SCE Tech Fest 25
Innovation Sustainability Community

Computer Science

Students: Shahar David and Roi Zur
Advisor: Dr. Guy Tel-Zur

SCE
SHAMOON COLLEGE OF ENGINEERING

Threat hunting - using YARA signatures to detect cyber attacks in the organization

Introduction:

This project enhances organizational cybersecurity by integrating email-specific YARA signatures with the Suricata IDS to detect and respond to email-based threats in real time. Leveraging curated YARA rules from the "Awesome YARA" database, the system continuously scans email traffic for malware patterns. Suricata's powerful detection engine ensures comprehensive analysis, enabling fast alerts and proactive defense against evolving threats.

Methods:

Proxmox – An Open-source virtualization platform used to deploy the test environment with isolated VMs, simulating a realistic enterprise network.

Kali Linux - Functions as the monitoring node. Runs Suricata for traffic inspection and a Python script for scanning files with YARA rules.

hMailServer - Acts as the internal mail server, enabling SMTP/POP3/IMAP communication between sender and receiver machines using realistic credentials.

Thunderbird -An open-source email client installed on Windows machines to simulate user interaction with emails, including opening attachments and viewing phishing content.

Python Detection Script - Parses Suricata's eve.json log file, which contains detailed, structured alerts and event data. The script extracts relevant files, scans them with YARA, logs the results, and supports modular extensions for future enhancements.

Test Scenario - Includes three Virtual machines: a security node and two Windows endpoints. Simulates email-based threats like phishing and malware to test detection effectiveness.

False Positive and False Negative Minimization – YARA rules are refined through controlled testing using both malicious and benign samples to ensure accurate detection while minimizing both false positives and false negatives.

Results:

- **Developed** a real-time email malware detection system using Suricata and YARA.
- **Built** a Proxmox-based testbed simulating enterprise communication between VMs.
- **Designed** a Python script to extract and scan files from Suricata logs with YARA.
- **Simulated** phishing and malware scenarios using hMailServer and Thunderbird.
- **Refined** YARA rules to minimize false positives through controlled testing.
- **Validated** threat detection on realistic user actions, including attachments and URLs.

Conclusions:

- System runs smoothly in a Proxmox-based virtual network.
- Suricata captures email traffic and file events reliably.
- Python script parses logs and scans files with YARA accurately.
- YARA rules refined to reduce false positives and improve precision.
- Simulated phishing and malware were successfully detected.
- Modular design supports easy debugging and future extensions.