axiom

The dynamic infrastructure framework for everybody

@pry0cc // Ben Bidmead - 0x00sec.org

Senior Cyber Security Consultant - TrueSec

What is axiom?

- Axiom is the dynamic infrastructure framework for everybody - it is designed to be easy to use, intuitive and simple.
- Axiom supports several cloud providers currently, DigitalOcean, Azure, Linode, and IBM Cloud
- Google Compute & AWS support is on the roadmap
- Axiom enables the average weekend warrior or pentesting professional to quickly spin up one or many disposable instances at a time, preloaded with many popular bug bounty & pentesting tools.
- Distributed scanning allows scan times 60x-100x faster than a traditional stand-alone VPS
- I wanted to create something that would enable the average person to compete with enterprise-level solutions, so it is very affordable.
- A standard axiom instance on DigitalOcean will cost you $0.007 per hour to run, and comes with 1GB of ram and a single CPU core.
- 15 instances for 2 hours = 15 * 0.007 * 2 == $0.21 / 21 cents

But why?

- Faster scanning times means you can scan more often, useful for bug bounty.
- Reduce timelines of penetration tests for large external scopes
- Faster scanning means you can throw more data at the problem - bigger wordlists, deeper coverage
- Many different instance IP’s, avoid block-lists
- Basically a fully legal botnet.
- Why not?

What does axiom come with?

Tools

- Subfinder
- HTTPx
- DNSx
- Amass
- Nuclei
- Dalfox
- Ffuf
- Shuffledns
- Hakrawler
- Gau
- Meg
- fff
- gowitness
- aquatone
- Many more…

