Where Am I

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Linux
Challenge | 2020 | CSICTF | Linux | Where Am I

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/linux/2020/07/22/Where-Am-I.html

by `vishalananth`

题目描述

> *Something is not right? I feel like I am in a prison!*

题目考点

解题思路

We netcat into the given ip and see that we are inside a Linux shell. We try going to the topmost directory and printing all files, but we did not get the flag. So we start inspecting things inside the shell one by one. We notice that, we are able to access the `/root` *directory. Inside that we see the* `.ssh` *directory with the SSH public and private keys.*

We notice that the public key and authorized key files contain the same key. Seeing this we realize that `root` *user can ssh into the machine without needing any password. So we try*

```
ssh root@localhost 2>&1
```

We see the error message and realize that it is checking for .ssh keys in `ctf` *user's repo. So we try explicity mentioning the root user's public key with:*

```
ssh -i /root/.ssh/id_rsa root@localhost
```

But, it still does not work. When trying to reproduce this in our local machine, we find that whenever we ssh for the first time, there is a prompt which appears, where we need to agree by typing `yes` *to add the system to the known hosts. So we try to supress the host checking with:*

```
ssh -i /root/.ssh/id_rsa -o StrictHostKeyChecking=no root@localhost
```

It worked and gave us the flag.

Flag

```
csictf{n1c3_d093_w0w_5uch_55h}
```

- *本文作者：* *CTFHub*
- *本文链接：* *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Linux/ven8mEkG5h8vTDCQ8Jxom4.html*
-

# Challenge # 2020 # Linux # CSICTF
find32
HTB 0x[2-6]