

Risk Assessment & Treatment

CS668 Course Project
Instructor - Prof. Sandeep K. Shukla

- Sumit Patel
- Rishik Jain
- Ayush Mohod
- Chandra Sekhar
- Bharat Kumar
- Sandeep Vissa



Agenda

- Motivation & Goal
- Design
- Tech Stack and References
- Implementation
- Results
- Demo
- Future Scope



Motivation & Goal

- In the ever-evolving threat landscape, organisations need to be regular in their effort to monitor the risks to their systems and apply suitable controls to reduce the risk
- There are abundant resources available to security engineers to perform vulnerability assessment, threat modelling etc. However, they often lack coherence and hence difficult to integrate
- The goal of this project was to design an interactive risk assessment and treatment application using open source tools and repositories.
- We hope that this project can be extended to include other parameters as mentioned in the future possibilities section later.



Design

Asset Inventory & Vulnerability assessment

Create a central asset inventory by listing CPE names (NVD) and their corresponding impact values.
Use NVD CVEs to perform a vulnerability assessment in an online manner

List relevant threats

Using MITRE ATT&CK techniques, we map the obtained CVEs to techniques and list all relevant techniques for each asset

Design risk scoring application

Construct a database for threat-probability and use the impact values to calculate an initial score as well as each asset's contribution

List relevant mitigations

Using MITRE ATT&CK mitigations for each technique, list the relevant mitigations in decreasing order of impact

Update risk score by applying mitigations

By allowing user to select a subset of mitigations, update the risk score by reducing the likelihood of corresponding threats



Tech Stack, References and Work Distribution

	Modelling & Design	Frontend	Backend	Data Collection
Technology stack	Python, AQL	HTML, CSS, ReactJS	NodeJS, MongoDB	JSON, CSV
Members assigned	Rishik Jain	Chandra Sekhar, Bharat Kumar	Sumit Patel, Sandeep Vissa	Ayush, Rishik Jain

References -

1. [MITRE ATT&CK](#)
2. [NIST National Vulnerability Database](#)
3. [Linking Threat Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations for Cyber Hunting](#)

Implementation

- Creation of Technique-Vulnerability map
 - By querying BRON database
- Creation of Technique-Prob map
 - Using number of CVEs corresponding to each technique
- Creation of Technique-Mitigation map
 - By querying BRON database

```
{
  "Technique": "Credential Stuffing",
  "Vuln": "CVE-2022-37145"
},
{
  "Technique": "Modify Registry",
  "Vuln": "CVE-2021-38453"
},
{
  "Technique": "Screen Capture",
  "Vuln": "CVE-2021-32739"
},
{
  "Technique": "Clipboard Data",
  "Vuln": "CVE-2021-32739"
},
{
  "Technique": "Domain Accounts",
  "Probability": 0.0720241878021068
},
{
  "Technique": "Dylib Hijacking",
  "Probability": 0.02553584840256514
},
{
  "Technique": "Dynamic Linker Hijacking",
  "Probability": 0.9523947079553989
},
{
  "Tactic": "collection",
  "Technique": "Input Capture",
  "Mitigation": "Privileged Account Management",
  "MITRE_ID": "M1026"
},
{
  "Tactic": "collection",
  "Technique": "GUI Input Capture",
  "Mitigation": "User Training",
  "MITRE_ID": "M1017"
},
{
  "Tactic": "collection",
  "Technique": "Web Portal Capture",
  "Mitigation": "Execution Prevention",
  "MITRE_ID": "M1038"
},
}
```

Implementation

- saveAsset API to save asset to the database and perform vulnerability assessment using NIST API
- calcRiskScore API to compute initial risk score based on weighted mean
- assetMitigation to list the mitigations for the entire system and reduceScore to update the risk score based on selected mitigations

The screenshot displays a web browser with two tabs. The top tab shows the NIST CVE API endpoint: `https://services.nvd.nist.gov/rest/json/cves/2.0?cpeName=cpe:2.3:hcisco:7200_router:::.*.*.*.*`. The response is a JSON array of CVE objects, including details like ID, source identifier, published date, last modified date, vulnerability status, and descriptions. The bottom tab shows a local application interface with a POST request to `localhost:4000/api/calculateRiskScore`. The request body is a JSON object with an `assetId`. The response is a JSON object containing asset details, a risk score, and a list of mitigations. The mitigations list includes various security measures such as "Audit", "Execution Prevention", "Restrict File and Directory Permissions", "User Account Management", "Operating System Configuration", "Limit Access to Resource Over Network", "Network Segmentation", "Privileged Account Management", "Software Configuration", "Environment Variable Permissions", "Antivirus/Antimalware", "Network Protection on Endpoint", "File Network Isolation", "Network Intrusion Prevention", "SQL Injection", "Disable or Remove Feature or Program", "Code Signing", "Multi-factor Authentication", and "Update Software".

Results Achieved

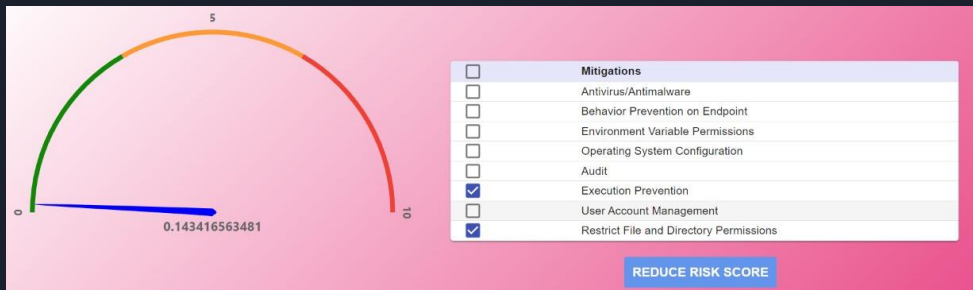
Asset	DeviceType	Impact	Vulnerabilities
cpe:2.3:a:novell:netmail:-:*:*:*:*:*	NW	1	CVE-2006-6424 ,CVE-2006-6425
cpe:2.3:a:apache:mod_perl:2.0.3:*:*:*:*	PC	1	CVE-2007-1349 ,CVE-2011-2767 CVE-2000-0268 ,CVE-2004-1111 ,CVE-2010-0578
cpe:2.3:h:cisco:7200_router:-:*:*:*:*	PC	1	

CALCULATE RISK SCORE



Assets	Contribution	Threats
cpe:2.3:h:cisco:7200_router:-:*:*:*:*	0	No threats Found
cpe:2.3:a:apache:mod_perl:2.0.3:*:*:*:*	9.09090909090909	<ul style="list-style-type: none">• Obfuscated Files or Information• Impair Command History Logging• Dynamic Linker Hijacking• Path Interception by PATH Environment Variable
cpe:2.3:a:novell:netmail:-:*:*:*:*	0	No threats Found

GO TO MITIGATIONS



REDUCE RISK SCORE

Demo



Future Possibilities

- Integration with OpenSCAP for each asset
 - List system hardening vulnerabilities using STIG files and tools (for eg. scc, oscap)
 - Map each vulnerability with CCI (Control Correlation Identifier)
 - Create a list of most relevant CCIs similar to MITRE mitigations
- Deploy an agent on organisational assets to perform real-time risk profiling
- Include information and human assets
 - Hard to assign impact scores and list weaknesses
- Include policy compliance as a parameter
 - Assign score based on whether policy is defined, understood and implemented

Thank You