Augmenting NVD Vulnerability Information for Classifying Attacker Privilages

Parsa Kootzari [1] Lianying Zhao [1] Taous Madi [2]

[1]Carleton University, School of Computer Science [2]Ericsson, Security Research Department, Canada

Attack Graph Generation

Modern cyberattacks exploit multiple vulnerabilities in sequence. Attack graphs analyze multi-step attacks by modeling the attacker's movement in the network as attack paths.

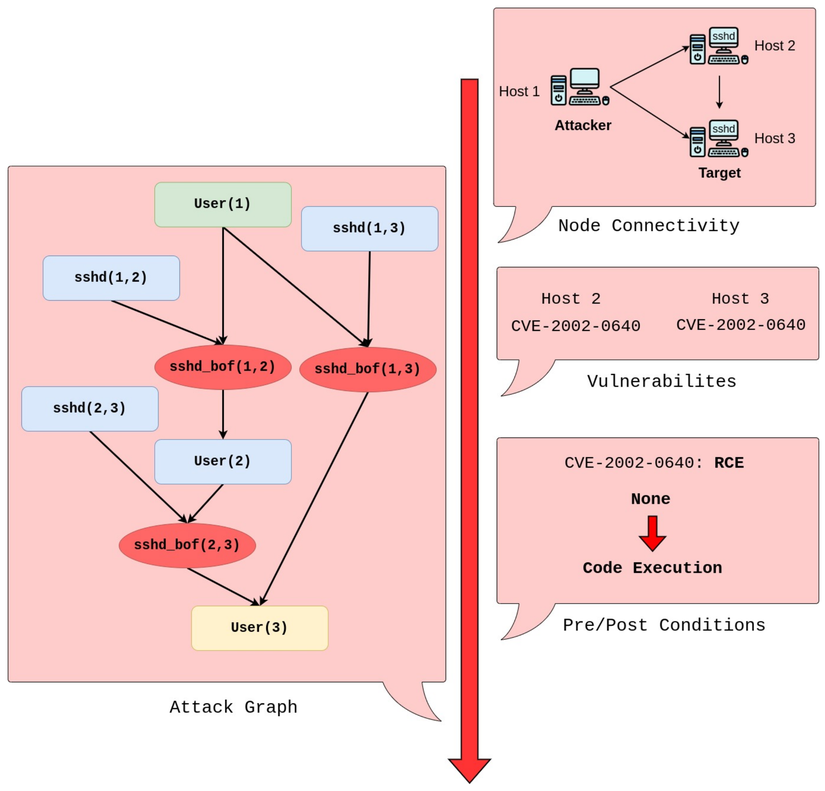

Figure 1. Attack Graph Generation Pipeline

Figure 1 shows the pipeline of creating the corresponding attack graph of a network with 3 hosts where the attack resides in *Host 1* and wants to reach *Host 3* by exploiting *CVE-2002-0640*.

National Vulnerability Database (NVD)

State-of-the-art CVE classification models rely on NVD as their source of information, However, previous studies show that there are occasional flaws in NVD records:

- Missing the key characteristics of the vulnerability (e.g. attack impact).
- Inconsistencies in CVSS metrics (vulnerabilities with similar descriptions are sometimes assigned differing scores).

Moreover, Product vendors are more reliable sources of CVE information. Because they know their product and its vulnerabilities, therefore, They can provide more accurate information than generalized CVE databases.

Low-Quality CVE Examples

Lack of Information

- CVE-2023-37214
- **NVD**:Heights Telecom ERO1xS-Pro Dual-Band FW version BZ_ERO1XP.025.
- **IBM X-Force Vulnerability Database**: Heights Telecom ERO1xS-Pro Dual-Band could allow a remote attacker to execute arbitrary commands on the system, caused by an unspecified flaw. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system.

Weakness instead of Consequence

- CVE-2022-35452
- **NVD**:OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b0b2c.
- **IBM X-Force Vulnerability Database**: Caryll OTFCC is vulnerable to a denial of service, caused by a heap-based buffer overflow in /release-x64/otfccdump+0x6b0b2c. By persuading a victim to open a specially crafted file, a remote attacker could exploit this vulnerability to cause the application to crash.

Technical Descriptions

- CVE-2022-2588
- **NVD**: It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0.
- **Red Hat CVE Database**: A use-after-free flaw was found in route4_change in the net/sched/cls_route.c filter implementation in the Linux kernel. This flaw allows a local user to crash the system and possibly lead to a local privilege escalation problem.

Methodology

Data Collection

We selected the following databases as the CVE information source and collected their reported CVEs from 2020 to 2024.

- National Vulnerability Database (NVD)
- IBM X-Force Vulnerability Database
- Aqua Vulnerability Database
- Red Hat CVE Database
- Ubuntu CVE Reports

Dataset

For evaluation purposes, we manually labeled the pre/postcondition of a set of randomly selected CVEs to serve as the ground truth. The pre/postcondition of each CVE are categorized into the following privilege levels:

- None
- User access level inside the application
- Code Execution Access within the context of the application
- User access level inside the operating system
- Root access level inside the operating system

Classification Model

We used LLMs, specifically GPT-4o, as our Classification model. The following information was fed to the LLM:

- Description of the task (categorizing pre/post condition)
- Definition of each privilege level
- CVE description + CVSS metrics

Then we asked the model to return the pre/postcondition class of the corresponding CVE.

Experiment Design and Results

We performed two experiments on the vulnerabilities with code execution and operating system postconditions and in each experiment we provided the following information as input to the model:

- CVE information from **NVD only**
- CVE information from **all the sources**

Precondition Classification

Class Name	Recall	F1 Score	F1 Score Change
None	**97.53**	95.66	↑7.21%
User Access on Application	77.93	84.01	↑22.48%
User Access on OS	84.02	87.05	↑13.25%
Overall F1 Score	-	91.36	**↑10.44%**

Table 1. The results for precondition classification and the percentage of improvement after augmenting CVE information.

Postcondition Classification

Class Name	Recall	F1 Score	F1 Score Change
Code Execution on Application	94.9	95.85	**↑18.75%**
User Access on OS	83.98	87.78	**↑26.99%**
Root Access on OS	90.42	89.47	**↑14.92%**
Overall F1 Score	-	91.1	**↑30.8%**

Table 2. The results for postcondition classification and the percentage of improvement after augmenting CVE information.

References

[1] Hao Guo, Sen Chen, Zhenchang Xing, Xiaohong Li, Yude Bai, and Jiamou Sun. Detecting and augmenting missing key aspects in vulnerability descriptions. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 31(3):1–27, 2022.

[2] Hailong Liu and Bo Li. Automated classification of attacker privileges based on deep neural network. In *Smart Computing and Communication: 4th International Conference, SmartCom 2019, Birmingham, UK, October 11–13, 2019, Proceedings 4*, pages 180–189. Springer, 2019.

[3] Sofonias Yitagesu, Zhenchang Xing, Xiaowang Zhang, Zhiyong Feng, Xiaohong Li, and Linyi Han. Extraction of phrase-based concepts in vulnerability descriptions through unsupervised labeling. *ACM Transactions on Software Engineering and Methodology*, 32(5):1–45, 2023.