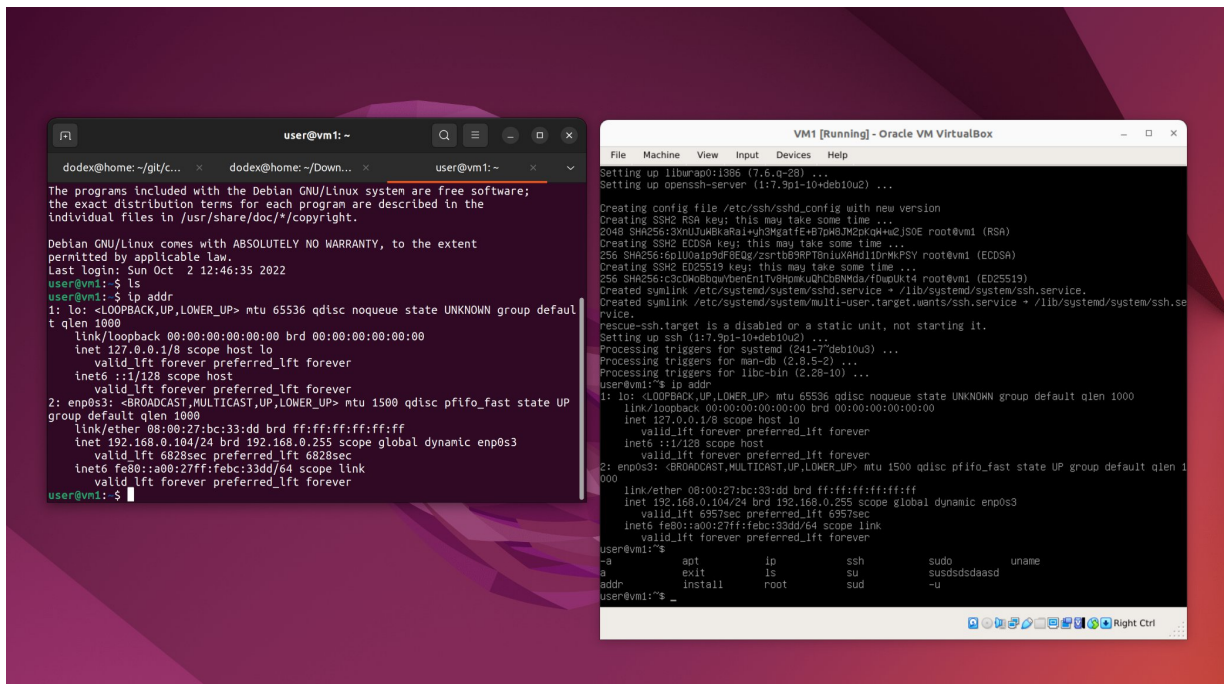


## 1. Удаленное подключение к Linux по ssh

- Установка на локальном ПК ssh-клиент и подключитесь к VM1



## 2. Безопасная аутентификация в Linux

- Настройте доступ через ключевую пару, запретите доступ к VM1 по логину и паролю `./userdata/vm1/etc/ssh/sshd config`

## Редактирование конфиг /etc/ssh/sshd\_config (./userdata)

## PermitRootLogin no – запрет логина по ssh из под root

### PasswordAuthentication no – запрет логина по pass.

Добавили authorized keys с хоста подключения

pubkeyс хоста поместили в ~/.ssh

### 3. Сканирование сети

```
./userdata/vm1/netcat scan vm2.txt
```

```
./userdata/vm1/nmap scan vm2.txt
```

## 4. Анализ трафика

- Установите на локальном ПК Wireshark
- Проанализируйте трафик VM2
- Заблокируйте вредоносный трафик VM2 с помощью встроенных средств операционной системы

