Go ahead, run your own mailserver!

What, are you Chicken?

/usr/bin/whoami

Matt Linton (amuse)
“Chaos Specialist” @ Google
Primary role: Incident Response
Secondary role: Forensics

Major: Emergency Management
Minor: Philosophy

Tech Career:
BBS > Hacking > Sysadmin > Defense > Pentest > Forensics/IR

“Offense informs Defense ↺ ”

- I’m a defender now, not a pen-tester (anymore)
- I have no new tools, new tricks, new methods to teach
- What I do have:
  - A very particular set of skills
  - Acquired over a long career
  - Make me a nightmare for people like you

Welcome to the world of defense.

Tool Jockey

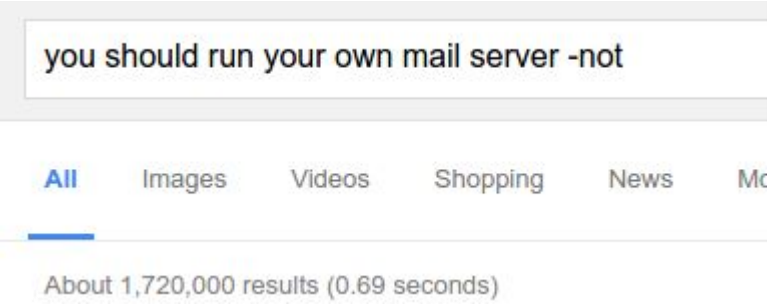
“Tool Jockey”
/to͞ol/jäkē/
Noun

1. A person who only knows how to use tools and read their output.
2. One who does not understand the underlying mechanics of the domain in which they operate.

synonyms: script kiddie, skid, griefer, lamer

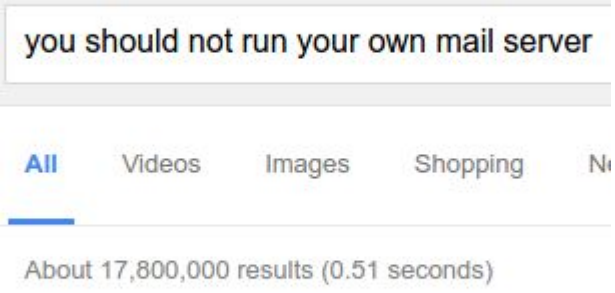
“Dave thinks he’s a l33t hacker, but he’s just a tool jockey. Take away metasploit and he’s completely lost.”

