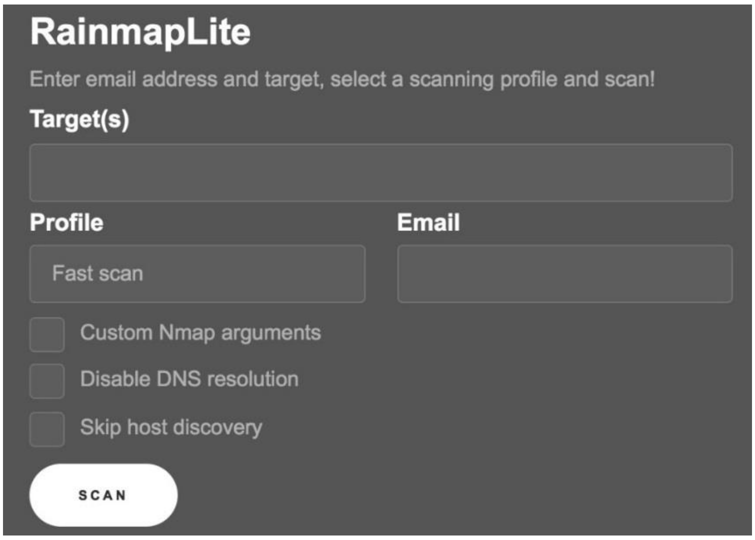
Chapter 1: Nmap Fundamentals



RainmapLite

Enter email address and target, select a scanning profile and scan!

Target(s)

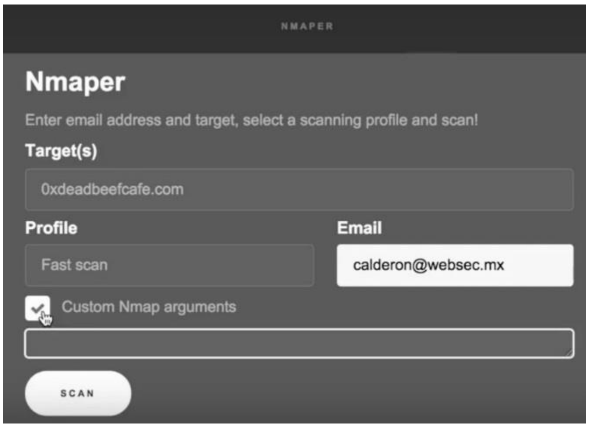
Profile: Fast scan

Email

□ Custom Nmap arguments

□ Disable DNS resolution

□ Skip host discovery



Nmaper

Enter email address and target, select a scanning profile and scan!

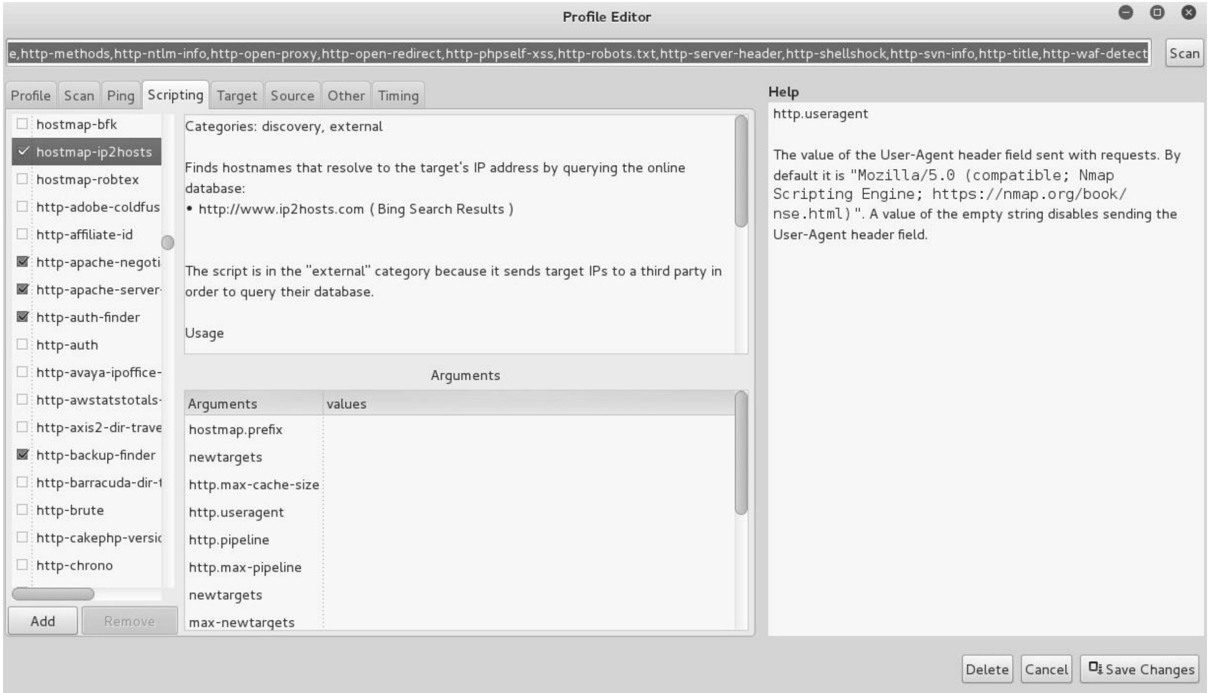
Target(s): 0xdeadbeefcafe.com

Profile: Fast scan

Email: calderon@websec.mx

☑ Custom Nmap arguments

Chapter 2: Getting Familiar with Nmap's Family



Profile Editor

e,http-methods,http-ntlm-info,http-open-proxy,http-open-redirect,http-phpself-xss,http-robots.txt,http-server-header,http-shellshock,http-svn-info,http-title,http-waf-detect

- □ hostmap-bfk
- ✓ hostmap-ip2hosts
- □ hostmap-robtex
- □ http-adobe-coldfus
- □ http-affiliate-id
- ☒ http-apache-negoti
- ☒ http-apache-server-
- ☒ http-auth-finder
- □ http-auth
- □ http-avaya-ipoffice-
- □ http-awstatstotals-
- □ http-axis2-dir-trave
- ☒ http-backup-finder
- □ http-barracuda-dir-t
- □ http-brute
- □ http-cakephp-versic
- □ http-chrono

Categories: discovery, external

Finds hostnames that resolve to the target's IP address by querying the online database:
• http://www.ip2hosts.com (Bing Search Results)

The script is in the "external" category because it sends target IPs to a third party in order to query their database.

Usage

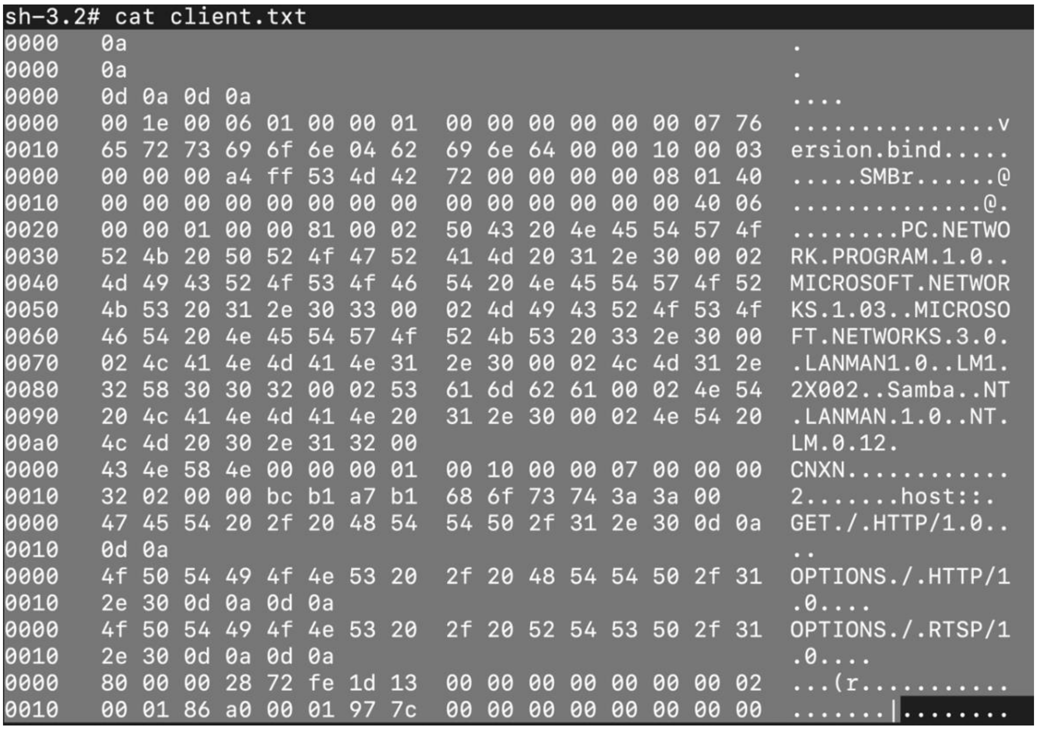
Arguments

Arguments	values
hostmap.prefix	
newtargets	
http.max-cache-size	
http.useragent	
http.pipeline	
http.max-pipeline	
newtargets	
max-newtargets	