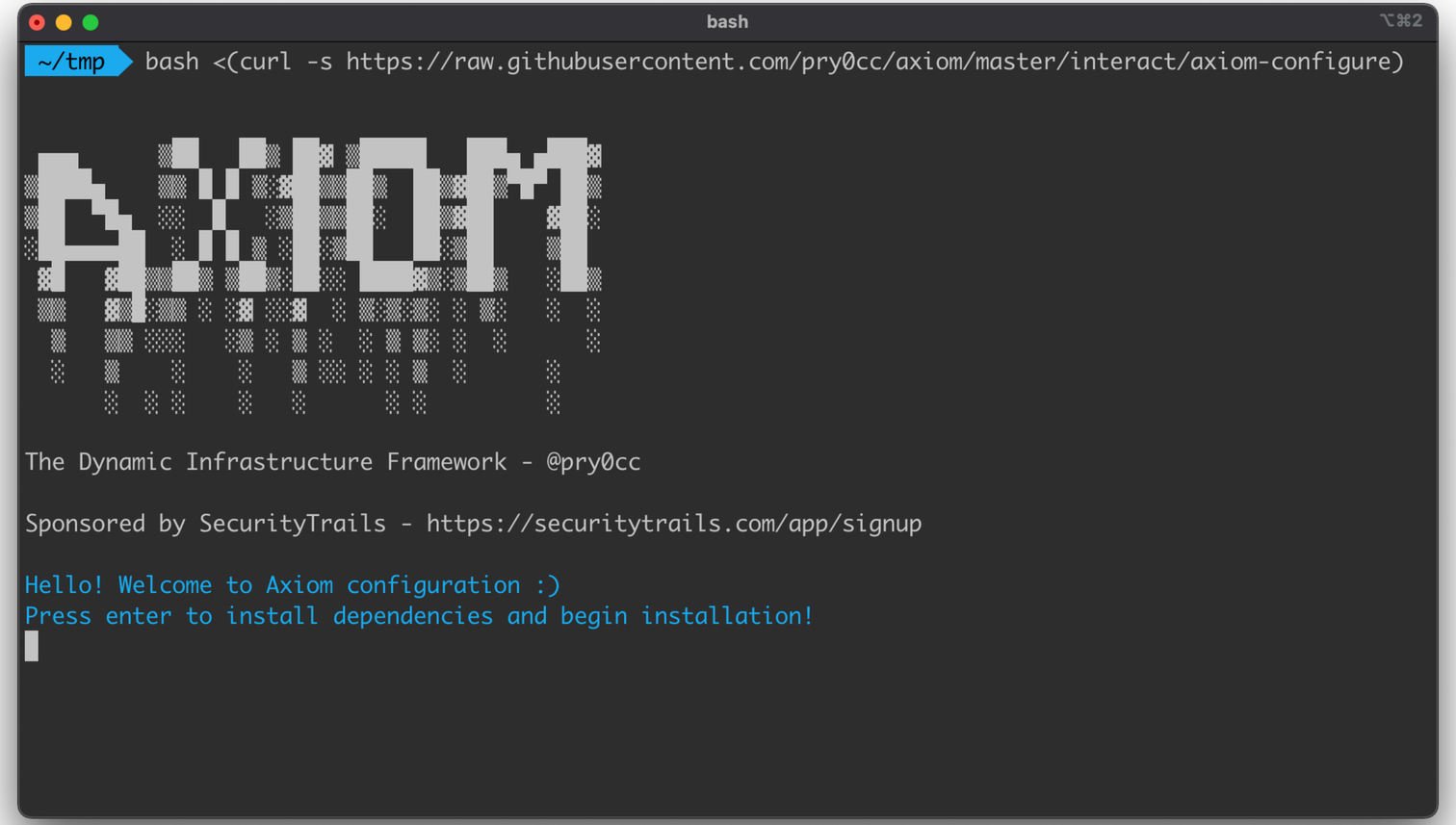
Wordlists

- Assetnote
- SecLists
- Jhaddix-all.txt

Crash Course Introduction

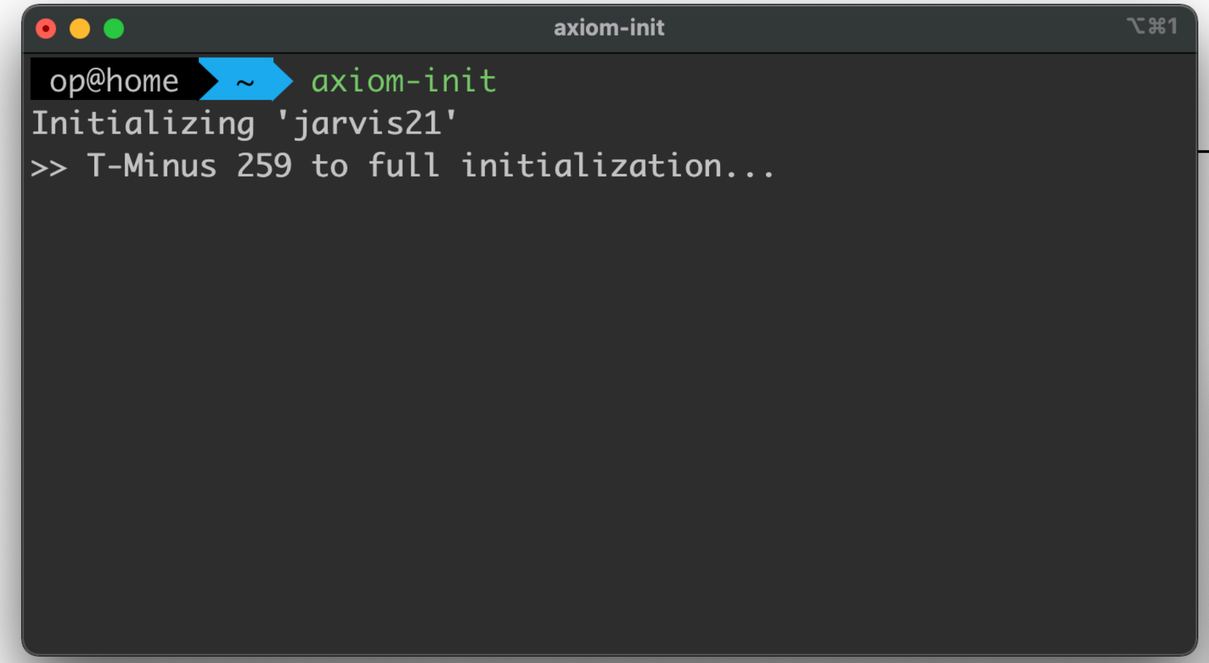
Installation

```
bash <(curl -s https://raw.githubusercontent.com/pry0cc/axiom/master/interact/axiom-configure)
```

