Ovaj tjedan sam se bavio istraživanjem kako implmentirati IDS u honeypot

prošao sam ugrubo ove materijale
https://www.fer.unizg.hr/_download/repository/rppiotprakticnimaterijali.pdf

neki od članaka koji su mi se činili korisni su navedeni
https://arxiv.org/ftp/arxiv/papers/0906/0906.5031.pdf

tu sam pročitao da postoje 2 načina kako implementirati IDS. Misuse detection ili anomaly detection. Misuse detection traži kroz bazu poznatih napada i malicioznih paketa i sprječava ih dok se kod Anomaly detectiona definira pravilno i očekivano ponašanje i onda se gleda na svako ponasanje koje odstupa od toga i preusmjerava ga na honeypot. Za potrebe našeg honeypota mi se čini bolje drugo ponašanje.

https://reader.elsevier.com/reader/sd/pii/S2590123022002468?token=3DD7F05F1E52106351ED1AF4EECEF73B13C7EC07E13C9B7E2AEF8AB1CFEBF08EB5F46D7143BA29FA13BBF285F2F2C894&originRegion=eu-west-1&originCreation=20230319160710

https://www.hhs.gov/sites/default/files/using-honeypots-network-intrusion-detection.pdf

Kao rijesenje potencionalno instalirati neki software kao suricata i postaviti ga na jedan čvor u mreži koji provjerava legitimnost paketa koji dolaze u sustav i ovisno o tome preusmjeriti na honeypot

https://security.stackexchange.com/questions/42553/suricata-ips-rules-for-honeypot

https://github.com/Nirusu/how-to-setup-a-honeypot