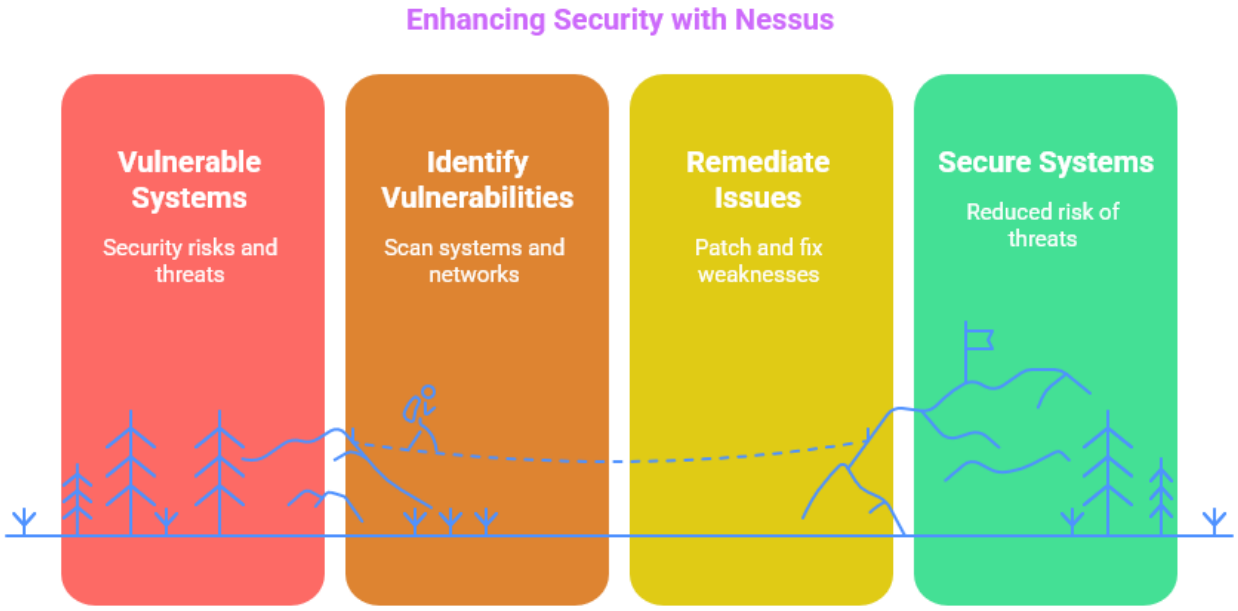
Nessus Overview:

Nessus is a widely used vulnerability assessment tool that helps organizations to identify and remediate security vulnerabilities in their systems and networks.

Nessus is developed by Tenable, Inc. and is known for its comprehensive scanning capabilities. It can detect vulnerabilities across various platforms, including Operating Systems, network devices, databases, and web applications. Nessus provides detailed reports that help security teams prioritize vulnerabilities based on their severity and potential impact.

Nessus is an essential tool for organizations looking to strengthen their security defenses through effective vulnerability management. By conducting regular assessments and addressing identified vulnerabilities, organizations can significantly reduce their risk exposure and enhance their overall security posture.



A SOC team uses Nessus to run weekly vulnerability scans across internal systems. When Nessus finds a high-severity vulnerability like **CVE-2021-34527 (PrintNightmare)**, the team cross-checks it in the NVD, exports the scan to their SIEM, and pushes a remediation ticket to IT. This cycle repeats, ensuring continuous hardening of their environment.

Nessus in Action:

1. You point Nessus at your network.
2. It scans for vulnerabilities like outdated software or open ports.
3. It gives you a report with **what's wrong** and **how to fix it**.

Nessus is one of the most widely used vulnerability scanners in the cybersecurity industry. It plays a key role in the proactive identification of vulnerabilities across systems, helping security teams prioritize remediation before attackers can exploit them.

Function	Description
Asset Discovery	Identifies systems and services in your environment
Vulnerability Detection	Scans for known CVEs using plugin signatures
Risk Scoring	Rates findings using **CVSS scores**
Reporting	Generates executive and technical remediation reports
Continuous Monitoring	Supports scheduled scans and compliance checks

Feature	Benefit
Accuracy	Low false-positive rate
Ease of Use	Easy web interface with ready-made templates
Extensive Plugin Library	190,000+ plugins regularly updated
Free Version (Essentials)	Great for learning and labs
Integrates with SOC Tools	Compatible with Metasploit, SIEMs, etc.
Policy & Compliance Scanning	Supports CIS, PCI-DSS, HIPAA templates

CVE-Based Scanning	Detects known vulnerabilities mapped to CVE IDs.
Plugin-Based Architecture	70,000+ plugins updated daily by Tenable Research.
Credentialed & Non-Credentialed	Deeper scans with admin/root access.
Custom Policies	Flexible scan profiles tailored to the environment.
Comprehensive Reporting	Risk-rated outputs in HTML, PDF, CSV.
Compliance Checks	Supports standards like PCI DSS, HIPAA, CIS, NIST.