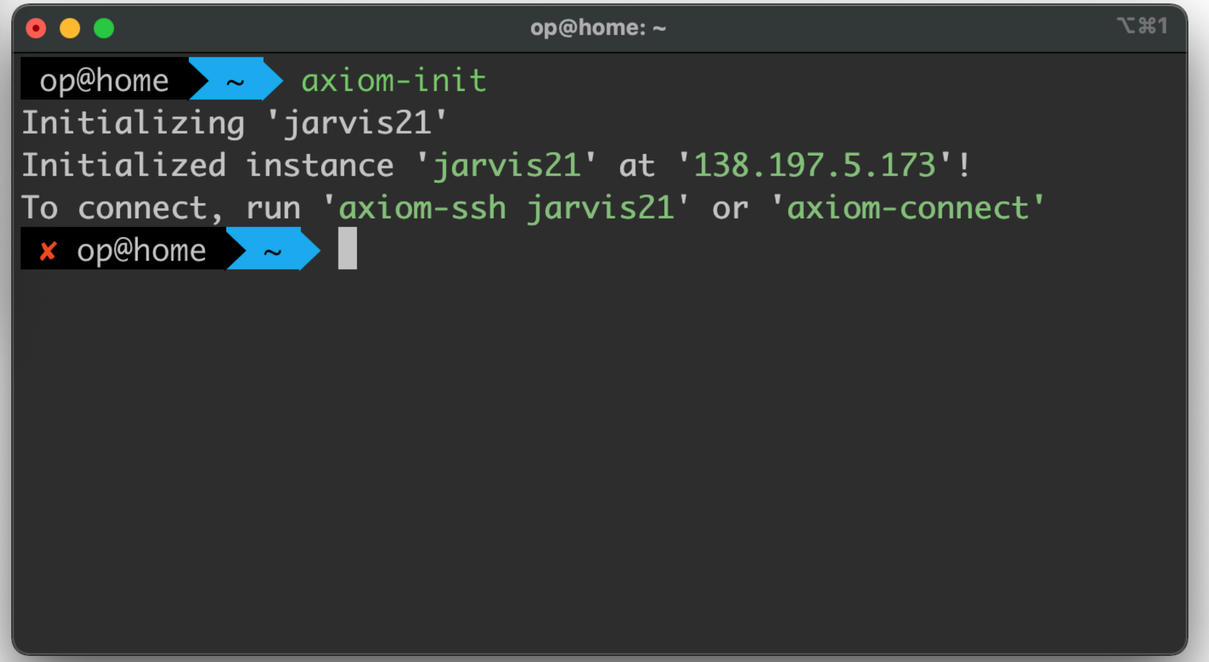


https://github.com/pry0cc/axiom/wiki

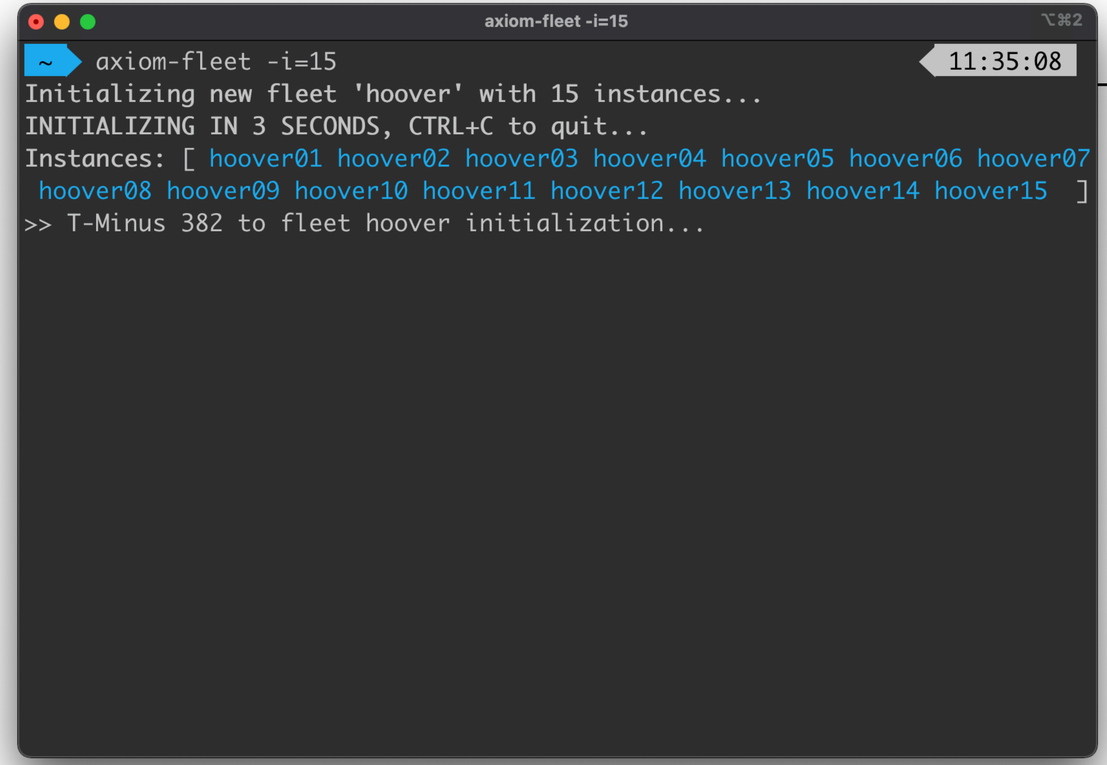
axiom-init



