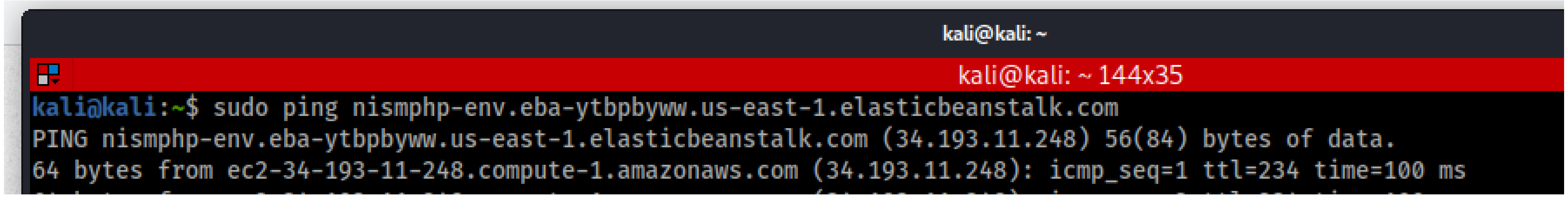
1 Inhaltsverzeichnis

Firewalls of security-conscious organizations often blanket-filter inbound ICMP messages, and so ICMP probing isn't effective; however, ICMP isn't filtered in most cases, as these messages are useful during network troubleshooting. McNab (2007)

McNab, C. (2007) Network Security Assessment. Sebastopol, CA: O'Reilly Media.

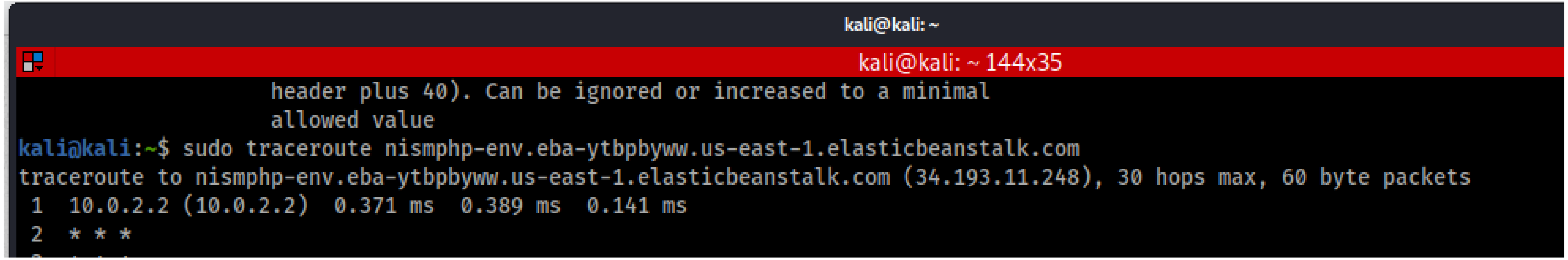
ICMP blocked, TCP handled by the router (so only two hops can be identified)

2 Basics – IP

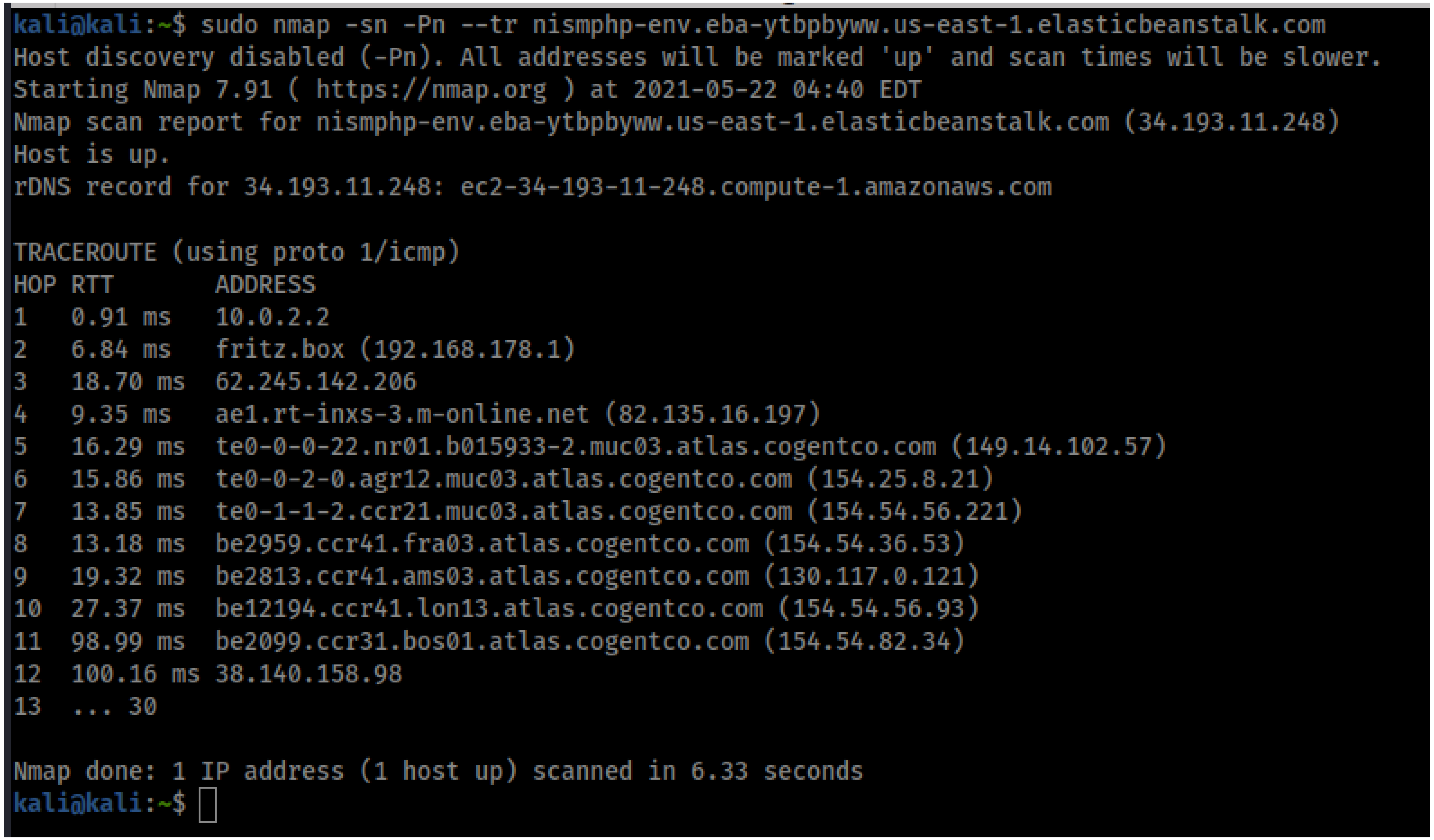


```
kali@kali:~$ sudo ping nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
PING nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com (34.193.11.248) 56(84) bytes of data.
64 bytes from ec2-34-193-11-248.compute-1.amazonaws.com (34.193.11.248): icmp_seq=1 ttl=234 time=100 ms
```

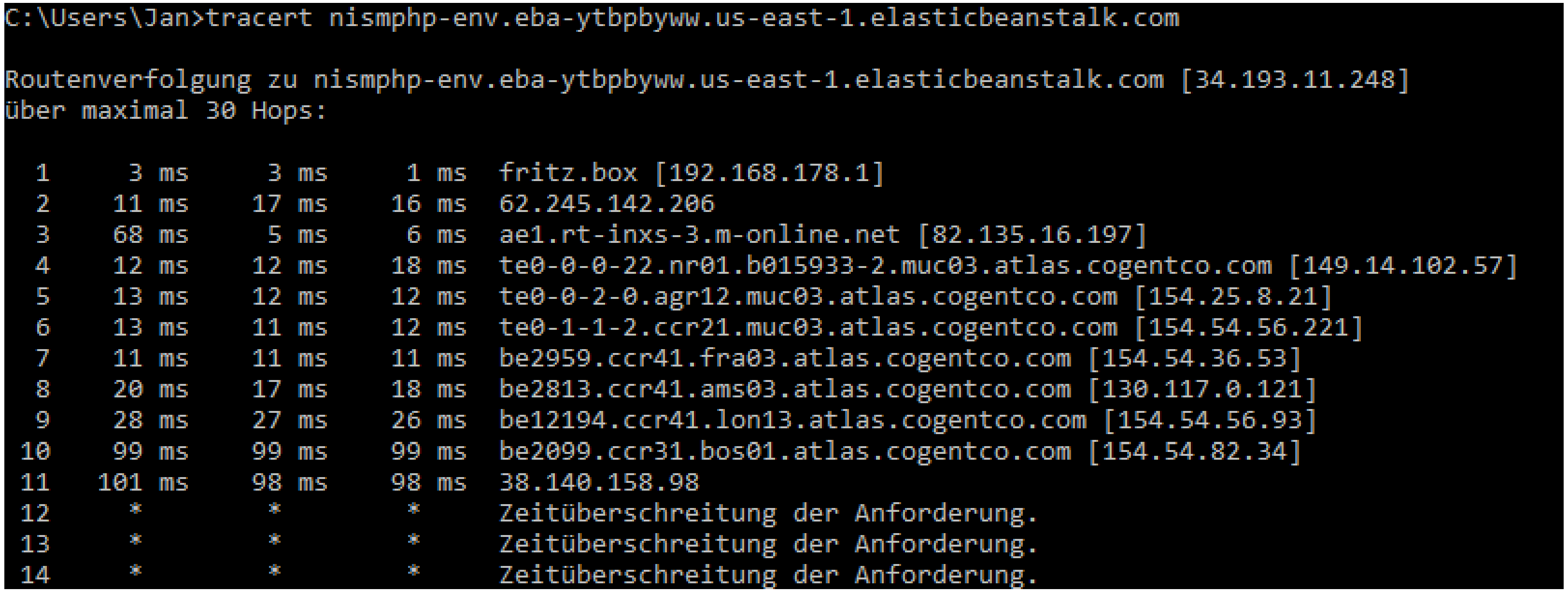
3 Question 1 - How many hops from your machine to your assigned website?



```
                    header plus 40). Can be ignored or increased to a minimal
                    allowed value
kali@kali:~$ sudo traceroute nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
traceroute to nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com (34.193.11.248), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.371 ms  0.389 ms  0.141 ms
 2  * * *
```