Help

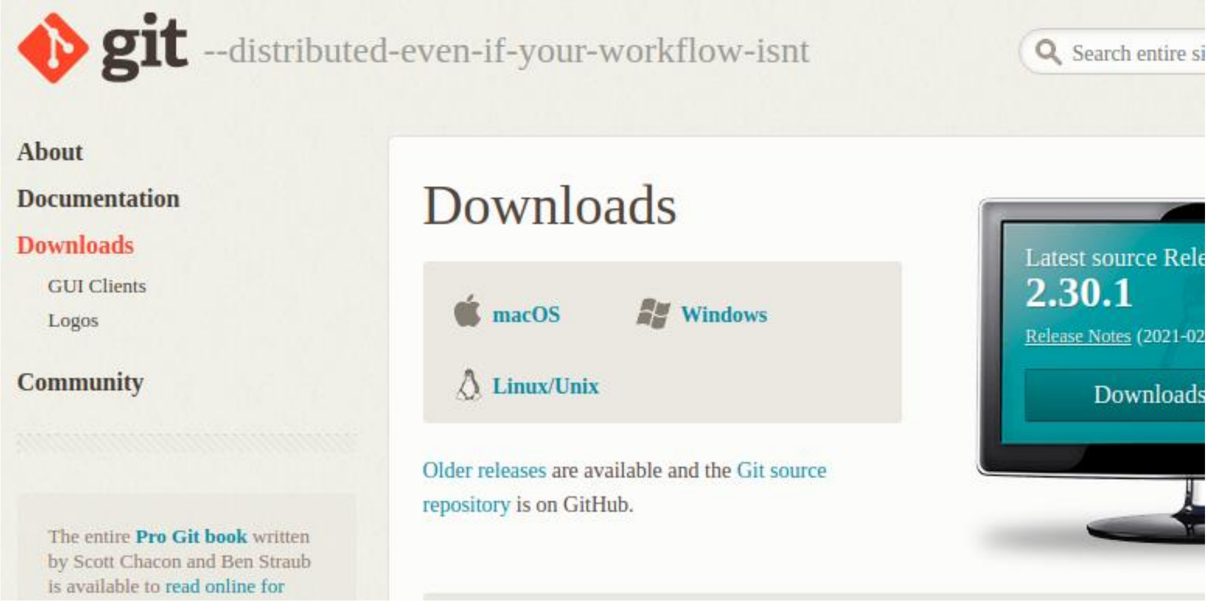
http.useragent

The value of the User-Agent header field sent with requests. By default it is "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)". A value of the empty string disables sending the User-Agent header field.



```
sh-3.2# cat client.txt
0000   0a                                                 .
0000   0a                                                 .
0000   0d 0a 0d 0a                                        ....
0000   00 1e 00 06 01 00 00 01  00 00 00 00 00 00 07 76   ...............v
0010   65 72 73 69 6f 6e 04 62  69 6e 64 00 00 10 00 03   ersion.bind.....
0000   00 00 00 a4 ff 53 4d 42  72 00 00 00 00 08 01 40   .....SMBr......@
0010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 40 06   ..............@.
0020   00 00 01 00 00 81 00 02  50 43 20 4e 45 54 57 4f   ........PC.NETWO
0030   52 4b 20 50 52 4f 47 52  41 4d 20 31 2e 30 00 02   RK.PROGRAM.1.0..
0040   4d 49 43 52 4f 53 4f 46  54 20 4e 45 54 57 4f 52   MICROSOFT.NETWOR
0050   4b 53 20 31 2e 30 33 00  02 4d 49 43 52 4f 53 4f   KS.1.03..MICROSO
0060   46 54 20 4e 45 54 57 4f  52 4b 53 20 33 2e 30 00   FT.NETWORKS.3.0.
0070   02 4c 41 4e 4d 41 4e 31  2e 30 00 02 4c 4d 31 2e   .LANMAN1.0..LM1.
0080   32 58 30 30 32 00 02 53  61 6d 62 61 00 02 4e 54   2X002..Samba..NT
0090   20 4c 41 4e 4d 41 4e 20  31 2e 30 00 02 4e 54 20   .LANMAN.1.0..NT.
00a0   4c 4d 20 30 2e 31 32 00                            LM.0.12.
0000   43 4e 58 4e 00 00 00 01  00 10 00 00 07 00 00 00   CNXN............
0010   32 02 00 00 bc b1 a7 b1  68 6f 73 74 3a 3a 00      2.......host::.
0000   47 45 54 20 2f 20 48 54  54 50 2f 31 2e 30 0d 0a   GET./.HTTP/1.0..
0010   0d 0a                                              ..
0000   4f 50 54 49 4f 4e 53 20  2f 20 48 54 54 50 2f 31   OPTIONS./.HTTP/1
0010   2e 30 0d 0a 0d 0a                                  .0....
0000   4f 50 54 49 4f 4e 53 20  2f 20 52 54 53 50 2f 31   OPTIONS./.RTSP/1
0010   2e 30 0d 0a 0d 0a                                  .0....
0000   80 00 00 28 72 fe 1d 13  00 00 00 00 00 00 00 02   ...(r...........
0010   00 01 86 a0 00 01 97 7c  00 00 00 00 00 00 00 00   ................
```

Chapter 3: Network Scanning



git --distributed-even-if-your-workflow-isnt

Search entire si

About

Documentation

Downloads

GUI Clients

Logos

Community

The entire Pro Git book written by Scott Chacon and Ben Straub is available to read online for

