**NetSpect - detecting cyber attacks in network traffic in real time**

SE-A-14

Shay Hahiashvili; shayha2@ac.sce.ac.il  
Maxim Subotin; maximsu@ac.sce.ac.il

Advisor: Ms. Alona Kutsyy

SCE - Shamoon College of Engineering, Be'er-Sheva

In the modern era, the dependence on technology and the internet is growing, and cyber attacks in the field of network communications pose serious risks to businesses and users, and can lead to data theft, service disruptions, and financial losses. As part of the project, we developed a real-time intrusion detection system (IDS) that monitors network traffic, detects attack patterns, and issues alerts. The hybrid system integrates cyber-attack detection algorithms with machine learning models to identify anomalies. It detects threats like port scanning, DoS, ARP spoofing, and DNS tunneling. Since existing datasets were ineffective for real-time detection, we manually collected optimal training data. Our system ensures high accuracy with minimal false alarms and features an intuitive and simple interface.

Keywords: arp spoofing, denial of service, dns tunneling, intrusion detection system, machine learning