

Команда rpcapd

Содержание

- Описание
- Параметры
- Примеры

Описание

Протокол RPCAP (Remote Packet Capture) предназначен для мониторинга сетевого трафика и захвата пакетов, поступающих на удаленное устройство в сети, для контроля и анализа транзитных потоков данных.


Протокол RPCAP подразумевает взаимодействие удаленного устройства и программы анализа сетевых данных (анализатора пакетов) по схеме сервер-клиент. На удаленном устройстве запускается демон RPCAP, который принимает запросы на соединение от клиентских приложений, производит аутентификацию и начинает обслуживание авторизованных клиентов: "прослушивает" сеть и передаёт запрошенные пакеты клиенту для обработки и анализа.

Устройства "Инфинет" имеют встроенный демон RPCAP. Его конфигурация производится с помощью команды `"rpcapd"`.

Синтаксис:

```
rpcapd -user=USERNAME -key[=PASSWORD] [add|del|change]
rpcapd [-port[=PORT]] [-maxconn[=MAXCONNECTIONS]] [start|stop]
rpcapd [-buffersize=[SND_BUFFER_SIZE]]
rpcapd {trace|notrace}
rpcapd show [-s=SOURCENAME]
rpcapd source
rpcapd clear
```

Параметры

Параметр	Описание
<code>-user=USERNAME -key [PASSWORD] [add del change]</code>	<div>Параметры управления учетными записями пользователей для подключения к устройству по протоколу RPCAP:</div> <ul style="list-style-type: none">"-user" - имя пользователя."-key" - пароль пользователя."add/del/change" - добавление/удаление/изменение учетной записи. По умолчанию работает параметр <code>"add"</code> или <code>"change"</code>, если указанное имя пользователя уже существует. <div><div></div><div>ВНИМАНИЕ Если в конфигурации RPCAP нет ни одного пользователя, то демон будет запрещать все попытки подключения к нему. Чтобы разрешить соединения от любых клиентов, необходимо использовать пустые значения параметров <code>"user"</code> и <code>"key"</code>.</div></div>
<code>[-port[=PORT]] [-maxconn [MAXCONNECTIONS]] [start stop]</code>	<div>Параметры запуска демона RPCAP.</div> <div>Если команда используется без параметров (<code>rpcapd start</code>), то она устанавливает стандартное значение порта RPCAP 2002 и разрешает неограниченное число клиентских соединений. Для установки других значений порта и максимально разрешённого количества соединений используются параметры <code>"port"</code> и <code>"maxconn"</code>.</div> <div>Параметры <code>"start/stop"</code> выполняют запуск/остановку демона.</div>
<code>[-buffersize= [SND_BUFFER_SIZE]]</code>	Устанавливает размер внутреннего буфера демона RPCAP на передачу захваченных пакетов клиенту. Размер буфера по умолчанию равен 32 Кб.
<code>{trace notrace}</code>	Включает/отключает запись отладочной информации демона в системный журнал устройства.

show [-s=SOURCENAME]	Отображает все активные клиентские сессии. С помощью параметра "-s" можно получить информацию об используемом фильтре PCAP для сессии с указанием ресурса.
source	Отображает список ресурсов на данном устройстве, доступных для мониторинга через протокол RPCAP.
clear	Удаление конфигурации и остановка демона RPCAP.

Примеры

Разрешим соединения от любых клиентов по протоколу RPCAP.

```
rpcapd -user= -key=
```

С помощью параметра "source" выведем список ресурсов доступных на устройстве.

```
rpcapd source
Type      Name      Description
-----
I   eth0          eth0  [link up-fd 100Mbps]=8103<UP,BROADCAST,PROMISC,MULTICAST>
I   rf5.0          rf5.0 [link up-hd 225Mbps]=8103<UP,BROADCAST,PROMISC,MULTICAST>
I   svil           [virtual]=8003<UP,BROADCAST,MULTICAST>
I   tun0           [virtual]=8010<POINTOPOINT,MULTICAST>
A   mint_rf5.0      rf5.0 MINT payload
```