Sprinkler: A Multi-Service Password Sprayer
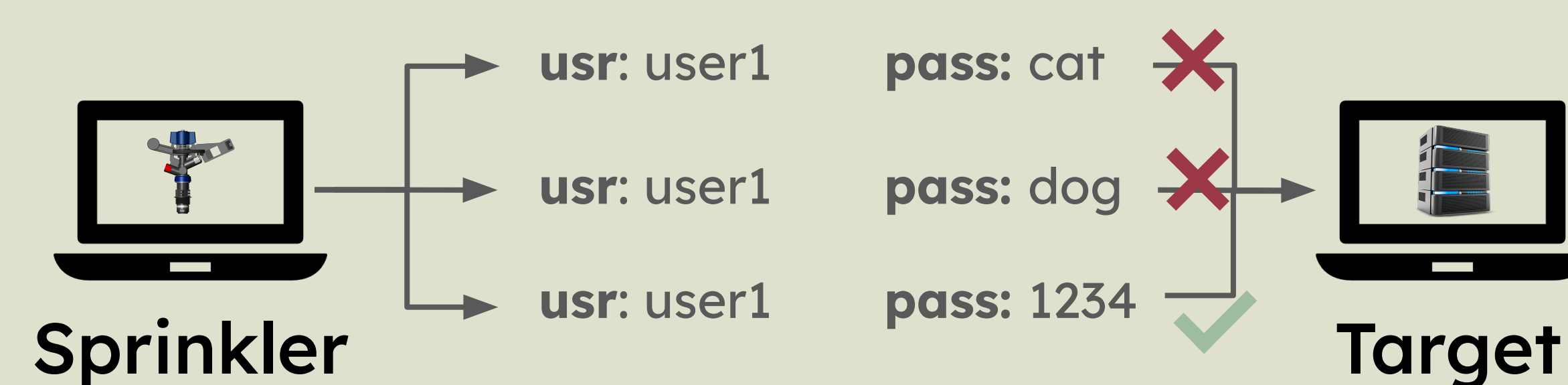
Sam Ederington, Prompt Eua-anant, advised by Jeff Ondich

References

What's password spraying?

- Guessing server login credentials as fast as possible, without getting detected

Sprinkler
- **usr**: user1 **pass**: cat ✗
- **usr**: user1 **pass**: dog ✗
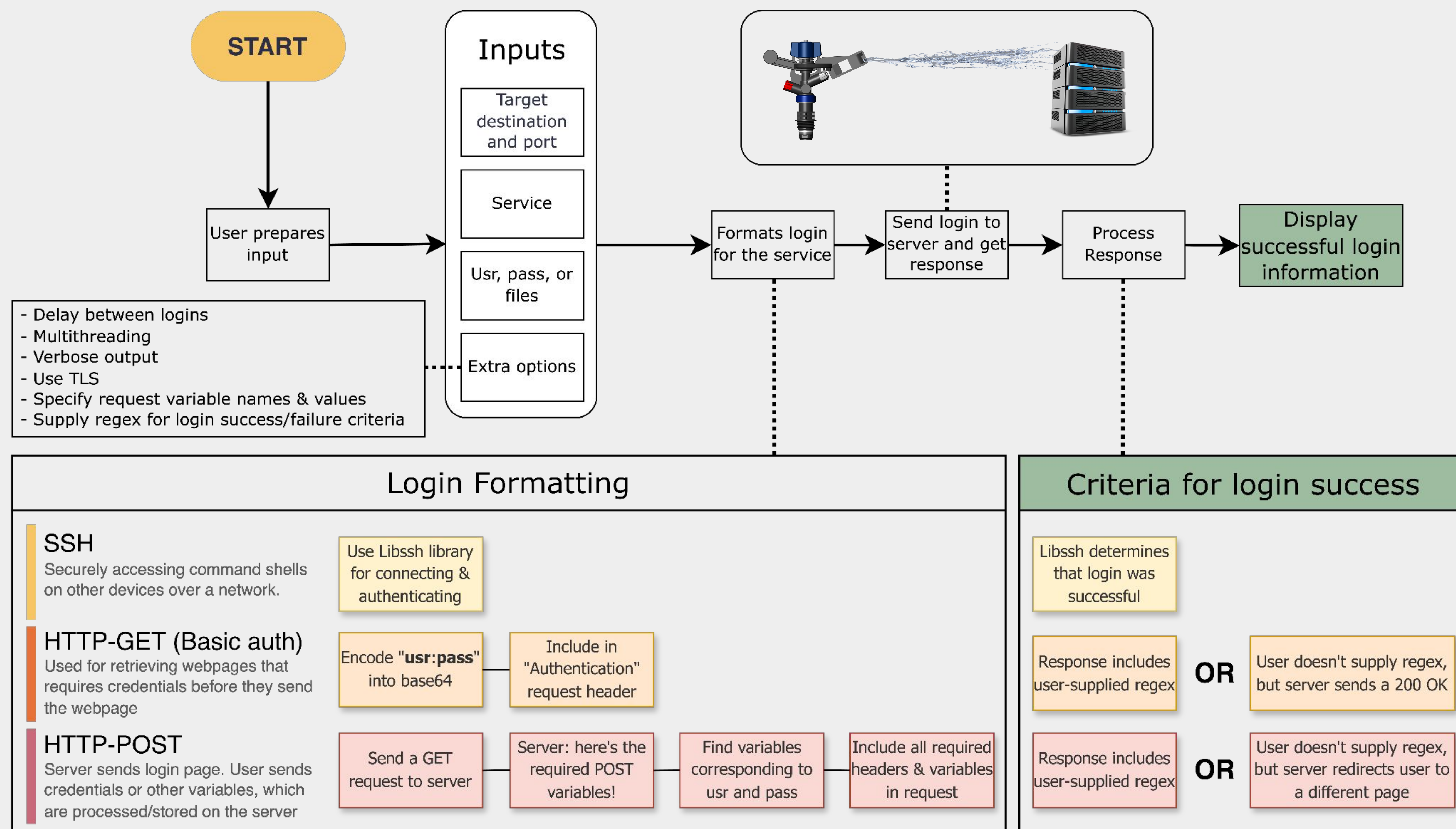- **usr**: user1 **pass**: 1234 ✓
Target

