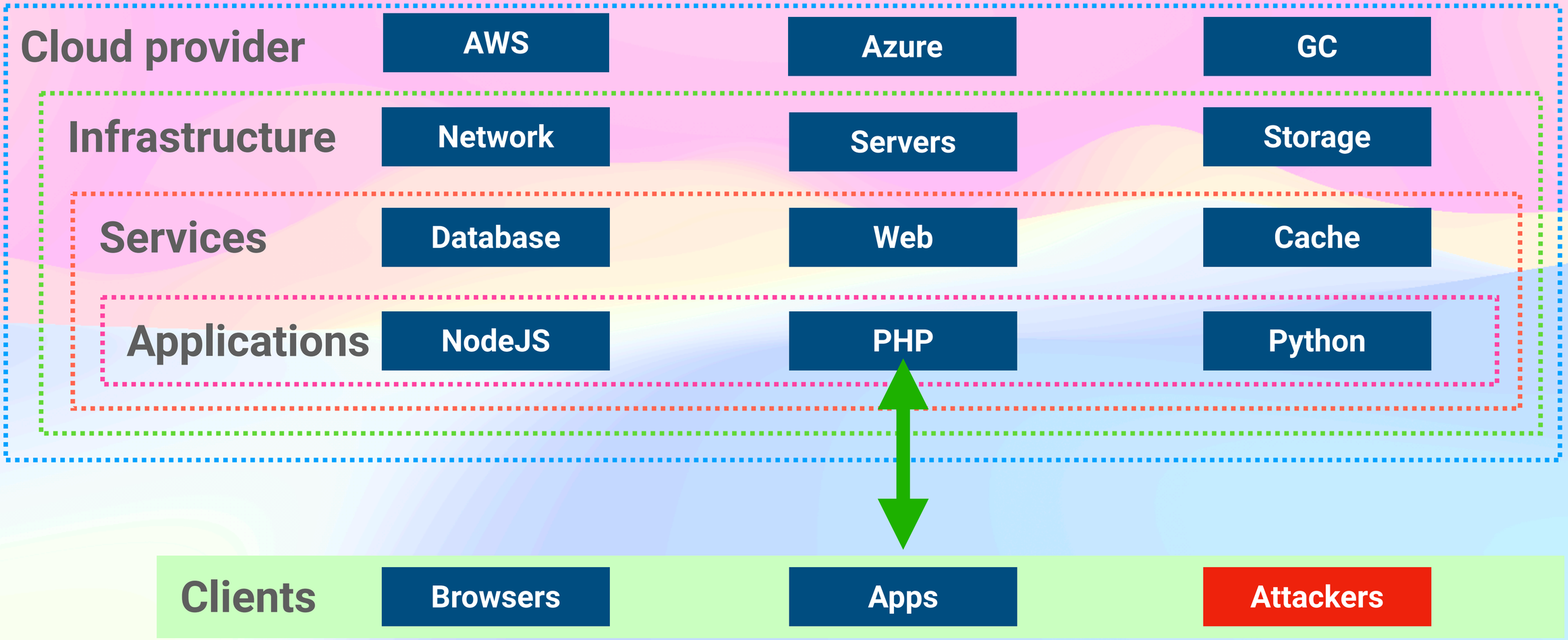
Picking the low-hanging fruit; Easy pentest wins

Avoiding security issues with up-front measures

Marcus Bointon – @Synchro@phpc.social – ConFoo Montreal 2025


Marcus Bointon
Skier
Songwriter
PHPMailer maintainer, Laravel dev
Radically Open Security
Pentests, code audits
TIL: *Everyone makes the same mistakes*

Typical deployment stack



Attacker targets

- Information disclosure
- Outdated software
- Misconfiguration
- Errors
- Validation & escaping

Cloud provider security

- IP addresses
- Security groups
- SSH bastions
- VM / container images

Cloud provider demo

Infrastructure

- VM images
  - Supported, up to date
  - Consider minimal images
- Containers
  - Docker, K8s, EKS
- Immutable instances, read-only FS, no FS