Premise:
Running your own mailserver is asking for trouble



you should run your own mail server -not

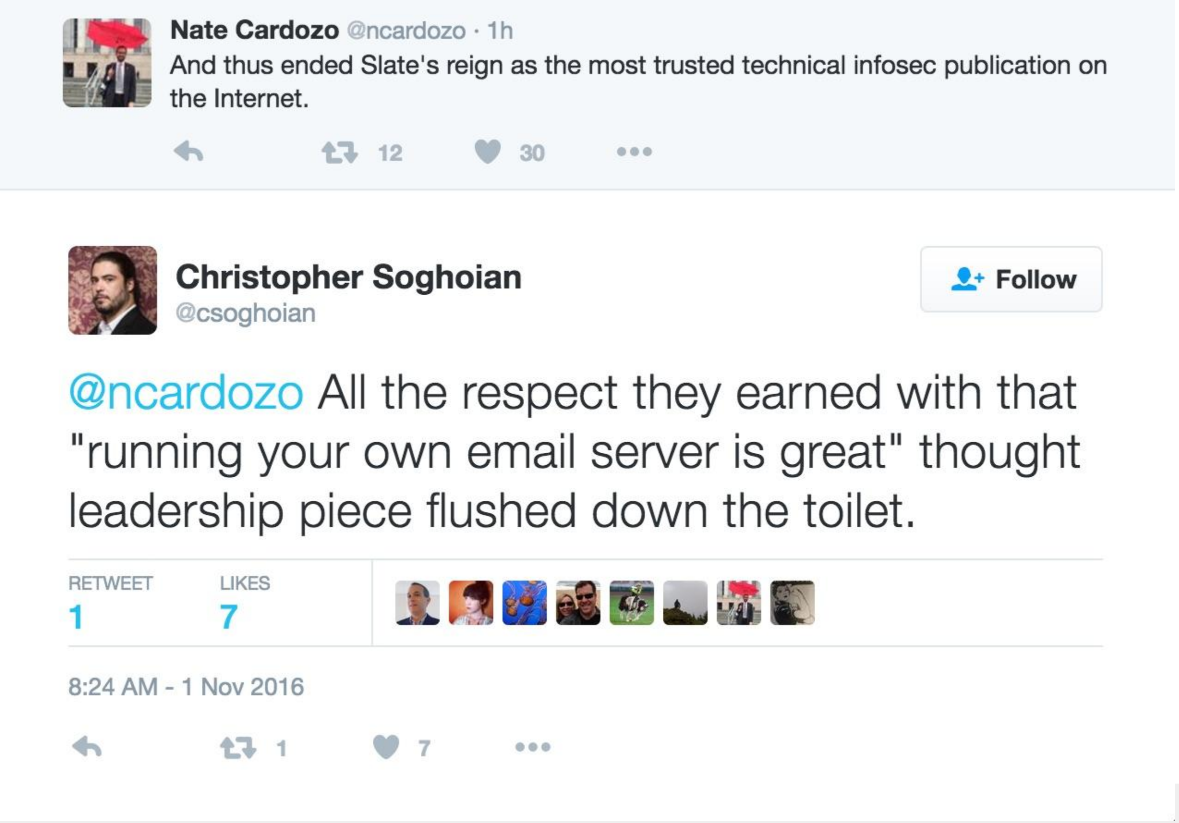
About 1,720,000 results (0.69 seconds)



you should not run your own mail server

About 17,800,000 results (0.51 seconds)

There's.... Some consensus



Nate Cardozo @ncardozo · 1h

And thus ended Slate's reign as the most trusted technical infosec publication on the Internet.

12 30

Christopher Soghoian
@csoghoian

@ncardozo All the respect they earned with that "running your own email server is great" thought leadership piece flushed down the toilet.

