ETraceRoute

ETrace

ETrace is a traceroute variant with customizable probe packets. It supports various protocols (ICMP, TCP, UDP and other IP protocols). A lot of the IP/TCP /UDP header fields and flags can be specified, as well as the data carried in the probe packets (e.g. one can run ETrace with DNS queries as the probe packets).

Example

```
root@sunbow:~# etrace --udp 53 --data-file @dns ns2.cisco.com
Starting udp/53 trace to 64.102.255.44
 1: 152.66.115.254 (vlan100.taz.bme.hu) [TTL Exceeded - TTL=255]
 2: 152.66.0.126 (tge2-2.sup720.bme.hbone.hu) [TTL Exceeded - TTL=254]
 3: 195.111.97.101 (c6513-tengbeth13-2.vh.hbone.hu) [TTL Exceeded - TTL=253]
 4: 195.111.97.241 (gsr16-gbeth10-0.vh.hbone.hu) [TTL Exceeded - TTL=252]
 5: 62.40.103.25 (hungarnet.hu1.hu.geant.net) [TTL Exceeded - TTL=250]
 6: 213.248.103.61 (bpt-b2-pos10-0.telia.net) [TTL Exceeded - TTL=250]
 7: 213.248.64.17 (hbg-bb1-pos7-2-2.telia.net) [TTL Exceeded - TTL=248]
 8: 80.91.249.10 (ldn-bb1-link.telia.net) [TTL Exceeded - TTL=246]
 9: 213.248.65.149 (ldn-bb1-pos7-0-0.telia.net) [TTL Exceeded - TTL=246]
10: 80.91.249.249 (nyk-bb1-link.telia.net) [TTL Exceeded - TTL=245]
11: 213.248.80.142 (atl-bb1-link.telia.net) [TTL Exceeded - TTL=243]
12: 213.248.80.142 (atl-bb1-link.telia.net) [TTL Exceeded - TTL=243]
13: 192.205.33.41 (ggr2-p3121.attga.ip.att.net) [TTL Exceeded - TTL=243]
14: 12.122.3.57 (gar1-p360.rlgnc.ip.att.net) [TTL Exceeded - TTL=241]
15: 12.119.93.78 (??) [TTL Exceeded - TTL=240]
16: 64.102.254.234 (rtp5-dmzbb-gw1.cisco.com) [TTL Exceeded - TTL=240]
17: 64.102.254.234 (rtp5-dmzbb-gw1.cisco.com) [TTL Exceeded - TTL=240]
18: 64.102.244.14 (rtp5-dmzdc-gw2-g1-1.cisco.com) [TTL Exceeded - TTL=240]
19: 64.102.255.44 (ns2.cisco.com) [UDP Packet - TTL=47]
root@sunbow:~#
```

The above etrace uses DNS query packets (payload provided with etrace as an example). This could help traversing firewalls, although in case of TCP probe packets, usually a normal SYN segment without any payload will be sufficient.

References

- http://www.bindshell.net/tools/etrace/

– Main.AndrasJako - 30 Aug 2006