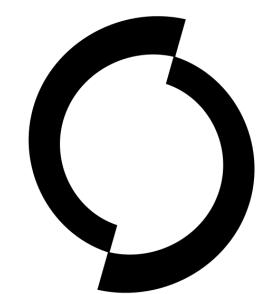


a x i o m

The dynamic infrastructure framework for everybody

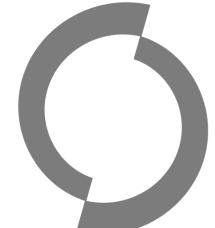


@pry0cc // Ben Bidmead - 0x00sec.org

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.
- $15 \text{ instances} \times 2 \text{ hours} = 15 * 0.007 * 2 == \$0.21 / 21 \text{ cents}$



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?



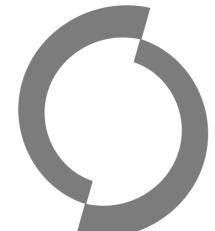
What does axiom come with?

Tools

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

Wordlists

- Assetnote
- SecLists
- Jhaddix-all.txt

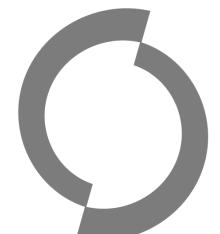
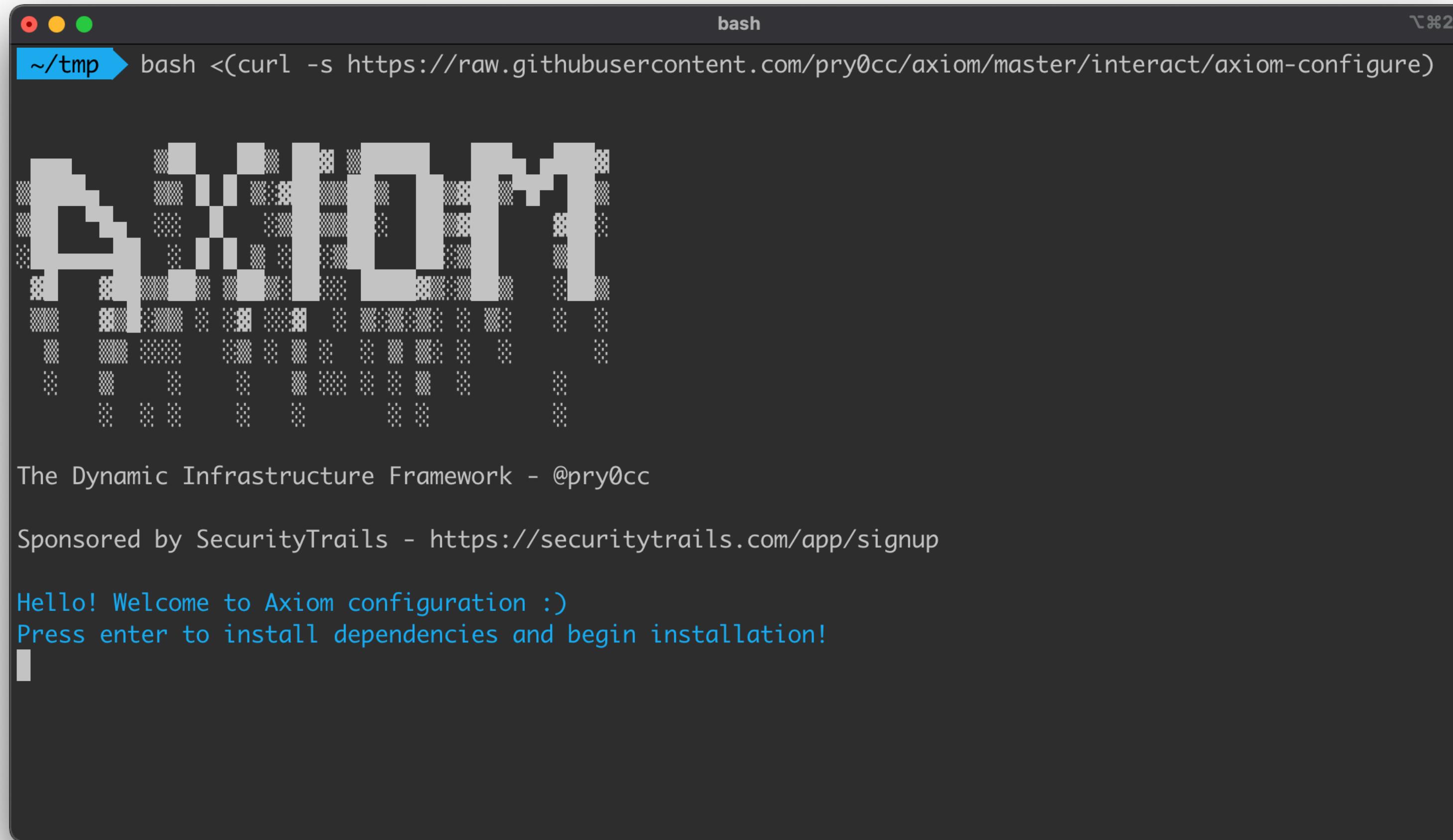