Блокировка по протоколу "tcp" INPUT - iptables -A INPUT -p tcp -j DROP

Отдельный IP - Iptables -A INPUT -s 76.23.12.11 -j DROP

The image shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (No. 4459), which is a TCP segment. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4455	1129.7418551	192.168.0.106	104.21.46.149	TCP	66	44592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1164415746 TSecr=0 WS=128
4456	1129.9670215	104.21.46.149	192.168.0.106	TCP	66	443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4457	1130.9702936	104.21.46.149	192.168.0.106	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4458	1130.9705470	192.168.0.106	104.21.46.149	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM=1 TSval=1164416975 TSecr=0 WS=...
4459	1131.1340442	104.21.46.149	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4460	1133.9585857	192.168.0.106	104.21.46.149	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM=1 TSval=1164419963 TSecr=0 WS=...
4461	1134.1475011	104.21.46.149	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=...
4462	1135.2690600	104.21.46.149	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4465	1138.8532550	192.168.0.106	104.21.46.149	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM=1 TSval=1164424050 TSecr=0 WS=...
4466	1139.8448431	104.21.46.149	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=...
4470	1140.0755534	104.21.46.149	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4475	1147.8201714	192.168.0.106	104.21.46.149	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM=1 TSval=1164433824 TSecr=0 WS=...
4476	1148.9873916	104.21.46.149	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=...
4477	1149.8957667	104.21.46.149	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4495	1165.0924524	192.168.0.106	172.67.140.53	TCP	74	57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM=1 TSval=2422969369 TSecr=0 WS=128
4496	1165.1838199	172.67.140.53	192.168.0.106	TCP	66	[TCP Port numbers reused] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4497	1166.1689333	192.168.0.106	172.67.140.53	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM=1 TSval=2422976385 TSecr=0 WS=...
4498	1166.2892297	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4502	1167.3246302	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4503	1168.1109729	192.168.0.106	172.67.140.53	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM=1 TSval=2422972394 TSecr=0 WS=...
4504	1168.2110993	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4509	1172.3727026	192.168.0.106	172.67.140.53	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM=1 TSval=2422976649 TSecr=0 WS=...
4510	1172.4648725	172.67.140.53	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=...
4511	1173.5689721	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192
4512	1180.5710642	192.168.0.106	172.67.140.53	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM=1 TSval=2422984848 TSecr=0 WS=...
4513	1180.6031113	172.67.140.53	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=...
4514	1181.7550620	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192

Frame 4459: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlo1, id 0  
Ethernet II, Src: Tp-LinkT.80:7b:18 (c0:c9:e3:80:7b:18), Dst: Chongqin.b7:9f:05 (4c:d5:77:b7:9f:05)  
Internet Protocol Version 4, Src: 104.21.46.149, Dst: 192.168.0.106  
Transmission Control Protocol, Src Port: 443, Dst Port: 48592, Seq: 0, Ack: 1, Len: 0

