

**Домашнее задание № 19**

***Основные виды СЗИ***

***часть 1 : AV, NGFW, PAM, DLP, XDR, EDR, MDR***

**1. Установить антивирус ClamAV**

* Также установить графическую оболочку
* Просканировать любую директорию

**2. Установить YARA**

* Создать текстовый файл и вычислить его hash
* Написать правило для детектирования данного файла

**\*3. Установить WAF (nginx + Modsecurity)**

* установить и протестировать запрет тестового запроса

Ссылки на дополнительные ресурсы

* [Настройка Jump Server - Bastion](https://habr.com/ru/companies/cloud4y/articles/530516/)
* [MDR архитектура от Kaspersky](https://support.kaspersky.com/MDR/ru-RU/196548.html)
* [YARA installation and docs](https://yara.readthedocs.io/en/latest/gettingstarted.html#)
* YARA команды проверки
* [Nginx + Modsecurity WAF](https://opsshield.com/help/cpguard/install-modsecurity-with-nginx-on-debian-ubuntu/)
* [Smirnov nginx + modsecurity github](https://github.com/sm1lexops/Profile_challenges?tab=readme-ov-file#5-%D0%BF%D1%80%D0%B5%D0%B4%D0%BB%D0%BE%D0%B6%D0%B8%D1%82%D0%B5-%D1%81%D1%85%D0%B5%D0%BC%D1%83-%D0%B8%D0%BD%D1%82%D0%B5%D0%B3%D1%80%D0%B0%D1%86%D0%B8%D0%B8-web-application-firewall-waf-%D0%B2-%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B5-%D0%BD%D0%B0%D0%BF%D0%B8%D1%88%D0%B8%D1%82%D0%B5-%D0%BA%D0%BE%D0%BD%D1%84%D0%B8%D0%B3%D1%83%D1%80%D0%B0%D1%86%D0%B8%D1%8E-%D0%B4%D0%BB%D1%8F-%D0%B2%D0%BD%D0%B5%D0%B4%D1%80%D0%B5%D0%BD%D0%B8%D1%8F-waf-%D0%BD%D0%B0%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80-modsecurity-%D0%B2-nginx-%D0%BD%D0%B0%D0%BF%D0%B8%D1%88%D0%B8%D1%82%D0%B5-%D0%BA%D0%BE%D0%BD%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D1%8B%D0%B5-%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80%D1%8B-%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BB-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%B5-%D0%B2%D1%8B-%D0%B1%D1%8B-%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B8%D0%BB%D0%B8-%D0%B2-waf-%D0%BD%D0%B0%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80-%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D0%B0%D1%86%D0%B8%D1%8F-sql-%D0%B8%D0%BD%D1%8A%D0%B5%D0%BA%D1%86%D0%B8%D0%B9-xss-%D0%B0%D1%82%D0%B0%D0%BA-%D0%B1%D0%BB%D0%BE%D0%BA%D0%B8%D1%80%D0%BE%D0%B2%D0%BA%D0%B0-%D0%B7%D0%B0%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85-%D0%BF%D0%B0%D1%82%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B2)
* [NGFW free course](https://www.youtube.com/watch?v=uOMiC1-iwIc&list=PLqio-3dnMW5_2cStMfIezwcAzzDCjX86C)