Crash Course Introduction



Installation

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



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

axiom-init

```
op@home ➤ ~ axiom-init
Initializing 'jarvis21'
>> T-Minus 259 to full initialization...
```

Initialize a single instance

```
op@home: ~
op@home ➤ ~ axiom-init
Initializing 'jarvis21'
Initialized instance 'jarvis21' at '138.197.5.173'!
To connect, run 'axiom-ssh jarvis21' or 'axiom-connect'
x op@home ➤ ~ |
```



axiom-fleet -i=15

```
axiom-fleet -i=15
Initializing new fleet 'hoover' with 15 instances...
INITIALIZING IN 3 SECONDS, CTRL+C to quit...
Instances: [ hoover01 hoover02 hoover03 hoover04 hoover05 hoover06 hoover07
  hoover08 hoover09 hoover10 hoover11 hoover12 hoover13 hoover14 hoover15 ]
>> T-Minus 382 to fleet hoover initialization...
```

Initialize 15 instances

```
~ axiom-fleet -i=15
Initializing new fleet 'hoover' with 15 instances...
INITIALIZING IN 3 SECONDS, CTRL+C to quit...
Instances: [ hoover01 hoover02 hoover03 hoover04 hoover05 hoover06 hoover07
  hoover08 hoover09 hoover10 hoover11 hoover12 hoover13 hoover14 hoover15 ]
Initialized instance 'hoover15' at '104.248.1.172'!
Initialized instance 'hoover04' at '165.22.38.110'!
Initialized instance 'hoover12' at '134.122.6.54'!
Initialized instance 'hoover06' at '167.172.234.43'!
Initialized instance 'hoover07' at '165.227.216.108'!
Initialized instance 'hoover08' at '64.225.24.23'!
Initialized instance 'hoover05' at '167.71.166.17'!
Initialized instance 'hoover02' at '165.22.40.71'!
Initialized instance 'hoover11' at '134.122.12.242'!
Initialized instance 'hoover14' at '159.89.45.227'!
Initialized instance 'hoover13' at '159.89.45.209'!
Initialized instance 'hoover03' at '159.89.45.179'
>> T-Minus 221 to fleet hoover initialization...
```