Downloads

macOS Windows

Linux/Unix

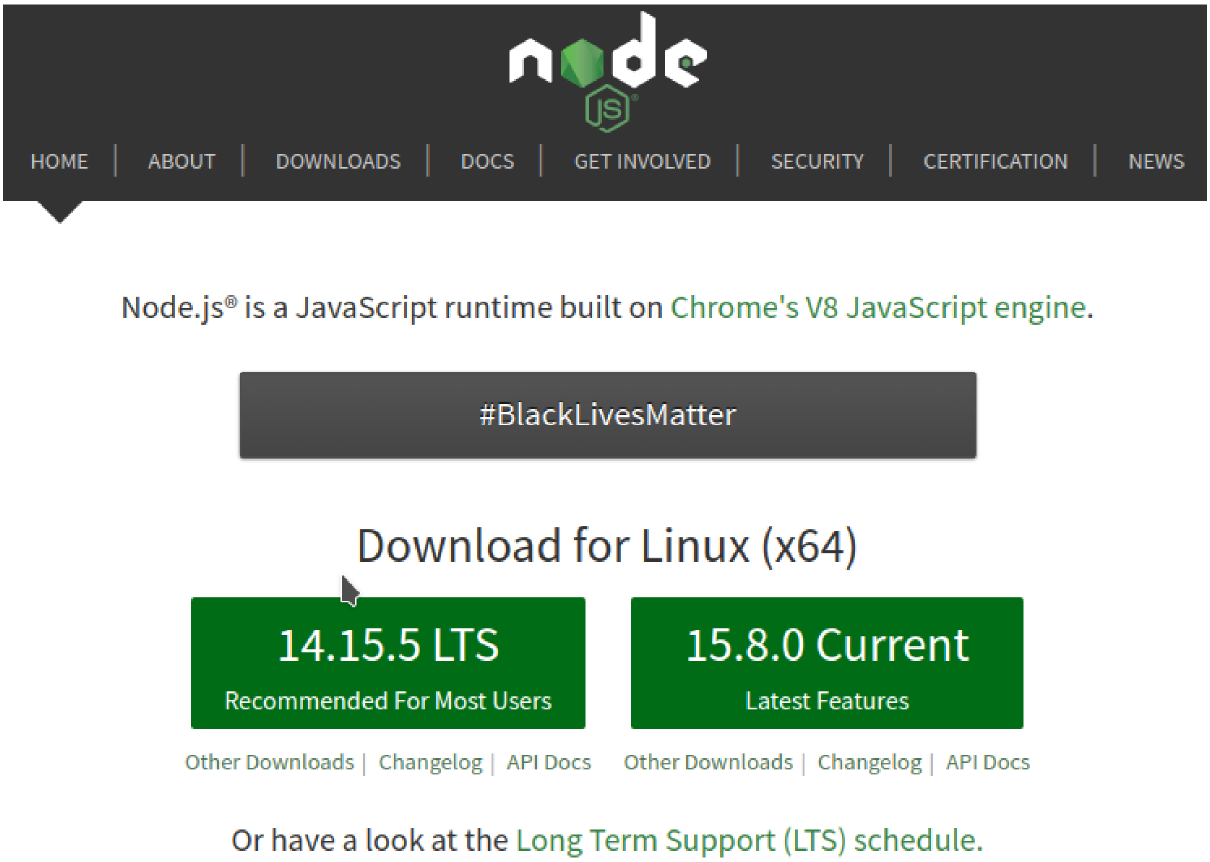
Older releases are available and the Git source repository is on GitHub.

Latest source Rele

2.30.1

Release Notes (2021-02

Downloads



HOME | ABOUT | DOWNLOADS | DOCS | GET INVOLVED | SECURITY | CERTIFICATION | NEWS

Node.js® is a JavaScript runtime built on Chrome's V8 JavaScript engine.

#BlackLivesMatter

Download for Linux (x64)

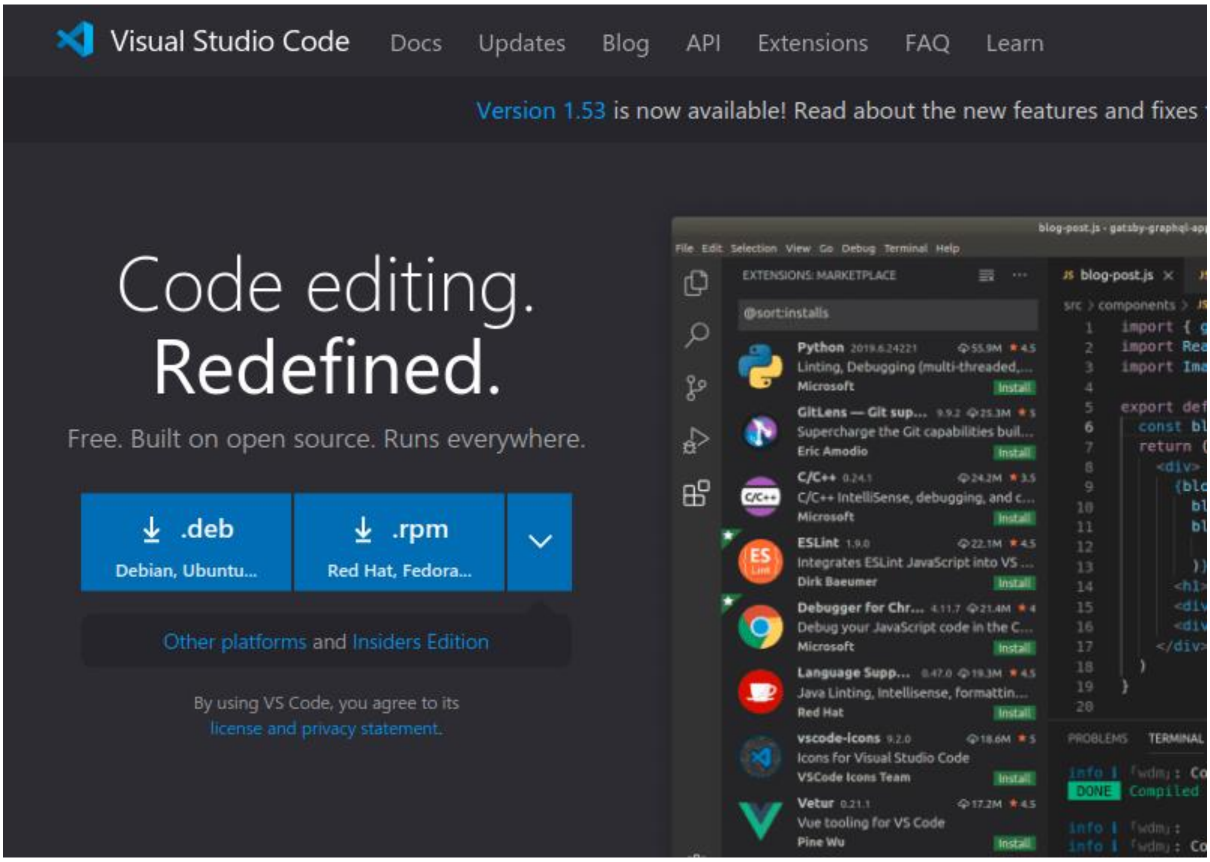
14.15.5 LTS
Recommended For Most Users

Other Downloads | Changelog | API Docs

15.8.0 Current
Latest Features

Other Downloads | Changelog | API Docs

Or have a look at the Long Term Support (LTS) schedule.



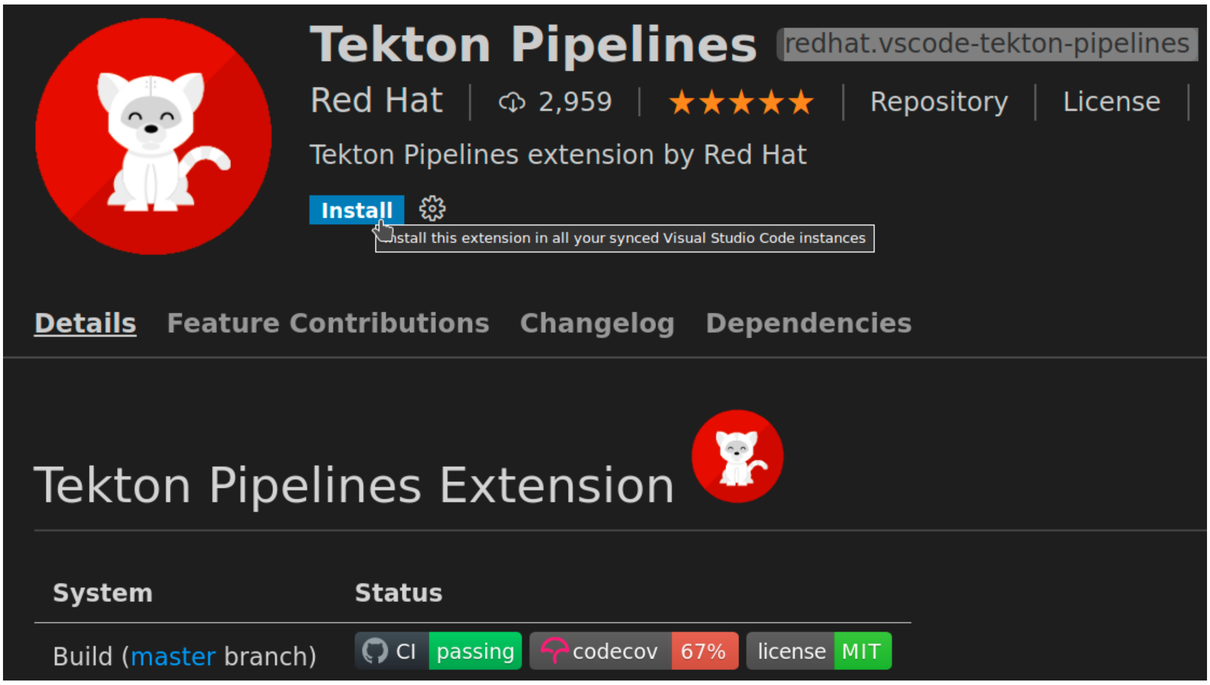
Version 1.53 is now available! Read about the new features and fixes

Code editing.
Redefined.

