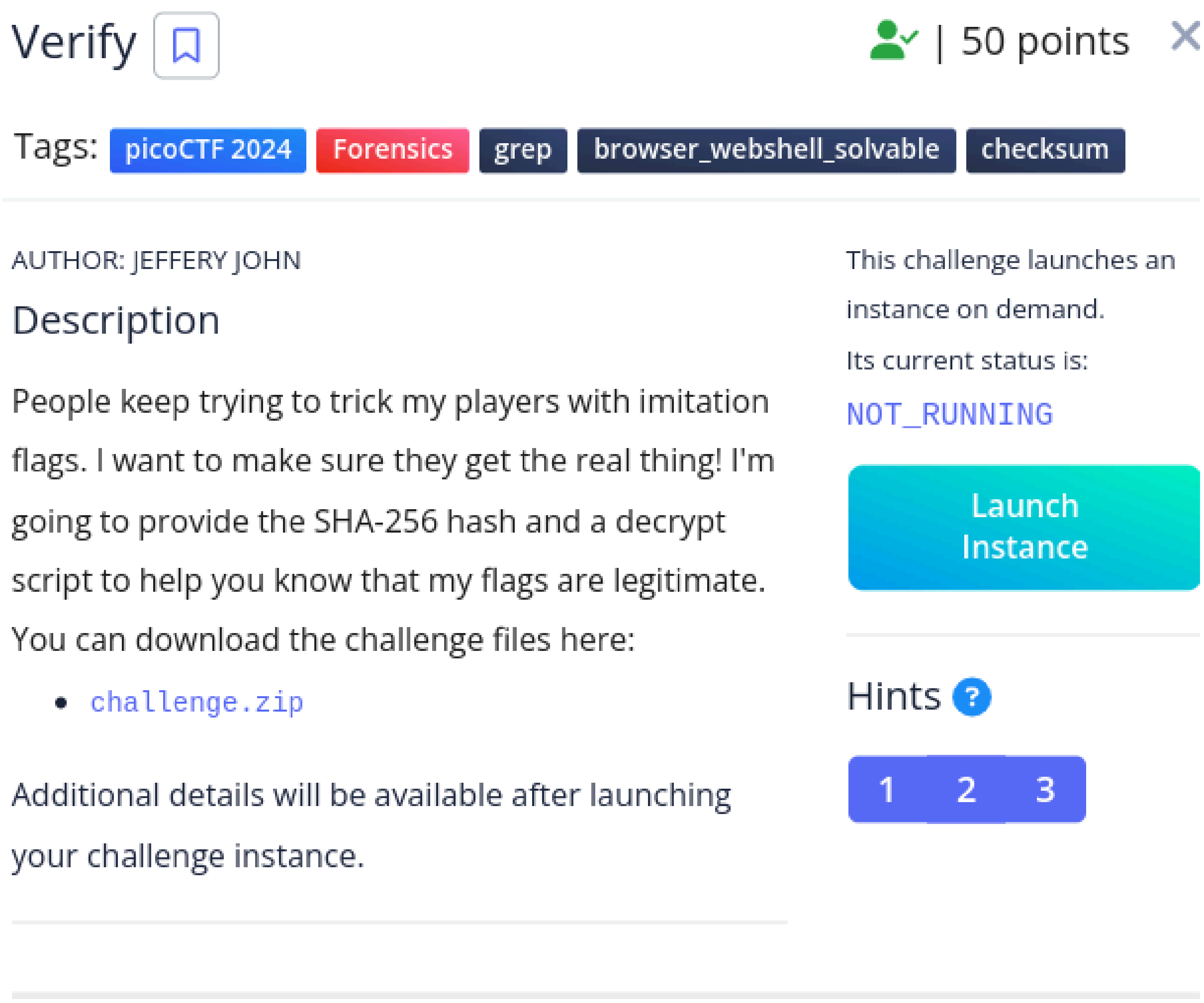
Verify

info about the challenge:



