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

Lukáš Matta, Martin Husák
Institute of Computer Science, Masaryk University, Brno, Czech Republic
lukasmatta@mail.muni.cz, husakm@ics.muni.cz

Abstract—**This demo paper presents a dashboard for network security management, a web application that visualizes data gathered by various sensors in the network and allows the user to achieve cyber situational awareness and provides decision support in the incident handling process. The dashboard and its underlying database use modern graph-based approaches to data modelling, storing, and querying. The dashboard speeds up routine tasks in incident handling, such as getting a context of a situation and quickly assessing the spread and impact of vulnerabilities. The implementation uses modern graph-based approaches to data storage and visualization.**

I. Introduction

The operations of cybersecurity teams and operation centers (CSIRT/CERT/SOC), especially incident handling and vulnerability assessment, consist of many routine, yet complex tasks that are often time-consuming, cannot be automated, and poses a risk of a human error. However, with a proper tools and practices, it is possible to semi-automate such tasks and reduce the time required to resolve a task. For example, if an infected machine is detected in the network, a firewalls rule is applied to drop traffic of that machine until it is disinfected. Such a routine operation may turn disastrous if the blocked device is a part of critical infrastructure of an organization. In another example, if a new vulnerability is found, it is crucial to estimate the risk it poses to the protected network, e.g., by estimating the number of vulnerable devices and locate them. Such a task is laborious if done with no prior knowledge, but can be automated to some extent with proper tools and continuous network monitoring. A continuous perception of the cyber environment and comprehension of the processes in it is referred to as cyber situational awareness (CSA). If the cybersecurity experts achieve CSA, they can prevent human errors and speed up decision-making and security analyses.

A crucial task in supporting CSA of cybersecurity experts is providing them with the right information at the right time and presenting them in a comprehensible manner, e.g., in a structured overview or a visualization. Although there are complex tools supporting CSA, such as CyGraph [1], it is often too laborious to provide them with all the information they require. In our previous works, we proposed a more lightweight data model to store CSA-related information [2] and investigated the options of gathering complex information via common means [3]. We set up a database and a set of tools to gather the data. In this paper, we present a dashboard that we designed and implemented to use the data in network security operations.

978-3-903176-32-4 © 2021 IFIP

II. Dashboard Overview

Our proposed dashboard[1] is a web application based on Angular[2] and connected to the database structured according to the CRUSOE data model [2]. The data are structured as a graph and stored in Neo4j[3] 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[4]. The dashboard consists of a menu on the left and four panels that are displaying content. For example, the *Task Manager* panel displays the status of data collectors.

The *Network Visualization* panel, displayed in Figure 1, 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 [2]. The user may then traverse the nodes in the displayed graph and open their neighboring nodes. The detailed information on a selected node are displayed on the right. In the example, we can see a result of search and traversal; the user searched for an IP address and traversed the graphs to get the information on its operating system and its assumed vulnerability.

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 as displayed in Figure 2.

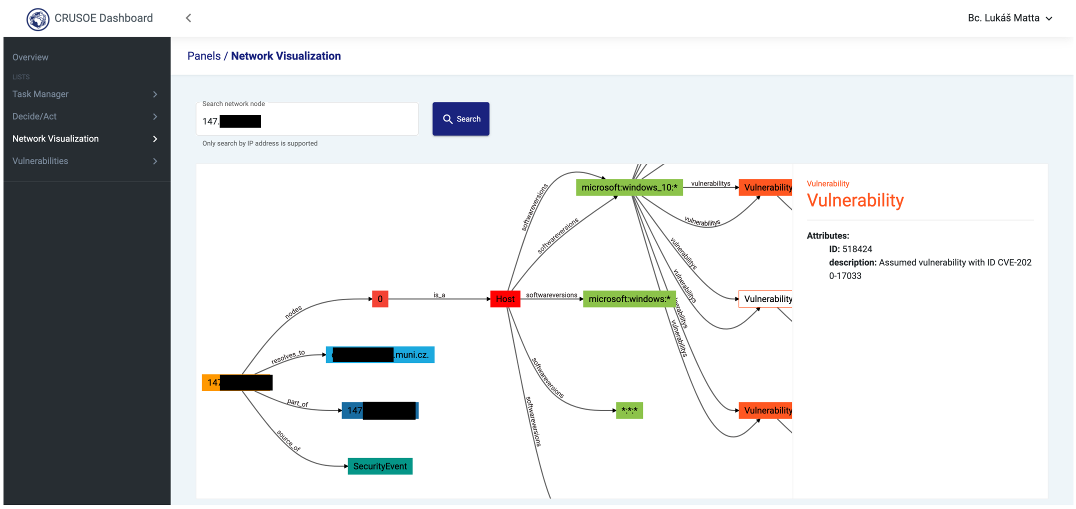
The *Decide/Act* panel serves as an interface to the decision support and mitigation management systems proposed in earlier work. The decision support system [4] uses a predefined