Infrastructure – Firewalls

- Block by default
- Allow only what's needed
- Set rate limits
- Consider outbound limits
- Don't forget IPv6
- Check with `nmap -p- <hostname>`

Infrastructure – SSH access

- Do you need it at all?
- Keys, not passwords
  - Prefer `ed25519` over `RSA`
- Non-standard ports
- Hardening
- Fail2Ban

Testing access

- `nmap`
  - Scans for open ports
  - Don’t test other people’s servers!
- `ssh-audit`
  - Follow its recommendations

UFW firewall example

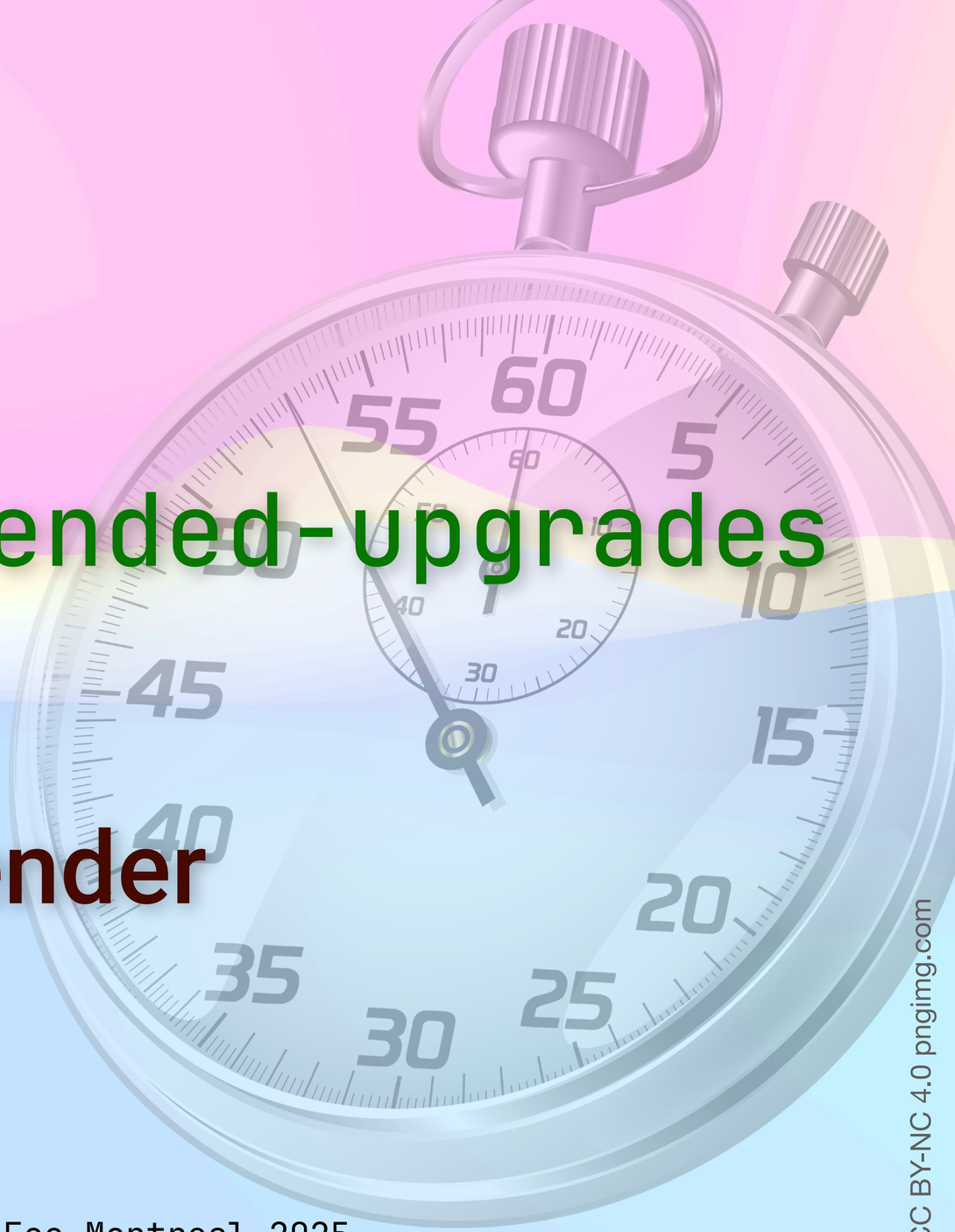
```
ufw reset
ufw default deny
ufw logging medium
ufw allow from x.x.x.x to any app OpenSSH
ufw limit from any to any app OpenSSH
ufw allow from any to any app "Nginx Full"
ufw allow proto udp from any to any port 443
ufw enable
```

