Auth0 CTF x HackTheBox

Minh Giang

2021-10-19

Contents

WEB - EsQueElle

> We think our agency's login panel application might be vulnerable. Agent, could you assess the security of the website, and help us prevent malicious actors from gaining access to our confidential information?

As this is a web challenge, let's first look at the login page of the application.

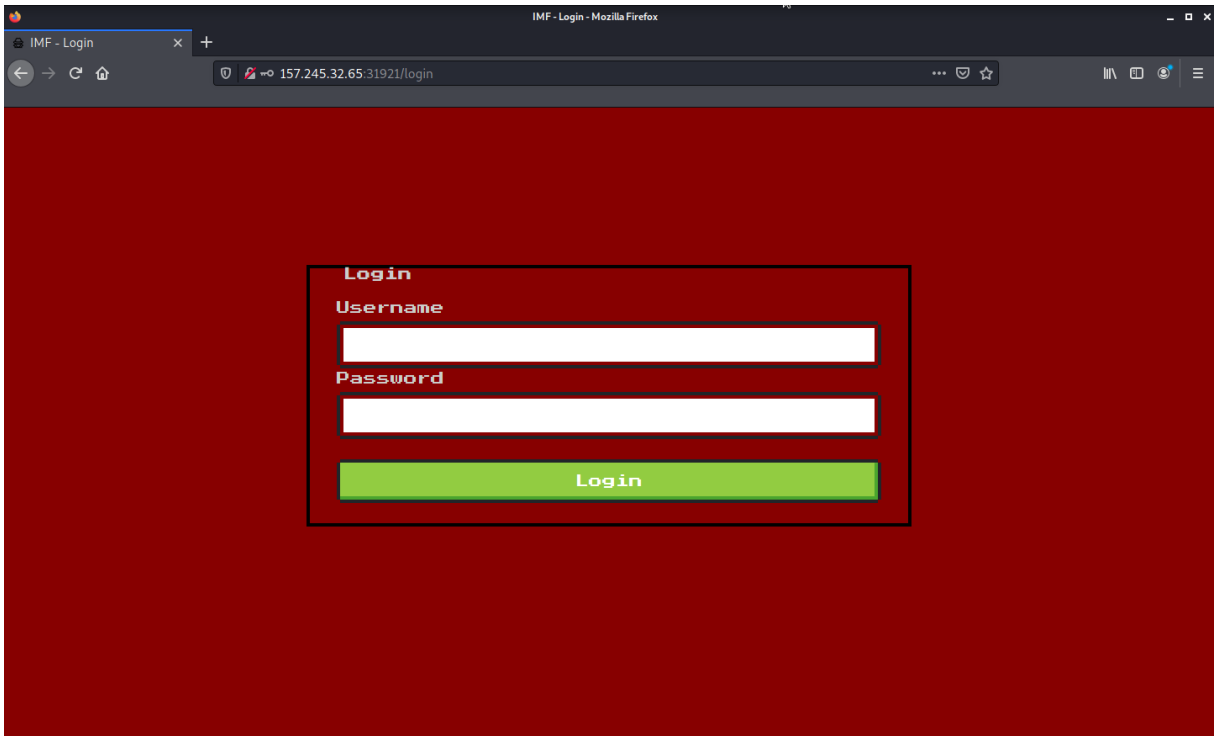


Figure 1: esqueelle0.png

First thing we can try is a SQL injection using `admin'or 1=1--` as the username and any character for the password (I'll be using `a` in this case).

