1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. —
4. Институт компьютерных наук и технологий
5. **Кафедра «Информационная безопасность компьютерных систем»**

**ОТЧЕТ**

**по лабораторной работе № 16**

По дисциплине «Основы информационной безопасности»

1. Выполнил
2. Студент гр. 13508/13 А.Э. Палёный

\_\_\_\_\_\_\_\_\_\_

1. Проверил
2. Преподаватель

\_\_\_\_\_\_\_\_\_\_ М.О.Калинин

1. Санкт-Петербург
2. 2016

# Цель работы:

1. Изучение механизма реализации компьютерной угрозы типа «отказ в обслуживании», ознакомление со способами защиты от такого рода угроз.

# Решаемы задачи

1. Создать сервер Apache
2. Реализовать на сервер два вида атак (TCP и ICMP)
3. Реализовать защиту от этих атак

Оглавление

[Цель работы: 2](#_Toc451824740)

[Решаемы задачи 2](#_Toc451824741)

[Ход работы 4](#_Toc451824742)

[Ответы на контрольные вопросы: 7](#_Toc451824743)

[Вывод: 8](#_Toc451824744)

# Ход работы

1. DDoS-атака - сокращение от Distributed Denial Of Service Attack.

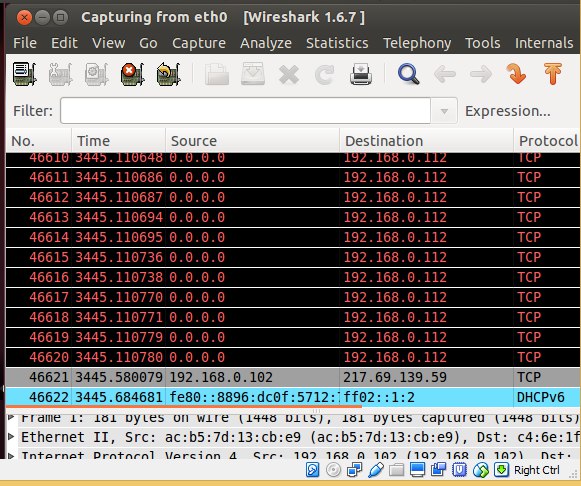
Особенностью данного вида компьютерного преступления является то, что злоумышленники не ставят своей целью незаконное проникновение в защищенную компьютерную систему с целью кражи или уничтожения информации. Цель данной атаки - парализовать работу атакуемого веб-узла. Первые сообщения о DDoS-атаках относятся к 1996 году. Но всерьез об этой проблеме заговорили в конце 1999 года, когда были выведены из строя веб-серверы таких корпораций, как Amazon, Yahoo, CNN, eBay, E-Trade и ряда других, немногим менее известных. Спустя год, в декабре 2000-го "рождественский сюрприз" повторился: серверы крупнейших корпораций были атакованы по технологии DDoS при полном бессилии сетевых администраторов. С тех пор сообщение о DDoS-атаке уже не являются сенсацией. Главной опасностью здесь является простота организации и то, что ресурсы хакеров являются практически неограниченными, так как атака является распределенной.

При исследовании механизма нападения, мы использовали – Colasoft.

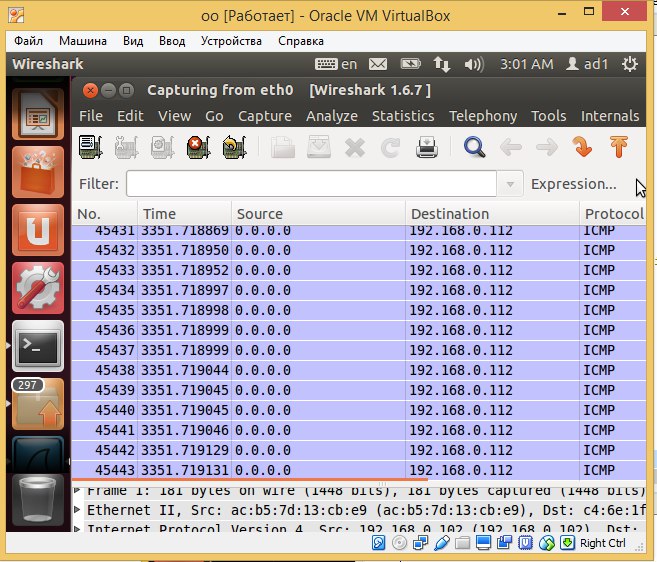
Для анализа трафика мы использовали – Wireshark - программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский интерфейс. В июне 2006 года проект был переименован в Wireshark из-за проблем с торговой маркой.