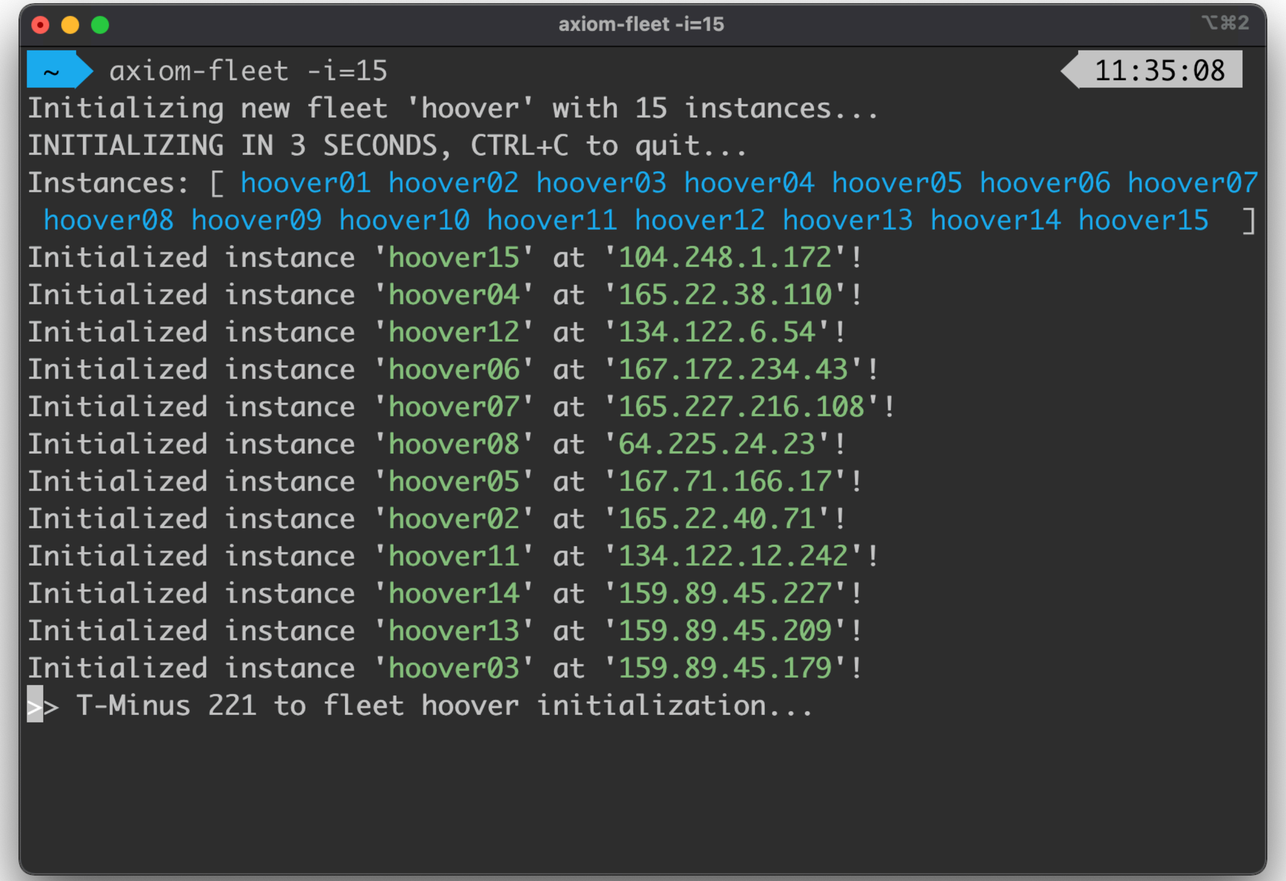
Initialize a single instance



axiom-fleet -i=15

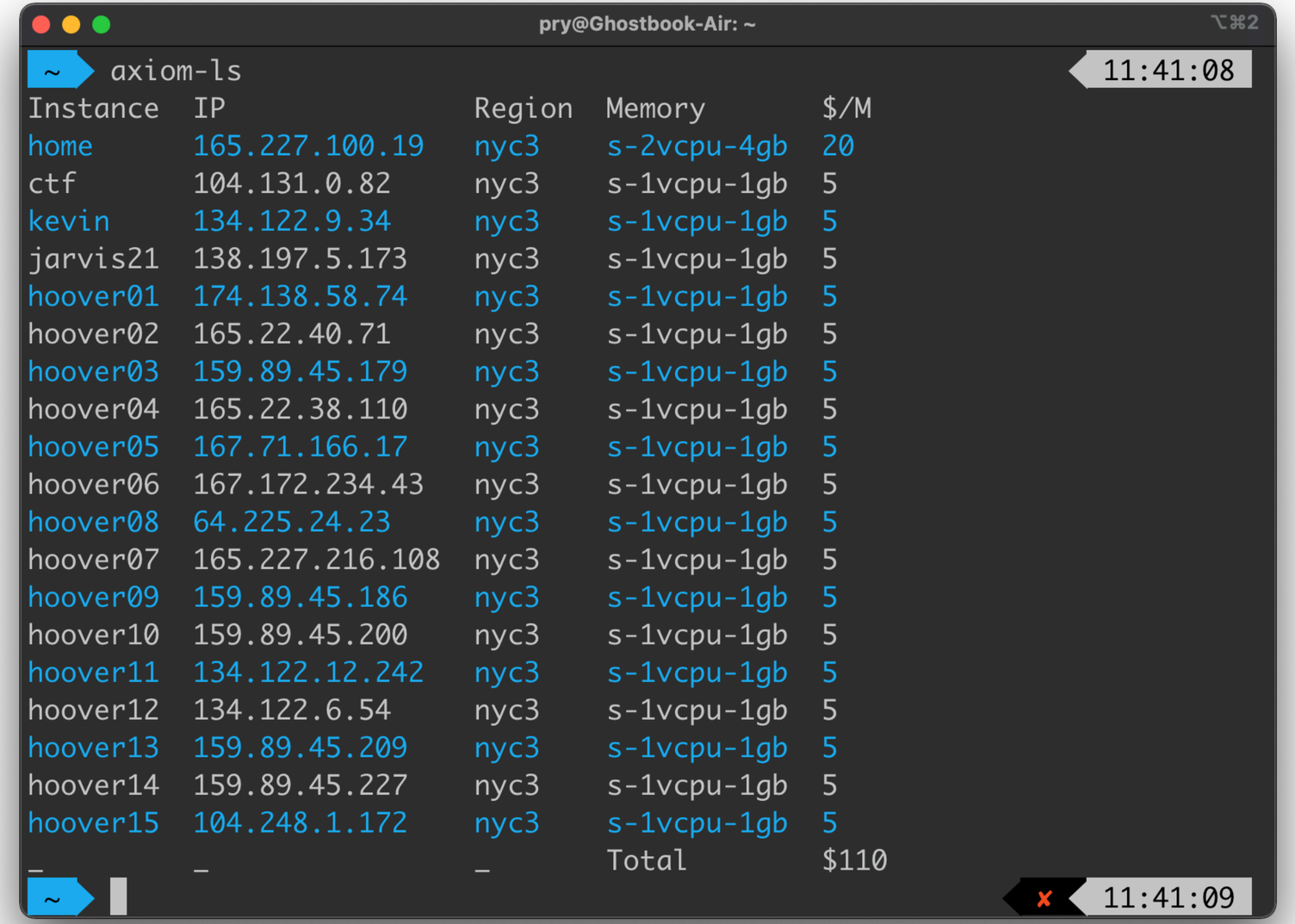


Initialize 15 instances