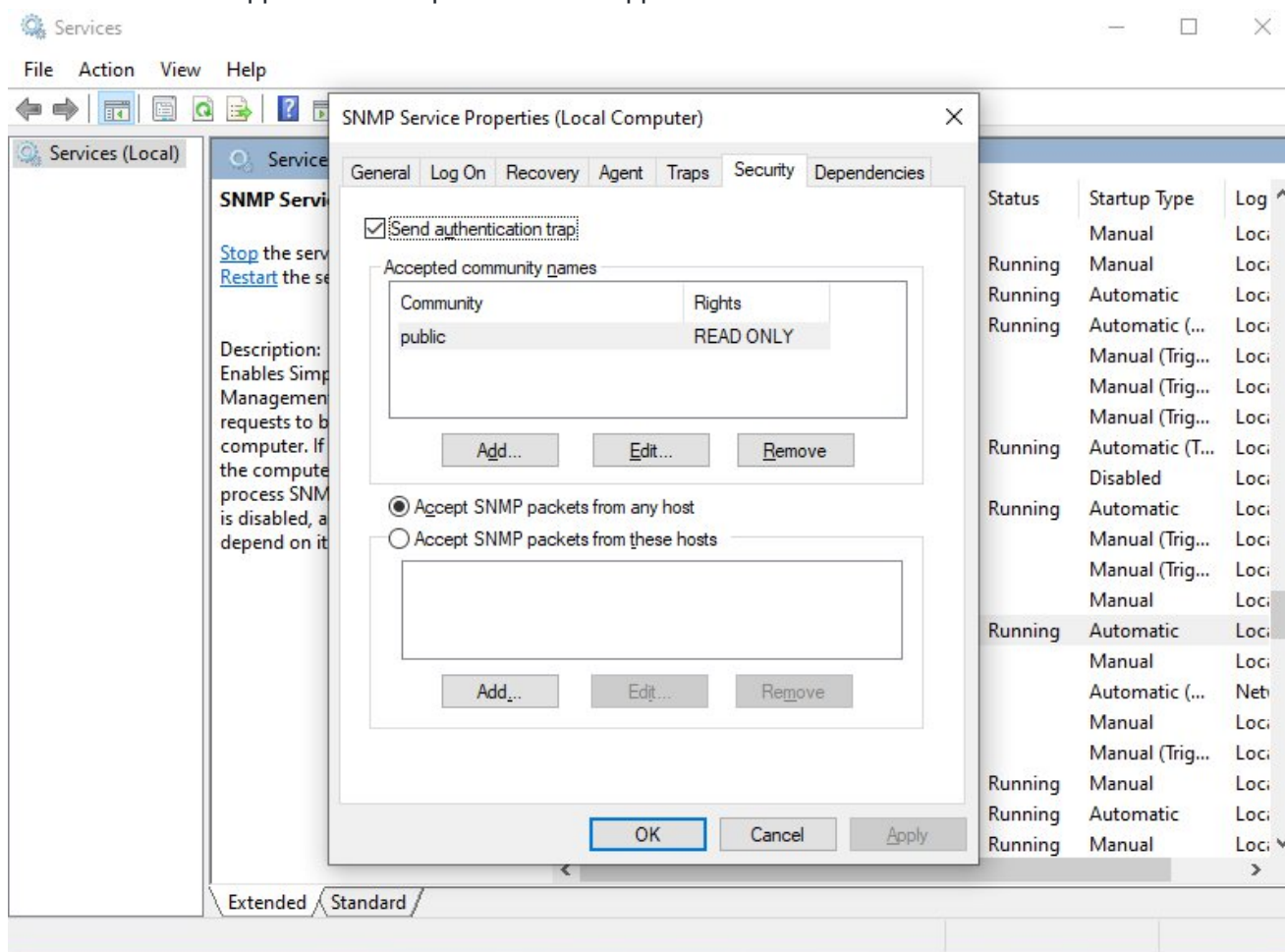
## 5. Мониторинг nginx

The image shows the Zabbix monitoring interface. The top navigation bar includes links for Monitoring, Inventory, Reports, Configuration, and Administration. The main content area displays the 'nginx: 11 items' monitoring dashboard. A line graph shows the 'nginx: Item values' over time. Below the graph, a table provides detailed performance metrics for various nginx components.