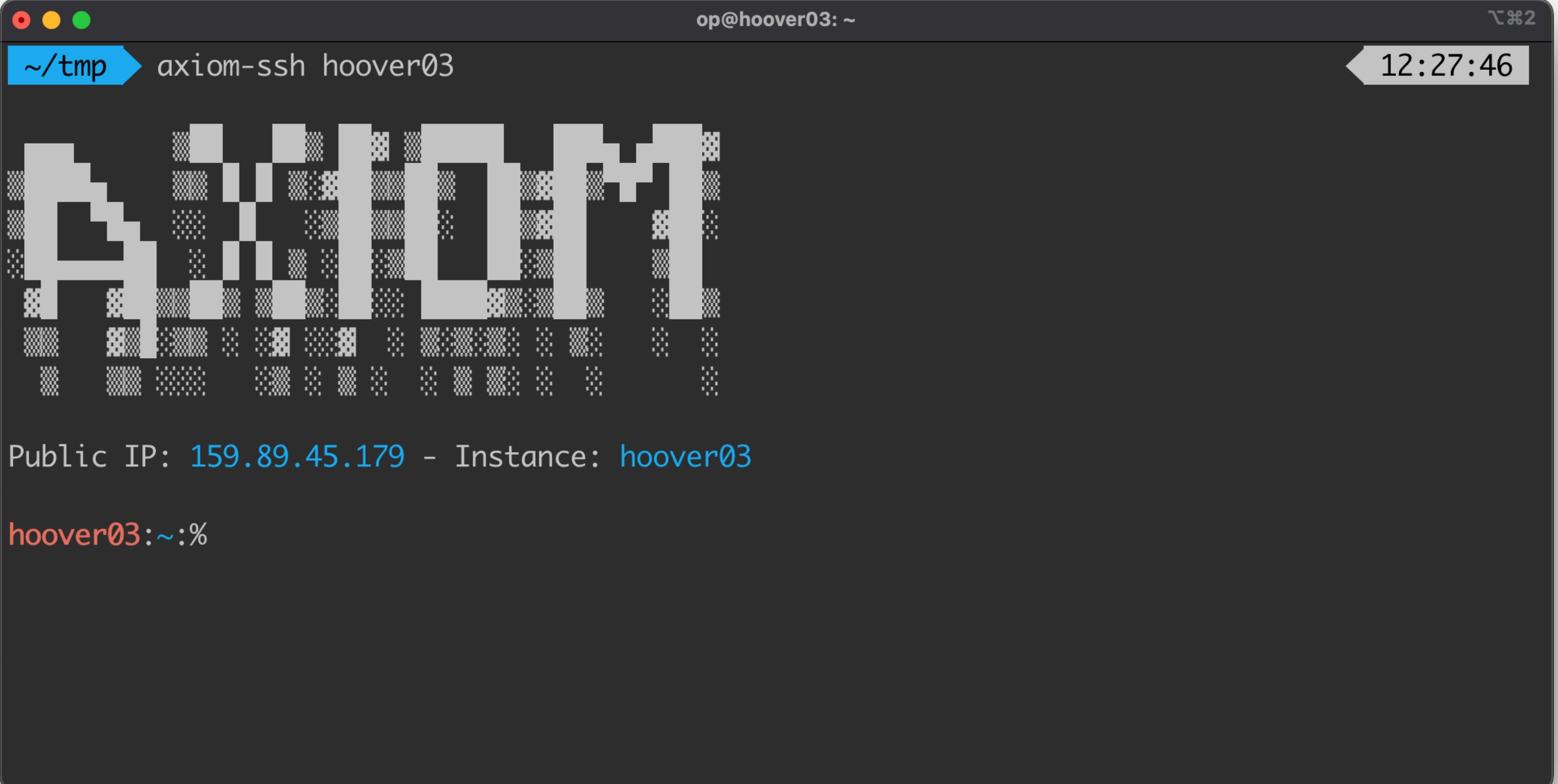
axiom-ls

List your instances

```
pry@Ghostbook-Air: ~ 11:41:08
~ ➔ axiom-ls
Instance IP Region Memory $/M
home 165.227.100.19 nyc3 s-2vcpu-4gb 20
ctf 104.131.0.82 nyc3 s-1vcpu-1gb 5
kevin 134.122.9.34 nyc3 s-1vcpu-1gb 5
jarvis21 138.197.5.173 nyc3 s-1vcpu-1gb 5
hoover01 174.138.58.74 nyc3 s-1vcpu-1gb 5
hoover02 165.22.40.71 nyc3 s-1vcpu-1gb 5
hoover03 159.89.45.179 nyc3 s-1vcpu-1gb 5
hoover04 165.22.38.110 nyc3 s-1vcpu-1gb 5
hoover05 167.71.166.17 nyc3 s-1vcpu-1gb 5
hoover06 167.172.234.43 nyc3 s-1vcpu-1gb 5
hoover08 64.225.24.23 nyc3 s-1vcpu-1gb 5
hoover07 165.227.216.108 nyc3 s-1vcpu-1gb 5
hoover09 159.89.45.186 nyc3 s-1vcpu-1gb 5
hoover10 159.89.45.200 nyc3 s-1vcpu-1gb 5
hoover11 134.122.12.242 nyc3 s-1vcpu-1gb 5
hoover12 134.122.6.54 nyc3 s-1vcpu-1gb 5
hoover13 159.89.45.209 nyc3 s-1vcpu-1gb 5
hoover14 159.89.45.227 nyc3 s-1vcpu-1gb 5
hoover15 104.248.1.172 nyc3 s-1vcpu-1gb 5
- - - Total $110
~ ➔ 11:41:09
```