Free. Built on open source. Runs everywhere.

Other platforms and Insiders Edition

By using VS Code, you agree to its license and privacy statement.



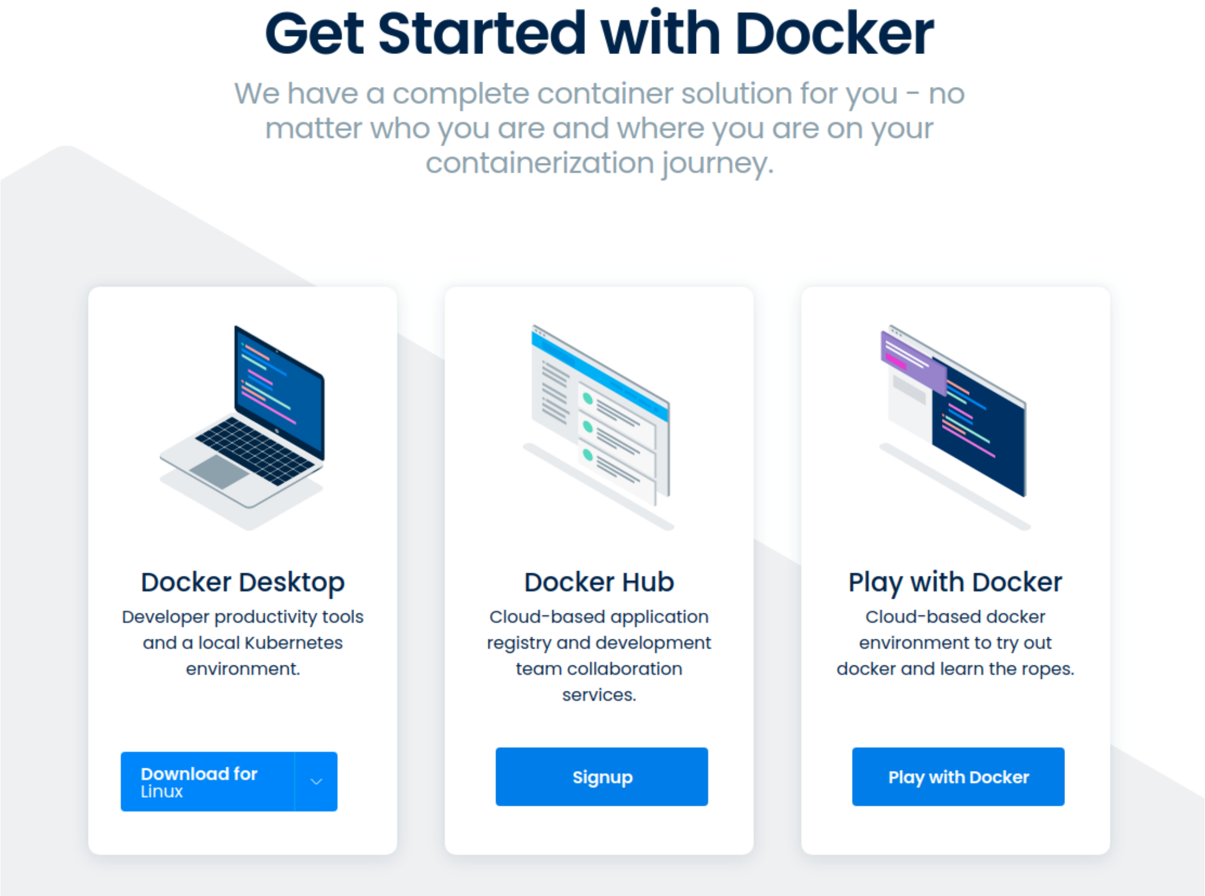
Tekton Pipelines

Tekton Pipelines extension by Red Hat

Install this extension in all your synced Visual Studio Code instances

Tekton Pipelines Extension

System	Status
Build (master branch)	CI passing · codecov 67% · license MIT



Get Started with Docker

We have a complete container solution for you - no matter who you are and where you are on your containerization journey.

Docker Desktop

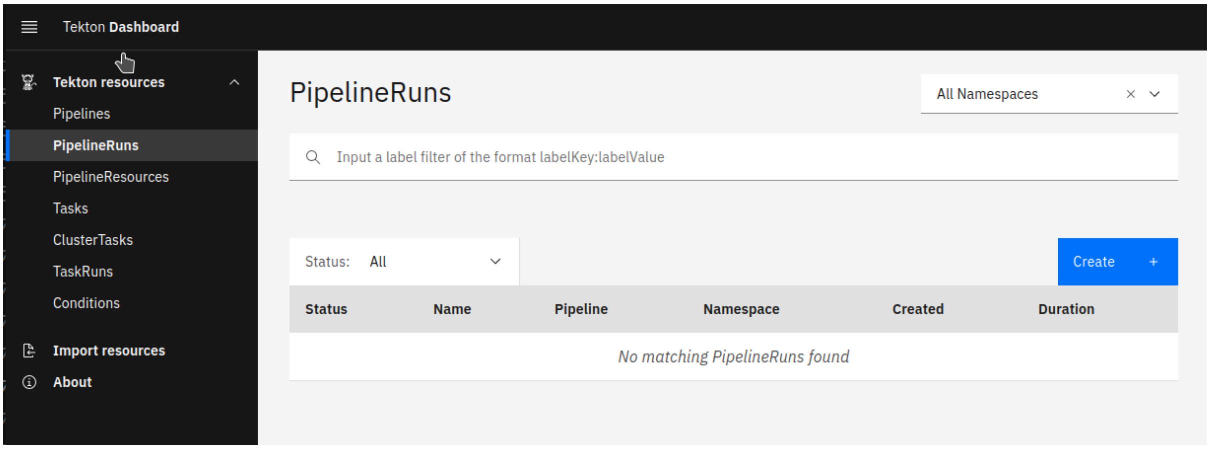
Developer productivity tools and a local Kubernetes environment.

Docker Hub

Cloud-based application registry and development team collaboration services.

Play with Docker

Cloud-based docker environment to try out docker and learn the ropes.



