DAY 5

* **NVD (National Vulnerability Database)**

The National Vulnerability Database (NVD) is a U.S. government repository of known cybersecurity vulnerabilities, managed by the National Institute of Standards and Technology (NIST).

* **Common Platform Enumerations (CPE)**
* CPE (Common Platform Enumeration) is a system for identifying software, hardware, and operating systems in a standard way.
* Each product gets a unique CPE name.
* Example- cpe:2.3:o:microsoft:windows\_10:1909:\*:\*:\*:\*:\*:\*:\*
* Break down in detail:
  + cpe:2.3 → This indicates the CPE version. Here, 2.3 means the identifier follows the CPE 2.3 standard.
  + 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.
  + microsoft → This is the vendor (company name) that develops the product. In this case, it is Microsoft.
  + windows\_10 → This is the product name, specifying that the CPE refers to Windows 10.
  + 1909 → This is the version number, indicating that it is Windows 10 version 1909.
  + **\*** (asterisks) → These are wildcards, representing optional or unspecified fields (such as updates, language, or edition) that are not explicitly provided here.
* **Importance of CPE:**

**1. Identifies Affected Systems**

* CPE links software, hardware, and operating systems to known vulnerabilities (CVEs).
* Helps security teams check if a specific version of software is at risk.

**2. Standardizes Product Naming**

* Avoids confusion by using a consistent format to name products.
* Example: Instead of different names like "Win10 v1909" or "Windows 10 1909," CPE uses a standard format.

**3. Enhances Threat Intelligence**

* Organizations can track vulnerabilities for specific products and plan updates or patches.
* Helps cybersecurity professionals manage risks more effectively.
* NVD provides:

1. **CVE Details: (Common Vulnerabilities and Exposures)**

* What the problem is
* Which software or system is affected
* How serious it is
* How to fix or reduce the risk

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

* The Common Vulnerability Scoring System (CVSS) is a way to measure how serious a cybersecurity flaw is.
* It gives each flaw a score from 0 to 10, with higher numbers meaning greater risk.
* CVSS Score Breakdown:
  + 0.0 - None → No risk
  + 0.1 - 3.9 - Low → Minor impact
  + 4.0 - 6.9 - Medium → Some risk, but not critical
  + 7.0 - 8.9 - High → Serious threat
  + 9.0 - 10.0 - Critical → Very dangerous, needs urgent fixing