Assignment Series #A2 Traceroute

1. Task description

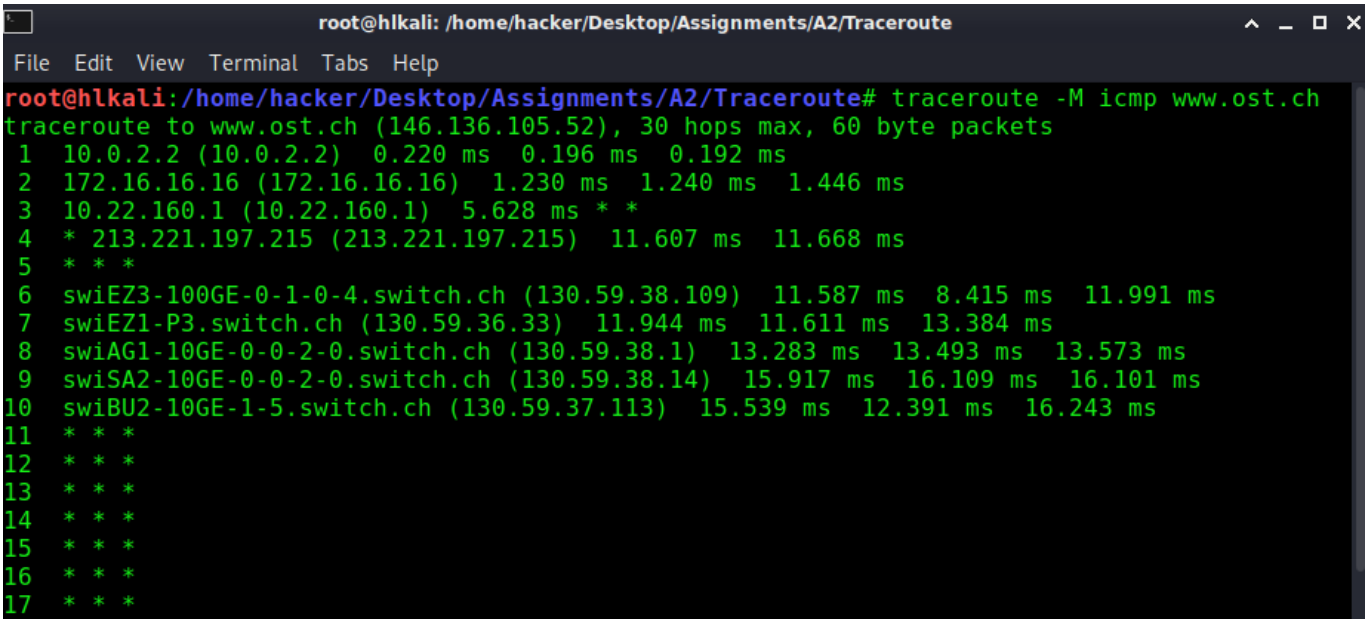
The Linux command traceroute shows how data transmission travelled from a local machine to a remote one. A typical example would be loading a web page over the internet that involves data flowing through a network and a number of routers. The traceroute command can show the route taken and the IP and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

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

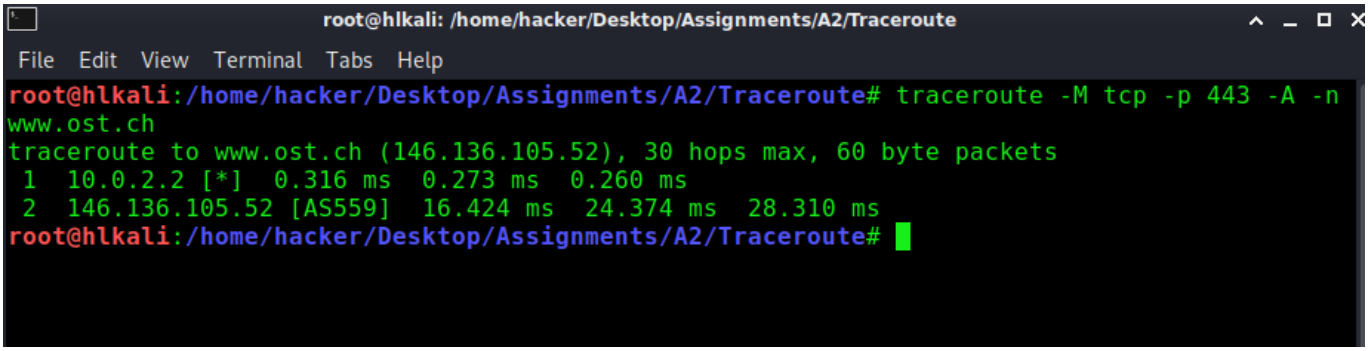
1. traceroute icmp www.ost.ch
2. traceroute tcp port 443 www.ost.ch with ASN resolution and disabled dns resolution
3. traceroute udp port 53 for ns1.compass-security.com and ns2.compass-security.com

2. Solution

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



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



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

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

```
root@hlkali:/home/hacker/Desktop/Assignments/A2/Traceroute# traceroute -M udp -p 53 ns1.com
pass-security.com
traceroute 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# traceroute -M udp -p 53 ns2.com
pass-security.com
traceroute 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 ✘  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.