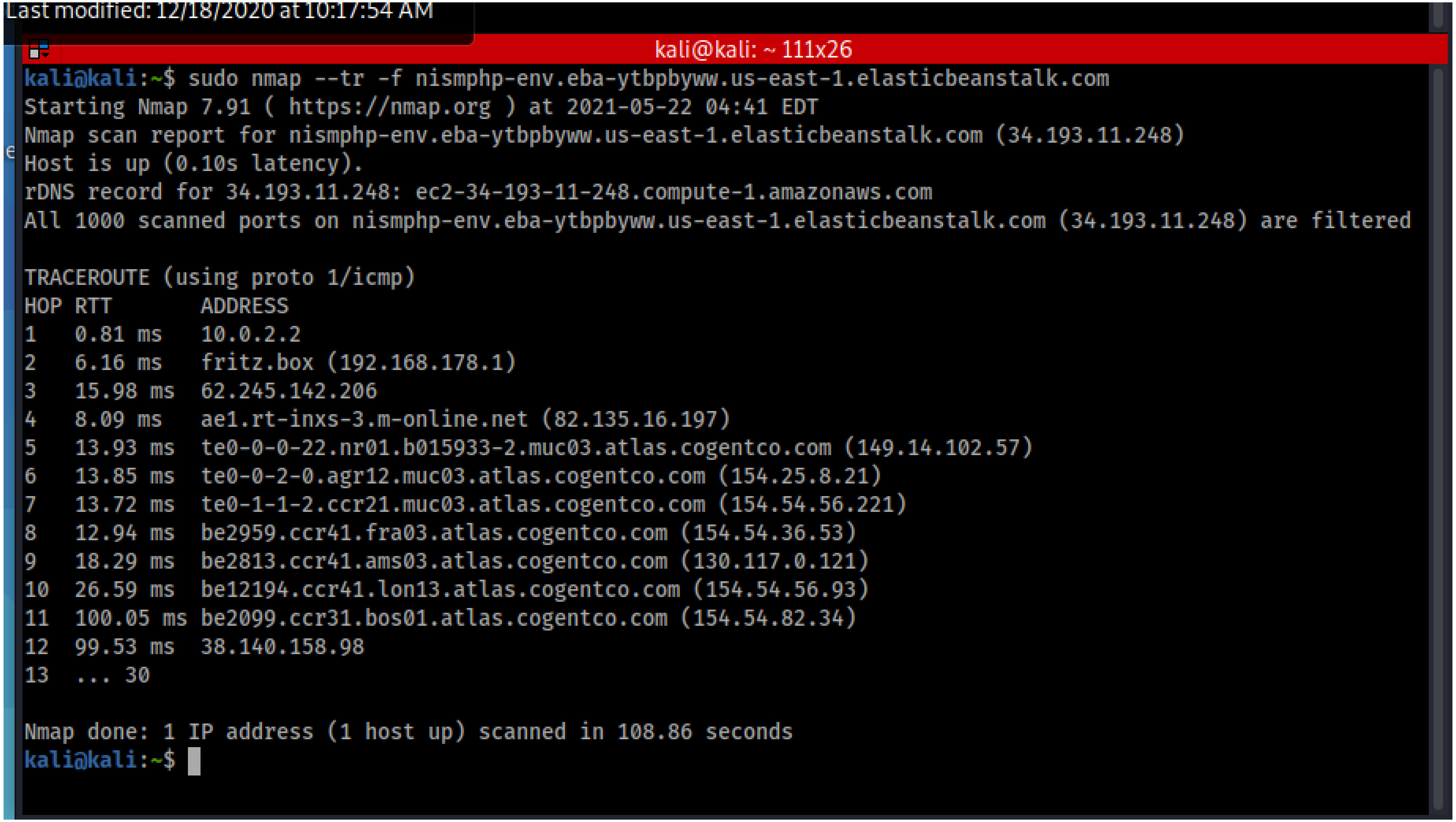
```
kali@kali:~$ sudo nmap -sn -Pn --tr nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-22 04:40 EDT
Nmap scan report for nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com (34.193.11.248)
Host is up.
rDNS record for 34.193.11.248: ec2-34-193-11-248.compute-1.amazonaws.com

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   0.91 ms   10.0.2.2
2   6.84 ms   fritz.box (192.168.178.1)
3   18.70 ms  62.245.142.206
4   9.35 ms   ae1.rt-inxs-3.m-online.net (82.135.16.197)
5   16.29 ms  te0-0-0-22.nr01.b015933-2.muc03.atlas.cogentco.com (149.14.102.57)
6   15.86 ms  te0-0-2-0.agr12.muc03.atlas.cogentco.com (154.25.8.21)
7   13.85 ms  te0-1-1-2.ccr21.muc03.atlas.cogentco.com (154.54.56.221)
8   13.18 ms  be2959.ccr41.fra03.atlas.cogentco.com (154.54.36.53)
9   19.32 ms  be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
10  27.37 ms  be12194.ccr41.lon13.atlas.cogentco.com (154.54.56.93)
11  98.99 ms  be2099.ccr31.bos01.atlas.cogentco.com (154.54.82.34)
12  100.16 ms 38.140.158.98
13  ... 30

Nmap done: 1 IP address (1 host up) scanned in 6.33 seconds
kali@kali:~$ 
```



```
C:\Users\Jan>tracert nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com

Routenverfolgung zu nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com [34.193.11.248]
über maximal 30 Hops:

  1     3 ms     3 ms     1 ms  fritz.box [192.168.178.1]
  2    11 ms    17 ms    16 ms  62.245.142.206
  3    68 ms     5 ms     6 ms  ae1.rt-inxs-3.m-online.net [82.135.16.197]
  4    12 ms    12 ms    18 ms  te0-0-0-22.nr01.b015933-2.muc03.atlas.cogentco.com [149.14.102.57]
  5    13 ms    12 ms    12 ms  te0-0-2-0.agr12.muc03.atlas.cogentco.com [154.25.8.21]
  6    13 ms    11 ms    12 ms  te0-1-1-2.ccr21.muc03.atlas.cogentco.com [154.54.56.221]
  7    11 ms    11 ms    11 ms  be2959.ccr41.fra03.atlas.cogentco.com [154.54.36.53]
  8    20 ms    17 ms    18 ms  be2813.ccr41.ams03.atlas.cogentco.com [130.117.0.121]
  9    28 ms    27 ms    26 ms  be12194.ccr41.lon13.atlas.cogentco.com [154.54.56.93]
 10    99 ms    99 ms    99 ms  be2099.ccr31.bos01.atlas.cogentco.com [154.54.82.34]
 11   101 ms    98 ms    98 ms  38.140.158.98
 12     *        *        *     Zeitüberschreitung der Anforderung.
 13     *        *        *     Zeitüberschreitung der Anforderung.
 14     *        *        *     Zeitüberschreitung der Anforderung.
```

