Project Category: IDS/IPS, Simulated Attack Testing, SOC, Security Monitoring

Project Name	IDS & IPS Implementation of Security Onion OS
Client Name	One of the University of Bangladesh
Industry	Education
Challenges (Work)	Clients are reaching out to us because they're setting up a cybersecurity lab for their university students and need to implement an Intrusion Detection and Prevention System with Logging with ElasticSearch and Kibana. They're willing to do it for explanation and demonstration purposes.
Type	Network Security, Internet Security, Virtualization, System & Network Administration
Project Duration	1 Month
Outcome	Our team has completed one part that is to implement IDS/IPS on security onion and setup elastic search and kibana. But we're struggling with the other part, which is to check whether someone tries to attack on this network then IDS/IPS sends alerts to logging softwares or not. But after lots of research we finally found a way. There is a problem with the IDS/IPS configuration file.