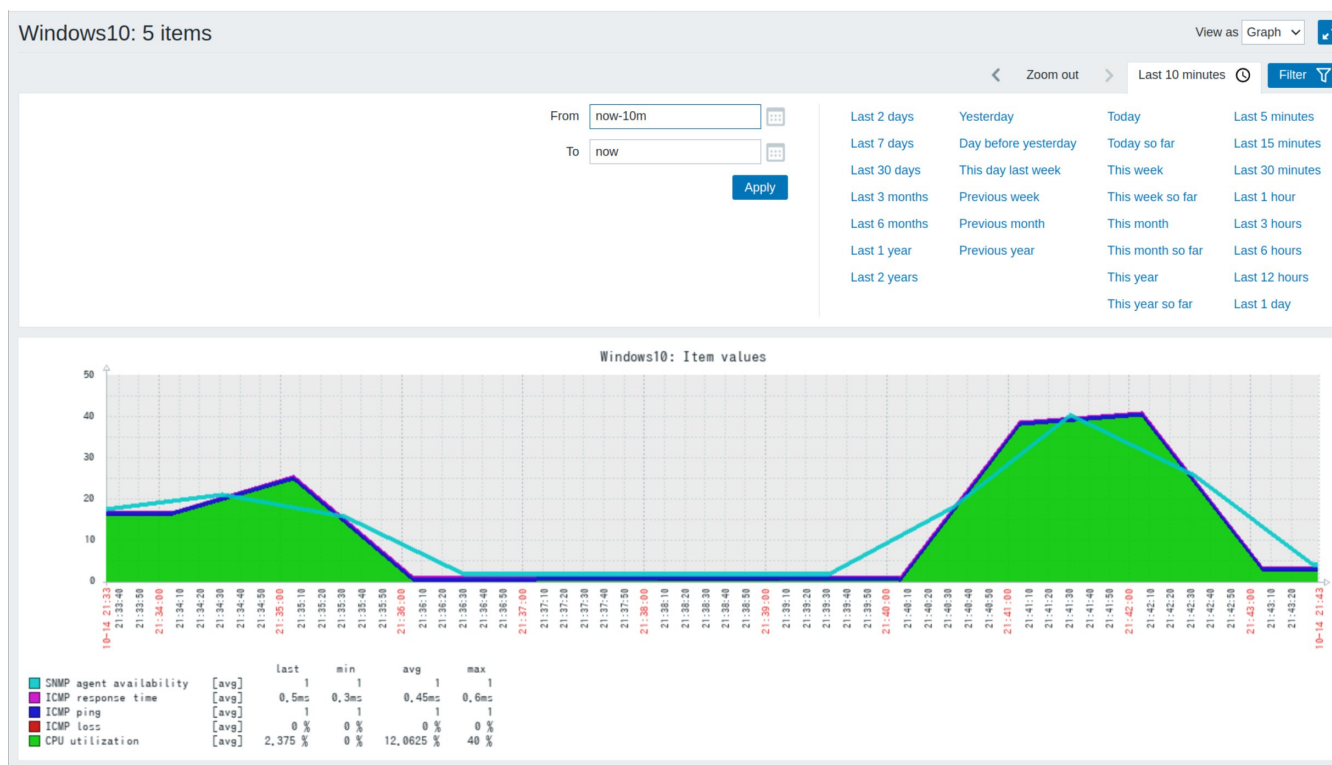
		last	min	avg	max
Nginx: Service status	[no data]				
Nginx: Service response time	[avg]	0,1ms	0,1ms	0,1ms	0,1ms
Nginx: Requests total	[avg]	141	108	116,4	141
Nginx: Requests per second	[avg]	0,4498	0,0167	0,1133	0,4498
Nginx: Connections writing	[avg]	1	1	1	1
Nginx: Connections waiting	[avg]	4	0	1,2	4
Nginx: Connections reading	[avg]	0	0	0	0
Nginx: Connections handled per second	[avg]	0,1	0,05	0,0667	0,1
Nginx: Connections dropped per second	[avg]	0	0	0	0
Nginx: Connections active	[avg]	5	1	2,2	5
Nginx: Connections accepted per second	[avg]	0,1	0,05	0,0667	0,1

## 6. Мониторинг Windows

- Настройте SNMP для принятия пакетов с любого хоста
- Создайте сообщество SNMP для чтения.



