Collaborative Discussion 2 – Peer Response 1 – Michael Geiger

The program NetScanTools was used to examine the tracerout command of ICMP, TCP and UDP packets (Northwest Performance Software, 2021). The results can be found in the appendix below.

During the investigation it became apparent that an echo was received from the destination IP for ICMP and TCP requests. In the tracerout investigation with UDP packets, however, the destination could not be reached. Another abnormality is Hop 2, which only received a response from the ICMP request. A reason in the results can be assumed to be due to blocked communication.

The Transmission Control Protocol (TCP) based on IP takes care of the connection-oriented data exchange. This is the usual form of maintaining two systems on the Internet and takes on tasks such as establishing the connection, protecting against transmission errors, dividing the data stream into packets at the sender and correctly merging the data segments at the recipient (Parziale et al., 2006).

The Internet Control Message Protocol (ICMP) sends control messages between computers on a network. ICMP is used, for example, to inform the recipient that the transmission should be stopped or that the recipient has not received a certain packet.

The User Datagram Protocol (UDP) is the simplest form of IP data transmission. In doing so, data is sent without checking whether it is free from errors or if it has arrived. UDP is therefore not suitable for the transmission of files or other information that must arrive exactly as it was sent. However, it makes sense, for example, for voice transmission.

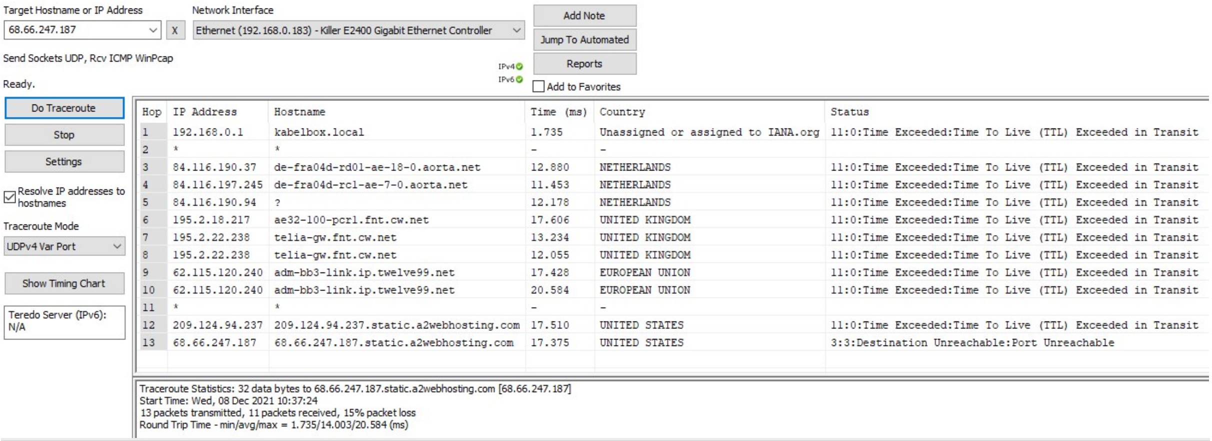
Since the website loadedwithstuff.co.uk is an e-commerse site, functions such as voice transmission and thus UDP, in contrast to ICMP and TCP, are not necessary. Therefore, a possible conclusion is that communication via UDP is prevented from the server side in order to close an unnecessary vulnerability (Shah et al., 2020).

References:

Northwest Performance Software, Inc. (2021)Traceroute Tool. Available from: https://www.netscantools.com/nstpro_traceroute.html [Accessed: 08.12.2021]

Parziale, L., Liu, W., Matthews, C., Rosselot, N., Davis, C., Forrester, J. & Britt, D. (2006) TCP/IP Tutorial and Technical Overview. Available from: https://www.redbooks.ibm.com/abstracts/gg243376.html?Open [Accessed: 08.12.2021]

Shah, A., Khan, Y. & Ashraf, M.(2020) Attacks Analysis of TCP and UDP of UNSW-NB15 Dataset. Transactions on Computer Sciences 8(1):48-54. Available from: https://vfast.org/journals/index.php/VTCS/article/view/528/552 [Accessed: 08.12.2021]



Target Hostname or IP Address: 68.66.247.187

Network Interface: Ethernet (192.168.0.183) - Killer E2400 Gigabit Ethernet Controller

Send Sockets UDP, Rcv ICMP WinPcap

Ready.