- ➔ Traceroute does not work neither on windows nor Linux

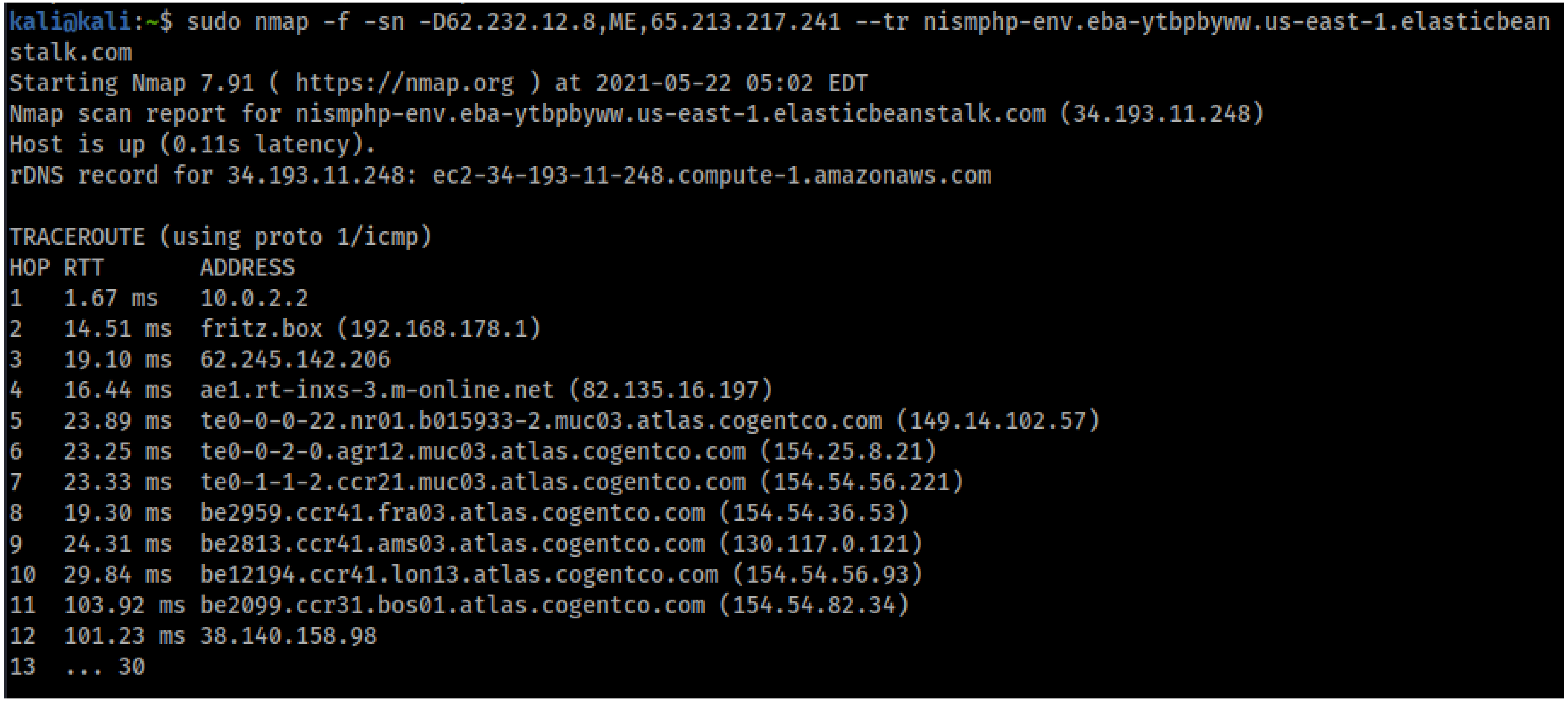
Even not with fragmented ICMP packets



Last modified: 12/18/2020 at 10:17:54 AM

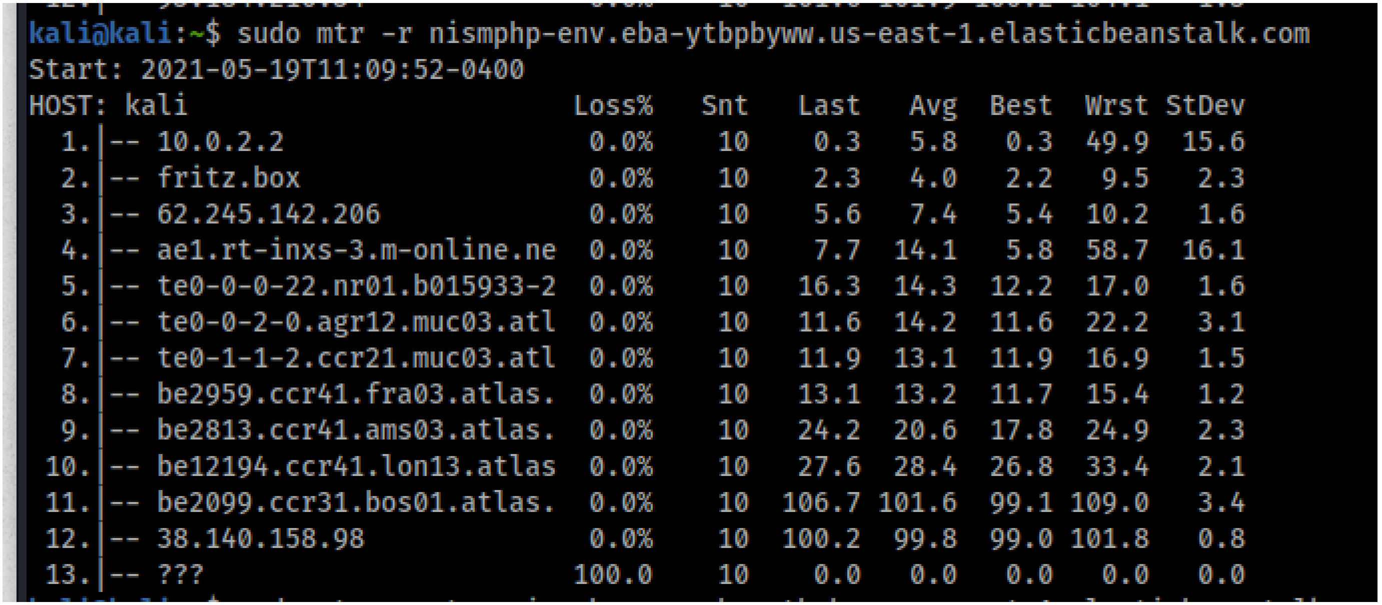
```
kali@kali:~$ sudo nmap --tr -f nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-22 04:41 EDT
Nmap scan report for nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com (34.193.11.248)
Host is up (0.10s latency).
rDNS record for 34.193.11.248: ec2-34-193-11-248.compute-1.amazonaws.com
All 1000 scanned ports on nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com (34.193.11.248) are filtered

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   0.81 ms   10.0.2.2
2   6.16 ms   fritz.box (192.168.178.1)
3   15.98 ms  62.245.142.206
4   8.09 ms   ae1.rt-inxs-3.m-online.net (82.135.16.197)
5   13.93 ms  te0-0-0-22.nr01.b015933-2.muc03.atlas.cogentco.com (149.14.102.57)
6   13.85 ms  te0-0-2-0.agr12.muc03.atlas.cogentco.com (154.25.8.21)
7   13.72 ms  te0-1-1-2.ccr21.muc03.atlas.cogentco.com (154.54.56.221)
8   12.94 ms  be2959.ccr41.fra03.atlas.cogentco.com (154.54.36.53)
9   18.29 ms  be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
10  26.59 ms  be12194.ccr41.lon13.atlas.cogentco.com (154.54.56.93)
11  100.05 ms be2099.ccr31.bos01.atlas.cogentco.com (154.54.82.34)
12  99.53 ms  38.140.158.98
13  ... 30

Nmap done: 1 IP address (1 host up) scanned in 108.86 seconds
kali@kali:~$
```