Why it's important?

- It's used for hacking and security purposes, finding accounts with vulnerable login permissions to attack or require changing.
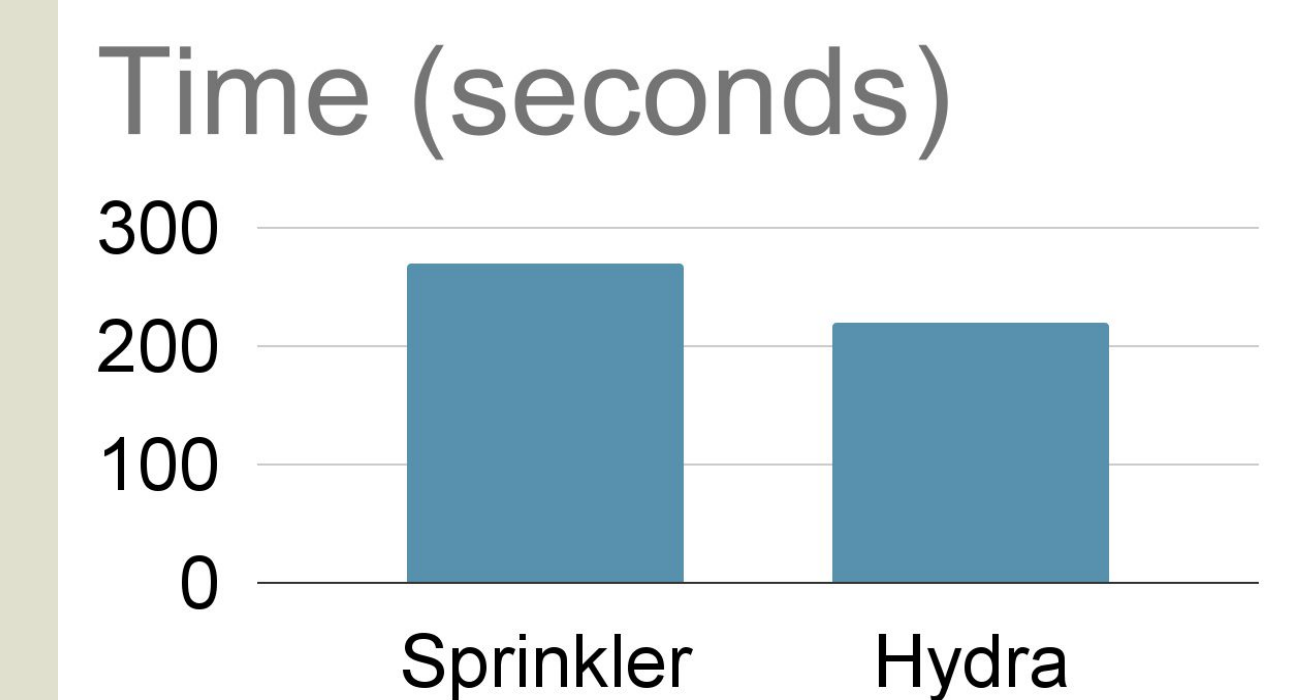
Our goal

