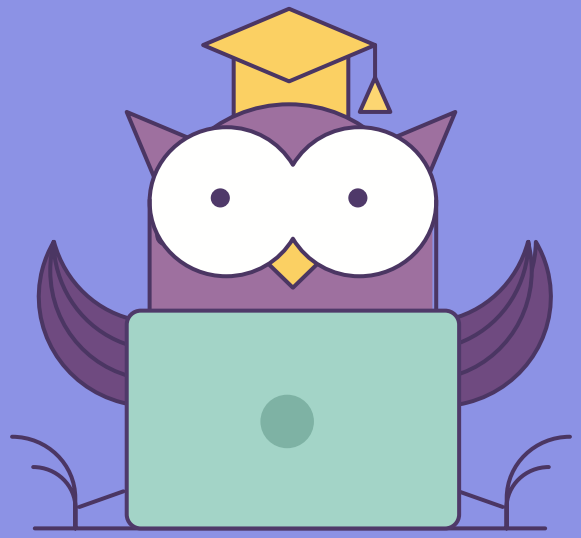
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Атаки на сетевое взаимодействие

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

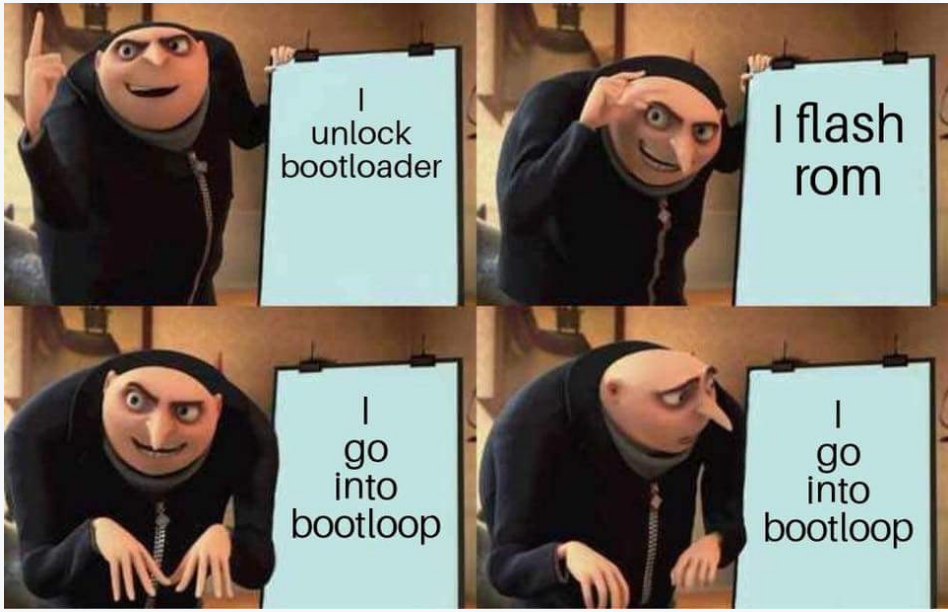
- **Основные типы атак**
  - Атаки относительно модели OSI
  - Kali Linux для атак на разные уровни

- **Методы проведения самых распространенных атак**
  - DDos атаки
    - Syn Flood
    - DNS Amplification

