Распознавание подозрительного трафика

Материалы по теме можно посмотреть, например, на ресурсах:

Finding Suspicious Traffic in Protocol Hierarchy
https://www.youtube.com/watch?v=OwQmwbD1uIs

Wireshark and Recognizing Exploits
https://www.youtube.com/watch?v=7iguG7va4l8

Данная тема является элективной и, в явном виде, в программу лабораторных работ этого курса не включена.
Однако, тема достаточно актуальна, и может быть реализована в виде самостоятельного исследования.
Вы можете включать результаты экспериментов по этой теме, также, в ваш отчет по лабораторным работам, это будет только приветствоваться.

ТРЕБОВАНИЯ К ОТЧЕТАМ

По результатам выполнения лабораторных работ необходимо составлять отчет. Рекомендуется составлять отчет параллельно с выполнением заданий лабораторных работ, не оставляя этот процесс на потом. Отчет должен быть оформлен с титульным листом с названием университета, института и высшей школы. На титульном листе указывается ф.и.о. студента исполнителя работы, номер студенческой группы и ф.и.о. преподавателя.

В отчете приводится информация, удостоверяющая выполнение студентом заданий лабораторных работ: скриншоты с результатами исполнения сценариев, команд и программ, командных файлов, дампы памяти и пакетов, составленные вами скрипты (*BASH* или др.), ответы на поставленные в заданиях вопросы и т.д.

Результаты выполнения каждого из заданий должны предваряться в отчете фрагментом текста, формулирующим само задание (фрагменты копируются прямо из текста заданий).

Защита лабораторных работ происходит по предъявлению оформленного отчета и сопровождается демонстрацией исполнения программ и командных файлов, а также ответами на вопросы преподавателя.

Отчет можно создавать под *ОС Linux*, например, с помощью приложения *LibreOffice Writer* , сохраняя в *Home* каталоге вашего рабочего компьютера. Либо можете использовать офисные средства от MS Windows или MacOS.