- Make a fast password sprayer that works for ssh, http-get (basic auth), http-post. Language = C

- Prepare a test server compatible with the services we need

- Compare Sprinkler's performance with Hydra, a popular password sprayer
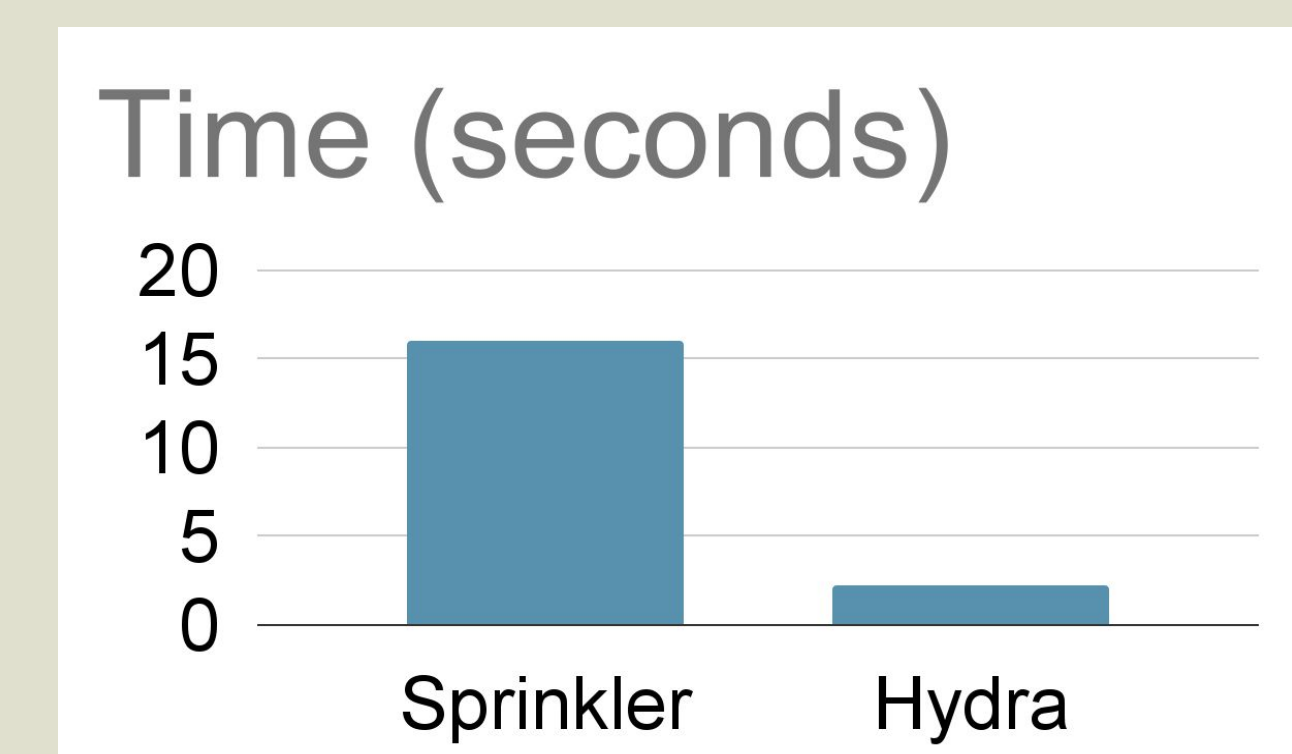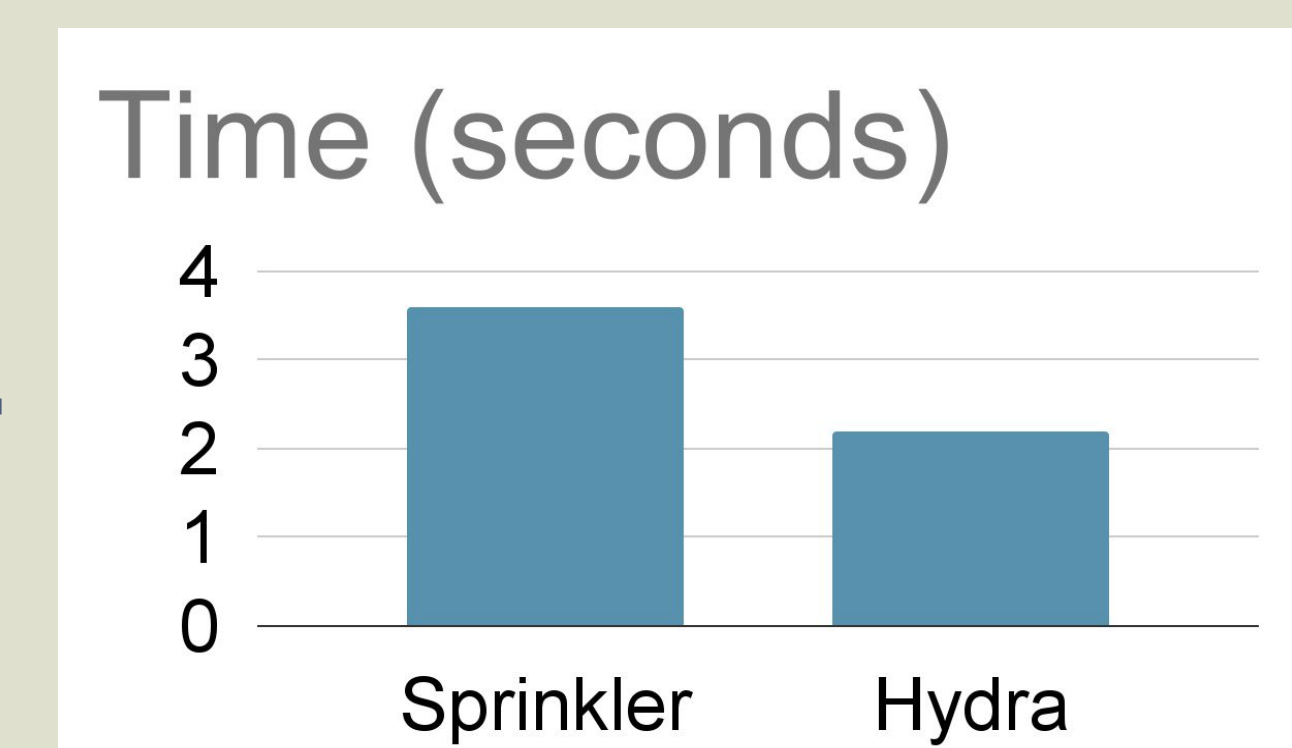
How Sprinkler works