Also with fragmented packages and spoof hosting

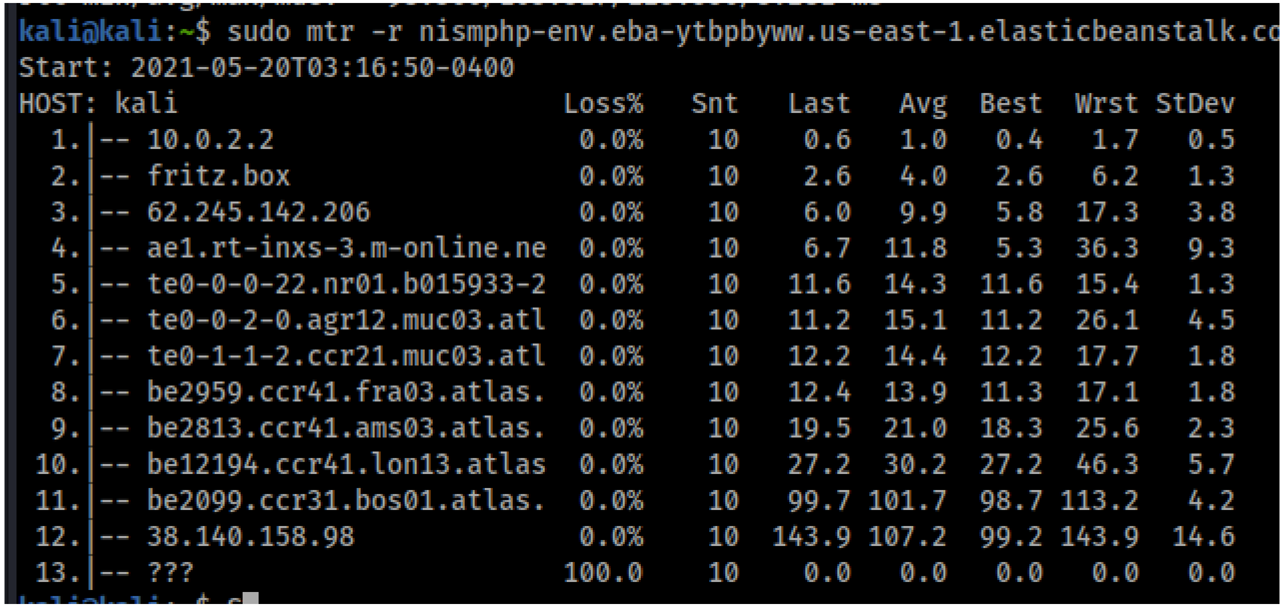


```
kali@kali:~$ sudo nmap -f -sn -D62.232.12.8,ME,65.213.217.241 --tr nismphp-env.eba-ytbpbyww.us-east-1.elasticbean
stalk.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-22 05:02 EDT
Nmap scan report for nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com (34.193.11.248)
Host is up (0.11s latency).
rDNS record for 34.193.11.248: ec2-34-193-11-248.compute-1.amazonaws.com

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   1.67 ms   10.0.2.2
2   14.51 ms  fritz.box (192.168.178.1)
3   19.10 ms  62.245.142.206
4   16.44 ms  ae1.rt-inxs-3.m-online.net (82.135.16.197)
5   23.89 ms  te0-0-0-22.nr01.b015933-2.muc03.atlas.cogentco.com (149.14.102.57)
6   23.25 ms  te0-0-2-0.agr12.muc03.atlas.cogentco.com (154.25.8.21)
7   23.33 ms  te0-1-1-2.ccr21.muc03.atlas.cogentco.com (154.54.56.221)
8   19.30 ms  be2959.ccr41.fra03.atlas.cogentco.com (154.54.36.53)
9   24.31 ms  be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
10  29.84 ms  be12194.ccr41.lon13.atlas.cogentco.com (154.54.56.93)
11  103.92 ms be2099.ccr31.bos01.atlas.cogentco.com (154.54.82.34)
12  101.23 ms 38.140.158.98
13  ... 30
```

➔ ICMP packages are very likely to be dropped

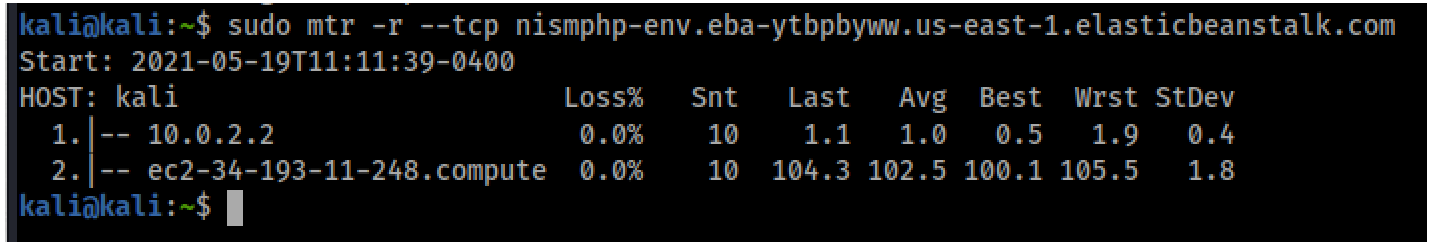


```
kali@kali:~$ sudo mtr -r nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Start: 2021-05-19T11:09:52-0400
HOST: kali                        Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 10.0.2.2                   0.0%    10    0.3   5.8   0.3  49.9  15.6
  2.|-- fritz.box                  0.0%    10    2.3   4.0   2.2   9.5   2.3
  3.|-- 62.245.142.206             0.0%    10    5.6   7.4   5.4  10.2   1.6
  4.|-- ae1.rt-inxs-3.m-online.ne  0.0%    10    7.7  14.1   5.8  58.7  16.1
  5.|-- te0-0-0-22.nr01.b015933-2  0.0%    10   16.3  14.3  12.2  17.0   1.6
  6.|-- te0-0-2-0.agr12.muc03.atl  0.0%    10   11.6  14.2  11.6  22.2   3.1
  7.|-- te0-1-1-2.ccr21.muc03.atl  0.0%    10   11.9  13.1  11.9  16.9   1.5
  8.|-- be2959.ccr41.fra03.atlas.  0.0%    10   13.1  13.2  11.7  15.4   1.2
  9.|-- be2813.ccr41.ams03.atlas.  0.0%    10   24.2  20.6  17.8  24.9   2.3
 10.|-- be12194.ccr41.lon13.atlas  0.0%    10   27.6  28.4  26.8  33.4   2.1
 11.|-- be2099.ccr31.bos01.atlas.  0.0%    10  106.7 101.6  99.1 109.0   3.4
 12.|-- 38.140.158.98              0.0%    10  100.2  99.8  99.0 101.8   0.8
 13.|-- ???                       100.0    10    0.0   0.0   0.0   0.0   0.0
```



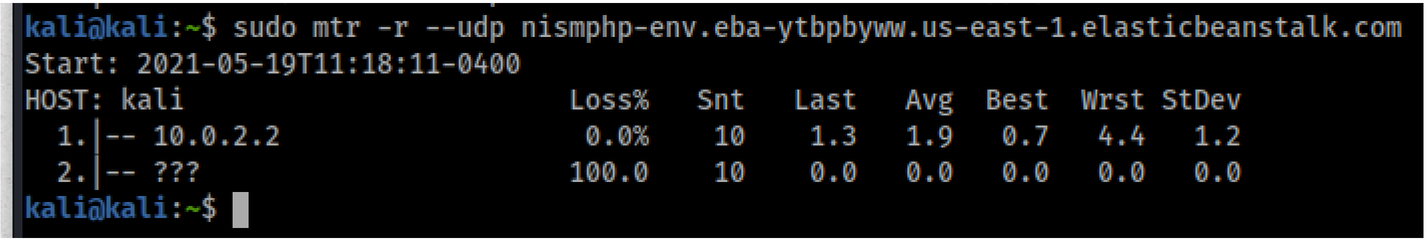
```
kali@kali:~$ sudo mtr -r nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.co
Start: 2021-05-20T03:16:50-0400
HOST: kali                        Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 10.0.2.2                   0.0%    10    0.6   1.0   0.4   1.7   0.5
  2.|-- fritz.box                  0.0%    10    2.6   4.0   2.6   6.2   1.3
  3.|-- 62.245.142.206             0.0%    10    6.0   9.9   5.8  17.3   3.8
  4.|-- ae1.rt-inxs-3.m-online.ne  0.0%    10    6.7  11.8   5.3  36.3   9.3
  5.|-- te0-0-0-22.nr01.b015933-2  0.0%    10   11.6  14.3  11.6  15.4   1.3
  6.|-- te0-0-2-0.agr12.muc03.atl  0.0%    10   11.2  15.1  11.2  26.1   4.5
  7.|-- te0-1-1-2.ccr21.muc03.atl  0.0%    10   12.2  14.4  12.2  17.7   1.8
  8.|-- be2959.ccr41.fra03.atlas.  0.0%    10   12.4  13.9  11.3  17.1   1.8
  9.|-- be2813.ccr41.ams03.atlas.  0.0%    10   19.5  21.0  18.3  25.6   2.3
 10.|-- be12194.ccr41.lon13.atlas  0.0%    10   27.2  30.2  27.2  46.3   5.7
 11.|-- be2099.ccr31.bos01.atlas.  0.0%    10   99.7 101.7  98.7 113.2   4.2
 12.|-- 38.140.158.98              0.0%    10  143.9 107.2  99.2 143.9  14.6
 13.|-- ???                       100.0    10    0.0   0.0   0.0   0.0   0.0
```

