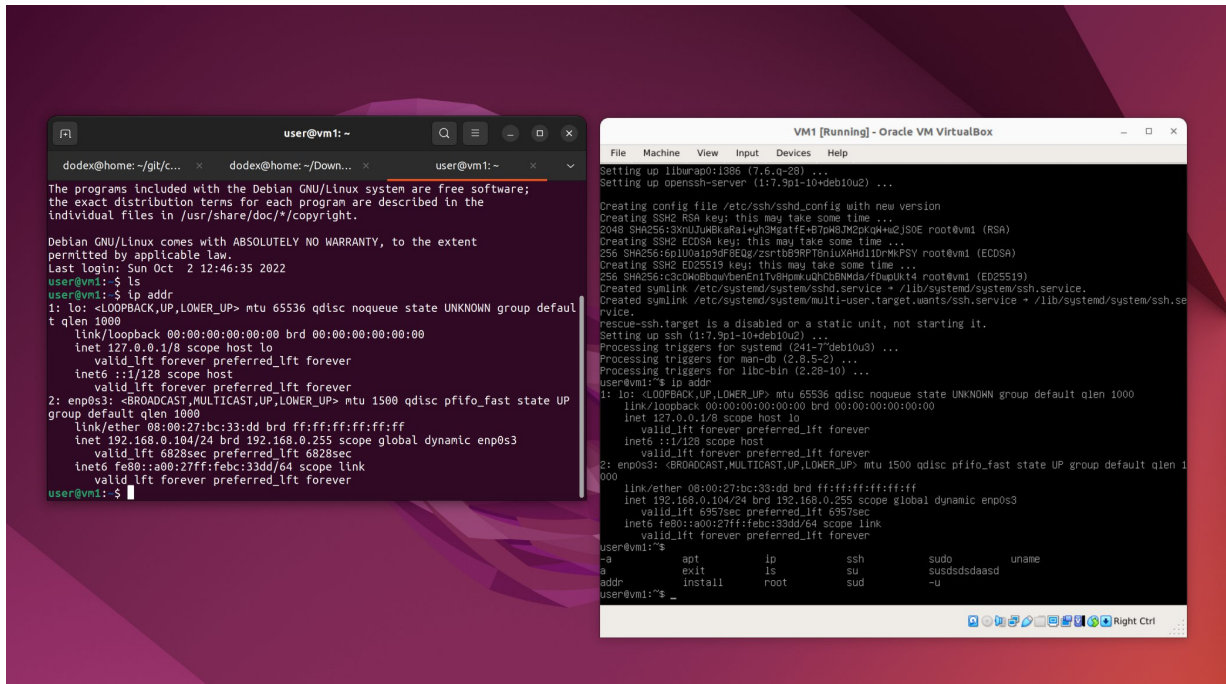


1) Удаленное подключение к Linux по ssh



2) Безопасная аутентификация в Linux

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

pubkeys хоста поместили в ~/.ssh

3) Файл с результатом сканирования сети

```
./userdata/vm1/netcat_scan_vm2.txt
```

```
./userdata/vm1/nmap_scan_vm2.txt
```

4) IPTABLES

Блокировка по протоколу "tcp" INPUT

```
iptables -A INPUT -p tcp -j DROP
```

Отдельный IP

```
Iptables -A INPUT -s 76.23.12.11 -j DROP
```

Wireshark capture showing network traffic on interface wlo1. The capture is filtered for IP address 192.168.0.106. The packet list shows several TCP segments, including a SYN packet (443) and a RETRANSMISSION (443). The packet details pane shows the structure of the captured packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4455	1129.7418551	192.168.0.106	104.21.46.149	TCP	74	48592 → 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=1460 SACK_PERM=1 WS=8192
4457	1130.0709303	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=1460 SACK_PERM=1 WS=8192
4458	1130.9785470	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=1460 SACK_PERM=1 TSval=1164410975 TSecr=0 WS=
4459	1131.1342042	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=1460 SACK_PERM=1 WS=8192
4460	1133.9588587	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=1460 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=1460 SACK_PERM=1 WS=
4462	1135.2000003	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=1460 SACK_PERM=1 WS=8192
4465	1138.8532359	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=1460 SACK_PERM=1 TSval=1164424858 TSecr=0 WS=
4466	1139.0448431	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=1460 SACK_PERM=1 WS=
4470	1140.8755534	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=1460 SACK_PERM=1 WS=8192
4475	1147.8291714	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=1460 SACK_PERM=1 TSval=1164433824 TSecr=0 WS=
4476	1148.0873916	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=1460 SACK_PERM=1 WS=
4477	1149.0957667	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=1460 SACK_PERM=1 WS=8192
4485	1165.8924524	192.168.0.106	172.67.140.53	TCP	74	57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2422969369 TSecr=0 WS=128
4496	1165.1830159	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=1460 SACK_PERM=1 WS=8192
4497	1166.1985830	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=1460 SACK_PERM=1 TSval=2422970385 TSecr=0 WS=
4498	1166.2092297	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=1460 SACK_PERM=1 WS=8192
4502	1167.3246392	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=1460 SACK_PERM=1 WS=8192
4503	1168.1169720	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=1460 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=1460 SACK_PERM=1 WS=8192
4509	1172.3727028	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=1460 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=1460 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=1460 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=1460 SACK_PERM=1 TSval=2422984848 TSecr=0 WS=
4513	1180.6653113	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=1460 SACK_PERM=1 WS=
4514	1181.7556020	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=1460 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 (c8: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) Nginx status:

Zabbix Monitoring Dashboard showing Nginx status. The dashboard includes a graph of Nginx item values over time, a table of Nginx status metrics, and a list of Nginx status items.

nginx: 11 items

View as: Values

Zoom out Last 5 minutes Filter

nginx: Item values

		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

Zabbix 4.4.8. © 2001–2020. Zabbix SIA