Path tracing with tracebox
MAMI summer school

Korian Edeline, Justin Iurman
University of Liège
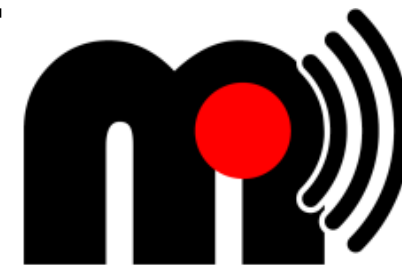
Milestone 2

Ping destination (10.0.0.10)

Traceroute

```
vagrant@mmb-tutorial:~$ sudo scamper -c trace -i 10.0.0.10
traceroute from 10.100.100.1 to 10.0.0.10
 1    10.100.100.2    20.827 ms
 2    10.202.129.2   154.803 ms
 3    30.1.3.3       203.855 ms
 4    30.0.5.7       173.032 ms
 5    20.55.55.6     366.602 ms
 6    30.101.0.6     323.826 ms
 7    30.111.2.2     269.028 ms
 8    10.0.0.10      385.667 ms
vagrant@mmb-tutorial:~$ sudo scamper -c trace -i 10.0.0.10
traceroute from 10.100.100.1 to 10.0.0.10
 1    10.100.100.2     6.053 ms
 2    10.202.129.2    95.930 ms
 3    30.0.3.3       107.594 ms
 4    30.1.2.13      283.031 ms
 5    20.55.55.6     402.940 ms
 6    30.101.0.6     188.789 ms
 7    30.111.2.2     675.775 ms
 8    10.0.0.10      479.871 ms
vagrant@mmb-tutorial:~$
```

Paris Traceroute

```
vagrant@mmb-tutorial:~$ sudo scamper -c tracelb -i 10.0.0.10
tracelb from 10.100.100.1 to 10.0.0.10, 6 nodes, 5 links, 49 probes, 95%
10.100.100.2 -> 10.202.129.2
10.202.129.2 -> (30.0.3.3, 30.1.3.3) -> (30.0.5.7, 30.1.2.13) -> 20.55.55.6
20.55.55.6 -> 30.101.0.6
30.101.0.6 -> 30.111.2.2
30.111.2.2 -> 10.0.0.10
vagrant@mmb-tutorial:~$
```

Middlebox

TCP Normalizer

```
vagrant@mmb-tutorial:~$ sudo python3 simple_tracebox.py 10.0.0.10
1:   10.100.100.2
options    : TCPOptionsField                    = [('WScale', 18), ('EOL', None)] ([])
6:   30.101.0.6
options    : TCPOptionsField                    = [('WScale', 14), ('EOL', None)] ([])
```

Rule	Match	Action
1	ip-proto == **UDP**	**ip-dscp = 14**
2	ip-proto == **ICMP**	**ip-dscp = 0**
3	ip-proto == **TCP**	**ip-dscp = 10** **Strip all TCP options but MSS, WScale**
4	ip-proto == **TCP (SYN flag)**	**MSS = 1460 (if found)** **Wscale = 14 (if found)**

Firewall

```
vagrant@mmb-tutorial:~$ sudo scamper -c "ping -P tcp-syn -d 53" -i 10.0.0.10
ping 10.100.100.1 to 10.0.0.10: 40 byte packets
--- 10.0.0.10 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
vagrant@mmb-tutorial:~$
```

```
vagrant@mmb-tutorial:~$ sudo scamper -c "ping -P udp -d 53" -i 10.0.0.10
ping 10.100.100.1 to 10.0.0.10: 40 byte packets
68 bytes from 10.0.0.10, seq=0 ttl=57 time=532.856 ms
68 bytes from 10.0.0.10, seq=1 ttl=57 time=532.616 ms
68 bytes from 10.0.0.10, seq=2 ttl=57 time=309.521 ms
68 bytes from 10.0.0.10, seq=3 ttl=57 time=407.359 ms
--- 10.0.0.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 309.521/445.588/532.856/93.762 ms
vagrant@mmb-tutorial:~$
```

Firewall (cont.)

Ports	UDP	TCP
25, 53, 445	✓	✗
80, 443, 8000, 8080	✗	✓
135, 139, 161, 162	✗	✗

Topology

Host

.1

10.100.100.0/24

.2

.13   .2

Router

10.202.129.0/24   Load
                         Balancer

.1

.3

30.0.3.0/24   Router   30.0.5.0/24

.2   .3

30.1.3.0/24   Router

.5   .13

30.1.2.0/24

.7

.1

Load
Balancer

.6

20.55.55.0/24

Router

.2.3

30.101.0.0/16

.6

.10   .11   .2   .3

Destination   10.0.0.0/24   Firewall   30.111.2.0/24   Middlebox