What can a threat actor achieve by exploiting a specific vulnerability?

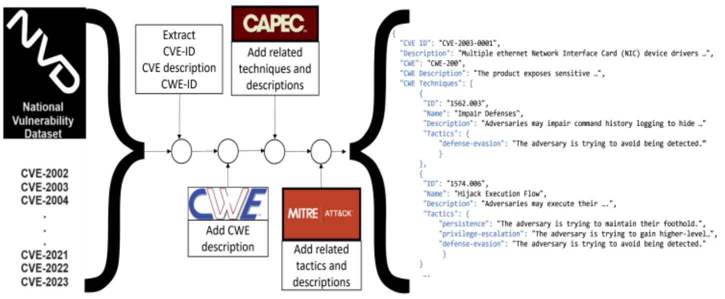
Stefano Simonetto - s.simonetto@utwente.nl

Why?

Prioritization based on what a threat actor can do

What?

Mapping security issues to TTPs


National Vulnerability Dataset
CVE-2002
CVE-2003
CVE-2004
.
.
.
CVE-2021
CVE-2022
CVE-2023
Extract CVE-ID CVE description CWE-ID
CWE
Add CWE description
CAPEC
Add related techniques and descriptions
MITRE ATT&CK
Add related tactics and descriptions

```
{
  "CVE ID": "CVE-2003-0001",
  "Description": "Multiple ethernet Network Interface Card (NIC) device drivers …",
  "CWE": "CWE-200",
  "CWE Description": "The product exposes sensitive …",
  "CWE Techniques": [
      {
       "ID": "1562.003",
       "Name": "Impair Defenses",
       "Description": "Adversaries may impair command history logging to hide …"
       "Tactics": {
           "defense-evasion": "The adversary is trying to avoid being detected."
           }
      },
      {
       "ID": "1574.006",
       "Name": "Hijack Execution Flow",
       "Description": "Adversaries may execute their ….",
       "Tactics": {
           "persistence": "The adversary is trying to maintain their foothold.",
           "privilege-escalation": "The adversary is trying to gain higher-level…",
           "defense-evasion": "The adversary is trying to avoid being detected."
            }
      }
       …
```

How?

Bridging gaps between frameworks

Approaches

Vulnerabilities to Weaknesses
CVE to CWEs

→ Unsupervised learning 😢

→ In-context learning to extract key terms from CVEs 😜

→ Mapping through fine-tuning LLM and exploiting CWE hierarchy 😜

🔗

Security issues to Weaknesses → Semi-supervised learning 😜

🔗

Weaknesses to Techniques → Graph Neural Networks (GNNs) 🤞
CWE to TTPs

UNIVERSITY OF TWENTE. | TUCCR Twente University Center for Cybersecurity Research

pervasive systems