Verify

| 50 points

Tags: picoCTF 2024 Forensics grep browser_webshell_solvable checksum

AUTHOR: JEFFERY JOHN

Description

People keep trying to trick my players with imitation flags. I want to make sure they get the real thing! I'm going to provide the SHA-256 hash and a decrypt script to help you know that my flags are legitimate. You can download the challenge files here:

- challenge.zip

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is:

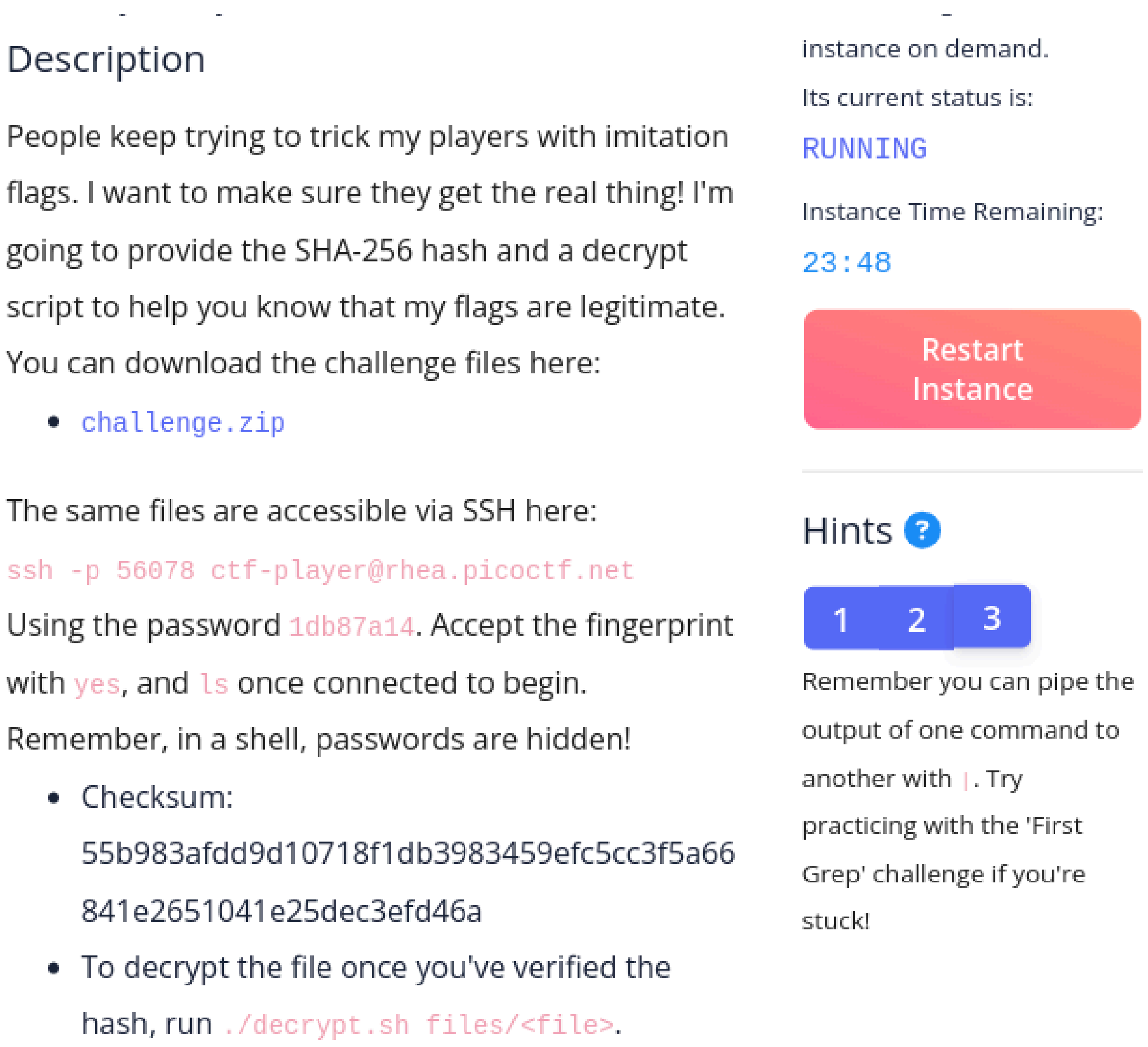
NOT_RUNNING

Description:

