STLLUG October 2023
Short Topics on Short Notice

About Me

I work as an independent consultant performing system and small network administration, and writing specialized technical documentation.

(Short) Notice

I committed to this session rather late last evening. It will be less organized, and there will be more issues ‘left as an exercise for the reader’ than usual.

Why these?

These are things that have interested me or that I have worked on recently.

Rough Outline

Real-life Email Trouble-shooting

Fossil and Git

ipset / aggregate / IP blocklists

MoveIT / PBI / TIAA-CREF / Krull

Real-Life Email Trouble-shooting

References:

https://explained-from-first-principles.com/email/

https://en.wikipedia.org/wiki/Sender_Policy_Framework

Real-Life Email Trouble-shooting

DNS trouble

SPF trouble

Email: DNS trouble

Many steps unrelated to problems found left out.

ken@example.com

MX record for example.com

Email: DNS trouble

```
# dig example.com MX
  …
 mailserver.example.com

# dig mailserver.example.com
  some IP address
```

Email: DNS trouble

What if there is no MX record?

```
# dig example.com
  …
  (probably some other) IP address,
  perhaps of the web server
```

Email: DNS trouble

In the event of certain failure modes,

ken@example.com and
ken@mailserver.example.com

are NOT the same.

Email: DNS trouble

Questions?

Email: SPF trouble

SPF – Sender Policy Framework

Identify the real and authorized outgoing mail servers for your domain.

Why?

Email: SPF trouble

SPF – Sender Policy Framework

Identify the real and authorized outgoing mail servers for your domain.

Why?

Email: SPF trouble

Financial institutions might prefer that their customer’s assets are not stolen.

Ordinary companies do not want to be spoofed just to get spam in the door – it injures their deliverability. Also, protect their own readers.

Email: SPF trouble

Later integrated into DMARC – not a topic for tonight.

Email: SPF trouble

```
# dig example.com TXT
```

look for “SPF=...”

I use pobox.com

Resideo vs. Gmail: Resideo loses

Email: SPF trouble

Questions?

Fossil vs. Git

https://fossil-scm.org/home/doc/trunk/www/
fossil-v-git.wiki

Is your project more like SQLite or the Linux Kernel?

ipset / aggregate / IP blocklists

‘Static’ (not fail2ban) to protect internet-exposed systems

fail2ban is good, I use that too.

-

Tools

bash

curl

cut

aggregate

sort -V

ipset

Sources -YMMV!

Bogons – www.team-cymru.org

Crowdsec

DROP – www.spamhaus.org

eDROP – www.spamhaus.org

dshield – feeds.dshield.org

feodot – feodotracker.abuse.ch

Sources -YMMV!

Geoblock – maxmind.com (free license)

Peter Hansteen – home.nuug.no,
www.bsdly.net

Scanners – isc.sans.edu

ipset / aggregate / IP blocklists

Questions?

Email: SPF trouble

Questions?

MoveIT / PBI / TIAA-CREF / Krull

No notes on this one.

Questions?

Real-life Email Trouble-shooting

Fossil and Git

ipset / aggregate / IP blocklists

MoveIT / PBI / TIAA-CREF / Krull

STLLUG October 2023
Short Topics on Short Notice