**Отчет по лабораторной работе «HTTPS Decrypt»**

|  |  |
| --- | --- |
| 1. **Скриншот расшифрованного трафика** |  |
| 1. **Поле для пояснений как делали работу** | Для захвата трафика запускаем утилиту tcpdump, указывая флагом -i интерфейс, который нужно прослушивать, флагом -w указываем, в какой файл сохранять результат работы.  Команда: “sudo tcpdump -i enp0s3 -w dump.pcap”    Для скачивания целевого PDF-файла используем утилиту curl.  Флаг -O предназначен для скачивания файла под оригинальным названием.  Флаг -A предназначен для изменения User-Agent, чтобы целевой хост не догадался, что мы используем curl, и не запретил обращения к ресурсу. В данном случае заменяем на стандартный User-Agent для Google Chrome.  Команда вида SSLKEYLOGFILE=File\_Path создаёт локальную переменную окружения, которая означает, куда будут сохраняться ключи наших соединений.  Полная команда для curl:  «SSLKEYLOGFILE=/home/roman/HTTPS\_Decrypt/keys curl -OA "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0" https://rt-solar.ru/upload/iblock/05b/DDOS\_ataki-za-tri-kvartala-2021-goda.pdf»    После завершения скачивания останавливаем прослушку интерфейса.  Настаиваем Wireshark, указывая ему, где икать файл с ключами для TLS-соединений    Загружаем полученный дамп в wireshark и видим, например, расшифрованное тело GET-запроса HTTP    Теперь надо бы восстановить файл.  Для этого можно перейти в тело HTTP-ответа, там скопировать содержимое, вставить в новый файл это содержимое, и открыть его как PDF, но wireshark также позволяет восстановить файлы более простым способом.  Нажимаем Файл -> Экспорт -> HTTP, и wireshark предлагает скачать восстановленные файлы    Сохранение файла    Папка с восстановленным PDF    Вы прекрасны! |