axiom-ssh

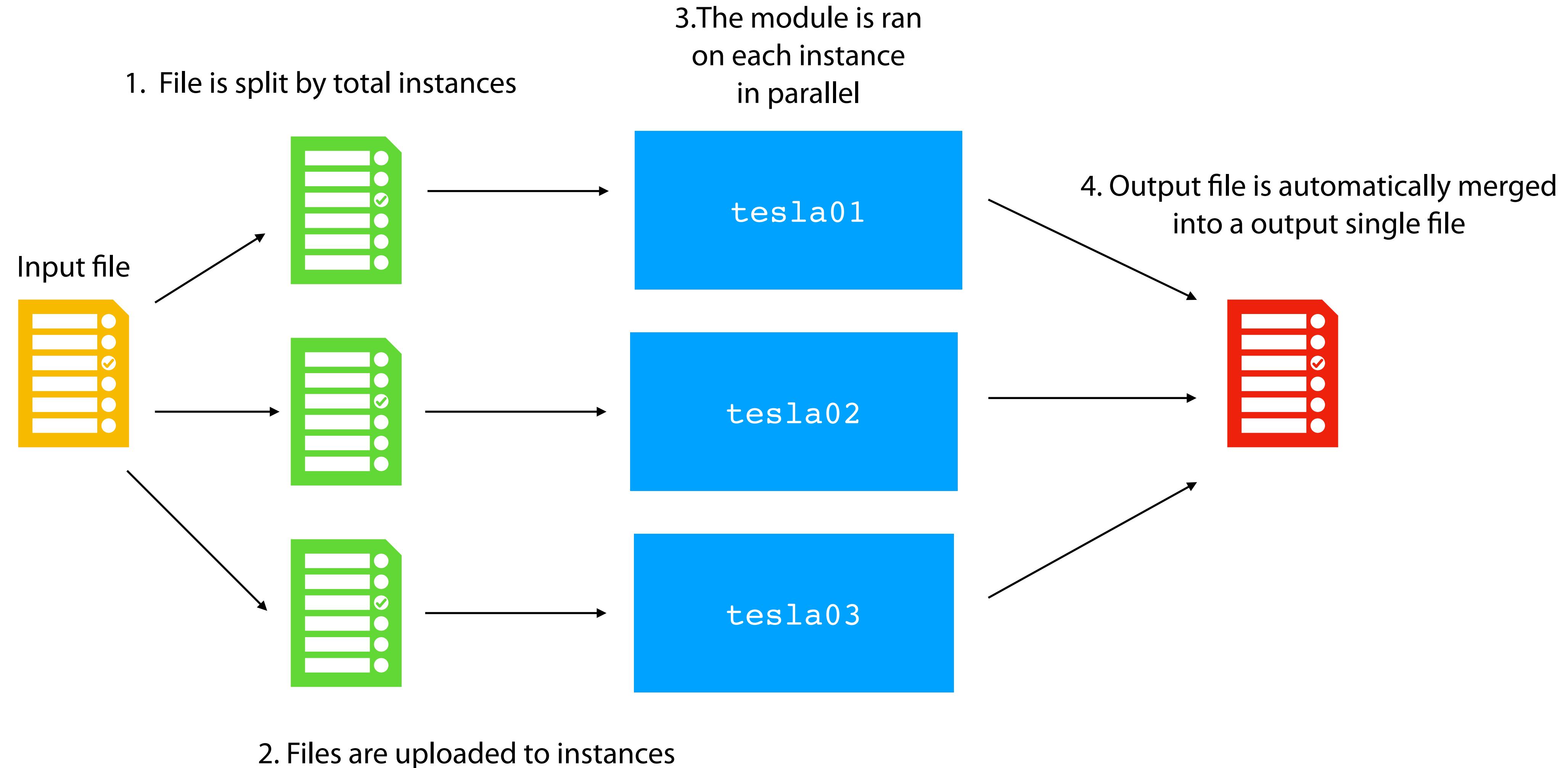
SSH into an instance



A terminal window titled "op@hoover03: ~" with a blue status bar showing the path "~/tmp" and the command "axiom-ssh hoover03". The status bar also shows the time "12:27:46". The terminal displays a pixelated version of the Axiom logo, which is a stylized letter 'A' composed of various shades of gray and black pixels. Below the logo, the text "Public IP: 159.89.45.179 - Instance: hoover03" is displayed in light blue. At the bottom of the terminal, the prompt "hoover03:~:%" is shown in red.



