IMPETUS

Cyber Threat Detection and Response

Detects cyber vulnerabilities in IT Systems: raises alerts and suggests countermeasures if they arise

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

Information systems typically have so many vulnerabilities that it is not feasible to continuously monitor or manually manage all of them. Moreover, there are complex dependencies between vulnerabilities. For example: some vulnerabilities only become critical when some other vulnerability has been exploited (i.e., there has been a successful attack). This tool:

- Identifies exploited threats and potentially exploited vulnerabilities
- Prioritises actions to tackle the exploited threats and any exploitable vulnerabilities based on criticality of the situation

Without the tool:

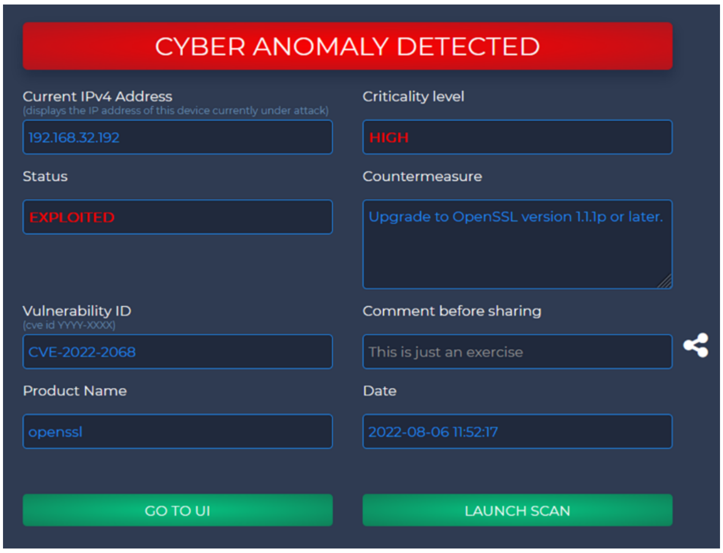
- Users' manual analyses of the system identify only a fraction of the vulnerabilities inherent within the system
- Users are not aware of how inter-linked vulnerabilities could expose the system
- Users are not aware when a vulnerability has been exploited

With the tool:

- Users can scan complex systems to identify all vulnerabilities and their relationships
- Users can monitor systems in real-time and receive an alert on the IMPETUS platform when a vulnerability has been exploited
- Countermeasures can be prioritized based on the criticality of the threat

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: (A) IT specialists responsible for protecting IT infrastructure against possible cyber-attacks (through analysis, monitoring and mitigation); (B) System operators and Security Centre operators who need notification of imminent threats/problematic situations.
- **What are the critical situations for deployment**: Regular: scans and analyses would be performed periodically. The tool is designed to provide up to date situational awareness.



CYBER ANOMALY DETECTED

Current IPv4 Address
(displays the IP address of this device currently under attack)
192.168.32.192

Criticality level
HIGH

Status
EXPLOITED

Countermeasure
Upgrade to OpenSSL version 1.1.1p or later.

Vulnerability ID
(cve id YYYY-XXXX)
CVE-2022-2068

Comment before sharing
This is just an exercise

Product Name
openssl

Date
2022-08-06 11:52:17

HOW DOES IT WORK?

The tool monitors network traffic data and correlates it with vulnerabilities discovered from a network scan. When an anomaly threatening a vulnerability on the system is detected, remedial actions are prioritised based on the severity of the threat. A cyber-security alert is generated, which is sent to the IMPETUS platform. Users can then take the prescribed action to mitigate the threat. For example, when a user tries to remotely access a machine several times, the tool will generate an alert to the IMPETUS platform suggesting the necessary countermeasures.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.