Hardened SSH config

```
PermitRootLogin without-password
LogLevel VERBOSE
PasswordAuthentication no
GSSAPIAuthentication no
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-
etm@openssh.com
Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
KexAlgorithms sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-
sha256@libssh.org,gss-curve25519-sha256-,diffie-hellman-group16-sha512,gss-group16-
sha512-,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha256
HostKeyAlgorithms ssh-ed25519,ssh-ed25519-cert-v01@openssh.com,sk-ssh-
ed25519@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,rsa-sha2-512,rsa-sha2-512-
cert-v01@openssh.com,rsa-sha2-256,rsa-sha2-256-cert-v01@openssh.com
DebianBanner no
```

OS updates

- Automate!
  - Debian/Ubuntu `unattended-upgrades`
  - RedHat `yum-cron`
- Windows Update & Defender



Nmap & SSH Demo

Service with a smile

- Web servers
  - TLS config
  - Security headers
  - https://ssl-config.mozilla.org/
- Database / cache / queue servers
  - Should not be accessible from outside
  - Avoid listening on all interfaces: 0.0.0.0, ::

Security headers

- `Strict-Transport-Security: max-age=31556952; includeSubDomains; preload`
- `Content-Security-Policy`
  - A talk in its own right
- `X-Content-Type-Options: nosniff`
- `Referrer-Policy: no-referrer`