→doesn’t work either on Linux or Windows



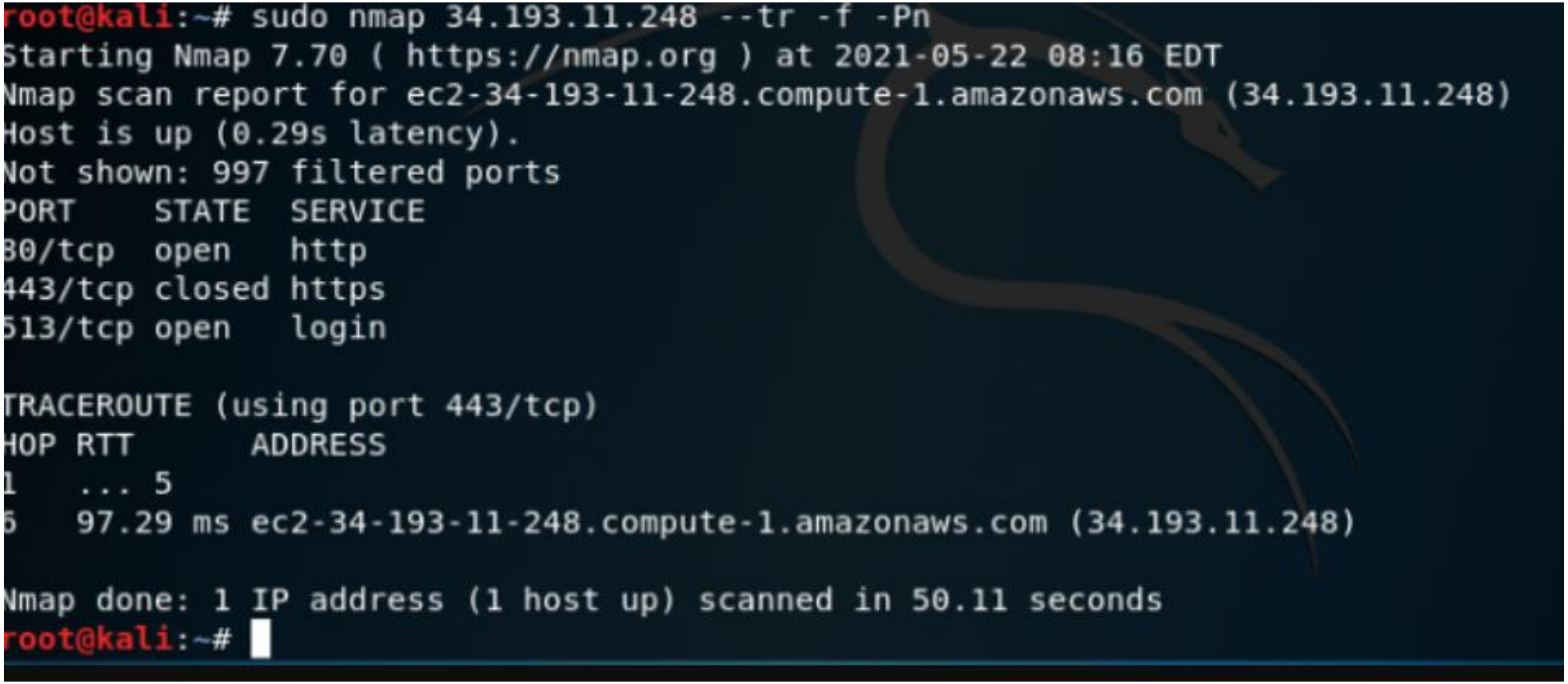
```
kali@kali:~$ sudo mtr -r --tcp nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Start: 2021-05-19T11:11:39-0400
HOST: kali                        Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 10.0.2.2                   0.0%    10    1.1   1.0   0.5   1.9   0.4
  2.|-- ec2-34-193-11-248.compute  0.0%    10  104.3 102.5 100.1 105.5   1.8
kali@kali:~$
```

→ if you use TCP packages it works 😊 however only two hops, due to possibly my NAT filtering of the router. Here a traceroute from a service seemingly not having NAT activated. It is however unclear, if this is a TCP or ICMP traceroute

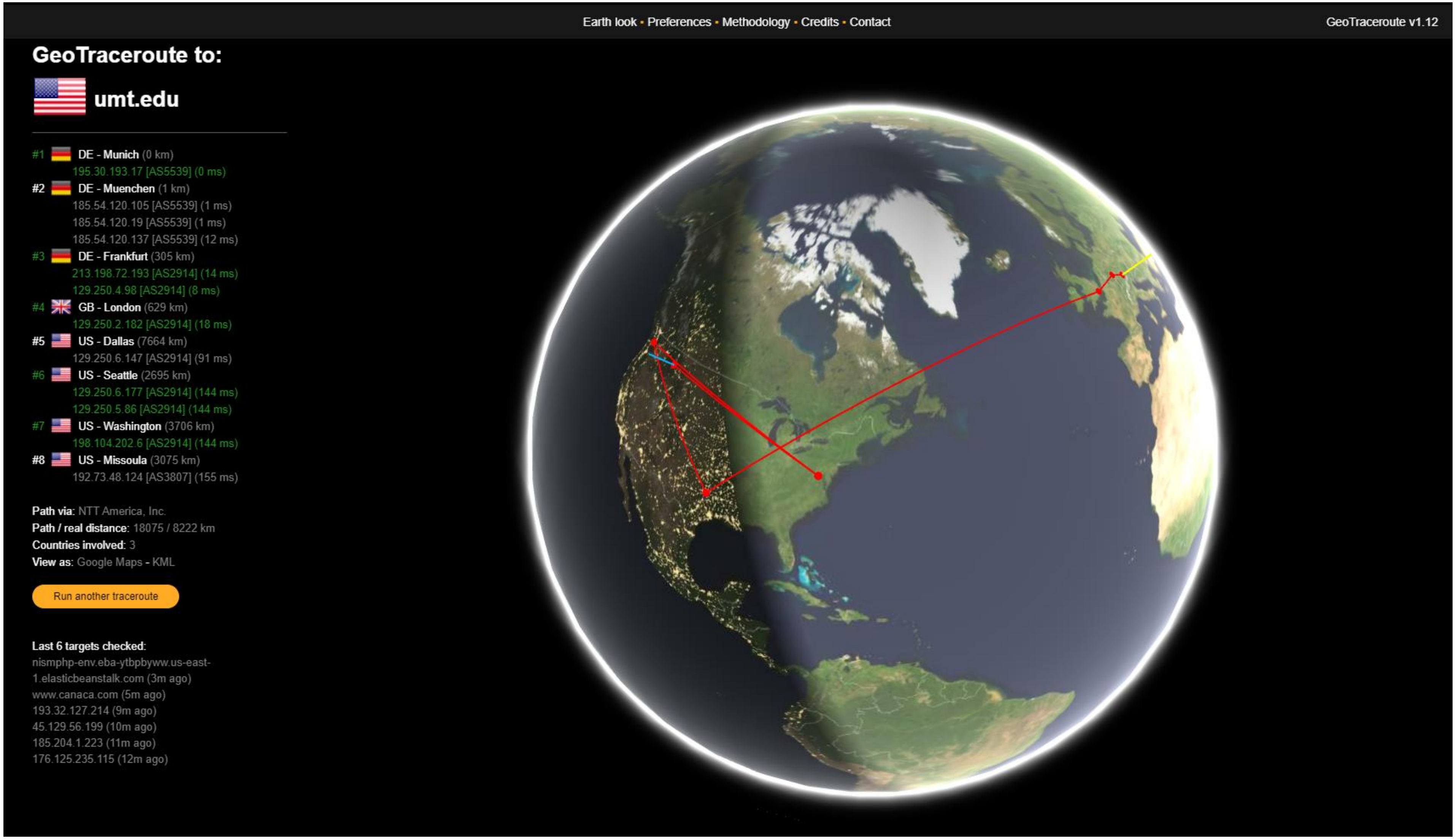


```
kali@kali:~$ sudo mtr -r --udp nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Start: 2021-05-19T11:18:11-0400
HOST: kali                        Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 10.0.2.2                   0.0%    10    1.3   1.9   0.7   4.4   1.2
  2.|-- ???                       100.0    10    0.0   0.0   0.0   0.0   0.0
kali@kali:~$
```

➔ UDP does not work either



```
root@kali:~# sudo nmap 34.193.11.248 --tr -f -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-22 08:16 EDT
Nmap scan report for ec2-34-193-11-248.compute-1.amazonaws.com (34.193.11.248)
Host is up (0.29s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
513/tcp open   login

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   ... 5
6   97.29 ms ec2-34-193-11-248.compute-1.amazonaws.com (34.193.11.248)

Nmap done: 1 IP address (1 host up) scanned in 50.11 seconds
root@kali:~#
```



GeoTraceroute to:

umt.edu

```
#1  DE - Munich (0 km)
    195.30.193.17 [AS5539] (0 ms)
#2  DE - Muenchen (1 km)
    185.54.120.105 [AS5539] (1 ms)
    185.54.120.19 [AS5539] (1 ms)
    185.54.120.137 [AS5539] (12 ms)
#3  DE - Frankfurt (305 km)
    213.198.72.193 [AS2914] (14 ms)
    129.250.4.98 [AS2914] (8 ms)
#4  GB - London (629 km)
    129.250.2.182 [AS2914] (18 ms)
#5  US - Dallas (7664 km)
    129.250.6.147 [AS2914] (91 ms)
#6  US - Seattle (2695 km)
    129.250.6.177 [AS2914] (144 ms)
    129.250.5.86 [AS2914] (144 ms)
#7  US - Washington (3706 km)
    198.104.202.6 [AS2914] (144 ms)
#8  US - Missoula (3075 km)
    192.73.48.124 [AS3807] (155 ms)
```