START

Inputs
- Target destination and port
- Service
- Usr, pass, or files
- Extra options

User prepares input → Formats login for the service → Send login to server and get response → Process Response → Display successful login information

- Delay between logins
- Multithreading
- Verbose output
- Use TLS
- Specify request variable names & values
- Supply regex for login success/failure criteria

Login Formatting

SSH
Securely accessing command shells on other devices over a network.
→ Use Libssh library for connecting & authenticating

HTTP-GET (Basic auth)
Used for retrieving webpages that requires credentials before they send the webpage
→ Encode "**usr:pass**" into base64 → Include in "Authentication" request header

HTTP-POST
Server sends login page. User sends credentials or other variables, which are processed/stored on the server
→ Send a GET request to server → Server: here's the required POST variables! → Find variables corresponding to usr and pass → Include all required headers & variables in request

Criteria for login success

- Libssh determines that login was successful

- Response includes user-supplied regex **OR** User doesn't supply regex, but server sends a 200 OK

- Response includes user-supplied regex **OR** User doesn't supply regex, but server redirects user to a different page

Performance

SSH
Time (seconds)
300 / 200 / 100 / 0
Sprinkler, Hydra

HTTP-GET
Time (seconds)
20 / 15 / 10 / 5 / 0
Sprinkler, Hydra

HTTP-POST
Time (seconds)
4 / 3 / 2 / 1 / 0
Sprinkler, Hydra