Атаки Slow HTTP DoS: кладём сайт одной командой

Разновидности, принцип работы, механизмы защиты и тесты на актуальном ПО

ДОКЛАДЧИК: @dmitry_metascan

1. Эффекты Slow HTTP DoS

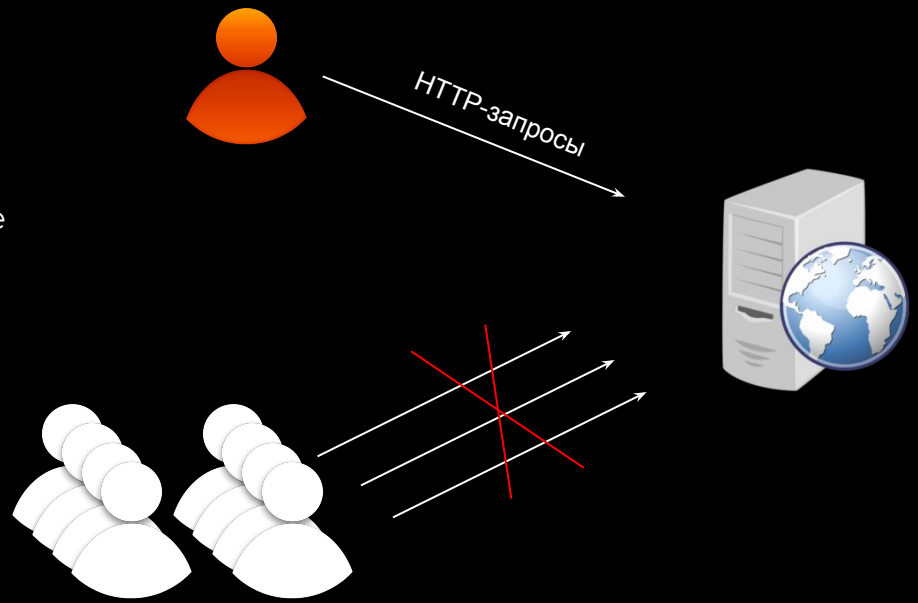

```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };
struct group_info *groups_alloc(int gidsetsize){
    struct group_info *group_info;
    int nblocks;
    int i;

    nblocks = (gidsetsize + NGROUPS_PER_BL
```

Атаки уровня L7 на исчерпание ресурсов веб-сервера

Достаточно послать N специально сформированных HTTP-запросов

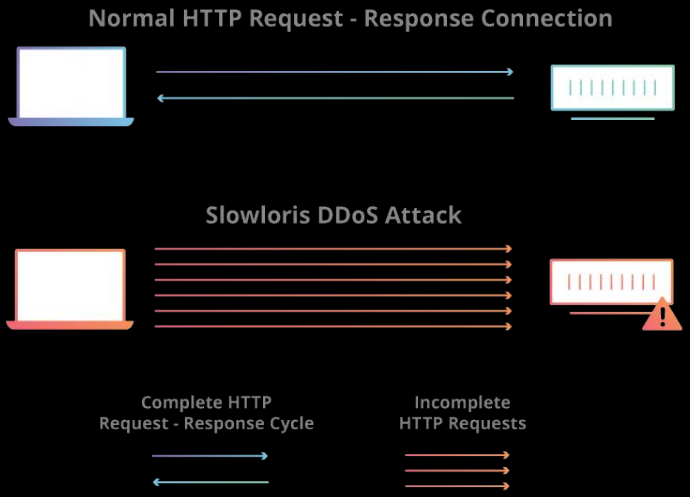
Сервер перестает принимать новые запросы, что приводит к отказу в обслуживании



2. Атаки

Эксплуатация проблем массового обслуживания

- Slowloris aka Slow headers
- R-U-Dead-Yet aka R-U-D-Y, Slow POST, Slow body
- Apache killer aka range header attack
- Slow Read aka TCP Persist Timer exploit
- ...