Path via: NTT America, Inc.
Path / real distance: 18075 / 8222 km
Countries involved: 3
View as: Google Maps - KML

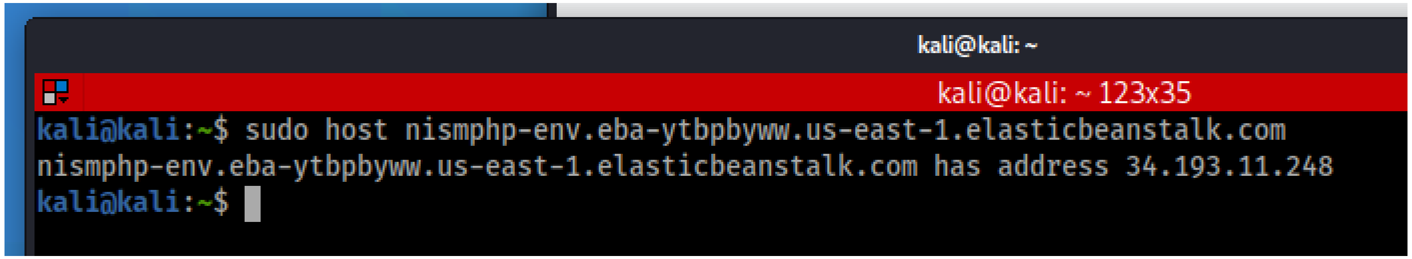
Last 6 targets checked:
nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com (3m ago)
www.canaca.com (5m ago)
193.32.127.214 (9m ago)
45.129.56.199 (10m ago)
185.204.1.223 (11m ago)
176.125.235.115 (12m ago)

4 Which step causes the biggest delay in the route? What is the average duration of that delay?

Hop 4 to 5 – GB to US

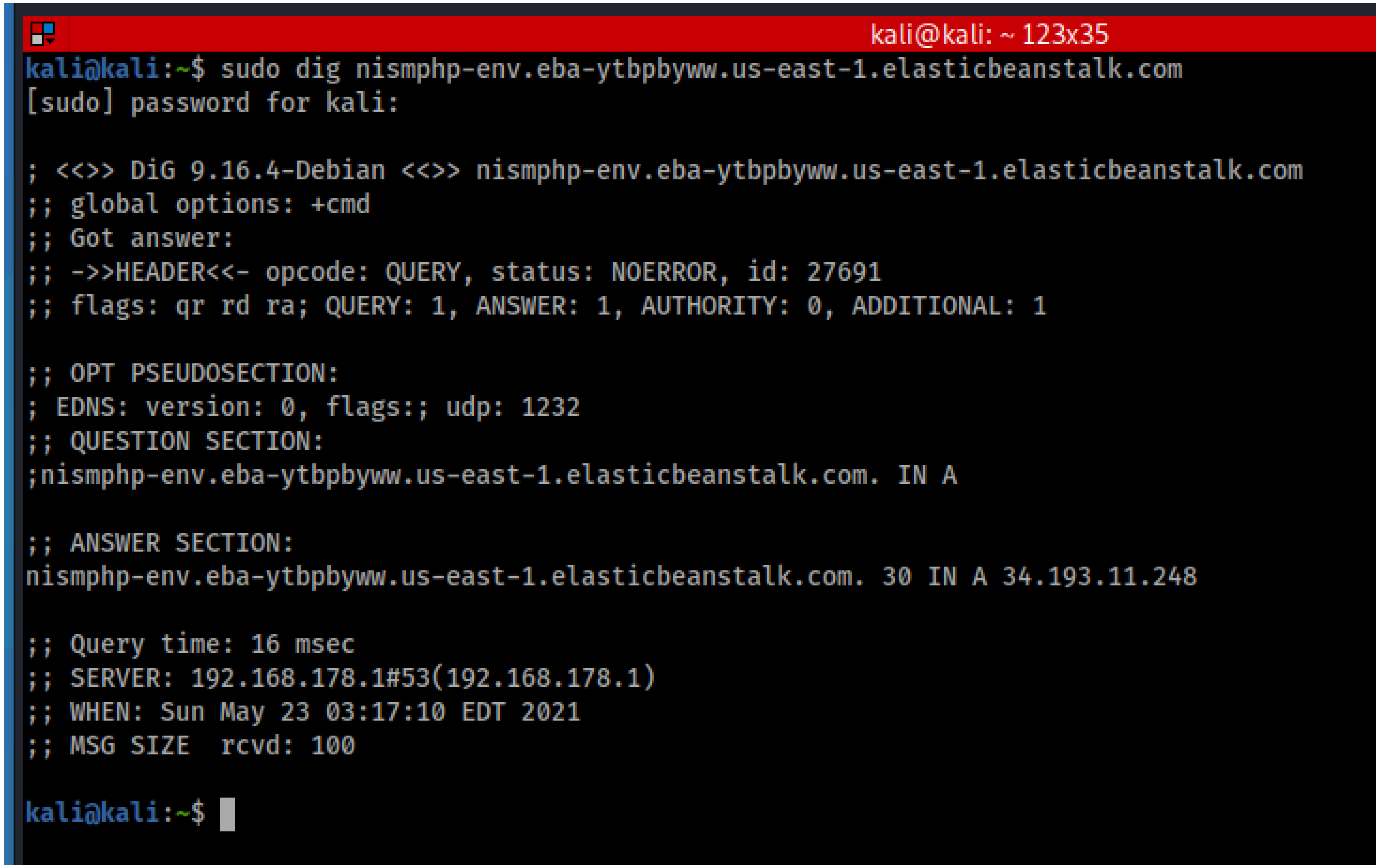
5 What are the main nameservers for the website?

5.1 Host (get-IP)



```
kali@kali:~$ sudo host nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com has address 34.193.11.248
kali@kali:~$ 
```

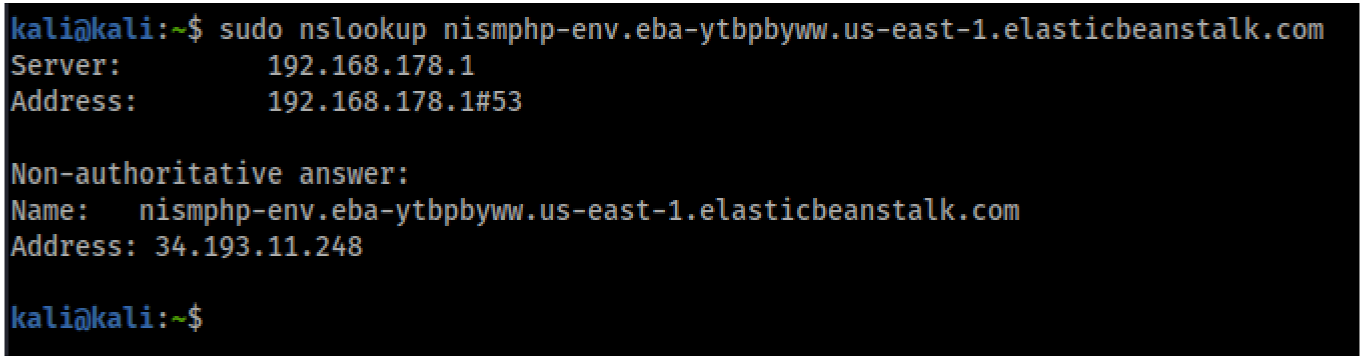
5.2 Dig



```
kali@kali:~$ sudo dig nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
[sudo] password for kali:

; <<>> DiG 9.16.4-Debian <<>> nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27691
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com. IN A

;; ANSWER SECTION:
nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com. 30 IN A 34.193.11.248

;; Query time: 16 msec
;; SERVER: 192.168.178.1#53(192.168.178.1)
;; WHEN: Sun May 23 03:17:10 EDT 2021
;; MSG SIZE  rcvd: 100

kali@kali:~$
```