RETWEET 1

LIKES 7

8:24 AM - 1 Nov 2016

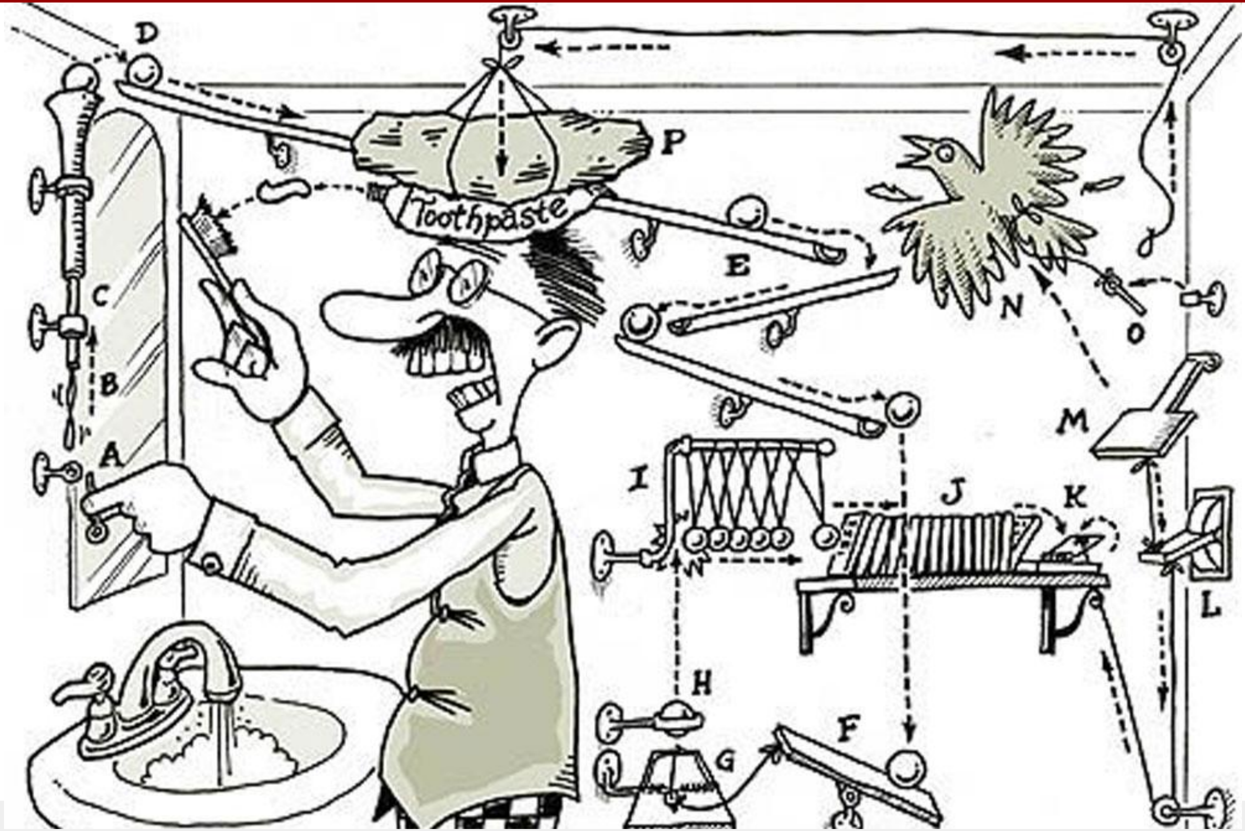
1 7

¯_(ツ)_/¯

Email isn't simple!

"So much trouble over such a small protocol."

Email isn’t simple!



¯_(ツ)_/¯

Your mission, should you choose to accept it:

- Install an email server which provides equal functionality to what’s available “out there” for free.
- Use it for 100% of your own email.
- Give a few friends/family free premium email accounts on it. No quota!
- Keep it up all the time.

Let’s get in trouble!

- Step one - you’ve got to pick a server & platform.
- Install OS, patch. Turn on auto-updates?
    - Maybe yes, maybe no. Lots of places don’t because the SMTP server is critical business-need, Reliability trumps security.
- Install mailserver. Exchange? Postfix stack?
- Enable POP/IMAP. Disable plaintext modes!
- Generate TLS certs, get signed, install in server, maintain those
- Create user accounts for people to log in.
- Create a domain name & MX Record somewhere.

Viola! You’re done!

Attack Surface

Current attack surface:

- OS exploits
- Mailserver exploits
- IMAP/POP server exploits
- Sending malware through to users
- Phishing the users / credential theft
- Brute-forcing
- Abuse (Open Relaying, Domain email on external interface)

Current operational status

SPAM SPAM SPAM SPAM SPAM SPAM SPAM

Filtering

- Maybe you’re receiving mail but who knows, you can’t find it among all the “herbal supplement” advertisements
- Y’all need SPAM and Virus filters.
- So you install them.
  - Commercial or OSS?
  - Relay like Sonicwall / Proofpoint?
  - OSS like ClamScan?
- Most of these run as daemons / other servers!

“You guys, this guy is a PRINCE. And he wants to just give us money!”

Attack Surface

Reduced attack efficacy:

- Sending malware through to users

Added attack surface:

- Exploitation of Filter server
- Exploitation of AV
- Denial of Service (resource exhaustion)
- Trust relationship with blacklist sources (eg, spamhaus, orbs, etc)

Current operational status

SMTP Error 550: Server not in whitelist and DMARC validation failed.

