

Assignment Series #A2 Traceroute

1. Task description

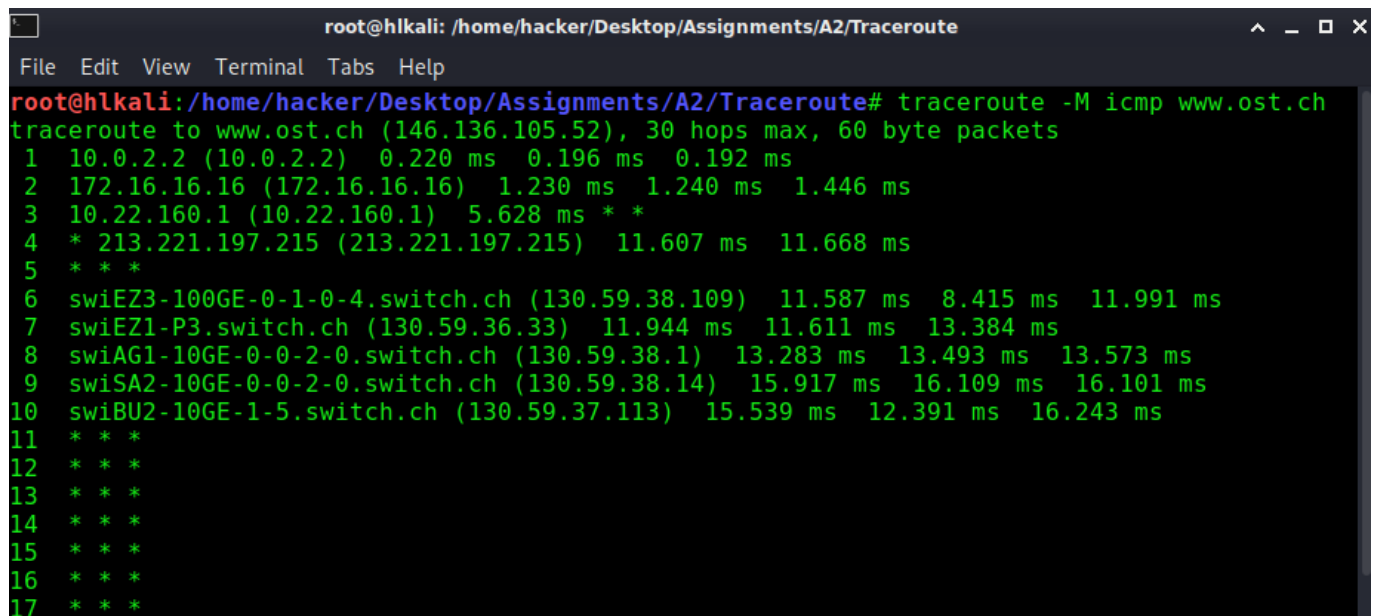
The Linux command `traceroute` shows how data transmission travelled from a local machine to a remote one. A typical example would be loading a web page over the internet that involves data flowing through a network and a number of routers. The `traceroute` command can show the route taken and the IP and hostnames of routers on the network. It can be useful for understanding latency or diagnosing network issues.

After getting familiar with the command `traceroute`, please list and run the following `traceroute` commands:

1. `traceroute icmp www.ost.ch`
2. `traceroute tcp port 443 www.ost.ch` with ASN resolution and disabled dns resolution
3. `traceroute udp port 53` for `ns1.compass-security.com` and `ns2.compass-security.com`

