Cybersecurity Lab Portfolio - Alen Guner

Lab: Phishing Email Investigation with Splunk & VirusTotal

Objective:

Investigate a suspicious phishing email, extract indicators of compromise (IOCs), and analyze the email content using Splunk and VirusTotal. Build an alerting workflow for similar future incidents.

Tools Used:

- Splunk (free version)
- VirusTotal
- Email logs or .eml files
- Python (optional for parsing)
- Dummy phishing email with malicious link and attachment

Steps Taken:

1. Email Log Review:
- Loaded a dummy email log dataset into Splunk.
- Identified suspicious subject lines, sender domains, and attachments.
- Filtered based on email headers, keywords like "password reset", and SPF/DKIM failures.

2. IOC Extraction:
- Extracted sender IP, domain, and URLs from the body and headers.
- Found attached file hash (SHA256) and URLs.

3. Threat Intelligence Enrichment:
- Submitted the file hash and URLs to VirusTotal.
- Correlated results with detection ratios and threat labels.

4. Alert Creation:
- Created a Splunk alert to trigger on similar email patterns (e.g., same domain, hash, or header anomalies).
- Documented response playbook for SOC escalation.

5. Reporting:
- Built a phishing triage report including timeline, evidence, and IOC summary.
- Stored logs and alerts for audit reference.

Outcome / What I Learned:

- Identified malicious phishing email with a known malware attachment.
- Successfully parsed and correlated IOCs with threat intelligence tools.
- Built a repeatable process for phishing investigation and detection using Splunk.
- Developed workflow documentation for junior analysts.

Cybersecurity Lab Portfolio - Alen Guner

Keywords:

Phishing, Email Security, Splunk, VirusTotal, IOCs, Threat Intelligence, SOC, Incident Response