УДК 621.396

ВОССТАНОВЛЕНИЕ ПЕРЕДАВАЕМЫХ СООБЩЕНИЙ НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Правило В.В., Белоха Д.К.
Институт телекоммуникационных систем КПИ им. Игоря Сикорского, Украина
E-mail: valeriy_pravilo@ukr.net, belohadk97@gmail.com

Restoring transfer messages based on network traffic analysis

In this paper, have been described the possibilities of restoring transfer messages based on network traffic analysis. Also, have researched the problems of the transmission protocols, the variety of possibilities saving them and creation of the automation system of providing information of the data.

На сегодняшний день существует задача восстановления и анализа информации, передаваемой в сети. Восстановление и обработку инорфмации можно проводить на разных уровнях. Чтобы собрать данные, нужно понимать протоколы передачи этих данных, как они работают и как с ними работать.

Протокол передачи данных − набор соглашений интерфейса логического уровня, которые определяют обмен данными между различными программами. Эти соглашения задают единообразный способ передачи сообщений и обработки ошибок при взаимодействии программного обеспечения разнесённой в пространстве аппаратуры, соединённой тем или иным интерфейсом.

Стек протоколов TCP/IP содержит 4 уровня:

- канальный уровень,
- сетевой уровень,
- транспортный уровень,
- прикладной уровень.

Наиболее известные протоколы, используемые в сети Интернет:

- HTTP (Hyper Text Transfer Protocol) − это протокол передачи гипертекста;
- FTP (File Transfer Protocol) − это протокол передачи файлов со специального файлового сервера на компьютер пользовател;
- POP3 (Post Office Protocol) − это стандартный протокол почтового соединени;
- SMTP (Simple Mail Transfer Protocol) − протокол, который задает набор правил для передачи почт;
- TELNET − это протокол удаленного доступа. TELNET дает возможность абоненту работать на любой ЭВМ находящейся с ним в одной сети, как на своей собственной, то есть запускать программы, менять режим работы.

При передаче данных от прикладного уровня к транспортному, затем через уровень сетевой взаимосвязи, каждый из протоколов, по которым проходят данные, выполняет свою личную логику для этих данных и конечный результат этой логики прикрепляет к началу заголовка.

На рис.1 представлены результаты обработки данных и формирования таких заголовков пакета в сети TCP\IP.

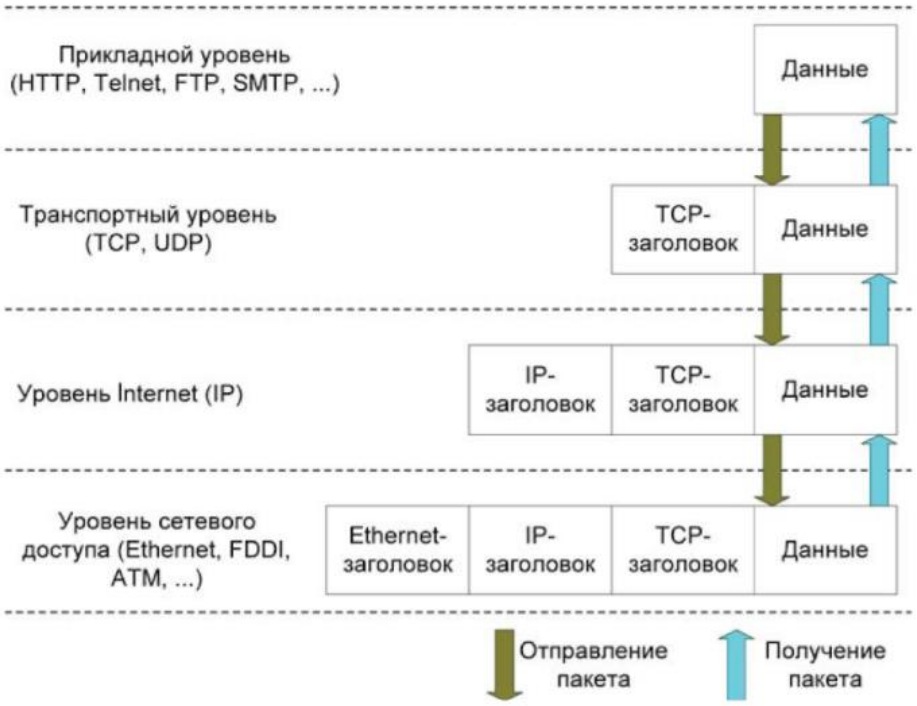

Рис. 1. Процесс обработки данных и формирования заголовков пакета в сети TCP\IP.