1. Существует три вида атак:
   1. TCP флуд или SYN флуд
   2. UDP пакет, который не предусматривает уведомления оп получении
   3. ICMP используется для служебных задач
2. В Colasoft пользователи могут редактировать пакеты в HEX редакторе и DECODE редакторе. Пользователь может создать абсолютно любой пакет.
3. Механизмы проведения атак:
4. SYN — атака, при которой заголовки пакетов подделывается таким образом, что место реального отправителя занимает произвольный либо несуществующий IP-адрес.
5. UDP атака. Данный метод основан на применении UDP протокола и используется обычно для вызова наиболее возможной нагрузки канала атакуемой системы. Метод UDP Flood не является атакой, использующей недостатки протокола, а основан на приложениях, работающих в рамках протокола UDP.
6. ICMP флуд - наиболее распространенным метод DDoS атак. Принцип его работы довольно прост. Злоумышленник, изменяя адрес источника, посылает пакет ICMP Echo Request (больше известный как пинг (ping)) к конкретным компьютерам, как правило, входящих в состав сети ddosnet). Эти компьютеры в свою очередь отвечают пакетом ICMP Echo Reply, отправляя его на IP адрес указанный хакером как источник. Часто для усиления атаки используются локальные сети (LAN) с включенной опцией направленной широковещательной рассылки (directed broadcast), в ответ на пинг с каждого компьютера в составе сети.
7. Была проведена атака на сервер apache. Мы отправляли SYN пакеты в огромном количестве. В результате сервер хоть и выстоял, но во время атаки на него нельзя было зайти. Также, была замечена особенность, что если в адресе отправителя указывать сервер, то требуется гораздо меньше пакетов для tcp флуд.

Вот, так wireshark изображает флуд сервера. Т.е. сервер буквально «захлёбывается» в этих пакетах.



Вторая атака – ICMP флуд.



Далее мы пытались организовать защиту от атак командами:  
sudo sysctl -w net.ipv4.tcp\_syncookies=1  
она запрещает передачу syn пакетов вызывающему, в случае переполнения очереди.

Далее мы определили максимальное время хранения SYN-запросов в памяти, до получения «закрывающего» пакета, командой:  
sudo sysctl –w net.ipv4.tcp\_max\_syn\_backlog=1024

Поэтому атакуемый сервер перестает отвечать на SYN запросы.

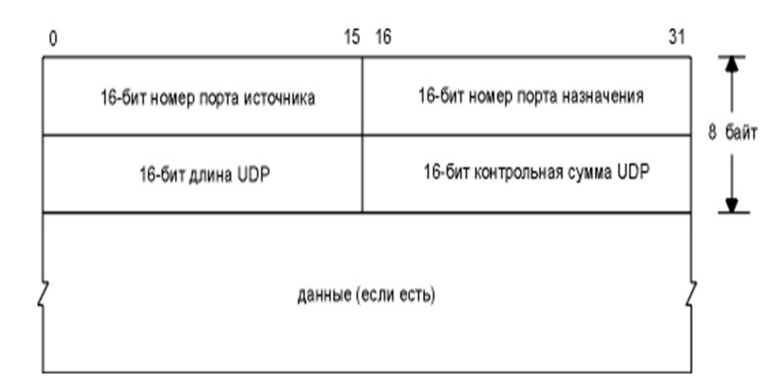
Далее была организована защита от флуд атак:

sudo sysctl net.ipv4.icmp\_echo\_ignore\_all=1

В результате, сервер переотвечать на запросы.

# Ответы на контрольные вопросы:

1. DOS атаки используются для, того чтобы сервер перествал отвечать на вопросы.
2. Структура UDP пакета:



Из-за отсутствия механизма перегрузок, UDP пакеты могут перекрывать трафик, и к серверу будет отсутствовать доступ.

1. Методы защиты от dos атак:

Отслеживаем источник атаки и перекрываем их

Ограничение допустимого предела соединений

Отключение ответов

1. Генератор пакетов создаёт и отправляет пакеты.

Настройки:  
Выбор адресов и физических адресов отправителей и получателей

Выбор порта. Выбор протокола и т.д.

1. ICMP пакеты – это служебные пакеты, которые отсылаются в основном с целью получить ответа. Если мы ответ не будем присылать ответные пакеты, то мы сэкономим половину трафика, а значит флуд не удасться.

# Вывод:

Мы провели DDos атаку. Это саамы распространённый вид атаки в интернете. Он довольно ресурсоёмкий, но эту проблемы помогают решить бот сети. В данный момент нет чёткой защиты от Dos атаки, так что эти атаки остаются самыми популярными атаками в Интернете.