[1] Currently hosted at https://is.muni.cz/publication/1724716/?lang=en

[2] https://angular.io/

[3] https://neo4j.com/

[4] https://graphql.org/



Search network node

147.[redacted]

Only search by IP address is supported

Vulnerability

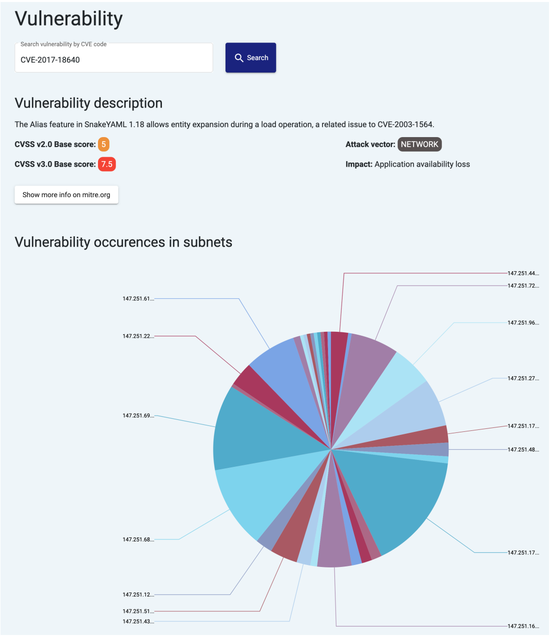
Vulnerability

Attributes:

ID: 518424

description: Assumed vulnerability with ID CVE-2020-17033

Fig. 1. The dashboard envelope and the panel for traversing the graph database.



Vulnerability

Search vulnerability by CVE code

CVE-2017-18640

Vulnerability description

The Alias feature in SnakeYAML 1.18 allows entity expansion during a load operation, a related issue to CVE-2003-1564.

CVSS v2.0 Base score: 5

CVSS v3.0 Base score: 7.5

Attack vector: NETWORK

Impact: Application availability loss

Vulnerability occurences in subnets

Fig. 2. Part of the visualization of the vulnerability assessment.

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.

III. Conclusion

In this demo paper, we presented a dashboard for cyber situational awareness and network security management that allows the user to query and traverse an underlying graph database that stored and interconnects various data on a computer network, including hosts and services in the network and their dependencies, fingerprints, vulnerabilities, and other information. The dashboard serves namely members of cybersecurity teams and operation centers and speeds up daily routines, such as getting a context to a particular hosts in the network and assessing a potential impact of a vulnerability.

In our future work, we are going to further extend the dashboard with other panels and visualization depending on the needs of cybersecurity teams and incident handlers, e.g., for a quick retrieval of data to resolve particular incident types. We are also going to evaluate and quantify the benefits of using the dashboard, e.g., via measuring the time spent on handling an incident and human errors caused by the lack of cyber situational awareness.

Acknowledgment

This research was supported by ERDF “CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence” (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

References

[1] S. Noel, E. Harley, K. H. Tam, M. Limiero, and M. Share, “CyGraph: Graph-Based Analytics and Visualization for Cybersecurity,” *Handbook of Statistics*, vol. 35, pp. 117–167, 2016.

[2] J. Komárková, M. Husák, M. Laštovička, and D. Tovarňák, “CRUSOE: Data Model for Cyber Situational Awareness,” in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 36:1–36:10.

[3] M. Laštovička, M. Husák, and L. Sadlek, “Network monitoring and enumerating vulnerabilities in large heterogeneous networks,” in *IEEE/IFIP Network Operations and Management Symposium*, 2020.

[4] M. Javorník, J. Komárková, L. Sadlek, and M. Husák, “Decision support for mission-centric network security management,” in *IEEE/IFIP Network Operations and Management Symposium*, 2020.