На приемной стороне эти заголовки удаляются в ходе того, как выполняются и проходят некоторые из этих протоколов.

Таким образом, получаем легкость и гибкость в настройке протоколов, ведь ни один из них не должен знать и не знает о существовании другого.

Рассмотрим методы перехвата данных сети:

1. Програмное обеспечение Wireshark,
2. Командная строка dumpcap,
3. TShark,
4. Использование устаревшего центра передачи,
5. Настройка порта на передатчик,
6. Использование сетевого контакта,
7. «Хакинг» ARP протокола.

Кроме того, необходимо сохранять принятые данные на диск. В этом случае наиболее целесообразно воспользоваться командной утилитой dumcap. Это решение, которое не имеет пользовательского интерфейса, что является

несомненым плюсом, в условиях того, что обрабатывается трафик сети, иначе обрабатывающие устройство могло бы не выдерживать то количество трафика, которое проходит через сеть. Решение поддерживает сбор всех типов данных. Фильтрование данных предлагается проводить на следующих этапах.

После сбора данных понадобиться их анализ и обработка. Есть несколько различных способов этой прорцедуры. Но на данный момент рассмотривается способ обработки данных с помощью NetworkMiner.

NetworkMiner – программное обеспечение, с помощью которого возможно получить доступ к файлам данных, которые были приняты ранее. При чем не важно – были эти данные в открытом или закрытом доступе. С помощью этой программы возможно извлечь ифнормацию из принятых данных, как показано на рис.2.

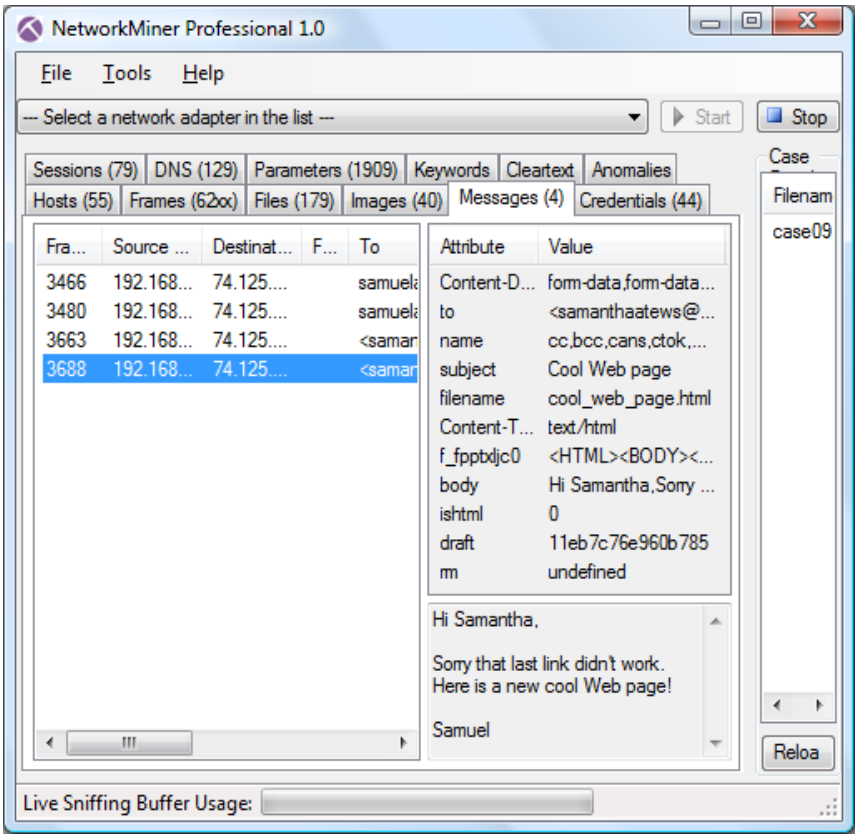

Рис. 2. Пример работы программы NetworkMiner по извлечению информации.

Как результат, при желании, найдя нужный кусок информации, можно с ним работать: удалять, изменять и т.д.

Литература

1. Erik Hjelmvik, http://netres.ec/?b=113EA66, 11 March 2011.
2. V. Shaniagin, Information Security, pp 362 – 365, Litres, 2017.
3. Erik Hjelmvik., http://netres.ec/?b=11100F0, 15 January 2011.