Cyber Security Tools and Technologies

Acknowledgement

- TryHackMe

Vulnerability

- A v**ulnerability** is defined as a weakness or flaw in the design, implementation or behaviors of a system or application.

NIST definition:

- “weakness in an information system, system security procedures, internal controls, or implementation that
  - could be exploited or triggered by a threat source”.

How Vulnerabilities occur:

- Vulnerabilities can originate from many factors, including a poor design of an application or an oversight of the intended actions from a user.

Main Categories of Vulnerabilities

- Operating System
- (Mis)Configuration-based
- Weak or Default Credentials
- Application Logic
- Human-Factor

- An **exploit** is something such as an action or behaviour that utilises a vulnerability on a system or application.
- A **Proof of Concept** (PoC) is a technique or tool that often demonstrates the exploitation of a vulnerability.

Main Categories of Vulnerabilities

Operating System

- These are found within Operating Systems
- often result in **privilege escalation**.
- Example: **Ping of Death' attack**
  - exploited a flaw in how the Windows OS handled large ICMP packets

(Mis)Configuration-based

- These stem from an incorrectly configured application or service.
- **For example**, a website exposing customer details.

Main Categories of Vulnerabilities

Weak or Default Credentials

- Applications and services having **authentication element** may come with **default credentials** when installed.
- For example, an administrator dashboard may have the username and password of "admin". These are easy to guess by an attacker.

Main Categories of Vulnerabilities

Application Logic

- As a result of poorly designed applications.
- For example, poorly **implemented authentication** mechanisms that may result in an attacker being able to impersonate a user
  - manage to bypass a login panel using cookies to authenticate

Human-Factor

- These leverage human behaviour.
- For example, phishing emails are designed to trick humans into believing they are legitimate.

Scoring Vulnerabilities

- **Vulnerability manage**ment is the process of evaluating, categorising and ultimately remediating threats (vulnerabilities) faced by an organisation.
- Impossible to patch and remedy every single vulnerability in a network or computer system and sometimes a waste of resources.
  - As only approximately 2% of vulnerabilities only ever end up being exploited
- Instead, address the most dangerous ones and reducing the likelihood of an attack vector being used to exploit a system.

Scoring Vulnerabilities

- **Vulnerability scoring is** used to determine the potential risk and impact a vulnerability may have on a network or computer system.

Vulnerabilities Management Frameworks

I. Common Vulnerability Scoring System (**CVSS**)
   - awards points to a vulnerability based upon its features, availability, and reproducibility.

II. **Vulnerability Priority Rating (**VPR)
   - another modern framework for vulnerability management

Scoring Vulnerabilities

Common Vulnerability Scoring System (**CVSS**)

- Has three major iterations
- a score is essentially determined by some of the following factors

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

Calculate the score using this framework:
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Scoring Vulnerabilities

CVSS Vulnerability Classification

- A vulnerability is given a classification (out of five) depending on the score that is has been assigned.
- Qualitative Severity Rating Scale and their score ranges

Rating	**Score**
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Scoring Vulnerabilities

CVSS Advantages

- around for a long time.
- popular in organisations, industries and government groups
  - Amazon, Huawei, MySDN, Philips Healthcare
- a free framework to adopt and recommended by organisations such as NIST

Scoring Vulnerabilities

CVSS Disdvantages

- never designed to help prioritise vulnerabilities, instead, just assign a value of severity
- heavily assesses vulnerabilities on an exploit being available
  - However, only 20% of all vulnerabilities have an exploit available
- rarely change scoring after assessment despite the fact that new developments such as exploits may be found.

Scoring Vulnerabilities

VPR Vulnerability Classification

- considered to be risk-driven, it means
  - vulnerabilities are given a score with a heavy focus on the **risk** a vulnerability poses to the organisation itself,
  - rather than factors such as impact (like with CVSS).
- It 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 organization (if no vulnerable software is used)

Scoring Vulnerabilities

VPR Vulnerability Classification

- Considerably **dynamic** in its scoring, where the **risk** that a vulnerability may pose can change almost daily.

Rating	**Score**
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Scoring Vulnerabilities

VPR Advantages

- a modern framework that is real-world.
- considers over 150 factors when calculating risk.
- risk-driven and used by organisations to help prioritise patching vulnerabilities.

Scoring Vulnerabilities

VPR Disadvantages

- not open-source like some others.
- can only be adopted apart of a commercial platform.
- does not consider the CIA triad to the extent that CVSS does;
  - meaning that risk to the confidentiality, integrity and availability of data does not play a large factor in scoring vulnerabilities

Vulnerabilities Databases

Resources on the internet keep track of vulnerabilities for all sorts of software, operating systems and more

Two databases to look up existing vulnerabilities for applications

- 1. https://nvd.nist.gov/vuln - NVD (National Vulnerability Database
- http://www.exploit-db.com/ - Exploit-DB