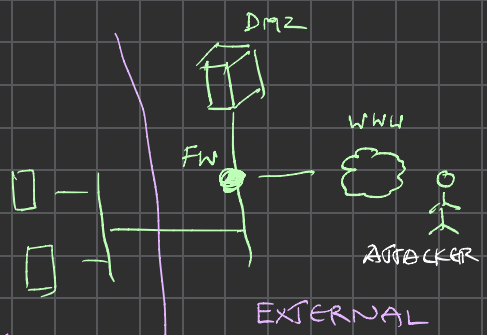
VULNERABILITIES

- ✓ Software Vuln (EXAMPLES threat vectors associated : SQL Injection, Buffer overflow)
- ✓ Configuration Vuln ('permit any' to all resources rule)
- ✓ Hardware Vuln (Flaws in H/W components)
- ✓ System Vuln (at OS level)
- ✓ Network Vuln (similer to config Vuln but specific to network components)
- ✓ Human Vuln (Social Engg attacks)
- ✓ Process Vuln (poor password policies, weak process controls)

→ Internal Vuln
→ External Vuln



- Misconfigured user perm
- Unpatched S/W
- Insider threats

- Unsecured web applications
- Open ports in FW
- Lack of encryption for data in transit
- Phishing attacks

CVSS

(Common Vulnerability Scoring System)

→ framework for measuring the severity of security Vuln

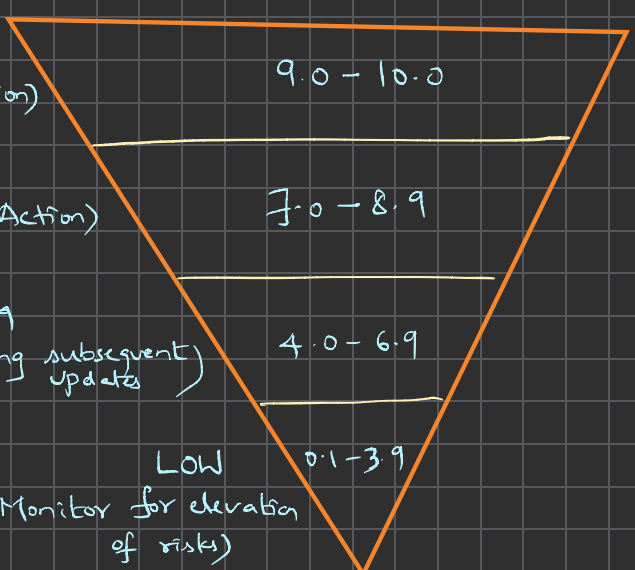
→ Scoring range → (0 – 10)

→ Severity Indication → Higher scores ⇒ severe security issue

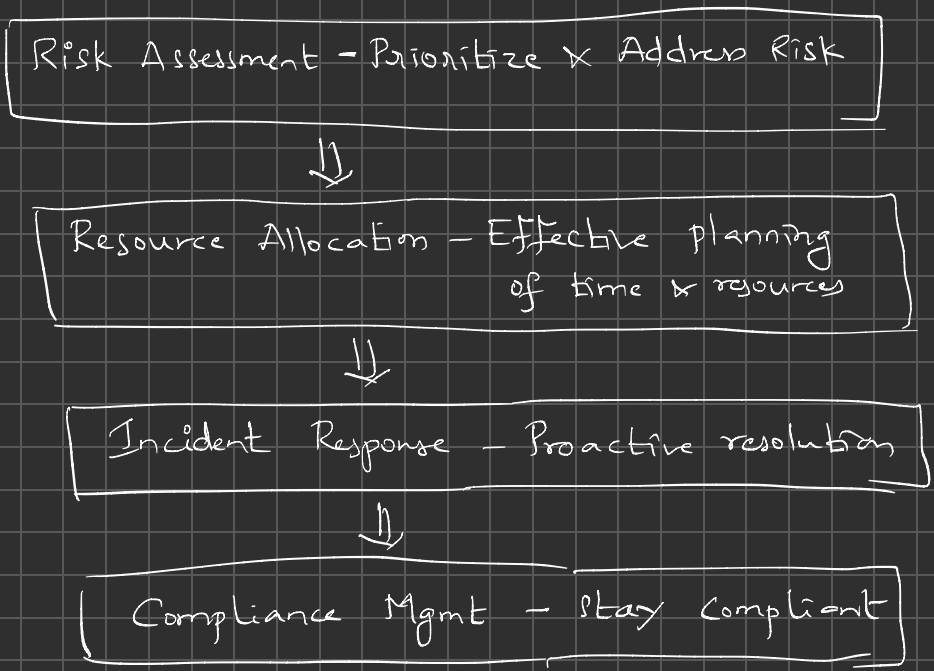
→ Purpose of CVSS → Helps companies prioritize security threats to address

