hping3数据包定制

TimeS0ng / 2017-11-13 12:54:00 / 浏览数 3848 安全工具 工具 顶(0) 踩(0)

0x00. hping3 简介

hping3
是一款相当杰出的发包工具，它几乎可以发送任何定制的TCP / IP数据包，这对于我们学习TCP / IP协议栈也是一种不错的选择，而且在渗透测试过程中也能扮演

0x01. 常用语法

常规用法

```
hping3 192.168.1.1
```

LandAttack

```
hping3 192.168.1.1 -S -a 192.168.1.1 -p 80
```

DoS Attack

```
hping3 192.168.1.1 -V -d 100 -S -w 64 -p 445 -s 445 --flood --rand-source
```

ICMP路由追踪

```
hping3 www.baidu.com -T -V -1
```

端口扫描

```
hping3 192.168.1.1 -S -8 1-1024
```

0x02. 参数介绍

基础参数：

-c 限制发送总数

-i 发包间隔X秒，ux 微妙

```
hping3 -ux100 192.168.1.1
```

--flood 利用主机最大性能发包，杀敌1000，自损800

-I 指定网卡

-D debug

-z Ctrl +z 绑定TTL值，按一下TTL值加一，按两下减一

-d 控制数据段大小

-E 指定文件内容作为数据发送

-e 指定特征码 / 数据内容

```
hping3 192.168.1.1 -e TimeS0ng
```

-T 路由探测

```
hping3 www.baidu.com -T -1
```

协议选择：

【*】默认使用TCP协议，默认端口0，无任何flag

-0 #rawip,默认TCP为上层协议，但无TCP头

-H 指定IP头协议字段，只能工作在rawip模式下

```
hping3 192.168.1.101 -0 -H 8
```

-1 ICMP模式，发送icmp包

-2 发送UDP包，默认端口0

-8 scan模式，对目标端口进行扫描(-S/F/X/Y/A/R/P/U)

```
hping3 192.168.1.101 -8 1-1024 -S
```

-9 listen模式，此处和-e 连用可以匹配特征码

```
hping3 -9 -e times0ng
```

定制IP头：

-a 伪造源IP

--rand-source 随机伪造原地址

```
hping3 192.168.1.1 --rand-source
```

--rand-dest 随机目的地址

```
hping3 -I eth0 --rand-source --rand-dest 192.168.1.x
```

-t 指定TTL值

-N 指定IPID，默认随机（当需要分片发送数据包时使用）

```
hping3 192.168.1.1 -1 -x -d 1000 -N 100 -c 1
```

```
hping3 192.168.1.1 -1 -d 200 -g 400 -N 100 -c 1
```

-r 发现IPID变化规律（注意看id 字段）

-f IP数据段每16字节分片，-m 指定具体数值

```
hping3 192.168.1.1 -f -d 200 -c 1
```

定制TCP / UDP

-s 指定源端口（第一个包会是被指定的端口，后续包的源端口会依次加一）

-p 指定目标端口

-w 指定window 大小（可用于进行slowhttp攻击）

-M 指定sequence number

-Q 发现目标机器sequence number变化规律

-b 指定checksum

--tcp-mss 指定最大TCP段大小

--tcp-timestamp 启动时间戳选项，猜测远程UP主机时间

[*] TCP Flag

```
-F : fin 、-S : syn 、-R : rst 、 -P : push 、 -A : ack 、 -U : urg 、 -X : xmas 、 -Y : ymas
```


上一篇：DNS查询工具 下一篇：Metasploit一条龙服务

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板