The Jester - th3j35t3r: TANGO DOWN

Примеры атак: WikiLeaks, 4chan, сайт иранского президента, сайты исламистов

[1] https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/
[2] https://www.defcon.org/images/defcon-19/dc-19-presentations/Bowne/DEFCON-19-Bowne-Three-Generations-of-DoS-Attacks.pdf

3. Slowloris

aka Slow headers

```
GET /  HTTP/1.1
Host: example.com
Connection: keet-alive
...
... waiting
...
X-a: 1
...
... waiting
...
X-a: 2
...
```

Discuss: 2007, Adrian Ilarion Ciobanu

2009, Robert "RSnake" Hansen
Defcon 17

Apache Foundation: не признали это багом

Microsoft: IIS не подвержен из-за таймаута на получение заголовков

Soft: slowloris.pl, slowhttptest, nmap scripts, etc.

[1] http://archive.is/xOJHa (http://ha.ckers.org/slowloris/)
[2] http://blog.spiderlabs.com/2010/11/advanced-topic-of-the-week-mitigating-slow-http-dos-attacks.html
[3] https://www.owasp.org/index.php/OWASP_HTTP_Post_Tool


What am I looking at?
Is this the log file?
This was a RUDY attack.

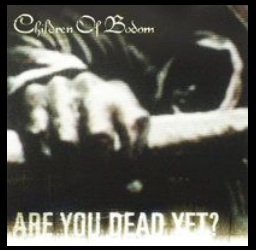
4. R-U-Dead-Yet

aka Slow body, Slow POST, R-U-D-Y

2009, Wong Onn Chee, Tom Brennan (OWASP DC 2010)

Apache Foundation: не признали это багом

Microsoft: выпустим патч в следующем сервис-паке



Children of Bodom

```
POST /form  HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (compatible; MSIE
8.0; Windows NT 6.0;) CRLF
Connection: close
Content-Type:
application/x-www-form-urlencoded
Content-Length: 512
Accept:
text/html;q=0.9,text/plain;q=0.8,image/png
,*/*;q=0.5

param=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaa...
```

Soft: r-u-dead-yet, slowhttptest

[1] http://web.archive.org/web/20110103185220/http://www.owasp.org/images/4/43/Layer_7_DDOS.pdf
[2] https://music.yandex.ru/album/87323
[3] http://web.archive.org/web/20111119183439/http://www.hybridsec.com/papers/OWASP-Universal-HTTP-DoS.ppt
[4] https://chaptersinwebsecurity.blogspot.com/2010/11/universal-http-dos-are-you-dead-yet.html

5. Apache killer

aka range header attack

Discuss: 2007, Michal Zalewski

CVE-2011-3192: Apache range header handling vulnerability

Apache 1.3.x, 2.0.0-2.0.64, 2.2.0-2.2.19

Apache Foundation: ого, пофиксим в течение 48 часов, даже нет, 24.

```
GET /HTTP / 1.1
Host: example.com
Range: bytes=0-,5-0,5-1,5-2,5-3,5-4,-5-5,5-6,5-7,5-8...
```

Soft: killapache.pl, slowhttptest, metasploit module

[1] http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0285.html
[2] https://www.computerworld.com/article/2510872/malware-vulnerabilities/apache-patches-web-server-dos-vulnerability.html