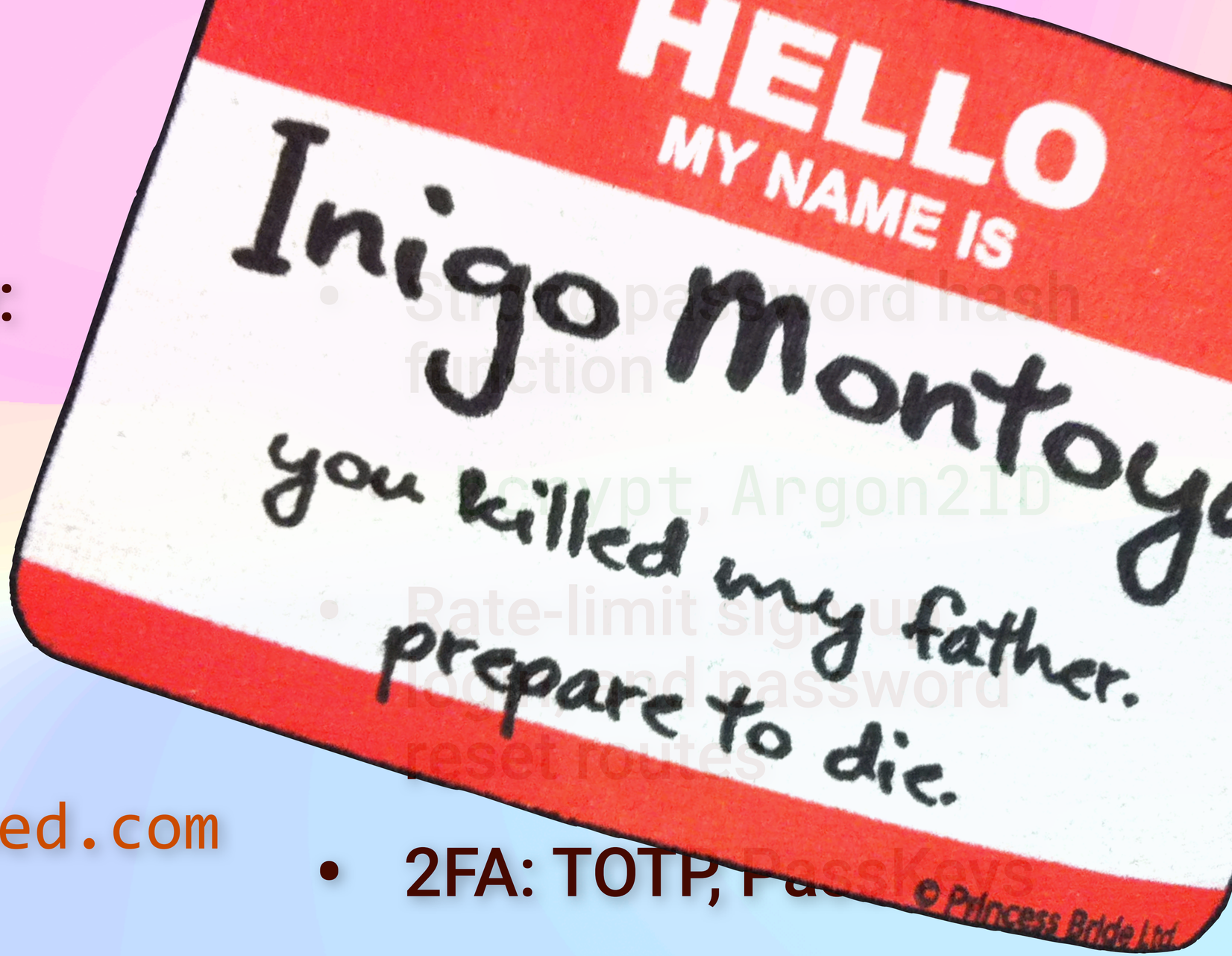
Testing TLS, HTTP, privacy

- www.ssllabs.com/ssltest/
- testssl.sh
- securityheaders.com
- http3check.com
- webbkoll.5july.net

Demo time!

Authentication

- Password policy:
  - Long
  - Random
  - Not in known breaches
  - haveibeenpwned.com



- Store password hash function
- bcrypt, Argon2ID
- Rate-limit sign up, login and password reset routes
- 2FA: TOTP, Passkeys

Authorisation

- Principle of least privilege
- Privilege separation

App dependencies

- NodeJS: `npm audit`
- Ruby: `ruby-audit`
- Python: `pip-audit`
- PHP: `composer audit`
  - `roave/security-advisories:dev-latest`

Cookie flags

- `Secure`
  - Protects against interception
- `HttpOnly`
  - Prevents scripts accessing cookies
- `SameSite` Lax/Strict
  - Protects against CSRF

Front-end shenanigans

- Sanitise
  - Ignore transgressions
- Validate
  - Fail hard on rule breaks
  - Implement same rules on back end
- Escape
  - Appropriately!

The great escape

- URL: `Hello%20world`
- HTML: `I <3 U`
- Shell: `file\ name, "${myarg}"`
- SQL: `'Bobby O\'Tables'`
- JSON: `"name": "Enni \"Hacker\" Nagy"`
- Email: `"Gergő Sp@mboy"@example.com`

Safe coding practices

- Use tools to help you
- Coding standards
- Static analysers
- IDE plugins
- Pre-commit hooks
  - Detect secrets, spot debug statements
- GPG-sign your commits

Security is a *process*

- It's not a *thing*
- A moving target that requires constant vigilance
- Made easier with automation

Now let the pentesters do the hard stuff

- @Synchro@phpc.social
- @SynchroM@x.com
- Synchro on GitHub and Stack Overflow
- https://marcus.bointon.com
  - Buy my music!
- Open to job offers!

Feedback please!