

Blocking by firewall

This is how we debugged a problem with gathering data from comsatsswl.seecs.edu.pk

The following works from pingman@brunsvigia.tenet.ac.za (196.21.99.222), from my home and from cottrell@rhel6-64d.slac.stanford.edu (134.79.120.158), lnxcron.slac.stanford.edu (134.79.196.17)

```
pingman@brunsvigia:~> /usr/bin/wget --verbose --tries=1 -O - --timeout=60 'http://comsatsswl.seecs.edu.pk:8080/cgi-bin/ping_data.pl?in_form=1&begin_hour=16&begin_min=00&begin_sec=00&begin_day=07&begin_month=12&begin_year=2016&begin_offset=&begin_point=y&end_hour=23&end_min=59&end_sec=59&end_day=07&end_month=12&end_year=2016&end_offset=&end_point=y'
```

The following also works from ocio-90575.win.slac.stanford.edu (134.79.80.11):

```
http://comsatsswl.seecs.edu.pk:8080/cgi-bin/ping_data.pl?in_form=1&begin_hour=00&begin_min=00&begin_sec=00&begin_day=7&begin_month=12&begin_year=2016&begin_offset=&begin_point=y&end_hour=23&end_min=59&end_sec=00&end_day=08&end_month=12&end_year=2016&end_offset=&end_point=y
```

However the following fails from cottrell@pinger.slac.stanford.edu (134.79.104.80) and pinger@pinger.slac.stanford.edu

```
317cottrell@pinger:~$ /usr/bin/wget --verbose --tries=1 -O - --timeout=60 'http://comsatsswl.seecs.edu.pk:8080/cgi-bin/ping_data.pl?in_form=1&begin_hour=16&begin_min=00&begin_sec=00&begin_day=07&begin_month=12&begin_year=2016&begin_offset=&begin_point=y&end_hour=23&end_min=59&end_sec=59&end_day=07&end_month=12&end_year=2016&end_offset=&end_point=y'
```

```
--2016-12-08 09:39:40-- http://comsatsswl.seecs.edu.pk:8080/cgi-bin/ping_data.pl?in_form=1&begin_hour=16&begin_min=00&begin_sec=00&begin_day=07&begin_month=12&begin_year=2016&begin_offset=&begin_point=y&end_hour=23&end_min=59&end_sec=59&end_day=07&end_month=12&end_year=2016&end_offset=&end_point=y
```

Resolving comsatsswl.seecs.edu.pk... 111.68.104.98

Connecting to comsatsswl.seecs.edu.pk[111.68.104.98]:8080... failed: Connection timed out.

Giving up.

Exit 4

Also the following fails:

```
320cottrell@pinger:~$ wget 'http://comsatsswl.seecs.edu.pk:8080/cgi-bin/traceroute.pl'
```

```
--2016-12-08 10:15:33-- http://comsatsswl.seecs.edu.pk:8080/cgi-bin/traceroute.pl
```

Resolving comsatsswl.seecs.edu.pk... 111.68.104.98

Connecting to comsatsswl.seecs.edu.pk[111.68.104.98]:8080... failed: Connection timed out.

Retrying.

```
--2016-12-08 10:16:37-- (try: 2) http://comsatsswl.seecs.edu.pk:8080/cgi-bin/traceroute.pl
```

Connecting to comsatsswl.seecs.edu.pk[111.68.104.98]:8080... failed: Connection timed out.

Retrying.

```
--2016-12-08 10:17:42-- (try: 3) http://comsatsswl.seecs.edu.pk:8080/cgi-bin/traceroute.pl
```

Connecting to comsatsswl.seecs.edu.pk[111.68.104.98]:8080... failed: Connection timed out.

Retrying.

```
--2016-12-08 10:18:48-- (try: 4) http://comsatsswl.seecs.edu.pk:8080/cgi-bin/traceroute.pl
```

Connecting to comsatsswl.seecs.edu.pk[111.68.104.98]:8080... ^C

iptables shows no blocking rules

```
337cottrell@pinger:~$ sudo iptables -L
```

```
[sudo] password for cottrell:
```

```
Chain INPUT (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain FORWARD (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target prot opt source destination
```

N.b pinger is on subnet http://network.slac.stanford.edu/hosts/on_subnet?name=SERV01-DMZ-IEPM (134.79.104.64/26)

Using the splunk query

```
index=pan_logs type=TRAFFIC
```

```
src_ip=134.79.104.80 dst_ip=111.68.104.98
```

```
|stats values(rule_name),values(src_ip),values(client_location),values(dst_ip), values(action),values(dst_port),values(protocol) count by application|rename comment AS "misc"
```

Turns out this subnet does not enable port 8080.

We requested opening port 8080 outbound from [SERV01-DMZ-IEPM](http://network.slac.stanford.edu/hosts/on_subnet?name=SERV01-DMZ-IEPM) via [ServiceNow ticket](#) INC0123421