DMARC / SPF / TLS

- Your mailserver isn’t trusted, you need DMARC / DKIM|SPF so your mail will be delivered
- Does your hosted DNS provider support arbitrary IN TXT records? Hope so or you’ll be maintaining a DNS server now too.
- Also you need to learn crypto / key management & signing now too.
- And publish a signing record.
- And integrate outbound message signing in the email server, which means a running daemon to perform that task....
- While you’re at it, you want TLS for mail send/receipt right?
- Your provider blocks outbound SMTP? Bummer, now you need to implement trusted relaying…..

A sloppy SPF mistake to exploit

- Many, many places use SPF as an anti-phish / fraud measure.
- Then they outsource their SMTP to a big provider (eg, sendgrid)
- Then publish a sloppy SPF record saying “Yeah, sendgrid can send as me”
- See the problem here?!

Attack Surface

Reduced attack efficacy:

- None, but improved organizational reputation
- You actually can deliver email to others now

Added attack surface:

- Maintaining DNS
- Additional complexity around crypto key management
- Trusted daemon running so you can sign outbound messages
- More [Open]SSL dependencies
- Relay credential management

Current operational status

Yay, you’ve got mail delivery!

But wait! Your users want webmail

- Install OSS webmail server maybe.
  - Zimbra? Squirrelmail? Roundcube?
  - Now you get to maintain Apache or nginx or lighttpd or IIS
  - Also need to run Python|PHP|Perl|MySQL (sorry)
- They also want ActiveSync support
  - Zimbra supports it - others maybe yes, maybe no

Attack Surface

Reduced attack efficacy:

- None

Added attack surface:

- Apache exploits
- LAMP exploits
- Writable webdirs
- Vulnerable stuff you fixed but it got replaced after you patched and is vulnerable again (hi, xmlrpc.php)
- SQL Injection

Passwords and you

- If you haven't implemented two-factor authentication yet you should

- Zimbra & Roundcube support it. There's PAM modules, or Duo.

- Otherwise →

Attack Surface

Reduced attack efficacy:

- Brute-forcing
- Phishing

Added attack surface:

- Third-party auth libraries

Other things you need to do

- Tighten your permissions
  - setfacl is a sysadmin’s best friend, why does no one use it?!

- Monitoring - learn the exciting world of HIDS/HIPS, logs & automatic countermeasures
  - Find another host somewhere for nagios? How will you know if your server is down?

- Auto-updates: Yes or no?

Where you are now:

- You’ve touched over two dozen RFCs (SMTP, POP, IMAP, DNS, Network, TLS, etc etc etc)
- Implemented multiple protocols
- Interacted with every layer from Kernel (facl) to web users
- Hardened: System, Network, Database, Webserver, User Accounts
- Watched your own attack surface grow, shrink, grow again

How many **weaknesses can you exploit**,
and **places can you hide** now?

Also: Pain will make you stronger

Be honest: Pen-testers can be jerks

… and in January I penetrated a mail server that had no dual factor auth and made fun of the sysadmins for being stupid but it was really a business decision their boss made.

And then in February I said a guy was incompetent and should be fired because there was no encryption on the file share but I found out he was “sysadmin” because they wouldn’t hire one and made the mail guy do it.

But the WORST thing I’ve ever done…..

Empathy will further your career

- Keeping services up and fully secure IS HARD.
- Your clients don’t need your scorn, they need your help.
- It’ll make you a better person and a better provider

Conclusion:

- Mailserver is just a great example of a fundamental truth: **Competence Counts**.
- “Vulnerabilities” are the tip of an iceberg
- Understand how everything works until you can run it yourself. DO run it yourself.
- The defender ***knows*** where the cracks are - so become the defender.

¯_(ツ)_/¯

Hate Mail

0xMatt

amuse@google.com

#irc @amuse / @docinabox

LOL NO