- Свяжите хост с шаблоном сетевого монитора
- Запустите мониторинг





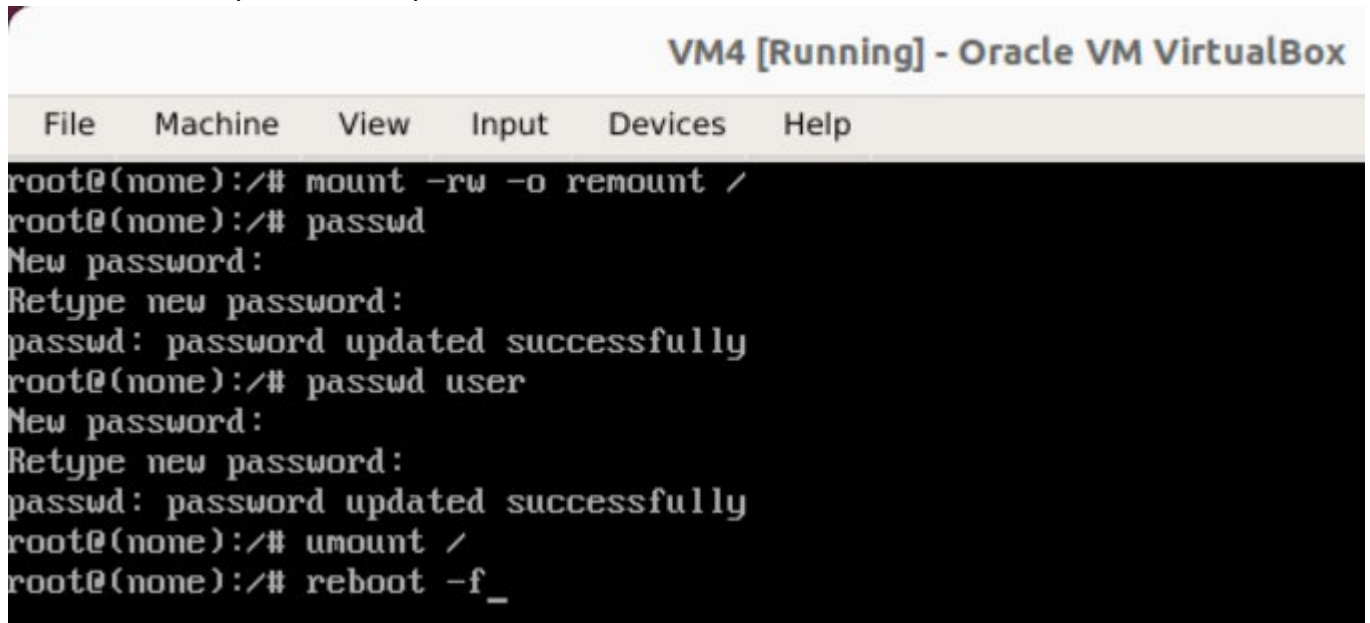
## Windows10 + Nginx

Windows10	CPU (1 Item)				
	CPU utilization	2022-10-14 21:34:07	15.875 %	+15.875 %	Graph
Windows10	General (6 Items)				
	SNMP traps (fallback)				History
	System contact details				History
	System description				History
	System location				History
	System name				History
	System object ID				History
nginx	Nginx (12 Items)				
	Nginx: Connections accepted per second	2022-10-14 21:34:10	0.0499	-0.0002	Graph
	Nginx: Connections active	2022-10-14 21:34:10	1		Graph
	Nginx: Connections dropped per second	2022-10-14 21:34:10	0		Graph
	Nginx: Connections handled per second	2022-10-14 21:34:10	0.0499	-0.0002	Graph
	Nginx: Connections reading	2022-10-14 21:34:10	0		Graph
	Nginx: Connections waiting	2022-10-14 21:34:10	0		Graph
	Nginx: Connections writing	2022-10-14 21:34:10	1		Graph
	Nginx: Requests per second	2022-10-14 21:34:10	0.0166	-0.0001	Graph
	Nginx: Requests total	2022-10-14 21:34:10	26	+1	Graph
	Nginx: Service response time	2022-10-14 21:34:08	0.1ms	- 0.1ms	Graph
	Nginx: Service status	2022-10-14 21:25:09	Up (1)		Graph
	Nginx: Version	2022-10-14 21:25:10	1.14.2		History
Windows10	Status (5 Items)				
	ICMP loss	2022-10-14 21:34:07	0 %		Graph
	ICMP ping	2022-10-14 21:34:07	Un (1)		Graph

### 7) Выход за пределы Docker-контейнера

- На VM4 изначально дан неверный pass от пользователя user и root. Заходим в настройки grub и дополняем конфиг, заходим от root

- Сбрасываем пароль



The screenshot shows a terminal window titled "VM4 [Running] - Oracle VM VirtualBox". The terminal has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The terminal text shows a root user at a prompt with the following commands and output:

```
root@(none):/# mount -rw -o remount /
root@(none):/# passwd
New password:
Retype new password:
passwd: password updated successfully
root@(none):/# passwd user
New password:
Retype new password:
passwd: password updated successfully
root@(none):/# umount /
root@(none):/# reboot -f_
```