**DAY 5**

**Notes on CVSS, CVE, and NVD**

**1. Common Vulnerability Scoring System (CVSS)**

* A standardized system for assessing the severity of security vulnerabilities.
* Provides an open framework for communicating vulnerability characteristics and impacts.
* **Scoring system:** Ranges from **0 to 10**, where **10** represents the highest severity.
* **Three metrics used for scoring:**
  1. **Base Score Metrics** – Represents intrinsic qualities of the vulnerability.
  2. **Temporal Score Metrics** – Reflects current state and exploitability.
  3. **Environmental Score Metrics** – Considers specific user environment.



**2. Common Vulnerabilities and Exposures (CVE)**

* A dictionary of publicly known cybersecurity vulnerabilities.
* Each vulnerability is assigned a **unique CVE identifier**.
* Acts as a **universal standard** for identifying and referencing vulnerabilities.
* Does not provide severity scores but includes a brief description of the issue.

**3. A** **Common Platform Enumeration (CPE)**

* Represents a specific product, software, or hardware version. Since vulnerabilities (CVEs) are often **version-specific**.
* It helps in standardizing product names for security tools, making it easier to track vulnerabilities (CVEs), manage assets, and perform security assessments.
* A single CPE can be associated with **multiple CVEs**, each affecting different versions or configurations of the product.
* **CPE Format Example:**
* *cpe:2.3:a:microsoft:windows\_10:1909:\*:\*:\*:\*:\*:\*:\**This refers to **Windows 10, version 1909**.
* This CPE identifier represents **Microsoft Windows 10, version 1909**.
* Break down in detail:

1. **cpe:2.3** → This indicates the **CPE version**. Here, **2.3** means the identifier follows the CPE 2.3 standard.
2. **o** → This represents the **Operating System (OS)**. If it were software, it would be **a** (for applications), and for hardware devices, it would be **h**.
3. **microsoft** → This is the **vendor (company name)** that develops the product. In this case, it is **Microsoft**.
4. **windows\_10** → This is the **product name**, specifying that the CPE refers to **Windows 10**.
5. **1909** → This is the **version number**, indicating that it is **Windows 10 version 1909**.
6. **\* (asterisks)** → These are wildcards, representing optional or unspecified fields (such as updates, language, or edition) that are not explicitly provided here.

**Use Case of This Example:**

* This CPE identifier is used in the **NVD (National Vulnerability Database)** and **cybersecurity systems** to track vulnerabilities (CVE - Common Vulnerabilities and Exposures).
* If any security flaw is found in Windows 10 version 1909, its CVE reports will be linked to this CPE identifier.
* Resource – [Link](https://nvd.nist.gov/products/cpe/detail/3AB38A7B-218B-41F2-9CB9-E7E4F4DFF539?namingFormat=2.3&orderBy=CPEURI&keyword=cpe%3A2.3%3Ao%3Amicrosoft%3Awindows_10&status=FINAL%2CDEPRECATED)
* CPEs are widely used in security databases like the **National Vulnerability Database (NVD)** to link vulnerabilities to specific products and versions.

**4. National Vulnerability Database (NVD)**

* An extension of the CVE system, offering additional analysis and metrics.
* Maintained by the **National Institute of Standards and Technology (NIST)**.
* Provides:
  + **CVSS scores** for vulnerabilities.
  + **Checklists, impact metrics, and fixes**.
  + A **comprehensive repository** of cybersecurity vulnerabilities.

**5. Differences Between CVSS, CVE, and NVD**

* **CVSS** → The **grading system** that evaluates severity.
* **CVE** → The **list of known vulnerabilities**, each with a unique ID.
* **NVD** → The **comprehensive database** containing CVEs, CVSS scores, and additional insights.

**6. Importance of CVSS, CVE, and NVD**

* Helps cybersecurity professionals **identify, evaluate, and manage** vulnerabilities.
* CVSS scores assist in prioritizing vulnerabilities based on severity.
* CVE allows for **standardized reporting** and easier collaboration.
* NVD provides a **detailed repository** to analyze and mitigate threats.

**7. Patching & Limitations**

* **Patching** vulnerabilities is crucial to prevent cyber-attacks.
* **Limitations:**
  + CVSS scores focus on **technical severity**, not always **real-world risk**.
  + CVE only catalogues **known** vulnerabilities.
  + Organizations must ensure **timely patching** to mitigate risks.

**Conclusion**

Understanding **CVSS, CVE, and NVD** is essential in cybersecurity for identifying, scoring, and mitigating vulnerabilities effectively. Despite their limitations, they remain **indispensable tools** in securing digital systems.