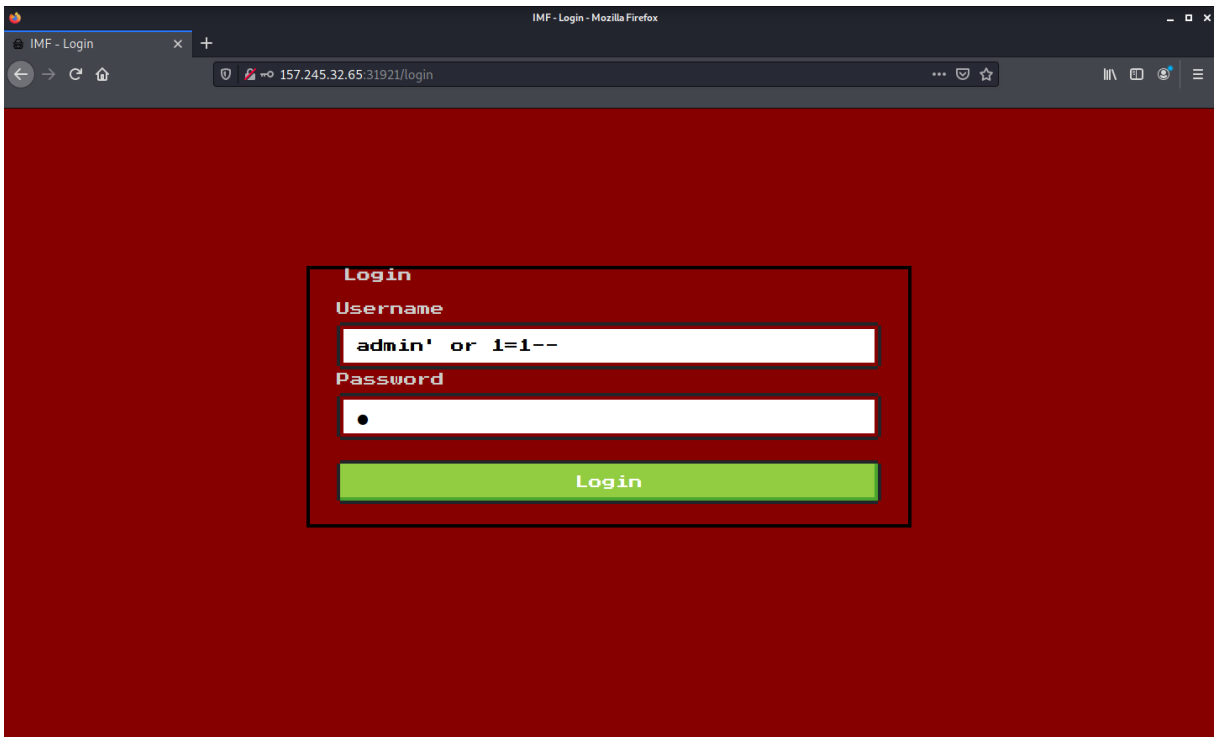


Figure 2: esqueelle1.png

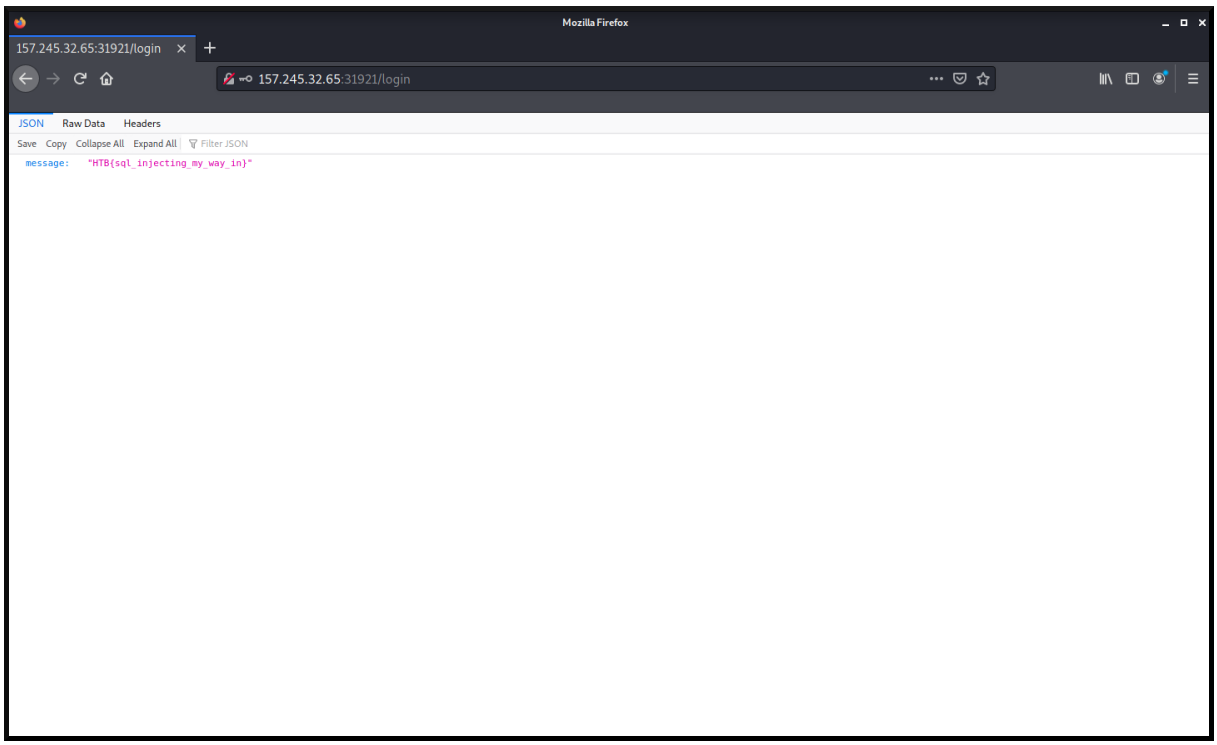


Figure 3: esqueelle2.png

Hooray, the login page is definitely vulnerable to SQL injections! The flag is HTB{sql_injecting_my_way_in}.

REVERSING - baby ransom

> One of your colleagues has downloaded this binary and after running it, all your files under ~/Documents have been encrypted inside a .zip file. You have to find the .zip password or pay 200k in order to decrypt them. p.s. All files are just copied and not moved/deleted just for the challenge.

From the challenge information, it says that everything under ~/Documents will be zipped and encrypted. So maybe if there were to be nothing in ~/Documents then the zip command will throw an error.

In my ~/Documents directory, I made sure that nothing was inside, then I executed the binary.

