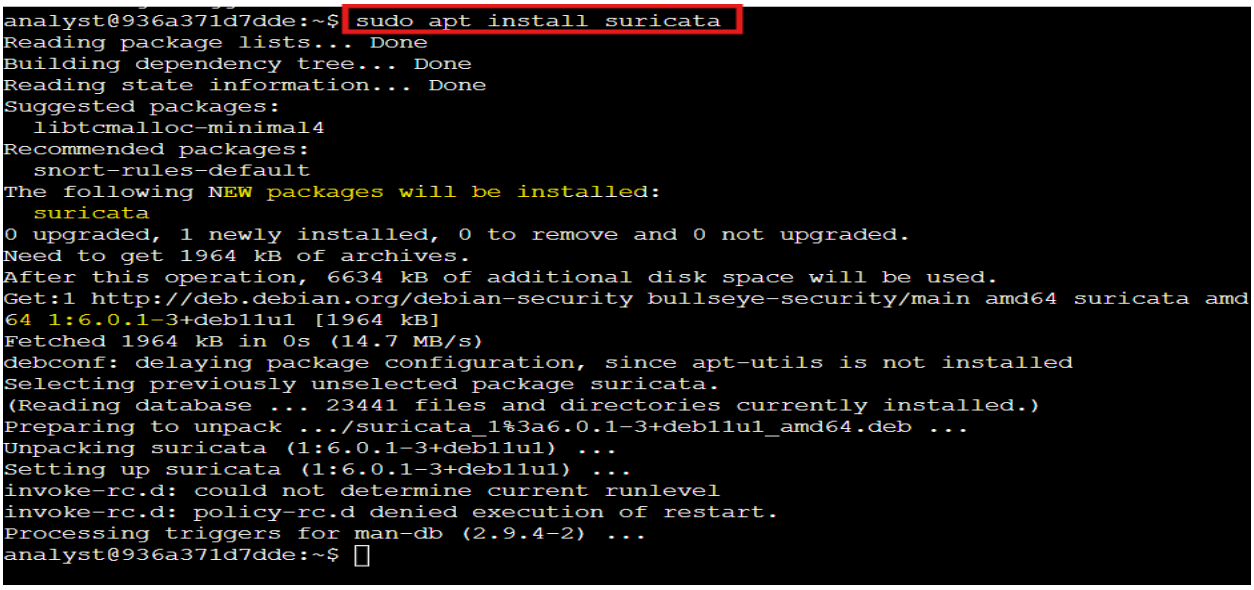
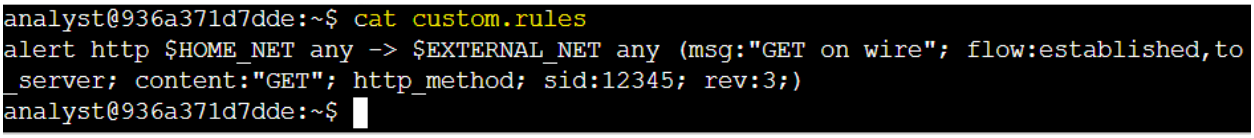
Reviewing Suricata Alert Logs

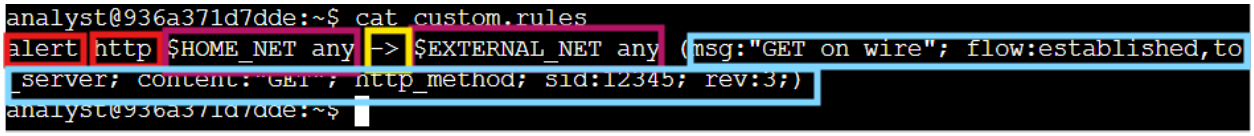
First, I install Suricata using the APT package mgr:



Next, I'll explore the custom rules file from the directory:



This shows me the action type (alert), the protocol (http), src ($Home_Net) & destination ($External_Net) IP, the direction of the traffic (->), as well as the rule options etc:



Based on the "content: GET" rule, this tells me whenever Suricata observes the text "GET" as the HTTP method, an alert will be triggered.

Capability	IDS	IPS	EDR
Detects malicious activity	✓	✓	✓
Prevents intrusions	N/A	✓	✓
Logs activity	✓	✓	✓
Generates alerts	✓	✓	✓
Performs behavioral analysis	N/A	N/A	✓

4 types of detection categories:

1. **A true positive** is an alert that correctly detects the presence of an attack.
2. **A true negative** is a state where there is no detection of malicious activity. This is when no malicious activity exists and no alert is triggered.
3. **A false positive** is an alert that incorrectly detects the presence of a threat. This is when an IDS identifies an activity as malicious, but it isn't. False positives are an inconvenience for security teams because they spend time and resources investigating an illegitimate alert.
4. **A false negative** is a state where the presence of a threat is not detected. This is when malicious activity happens but an IDS fails to detect it. False negatives are dangerous because security teams are left unaware of legitimate attacks that they can be vulnerable to.