Cluster : Systems & Software Security

Problem Statement title : Ransomware Behaviour Detection Engine

Description:

Develop a machine learning based DDoS mitigation system capable of distinguishing legitimate traffic spikes from malicious floods, providing adaptive and automated defenses against hyper volumetric attacks.

Exact Deliverables :

- Traffic shaping proxy implementation with fast BPF filters and auto signature generation.

- ML based anomaly detection module to differentiate real traffic surges from attacks.

- Simulation framework to test floods and chart mitigation latency vs. packet-rate peaks.

- Comparative benchmarking report vs. traditional appliance based solutions.

Milestones, Evolution Parameters:

- Phase 1: Implement baseline traffic anomaly detection**.**

- Phase 2: Add ML based classification for attack vs. legitimate surges.

- Phase 3: Deploy traffic shaping proxy and validate on large, simulated floods.

Additional Information:

- Students should focus on real-time mitigation capabilities.

- Lightweight ML models are preferred to ensure high speed packet filtering.

- Prototypes should be benchmarked against attack scales relevant to India’s internet exchanges.