Цель занятия

1. Изучить подходы к атакам на сетевое взаимодействие

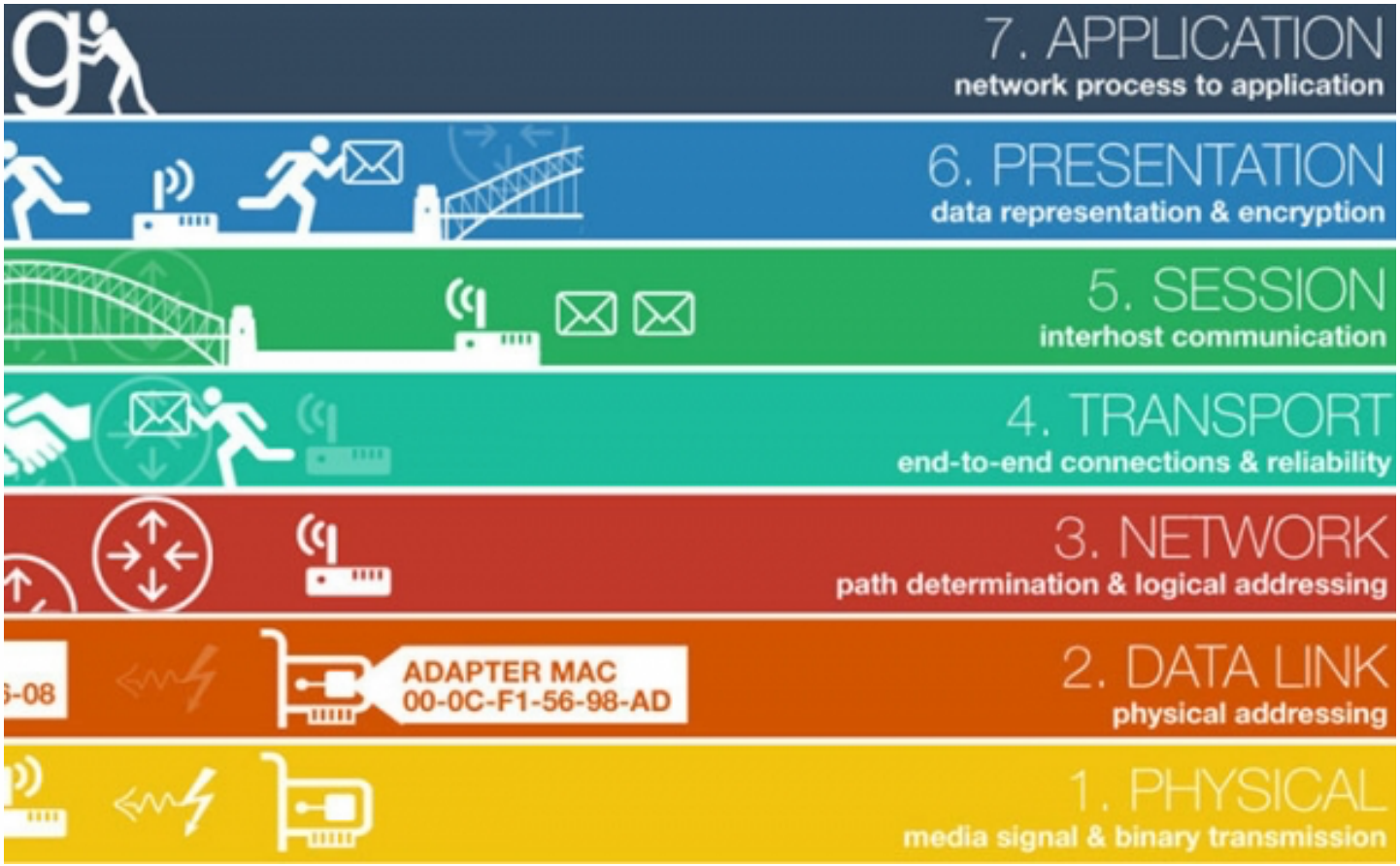
2. Закрепить полученные знания в практической работе