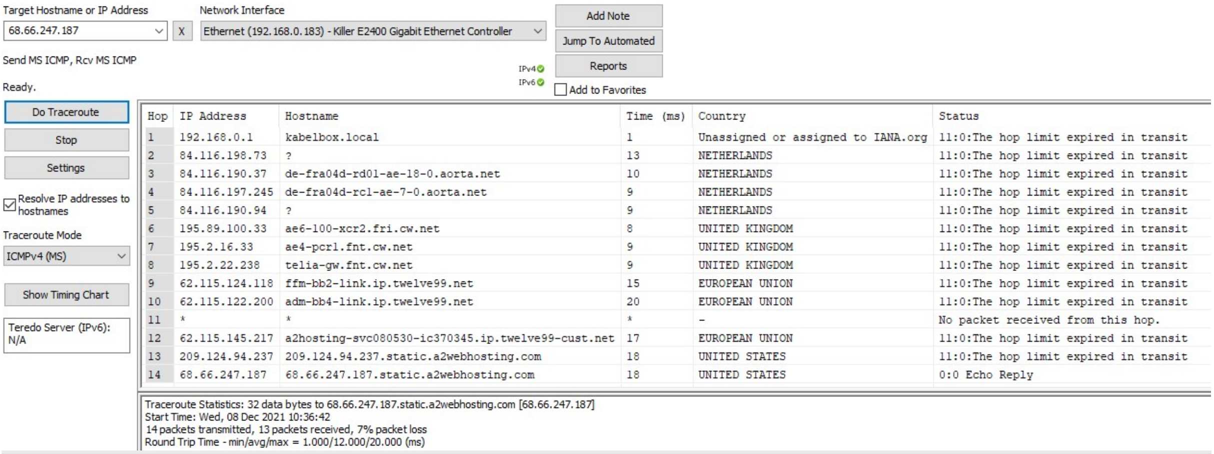
☑ Resolve IP addresses to hostnames

Traceroute Mode: UDPv4 Var Port

Teredo Server (IPv6):
N/A

Hop	IP Address	Hostname	Time (ms)	Country	Status
1	192.168.0.1	kabelbox.local	1.735	Unassigned or assigned to IANA.org	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
2	*	*	-	-	
3	84.116.190.37	de-fra04d-rd01-ae-18-0.aorta.net	12.880	NETHERLANDS	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
4	84.116.197.245	de-fra04d-rc1-ae-7-0.aorta.net	11.453	NETHERLANDS	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
5	84.116.190.94	?	12.178	NETHERLANDS	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
6	195.2.18.217	ae32-100-pcr1.fnt.cw.net	17.606	UNITED KINGDOM	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
7	195.2.22.238	telia-gw.fnt.cw.net	13.234	UNITED KINGDOM	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
8	195.2.22.238	telia-gw.fnt.cw.net	12.055	UNITED KINGDOM	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
9	62.115.120.240	adm-bb3-link.ip.twelve99.net	17.428	EUROPEAN UNION	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
10	62.115.120.240	adm-bb3-link.ip.twelve99.net	20.584	EUROPEAN UNION	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
11	*	*	-	-	
12	209.124.94.237	209.124.94.237.static.a2webhosting.com	17.510	UNITED STATES	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
13	68.66.247.187	68.66.247.187.static.a2webhosting.com	17.375	UNITED STATES	3:3:Destination Unreachable:Port Unreachable

```
Traceroute Statistics: 32 data bytes to 68.66.247.187.static.a2webhosting.com [68.66.247.187]
Start Time: Wed, 08 Dec 2021 10:37:24
13 packets transmitted, 11 packets received, 15% packet loss
Round Trip Time - min/avg/max = 1.735/14.003/20.584 (ms)
```



Target Hostname or IP Address: 68.66.247.187

Network Interface: Ethernet (192.168.0.183) - Killer E2400 Gigabit Ethernet Controller

Send MS ICMP, Rcv MS ICMP

Ready.

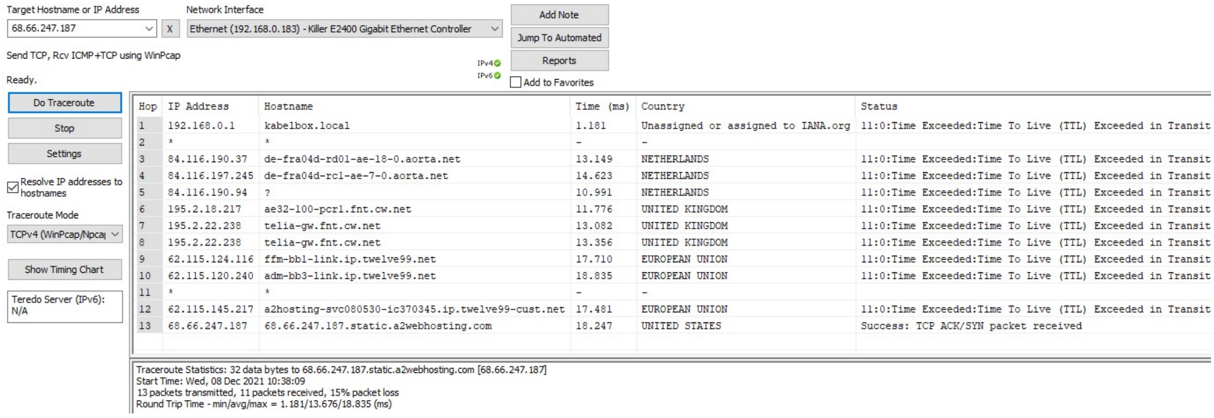
☑ Resolve IP addresses to hostnames

Traceroute Mode: ICMPv4 (MS)