→ Only one IP

5.3 Nslookup DNS querying

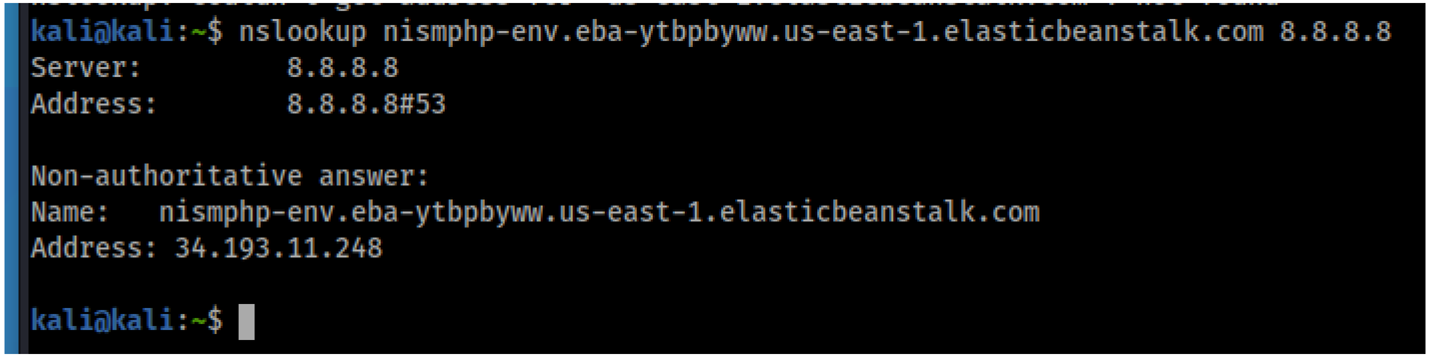


```
kali@kali:~$ sudo nslookup nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Server:         192.168.178.1
Address:        192.168.178.1#53

Non-authoritative answer:
Name:   nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Address: 34.193.11.248

kali@kali:~$
```

→Nameserver: actually my router (it seems to cache DNS lookups)

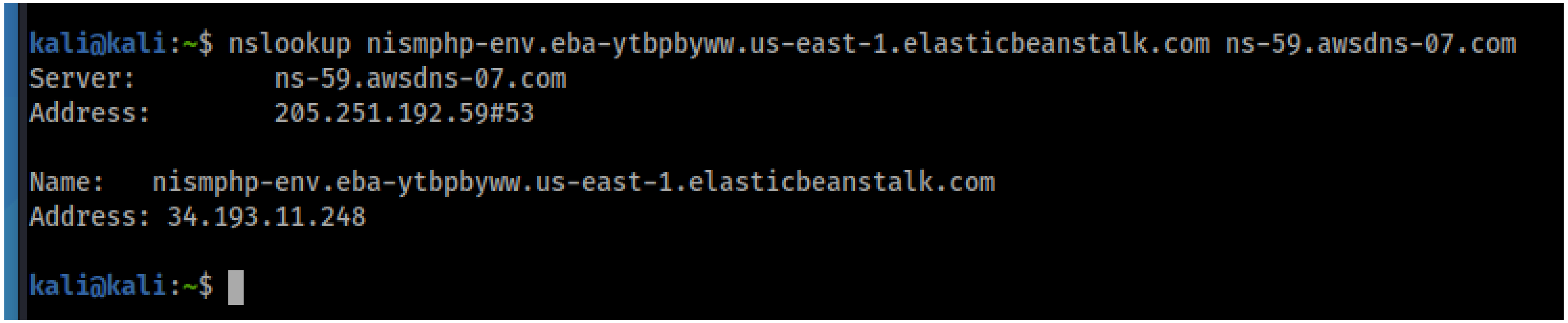
→Communicating with it at port 53

Same results with google DNS



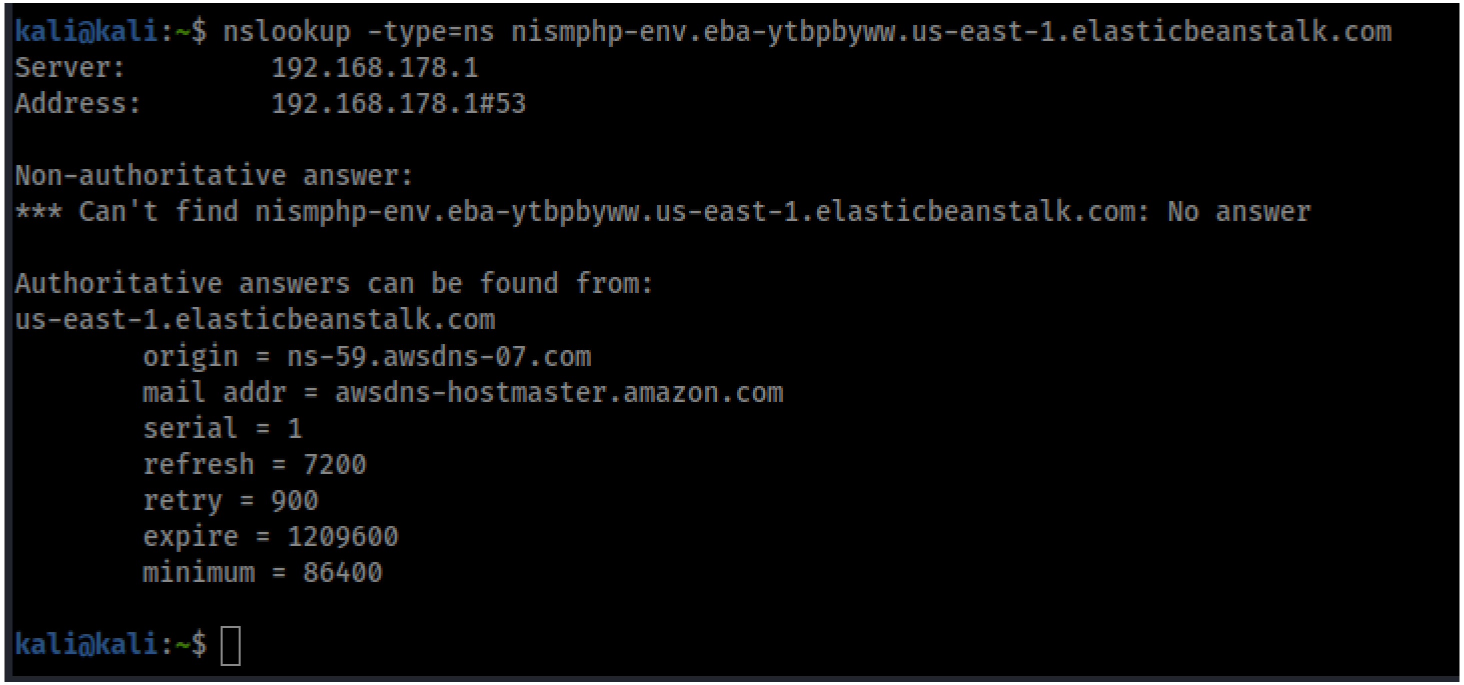
```
kali@kali:~$ nslookup nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Address: 34.193.11.248

kali@kali:~$
```

Same results with Authoritative answer:



```
kali@kali:~$ nslookup nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com ns-59.awsdns-07.com
Server:         ns-59.awsdns-07.com
Address:        205.251.192.59#53

Name:   nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Address: 34.193.11.248

kali@kali:~$ 
```

Querying for more nameservers



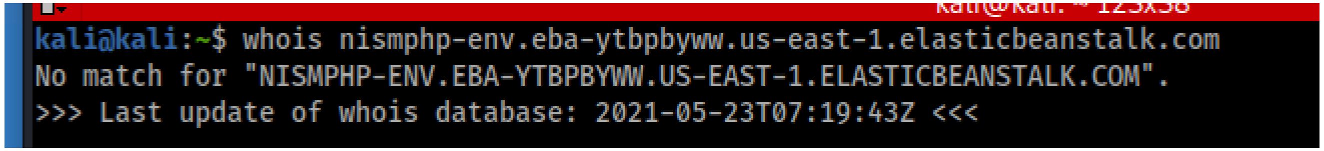
```
kali@kali:~$ nslookup -type=ns nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Server:         192.168.178.1
Address:        192.168.178.1#53

Non-authoritative answer:
*** Can't find nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com: No answer

Authoritative answers can be found from:
us-east-1.elasticbeanstalk.com
        origin = ns-59.awsdns-07.com
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400

kali@kali:~$ 
```

5.3.1 Result

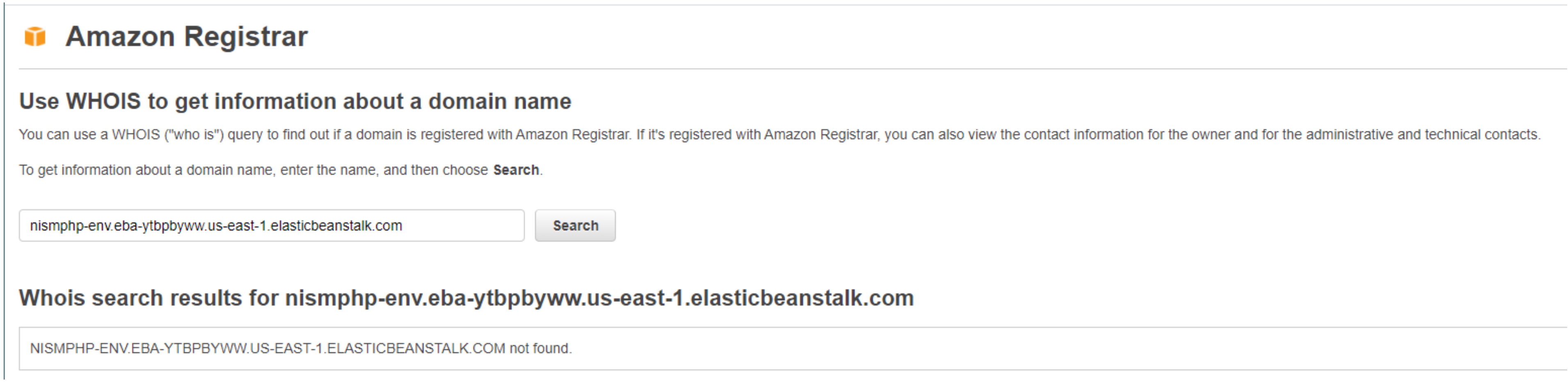
Authoritative: ns-59.awsdns-07.com

My router LOL, 8.8.8.8 (google DNS)