PipelineRuns

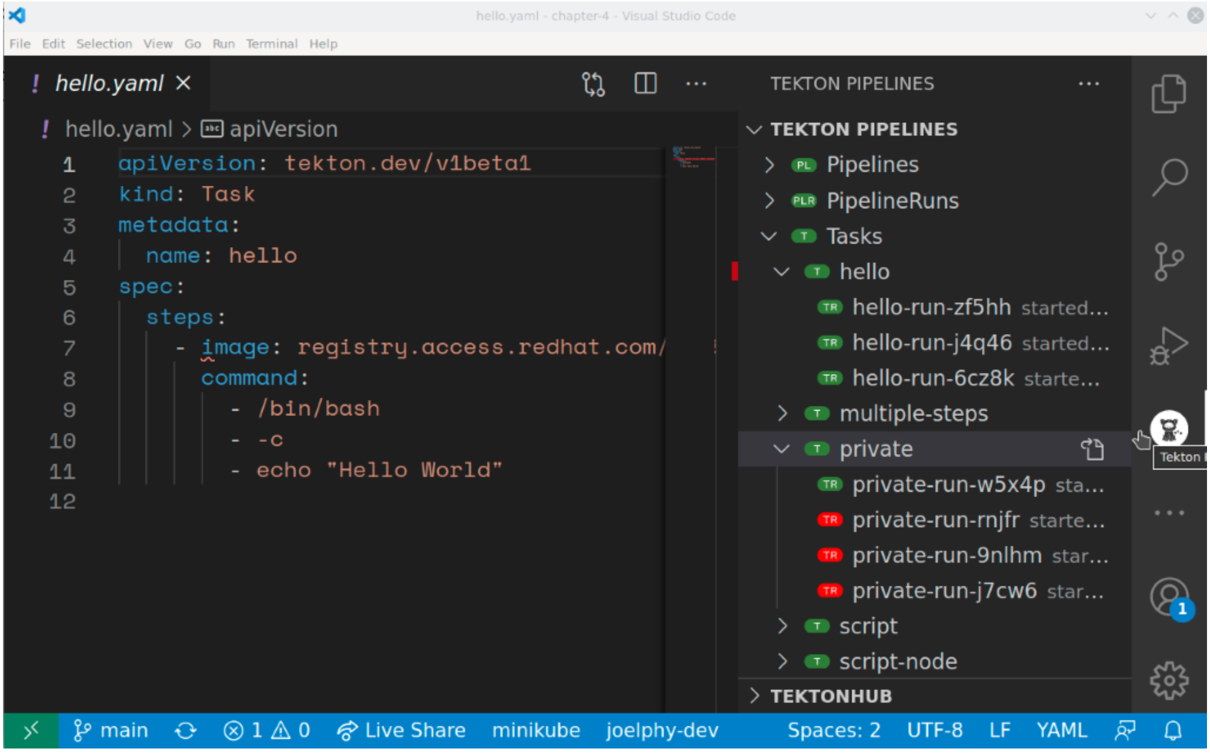
Input a label filter of the format labelKey:labelValue

Status: All

Status	Name	Pipeline	Namespace	Created	Duration

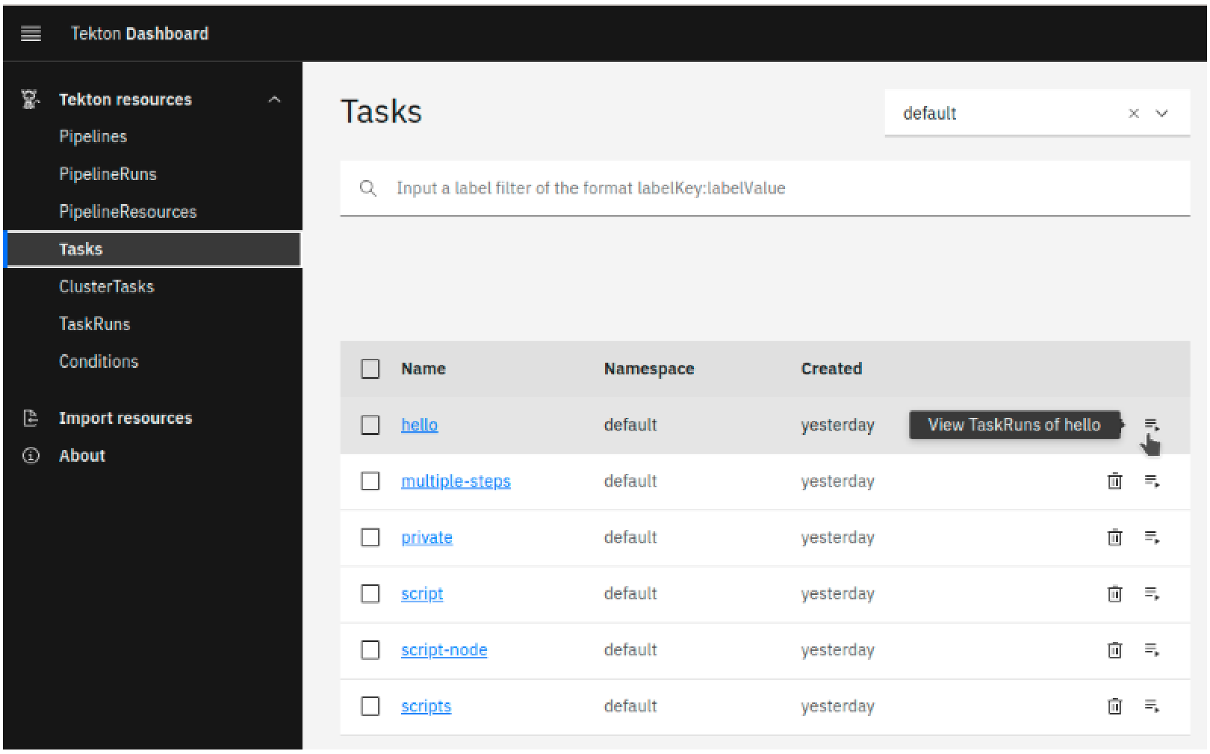
No matching PipelineRuns found

Chapter 4: Reconnaissance Tasks


hello.yaml - chapter-4 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
! hello.yaml ×
! hello.yaml > apiVersion
TEKTON PIPELINES
TEKTON PIPELINES
Pipelines
PipelineRuns
Tasks
hello
hello-run-zf5hh started...
hello-run-j4q46 started...
hello-run-6cz8k starte...
multiple-steps
private
private-run-w5x4p sta...
private-run-rnjfr starte...
private-run-9nlhm star...
private-run-j7cw6 star...
script
script-node
TEKTONHUB
Tekton
main
⊗ 1 ⚠ 0
Live Share
minikube
joelphy-dev
Spaces: 2
UTF-8
LF
YAML

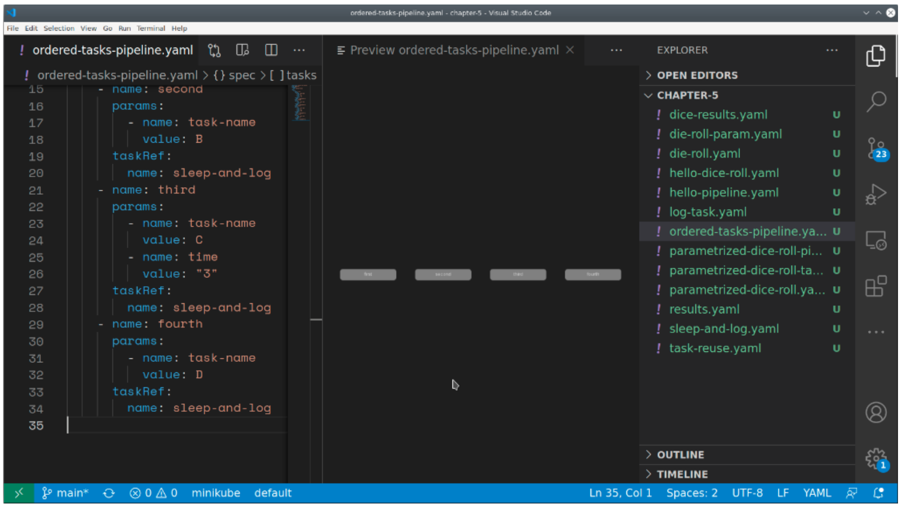
```yaml
apiVersion: tekton.dev/v1beta1
kind: Task
metadata:
  name: hello
spec:
  steps:
    - image: registry.access.redhat.com/
      command:
        - /bin/bash
        - -c
        - echo "Hello World"