01

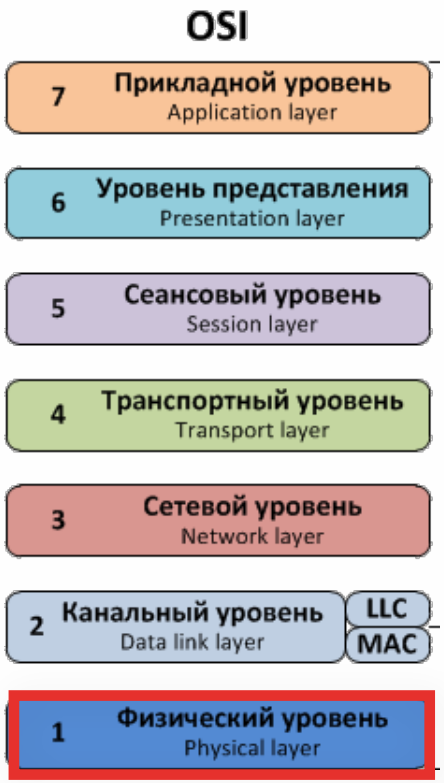
Атаки относительно модели OSI

Особенности взлома уровня в модели

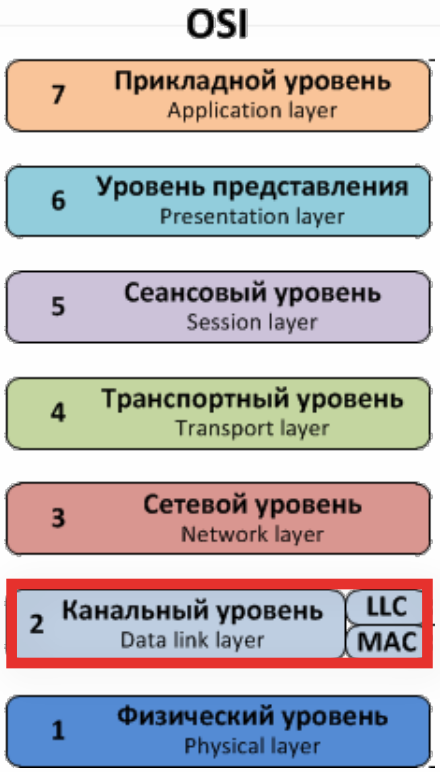


Атаки на физическом уровне

- Канал, который позволяет передавать сигналы от одного устройства к другому.
- Правила передачи информации диктуются средой передачи.
- Способы проведения атак:
  - Прямое включение в линию связи
  - Искажение данных путем воздействия на среду передачи
  - Физический разрыв линии



Атаки на канальном уровне

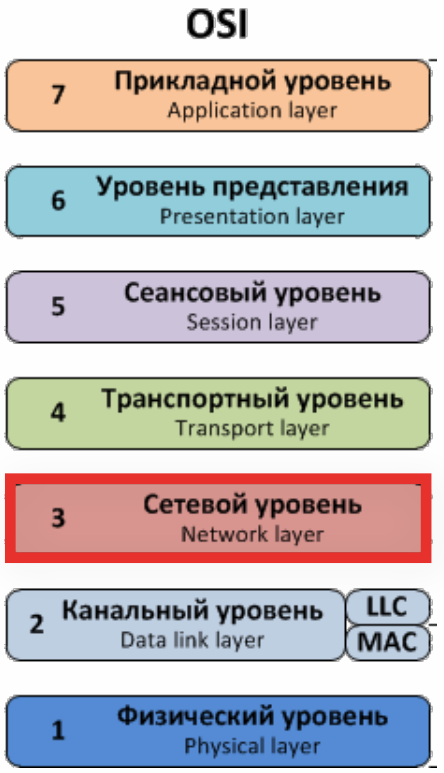


- Уровень, который представляет собой базу и фундамент для построения локальных сетей.

- Основные атаки проводимые на этом уровне*:
  - MiTM
  - DDoS
  - Несанкционированный доступ к другим участкам соединения
  - Нарушение работы сегментов и отрезков сети
    - Атаки на коммутаторы
    - Атаки на искажение информации в структурах, которые используют алгоритмы функционирования в сети

Атаки на сетевом уровне

- Уровень, который определяет положение хостов внутри сети
- Согласно алгоритмам этого уровня происходит адресация данных
- Атаки на уровень:
  - Нарушение маршрутизации
  - Подмена данных, которые были назначены в процессе адресации
  - DDoS - ICMP Smurf, ARPSpoofing

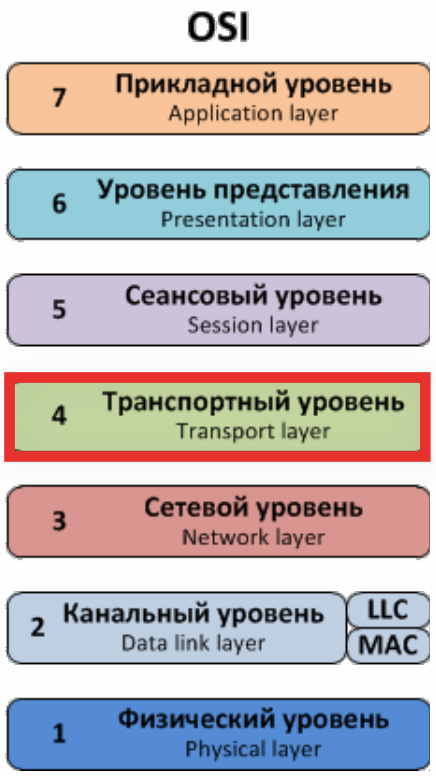


Атаки на транспортном уровне

- Способ передачи информации в сети, отдельные механизмы с контролем соединения и без него

- Атаки на уровень:
  - DDos
  - Нарушение соединения
  - Даунгрейд атаки
  - Организация управления атаками

