Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

Отчет по лабораторной работе №3
по курсу «СиМОИБ»
на тему: «Наблюдение за стеком TCP/IP»

Выполнил студент группы 421702: Бруцкий Д.С.

Проверил: Захаров В.В.

МИНСК
2016

Задание для самостоятельной работы

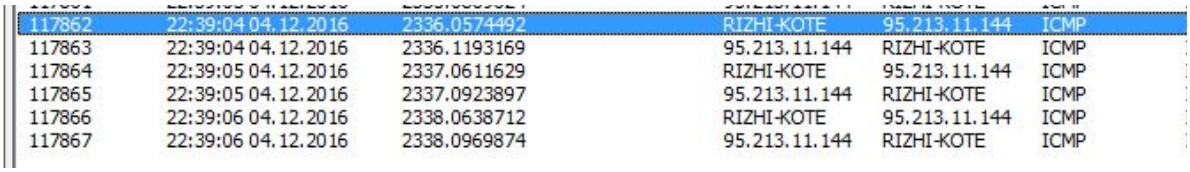
- Установите программы, необходимые для перехвата сетевого трафика.
- Изучите различные параметры работы программ для перехвата сетевого трафика.
- Выполните анализ трафика (с различными параметрами детализации):
  - ping запроса,
  - HTTP трафика при загрузке любого веб-ресурса,
  - аутентификацию в веб-ресурсе, на котором не настроен HTTPS,
  - SSH, SCP трафика,
  - FTP трафика и т. д.
- Определите, к каким портам и адресам были выполнены обращения.
- Используя дополнительную литературу, расшифруйте содержание перехваченных пакетов.

Ход работы:

Для перехвата и анализа сетевого трафика использовалась программа network monitor

Ping запрос:

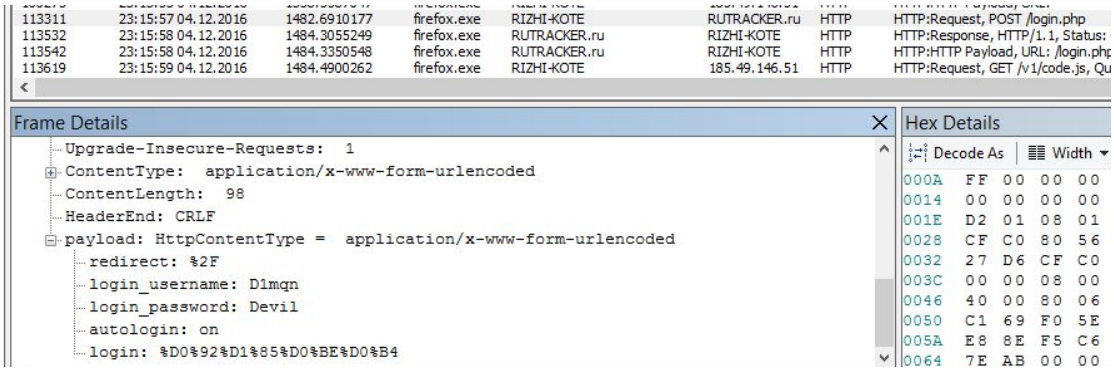
При вызове команды ping она отправляет ICMP пакет по указанному адресу и дожидается ответа, затем отправляет еще 3 раза.



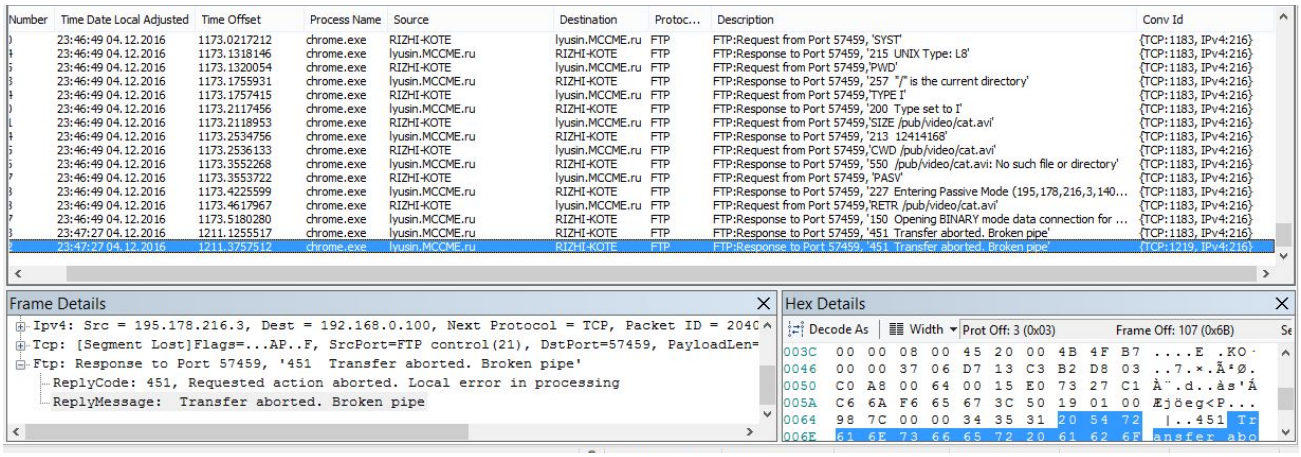
117862	22:39:04 04.12.2016	2336.0574492	RIZHI-KOTE	95.213.11.144	ICMP
117863	22:39:04 04.12.2016	2336.1193169	95.213.11.144	RIZHI-KOTE	ICMP
117864	22:39:05 04.12.2016	2337.0611629	RIZHI-KOTE	95.213.11.144	ICMP
117865	22:39:05 04.12.2016	2337.0923897	95.213.11.144	RIZHI-KOTE	ICMP
117866	22:39:06 04.12.2016	2338.0638712	RIZHI-KOTE	95.213.11.144	ICMP
117867	22:39:06 04.12.2016	2338.0969874	95.213.11.144	RIZHI-KOTE	ICMP

Аутентификация в веб-ресурсе, на котором не настроен HTTPS.

При аутентификации на сайте без HTTPS можно из перехваченного пакета достать логин пароль, переданные на сайт. Были перехвачены пакеты с сайта rutracker.org . На снимке ниже приведен перехваченный пакет, содержащий передаваемую информацию пользователя.



Анализ FTP трафика.



Вывод:

В данной работе я наблюдал за сетевым трафиком проходящим через сетевую карту. А именно за стеком протоколов TCP/IP. Исследовав пакеты протоколов UDP, TCP, FTP замечено что все они используют протокол IP на сетевом уровне. В ходе проведения работы было замечено, что наблюдать за чужим трафиком очень просто. У большинства протоков не предусмотрено никакой аутентификации, у FTP есть возможность аутентифицировать пользователя с помощью пароля, но передача этих данных ничем не защищена.