How distributed scanning works



dWdnY2Y6Ly9mcnBoZXZnbGdlbnZ5Zi5wYnovbmNjL25wcGJ0YWcvY2ViemJndmJhZj9jZWJ6YnBicXI9UEQwODlHOUEWQ==

Scan modules

The anatomy of an axiom-scan module



A terminal window with a dark background and light-colored text. The title bar shows "pry@Ghostbook-Air: ~/tmp". The command entered is "cat ~/.axiom/modules/httpx.json | jq". The output is a JSON array containing one object:

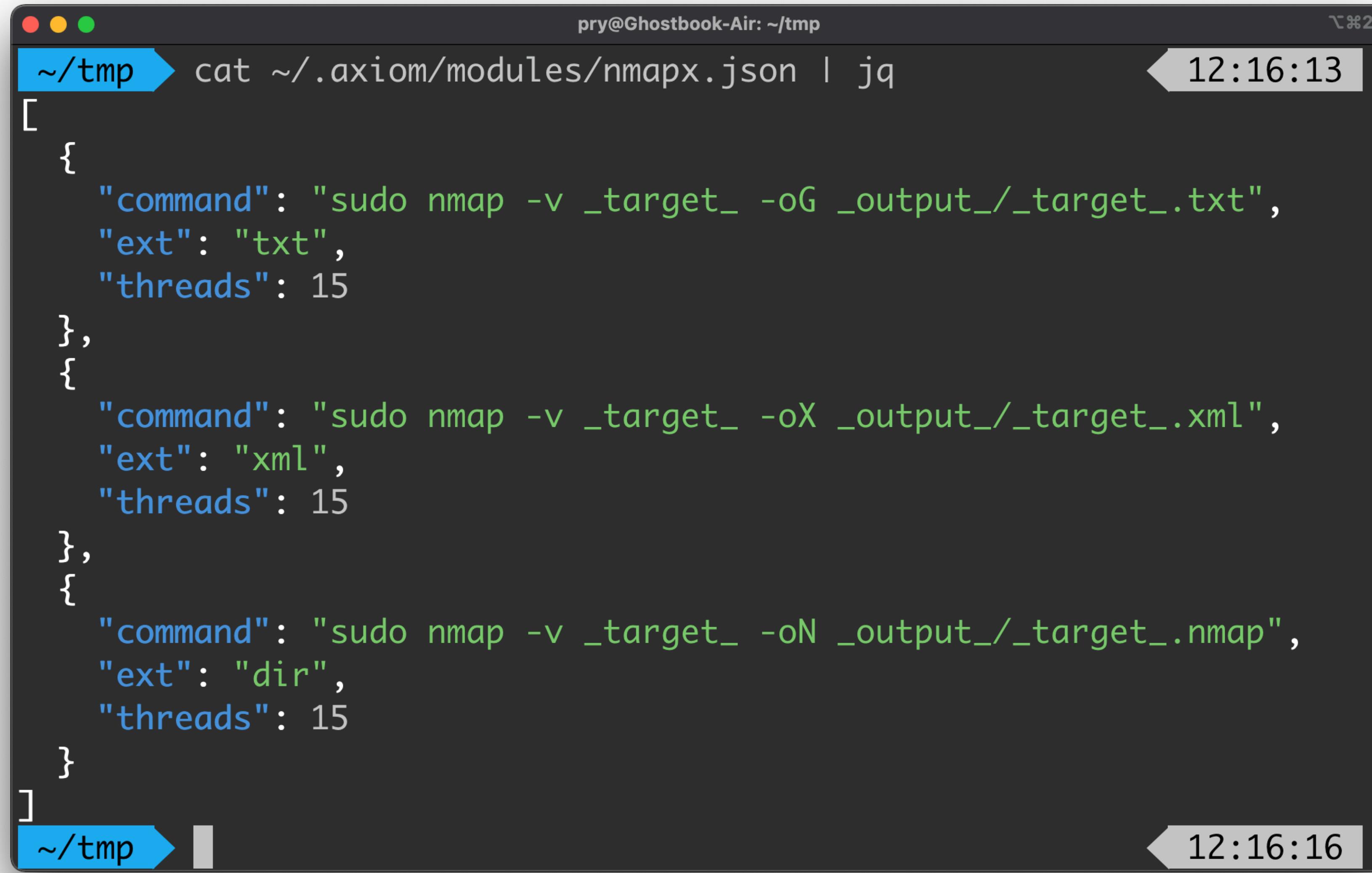
```
[{"command": "cat input | /home/op/go/bin/httpx -o output", "ext": "txt"}]
```