6 Who is the registered contact?



```
kali@kali:~$ whois nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
No match for "NISMPHP-ENV.EBA-YTBPBYWW.US-EAST-1.ELASTICBEANSTALK.COM".
>>> Last update of whois database: 2021-05-23T07:19:43Z <<<
```



Amazon Registrar

Use WHOIS to get information about a domain name

You can use a WHOIS ("who is") query to find out if a domain is registered with Amazon Registrar. If it's registered with Amazon Registrar, you can also view the contact information for the owner and for the administrative and technical contacts.

To get information about a domain name, enter the name, and then choose **Search**.

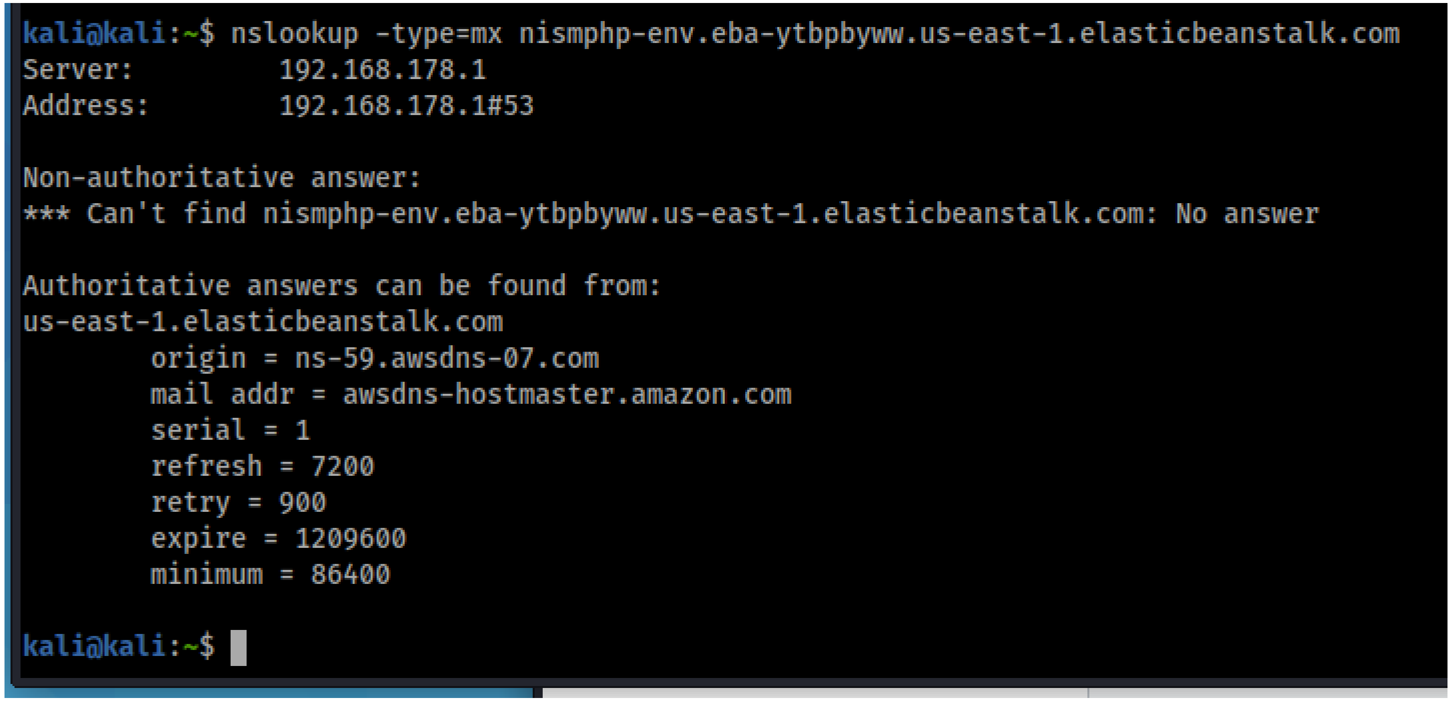
nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com

Whois search results for nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com

NISMPHP-ENV.EBA-YTBPBYWW.US-EAST-1.ELASTICBEANSTALK.COM not found.

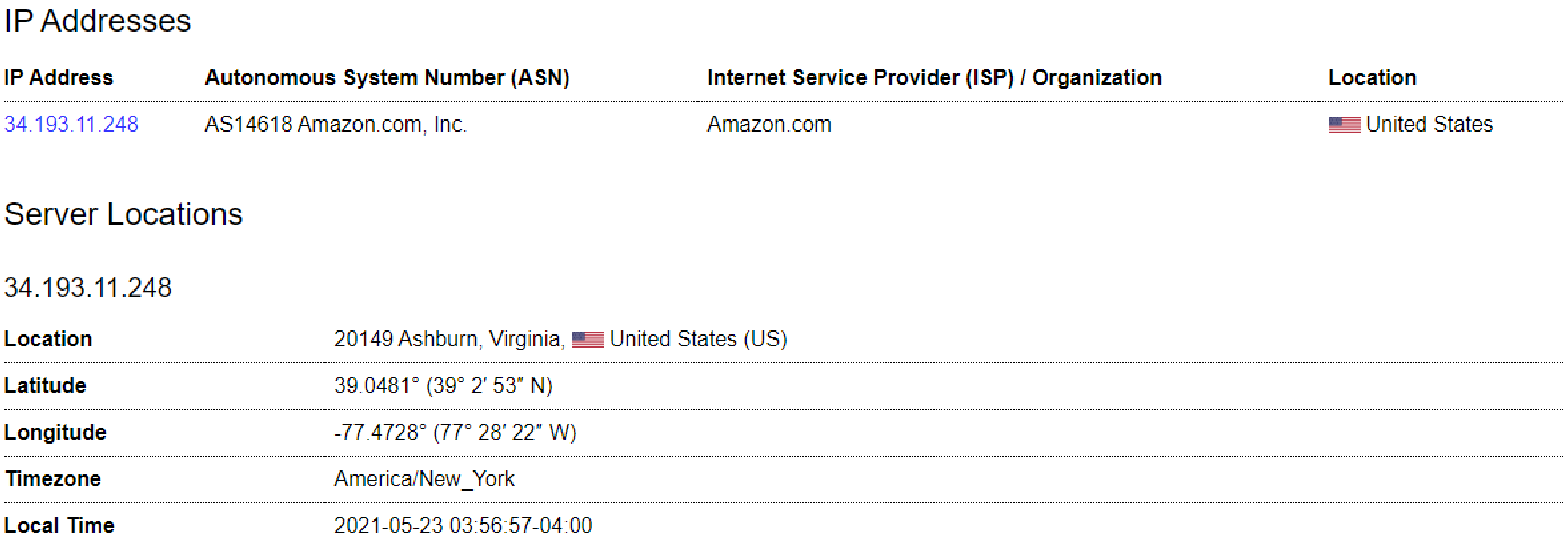
https://registrar.amazon.com/whois?domain=nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com

7 What is the MX record for the website?



```
kali@kali:~$ nslookup -type=mx nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com
Server:         192.168.178.1
Address:        192.168.178.1#53

Non-authoritative answer:
*** Can't find nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com: No answer

Authoritative answers can be found from:
us-east-1.elasticbeanstalk.com
        origin = ns-59.awsdns-07.com
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400

kali@kali:~$
```

8 Where is the website hosted?



IP Addresses

IP Address	Autonomous System Number (ASN)	Internet Service Provider (ISP) / Organization	Location
34.193.11.248	AS14618 Amazon.com, Inc.	Amazon.com	United States

Server Locations

34.193.11.248

Location	20149 Ashburn, Virginia, United States (US)
Latitude	39.0481° (39° 2′ 53″ N)
Longitude	-77.4728° (77° 28′ 22″ W)
Timezone	America/New_York
Local Time	2021-05-23 03:56:57-04:00

Ip-adress.com