It's easy :>

Solution:

1/launch instance



Description

People keep trying to trick my players with imitation flags. I want to make sure they get the real thing! I'm going to provide the SHA-256 hash and a decrypt script to help you know that my flags are legitimate. You can download the challenge files here:

- challenge.zip

The same files are accessible via SSH here:

```
ssh -p 56078 ctf-player@rhea.picoctf.net
```

Using the password `1db87a14`. Accept the fingerprint with `yes`, and `ls` once connected to begin. Remember, in a shell, passwords are hidden!

- Checksum: 55b983afdd9d10718f1db3983459efc5cc3f5a66841e2651041e25dec3efd46a
- To decrypt the file once you've verified the hash, run `./decrypt.sh files/<file>`.

instance on demand.

Its current status is:

RUNNING

Instance Time Remaining:

23:48

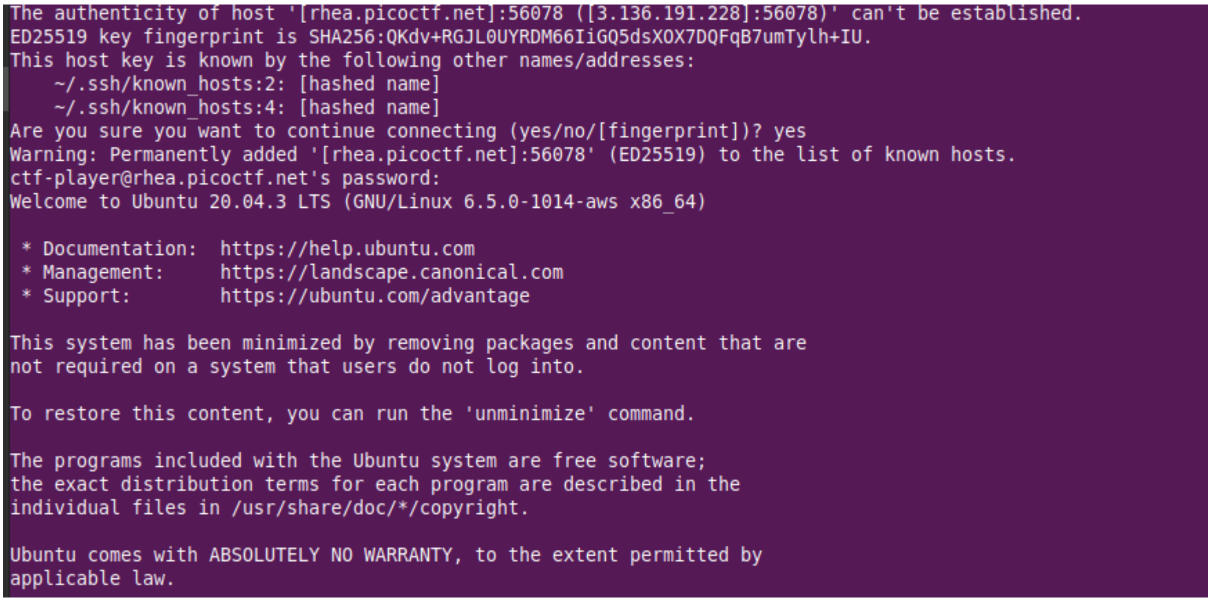
Hints

Remember you can pipe the output of one command to another with `|`. Try practicing with the 'First Grep' challenge if you're stuck!