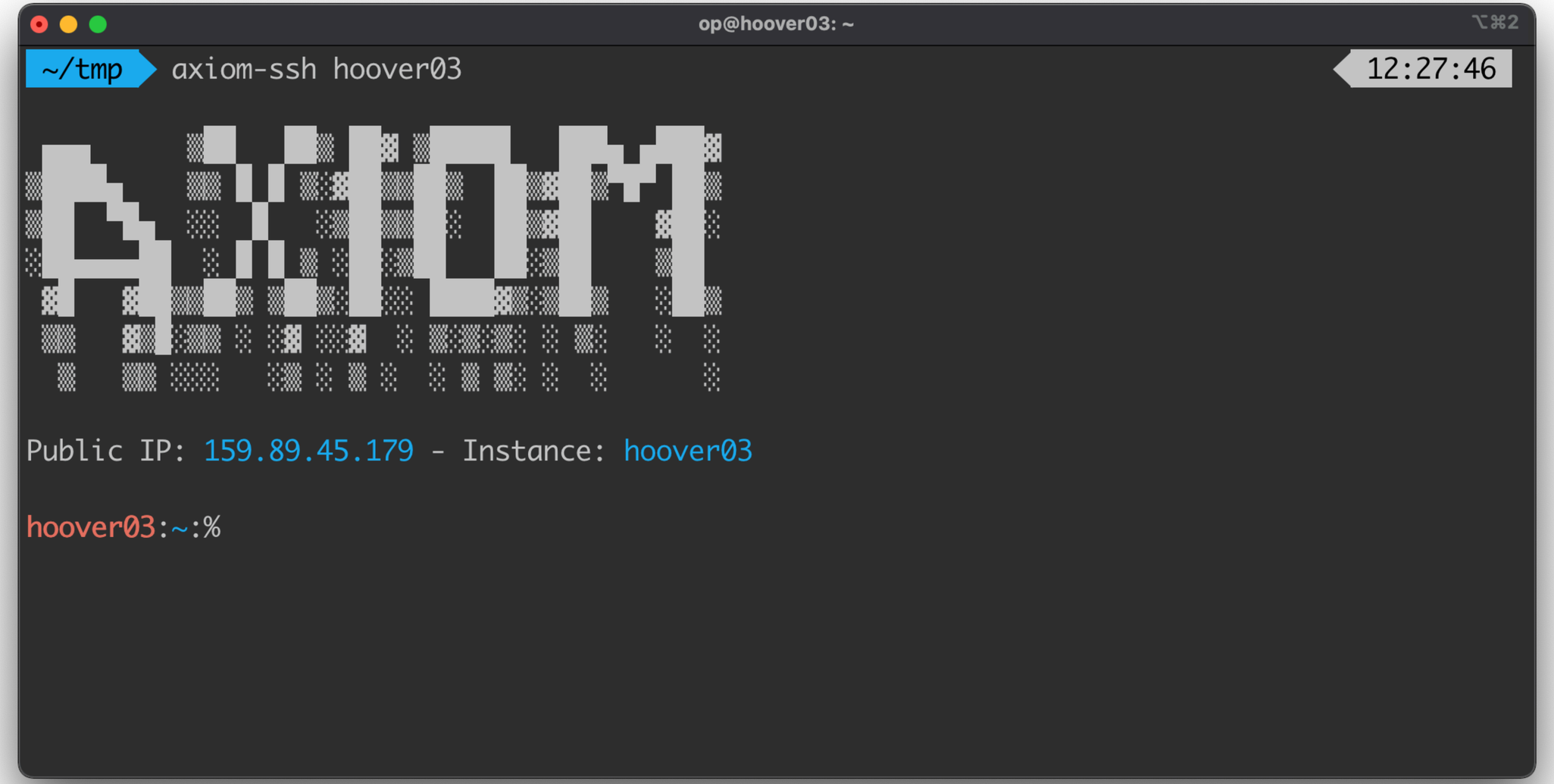
axiom-ls

List your instances

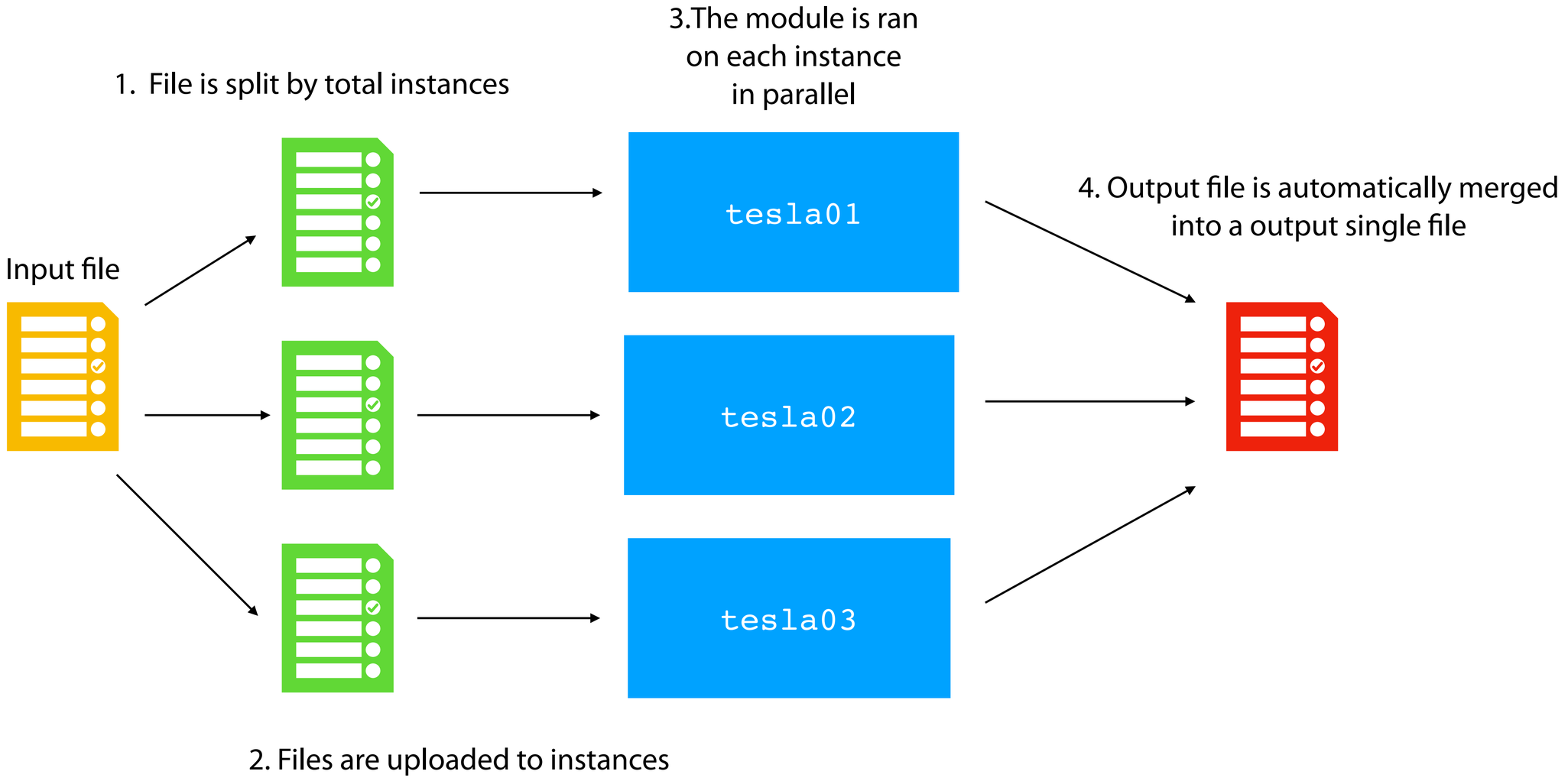


axiom-ssh

SSH into an instance



How distributed scanning works



