

**Домашнее задание № 20**

***Основные виды СЗИ***

***часть 2 : Dos/DDos, IDS/IPS, Windows Defender***

**1. Установка и тестирование Suricata IDS**

* Установить Suricata
* Добавить правило FIN or SIN сканирования в suricata
* Перезагрузить suricata
* Запустить kali linux и просканировать виртуалку suricata
* Предоставить скрины и лог файла suricata при сканировании

Ссылки на дополнительные ресурсы

* [Fail to ban - анализ лога и блокировка](https://github.com/fail2ban/fail2ban)
* [Hydra - инструмент подбора паролей, bruteforce](https://github.com/vanhauser-thc/thc-hydra)
* [Suricata - сетевая IDS система](http://suricata.io)
* [Suricata- docs, документация](https://docs.suricata.io/en/suricata-6.0.2/)
* [Windows Defender - что это и как с ним работать](https://journal.tinkoff.ru/windows-defender/#two)
* [Passwords and Users database](https://github.com/danielmiessler/SecLists/blob/master/Usernames/xato-net-10-million-usernames-dup.txt)