Two timestamp markers "12:14:11" are visible on the right side of the terminal window.



Oneshot modules

For tools that take a single target as input



A terminal window titled "pry@Ghostbook-Air: ~/tmp" showing the output of a command. The command is "cat ~/.axiom/modules/nmapx.json | jq". The output is a JSON array containing three objects, each defining a module. Each module has a "command" field (a green string) and "ext" and "threads" fields (both blue). The "command" field for each module uses the placeholder "_target_" which is highlighted in green.

```
[{"command": "sudo nmap -v _target_ -oG _output/_target_.txt", "ext": "txt", "threads": 15}, {"command": "sudo nmap -v _target_ -oX _output/_target_.xml", "ext": "xml", "threads": 15}, {"command": "sudo nmap -v _target_ -oN _output/_target_.nmap", "ext": "dir", "threads": 15}]
```

axiom-scan --list

List your available axiom-scan modules

```
~ ➜ axiom-scan --list
Available Modules:
MODULE
/Users/pry/.axiom/modules//soxy
/Users/pry/.axiom/modules//amass
/Users/pry/.axiom/modules//meg
/Users/pry/.axiom/modules//nuclei
/Users/pry/.axiom/modules//gau
/Users/pry/.axiom/modules//ffuf
/Users/pry/.axiom/modules//gowitness
/Users/pry/.axiom/modules//findomain
/Users/pry/.axiom/modules//arjun
/Users/pry/.axiom/modules//masscan
/Users/pry/.axiom/modules//dnsx
/Users/pry/.axiom/modules//gospider
/Users/pry/.axiom/modules//hakrawler
/Users/pry/.axiom/modules//feroxbuster
/Users/pry/.axiom/modules//subfinder
/Users/pry/.axiom/modules//rustscan
/Users/pry/.axiom/modules//shuffledns
/Users/pry/.axiom/modules//ffuz
/Users/pry/.axiom/modules//fff
/Users/pry/.axiom/modules//httpprobe
/Users/pry/.axiom/modules//cngo
/Users/pry/.axiom/modules//naabu
/Users/pry/.axiom/modules//nmap
/Users/pry/.axiom/modules//massdns
/Users/pry/.axiom/modules//gorgo
/Users/pry/.axiom/modules//dnsgen
/Users/pry/.axiom/modules//httpx
/Users/pry/.axiom/modules//dalfox
/Users/pry/.axiom/modules//tlstout
/Users/pry/.axiom/modules//nmapx

COMMAND
cat input | /home/op/bin/soxy | tee output
/usr/bin/amass enum -df input -o output
/home/op/go/bin/meg -v / input output
/home/op/go/bin/nuclei -silent -update-templates ; cat input | /home/op/go/bin/nuclei -t _wordlist_ -o output
cat input | /home/op/go/bin/gau | tee output
/home/op/bin/ffuf -t 150 -w _wordlist_ -u '_target_/FUZZ' -of csv -o _output_/_cleantarget_ -ac
gowitness file -f input -P output
/usr/bin/findomain -f input -u output
/usr/local/bin/arjun -i input -oT output
sudo masscan -iL input -oG output
cat input | /home/op/bin/dnsx -silent -r /home/op/lists/resolvers.txt -o output