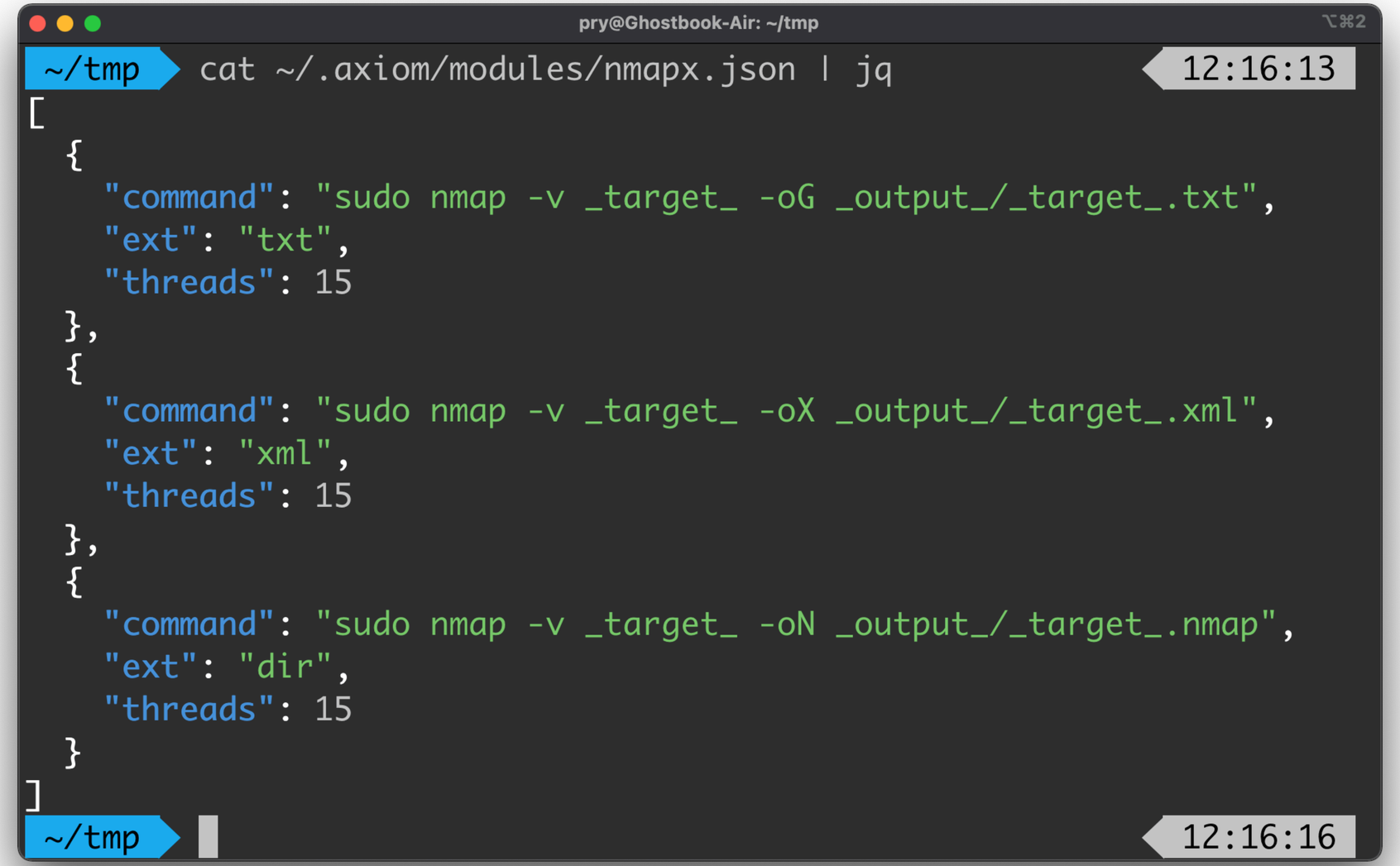
dWdnY2Y6Ly9mcnBoZXZnbGdlbnZ5Zi5wYnovbmNjL25wcGJoYWcvY2ViemJndmJhZj9jZWJ6YnBicXI9UEQwODlHOUlEWQ==