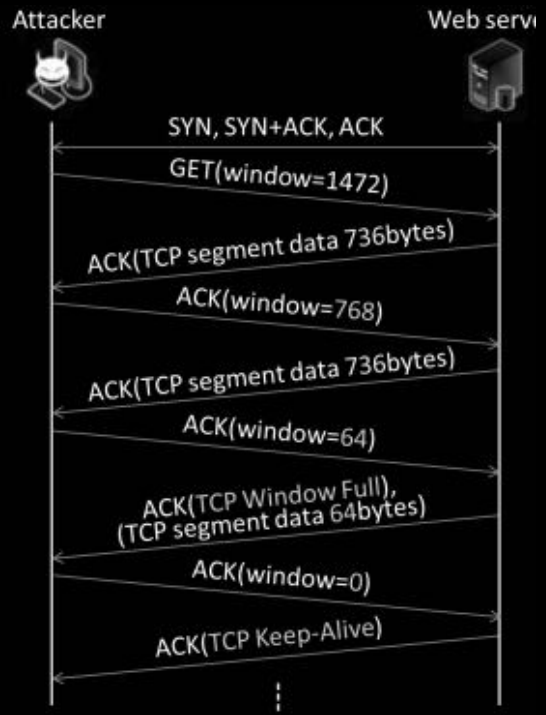
6. Slow Read

aka TCP Persist Timer Infiniteness Attack, TCP Persist Timer exploit

2008, Jack C. Louis
2009 , Fotis Hantzis, a.k.a. ithilgore

MS09-048, CVE-2008-4609, CVE-2009-1925, CVE-2009-1926

Здесь были
логи
wireshark



Soft: sockstress, slowhttptest, Nkiller2

[1] http://phrack.org/issues/66/9.html
[2] http://blog.shekyan.com/2012/01/are-you-ready-for-slow-rea
[3] https://www.owasp.org/images/a/a6/Owasp_KS_slowDoS.p

7. Тесты на актуальных серверах*

	Slowloris	RUDY	Apache killer	Slow Read
nginx/1.15.8				
Apache/2.4.37				
lighttpd/1.4.52				
IIS/10.0				

* но это не точно

8. Базовая защита

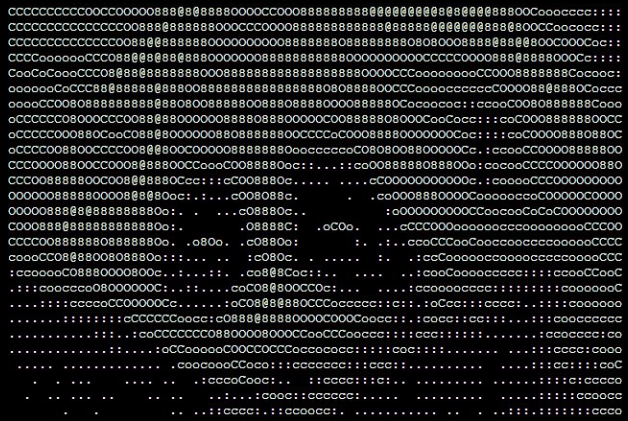
- Установить минимальную скорость передачи и дропать все более медленные соединения
- Установить максимальный таймаут запроса, например, ориентируясь на статистику реального использования
- Ограничить величину заголовков и тела запроса
- Увеличить максимальное количество соединений
- Иметь достаточно большой бэклог соединений для сервера
- Установить лимиты по размеру запроса для указанного URL
- Дропать HTTP-соединения с методами запроса, невалидными для указанного URL

Уязвимые и запатченные экземпляры bWAPP на nginx и apache2

[1] http://blog.shekyan.com/2011/07
[2] https://blog.qualys.com/securitylabs/2011/11/02/how-to-protect-against-slow-http-attacks/

9. Защита: nginx

- client_max_body_size, client_body_buffer_size, client_header_buffer_size, large_client_header_buffers
- client_body_timeout, client_header_timeout
- worker_processes, worker_connections (max_clients = worker_processes * worker_connections)
- HttpLimitReqModule, HttpLimitZoneModule
- $request_method



[1] https://xakep.ru/2012/12/29/16-antiddos-recipes/
[2] https://www.nginx.com/blog/mitigating-ddos-attacks-with-nginx-and-nginx-plus/

10. Защита: Apache

- Mod_reqtimeout, mod_qos
- LimitRequestFields, LimitRequestFieldSize, LimitRequestBody, LimitRequestLine, LimitXMLRequestBody
- MaxRequestWorkers
- ListenBackLog
- TimeOut, KeepAliveTimeOut
- ServerLimit, MaxRequestWorkers
- AcceptFilter
- MPM Prefork/Worker/Event

Loading new, exciting life.
Please stand by.

[1] https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/
[2] https://www.howtoforge.com/how-to-defend-slowloris-ddos-with-mod_qos-apache2-on-debian-lenny

Connection refused

@dmitry_metascan

metascan.ru
metascan.me

[1] https://news.mynavi.jp/article/20151228-a347/