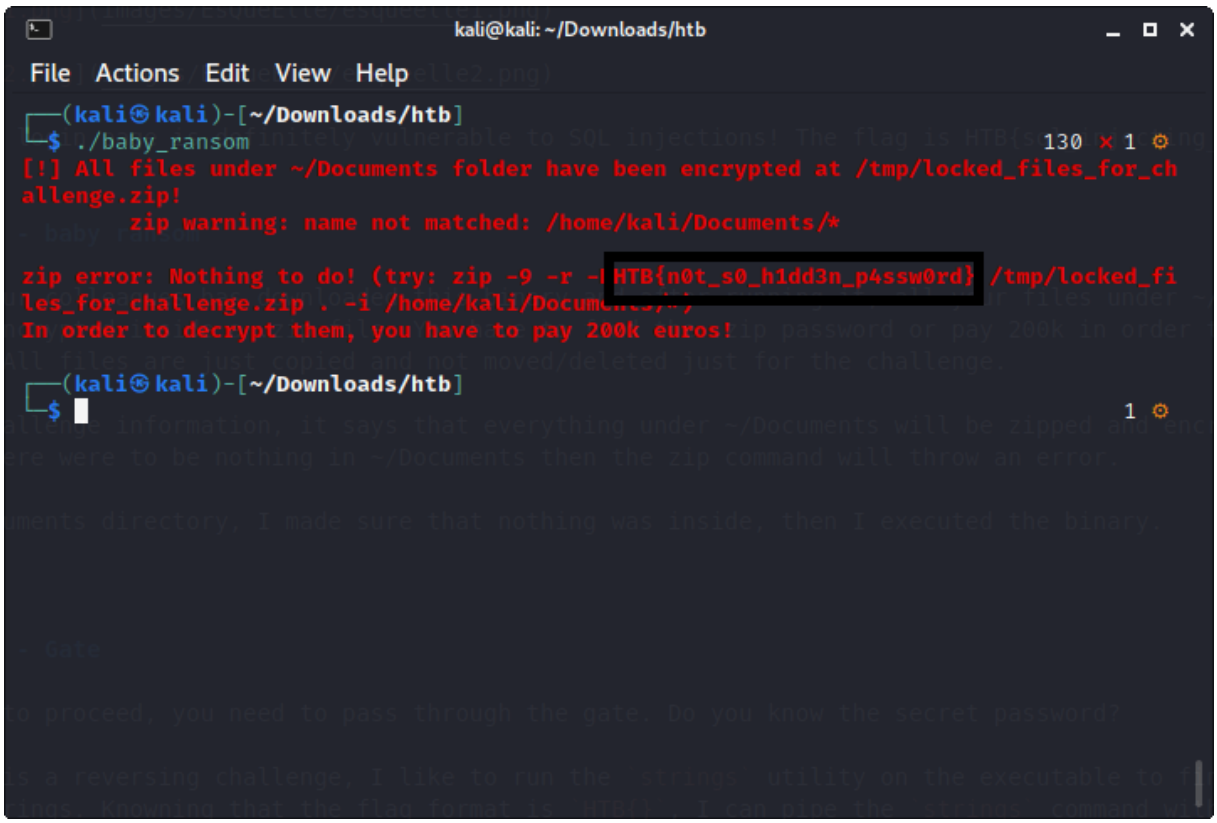


Figure 4: babyransom.png

Nice, seems like the zip command that is used does return an error, where we can see the password that was used is HTB{n0t_s0_h1dd3n_p4ssw0rd}.

REVERSING - Gate

> In order to proceed, you need to pass through the gate. Do you know the secret password?

Since this is a reversing challenge, I like to run the `strings` utility on the executable to find any readable strings. Knowning that the flag format is `HTB{}`, I can pipe the `strings` command with `grep`.

```
kali@kali:~$ strings gate | grep HTB
HTB{s3cr3t_p455w0rd_1n_str1ngs}
```

Yay, the execuatable's passphrase is revealed and it's HTB{s3cr3t_p455w0rd_1n_str1ngs}.

FORENSICS - Log

> I recently found a file in my personal folder which is not mine. I dont know what it is but I hope that none messed with my PC.

TODO

FORENSICS - Compromised

> Along with the previous attack, we suspect that there were more following. They believe that they can gain access to every system we own without being detected. Do they have enough skills? Find the attacker's IP Find the malicious's process ID Find the timestamp that the malicious process had been initiated Flag format: HTB{attacker's-IP_malicious-proc-ID_YYYY-MM-DD_HH:MM:SS} Mirror: 165.22.118.226/forensics_compromised.tar.gz

After decompressing this archive file, I noticed that its a `.raw` file so I instantly thought of using Volatility.

First, let's determine the profile.