```



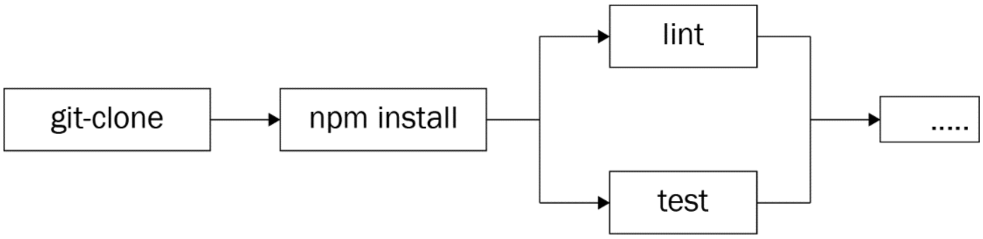
□	Name	Namespace	Created
□	hello	default	yesterday
□	multiple-steps	default	yesterday
□	private	default	yesterday
□	script	default	yesterday
□	script-node	default	yesterday
□	scripts	default	yesterday

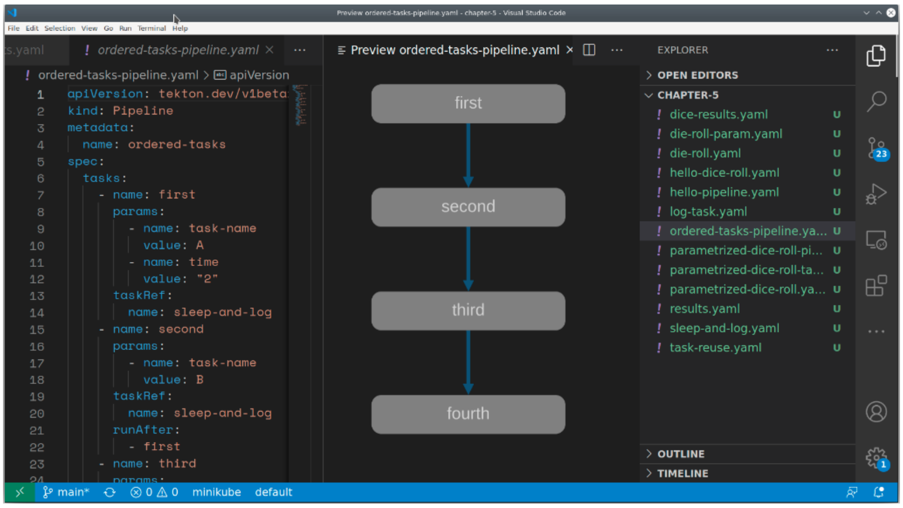
Chapter 5: Scanning Web Servers



ordered-tasks-pipeline.yaml - chapter-5 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
ordered-tasks-pipeline.yaml
ordered-tasks-pipeline.yaml > {} spec > [ ] tasks
Preview ordered-tasks-pipeline.yaml
EXPLORER
OPEN EDITORS
CHAPTER-5
dice-results.yaml U
die-roll-param.yaml U
die-roll.yaml U
hello-dice-roll.yaml U
hello-pipeline.yaml U
log-task.yaml U
ordered-tasks-pipeline.ya... U
parametrized-dice-roll-pi... U
parametrized-dice-roll-ta... U
parametrized-dice-roll.ya... U
results.yaml U
sleep-and-log.yaml U
task-reuse.yaml U
OUTLINE
TIMELINE
main* 0 0 minikube default
Ln 35, Col 1 Spaces: 2 UTF-8 LF YAML

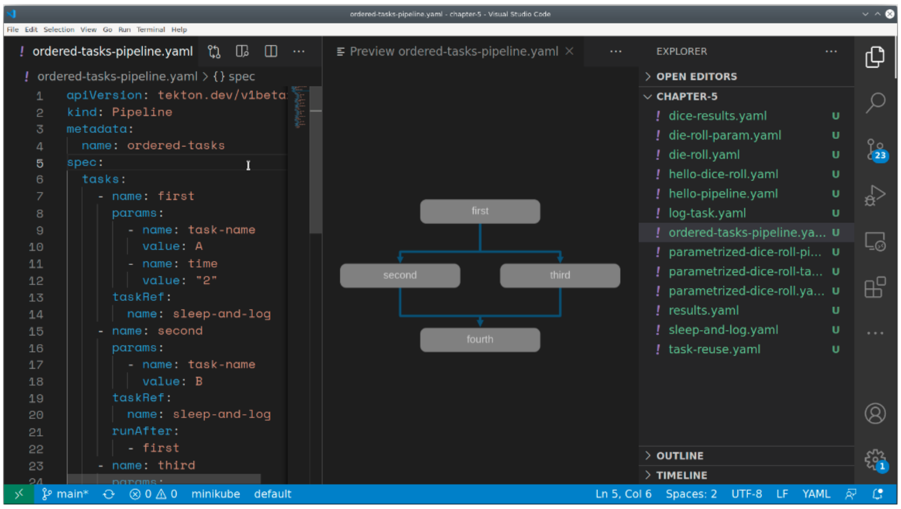
```
    - name: second
      params:
        - name: task-name
          value: B
      taskRef:
        name: sleep-and-log
    - name: third
      params:
        - name: task-name
          value: C
        - name: time
          value: "3"
      taskRef:
        name: sleep-and-log
    - name: fourth
      params:
        - name: task-name
          value: D
      taskRef:
        name: sleep-and-log
```



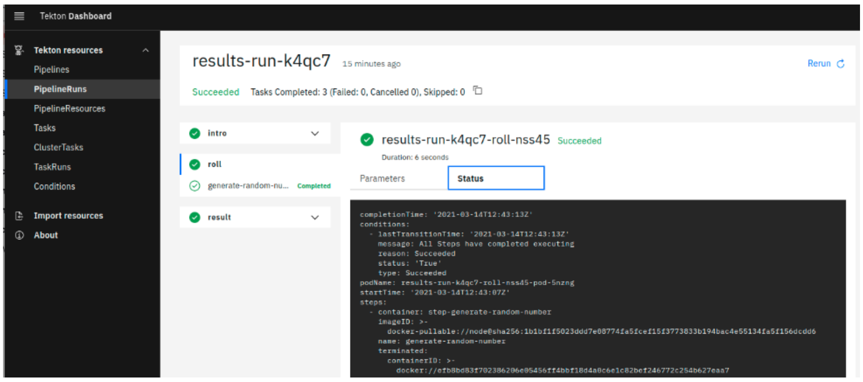


Preview ordered-tasks-pipeline.yaml - chapter-5 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
s.yaml
ordered-tasks-pipeline.yaml
ordered-tasks-pipeline.yaml > apiVersion
Preview ordered-tasks-pipeline.yaml
first
second
third
fourth
EXPLORER
OPEN EDITORS
CHAPTER-5
dice-results.yaml U
die-roll-param.yaml U
die-roll.yaml U
hello-dice-roll.yaml U
hello-pipeline.yaml U
log-task.yaml U
ordered-tasks-pipeline.ya... U
parametrized-dice-roll-pi... U
parametrized-dice-roll-ta... U
parametrized-dice-roll.ya... U
results.yaml U
sleep-and-log.yaml U
task-reuse.yaml U
OUTLINE
TIMELINE
main* 0 0 minikube default

```
apiVersion: tekton.dev/v1beta
kind: Pipeline
metadata:
  name: ordered-tasks
spec:
  tasks:
    - name: first
      params:
        - name: task-name
          value: A
        - name: time
          value: "2"
      taskRef:
        name: sleep-and-log
    - name: second
      params:
        - name: task-name
          value: B
      taskRef:
        name: sleep-and-log
      runAfter:
        - first
    - name: third
      params:
```


ordered-tasks-pipeline.yaml - chapter-5 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
ordered-tasks-pipeline.yaml
ordered-tasks-pipeline.yaml > {} spec
Preview ordered-tasks-pipeline.yaml
first
second
third
fourth
EXPLORER
OPEN EDITORS
CHAPTER-5
dice-results.yaml U
die-roll-param.yaml U
die-roll.yaml U
hello-dice-roll.yaml U
hello-pipeline.yaml U
log-task.yaml U
ordered-tasks-pipeline.ya... U
parametrized-dice-roll-pi... U
parametrized-dice-roll-ta... U
parametrized-dice-roll.ya... U
results.yaml U
sleep-and-log.yaml U
task-reuse.yaml U
OUTLINE
TIMELINE
main* 0 0 minikube default
Ln 5, Col 6 Spaces: 2 UTF-8 LF YAML

```
apiVersion: tekton.dev/v1beta
kind: Pipeline
metadata:
  name: ordered-tasks
spec:
  tasks:
    - name: first
      params:
        - name: task-name
          value: A
        - name: time
          value: "2"
      taskRef:
        name: sleep-and-log
    - name: second
      params:
        - name: task-name
          value: B
      taskRef:
        name: sleep-and-log
      runAfter:
        - first
    - name: third
      params:
```



