Vulnerability Management

What is Vulnerability?

- A vulnerability is a weakness in a system, network or application.
  - System – Running with older version of a software
  - Network – Use of unsecure protocols
  - Application – No user input validation (leads to injection attacks)

What is Threat?

- Anything/Anyone that can exploit a vulnerability, intentionally or accidentally is a Threat

  Example: An attacker or Earthquake or Untrained Staff

What is Risk?

- The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

  Example: Financial losses because a e-commerce server is down, Loss of reputation etc.

What is Exploit?

- A tool used to take advantage of the vulnerability.

  Example: Eternal Blue (take advantage of SMB vulnerability)

What is Vulnerability Assessment?

- Vulnerability Assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures.
- Vulnerability Assessment team closely works with other infrastructure teams to help them remediate/patch vulnerabilities with the systems they manage.

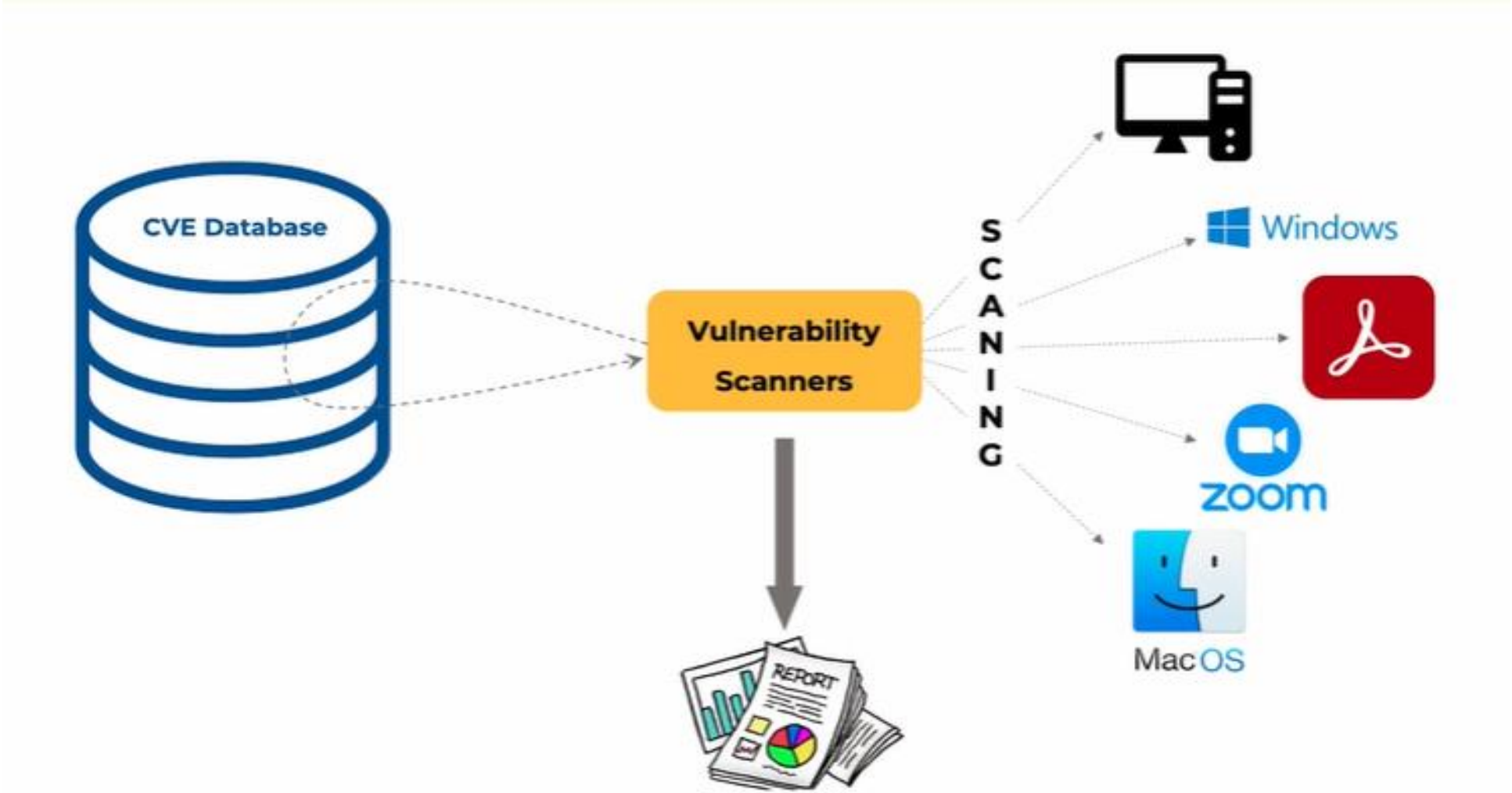
Explain Vulnerability Management life cycle.

- **Discover** - Discover all the assets (using an host discovery scan)
- **Prioritize Assets** - Prioritize the assets based on the criticality and risk.
- **Assess** - Perform Vulnerability Assessment to identify vulnerabilities
- **Report** - Report all the vulnerabilities, based on criticality and business risk
- **Remediate** - Remediate the vulnerabilities by applying the patches or modifying the configurations
- **Verify** - Confirm that the patch has be applied successfully by rescanning the machines

Name few VA tools?

- The popular Vulnerability Assessment tools are
  - ✓ Tenable Nessus
  - ✓ Qualys Guard
  - ✓ Rapid7 Nexpose
  - ✓ OpenVAS (Open Vulnerability Scanner) – Open source tool

Vulnerability Scanners



Where do you find Vulnerability details?

- Few good source of all the vulnerabilities are
  - www.cvedetails.com
  - www.nvd.nist.gov (National Vulnerability Database)
  - www.cve-mitre.org

What is CVE?

- CVE stands for Common Vulnerabilities and Exploits. It is a number given to each identified vulnerability.
- CVE is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.
- The format of the CVE is:

  CVE prefix + Year + 4 Arbitrary Digits (CVE-YYYY-NNNN)

  Example: CVE-2019-1760

What is CVSS?

- CVSS stands for Common Vulnerability Scoring System. It is an industry standard used by vendors to define the criticality of a vulnerability. The score ranges from 0 to 10.
- CVSS are categorized as below:

Categories of CVSS v3.0

How frequently should a Vulnerability scans be run?

When does a company run Vulnerability Scans?

- Vulnerability assessments are usually performed on a scheduled basis, typically Monthly once or Quarterly once.
- Also scan can be run on need basis. A solid example is when a new headline vulnerability emerges. When this vulnerability assessment is performed, the scan are configured to specifically look for the new vulnerability.

- Vulnerability scans are usually performed on a scheduled basis **Monthly** **Quarterly**

- Scans are run on - need basis (Ad hoc Scans)

E.g.: When a new critical headline vulnerability emerges.

The scan is configured to look for the specific (new) vulnerability.

SOC Team and VA Team

- SOC Team provide assistance in Reporting & Prioritizing Vulnerabilities
- Coordinate with various teams for patching status.
- SOC Team raise tickets and assign it to VA teams in order to run Ad-hoc scans.