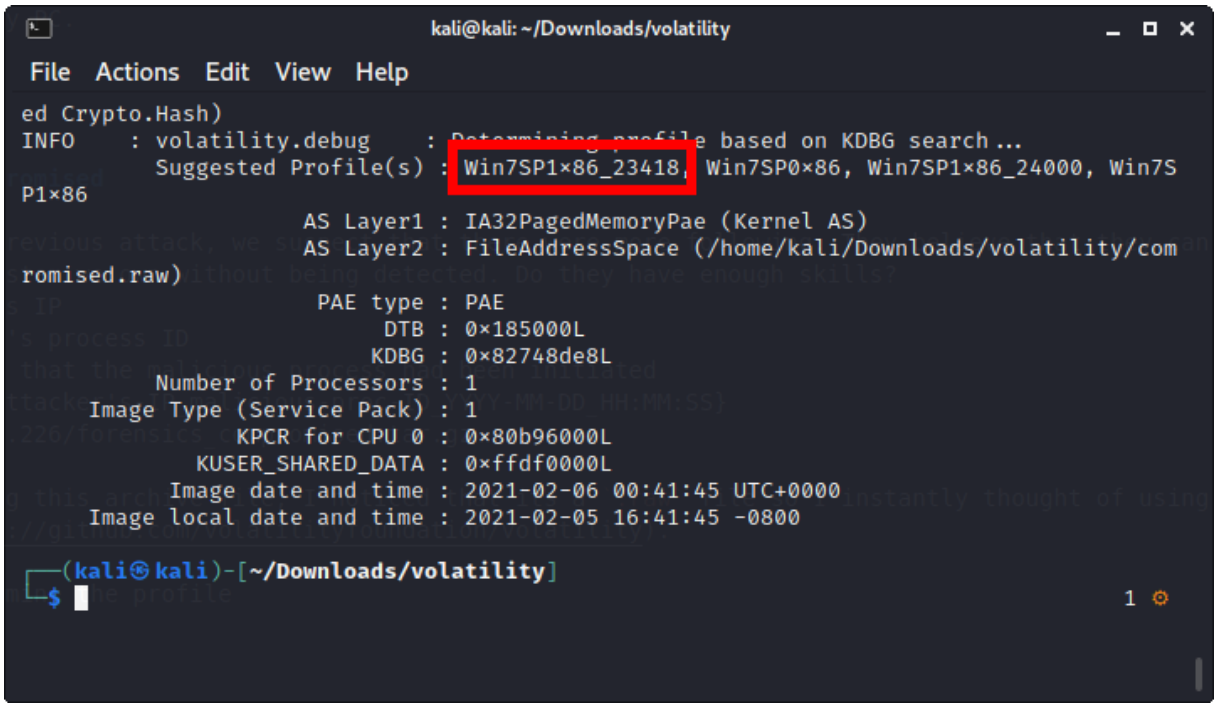


Figure 5: compromised0.png

We can now set the profile as `Win7SP1x86_23418` and then list the command line commands using `cmdline`.

