Vulnerabilities 101

In this module we learn the importance of what a vulnerability is, why they are worth learning about and how they are rated.

A vulnerability is a **weakness or flaw in design.** This is a result of the implementation behaviours of a system. An attacker can exploit these weaknesses to gain access to unauthorised information, or perform unauthorised actions.

NIST - National Institute of science and technologies defines a vulnerability as a **weakness in an information system.** System security procedures, internal controls or implementation could be exploited or triggered by a threat source.

VULNERABILITIES:

Operating System: These are vulnerabilities found within the operating system itself, often the result of privilege escalation.

Misconfiguration based: Stemming from incorrectly configured application or services. For example a website exposing user details.

Weak of default credentials: Application and services that have an element of authentication will come with default credentials. But these credentials may be easy and unchanged and therefore easy to be compromised.

Application logic: A result of poorly designed applications. An example of this could be poorly implemented authentication mechanisms that may result in an attacker being able to impersonate a user.

Human-Factor: Vulnerabilities that leverage human behaviour. For example phishing emails, tricking people into believing they are legitimate.

Questions:

1. An attacker is able to upgrade the permissions of their system from user to admin, what vulnerability is this? **Operating system**
2. You manage to bypass a login panel using cookies to authenticate. What vulnerability is this? **Application logic**

Scoring Vulnerabilities (CVSS & VPR)
Vulnerability management is the combined process of evaluation and remediating threats faced by organisations. It is arguable that there is a patch or immediate fix that is available for every vulnerability.

Approximately 2% of vulnerabilities only ever end up being exploited. Instead it is all about **addressing the most dangerous vulnerabilities and reducing the likelihood of an attack vector being used to exploit a system.**

This is where vulnerability scoring comes into play. This serves a vital role in vulnerability management and is used to determine the potential risk and impact a vulnerability may have on a network of computer system. Eg **CVSS = Common Vulnerability Scoring System** which awards points. Awards points to a vulnerability based upon its features, availability and reproducibility.

Common Vulnerability scoring system

1. **How easy is it to exploit**
2. **Do exploits exist for this**
3. **How does the vulnerability interfere with the CIA triad?**

RATING SCALE | SCORE
None = 0
Low = 0.1-3.9
Medium = 4.0-6.9
High = 7.0 - 8.9
Critical = 9.0 - 10.0

Advantage of CVSS

1. Been around for a long time
2. Popular in organisations
3. Free framework to adopt and recommended by organisations such as NIST

Disadvantages of CVSS

1. CVSS was never designed to help prioritise vulnerabilities. Just value of severity
2. CVSS heavily assesses vulnerabilities on an exploit being available. Only 20% of all vulnerabilities have an exploit available
3. Vulnerabilities rarely change scoring after assessment despite the fact that new developments such as exploits can be found

Vulnerability Priority Rating (VPR)

It’s a much more modern framework in vulnerability management. Developed by tenable-industry solutions provider for vulnerability management. It is **risk driven** meaning vulnerabilities are scored with heavy focus to the risk posed to the organisation itself.

Unlike CVSS, VPR takes into account the relevancy of a vulnerability. For example no risk is considered regarding a vulnerability if that vulnerability does not apply to the organisation. VPR is also considered dynamic in its scoring, where the risk may change almost daily as it ages.

RATING SCALE | SCORE
Low = 0.0-3.9
Medium = 4.0-6.9
High = 7.0-8.9
Critical = 9.0 - 10.0

Advantages of VPR

1. Modern framework - Real World
2. Considers over 150 factors when calculating risk
3. Risk driven and used by organisations to help prioritise patching vulnerabilities
4. Scorings are not final and are very dynamic. Meaning priority should be given “Can change” as it ages

Disadvantages of VPR

1. VPR is not open source like some other vulnerability management frameworks
2. VPR can only be adopted a part of a commercial platform
3. VPR does not consider CIA triad to the extent that CVSS does, meaning that risk to confidentiality, integrity and availability of data does not play a large factor in scoring when using VPR.
4. BLANK

When was CVSS Published? 2005
Vulnerability based on the risk it poses to organisation? VPR
Framework that is free and open source? CSS

Vulnerability: Weakness of flaw in the design of an application.
Exploit: Action or behaviour that utilizes the vulnerability on a system or application.
Proof of Concept (PoC): Technique or tool demonstrating the exploitations of a vulnerability.

NVD - National Vulnerability Database
Website that lists all publically categorized vulnerabilities. **CVE -** Common Vulnerabilities Exposures.

These have the formatting : **CVE-YEAR-IDNUMBER eg - CVE-2017-0144**
NVD allows us to see all CVEs that have been confirmed using filters by category and month of submission.

Exploit-DB
Resource we have as hacker, helps us during an assessment exploit-DB. It retains for software and applications stored under the name, author and version of the software application.

We can exploit DB to look for snippets. To exploit a specific vulnerability.