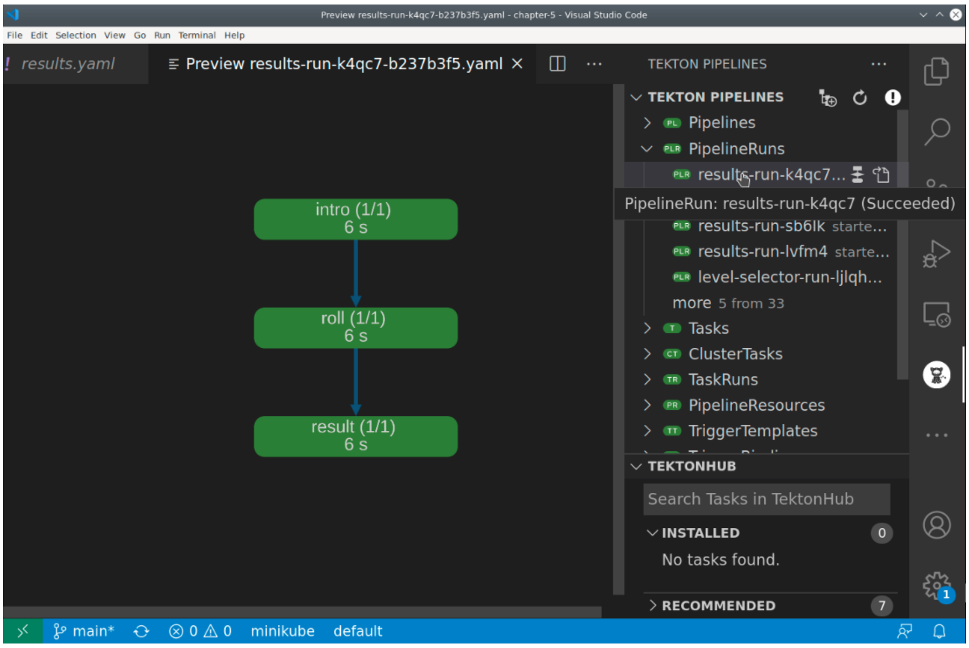
results-run-k4qc7 15 minutes ago

Succeeded Tasks Completed: 3 (Failed: 0, Cancelled 0), Skipped: 0

results-run-k4qc7-roll-nss45 Succeeded

Duration: 6 seconds

```
completionTime: '2021-03-14T12:43:13Z'
conditions:
  - lastTransitionTime: '2021-03-14T12:43:13Z'
    message: All Steps have completed executing
    reason: Succeeded
    status: 'True'
    type: Succeeded
podName: results-run-k4qc7-roll-nss45-pod-5nzng
startTime: '2021-03-14T12:43:07Z'
steps:
  - container: step-generate-random-number
    imageID: >-
      docker-pullable://node@sha256:1b1bf1f5023ddd7e08774fa5fcef15f3773833b194bac4e55134fa5f156dcdd6
    name: generate-random-number
    terminated:
      containerID: >-
        docker://efb8bd83f702386206e05456ff4bbf18d4a8c6e1c82bef246772c254b627eaa7
```


Preview results-run-k4qc7-b237b3f5.yaml - chapter-5 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
results.yaml
Preview results-run-k4qc7-b237b3f5.yaml
intro (1/1)
6 s
roll (1/1)
6 s
result (1/1)
6 s
TEKTON PIPELINES
TEKTON PIPELINES
PL Pipelines
PLR PipelineRuns
PLR results-run-k4qc7...
PipelineRun: results-run-k4qc7 (Succeeded)
PLR results-run-sb6lk starte...
PLR results-run-lvfm4 starte...
PLR level-selector-run-ljlqh...
more 5 from 33
T Tasks
CT ClusterTasks
TR TaskRuns
PR PipelineResources
TT TriggerTemplates
TEKTONHUB
Search Tasks in TektonHub
INSTALLED 0
No tasks found.
RECOMMENDED 7
main* 0 0 minikube default

Chapter 6: Scanning Databases

No Images

Chapter 7: Scanning Mail Servers

No Images

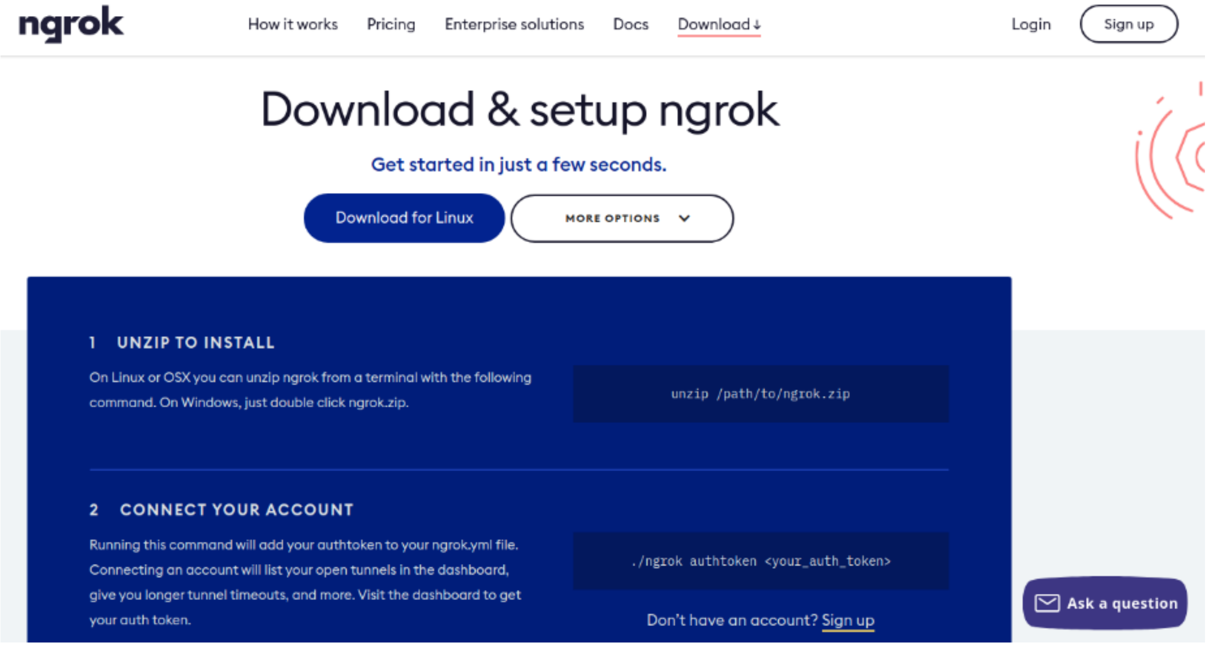
Chapter 8: Scanning Windows Systems

No Images

Chapter 9: Scanning ICS/SCADA Systems

No Images

Chapter 10: Scanning Mainframes



Download & setup ngrok

Get started in just a few seconds.

1 UNZIP TO INSTALL

On Linux or OSX you can unzip ngrok from a terminal with the following command. On Windows, just double click ngrok.zip.