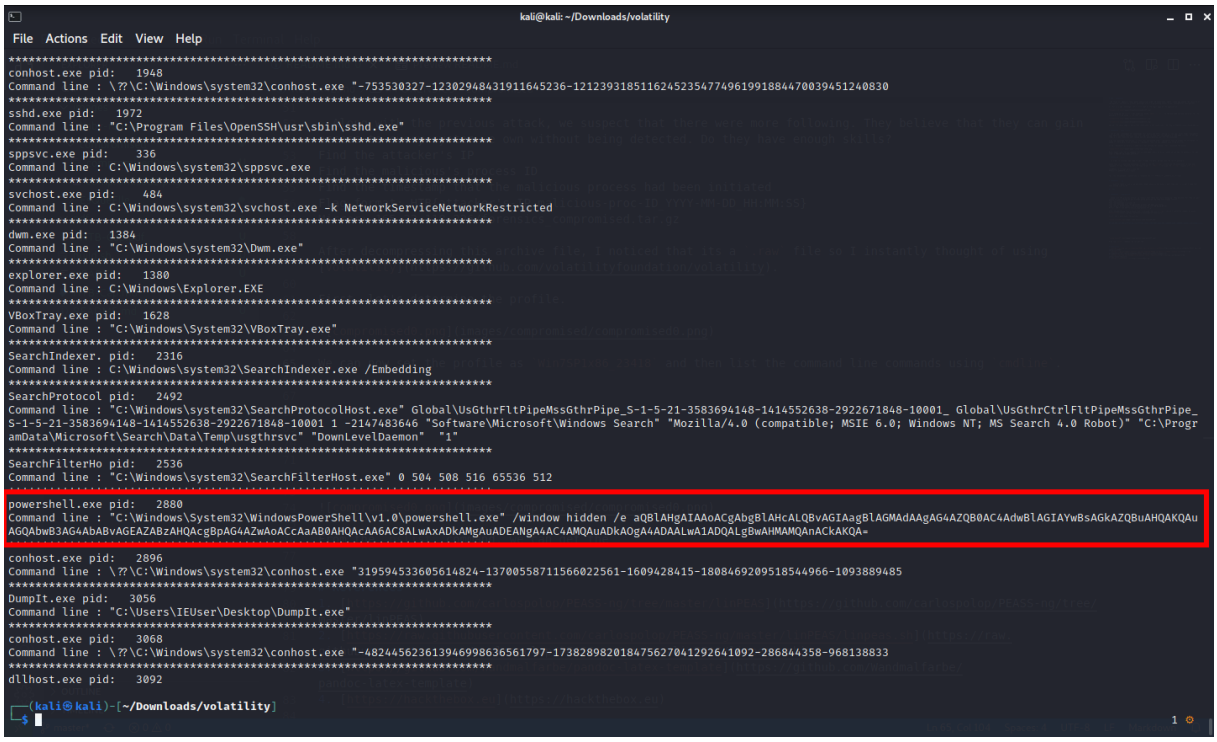


Figure 6: compromised1.png

From the `cmdline` command, we can see that a `powershell.exe` was ran, and a base64 encoded string was passed to it.

`aQBlAHgAIAAoACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAKQAuAGQA`
`=`

We can try to decode it using CyberChef.

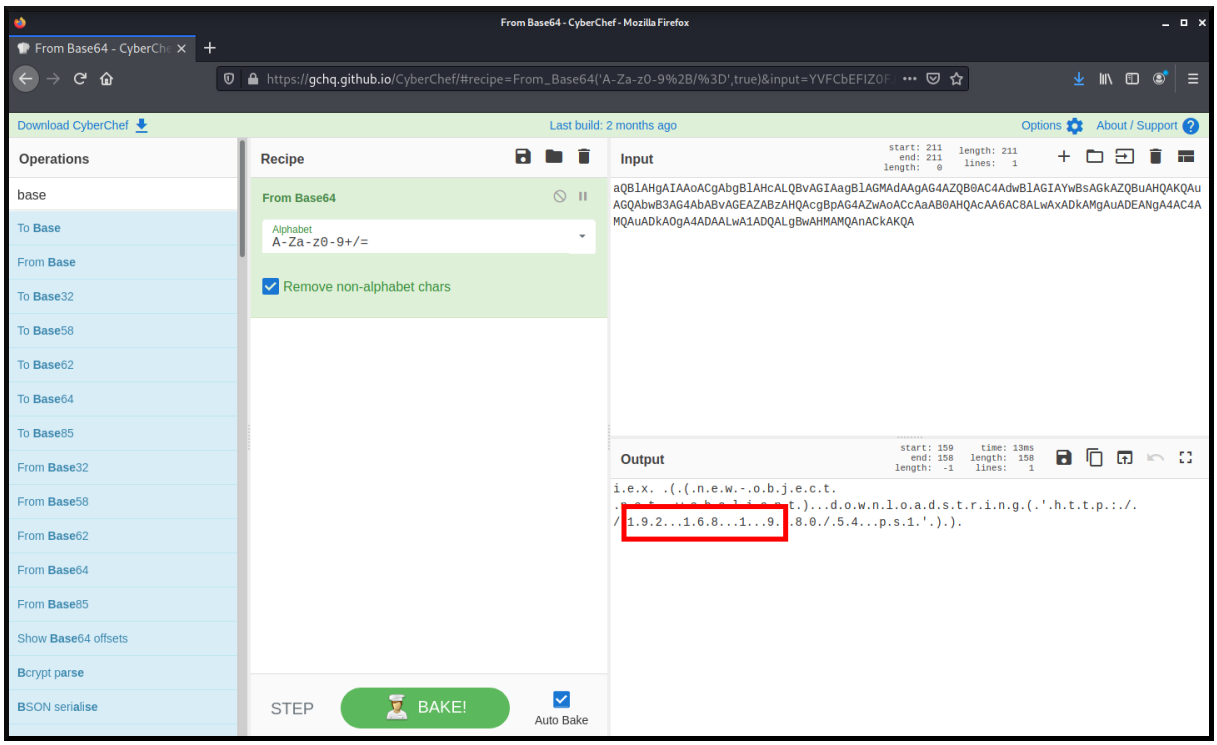
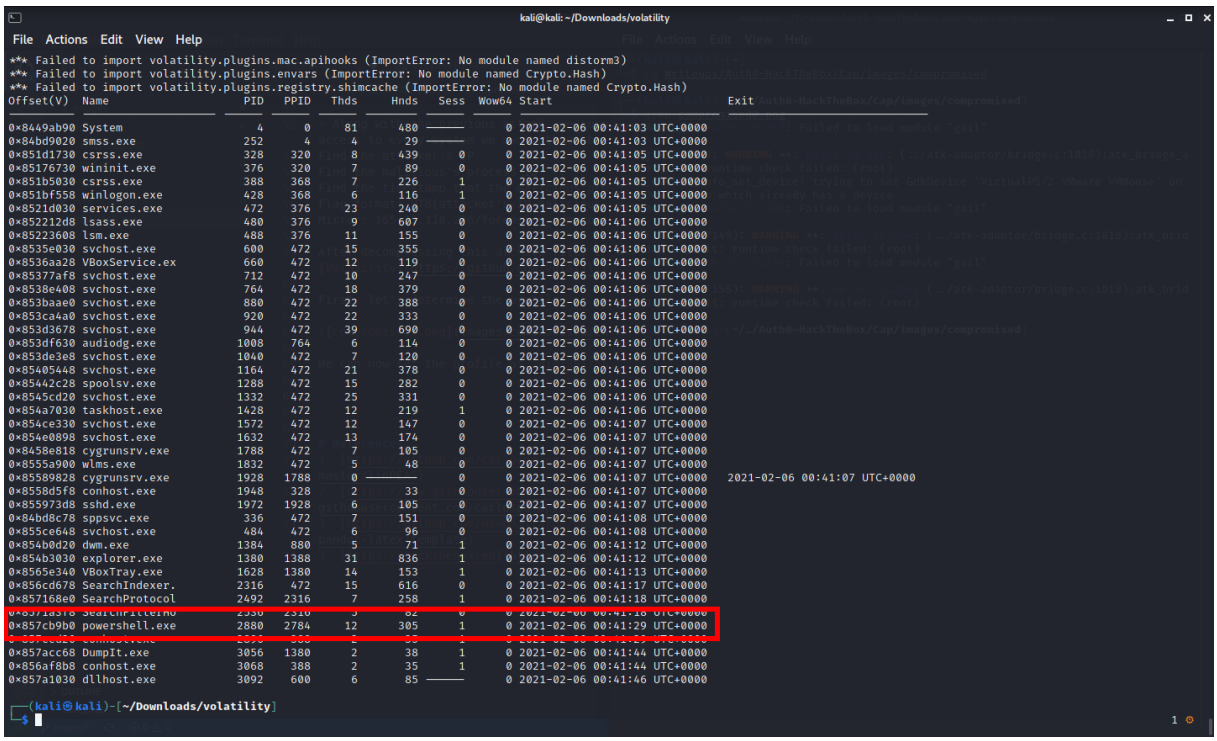


