A Dashboard for Cyber Situational Awareness and Decision Support in Network Security Management

Lukáš Matta and Martin Husák, Institute of Computer Science, Masaryk University, Brno, Czech Republic

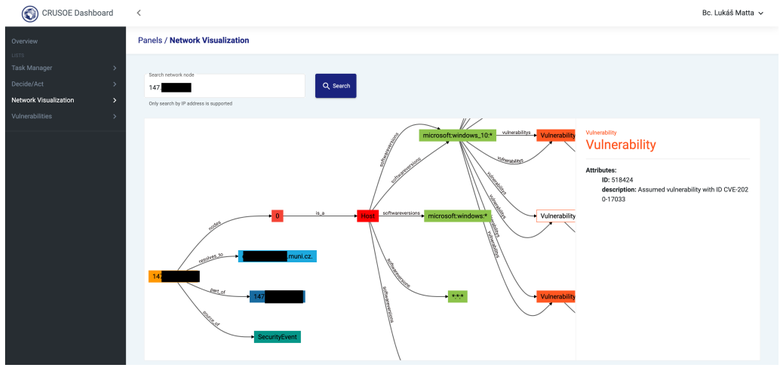
cm cm

Dashboard Overview

Our proposed dashboard is a web application based on Angular and connected to the database structured according to the CRUSOE data model. The data are structured as a graph and stored in Neo4j graph database. The database is filled by a number of tools, such as network and vulnerability scanners, network traffic analyzers, connectors to global vulnerability databases, and local asset management systems. Other information, such as location of critical devices, network partitioning, and contacts to devices' administrators can be filled in manually. The dashboard leverages the graph-based representation of the data and uses modern querying tool GraphQL.

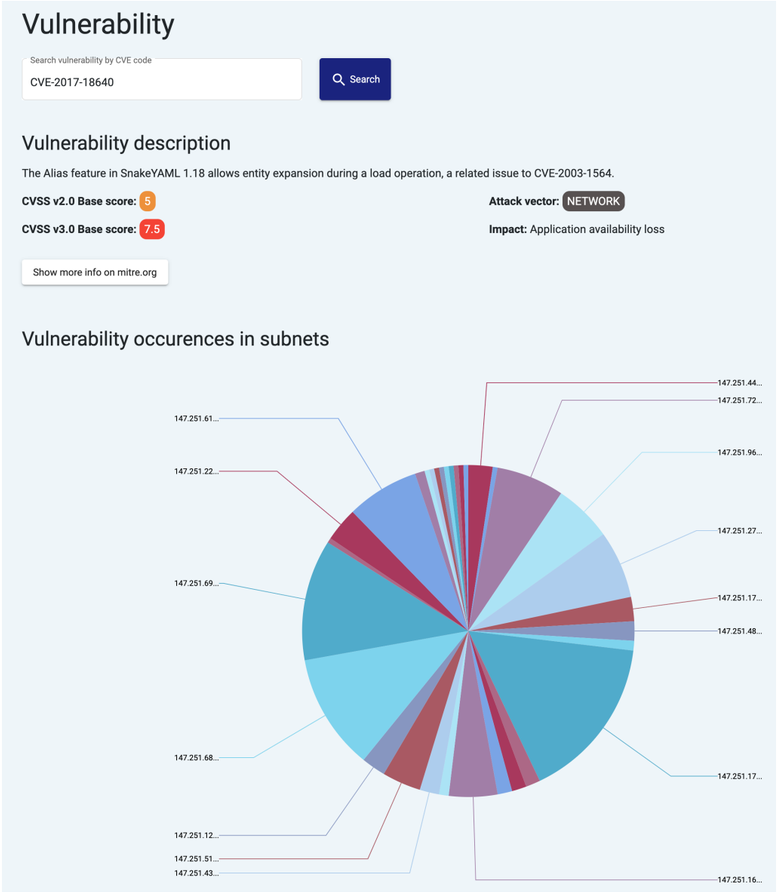
Network Visualization

The *Network Visualization* panel allows the user to traverse the graph database, in which the data collected by the provisioning tools and connectors are stored. The panel allows searching for a specific host in the network and displays its neighborhood in the graph database, i.e., various relations of the host with other entities, such as software versions, vulnerabilities, and contacts on administrators. The user may then traverse the nodes and open their neighbors. The detailed information on a selected node are displayed on the right.



Vulnerabilities

The *Vulnerabilities* panel allows the user to search for a particular vulnerability by its CVE identifier and displays its selected CVSS scores and a link to a full record at *cve.mitre.org*. Further, the panel shows the pie chart that shows the numbers of potentially vulnerable hosts in subnets of a monitored network.



Decide/Act

The *Decide/Act* panel serves as an interface to the decision support and mitigation management systems proposed in earlier work. The decision support system uses a predefined mapping of enterprise missions to their supporting host and services in the network and calculates the impact of exploiting vulnerabilities found on such components. The system finds the most resilient configuration, i.e., a configuration that fully supports the mission but has the lowest risk of mission disruption via exploitation. The mitigation management system provides a unified interface to various attack mitigation systems, such as firewalls and traffic redirection and filtering mechanisms. The panel presents the latest recommendations by the decision support systems and displays mitigation system controls that allow the user to enforce the recommended configuration, e.g., by allowing and disabling the hosts and service at firewall.