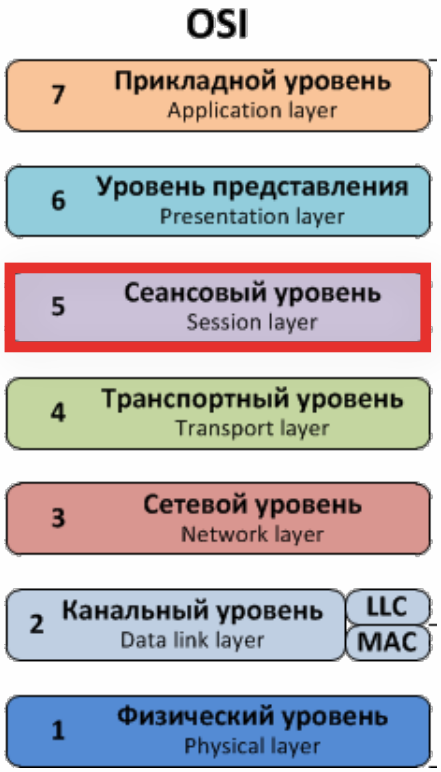
  более низких уровней



Атаки на уровне сеанса

- Уровень, который предоставляет возможность проводить сеанс связи.

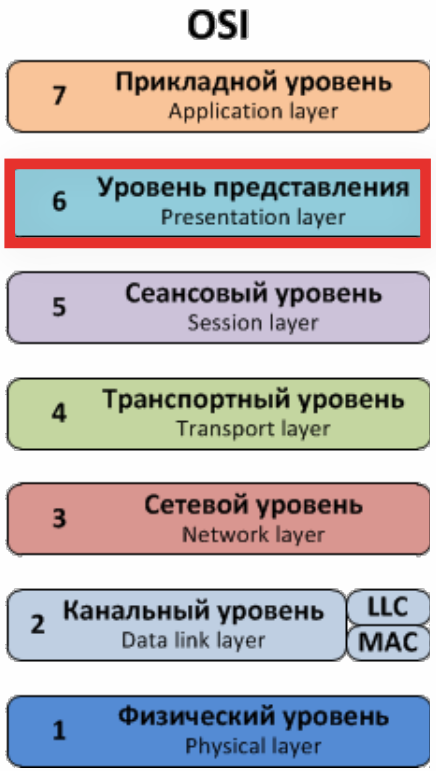
- Основные типы атак:
  - Уровень имеет тот же набор уязвимостей, что и конечная программа, которая его использует
  - DDoS
  - Атаки на сетевое оборудование



Атаки на уровне представления данных

- Уровень, который может определить в каком виде передавать данные.
- Именно на этом уровне может быть организовано шифрование.

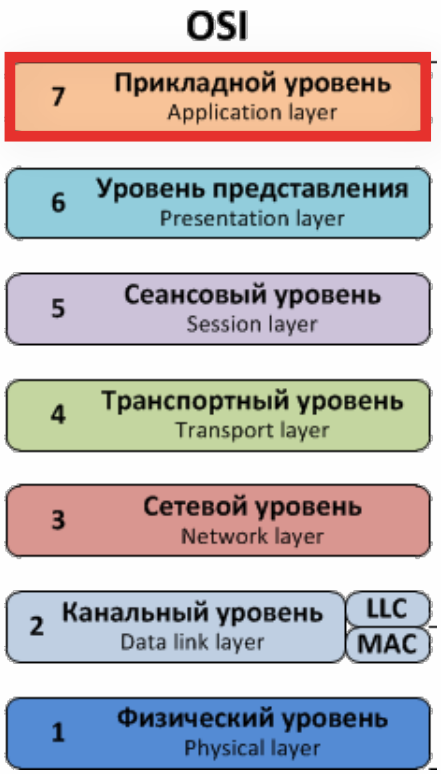
- Атаки на уровень:
  - Атаки на даунгрейд алгоритма шифрования
  - DDos
  - Атаки на алгоритмы, которые используются приложениями



Атаки на прикладном уровне

- Уровень, который представляет собой в первую очередь протоколы, которые используются для обмена информацией между приложениями.

- Атаки на уровень:
  - DDos
  - Атаки на приложения, которые используют протоколы для передачи данных



02

Kali Linux для атак на разные уровни

Физический уровень

Большинство утилит направлены на атаки радио каналов разных частот и диапазонов.