cat input | /home/op/bin/gospider -S - --depth 3 -v -t 50 -c 3 -o output
cat input | /home/op/bin/hakrawler | tee output
/usr/bin/feroxbuster -u _target_ -w _wordlist_ -o _output_/_cleantarget_
/home/op/bin/subfinder -silent -d _target_ -o _output_/_target_
/usr/bin/rustscan -a input -g | tee output
echo _target_ | /home/op/bin/shuffledns -v -d _target_ -r /home/op/lists/resolvers.txt -w _wordlist_ -o _output_/_target_
cat input | /home/op/bin/ffuz -s -o output
cat input | /home/op/bin/fff | tee output
cat input | /home/op/bin/httpprobe | tee output
/home/op/bin/cngo -f input | tee output
cat input | /home/op/bin/naabu -o output
sudo nmap -iL input -oG output
sudo /usr/bin/massdns -r /home/op/lists/resolvers.txt -t A -o F input -w output
/home/op/bin/gorgo.py -i input -o output
cat input | dnsgen -l tee output
cat input | /home/op/bin/httpx -o output
/home/op/bin/dalfox file input -o output
cat input | /home/op/bin/tlstout -o output
sudo nmap -v _target_ -oG _output_/_target_.txt
```

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

Scan your input using selected module

```
axiom-scan subdomains.txt -m httpx -o http
@pry0cc

Module: [ httpx ] | Input: [ 28968 targets ] | Instances: 15 [ hoover01 hoover02 hoover03 hoover04 hoover05 hoover06 hoover07 hoover08 hoover09 hoover10 hoover11 hoover12 hoover13 hoover14 hoover15 ]
Command: [ cat input | /home/op/go/bin/httpx -o output ] | Ext: [txt]
Building file structure...[ OK ]
Uploading input files...
80% | 12/15 [00:00<00:00, 106.72it/s]
```

axiom-rm 'query*'

Delete your instances

A screenshot of a terminal window titled "pry@Ghostbook-Air: ~/tmp". The window shows the command "axiom-rm 'knox*' -f" being run in the directory "~/tmp". The output of the command is displayed in red text, showing the deletion of ten instances named "knox01" through "knox10". The terminal has a dark theme with blue arrows for the command line and status bar. The status bar at the bottom right shows the time as 12:41:45.

```
~/tmp ➤ axiom-rm 'knox*' -f
Deleting 'knox01'...
Deleting 'knox02'...
Deleting 'knox03'...
Deleting 'knox04'...
Deleting 'knox05'...
Deleting 'knox06'...
Deleting 'knox07'...
Deleting 'knox08'...
Deleting 'knox09'...
Deleting 'knox10'...
~/tmp ➤ 12:41:45
```

Live Demo





Q & A

dWdnY2Y6Ly9mcnBoZXZnbGdlbnZ5Zi5wYnovbmNjL25wcGJ0YWcvY2ViemJndmJhZj9jZWJ6YnBicXI9UEQwODlHOULEWQ==

Thank you!

twitter.com/pry0cc

github.com/pry0cc/axiom

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

AXIOM IS SPONSORED BY

 **SecurityTrails**