Figure 7: compromised2.png

After decoding the base64 strings, we can see that the attackers IP address is `192.168.1.9`.

Now we need to get the timestamp of this command being run. To do that, we can use Volatility's `pslist` command. With this command you can also reveal the process ID.



```
kali@kali: ~/Downloads/volatility
File  Actions  Edit  View  Help
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- ------------------ ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x8449ab90 System                    4      0     81      480 ------      0 2021-02-06 00:41:03 UTC+0000
0x84bd9020 smss.exe                252      4      4       29 ------      0 2021-02-06 00:41:03 UTC+0000
0x851d1730 csrss.exe               328    320      8      439      0      0 2021-02-06 00:41:05 UTC+0000
0x85176730 wininit.exe             376    320      7       89      0      0 2021-02-06 00:41:05 UTC+0000
0x851b5030 csrss.exe               388    368      7      226      1      0 2021-02-06 00:41:05 UTC+0000
0x851bf558 winlogon.exe            428    368      6      116      1      0 2021-02-06 00:41:05 UTC+0000
0x8521d030 services.exe            472    376     23      240      0      0 2021-02-06 00:41:05 UTC+0000
0x852212d8 lsass.exe               480    376      9      607      0      0 2021-02-06 00:41:06 UTC+0000
0x85223608 lsm.exe                 488    376     11      155      0      0 2021-02-06 00:41:06 UTC+0000
0x8535e030 svchost.exe             600    472     15      355      0      0 2021-02-06 00:41:06 UTC+0000
0x8536aa28 VBoxService.ex          660    472     12      119      0      0 2021-02-06 00:41:06 UTC+0000
0x85377af8 svchost.exe             712    472     10      247      0      0 2021-02-06 00:41:06 UTC+0000
0x8538e408 svchost.exe             764    472     18      379      0      0 2021-02-06 00:41:06 UTC+0000
0x853baae0 svchost.exe             880    472     22      388      0      0 2021-02-06 00:41:06 UTC+0000
0x853ca4a0 svchost.exe             920    472     22      333      0      0 2021-02-06 00:41:06 UTC+0000
0x853d3678 svchost.exe             944    472     39      690      0      0 2021-02-06 00:41:06 UTC+0000
0x853df630 audiodg.exe            1008    764      6      114      0      0 2021-02-06 00:41:06 UTC+0000
0x853de3e8 svchost.exe            1040    472      7      120      0      0 2021-02-06 00:41:06 UTC+0000
0x85405448 svchost.exe            1164    472     21      378      0      0 2021-02-06 00:41:06 UTC+0000
0x85442c28 spoolsv.exe            1288    472     15      282      0      0 2021-02-06 00:41:06 UTC+0000
0x8545cd20 svchost.exe            1332    472     25      331      0      0 2021-02-06 00:41:06 UTC+0000
0x854a7030 taskhost.exe           1428    472     12      219      1      0 2021-02-06 00:41:06 UTC+0000
0x854ce330 svchost.exe            1572    472     12      147      0      0 2021-02-06 00:41:07 UTC+0000
0x854e0898 svchost.exe            1632    472     13      174      0      0 2021-02-06 00:41:07 UTC+0000
0x8458e818 cygrunsrv.exe          1788    472      7      105      0      0 2021-02-06 00:41:07 UTC+0000
0x8555a900 wlms.exe               1832    472      5       48      0      0 2021-02-06 00:41:07 UTC+0000
0x85589828 cygrunsrv.exe          1928   1788      0 --------      0      0 2021-02-06 00:41:07 UTC+0000   2021-02-06 00:41:07 UTC+0000
0x8558d5f8 conhost.exe            1948    328      2       33      0      0 2021-02-06 00:41:07 UTC+0000
0x855973d8 sshd.exe               1972   1928      6      105      0      0 2021-02-06 00:41:07 UTC+0000
0x84bd8c78 sppsvc.exe              336    472      7      151      0      0 2021-02-06 00:41:08 UTC+0000
0x855ce648 svchost.exe             484    472      6       96      0      0 2021-02-06 00:41:08 UTC+0000
0x854b0d20 dwm.exe                1384    880      5       71      1      0 2021-02-06 00:41:12 UTC+0000
0x854b3030 explorer.exe           1380   1388     31      836      1      0 2021-02-06 00:41:12 UTC+0000
0x8565e340 VBoxTray.exe           1628   1380     14      153      1      0 2021-02-06 00:41:13 UTC+0000
0x856cd678 SearchIndexer.         2316    472     15      616      0      0 2021-02-06 00:41:17 UTC+0000
0x857168e0 SearchProtocol         2492   2316      7      258      1      0 2021-02-06 00:41:18 UTC+0000
0x857cb9b0 powershell.exe         2880   2784     12      305      1      0 2021-02-06 00:41:29 UTC+0000
0x857acc68 DumpIt.exe             3056   1380      2       38      1      0 2021-02-06 00:41:44 UTC+0000
0x856af8b8 conhost.exe            3068    388      2       35      1      0 2021-02-06 00:41:44 UTC+0000
0x857a1030 dllhost.exe            3092    600      6       85 ------      0 2021-02-06 00:41:46 UTC+0000

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$
```

Figure 8: compromised3.png

Finally, we can now craft the flag using:

attacker's-IP == `192.168.1.9`, malicious-proc-ID == `2880`, YYYY-MM-DD == `2021-02-06`, HH:MM:SS == `00:41:29`

The flag is HTB{192.168.1.9_2880_2021-02-06_00:41:29}.

FORENSICS - Suspicious

TODO

References

1. https://gchq.github.io/CyberChef/
2. https://github.com/Wandmalfarbe/pandoc-latex-template
3. https://ctf.hackthebox.com/ctfs