Основные технологии:

- Wi-Fi
- BlueTooth

Наименования утилит:

- Aireplay-ng
- air-crack
- air-base

Основные атаки:

- EvilTwin

Данные	Элементы
Нули и единицы	Радио канал

Канальный уровень

Уровень, который ориентируется на Mac адреса. Так же в разрезе беспроводных сетей это SSID идентификаторы.

Основные технологии:

- 802.11
- Ethernet

Наименования утилит:

- Macchanger
- air-crack

Основные атаки:

- Death attack
- Brute force

Данные	Элементы
Mac	Устройство
SSID	Точка доступа

Сетевой уровень

Уровень, который занимается построением маршрутов в сети.

Основные протоколы:

- ARP
- IP
- Ethernet

Наименования утилит:

- bettercap
- netwox

Основные атаки:

- Wormhole
- Black hole
- Byzantine Attack
- Sleep Deprivation
- Port Stealing
- Routing Table overflow
- Routing attack

Данные	Элементы
IP	Устройство
Route	Маршрут сети

Транспортный уровень

Занимается передачей пакетов, на этом уровне так же формируются безопасные/ шифрованные соединения.

Основные протоколы:

- TCP
- UDP

Наименования утилит:

- bettercap
- Wireshark
- Sslsniff
- Sslstrip

Основные атаки:

- Sniffing
- Smurf Attack
- Syn Flood
- DHCP Starvation
- DNS Hijacking

Данные	Элементы
PORT	Сервис
Connection	Канал между хостами

Уровень сессии

Устанавливает идентификаторы для ведения сессии работы пользователя конкретного хоста.

Основные протоколы:

- Любой возможный

Наименования утилит:

- bettercap

Основные атаки:

