MAY MONTH

Week – 2

1. CVSS

* CVSS abbreviates to Common Vulnerability Scoring System.
* First.org – introduced in 2005.
* Most used version – 3.O(2019)
* CVSS metrics can be categorized into three types:

1. Basic metric group
2. Temporal metric group
3. Environmental metric group

CVSS is used to evaluate vulnerabilities on applications. It can be scored from 0 to 10, from low to high risk of having vulnerability.

|  |  |
| --- | --- |
| **SCORE** | **RISK** |
| 0 | NONE |
| 0.1 to 3.9 | LOW |
| 4.0 to 6.9 | MEDIUM |
| 7.0 to 8.9 | HIGH |
| 9.0 to 10 | CRITICAL |

**Base metrics:**

Factors influence CVSS scores:

* Can be divided into 3 groups:

1. Exploitability
2. Impact
3. Scope
4. Exploitability metric
5. Attack vector

* Attackers’ ability to attack or exploit the system / where attack can happen  
  🡪 Network – if it can be exploited through internet – High score

🡪 Adjacent

🡪 Local

🡪 Physical

1. Attack complexity

* Difficulty of executing an attack. It can be either  
  🡪 high

🡪 low – if yes, score is high

1. Privileges required

* Access needed to perform a successful attack. It can be:  
  🡪 None – if yes, score is high

🡪 High

🡪 Low

1. User interaction

* User involvement to succeed in attack

🡪 None – if yes, severity is high

🡪 Required

1. Impact
2. Confidentiality impact

* Potential of unauthorized access
* Disclosure of data

🡪 None

🡪 High - if yes, severity is high

🡪 Low

1. Integrity impact

* Potential of unauthorized modification of data

🡪 None

🡪 High - if yes, severity is high

🡪 Low

1. Availability impact

* Potential of denial of access

🡪 None

🡪 High - if yes, severity is high

🡪 Low

1. Scope

* Existing vulnerability can affect other components. It can be either

🡪 Changed – if yes, score is high.

🡪 Unchanged

**Temporal metrics**

* It is based on the vulnerabilities that change over time.

**Environmental metrics**

* It is based on the specific organization’s needs