2/run in terminal

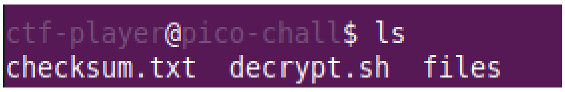
```
ssh -p <port> ctf-player@rhea.picoctf.net
```

3/tab yes and use the password that it gives you



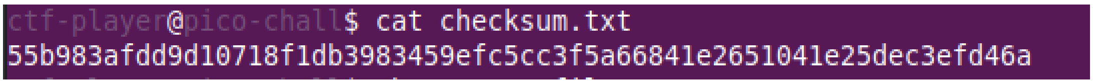
```
The authenticity of host '[rhea.picoctf.net]:56078 ([3.136.191.228]:56078)' can't be established.
ED25519 key fingerprint is SHA256:QKdv+RGJL0UYRDM66IiGQ5dsXOX7DQFqB7umTylh+IU.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[rhea.picoctf.net]:56078' (ED25519) to the list of known hosts.
ctf-player@rhea.picoctf.net's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 6.5.0-1014-aws x86_64)

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

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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

4/tab ls



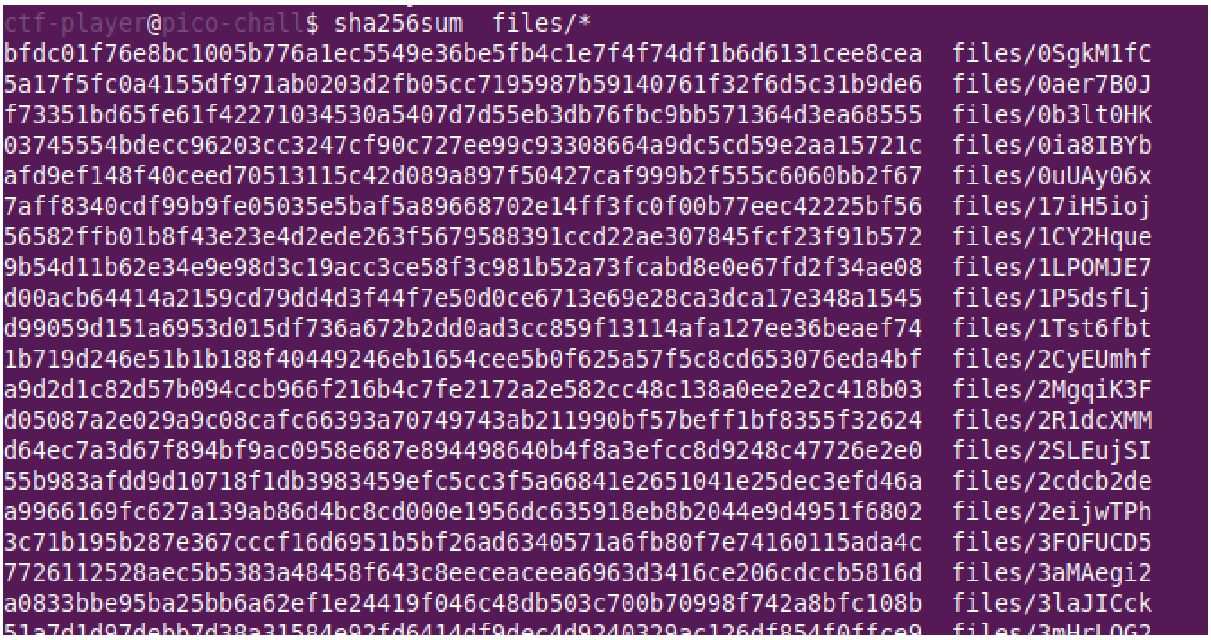
```
ctf-player@pico-chall$ ls
checksum.txt  decrypt.sh  files
```

5/check checksum.txt



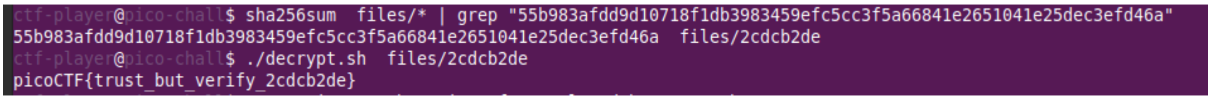
```
ctf-player@pico-chall$ cat checksum.txt
55b983afdd9d10718f1db3983459efc5cc3f5a66841e2651041e25dec3efd46a
```

6/check all files using this command sha256sum