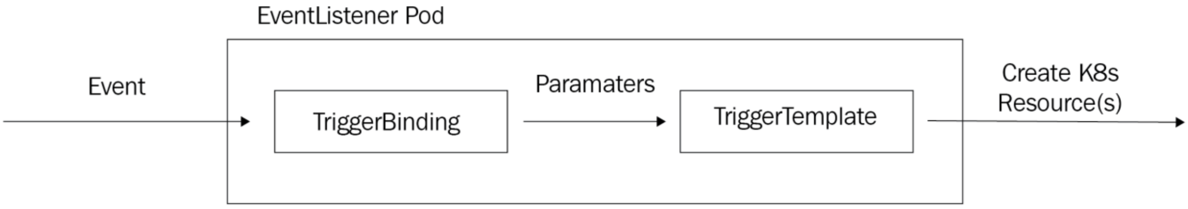
```
unzip /path/to/ngrok.zip
```

2 CONNECT YOUR ACCOUNT

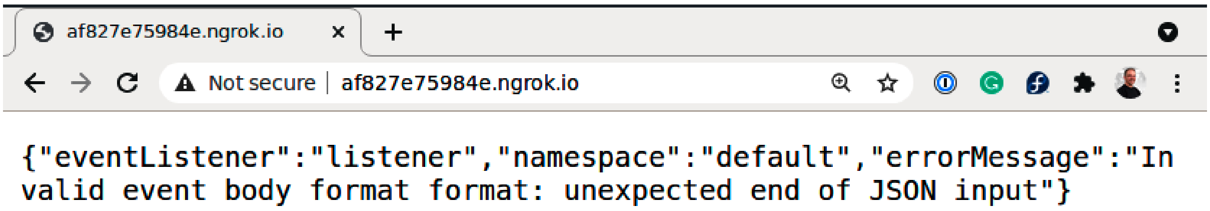
Running this command will add your authtoken to your ngrok.yml file. Connecting an account will list your open tunnels in the dashboard, give you longer tunnel timeouts, and more. Visit the dashboard to get your auth token.

```
./ngrok authtoken <your_auth_token>
```

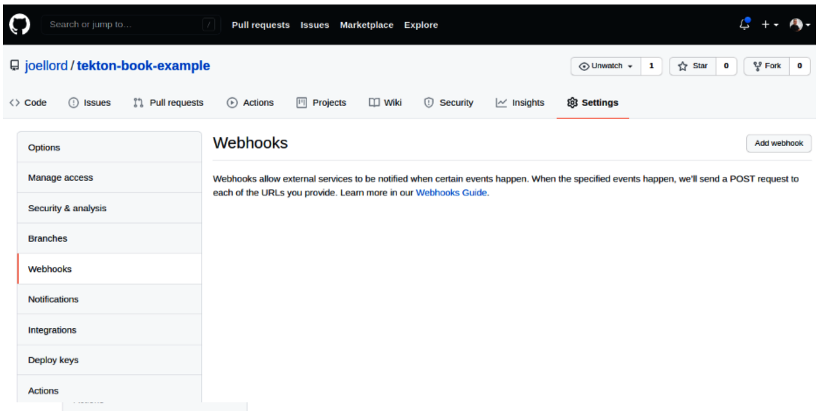
Don't have an account? Sign up



Chapter 11: Optimizing Scans

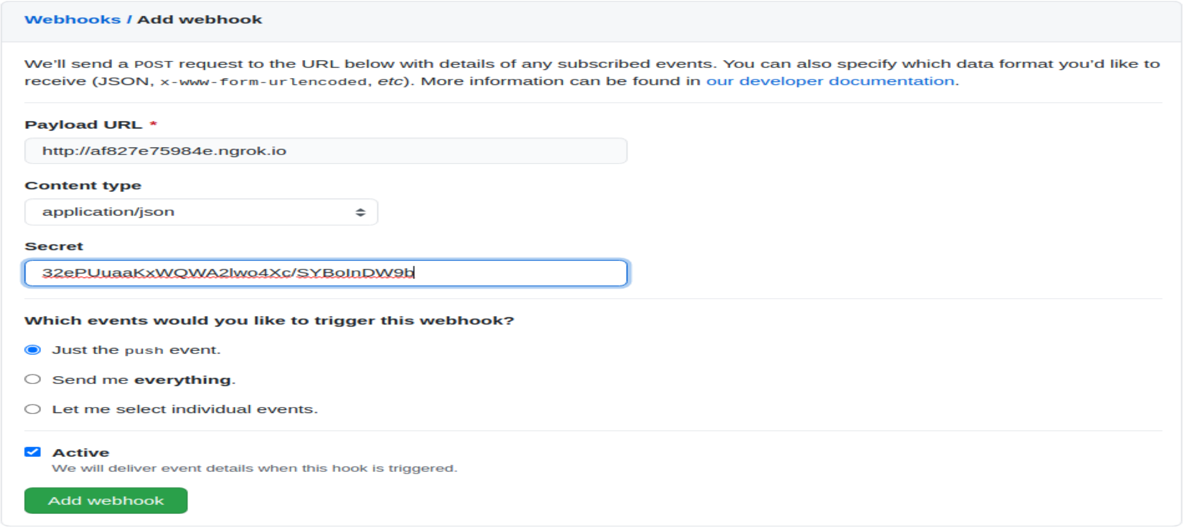


```
{"eventListener":"listener","namespace":"default","errorMessage":"Invalid event body format format: unexpected end of JSON input"}
```



Webhooks

Webhooks allow external services to be notified when certain events happen. When the specified events happen, we'll send a POST request to each of the URLs you provide. Learn more in our Webhooks Guide.



Webhooks / Add webhook

We'll send a POST request to the URL below with details of any subscribed events. You can also specify which data format you'd like to receive (JSON, x-www-form-urlencoded, *etc*). More information can be found in our developer documentation.

Payload URL *
http://af827e75984e.ngrok.io

Content type
application/json

Secret
32ePUuaaKxWQWA2lwo4Xc/SYBoInDW9b

Which events would you like to trigger this webhook?

● Just the push event.

○ Send me **everything**.

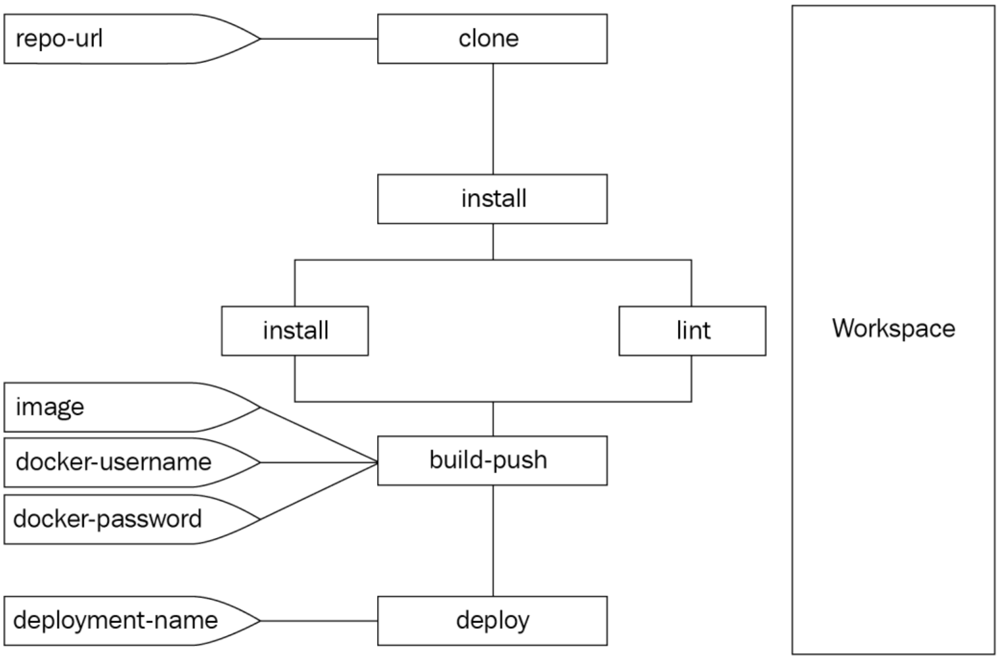
○ Let me select individual events.

☑ **Active**
We will deliver event details when this hook is triggered.

Chapter 12: Generating Scan Reports

No Images

Chapter 13: Developing for the Nmap Scripting Engine



Chapter 14: Exploiting Vulnerabilities with the Nmap Scripting Engine

No Images