- MiTM

Данные	Элементы
Cookie	Идентификатор

01

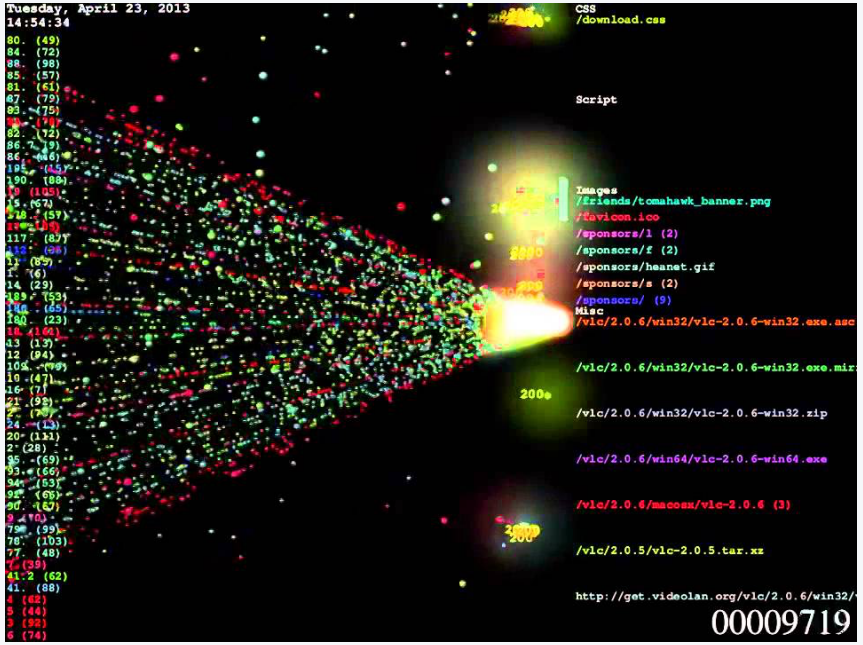
Примеры атак

DDos атака

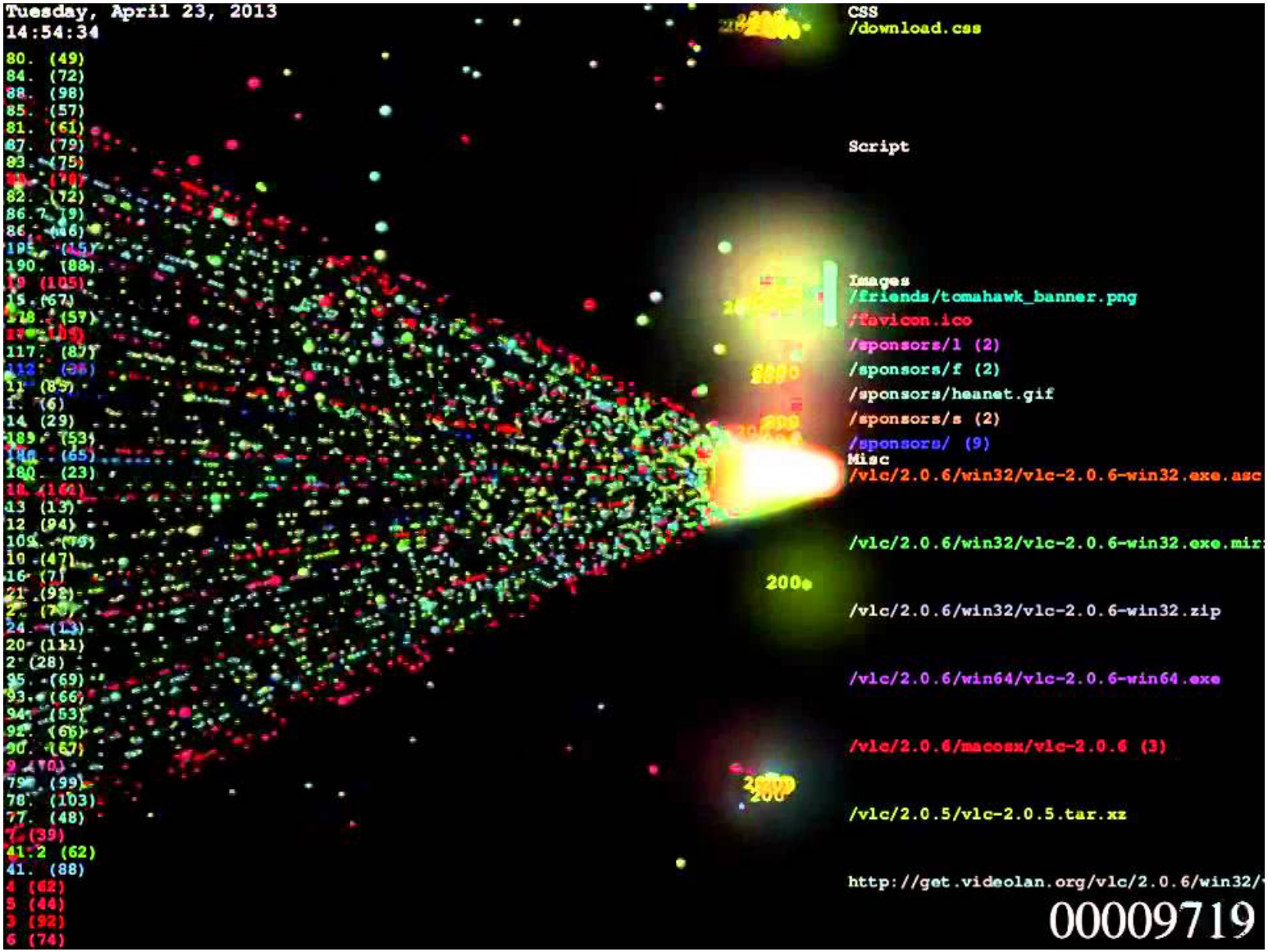
Тип атаки при которой генерируется большая нагрузка для хоста в сети, с которой он не справляется за длительный промежуток времени. Иногда вызывает отказ в обслуживании физических элементов.

Утилиты для проведения атаки:

- netwox
- ettercap
- bettercap
- scapy
- ....



DDOS


Tuesday, April 23, 2013
14:54:34
CSS
/download.css
Script
Images
/friends/tomahawk_banner.png
/favicon.ico
/sponsors/1 (2)
/sponsors/f (2)
/sponsors/heanet.gif
/sponsors/s (2)
/sponsors/ (9)
Misc
/vlc/2.0.6/win32/vlc-2.0.6-win32.exe.asc
/vlc/2.0.6/win32/vlc-2.0.6-win32.exe.mir
/vlc/2.0.6/win32/vlc-2.0.6-win32.zip
/vlc/2.0.6/win64/vlc-2.0.6-win64.exe
/vlc/2.0.6/macosx/vlc-2.0.6 (3)
/vlc/2.0.5/vlc-2.0.5.tar.xz
http://get.videolan.org/vlc/2.0.6/win32/
00009719

02

Примеры атак: Syn flood

Amplification

OTUS

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—

03

DNS Amplification

Александр Колесников

Спасибо
за внимание!