Teredo Server (IPv6):
N/A

Hop	IP Address	Hostname	Time (ms)	Country	Status
1	192.168.0.1	kabelbox.local	1	Unassigned or assigned to IANA.org	11:0:The hop limit expired in transit
2	84.116.198.73	?	13	NETHERLANDS	11:0:The hop limit expired in transit
3	84.116.190.37	de-fra04d-rd01-ae-18-0.aorta.net	10	NETHERLANDS	11:0:The hop limit expired in transit
4	84.116.197.245	de-fra04d-rc1-ae-7-0.aorta.net	9	NETHERLANDS	11:0:The hop limit expired in transit
5	84.116.190.94	?	9	NETHERLANDS	11:0:The hop limit expired in transit
6	195.89.100.33	ae6-100-xcr2.fri.cw.net	8	UNITED KINGDOM	11:0:The hop limit expired in transit
7	195.2.16.33	ae4-pcr1.fnt.cw.net	9	UNITED KINGDOM	11:0:The hop limit expired in transit
8	195.2.22.238	telia-gw.fnt.cw.net	9	UNITED KINGDOM	11:0:The hop limit expired in transit
9	62.115.124.118	ffm-bb2-link.ip.twelve99.net	15	EUROPEAN UNION	11:0:The hop limit expired in transit
10	62.115.122.200	adm-bb4-link.ip.twelve99.net	20	EUROPEAN UNION	11:0:The hop limit expired in transit
11	*	*	*	-	No packet received from this hop.
12	62.115.145.217	a2hosting-svc080530-ic370345.ip.twelve99-cust.net	17	EUROPEAN UNION	11:0:The hop limit expired in transit
13	209.124.94.237	209.124.94.237.static.a2webhosting.com	18	UNITED STATES	11:0:The hop limit expired in transit
14	68.66.247.187	68.66.247.187.static.a2webhosting.com	18	UNITED STATES	0:0 Echo Reply

```
Traceroute Statistics: 32 data bytes to 68.66.247.187.static.a2webhosting.com [68.66.247.187]
Start Time: Wed, 08 Dec 2021 10:36:42
14 packets transmitted, 13 packets received, 7% packet loss
Round Trip Time - min/avg/max = 1.000/12.000/20.000 (ms)
```



Target Hostname or IP Address: 68.66.247.187

Network Interface: Ethernet (192.168.0.183) - Killer E2400 Gigabit Ethernet Controller

Send TCP, Rcv ICMP+TCP using WinPcap

Ready.

☑ Resolve IP addresses to hostnames

Traceroute Mode: TCPv4 (WinPcap/Npca|

Teredo Server (IPv6):
N/A

Hop	IP Address	Hostname	Time (ms)	Country	Status
1	192.168.0.1	kabelbox.local	1.181	Unassigned or assigned to IANA.org	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
2	*	*	-	-	
3	84.116.190.37	de-fra04d-rd01-ae-18-0.aorta.net	13.149	NETHERLANDS	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
4	84.116.197.245	de-fra04d-rc1-ae-7-0.aorta.net	14.623	NETHERLANDS	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
5	84.116.190.94	?	10.991	NETHERLANDS	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
6	195.2.18.217	ae32-100-pcr1.fnt.cw.net	11.776	UNITED KINGDOM	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
7	195.2.22.238	telia-gw.fnt.cw.net	13.082	UNITED KINGDOM	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
8	195.2.22.238	telia-gw.fnt.cw.net	13.356	UNITED KINGDOM	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
9	62.115.124.116	ffm-bb1-link.ip.twelve99.net	17.710	EUROPEAN UNION	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
10	62.115.120.240	adm-bb3-link.ip.twelve99.net	18.835	EUROPEAN UNION	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
11	*	*	-	-	
12	62.115.145.217	a2hosting-svc080530-ic370345.ip.twelve99-cust.net	17.481	EUROPEAN UNION	11:0:Time Exceeded:Time To Live (TTL) Exceeded in Transit
13	68.66.247.187	68.66.247.187.static.a2webhosting.com	18.247	UNITED STATES	Success: TCP ACK/SYN packet received

```
Traceroute Statistics: 32 data bytes to 68.66.247.187.static.a2webhosting.com [68.66.247.187]
Start Time: Wed, 08 Dec 2021 10:38:09
13 packets transmitted, 11 packets received, 15% packet loss
Round Trip Time - min/avg/max = 1.181/13.676/18.835 (ms)
```