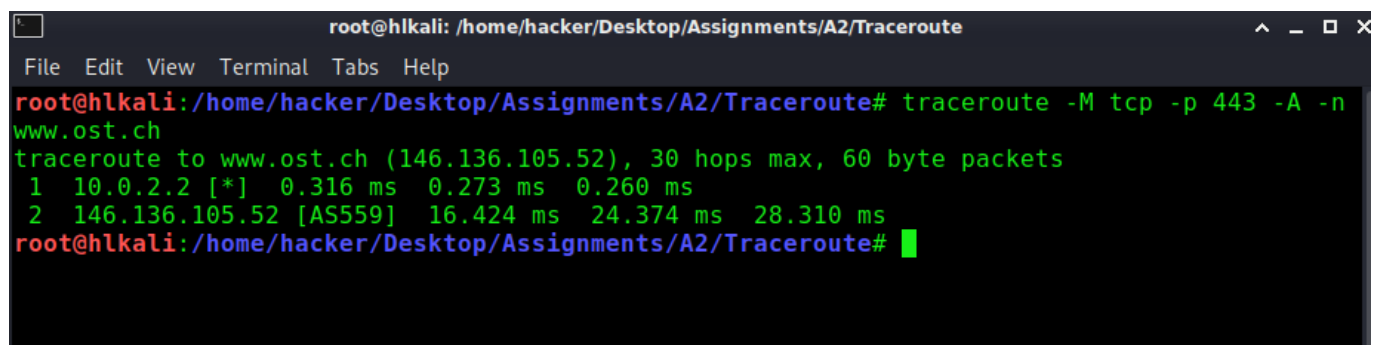
2. Solution

1. Syntax of `traceroute` command is: `traceroute -M icmp www.ost.ch`



```
root@hlkali: /home/hacker/Desktop/Assignments/A2/Traceroute
File Edit View Terminal Tabs Help
root@hlkali: /home/hacker/Desktop/Assignments/A2/Traceroute# traceroute -M icmp www.ost.ch
traceroute to www.ost.ch (146.136.105.52), 30 hops max, 60 byte packets
 1 10.0.2.2 (10.0.2.2) 0.220 ms 0.196 ms 0.192 ms
 2 172.16.16.16 (172.16.16.16) 1.230 ms 1.240 ms 1.446 ms
 3 10.22.160.1 (10.22.160.1) 5.628 ms * *
 4 * 213.221.197.215 (213.221.197.215) 11.607 ms 11.668 ms
 5 * * *
 6 swiEZ3-100GE-0-1-0-4.switch.ch (130.59.38.109) 11.587 ms 8.415 ms 11.991 ms
 7 swiEZ1-P3.switch.ch (130.59.36.33) 11.944 ms 11.611 ms 13.384 ms
 8 swiAG1-10GE-0-0-2-0.switch.ch (130.59.38.1) 13.283 ms 13.493 ms 13.573 ms
 9 swiSA2-10GE-0-0-2-0.switch.ch (130.59.38.14) 15.917 ms 16.109 ms 16.101 ms
10 swiBU2-10GE-1-5.switch.ch (130.59.37.113) 15.539 ms 12.391 ms 16.243 ms
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
```

2. Syntax of `traceroute` command is: `traceroute -M tcp -p 443 -A -n www.ost.ch`



```
root@hlkali: /home/hacker/Desktop/Assignments/A2/Traceroute
File Edit View Terminal Tabs Help
root@hlkali: /home/hacker/Desktop/Assignments/A2/Traceroute# traceroute -M tcp -p 443 -A -n
www.ost.ch
traceroute to www.ost.ch (146.136.105.52), 30 hops max, 60 byte packets
 1 10.0.2.2 [*] 0.316 ms 0.273 ms 0.260 ms
 2 146.136.105.52 [AS559] 16.424 ms 24.374 ms 28.310 ms
root@hlkali: /home/hacker/Desktop/Assignments/A2/Traceroute#
```

3. Syntax of `traceroute` command is:
 - `traceroute -M udp -p 53 ns1.compass-security.com`

- `tracertoute -M udp -p 53 ns2.compass-security.com`

```

root@hlkali:/home/hacker/Desktop/Assignments/A2/Traceroute# tracertoute -M udp -p 53 ns1.com
pass-security.com
tracertoute to ns1.compass-security.com (193.135.215.40), 30 hops max, 60 byte packets
 1 10.0.2.2 (10.0.2.2) 0.328 ms 0.552 ms 0.510 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 grobi.compass-security.com (193.135.215.40) 17.137 ms * 17.082 ms
root@hlkali:/home/hacker/Desktop/Assignments/A2/Traceroute# tracertoute -M udp -p 53 ns2.com
pass-security.com
tracertoute to ns2.compass-security.com (80.74.140.181), 30 hops max, 60 byte packets
 1 10.0.2.2 (10.0.2.2) 0.375 ms 0.312 ms 0.264 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 urb80-74-140-181.ch-meta.net (80.74.140.181) 14.132 ms 9.375 ms 9.329 ms
root@hlkali:/home/hacker/Desktop/Assignments/A2/Traceroute# █

```

3. Command Switches and Comments

- M protocol
- p port
- A with ASN resolution
- n with disabled dns resolution

www.ost.ch is blocking icmp requests

```

~
ping www.ost.ch
PING web02.ost.ch (146.136.105.52) 56(84) bytes of data.
^C
--- web02.ost.ch ping statistics ---
17 packets transmitted, 0 received, 100% packet loss, time 16362ms

~ 1 x 17s

```

hop Nr. 10 is the last answer before the firewall

```
10 swiBU2-10GE-1-5.switch.ch (130.59.37.113) 58.086 ms 58.309 ms 57.991 ms
```

Just a short repetition from the OSINT exercise howto get the ASN and compare it with the traceroute output:

```

~ /Desktop/Assignments/A2/Traceroute ✓
└─ dig +short www.ost.ch
web02.ost.ch.
146.136.105.52

~ /Desktop/Assignments/A2/Traceroute ✓
└─ whois -h riswhois.ripe.net '146.136.105.52' | egrep -i "origin|desc"

```

```
% IPv4 or IPv6 address to origin prefix match  
origin: AS559  
descr: SWITCH SWITCH, EU  
  
└─ ~/Desktop/Assignments/A2/Traceroute ✓  
└─
```

Instead of using `traceroute -M udp -p 53`, I can also use `traceroute -U` which give me the same result.