DNS2TCP

Oder: Tunnelgraben für Fortgeschrittene

29. 1. 2010

Jannis Andrija Schnitzer

Bild: telmo32 @ Flickr

Gliederung

- Motivation und Zielsetzung
- Funktionsweise
- Installation und Konfiguration
- Demo

Motivation und Zielsetzung

- Ziel: Zugriff aufs Internet
- Situation: alle Ports gefiltert, nur DNS verfügbar
- DNS-Server hat (logischerweise) Zugriff aufs Internet
  - Da müssen wir durch

Funktionsweise

- DNS ist ein hierarchisches System, eingeteilt in Zonen
- Beispiel `www.ccc-mannheim.de.`
  - Server für Zone `.` wird nach `de` gefragt
    - Server für Zone `de.` wird nach `ccc-mannheim` gefragt
      - Server für `ccc-mannheim.de` wird nach `www` gefragt
        - Der weiß was und verrät die IP
- `DNS2TCP` spielt DNS-Server für eine eigene öffentliche Zone

Funktionsweise

- DNS-Anfragen: Text
- Antworten können verschiedene Typen haben
  - Adresse, Mailserver, Dienst, etc...
- `TXT` für beliebigen Text
- DNS-Request enthält zu sendende Daten, DNS-Reply enthält die Antwort
- Client pollt außerdem ständig

Installation

- `DNS2TCP` ist GPL-lizensiert

  http://www.hsc.fr/ressources/outils/dns2tcp/index.html.en

- Good old `./configure && make && su -c "make install"`

Konfiguration

- DNS-Zone
- Beispiel: `to.mmpf.org`

```
41 ; DNS2TCP
42 to.mmpf.org.      IN  NS  atropos.ath.cx.
43
44 ; compatibility for clients
```

Konfiguration

- `dns2tcpd` auf `atropos.ath.cx`:

```
listen = 94.23.166.62
port = 53
user = nobody
chroot = /var/empty/dns2tcp/
domain = to.mmpf.org
ressources = ssh:[::1]:22
```

Konfiguration

- `dns2tcpc` auf dem Client:

```
domain = to.mmpf.org
ressource = ssh
local_port = 5322

$ dns2tcpc 10.16.1.1
```

Demo

DNS2TCP live im Hochschul-Netzwerk

Danke übrigens für Eure Aufmerksamkeit.

Bild: Philippe Leroyer @ Flickr