Contribution ID: **193** Type: **Paper presentation**

Enriching IP Scanning Results with Structured Threat Intelligence: Toward Actionable Reconnaissance in Cybersecurity Operations

Friday 19 September 2025 10:30 (15 minutes)

Reconnaissance data generated from scanning engines often provide limited context for actionable decisions to improve cyber defenses. The identification of open ports and exposed services provide a baseline mapping of the digital surface but only present real value in the form of contextualized threat intelligence. This paper puts forth a repeatable process that leverages raw scan results with vulnerability databases and adversarial tactics frameworks to move from passive reconnaissance to an active and threat-informed posture.

The proposed framework is built upon a previously vetted modular scanning engine and was designed to add data from open-source and government intelligence feeds (CVE, CISA KEV, and MITRE ATT&CK) to map the identified services by risk, known exploitability and observed attacker behavior. The enrichment pipeline was developed for semi-automated workstations to run offline data analysis and provide real-time actionable alerts.

The methodology was validated through targeted simulation exercises where the enriched outputs were compared to the raw scanned outputs on situational awareness, triage, and relevance to actual threat models. The results indicate highly improved decision-making quality and reduced analyst workload, particularly in high-noise environments.

By integrating threat intelligence into the scanning and analysis cycle, this work presents a tangible and repeatable approach for active defense. More importantly, it presents a clear need for risk contextualization for evidence-based decision-making in today's cyber threat landscape, while providing a repeatable framework for enhancing active reconnaissance systems within government and enterprises.

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, Alexandra (”Ștefan cel Mare”University of Suceava)

Session Classification: Network Security

Track Classification: Networking in Education and Research