Scan modules

The anatomy of an axiom-scan module

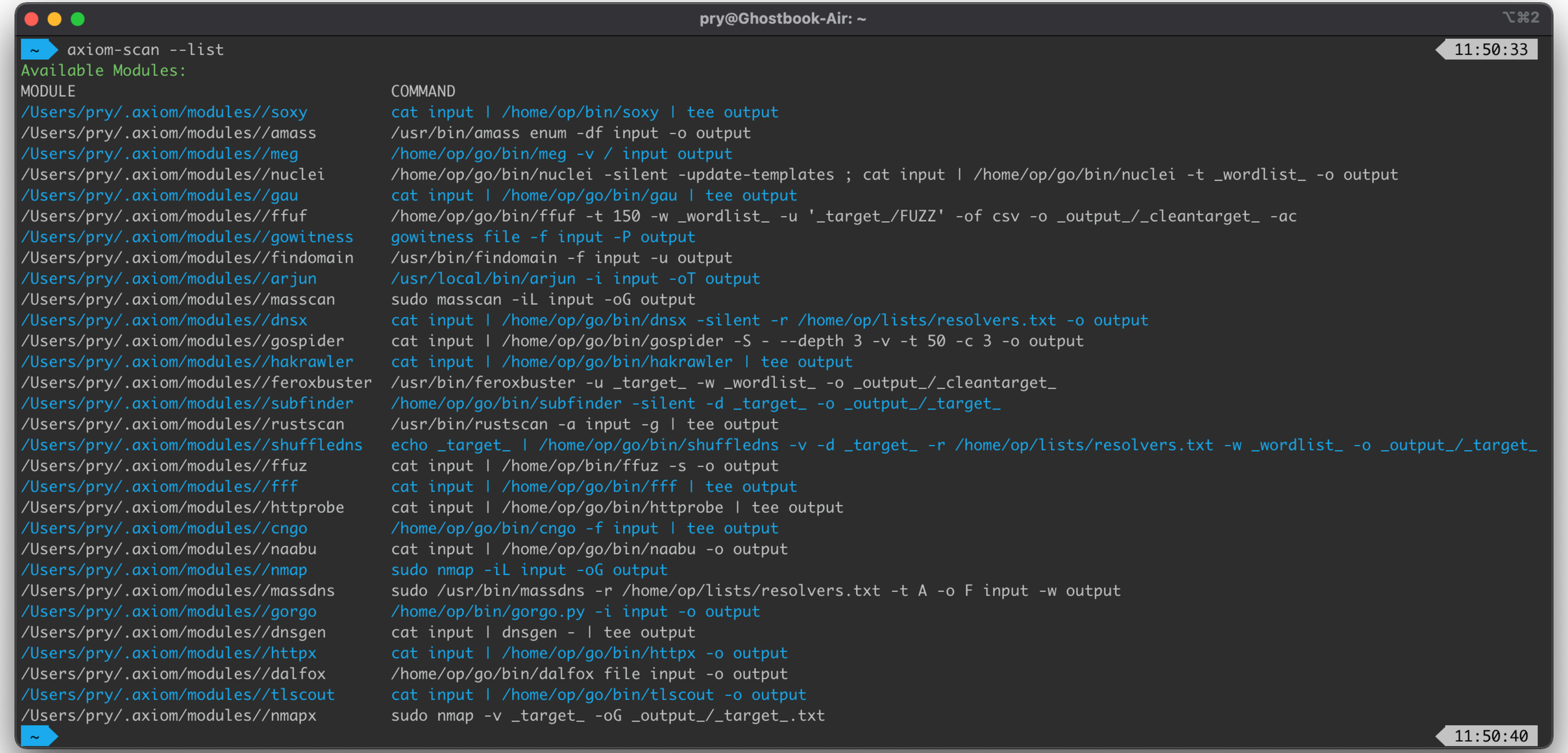
Oneshot modules

For tools that take a single target as input



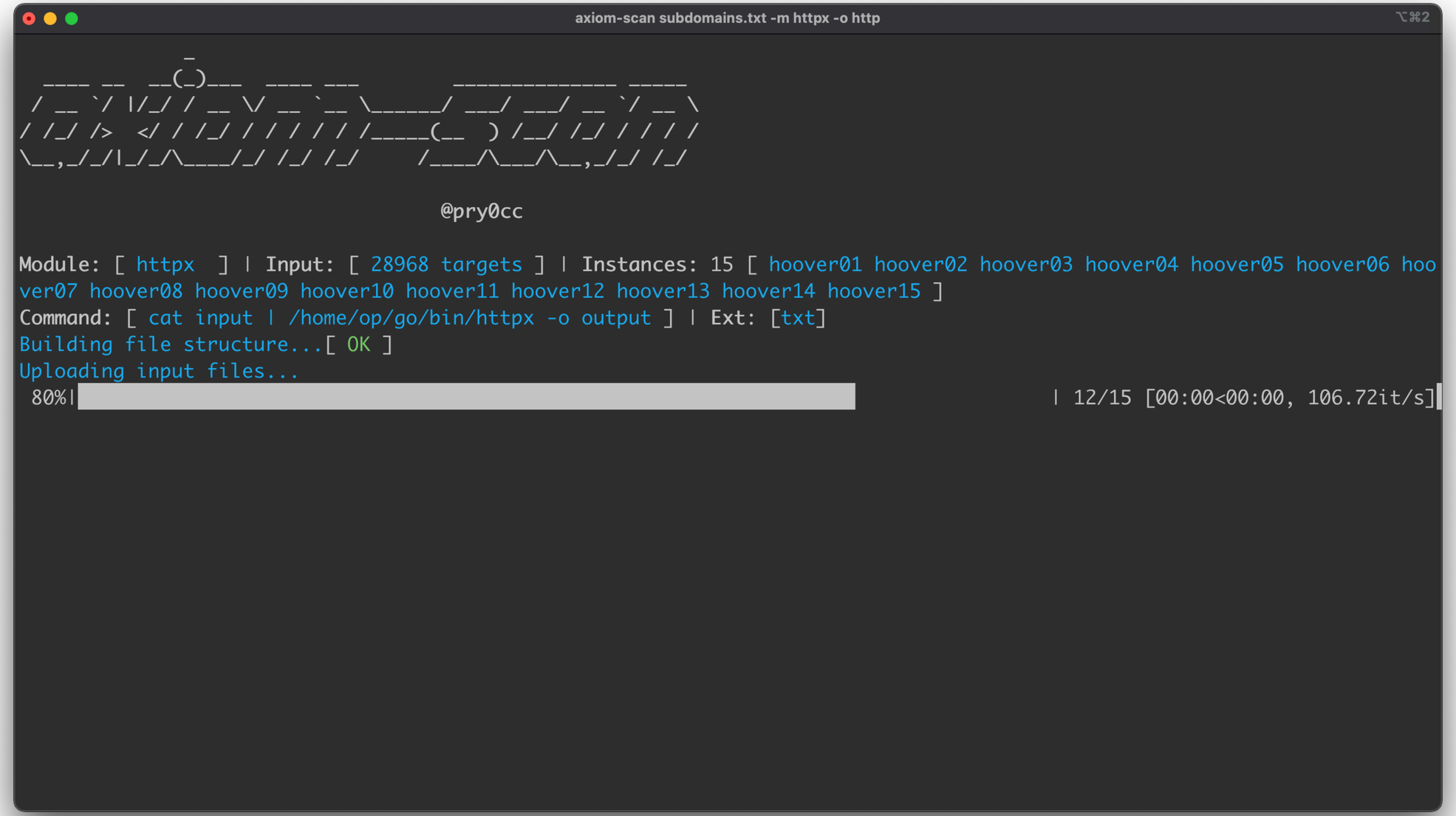
axiom-scan --list

List your available axiom-scan modules



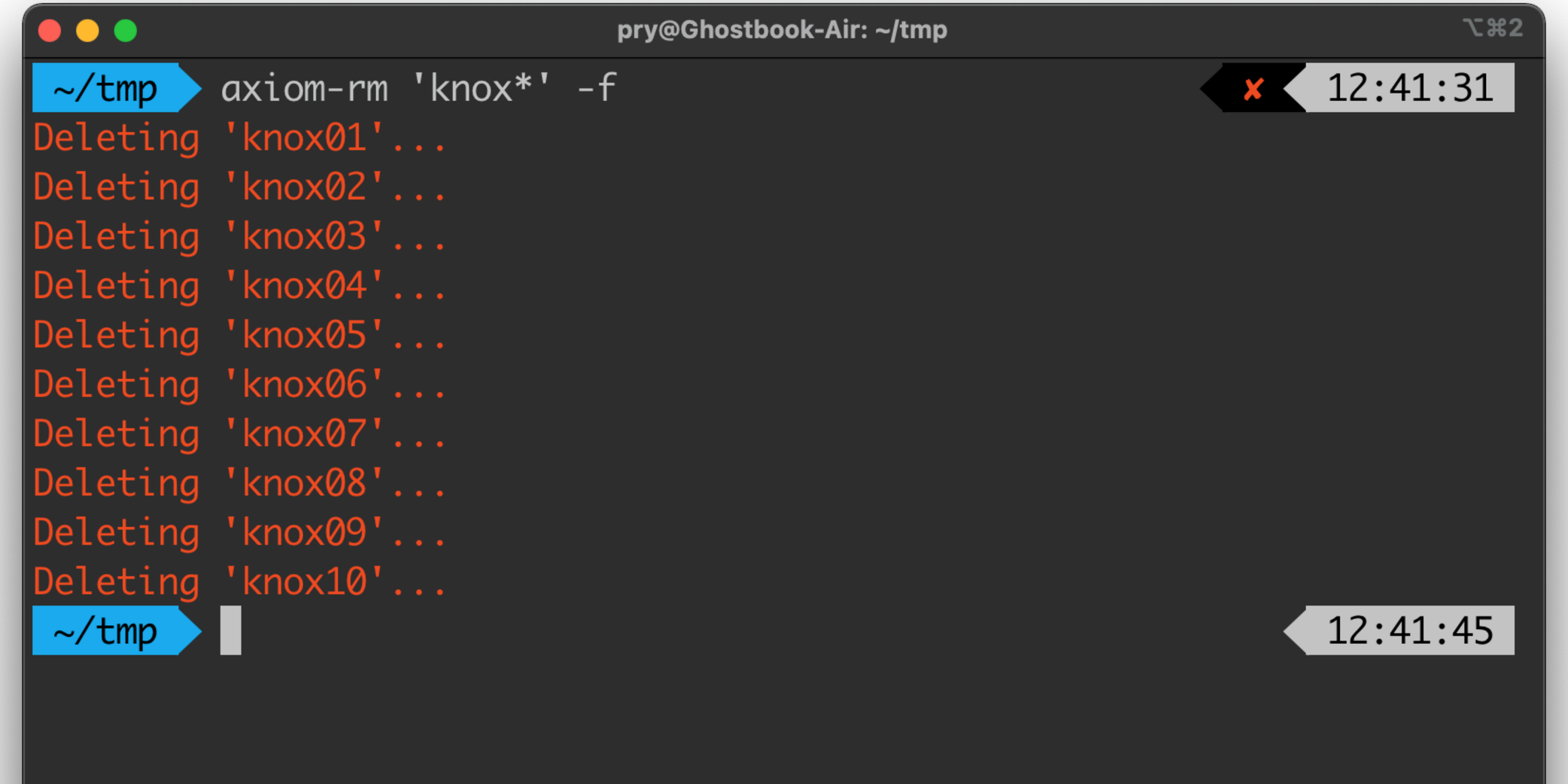
axiom-scan input.txt -m module -o output.txt

Scan your input using selected module



axiom-rm ‘query*’

Delete your instances



Live Demo

Q & A

dWdnY2Y6Ly9mcnBoZXZnbGdlbnZ5Zi5wYnovbmNjL25wcGJoYWcvY2ViemJndmJhZj9jZWJ6YnBicXI9UEQwODlHOUlEWQ==

Thank you!

twitter.com/pry0cc
github.com/pry0cc/axiom
github.com/pry0cc/nahamcon-axiom-demo-2021