netstat

Использование netstat

#netstat -I em0 => посмотреть ошибки интерфейса
#systat -ifstat => вывод
#netstat –na => просмотр всех открытых портов
#netstat -w 1 -h -d => весь трафик
#netstat -w 1 -h -d -I rl0 => трафик с интерфейса rl0
#netstat –nat – просмотр всех откры TCP-портов
#netstat –nau – просмотр всех откры UDP-портов
#netstat –npl – просмотр всех прослушиваемых портов(TCP,UDP,unix-сокеты)
#netstat –nptl – просмотр всех прослушиваемых портов TCP
#netstat –npul – просмотр всех прослушиваемых портов UDP
#netstat –nplx – просмотр всех прослушиваемых unix-сокетов
#netstat –s => просмотр статистики всех протоколов()
#netstat –st – просмотр статистики TCP-протокола
#netstat –su – просмотр статистики UDP-протокола
#netstat –r => просмотр таблицы маршрутизации
#netstat –i => просмотр статистики сетевых интерфейсов
#netstat -nid =>
#netstat -ic 2 – просмотр статистики сетевых интерфейсов в режиме реального времени с обновлением каждые 2 секунды.
#netstat –ie – просмотр расширенной информации о сетевых интерфейсах (аналог ifconfig)

Использование Netstat для определения DoS/DDoS

Отображение количества подключений на каждый IP-адрес в состоянии ESTABLISHED

```
netstat -naltp | grep ESTABLISHED | awk ‘{print $5}’ | awk -F: ‘{print $1}’ | sort -n | uniq -c
```

или

```
netstat -nalpt | grep ESTABLISHED | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort -rn
```

Отобразить все активные Интернет-подключения на 80 порт

сервера с их сортировкой
Полезно для определения большого количества запросов с одного IP-адреса(DoS)

```
netstat -na | grep :80 | sort
```

Подсчет количества подключений с каждого Ip-адреса на 80-порт сервера.

```
netstat -npla | grep :80 | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort –rn
```

Определение количества запросов на соединение было получено из сети

Число должно быть достаточно низким(менее 5).Во время DoS/DDoS-атаки такое количество может иметь высокое значение.Однако значение всегда зависит от системы(высокое значение на одном сервере может быть средним на другом)

```
netstat -np | grep SYN_RECV | wc –l
```

Список всех IP-адресов, с которых поступают соединения со статусом SYN_RECV

```
netstat -np | grep SYN_RECV | awk ‘{print $5}’ | awk -F: ‘{print $1}’
```

Подсчет количества подключений с каждого IP-адреса

```
netstat -ntu | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort –rn
```

Подсчет количества подключений с каждого IP-адреса по протоколу TCP или UDP

```
netstat -nap | grep ‘tcp\|udp’ | awk ‘{print $5}’ | cut -d: -f1| sort | uniq -c | sort –rn
```