Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Установление обстоятельств работы пиринговых приложений в локальной сети

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 090102.65 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Гроля Егора Андреевича

Научный руководитель
доцент, к.ю.н. А.В. Гортинский

Заведующий кафедрой
профессор, к.ф.-м.н. В.Н. Салий

Саратов 2016

ВВЕДЕНИЕ

В данной работе рассматриваются основные способы установления обстоятельств работы p2p-приложений. Основной упор сделан на те приложения, которые работают по протоколам DC, Edonkey, Bittrorent.

Данная проблема является в данный момент актуальной, т.к. нет известных коммерческих и некоммерческих программ для решения этой задачи и данные протоколы на сегодняшний день является одними из наиболее популярных для передачи информации в пиринговых сетях. Эти протоколы используют довольно большое число p2p-приложений для передачи файлов: DC++, NMDC, EiskaltDC++, LinuxDC++, ApexDC++, eMule, iMule, mlDonkey, Shareaza, Lphunt, BitTorrent, Mtorrent, BitComet, RTorrent и много других.

Конечной целью данной дипломной работы является реализация программного комплекса для решения данной задачи, которая будет полезна для проведения криминалистических работ, связанных с определением факта поиска файлов с определенным именем и загруженных файлов пользователями, использующие популярные на данный момент файлообменные сети, которые организовывают передачу файлов по протоколам DC, Edonkey, BitTorrent. То есть, наиболее подробно этой программой должны быть проанализированы следующие обстоятельства работы пиринговых приложений:

1. вход на сервер
2. поиск файлов
3. скачивание файла
4. соединения с клиентами (рукопожатия)
5. получение хэш-кода (TTH, SHA, MD5) скачанного файла

Данная программа должна будет уметь работать в режиме пассивного перехвата пакетов в локальной сети для анализа описанных выше действий определенного узла этой сети.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе дипломной работы рассмотрены наиболее эффективные способы обнаружения p2p-трафика в локальной сети. В этой главе рассматривается как перехват трафика, типичный для p2p-приложений, так и те способы, которые позволяют установить только сам факт наличия p2p трафика.

Во второй, третьей и четвертой главе описаны протоколы соответственно: DirectConnect, Edonkey, BitTorrent и как с помощью этого описания можно извлечь ту или иную информацию о действиях пользователей в локальной сети. Каждая из этих глав содержит подразделы, описывающие общую структуру команд соответствующего протокола, непосредственно, сами команды, которые являются наиболее значимыми с точки зрения установления обстоятельств их работы и, также, разобран порядок взаимодействия элементов сети протокола. Описанная информация в этих главах представляет собой результат анализа официальных спецификаций данных протоколов.

В пятой главе описана конкретная реализация для решения поставленной выше задачи. Дана детальная информация об интерфейсе программы, её технических возможностей, а так же кратко описано как пользователь может, используя данную программу, запустить анализ поведения определенного узла локальной сети, сохранить детальный отчет в файл, проводить более глубокий ручной анализ перехваченных пакетов.

В шестой главе рассмотрены примеры работы реализованного программного комплекса. Описан краткий анализ разбора наиболее типичных перехваченных пакетов и представлены снимки экрана работающей программы. Так же в этой главе приведено сравнение данной реализации с другими подобными анализаторами трафика и показано какие имеются преимущества перед ними.

ЗАКЛЮЧЕНИЕ

В работе были рассмотрены методы установления обстоятельств работы p2p-приложений, работающих по протоколам DC, BitTorrent, Edonkey в локальной сети. В частности, для решения этой задачи были проведены детальные исследования протоколов (описание команд, алгоритмы входа на хаб, получения TTH, получение MD5, получение SHA, получения списка пользователей, последовательность действий при поиске файлов и т.д.). Так же были рассмотрены способы получения информации о трафике в локальной сети и анализ данного трафика на предмет обнаружения в нем команд, присущих исследуемым протоколам. Предложена конкретная реализация программного модуля с помощью которого возможно установление обстоятельств работы p2p-приложений, работающих в локальной сети.

Следует отметить, что описанными способами возможен анализ обстоятельств работы и тех хостов, которые используют другие протоколы пирингового обмена данных, даже в случае использования шифрования (разумеется, в этом случае информации можно извлечь меньше).

Таким образом, поставленная задача успешно решена.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

6. Касперски Крис. Рыбная ловля в локальной сети [Электронный ресурс] / Журнал Хакер [Электронный ресурс]. URL: http://www.xakep.ru/magazine/xs/047/028/1.asp (дата обращения: 01.10.2015). Загл. с экрана. Яз. рус.
7. Cisco Systems NetFlow Services Export Version 9 [Электронный ресурс] / The Internet Engineering Task Force [Электронный ресурс]. URL: http://www.ietf.org/rfc/rfc3954.txt (дата обращения: 01.10.2015).Загл. с экрана. Яз. англ.
8. Спецификация протокола sFlow [Электронный ресурс] / sFlow.org [Электронный ресурс]. URL: http://www.sflow.org/developers/specifications.php(дата обращения: 01.10.2015).Яз. англ.
9. Гонг Йеминг. Identifying P2P users using traffic analysis [Электронныйресурс] URL: http://www.symantec.com/connect/articles/identifying-p2p-users-using-traffic-analysis (дата обращения: 01.05.2014). Загл. с экрана. Яз. англ.
10. КарагианнисТ. File-sharing in the Internet: A characterization of p2p traffic in the backbone: Tech. report [Электронныйресурс] / Department of Computer Science & Engineering [Электронный ресурс] – 2004. URL: http://www.cs.ucr.edu/tkarag/papers/tech.pdf (дата обращения: 01.10.2015).Яз. англ.Загл. с экрана.
11. NMDC protocol [Электронный ресурс] /sourceforge.net [Электронный ресурс]. URL: http://nmdc.sourceforge.net/NMDC.html (дата обращения: 01.10.2015).Яз. англ.Загл. с экрана.
12. WindowsAPI [Электронный ресурс] / Microsoft Developer Network [Электронный ресурс]. URL: http://msdn.microsoft.com/en-

us/library/ff818516%28v=vs.85%29.aspx (дата обращения: 01.10.2015).Яз. англ.Загл. с экрана.

13. Internet Protocol [Электронный ресурс] / The Internet Engineering Task Force [Электронный ресурс]. URL: http://tools.ietf.org/html/rfc791 (дата обращения: 01.10.2015).Загл. с экрана. Яз. англ.
14. Edonkey protocol [Электронный ресурс] /jmule.org [Электронный ресурс]. URL: http://www.jmule.org/files/eDonkey-protocol-0.6.2.html (дата обращения: 01.10.2015).Яз. англ.
15. The Bit Torrent Protocol Specification [Электронный ресурс] / bittorrent.org [Электронный ресурс]. URL:http://www.bittorrent.org/beps/bep_0003.html (дата обращения: 01.10.2015).Яз. англ.Загл. с экрана.
16. WinPcap: Documentation [Электронный ресурс] / winpcap.org [Электронный ресурс]. URL:https://www.winpcap.org/docs/ (дата обращения: 01.10.2015).Яз. англ.Загл. с экрана.
17. LibPcap: Documentation [Электронный ресурс] / tcpdump.org [Электронный ресурс]. URL: http://www.tcpdump.org/#documentation (дата обращения: 01.10.2015).Яз. англ.