Contribution ID: **192** Type: **Paper presentation**

Controlled Evaluation of a Distributed Cyber Scan Engine: Architecture, Simulation and Threat-Aware Performance Metrics

Friday 19 September 2025 10:15 (15 minutes)

As the challenges with cyber threats increase, prompt detection of exposed assets is needed to minimize attack surfaces and maintain resilience in networked systems. This paper outlines the design and testing of a distributed scanning engine, developed as part of a national cybersecurity initiative on actively advancing active defense capabilities. The system is constructed using simple modular components to operate in lightweight hybrid infrastructures capable of scanning workloads across on-premises, edge, and cloud environments.
The scanning module contains configurable routines performed for detection of ports and services, OS fingerprinting, and profiling targets; enabling simple user access to contexts; configuring threat intelligence workflows; and data pipelines. Unlike many traditional scanning type tools, the engine has built in features for automation and ethical compliance which allows for it to be appropriate for reconnaissance (within legally defined operational limits) for real-time usage.
In total a full testing campaign was completed across controlled testing environments created to reproduce operational, threat network typologies, and adversarial conditions. The testing scenarios were framed around in understanding key performance indicators including the capability for reliability detection, loading responses, and adaptation to performance actions. Specific focus was placed on how the module would combine with technical vectors used by attackers and what might advance towards functionally operationally recency recently, that included autonomous threat hunting and mapping pre-attack reconnaissance.
The outcomes of this work include a validated prototype, and organized architecture to evaluate scan engines within operationally realistic environments. The work demonstrates immediate utility against a recognized gap and need for a systematic proactive reconnaissance tool, while managing performance, compliance, and flexibility for ease of use, setting the basis for more focused research and development of automated cyber resilient systems to facilitate responsive and adaptive cyber defense.

Authors: BALAN, Alexandra (”Ștefan cel Mare”University of Suceava); POTORAC, Alin (”Ștefan cel Mare” University of Suceava); BALAN, Doru (”Ștefan cel Mare”University of Suceava); TIMOFTE, Edi (”Ștefan cel Mare” University of Suceava); CROITORU, Ionut (”Ștefan cel Mare”University of Suceava)

Presenter: BALAN, Doru (”Ștefan cel Mare”University of Suceava)

Session Classification: Network Security

Track Classification: Networking in Education and Research