→ Key benefits → Streamlines Vuln Assessment
↳ helps in decision-making for risk mitigation

Metrics



CVSS Applications

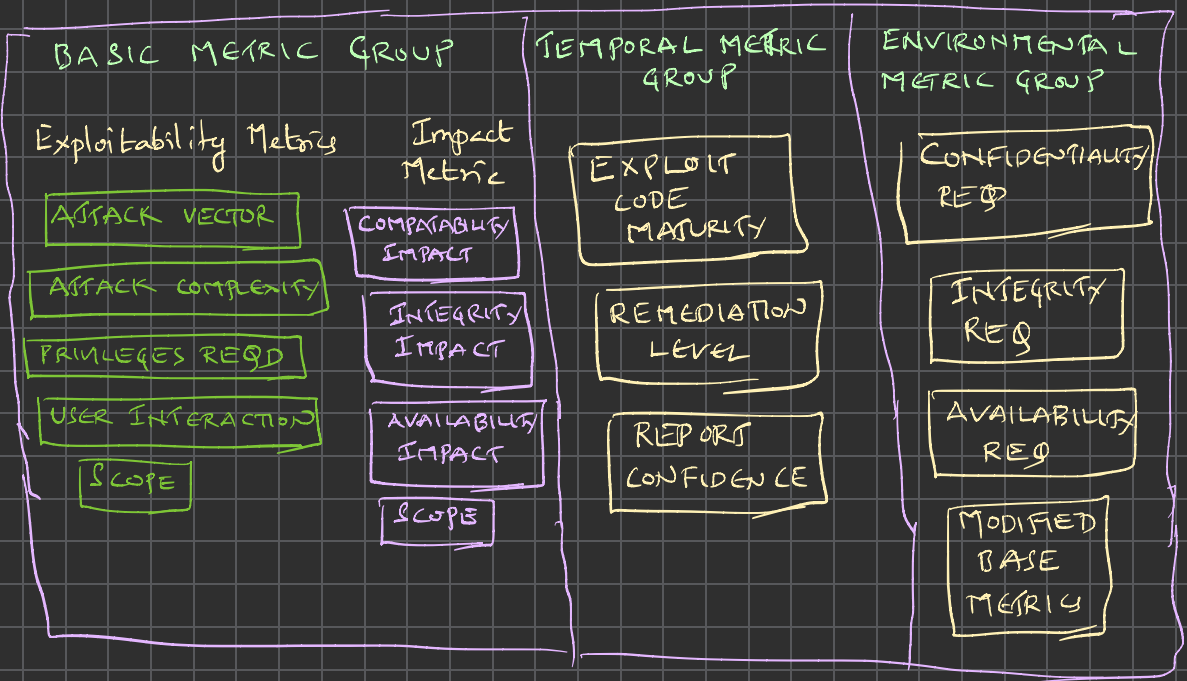


CVSS Calculation

A CVSS score — based on 3 metrics : Base, Temporal, Environmental.

Each has its own scoring elements

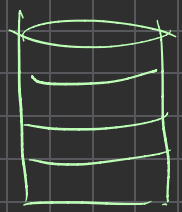
CVSS SCORE METRIC



National Vulnerability Database (NVD) ← maintained by NIST

nvd.nist.gov

VULNERABILITY DATABASES



Collection of known (confirmed) security vulnerabilities

Why this DB is read? (helps in risk assessment exercises)

1. Centralized source for identifying security weaknesses
2. Proactive defense and patch management
3. Risk assessment and compliance

Types of Vuln. Databases:

Public Vuln Databases

- NVD maintained by NIST

Private Vuln. Databases

- Vendor specific (eg: Microsoft, Cisco)
- Subscription-based services (eg: Qualys, Tenable)

Understanding CVE ID

Each Vulnerability stored in Vuln. Database has a unique ID known as CVE-ID

ex: MS Office Privilege Escalation vulnerability
CVE-2023-23397