Tutorial No. 3

Title: CVSS and report on Exploit DB

Roll No.: 16010420075 **Experiments No.: 3**

Aim :

1. Discuss what is CVSS and how security community refer it?
2. Write report on Exploit Db. Add scenario to explain how use of ExploitDb would be useful.

\

Resources : None

IMPLEMENTATION AND RESULTS:

1. What is CVSS? How does security community refer to it?

The Common Vulnerability Scoring System (CVSS) is a method for capturing a vulnerability's key characteristics and generating a numerical score that reflects its severity. The numerical score can then be converted to a qualitative representation (low, medium, high, and critical) to assist companies in correctly assessing and prioritizing their vulnerability management activities.

The CVSS SIG's aim is to continue to improve a published standard that is used by businesses all around the world.

For each vulnerability, the standard assigns a severity score from 0.0 (the lowest amount of risk) to 10.0 (the highest amount of risk), which enables you to more effectively prioritize remediation of vulnerabilities.

CVSS v3.0 Ratings	
Severity	**Base Score Range**
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

There are three types of metrics in the Common Vulnerability Scoring System: base, temporal, and environmental.

Base Metrics

Base metrics are divided into two groups: exploitability and impact.

Exploitability Metrics

Exploitability metrics refer to the characteristics of the piece of software or product that make it vulnerable.

- **Attack Vector —** Shows how a vulnerability may be exploited.
- **Attack Complexity —** Refers to how easy or difficult it is to exploit the discovered vulnerability.
- **Authentication —** Refers to the number of times that an attacker must authenticate to a target to exploit it.
- **User Interaction (UI) —** Refers to the requirement for a human user — other than the attacker — to participate in the successful compromise of the vulnerable component.
- **Privileges Required (PR) —** Refers to the level of privileges an attacker must possess before successfully exploiting the vulnerability.

Impact Metrics

Impact metrics deal with the worst-case scenario if the piece of software or product were to be attacked and the effects of a successfully exploited vulnerability.

- **Confidentiality —** Refers to the impact on the confidentiality of data processed by the system.
- **Integrity —** Refers to the impact on the integrity of the exploited system.
- **Availability —** Refers to the impact on the availability of the target system.

Temporal Metrics

Unlike the other CVSS metrics, the value of temporal metrics changes over the lifetime of the vulnerability. This is due to exploits being developed, disclosed, and automated along with mitigations and fixes being made available.

- **Exploitability —** Refers to the current state of exploitation techniques or automated exploitation code.
- **Remediation Level —** Refers to the number of mitigations and official fixes that are available to decrease the number of vulnerabilities.
- **Report Confidence —** Refers to the level of confidence in the existence of the vulnerability and the credibility of the technical details for the vulnerability.

Environmental Metrics

The environmental metrics use the base metrics score and the temporal metrics score to assess the severity of a vulnerability to the piece of software or product that is currently in development.

- **Collateral Damage Potential —** Measures the potential loss or impact on either physical asset — such as equipment, hardware, and users — or the financial impact, if the vulnerability is exploited.
- **Target Distribution —** Measures the proportion of vulnerable systems.
- **Impact Subscore Modifier —** Measures the specific security requirements for confidentiality, integrity, and availability. This metric enables you to customize the environmental score based upon your environment.

2. ExploitDB and its uses

Offensive Security, an information security training organisation that offers numerous information security certifications as well as high-end penetration testing services, maintains the Exploit Database. This is a non-profit project that Offensive Security offers as a public service.

The Exploit Database is a CVE-compliant archive of publicly available exploits and their accompanying susceptible software, created for penetration testers and vulnerability researchers. Our goal is to provide the most comprehensive collection of exploits possible, compiled from direct contributions, mailing lists, and other publicly available sources, and to present them in a freely accessible and easy-to-navigate database. The Exploit Database, rather than advisories, is a repository for exploits and proof-of-concepts, making it a useful resource for individuals who require actionable data right away.

History

- 2004
  In early 2004, str0ke, one of the leaders of the ex-hacking organisation milw0rm, which disbanded in 1998, created a public exploit archive. When 'FrSIRT' (another exploit source) became a private, paid source, he elected to do so (which in 2008 became VUPEN). Milw0rm developed a reputation as a reliable source of information over time since all exploits were thoroughly tested before being added. As the site's popularity expanded, so did the number of submissions and, with them, the amount of work made for str0ke.

- July 8, 2009
  Str0ke announced the site's closure. However, due to tremendous community demand, he publicly said the project will continue for the time being until he could hand it off to someone else the next day.

- November 4th, 2009

  Offensive Security was the group to whom he gave the database. On November 4th, 2009, this was made public (This was revealed ahead of time to help stop some of the rumors being spread).

- 16 Nov 2009

  On November 16th, 2009, the handover went live. On November 17th, 2009, the domain exploit-db.com was registered, and it is still active today. Milw0rm stopped accepting updates after September 2009, and eventually shuttered its doors for good in late 2010.

Uses

The Exploit Database (ExploitDB) is a repository of exploits for the aim of public security, and it describes what may be found there.

The ExploitDB is a great tool for identifying potential vulnerabilities in your network and keeping up with current attacks on other networks. This repository allows us to gain a better understanding of hacker tactics and improve our own security as a result.

One of the most often used public resources for official CVEs is ExploitDB. 69 percent of CVEs with initial announcements from the ExploitDB have a severity of HIGH or CRITICAL. Unlike many vendor- and project-specific sources (e.g., IBM X-Force), ExploitDB is crowdsourced.

Anyone who comes across new exploits for any product can post them to the ExploitDB website. They are not obligated, however, to report found exploits to product vendors or Mitre (so-called CVE Numbering Authorities, CNA), who are permitted to assign CVE IDs to vulnerabilities. In fact, in order to seek a new CVE ID, the exploit discoverer must compile the vulnerability information in the required format and engage with product suppliers and Mitre through a complicated process.

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Details on CVSS and ExploitDB along with it's uses were specified and concepts were grasped along.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- https://www.first.org/cvss/
- https://www.perforce.com/blog/kw/what-is-CVSS
- https://www.exploit-db.com/
- https://arxiv.org/pdf/2101.01431.pdf