```
ctf-player@pico-chall$ sha256sum  files/*
bfdc01f76e8bc1005b776a1ec5549e36be5fb4c1e7f4f74df1b6d6131cee8cea  files/0SgkM1fC
5a17f5fc0a4155df971ab0203d2fb05cc7195987b59140761f32f6d5c31b9de6  files/0aer7B0J
f73351bd65fe61f42271034530a5407d7d55eb3db76fbc9bb571364d3ea68555  files/0b3lt0HK
03745554bdecc96203cc3247cf90c727ee99c93308664a9dc5cd59e2aa15721c  files/0ia8IBYb
afd9ef148f40ceed70513115c42d089a897f50427caf999b2f555c6060bb2f67  files/0uUAy06x
7aff8340cdf99b9fe05035e5baf5a89668702e14ff3fc0f00b77eec42225bf56  files/17iH5ioj
56582ffb01b8f43e23e4d2ede263f5679588391ccd22ae307845fcf23f91b572  files/1CY2Hque
9b54d11b62e34e9e98d3c19acc3ce58f3c981b52a73fcabd8e0e67fd2f34ae08  files/1LPOMJE7
d00acb64414a2159cd79dd4d3f44f7e50d0ce6713e69e28ca3dca17e348a1545  files/1P5dsfLj
d99059d151a6953d015df736a672b2dd0ad3cc859f13114afa127ee36beaef74  files/1Tst6fbt
1b719d246e51b1b188f40449246eb1654cee5b0f625a57f5c8cd653076eda4bf  files/2CyEUmhf
a9d2d1c82d57b094ccb966f216b4c7fe2172a2e582cc48c138a0ee2e2c418b03  files/2MgqiK3F
d05087a2e029a9c08cafc66393a70749743ab211990bf57beff1bf8355f32624  files/2R1dcXMM
d64ec7a3d67f894bf9ac0958e687e894498640b4f8a3efcc8d9248c47726e2e0  files/2SLEujSI
55b983afdd9d10718f1db3983459efc5cc3f5a66841e2651041e25dec3efd46a  files/2cdcb2de
a9966169fc627a139ab86d4bc8cd000e1956dc635918eb8b2044e9d4951f6802  files/2eijwTPh
3c71b195b287e367cccf16d6951b5bf26ad6340571a6fb80f7e74160115ada4c  files/3FOFUCD5
7726112528aec5b5383a48458f643c8eeceaceea6963d3416ce206cdccb5816d  files/3aMAegi2
a0833bbe95ba25bb6a62ef1e24419f046c48db503c700b70998f742a8bfc108b  files/3laJICck
51a7d1d97debb7d38a31584e92fd6414df9dec4d9240329ac126df854f0ffce9  files/3mHrLOG2
```

7/use it now for the SHA-256 that you find it in checksum.txt and run the command indicated in the challenge now



```
ctf-player@pico-chall$ sha256sum  files/* | grep "55b983afdd9d10718f1db3983459efc5cc3f5a66841e2651041e25dec3efd46a"
55b983afdd9d10718f1db3983459efc5cc3f5a66841e2651041e25dec3efd46a  files/2cdcb2de
ctf-player@pico-chall$ ./decrypt.sh  files/2cdcb2de
picoCTF{trust_but_verify_2cdcb2de}
```

THE FLAG:

picoCTF{trust_but_verify_2cdcb2de}